ESET Internet Security

Vartotojo vadovas

Jei norite peržiūrėti šio dokumento internetinę versiją spustelėkite čia

Digital Security
Progress. Protected.

ESET Internet Security sukūrė ESET, spol. s r.o.

Norėdami gauti daugiau informacijos, apsilankykite https://www.eset.com.

Techninė pagalba: https://support.eset.com

REV. 2024.4.12

1 ESET Internet Security 1
1.1 Kas naujo? 2
1.2 Kokį produktą naudoju? 2
1.3 Sistemos reikalavimai 3
1.3 Pasenusi „Microsoft Windows“ versija 4
1.4 Prevencija 5
1.5 Žinyno puslapiai 6
2 Diegimas 7
2.1 Tiesioginio diegimo programa 7
2.2 Diegimas neprisijungus 9
2.2 Prenumeratos naujovinimas 10
2.2 Produkto keitimas į aukštesnę versiją 11
2.2 Prenumeratos pakeitimas į ankstesnę versiją 12
2.2 Produkto keitimas į žemesnę versiją 13
2.3 Diegimo trikčių diagnostikos priemonė 14
2.4 Pirmas nuskaitymas po diegimo 14
2.5 Naujinimas į naujesnę versiją 15
2.5 Senojo produkto automatinis naujinimas 15
2.5 ESET Internet Security bus įdiegta 16
2.5 Keisti į kitą produktų liniją 16
2.5 Registracija 16
2.5 Aktyvinimo eiga 16
2.5 Sėkmingai suaktyvinta 16
3 Pradžia 16
3.1 Sistemos dėklo piktograma 17
3.2 Spartieji klavišai 17
3.3 Profiliai 18
3.4 Naujinimai 19
3.5 Tinklo apsaugos konfigūravimas 21
3.6 Įjungti Anti-Theft 22
3.7 Tėvų kontrolė 23
4 Produkto aktyvinimas 23
4.1 Aktyvinimo rakto įvedimas aktyvinimo metu 24
4.2 Naudoti ESET HOME paskyrą 24
4.3 Aktyvinti nemokamą bandomąją versiją 25
4.4 Nemokamas ESET aktyvinimo raktas 26
4.5 Aktyvinti nepavyko – dažniausi scenarijai 26
4.6 Prenumeratos būsena 27
4.6 Aktyvinti nepavyko dėl pereikvotos prenumeratos 28
5 Darbas su ESET Internet Security 29
5.1 Apžvalga 30
5.2 Kompiuterio nuskaitymas 33
5.2 Pasirinktinio nuskaitymo paleidimo priemonė 35
5.2 Nuskaitymo eiga 37
5.2 Kompiuterio nuskaitymo žurnalas 39
5.3 Naujinti 41
5.3 Dialogo langas – būtina paleisti iš naujo 43
5.3 Kaip sukurti naujinimo užduotis 43
5.4 Įrankiai 44
5.4 Žurnalo failai 45

5.4 Žurnalo filtravimas 48
5.4 Vykdomi procesai 49
5.4 Saugumo ataskaita 51
5.4 Tinklo ryšiai 53
5.4 Tinklo veikla 54
5.4 ESET SysInspector 55
5.4 Planuoklė 56
5.4 Suplanuoto nuskaitymo parinktys 58
5.4 Suplanuotų užduočių apžvalga 59
5.4 Užduoties informacija 59
5.4 Užduočių sinchronizacija 60
5.4 Užduoties laikas – vieną kartą 60
5.4 Užduoties laikas – kasdien 60
5.4 Užduoties laikas – kas savaitę 60
5.4 Užduoties laikas – suaktyvintas įvykis 60
5.4 Praleista užduotis 61
5.4 Išsami užduoties informacija – naujinti 61
5.4 Išsami užduoties informacija – Vykdyti taikomąją programą 61
5.4 Sistemos valymo priemonė 62
5.4 Tinklo tikrinimo įrankis 63
5.4 Tinklo įrenginys Tinklo tikrinimo įrankyje 66
5.4 Pranešimai | Tinklo tikrinimo įrankis 67
5.4 Karantinas 67
5.4 Pasirinkti mėginį analizei 70
5.4 Pasirinkti pavyzdį analizei – įtartinas failas 71
5.4 Pasirinkti pavyzdį analizei – įtartinas svetainė 71
5.4 Pasirinkti pavyzdį analizei – klaidingai aptiktas failas 71
5.4 Pasirinkti pavyzdį analizei – klaidingai aptikta svetainė 72
5.4 Pasirinkti pavyzdį analizei – kitas 72
5.5 Nustatymai 72
5.5 Kompiuterio apsauga 73
5.5 Aptiktas įsiskverbimas 75
5.5 Interneto apsauga 78
5.5 Apsauga nuo sukčiavimo apsimetant 79
5.5 Tėvų kontrolė 81
5.5 Svetainių išimtys 83
5.5 Kopijuoti išimtį iš naudotojo 85
5.5 Kopijuoti kategorijas iš paskyros 85
5.5 Tinklo apsauga 85
5.5 Tinklo ryšiai 86
5.5 Išsami tinklo ryšio informacija 87
5.5 Tinklo prieigos trikčių šalinimas 88
5.5 Laikinas IP adresų juodasis sąrašas 88
5.5 Tinklo apsaugos žurnalai 89
5.5 Užkardos problemų sprendimas 90
5.5 Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo 90
5.5 Sukurti taisyklę iš žurnalo 91
5.5 Išimčių kūrimas iš asmeninės užkardos pranešimų 91
5.5 Tinklo apsaugos išplėstinį registravimą 91
5.5 Tinklo duomenų srauto skaitytuvo problemų sprendimas 92
5.5 Užblokuota tinklo grėsmė 93

5.5 Aptiktas naujas tinklas ... 93
5.5 Ryšio nustatymas – aptikimas ... 94
5.5 Programos keitimas ... 96
5.5 Gaunamas patikimas ryšys ... 96
5.5 Siunčiamas patikimas ryšys ... 97
5.5 Gaunamas ryšys ... 99
5.5 Siunčiamas ryšys ... 100
5.5 Ryšio rodinio nustatymas ... 101
5.5 Saugumo priemonės ... 102
5.5 Saugi bankininkystė ir naršymas ... 102
5.5 Naršyklės pranešimas ... 103
5.5 Naršyklės privatumas ir sauga ... 103
5.5 Anti-Theft ... 105
5.5 Prisijungti prie savo ESET HOME paskyros. ... 107
5.5 Nustatyti įrenginio pavadinimą ... 108
5.5 Anti-Theft įgalinta / išjungta ... 108
5.5 Nepavyko pridėti naujo įrenginio ... 108
5.5 Parametrų importavimas ir eksportavimas ... 109
5.6 Žinynas ir palaikymas ... 110
5.6 Apie ESET Internet Security ... 110
5.6 ESET naujienos ... 111
5.6 Sistemos konfigūracijos duomenų pateikimas ... 112
5.6 Techninė pagalba ... 112
5.7 „ESET HOME“ paskyra ... 113
5.7 Prisijunkite prie „ESET HOME“ ... 114
5.7 Prisijungti prie ESET HOME ... 115
5.7 Prisijungti nepavyko – dažniausios klaidos ... 116
5.7 Įtraukti įrenginį į ESET HOME ... 117
6 Išplėstiniai nustatymai ... 117
6.1 Aptikimo modulis ... 118
6.1 Išimtys ... 119
6.1 Našumo išimtys ... 119
6.1 Pridėti arba redaguoti našumo išimtis ... 120
6.1 Kelio išskyrimo formatas ... 122
6.1 Aptikimo išimtys ... 122
6.1 Pridėti arba redaguoti aptikimo išimtį ... 124
6.1 Aptikimo išimčių kūrimo vedlys vedlį ... 125
6.1 Aptikimo modulio išplėstinės parinktys ... 126
6.1 Tinklo duomenų srauto skaitytuvas ... 126
6.1 Debesimi paremta apsauga ... 126
6.1 Debesimi paremtos apsaugos išimčių filtras ... 129
6.1 Kenkėjiškų programų nuskaitymai ... 129
6.1 Nuskaitymo profiliai ... 130
6.1 Nuskaitymo tikslai ... 130
6.1 Nuskaitymas laukimo būsenoje ... 131
6.1 Laukimo būsenos aptikimas ... 132
6.1 Nuskaitymas paleidžiant ... 132
6.1 Automatinė paleidimo failo patikra ... 132
6.1 Nešiojamoji laikmena ... 133
6.1 Dokumentų apsauga ... 134
6.1 HIPS – Įsibrovimo į pagrindinį kompiuterį prevencijos sistema ... 134

6.1 HIPS išskyrimai ... 137
6.1 HIPS išplėstinis nustatymai ... 137
6.1 Tvarkyklės, kurias leidžiama įkelti visada ... 137
6.1 HIPS interaktyvusis langas ... 138
6.1 Mokymosi režimas užbaigtas ... 139
6.1 Aptiktas potencialus „Ransomware“ viruso elgesys ... 139
6.1 HIPS taisyklių tvarkymas ... 140
6.1 HIPS taisyklės parametrai ... 141
6.1 Pridėti programos / registro kelią HIPS ... 144
6.2 Naujinti ... 144
6.2 Naujinimo atšaukimas ... 146
6.2 Grąžinimo laiko intervalas ... 148
6.2 Produkto naujinimai ... 148
6.2 Ryšio parinktys ... 148
6.3 Apsaugos priemonės ... 149
6.3 Failų sistemos apsauga realiuoju laiku ... 152
6.3 Procesų išimtys ... 154
6.3 Pridėti arba redaguoti procesų išskyrimus ... 155
6.3 Kada keisti apsaugos realiuoju laiku konfigūraciją ... 155
6.3 Apsaugos realiuoju laiku tikrinimas ... 155
6.3 Ką daryti, jeigu apsauga realiuoju laiku neveikia ... 156
6.3 Tinklo prieigos apsauga ... 156
6.3 Tinklo ryšio profiliai ... 157
6.3 Tinklo ryšio profilių pridėjimas arba redagavimas ... 158
6.3 Aktyvatoriai ... 159
6.3 IP rinkiniai ... 161
6.3 IP rinkinių redagavimas ... 161
6.3 Tinklo tikrinimo įrankis ... 162
6.3 Užkarda ... 163
6.3 Mokymosi režimo nuostatos ... 165
6.3 Užkardos taisyklės ... 166
6.3 Užkardos taisyklių įtraukimas arba redagavimas ... 167
6.3 Programos modifikavimo aptikimas ... 170
6.3 Neaptinkamų programų sąrašas ... 170
6.3 Apsauga nuo atakos iš tinklo (IDS) ... 171
6.3 IDS taisyklės ... 171
6.3 Apsauga nuo grubios jėgos atakų ... 174
6.3 Taisyklės ... 175
6.3 Išplėstinės parinktys ... 177
6.3 SSL/TLS ... 178
6.3 Programos nuskaitymo taisyklės ... 180
6.3 Sertifikavimo taisyklės ... 181
6.3 Šifruotas tinklo srautas ... 182
6.3 El. pašto programų apsauga ... 182
6.3 Pašto perdavimo apsauga ... 182
6.3 Neįtrauktos programos ... 184
6.3 Neįtraukti IP ... 185
6.3 Pašto dėžutės apsauga ... 186
6.3 Integravimo priemonės ... 188
6.3 „Microsoft Outlook“ įrankių juosta ... 188
6.3 Patvirtinimo dialogas ... 189

6.3 Nuskaityti iš naujo laiškus ... 189
6.3 Atsakas ... 189
6.3 Adresų sąrašų tvarkymas ... 190
6.3 Adresai sąrašas ... 191
6.3 Adreso pridėjimas / redagavimas ... 192
6.3 Adreso apdorojimo rezultatas ... 193
6.3 ThreatSense ... 193
6.3 Prieigos prie saityno apsauga ... 196
6.3 Neįtrauktos programos ... 198
6.3 Neįtraukti IP ... 199
6.3 URL adresų sąrašo tvarkymas ... 200
6.3 Adresų sąrašas ... 201
6.3 Naujo adresų sąrašo kūrimas ... 202
6.3 Kaip pridėti URL kaukę ... 203
6.3 HTTP(S) srauto nuskaitymas ... 204
6.3 ThreatSense ... 204
6.3 Tėvų kontrolė ... 207
6.3 Vartotojo paskyros ... 207
6.3 Naudotojo paskyros nustatymai ... 208
6.3 Kategorijos ... 210
6.3 Naršyklės apsauga ... 211
6.3 Saugi bankininkystė ir naršymas ... 211
6.3 Įrenginio kontrolė ... 212
6.3 Įrenginio kontrolės taisyklių rengyklė ... 213
6.3 Aptikti įrenginiai ... 214
6.3 Įrenginio kontrolės taisyklių pridėjimas ... 214
6.3 Įrenginių grupės ... 217
6.3 Interneto kameros apsauga ... 218
6.3 Interneto kameros apsaugos taisyklių rengyklė ... 219
6.3 ThreatSense ... 219
6.3 Valymo lygiai ... 222
6.3 Failų plėtiniai, kurie nebus nuskaitomi ... 223
6.3 Papildomi „ThreatSense“ parametrai ... 223
6.4 Įrankiai ... 224
6.4 „Microsoft Windows®“ naujinimas ... 224
6.4 Dialogo langas – sistemos naujinimai ... 225
6.4 Naujinimo informacija ... 225
6.4 ESET CMD ... 225
6.4 Žurnalo failai ... 227
6.4 Žaidimų režimas ... 228
6.4 Diagnostika ... 228
6.4 Techninė pagalba ... 230
6.5 Junglumas ... 230
6.6 Vartotojo sąsaja ... 231
6.6 Naudotojo sąsajos elementai ... 231
6.6 Prieigos nustatymas ... 232
6.6 Išplėstinio nustatymo slaptažodis ... 233
6.6 Ekrano skaitytuvo palaikymas ... 234
6.7 Pranešimai ... 234
6.7 Dialogo langas – programos būsenos ... 235
6.7 Darbalaukio pranešimai ... 235

6.7 Darbalaukio pranešimų sąrašas 237
6.7 Interaktyvūs įspėjimai 238
6.7 Patvirtinimo pranešimai 240
6.7 Peradresavimas 241
6.8 Privatumo parametrai 243
6.8 Numatytųjų parametrų grąžinimas 244
6.8 Atkurti visus esamojo skyriaus parametrus 244
6.8 Klaida išsaugant konfigūraciją 245
6.9 Komandos eilutės skaitytuvas 245
7 DUK 247
7.1 Kaip naujinti ESET Internet Security 248
7.2 Kaip pašalinti virusą iš mano kompiuterio 249
7.3 Kaip leisti ryšį tam tikroms taikomosioms programoms 249
7.4 Kaip įjungti paskyros tėvų kontrolę 250
7.5 Kaip sukurti naują užduotį planuoklėje 251
7.6 Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą 252
7.7 Kaip atrakinti išplėstinį nustatymą 253
7.8 Kaip išspręsti produkto išaktyvinimo problemą naudojant ESET HOME 253
7.8 Produktas išjungtas, įrenginys atjungtas 254
7.8 Produktas nesuaktyvintas 254
8.1 Tobulinimo pagal naudotojų patirtį programa 254
8.2 Galutinio vartotojo licencijos sutartis 255
8.3 Privatumo politika 266

ESET Internet Security

ESET Internet Security pristato naują būdą suteikti tikrai integruotą kompiuterių saugos sprendimą. Naujausia ESET LiveGrid® nuskaitymo variklio versija, suderinta su mūsų pasirinktine užkarda ir apsaugos nuo brukalo moduliais, užtikrina greitį ir tikslumą, kad jūsų kompiuteris būtų saugus. Rezultatas – sumani sistema, kuri nuolat pasiruošusi atremti atakas ir kenkėjiškas programas, kurios gali kelti pavojų jūsų kompiuteriui.

ESET Internet Security yra visavertis saugos sprendimas, kuris suderina geriausią apsaugą ir mažiausią poveikį sistemai. Mūsų modernios technologijos naudoja dirbtinį intelektą ir neleidžia įsiskverbti virusams, šnipinėjimo programoms, Trojos arkliams, kirminams, reklamos programoms, kenkėjiškos prieigos programoms ir kitoms grėsmėms – jos nemažina sistemos efektyvumo ir netrukdo jūsų kompiuteriui.

Funkcijos ir privalumai

Naujas vartotojo sąsajos dizainas	Šios versijos vartotojo sąsajos dizainas iš esmės pakeistas ir supaprastintas vadovaujantis patogaus naudojimo bandymais. Visas GUI tekstas ir pranešimai atidžiai peržiūrėti, o sąsaja dabar palaiko iš dešinės į kairę skaitomas kalbas, tokias kaip hebrajų ir arabų. Interneto žinynas dabar integruotas į ESET Internet Security ir pateikia dinamiškai atnaujinamą pagalbos turinį.
Tamsusis režimas	Plėtinys, padedantis greitai perjungti ekraną į tamsią temą. Pageidaujamą spalvų schemą galite pasirinkti naudotojo sąsajos elementuose.
Apsauga nuo virusų ir šnipinėjimo programų	Aktyviai aptinka ir valo daugiau žinomų ir nežinomų virusų, kirminų, Trojos arklių ir kenkėjiškų prieigos programų. Pažangi euristika pažymi net anksčiau niekada nematytas kenkėjiškas programas ir apsaugo jus nuo nežinomų grėsmių, neutralizuoja jas, kol nepridarė jokios žalos. Prieigos prie saityno apsauga ir apsauga nuo sukčiavimo apsimetant stebi ryšį tarp interneto naršyklių ir nuotolinių serverių (įskaitant SSL). El. pašto programos apsauga kontroliuoja el. pašto ryšį, gaunamą POP3(S) ir IMAP(S) protokolais.
Reguliarūs naujinimai	Reguliariai naujinti aptikimo modulį (anksčiau vadintą „virusų kodų duomenų baze“) ir programos modulius yra geriausias būdas užtikrinti maksimalų saugos lygį kompiuteryje.
ESET LiveGrid® (Debesų išteklius naudojanti reputacija)	Jūs galite patikrinti vykdomų procesų ir failų reputaciją tiesiai iš ESET Internet Security.
Įrenginio kontrolė	Automatiškai nuskaito visas USB atmintines, atminties korteles ir CD / DVD diskus. Blokuoja nešiojamąją laikmeną atsižvelgiant į laikmenos tipą, gamintoją, dydį ir kitus atributus.
HIPS funkcionalumas	Galite dar išsamiau tinkinti sistemos veiksmus; nurodyti taisykles sistemos registrui, aktyviems procesams ir programoms bei tiksliai suderinti savo saugos parametrus.
Žaidimų režimas	Atideda visus iškylančiuosius langus, naujinimus arba kitus intensyvius sistemos veiksmus, kad išsaugotų sistemos išteklius žaidimams ir kitiems veiksmams visame ekrane.

ESET Internet Security Funkcijos

Saugi bankininkystė ir naršymas	Saugi bankininkystė ir naršymas pateikia apsaugotą naršyklę, kurią galima naudoti jungiantis prie internetinės bankininkystės ar internetinių mokėjimų šliuzų, kad visos internetinės operacijos būtų atliekamos patikimoje ir saugioje aplinkoje.

Tinklo parašų palaikymas	Tinklo parašai leidžia greitai identifikuoti ir užblokuoti kenkėjišką srautą į ir iš vartotojų įrenginių, pavyzdžiui, užgrobtų kompiuterių tinklų ir išnaudojimo paketų. Ši funkcija gali būti laikoma apsaugos nuo užgrobtų kompiuterių tinklų sustiprinimu.
Išmanioji užkarda	Neleidžia neįgaliotiesiems vartotojams patekti į jūsų kompiuterį ir pasinaudoti asmeniniais duomenimis.
El. pašto programos apsauga nuo brukalo	Brukalas užima iki 50 procentų visų el. pašto ryšių. El. pašto programos apsauga nuo brukalo apsaugo nuo šios problemos.
Anti-Theft	Anti-Theft išplečia vartotojo lygmens saugą, kai kompiuteris pametamas ar pavagiamas. Kai įdiegsite „ESET Internet Security“ ir „Anti-Theft“, jūsų įrenginys bus įtrauktas į sąrašą saityno sąsajoje. Saityno sąsaja leidžia tvarkyti „Anti-Theft“ konfigūraciją ir administruoti „Anti-Theft“ funkcijas savo įrenginyje.
Tėvų kontrolė	Apsaugo jūsų šeimą nuo galbūt kenkėjiško saityno turinio blokuodama įvairias svetainių kategorijas.

Prenumerata turi būti aktyvi, kad „ESET Internet Security“ funkcijos veiktų. Rekomenduojame atnaujinti prenumeratą likus kelioms savaitėms iki „ESET Internet Security“ prenumeratos galiojimo pabaigos.

Kas naujo?

Kas naujo ESET Internet Security 17.1 versijoje

- Nedideli tinklo tikrinimo įrankio patobulinimai
- Nedideli saugios bankininkystės ir naršymo patobulinimai
- Kiti nedideli klaidų pataisymai ir patobulinimai

Norėdami išjungti **naujienų pranešimus**:
1. Atidarykite Išplėstinis nustatymas > **Pranešimai** > **Darbalaukio pranešimai**.
2. Spustelėkite **Redaguoti** šalia **Darbalaukio pranešimai**.
3. Pašalinkite parinkties **Rodyti naujienų pranešimus** žymėjimą ir spustelėkite **Gerai**.

Norėdami gauti daugiau informacijos apie pranešimus, žr. skyrių Pranešimai.

Išsamų pakeitimų sąrašą ESET Internet Security, rasite ESET Internet Security pakeitimų žurnaluose.

Kokį produktą naudoju?

ESET suteikia kelis apsaugos lygmenis naujais savo produktais: pradedant galingais ir greitais apsaugos nuo virusų sprendimais, baigiant universaliais apsaugos sprendimais, kurie minimaliai veikia sistemą:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

Jei norite sužinoti, kokį produktą esate įdiegę, atidarykite pagrindinį programos langą ir lango viršuje pamatysite produkto pavadinimą (žr. žinių bazės straipsnį).

Toliau esančioje lentelėje pateikiamos kiekvieno produkto funkcijos.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Aptikimo modulis	✔	✔	✔	✔
Išplėstinis mašininis mokymasis	✔	✔	✔	✔
Įsilaužimų blokatorius	✔	✔	✔	✔
Apsauga nuo scenarijumi paremtų atakų	✔	✔	✔	✔
Apsauga nuo sukčiavimo	✔	✔	✔	✔
Prieigos prie saityno apsauga	✔	✔	✔	✔
HIPS (įskaitant apsaugą nuo „Ransomware“)	✔	✔	✔	✔
Apsauga nuo brukalo		✔	✔	✔
Užkarda		✔	✔	✔
Tinklo tikrinimo įrankis		✔	✔	✔
Interneto kameros apsauga		✔	✔	✔
Tinklo apsauga nuo atakų		✔	✔	✔
Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą		✔	✔	✔
Saugi bankininkystė ir naršymas		✔	✔	✔
Naršyklės privatumas ir sauga		✔	✔	✔
Tėvų kontrolė		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Kai kurie anksčiau išvardytų produktų gali nebūti jūsų kalba arba jie gali būti neteikiami jūsų regione.

Sistemos reikalavimai

Jūsų sistema turi atitikti toliau nurodytus aparatinės ir programinės įrangos reikalavimus, kad ESET Internet Security veiktų optimaliai:

Palaikomi procesoriai

Intel arba AMD procesorius, 32 bitų (x86) su SSE2 instrukcijų rinkiniu arba 64bit (x64), 1 GHz arba daugiau
ARM64 pagrindu pagamintas procesorius, 1 GHz arba spartesnis

Palaikomos operacinės sistemos

Microsoft® Windows® 11

Microsoft® Windows® 10

„Azure“ kodo pasirašymo palaikymas turi būti įdiegtas visose "Windows" operacinėse sistemose, kad būtų galima įdiegti arba naujovinti ESET produktus, išleistus po 2023 m. liepos mėn. Daugiau informacijos.

Visada stenkitės užtikrinti, kad jūsų operacinė sistema būtų atnaujinta.

„ESET Internet Security“ funkcijų reikalavimai

Sistemos reikalavimus konkrečių „ESET Internet Security“ funkcijų atveju žiūrėkite toliau pateiktoje lentelėje:

Funkcija	Reikalavimai
Intel® Threat Detection Technology	Peržiūrėkite palaikomus procesorius.
Saugi bankininkystė ir naršymas	Peržiūrėkite palaikomas žiniatinklio naršykles.
Skaidrus fonas	„Windows 10“ RS4 ir naujesnė versija.
Specializuota valymo programa	Ne ARM64 pagrindo procesorius.
Sistemos valymo priemonė	Ne ARM64 pagrindo procesorius.
Įsilaužimų blokatorius	Ne ARM64 pagrindo procesorius.
Išsamios elgsenos patikrinimas	Ne ARM64 pagrindo procesorius.

Kita

Norint suaktyvinti ir naujinti ESET Internet Security, kad tinkamai veiktų, reikalingas interneto ryšys.

Dvi antivirusinės programos, vienu metu veikiančios viename įrenginyje, sukelia neišvengiamus sistemos išteklių konfliktus, pvz., sulėtina sistemą taip, kad jos nebegalima valdyti.

Pasenusi „Microsoft Windows“ versija

Problema

- Norite įdiegti naujausią „ESET Internet Security“ versiją kompiuteryje su „Windows 7“, „Windows 8“ (8.1) arba „Windows Home Server 2011“
- Diegiant „ESET Internet Security“ rodoma klaida **Pasenusi operacinė sistema**

Išsami informacija

Naujausiai „ESET Internet Security“ versijai reikalinga operacinė sistema „Windows 10“ arba „Windows 11“.

Sprendimas

Galimi šie sprendimai:

Versijos naujinimas į „Windows 10“ arba „Windows 11“

Atnaujinimo procedūra yra gana paprasta ir daugeliu atvejų tai galite padaryti neprarasdami savo failų. Prieš naujinant į „Windows 10“:

1. Svarbių duomenų atsarginių kopijų kūrimas.

2. Skaitykite „Microsoft“ 10 dažnai užduodamų klausimų apie „Windows“ atnaujinimą arba 11 dažnai užduodamų klausimų apie „Windows“ atnaujinimą ir atnaujinkite savo „Windows“ OS.

Įdiekite „ESET Internet Security“ 16.0 versiją

Jei negalite naujovinti „Windows“, įdiekite „ESET Internet Security“ 16.0 versiją. Išsamesnės informacijos rasite „ESET Internet Security“ (16.0 versija) žinyne internete.

Prevencija

Kai dirbate su kompiuteriu ir ypač – kai naršote internete – atsiminkite, kad jokia antivirusinė sistema pasaulyje negali visiškai pašalinti pavojaus, kurį kelia aptikimai ir nuotolinės atakos. Kad būtų užtikrinta maksimali apsauga ir patogus naudojimas, itin svarbu teisingai naudoti antivirusinį sprendimą ir laikytis keleto naudingų taisyklių.

Reguliariai naujinkite

Pagal ESET LiveGrid® statistiką, kasdien sukuriama tūkstančiai naujų, unikalių įsiskverbimų, bandančių apeiti esamas apsaugos priemones ir siekiančių duoti pelno jų autoriams – visa tai vykdoma kitų vartotojų sąskaita. ESET tyrimų laboratorijos specialistai kasdien analizuoja šias grėsmes ir paruošia bei išleidžia naujinimus, kad būtų nuolatos gerinamas mūsų vartotojų apsaugos lygis. Kad būtų užtikrintas maksimalus šių naujinimų efektyvumas, svarbu, kad naujinimai būtų tinkamai sukonfigūruoti jūsų sistemoje. Jeigu norite rasti daugiau informacijos, kaip konfigūruoti naujinimus, žiūrėkite skyrių Naujinimo nustatymai.

Atsisiųskite saugos pataisas

Kenkėjiškų programų autoriai dažnai išnaudoja įvairias sistemos spragas, kad galėtų efektyviau platinti kenkėjišką kodą. Atsižvelgdamos į tai programinės įrangos įmonės atidžiai ieško bet kokių spragų savo programose ir reguliariai išleidžia saugos naujinimus, kurie apsaugo nuo galimų grėsmių. Svarbu atsisiųsti šiuos saugos naujinimus, kai jie išleidžiami. Microsoft Windows ir tokios interneto naršyklės kaip Internet Explorer yra du programų, kurioms saugos naujinimai išleidžiami reguliariai, pavyzdžiai.

Svarbių duomenų atsarginių kopijų kūrimas

Kenkėjiškų programų kūrėjai paprastai nekreipia dėmesio į vartotojų poreikius, kenkėjiškų programų veikla dažnai sukelia kritines operacinės sistemos klaidas ir sugadina svarbius duomenis. Svarbu reguliariai daryti svarbių ir slaptų duomenų atsargines kopijas į išorinį šaltinį, tokį kaip DVD arba išorinį standųjį diską. Tai leidžia lengviau ir greičiau atkurti duomenis įvykus sistemos gedimui.

Reguliariai nuskaitykite kompiuterį tikrindami, ar jame nėra virusų

Daugiau žinomų ir nežinomų virusų, kirminų, Trojos arklių ir kenkėjiškų prieigos programų aptikimą vykdo failų sistemos apsaugos realiuoju laiku modulis. Tai reiškia, kad kaskart, kai pasiekiate failą arba jį atidarote, jis nuskaitomas dėl kenkėjiškų veiksmų. Mes rekomenduojame atlikti viso kompiuterio nuskaitymą bent vieną kartą per mėnesį, nes kenkėjiškų programų kodai kinta, aptikimo modulis kasdien savaime atsinaujina.

Laikykitės pagrindinių saugos taisyklių

Tai pati naudingiausia ir pati veiksmingiausia taisyklė – visada būkite atsargūs. Šiandien, daugeliui įsiskverbimų reikalingi vartotojo veiksmai, kad jie galėtų veikti ir būti platinami. Jeigu būsite atidūs atidarydami naujus failus, sutaupysite daug laiko ir pastangų, reikalingų išvalyti įsiskverbimams. Čia pateikiama keletas naudingų nurodymų:

- Nesilankykite įtartinose svetainėse su daug iškylančiųjų langų ir mirksinčiais reklaminiais skelbimais.
- Būkite atidūs diegdami nemokamas programas, kodekų paketus ir t. t. Naudokite tik saugias programas ir lankykitės tik saugiose interneto svetainėse.
- Būkite atsargūs atidarydami el. laiškų priedus, ypač kai gaunate laiškus, skirtus daugeliui gavėjų, arba gaunamus iš nežinomų siuntėjų.
- Nenaudokite administratoriaus paskyros kasdieniam darbui su kompiuteriu.

Žinyno puslapiai

Sveiki! Tai ESET Internet Security vartotojo vadovas. Čia pateikiama informacija supažindins jus su gaminiu ir padės padaryti jūsų kompiuterį saugesnį.

Pradžia

Prieš pradedant naudotis „ESET Internet Security“, galite susipažinti su įvairiais aptikimo tipais ir nuotolinėmis atakomis, kurios gali užpulti kompiuterį. Be to, sudarėme „ESET Internet Security“ naujų funkcijų sąrašą.

Pradėkite įdiegdami „ESET Internet Security“. Jei „ESET Internet Security“ jau įdiegėte, žiūrėkite Darbas su „ESET Internet Security“.

Kaip naudoti ESET Internet Security žinyno puslapius

Internetinis žinynas yra suskirstytas į kelis skyrius ir poskyrius. „ESET Internet Security“ paspauskite **F1**, kad peržiūrėtumėte informaciją apie šiuo metu atidarytą langą.

Programa leidžia ieškoti temos žinyne pagal raktažodį (-ius) arba ieškoti turinio pagal įvestus žodžius ar frazes. Šie du metodai skiriasi tuo, kad raktažodis gali būti logiškai susietas su žinyno puslapiais, kurių tekste gali nebūti šio konkretaus raktažodžio. Leškant pagal žodžius ar frazes bus ieškoma visuose puslapiuose ir rodomi tik tie puslapiai, kurių tekste yra ieškomas žodis ar frazė.

Siekiant išlaikyti nuoseklumą ir išvengti painiavos, šiame vadove vartojama terminija yra sudaryta pagal „ESET Internet Security“ naudotojo sąsają. Be to, ypač reikšmingoms ar svarbioms temoms išskirti naudojame vienodą simbolių rinkinį.

Pastaba yra tiesiog trumpas paaiškinimas. Nors galite jas praleisti, pastabose pateikiama vertingos informacijos, pavyzdžiui, tam tikros funkcijos arba nuorodos į kai kurias susijusias temas.

Į tai reikia atkreipti dėmesį, todėl šios informacijos raginame nepraleisti. Paprastai čia pateikiama ne pati svarbiausia, bet svarbi informacija.

Tai informacija, kuriai reikalingas ypatingas dėmesys ir dėl kurios reikia būti itin atsargiems. Įspėjimai dažniausiai pateikiami siekiant jus perspėti, kad nepadarytumėte galimai pavojingų klaidų. Perskaitykite ir įsigilinkite į tekstą, nes jis skirtas itin jautriems sistemos parametrams arba kam nors pavojingam.

Tai – konkretus panaudojimo būdas arba praktinis pavyzdys, padedantis suprasti, kaip galima naudotis tam tikra funkcija ar galimybe.

Sutartinis pavadinimas	Reikšmė
Paryškintasis tipas	Sąsajos elementų pavadinimai, pvz., langų ir parinkčių mygtukų.
Pasvirasis tipas	Vietos rezervavimo ženklai jūsų pateikiamai informacijai. Pavyzdžiui, failo pavadinimas arba kelias reiškia, kad reikia įvesti tikrą kelią ar failo pavadinimą.
`Courier New`	Kodo pavyzdžiai arba komandos.
Hipersaitas	Leidžia greitai ir lengvai pasiekti nurodomas temas ar išorines saityno vietas. Hipersaitai yra paryškinti mėlynai ir gali būti pabraukti.
%ProgramFiles%	„Windows“ sistemos katalogas, kuriame saugomos „Windows“ sistemoje įdiegtos programos.

Internetinis žinynas yra pagrindinis žinyno turinio šaltinis. Kai būsite prisijungę prie veikiančio interneto ryšio, bus rodoma naujausia internetinio žinyno versija.

Diegimas

Yra keletas ESET Internet Security diegimo kompiuteryje būdų. Diegimo būdas priklauso nuo šalies ir platinimo priemonių:

- Tiesioginio diegimo programa – atsisiunčiama iš ESET svetainės ar naudojant CD / DVD. Šis diegimo paketas yra universalus ir gali būti naudojamas su visomis kalbomis (pasirinkite reikiamą kalbą). Tiesioginio diegimo programa yra nedidelis failas; ESET Internet Security diegti reikalingi papildomi failai atsisiunčiami automatiškai.

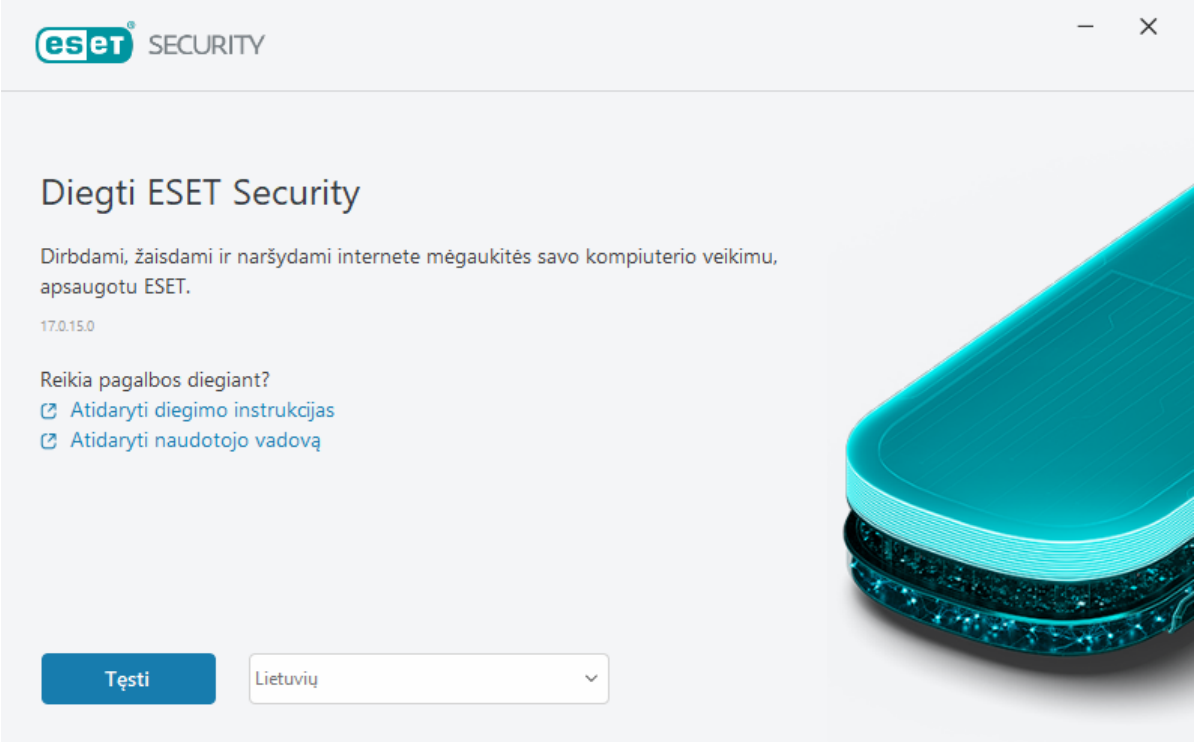
- Diegimas neprisijungus – naudojamas .exe failas, kuris yra didesnis nei tiesioginio diegimo programos failas; diegiant nereikia prisijungti prie interneto arba jokių papildomų failų.

Prieš diegdami ESET Internet Security įsitikinkite, kad kompiuteryje nėra įdiegta kitų antivirusinių programų. Jeigu du arba daugiau antivirusinių sprendimų yra įdiegta viename kompiuteryje, jie gali konfliktuoti vienas su kitu. Rekomenduojame išdiegti visas kitas antivirusines programas savo sistemoje. Žiūrėkite mūsų ESET žinių bazės straipsnį, kuriame rasite įprastinės antivirusinės programinės įrangos pašalinimo įrankių sąrašą (pateikiamą anglų ir keliomis kitomis kalbomis).

Tiesioginio diegimo programa

Kai atsisiuntėte Diegimo įrankio diegimo paketą, dukart spustelėkite diegimo failą ir vykdykite nuoseklius nurodymus, kurie pateikiami diegimo programos vedlyje.

Atlikdami šio tipo diegimą turite būti prisijungę prie interneto.



1. Išskleidžiamajame meniu pasirinkite tinkamą kalbą ir spustelėkite **Tęsti**.

Jei diegiate naujesnę versiją, palyginti su ankstesne versija, su slaptažodžiu apsaugotais nustatymais, įveskite slaptažodį. Nustatymų slaptažodį galite konfigūruoti Prieigos nustatymuose.

2. Pasirinkite pageidaujamas funkcijas, perskaitykite galutinio naudotojo licencijos sutartį ir privatumo politiką ir spustelėkite **Tęsti**, arba spustelėkite **Leisti viską ir tęsti**, kad įgalintumėte visas funkcijas:

- ESET LiveGrid® atsiliepimų sistema
- Galimai nepageidaujamos programos
- Tobulinimo pagal naudotojų patirtį programa

Spustelėdami **Tęsti** arba **Leisti viską ir tęsti**, sutinkate su galutinio naudotojo licencijos sutartimi ir pripažįstate privatumo politiką.

3. Norėdami aktyvinti, valdyti ir peržiūrėti įrenginio saugą naudodami ESET HOME, prijunkite įrenginį prie ESET HOME paskyros. Spustelėkite **Praleisti prisijungimą,** kad tęstumėte neprisijungę prie ESET HOME. Vėliau galite prijungti įrenginį prie ESET HOME paskyros.

4. Jei tęsite neprisijungę prie ESET HOME, pasirinkite aktyvinimo parinktį. Jei diegiate naujesnę versiją vietoj ankstesnės, jūsų **aktyvinimo raktas** bus įvestas automatiškai.

5. Diegimo vediklis nustato, kuris ESET produktas bus įdiegtas, remiantis jūsų prenumerata. Visada iš anksto parenkama versija, kurioje yra daugiausiai saugos funkcijų. Jei norite **įdiegti kitą ESET produko versiją**, spustelėkite Pakeisti produktą. Spustelėkite **Tęsti**, kad pradėtumėte diegimo procesą. Tai gali užtrukti kelias akimirkas.

Jei yra kokių nors ESET produktų likučių (failų ar aplankų), išdiegtų praeityje, būsite paraginti leisti juos pašalinti. Norėdami tęsti, spustelėkite **Diegti**.

6. Kad išeitumėte iš diegimo vedlio, spustelėkite **Atlikta**.

Diegimo trikčių diagnostikos priemonė.

Kai produktas įdiegiamas ir suaktyvinamas, pradedama siųsti modulius. Inicijuojama apsauga ir kai kurios funkcijos gali neveikti visiškai tinkamai, kol atsisiuntimas nebus baigtas.

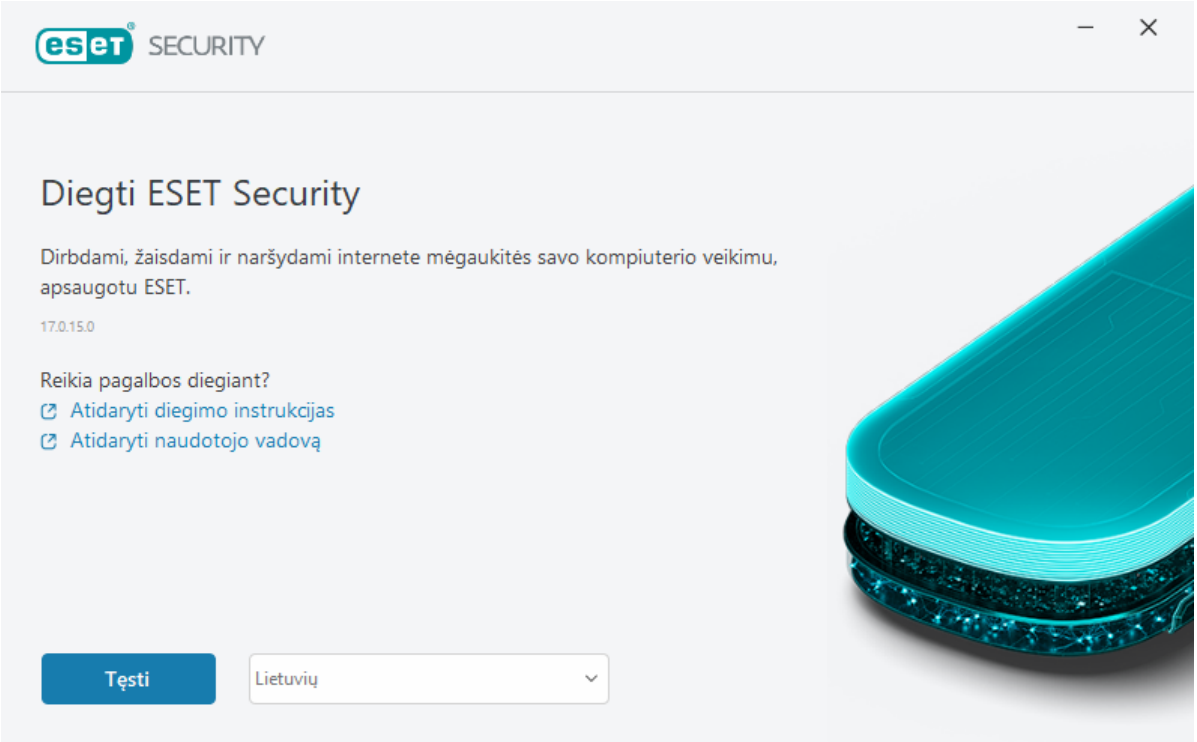
Diegimas neprisijungus

Atsisiųskite ir įdiekite savo ESET „Windows Home“ produktą naudodami toliau pateiktą diegimo neprisijungus priemonę (.exe). Pasirinkite, kurią ESET HOME produkto versiją atsisiųsti (32 bitų, 64 bitų arba ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
64 bitų atsisiuntimas 32 bitų atsisiuntimas ARM atsisiuntimas	64 bitų atsisiuntimas 32 bitų atsisiuntimas ARM atsisiuntimas	64 bitų atsisiuntimas 32 bitų atsisiuntimas ARM atsisiuntimas	64 bitų atsisiuntimas 32 bitų atsisiuntimas ARM atsisiuntimas

Jei turite aktyvų interneto ryšį, įdiekite savo ESET produktą naudodami diegimo įrankį.

Kai paleisite diegimą neprisijungus (.exe), diegimo vedlys jums padės atlikti nustatymo procesą.



1. Išskleidžiamajame meniu pasirinkite tinkamą kalbą ir spustelėkite **Tęsti**.

Jei diegiate naujesnę versiją, palyginti su ankstesne versija, su slaptažodžiu apsaugotais nustatymais, įveskite slaptažodį. Nustatymų slaptažodį galite konfigūruoti Prieigos nustatymuose.

2. Pasirinkite pageidaujamas funkcijas, perskaitykite galutinio naudotojo licencijos sutartį ir privatumo politiką ir spustelėkite **Tęsti**, arba spustelėkite **Leisti viską ir tęsti**, kad įgalintumėte visas funkcijas:

- ESET LiveGrid® atsiliepimų sistema
- Galimai nepageidaujamos programos
- Tobulinimo pagal naudotojų patirtį programa

Spustelėdami **Tęsti** arba **Leisti viską ir tęsti**, sutinkate su galutinio naudotojo licencijos sutartimi ir pripažįstate privatumo politiką.

3. Spustelėkite **Praleisti prisijungimą**. Kai turėsite interneto ryšį, galėsite prijungti savo įrenginį prie savo paskyra ESET HOME paskyros.

4. Spustelėkite **Praleisti aktyvinimą**. Kad visiškai veiktų, po įdiegimo būtina suaktyvinti ESET Internet Security. Produkto aktyvinimui reikalingas aktyvus interneto ryšys.

5. Diegimo vediklis rodo, kuris ESET produktas bus įdiegtas pagal atsisiųsta diegimo neprisijungus priemonę. Spustelėkite **Tęsti**, kad pradėtumėte diegimo procesą. Tai gali užtrukti kelias akimirkas.

Jei yra kokių nors ESET produktų likučių (failų ar aplankų), išdiegtų praeityje, būsite paraginti leisti juos pašalinti. Norėdami tęsti, spustelėkite **Diegti**.

6. Kad išeitumėte iš diegimo vedlio, spustelėkite **Atlikta**.

Diegimo trikčių diagnostikos priemonė.

Prenumeratos naujovinimas

Šis pranešimo langas rodomas, jei jūsų ESET produktui aktyvinti naudota prenumerata buvo pakeista. Pakeista prenumerata leidžia aktyvinti produktą, turintį daugiau saugos funkcijų. Jei nieko nekeitėte, ESET Internet Security vieną kartą parodys įspėjimo langą, raginantį **Pakeisti į produktą, turintį daugiau funkcijų**.

Taip (rekomenduojama) – automatiškai įdiegs produktą su daugiau saugos funkcijų.

Ačiū, ne – nebus atlikta jokių pakeitimų ir pranešimas daugiau nebepasirodys.

Norėdami pakeisti produktą vėliau, skaitykite mūsų ESET žinių bazės straipsnį. Daugiau informacijos apie ESET prenumeratą rasite DUK apie prenumeratą.

Toliau esančioje lentelėje pateikiamos kiekvieno produkto funkcijos.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Aptikimo modulis	✔	✔	✔	✔
Išplėstinis mašininis mokymasis	✔	✔	✔	✔
Įsilaužimų blokatorius	✔	✔	✔	✔
Apsauga nuo scenarijumi paremtų atakų	✔	✔	✔	✔
Apsauga nuo sukčiavimo	✔	✔	✔	✔
Prieigos prie saityno apsauga	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
HIPS (įskaitant apsaugą nuo „Ransomware“)	✔	✔	✔	✔
Apsauga nuo brukalo		✔	✔	✔
Užkarda		✔	✔	✔
Tinklo tikrinimo įrankis		✔	✔	✔
Interneto kameros apsauga		✔	✔	✔
Tinklo apsauga nuo atakų		✔	✔	✔
Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą		✔	✔	✔
Saugi bankininkystė ir naršymas		✔	✔	✔
Naršyklės privatumas ir sauga		✔	✔	✔
Tėvų kontrolė		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Produkto keitimas į aukštesnę versiją

Atsisiuntėte numatytąją diegimo programą ir nusprendėte pakeisti aktyvintą produktą arba norite pakeisti įdiegtą produktą saugesne versija.

Pakeiskite produktą diegimo metu.

Toliau esančioje lentelėje pateikiamos kiekvieno produkto funkcijos.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Aptikimo modulis	✔	✔	✔	✔
Išplėstinis mašininis mokymasis	✔	✔	✔	✔
Įsilaužimų blokatorius	✔	✔	✔	✔
Apsauga nuo scenarijumi paremtų atakų	✔	✔	✔	✔
Apsauga nuo sukčiavimo	✔	✔	✔	✔
Prieigos prie saityno apsauga	✔	✔	✔	✔
HIPS (įskaitant apsaugą nuo „Ransomware“)	✔	✔	✔	✔
Apsauga nuo brukalo		✔	✔	✔
Užkarda		✔	✔	✔
Tinklo tikrinimo įrankis		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Interneto kameros apsauga		✔	✔	✔
Tinklo apsauga nuo atakų		✔	✔	✔
Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą		✔	✔	✔
Saugi bankininkystė ir naršymas		✔	✔	✔
Naršyklės privatumas ir sauga		✔	✔	✔
Tėvų kontrolė		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Prenumeratos pakeitimas į ankstesnę versiją

Šis dialogo langas rodomas, jei jūsų ESET produktui aktyvinti naudota prenumerata buvo pakeista. Pakeistą prenumeratą galima naudoti tik kitam ESET produktui, turinčiam mažiau saugos funkcijų. Produktas buvo pakeistas automatiškai, kad neprarastumėte apsaugos.

Daugiau informacijos apie ESET prenumeratą rasite DUK apie prenumeratą.

Toliau esančioje lentelėje pateikiamos kiekvieno produkto funkcijos.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Aptikimo modulis	✔	✔	✔	✔
Išplėstinis mašininis mokymasis	✔	✔	✔	✔
Įsilaužimų blokatorius	✔	✔	✔	✔
Apsauga nuo scenarijumi paremtų atakų	✔	✔	✔	✔
Apsauga nuo sukčiavimo	✔	✔	✔	✔
Prieigos prie saityno apsauga	✔	✔	✔	✔
HIPS (įskaitant apsaugą nuo „Ransomware“)	✔	✔	✔	✔
Apsauga nuo brukalo		✔	✔	✔
Užkarda		✔	✔	✔
Tinklo tikrinimo įrankis		✔	✔	✔
Interneto kameros apsauga		✔	✔	✔
Tinklo apsauga nuo atakų		✔	✔	✔
Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Saugi bankininkystė ir naršymas		✔	✔	✔
Naršyklės privatumas ir sauga		✔	✔	✔
Tėvų kontrolė		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Produkto keitimas į žemesnę versiją

Šiuo metu įdiegtame produkte yra daugiau saugumo funkcijų nei tame, kurį ketinate suaktyvinti. Prarasite apsaugą ir prieigą prie susijusių duomenų, saugomų ESET HOME.

Toliau esančioje lentelėje pateikiamos kiekvieno produkto funkcijos.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Aptikimo modulis	✔	✔	✔	✔
Išplėstinis mašininis mokymasis	✔	✔	✔	✔
Įsilaužimų blokatorius	✔	✔	✔	✔
Apsauga nuo scenarijumi paremtų atakų	✔	✔	✔	✔
Apsauga nuo sukčiavimo	✔	✔	✔	✔
Prieigos prie saityno apsauga	✔	✔	✔	✔
HIPS (įskaitant apsaugą nuo „Ransomware“)	✔	✔	✔	✔
Apsauga nuo brukalo		✔	✔	✔
Užkarda		✔	✔	✔
Tinklo tikrinimo įrankis		✔	✔	✔
Interneto kameros apsauga		✔	✔	✔
Tinklo apsauga nuo atakų		✔	✔	✔
Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą		✔	✔	✔
Saugi bankininkystė ir naršymas		✔	✔	✔
Naršyklės privatumas ir sauga		✔	✔	✔
Tėvų kontrolė		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Diegimo trikčių diagnostikos priemonė

Jei diegiant kyla problemų, diegimo vedlys pateikia trikčių diagnostikos priemonę, kuri, jei įmanoma, išsprendžia problemą.

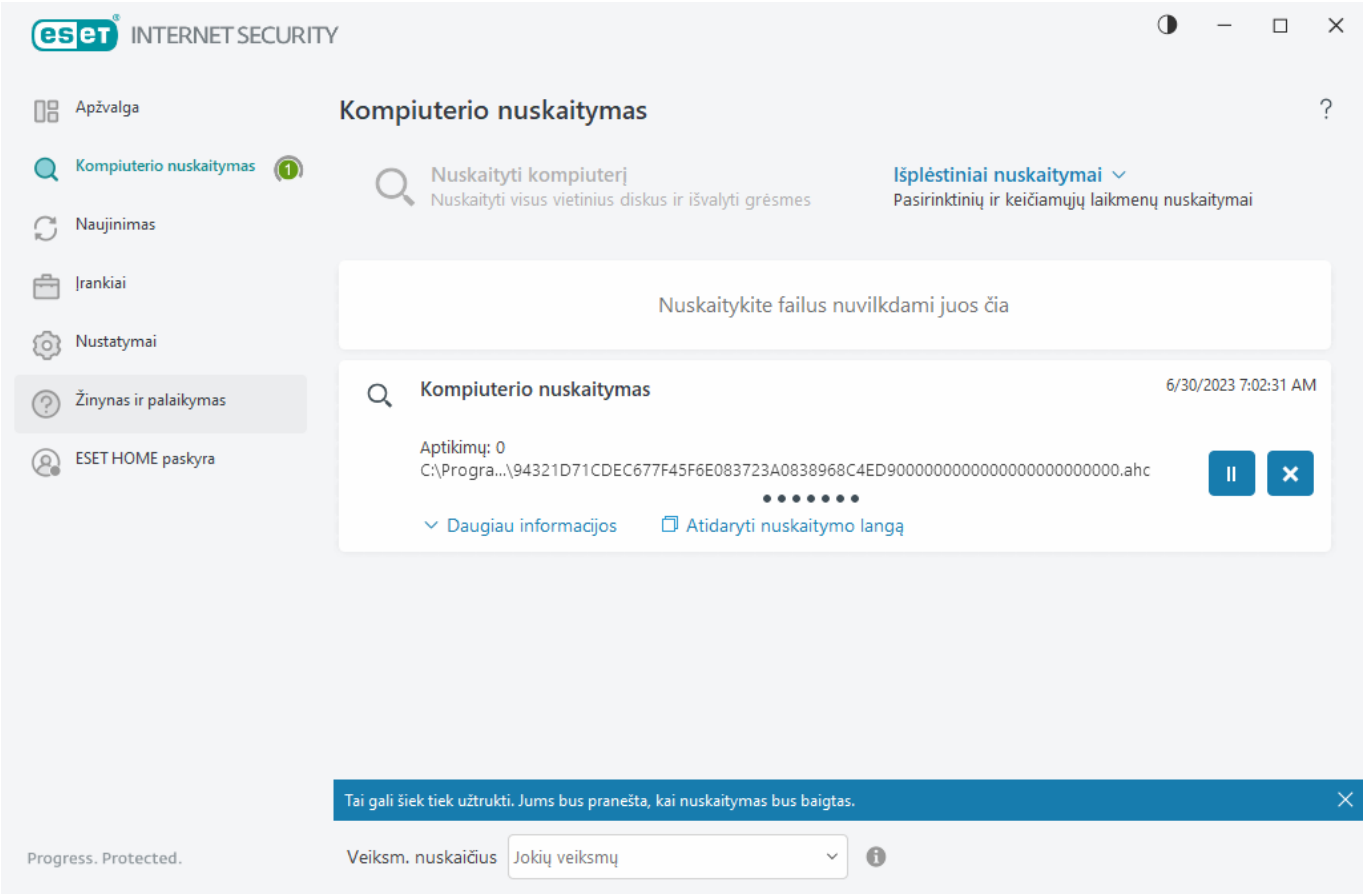
Spustelėkite **Paleisti trikčių diagnostikos priemonė**, kad paleistumėte trikčių diagnostikos priemonę. Kai trikčių diagnostikos priemonė baigs darbą, vadovaukitės rekomenduojamu sprendimu.

Jei problema išlieka, peržiūrėkite dažniausiai pasitaikančių diegimo klaidų ir sprendimų sąrašą.

Pirmas nuskaitymas po diegimo

Įdiegus ESET Internet Security, praėjus 20 minučių nuo įdiegimo arba paleidimo iš naujo bus pradėtas kompiuterio nuskaitymas, kad būtų patikrinta, ar nėra kenkėjiškų kodų.

Kompiuterio nuskaitymą galite pradėti ir rankiniu būdu, pagrindiniame programos lange spustelėdami **Kompiuterio nuskaitymas** > **Nuskaityti jūsų kompiuterį**. Daugiau informacijos apie kompiuterio nuskaitymus rasite skyriuje Kompiuterio nuskaitymas.



Naujinimas į naujesnę versiją

Naujos ESET Internet Security versijos yra išleidžiamos įvedus patobulinimus arba išsprendus problemas, kurių negalima išspręsti automatiškai atnaujinant programos modulius. Atnaujinti į naujesnę versiją galima keliais būdais:

1. Automatiškai atliekant programos naujinimą.
Kadangi programos naujinimai yra pateikiami visiems vartotojams ir gali turėti įtakos tam tikroms sistemų konfigūracijoms, jie išleidžiami atlikus ilgalaikius tikrinimus, kurie užtikrina programos veikimą visose galimose sistemos konfigūracijose. Jei norite išplėtoti programą į naujesnę versiją iš karto po jos išleidimo, taikykite vieną iš toliau pateiktų metodų.
Įsitikinkite, kad įgalinote **Programos funkcijų atnaujinimai** dalyje Išplėstinis nustatymas > **Naujinti** > **Profiliai** > **Atnaujinimai**.

2. Rankiniu būdu pagrindiniame programos lange spustelint **Ieškoti naujinimų** dalyje **Naujinimas**.

3. Rankiniu būdu atsisiunčiant ir įdiegiant naujesnę versiją vietoj ankstesnės.

Daugiau informacijos ir iliustruotos instrukcijos pateikiamos svetainėje:

- Naujinkite ESET produktus – išbandykite naujausius produktų modulius
- Kokių skiriasi skirtingų tipų ESET produktų naujiniai ir leidimų tipai?

Senojo produkto automatinis naujinimas

Jūsų ESET produkto versija nebepalaikoma, produktas atnaujintas iki naujausios versijos.

Dažniausios diegimo problemos

Kiekvienoje naujoje ESET produktų versijoje yra daug klaidų ištaisymų ir patobulinimų. Esami klientai, turintys galiojančią ESET produkto prenumeratą, gali nemokamai atsinaujinti į naujausią to paties produkto versiją.

Norėdami užbaigti diegimą:

1. Spustelėkite **Sutikti ir tęsti**, kad sutiktumėte su Galutinio vartotojo licencijos sutartimi ir sutiktumėte su Privatumo politika. Jei nesutinkate su galutinio vartotojo licencine sutartimi, spustelėkite **Išdiegti**. Negalite grįžti prie ankstesnės versijos.

2. Spustelėkite **Leisti viską ir tęsti**, kad leistumėte Atgalinio ryšio sistemą „ESET LiveGrid®“ ir Tobulinimo pagal naudotojų patirtį programą, arba spustelėkite **Tęsti**, jei nenorite dalyvauti.

3. Aktyvinus naują ESET produktą naudojant aktyvinimo raktą, bus rodomas apžvalgos puslapis. Jei jūsų prenumeratos informacija nerasta, tęskite veiksmus naudodami nemokamą bandomąją versiją. Jei ankstesnio produkto prenumerata negalioja, aktyvinkite savo ESET produktą.

4. Kad diegimo procesas būtų užbaigtas, reikia iš naujo paleisti įrenginį.

ESET Internet Security bus įdiegta

Šis dialogo langas gali būti rodomas:

- Diegimo proceso metu – spustelėkite **Tęsti**, kad įdiegtumėte ESET Internet Security.
- Keičiant prenumeratą „ESET Internet Security“ – spustelėkite **Aktyvinti**, kad pakeistumėte prenumeratą ir aktyvintumėte „ESET Internet Security“.

Parinktis **Keisti produktą** leidžia perjungti skirtingus ESET „Windows“ namų produktus pagal jūsų ESET prenumeratą. Norėdami gauti daugiau informacijos, žr. Kokį produktą naudoju?

Keisti į kitą produktų liniją

Pagal jūsų ESET prenumeratą galite perjungti skirtingus ESET „Windows“ namų produktus. Norėdami gauti daugiau informacijos, žr. Kokį produktą naudoju?

Registracija

Užregistruokite savo prenumeratą užpildydami registracijos formos laukus ir spustelėdami **Aktyvinti**. Laukus, kurie nurodyti kaip privalomieji (skliausteliuose), užpildyti būtina. Jūsų pateikta informacija bus naudojama tik veiksmams, susijusiems su ESET prenumerata.

Aktyvinimo eiga

Palaukite keletą sekundžių, kol pasibaigs aktyvinimo procesas (reikalingas laikas gali skirtis dėl jūsų interneto ryšio arba kompiuterio).

Sėkmingai suaktyvinta

Aktyvinimo procesas užbaigtas. Vykdykite po diegimo pasirodžiusio vedlio nurodymus ir užbaikite ESET Internet Security nustatymą.

Modulio naujinimas bus pradėtas po kelių sekundžių. Reguliarus ESET Internet Security naujinimas bus pradėtas iškart.

Pradinis nuskaitymas bus pradėtas automatiškai per 20 minučių po modulio atnaujinimo.

> Aktyvinimo procesas gali būti nutrauktas, jei pasiūlymas nėra susietas su ESET HOME. Prisijunkite prie ESET HOME arba susikurkite paskyrą.

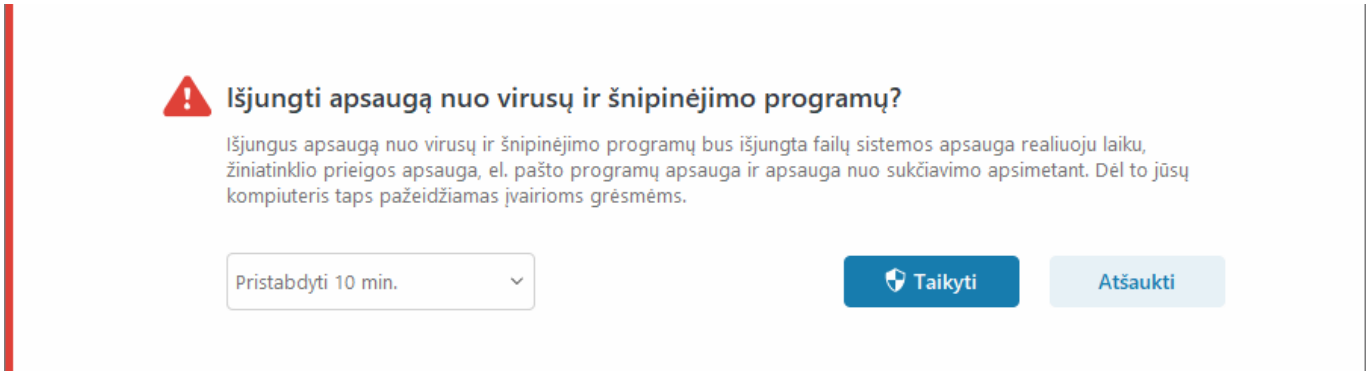
Pradedančiojo vadovas

Šiame skyriuje pateikiama bendra ESET Internet Security apžvalga ir pagrindiniai parametrai.

Sistemos dėklo piktograma

Kai kurias svarbiausias nustatymų parinktis ir funkcijas galima pasiekti dešiniuoju pelės klavišu spustelint sistemos dėklo piktogramą .

Pristabdyti apsaugą – pateikia patvirtinimo dialogo langą, kuris išjungia Aptikimo modulį, saugantį nuo kenkėjiškų sistemos atakų, kontroliuojančią failus, saityno ir el. pašto ryšį. Išskleidžiamasis meniu **Laiko intervalas** galima pasirinkti, kuriam laikui bus išjungta apsauga.



Pristabdyti užkardą (leisti visus duomenų srautus) – perjungia užkardą į neaktyvią būseną. Žr. Tinklas, kur rasite daugiau informacijos.

Blokuoti visus tinklo duomenų srautus – blokuoja visus tinklo duomenų srautus. Vėl įjungti galite spustelėję **Stabdyti visų tinklo duomenų srautų blokavimą**.

Išplėstinis nustatymas – atidaromas ESET Internet Security išplėstinis nustatymas. Norėdami atidaryti išplėstinį nustatymą pagrindiniame produkto lange, klaviatūroje paspauskite F5 arba spustelėkite **Nustatymas** > **Išplėstinis nustatymas**.

Žurnalų failai – žurnalų failuose pateikiama informacijos apie svarbius programos įvykius ir aptikimų apžvalga.

Atidaryti „ESET Internet Security“ – atsidaro „ESET Internet Security“ pagrindinis programos langas.

Iš naujo nustatyti langų išdėstymą – atkuria ESET Internet Security langų numatytuosius dydžius ir padėtis ekrane.

Spalvų režimas – atsidaro naudotojo sąsajos nustatymai, kuriuose galite pakeisti GUI spalvą.

Tikrinti, ar yra atnaujinimų – paleidžia modulį arba produkto naujinį, kad įsitikintumėte, jog esate apsaugoti. „ESET Internet Security“ automatiškai kelis kartus per dieną tikrina, ar nėra naujinių.

Apie – pateikia sistemos informaciją bei išsamią informaciją apie įdiegtą „ESET Internet Security“ versiją, įdiegtus programos modulius ir informacijos apie operacinę sistemą bei sistemos išteklius.

Spartieji klavišai

Norėdami patogiau naršyti ESET Internet Security, galite naudoti šiuos sparčiuosius klavišus:

Spartieji klavišai	Veiksmas
F1	atidaro žinyno puslapius
F5	atidaro išplėstinį nustatymą
Rodyklė aukštyn / rodyklė žemyn	naršymas išplečiamojo meniu elementuose
TAB	pereina prie kito GUI elemento lange
Shift+TAB	pereina prie ankstesnio GUI elemento lange
ESC	uždaro aktyvų dialogo langą
Ctrl+U	rodo informaciją apie ESET prenumeratą ir jūsų kompiuterį (išsamią informaciją apie techninę pagalbą)
Ctrl+R	iš naujo nustato produkto lango numatytąjį dydį ir padėtį ekrane
ALT + Rodyklė kairėn	naršo atgal
ALT + Rodyklė dešinėn	naršo į priekį
ALT+Home	naršo į pagrindinį puslapį

Naršymui taip pat galite naudoti pelės mygtukus atgal arba į priekį.

Profiliai

Profilių tvarkytuvas yra naudojamas dviejose ESET Internet Security vietose – skyriuje **Nuskaitymas pareikalavus** ir **Naujinimas**.

Kompiuterio nuskaitymas

ESET Internet Security yra 4 iš anksto apibrėžti nuskaitymo profiliai:

- **Išmanusis nuskaitymas** – tai numatytasis išplėstinis nuskaitymo profilis. Išmaniojo nuskaitymo profilyje naudojama išmaniojo optimizavimo technologija, kuri neapima failų, kurie ankstesnio nuskaitymo metu buvo rasti švarūs ir po šio nuskaitymo nebuvo pakeisti. Tai leidžia sutrumpinti nuskaitymo laiką ir daro mažiausią poveikį sistemos saugumui.

- **Kontekstinio meniu nuskaitymas** – pagal poreikį galite pradėti bet kurio failo nuskaitymą iš kontekstinio meniu. Kontekstinio meniu nuskaitymo profilis leidžia nustatyti nuskaitymo konfigūraciją, kuri bus naudojama paleidus nuskaitymą tokiu būdu.

- **Giluminis nuskaitymas** – giluminio nuskaitymo profilyje pagal numatytuosius parametrus išmanusis optimizavimas nenaudojamas, todėl naudojant šį profilį nuskaitomi visi failai.

- **Kompiuterio nuskaitymas** – numatytasis profilis, naudojamas įprastai nuskaitant kompiuterį.

Jūsų pasirinkti nuskaitymo parametrai gali būti išsaugoti, kad galėtumėte juos panaudoti nuskaitydami kitą kartą. Rekomenduojame susikurti skirtingus profilius (su skirtingais nuskaitymo tikslais, nuskaitymo metodais ir kitais parametrais) kiekvienam reguliariai atliekamam nuskaitymui.

Norėdami sukurti naują profilį, atidarykite langą Išplėstinis nustatymas > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nuskaitymas pareikalavus** > **Profilių sąrašas** > **Redaguoti**. **Profilių tvarkytuvės** lange yra **Pasirinkto profilio** išskleidžiamasis meniu, kuriame pateikti nuskaitymo profiliai ir naujo profilio kūrimo parinktis. Norėdami sukurti nuskaitymo profilį, kuris atitiktų jūsų poreikius, žiūrėkite skyrių ThreatSense, kuriame aprašytas

kiekvienas nuskaitymo nustatymų parametras.

> Tarkime, norite sukurti savo nuskaitymo profilį ir jums iš dalies tinka **kompiuterio nuskaitymo** konfigūracija, tačiau nenorite nuskaityti pakavimo programos arba galimas nesaugias taikomąsias programas, be to, norite taikyti **Visada ištaisyti aptikimą**. Įveskite savo naujojo profilio pavadinimą į langą **Profilių tvarkytuvas** ir spustelėkite **Pridėti**. **Pasirinkto profilio** išskleidžiamajame meniu pasirinkite naująjį profilį ir pakeiskite likusius parametrus pagal savo reikalavimus, tada spustelėkite **Gerai**, kad naująjį profilį įrašytumėte.

Naujinti

Profilių rengyklė skyriuje Naujinimo nustatymai leidžia jums kurti naujus naujinimų profilius. Kurkite ir naudokite savo pasirinktinius profilius (kitus nei numatytasis **Mano profilis**), tik jeigu kompiuteris naudoja kelis būdus jungtis prie naujinimo serverių.

Pavyzdžiui, nešiojamasis kompiuteris, kuris paprastai jungiasi prie vietinio (veidrodinio atspindžio) serverio vietiniame tinkle, bet kuris atsisiunčia naujinimų failus tiesiai iš ESET naujinimo serverių, kai yra atjungtas nuo vietinio tinklo (komandiruotėje), gali naudoti du profilius: pirmasis naudojamas jungtis prie vietinio serverio, kitas – prie ESET serverių. Kai šie profiliai yra sukonfigūruoti, eikite į **Įrankiai** > **Planuoklė** ir redaguokite naujinimo užduoties parametrus. Nustatykite vieną profilį kaip pagrindinį, o kitą kaip antrinį.

Naujinimo profilis – šiuo metu naudojamas naujinimo profilis. Norėdami jį pakeisti, pasirinkite profilį iš išskleidžiamojo meniu.

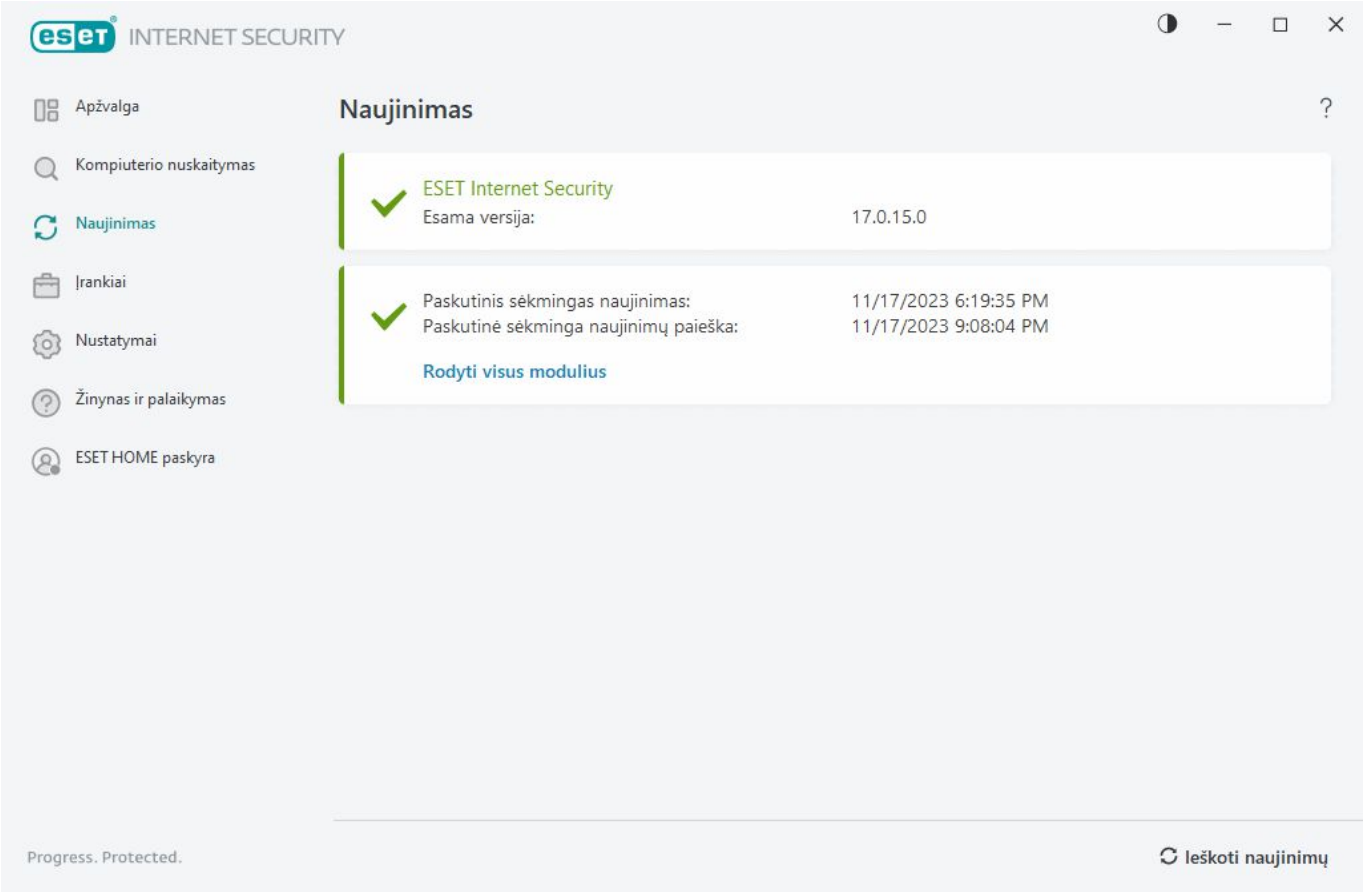
Profilių sąrašas – sukurkite naują arba pašalinkite esamus naujinimo profilius.

Naujinimai

Reguliariai naujinti ESET Internet Security yra geriausias būdas užtikrinti maksimalų saugos lygį jūsų kompiuteryje. Naujinimo modulis užtikrina, kad programų moduliai ir sistemos komponentai visada būtų atnaujinti.

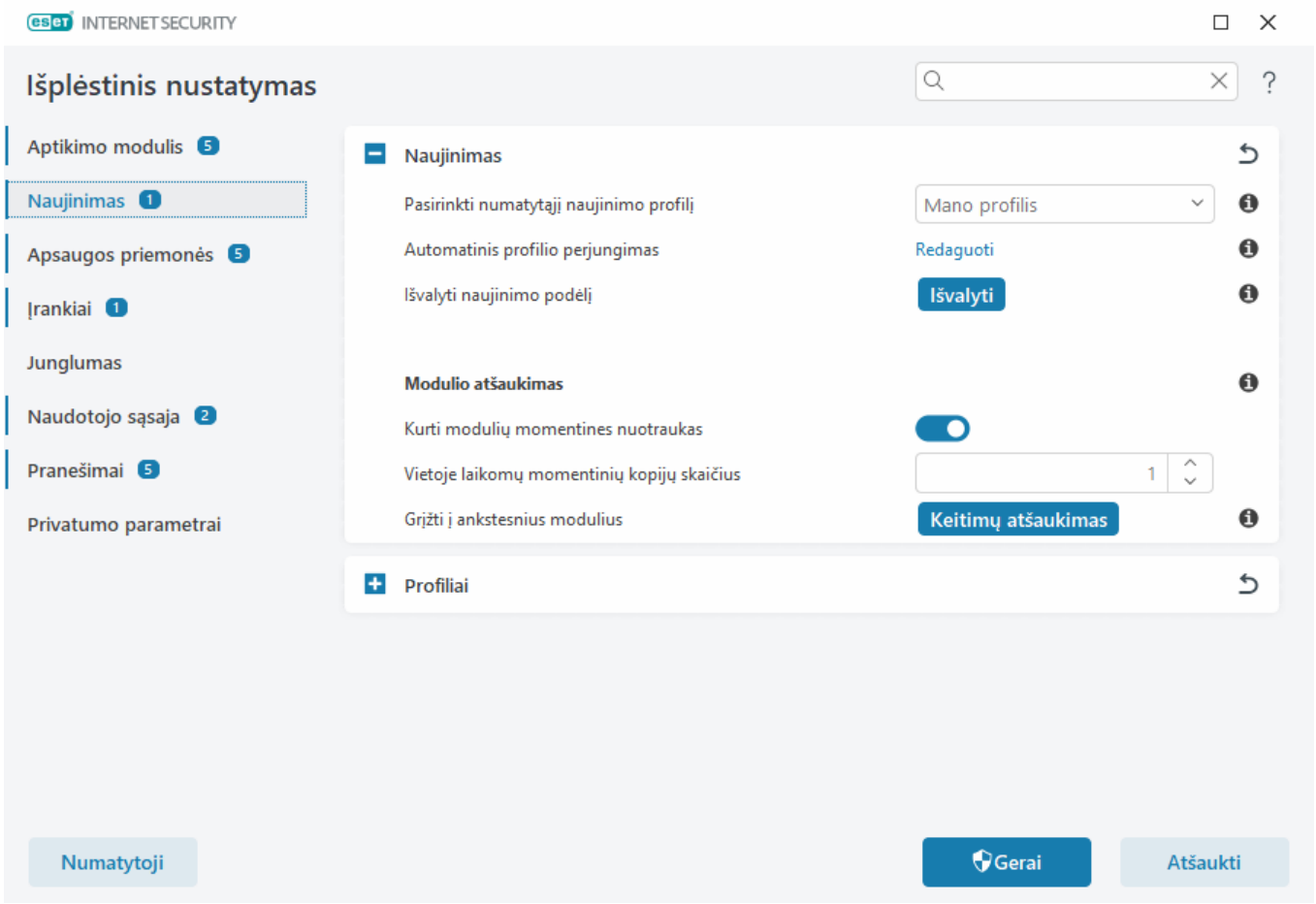
Spustelėję **Naujinimas** pagrindiniame programos lange, galite rasti esamą naujinimo būseną, įskaitant paskutinio sėkmingo naujinimo datą ir laiką ir ar reikalingas naujinimas.

Be automatinių naujinimų, galite spustelėti **Tikrinti, ar yra naujinimų**, kad suaktyvintumėte neautomatinį naujinimą.



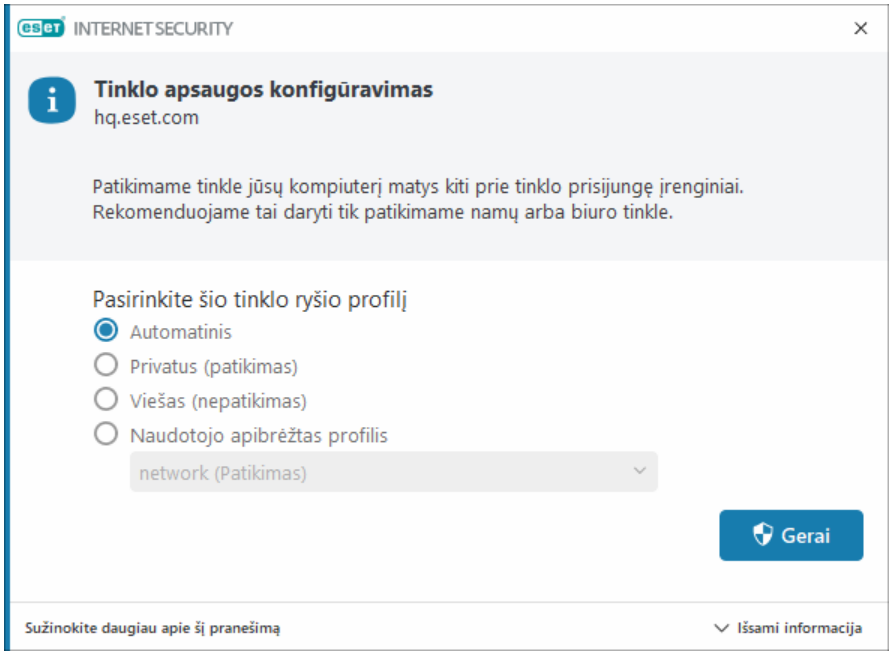
Pasirinkę Išplėstinis nustatymas > **Naujinimai**, rasite papildomų naujinimo parinkčių, pvz., naujinimo režimas, prieiga prie įgaliotojo serverio ir LAN ryšiai.

Jei susiduriate su naujinimo problemomis, spustelėkite **Valyti**, kad išvalytumėte naujinimų podėlį. Jei vis tiek negalite atnaujinti programos modulių, žr. skyrių Pranešimo „Modulių naujinimas nepavyko“ trikčių šalinimas.



Tinklo apsaugos konfigūravimas

Pagal numatytuosius nustatymus, ESET Internet Security naudoja „Windows“ nustatymus, kai aptinkamas naujas tinklo ryšys. Norėdami, kad aptikus naują tinklą būtų rodomas dialogo langas, pakeiskite Tinklo apsaugos profilio priskyrimas į **Klausti**. Tinklo apsauga konfigūruojama visada, kai jūsų kompiuteris jungiasi prie naujo tinklo.



Galite rinktis iš šių tinklo ryšio profilių:

Automatinis – ESET Internet Security profilis bus parinktas automatiškai, pagal kiekvienam profiliui sukonfigūruotus aktyvatorius.

Asmeninis – patikimam tinklui (namų arba biuro tinklui). Kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuteryje saugomus failus bei pasiekti sistemos išteklius (suteikta prieiga prie bendrinamų failų ir spausdintuvų, gaunamas RPC ryšys yra įgalintas ir leidžiama bendrinti nuotolinį darbalaukį). Rekomenduojame naudoti šį parametrą jungiantis prie saugaus vietinio tinklo. Šis profilis automatiškai priskiriamas tinklo ryšiui, jei jis sukonfigūruotas kaip domenas arba privatus tinklas Windows.

Viešasis – nepatikimam tinklui (viešajam tinklui). Failai ir aplankai jūsų sistemoje nėra bendrinami su kitais tinklo vartotojais arba nematomi kitiems vartotojams, o sistemos išteklių bendrinimas išjungiamas. Rekomenduojame naudoti šį parametrą, kai naudojatės belaidžiais tinklais. Šis profilis automatiškai priskiriamas bet kokiam tinklo ryšiui, kuris nesukonfigūruotas kaip domenas arba privatus tinklas Windows.

Naudotojo nustatytas profilis – išplečiamajame meniu galite pasirinkti jūsų sukurtą profilį. Ši parinktis galima tik tuo atveju, jei sukūrėte bent vieną pasirinktinį profilį.

⚠ Neteisingai sukonfigūravus tinklą jūsų kompiuterio saugai gali iškilti grėsmė.

Įjungti Anti-Theft

Kasdien iš namų vykstant į darbą ar kitose viešose vietose nuolat kyla pavojus, kad savo asmeninius įrenginius pamesite arba juos pavogs. Anti-Theft – funkcija, leidžianti padidinti naudotojo lygio apsaugą pamesto arba pavogto įrenginio atveju. Anti-Theft suteikia galimybę stebėti įrenginio naudojimą ir nustatyti jūsų pamesto įrenginio vietą nustatant IP adresą ESET HOME – tai padės įrenginį atgauti ir apsaugoti asmens duomenis.

Tokios modernios Anti-Theft technologijos kaip geografinė IP adresų paieška, vaizdo fiksavimas saityno kamera, naudotojo paskyros apsauga ir įrenginio stebėjimas gali padėti jums ir teisėsaugos organizacijoms surasti jūsų kompiuterį ar įrenginį, jei jį pamestumėte ar pavogtų. ESET HOME galite matyti, kokia veikla vykdoma kompiuteryje arba įrenginyje.

Norėdami sužinoti daugiau apie Anti-Theft programoje ESET HOME, žr. ESET HOME Internetinis žinynas.

„Anti-Theft“ gali netinkamai veikti domenų kompiuteriuose dėl naudotojų paskyrų valdymo apribojimų.

Norėdami įgalinti Anti-Theft ir apsaugoti įrenginį praradimo ar vagystės atveju, pasirinkite vieną iš šių parinkčių:

- Pasirinkite Pagrindinis programos langas > **Apžvalga** ekrane spustelėkite **NUSTATYTI** šalia **Anti-Theft**.
- Jei pagrindinio programos lango **Apžvalga** ekrane matote pranešimą „Anti-Theft“ pasiekiama“, spustelėkite **Įgalinti Anti-Theft**.
- Pagrindiniame programos lange spustelėkite **Nustatymai** > **Saugumo priemonės**. Įjunkite perjungiklį **Anti-Theft** ir vykdykite ekrane pateikiamas instrukcijas.

Jei įrenginys neprijungtas prie ESET HOME, turite atlikti šiuos veiksmus:
1. Prisijunkite prie ESET HOME paskyros, kai įgalinate Anti-Theft.
2. Nustatyti įrenginio pavadinimą.

Anti-Theft nepalaiko Microsoft Windows Home Server.

Įgalinę Anti-Theft, galite optimizuoti įrenginio saugą pagrindiniame programos lange > **Nustatymai** > **Saugumo priemonės** > **Anti-Theft**.

Tėvų kontrolė

Jei naudodami ESET Internet Security jau įjungėte tėvų kontrolę, turite sukonfigūruoti ir visoms susijusioms vartotojų paskyroms skirtą tėvų kontrolę.

Kai tėvų kontrolė yra aktyvi ir naudotojų paskyros nesukonfigūruotos, „ESET Internet Security“ **apžvalgos** ekrane rodomas pranešimas „Tėvų kontrolė nenustatyta“. Spustelėkite **Nustatyti taisykles** ir skaitykite skyrių Tėvų kontrolė, kuriame pateikiama išsamesnė informacija.

Produkto aktyvinimas

Yra keletas būdų, kuriais galite suaktyvinti produktą. Konkretus aktyvinimo scenarijus aktyvinimo lange gali skirtis ir priklauso nuo šalies ir platinimo būdo (CD / DVD, ESET tinklalapis ir t. t.).

- Jei įsigijote mažmeninę produkto versiją dėžutėje arba gavote el. laišką su prenumeratos informacija, aktyvinkite produktą spustelėdami **Naudoti įsigytą aktyvinimo raktą**. Kad aktyvinimas būtų sėkmingas, aktyvinimo raktą reikia įvesti tokį, koks jis yra pateiktas. Aktyvinimo raktas – tai unikali simbolių seka, atitinkanti formatą „XXXX-XXXX-XXXX-XXXX-XXXX“ arba „XXXX-XXXXXXXX“ ir naudojama prenumeratos savininkui identifikuoti bei produktui aktyvinti. Aktyvinimo raktas paprastai yra produkto pakuotės viduje arba ant jos galinės nugarėlės.

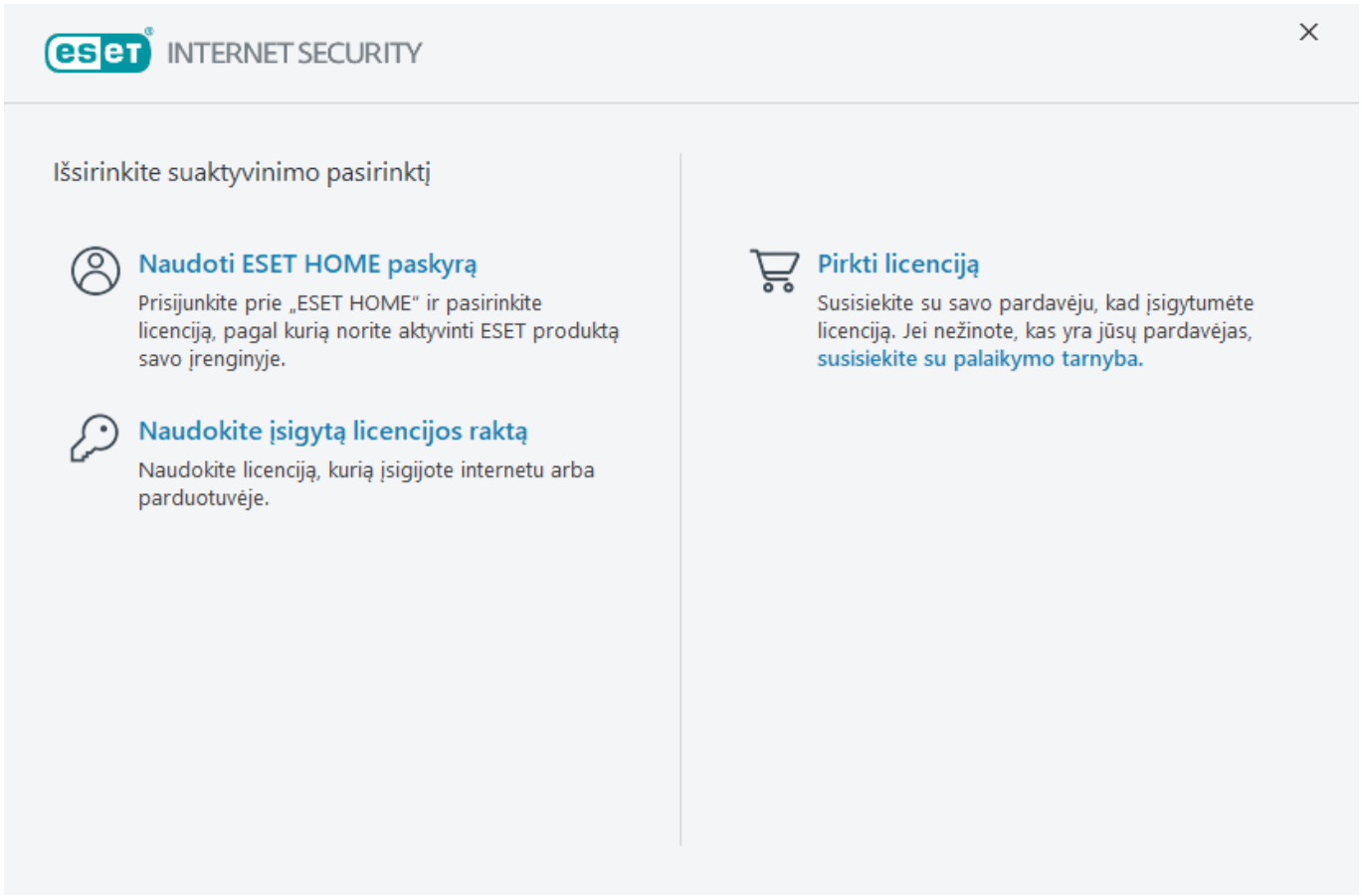
- Pasirinkę Naudoti ESET HOME paskyrą, būsite paraginti prisijungti prie savo ESET HOME paskyros.

- Jei prieš pirkdami norite įvertinti ESET Internet Security, pasirinkite Nemokama bandomoji licencija. Įveskite savo el. pašto adresą ir šalį, kad suaktyvintumėte ESET Internet Security ribotam laikotarpiui. Jūsų nemokama bandomoji versija bus išsiųsta jums el. paštu. Nemokama bandomoji versija gali būti aktyvinta tik vieną kartą vienam klientui.

- Jei neturite prenumeratos ir norite ją įsigyti, spustelėkite **Įsigyti prenumeratą**. Tai nukreips jus į jūsų vietinio ESET atstovo svetainę. ESET „Windows“ namų produktų prenumeratos nėra nemokamos.

Produkto prenumeratą galite pakeisti bet kuriuo metu. Jei norite tai padaryti, pagrindiniame programos lange spustelėkite **Žinynas ir palaikymas** > **Keisti prenumeratą**. Matysite viešą ID, pagal kurį ESET techninės pagalbos tarnyba identifikuoja jūsų prenumeratą.

Nepavyko aktyvinti produkto?



Aktyvinimo rakto įvedimas aktyvinimo metu

Automatiniai atnaujinimai yra svarbūs jūsų saugumui. ESET Internet Security gaus atnaujinimus tik jį suaktyvinus.

Įvedant **aktyvinimo raktą**, svarbu jį įvesti tiksliai taip, kaip jis užrašytas. Aktyvinimo raktas – tai unikali simbolių seka, atitinkanti formatą XXXX-XXXX-XXXX-XXXX-XXXX ir naudojama prenumeratos savininkui identifikuoti bei prenumeratai aktyvinti.

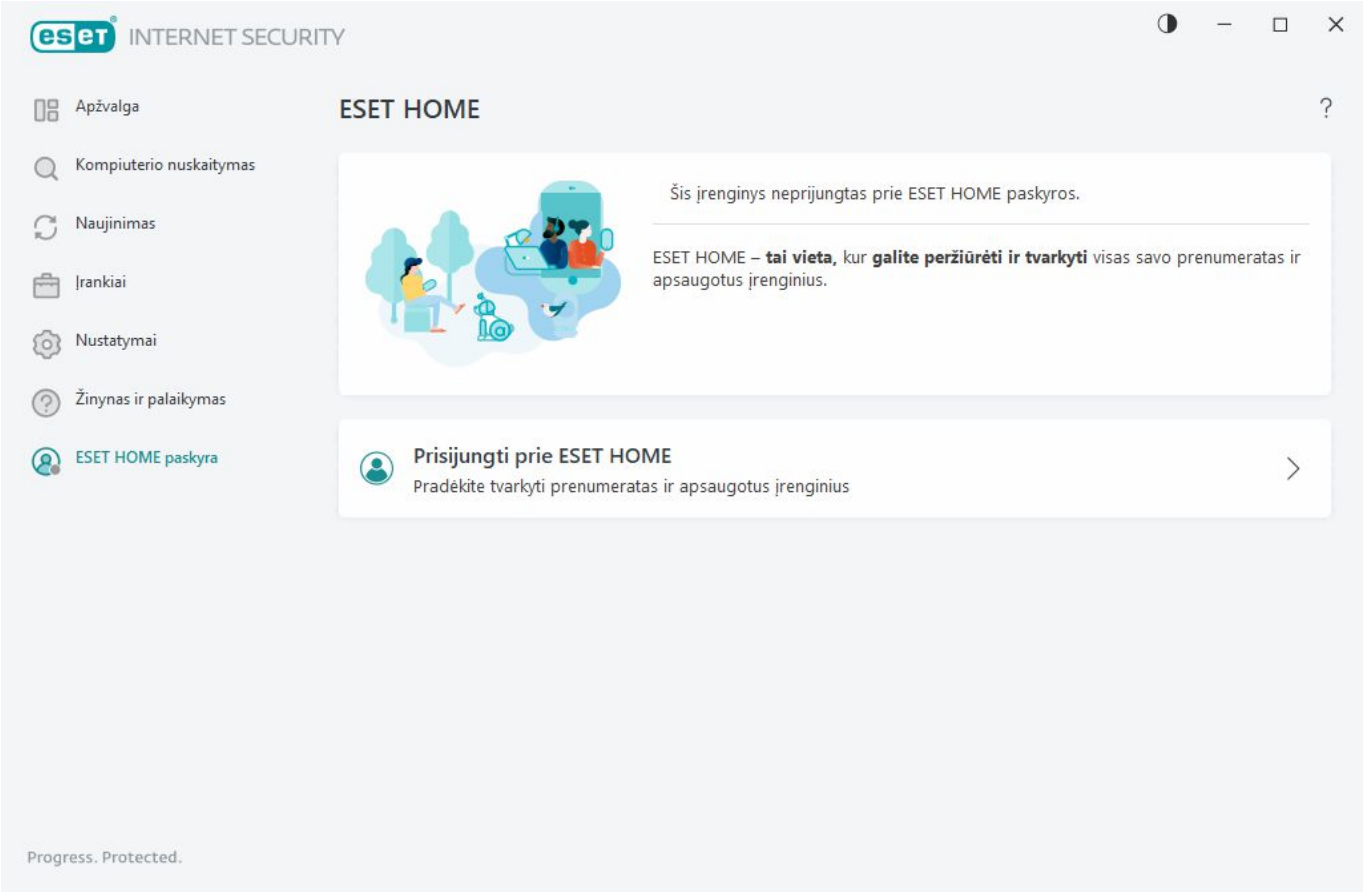
Kad viską atliktumėte tiksliai, aktyvinimo raktą rekomenduojame įklijuoti nukopijavus iš registracijos el. laiško.

Jei baigę diegti neįvedėte aktyvinimo rakto, jūsų produktas nebus aktyvintas. Galite aktyvinti „ESET Internet Security“ pasirinkę pagrindinis programos langas > **Žinynas ir palaikymas** > **Aktyvinti prenumeratą**.

ESET „Windows“ namų produktų prenumeratos nėra nemokamos.

Naudoti ESET HOME paskyrą

Susiekite įrenginį su ESET HOME, kad peržiūrėtumėte ir valdytumėte visas savo aktyvintas ESET prenumeratas ir įrenginius. Galite atnaujinti, naujovinti ar pratęsti prenumeratą bei peržiūrėti svarbią prenumeratos informaciją. ESET HOME valdymo portale arba mobiliojoje programėlėje galite pridėti kitų prenumeratų, atsisiųsti produktus į savo įrenginius, patikrinti produkto saugos būseną ar bendrinti prenumeratas el. paštu. Daugiau informacijos rasite apsilankę ESET HOME internetiniame žinyne.



Pasirinkus **Naudoti ESET HOME paskyrą** kaip aktyvinimo būdą ar prijungtiant prie ESET HOME paskyros diegimo metu:

1. Prisijungti prie savo ESET HOME paskyros.

> Jeigu dar neturite ESET HOME paskyros, spustelėkite **Sukurti paskyrą**, kad užsiregistruotumėte arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.
> Jei pamiršote slaptažodį, spustelėkite **Pamiršau savo slaptažodį** ir atlikite ekrane pateikiamus veiksmus arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.

2. Nustatykite savo **įrenginio pavadinimą**, kuris bus naudojamas visose ESET HOME paslaugose, ir spustelėkite **Tęsti**.

3. Pasirinkite norimą aktyvinti prenumeratą arba pridėkite naują prenumeratą. Spustelėkite **Tęsti**, kad suaktyvintumėte ESET Internet Security.

Aktyvinti nemokamą bandomąją versiją

Norėdami aktyvinti ESET Internet Security bandomąją versiją, įveskite galiojantį el. pašto adresą laukuose **El. pašto adresas** ir **Patvirtinti el. pašto adresą**. Aktyvinus, jūsų ESET prenumerata bus sugeneruota ir išsiųsta jūsų el. pašto adresu. Šis el. pašto adresas bus naudojamas norint pranešti apie produkto galiojimo pabaigą ir kitaip susisiekti su ESET. Nemokamą bandomąją versiją galima aktyvinti tik vieną kartą.

Pasirinkite savo šalį išskleidžiamajame meniu **Šalis**, kad užregistruotumėte ESET Internet Security pas vietinį atstovą, kuris teiks techninį palaikymą.

Nemokamas ESET aktyvinimo raktas

„ESET Internet Security“ prenumerata nėra nemokama.

ESET aktyvinimo raktas yra išskirtinė brūkšniu atskirtų raidžių ir skaičių seka, kurią suteikia ESET, kad galėtumėte teisėtai naudotis ESET Internet Security pagal galutinio naudotojo licencijos sutartį. Kiekvienam galutiniam naudotojui suteikiama teisė naudoti aktyvinimo raktą tik tiek, kiek jis teisėtai gali naudotis „ESET Internet Security“, atsižvelgiant į ESET suteiktų licencijų skaičių. Aktyvinimo raktas laikomas konfidencialiu ir jo negalima bendrinti; tačiau galite bendrinti prenumeratą naudodami ESET HOME.

Internete yra šaltinių, kurie jums gali suteikti „nemokamą“ ESET aktyvinimo raktą, bet atminkite:

- Spustelėjus skelbimą „Nemokama ESET prenumerata“, galima sukelti pavojų kompiuteriui arba įrenginiui ir užkrėsti jį kenkėjiška programine įranga. Kenkėjiška programinė įranga gali slypėti neoficialiame žiniatinklio turinyje (pvz., vaizdo įrašuose), svetainėse, kuriose siūloma užsidirbti pinigų lankantis svetainėse, ir t. t. Paprastai tai būna spąstai.
- ESET išjungia piratinę prenumeratą.
- Piratinių aktyvinimo raktų naudojimas nesuderintas su galutinio naudotojo licencijos sutartimi, su kuria turite sutikti, norėdami įdiegti „ESET Internet Security“.
- ESET prenumeratą įsigykite tik iš oficialių kanalų, pvz., www.eset.com, ESET platintojų arba pardavėjų (nepirkite prenumeratos iš neoficialių trečiųjų šalių svetainių, pvz., eBay arba bendros prenumeratos iš trečiųjų šalių).
- Atsisiųsti ESET Internet Security galima nemokamai, bet norint aktyvinti diegimo metu, būtinas ESET aktyvinimo raktas (galite ją atsisiųsti ir įdiegti, bet neaktyvinta ji neveiks).
- Nebendrinkite savo prenumeratos internete arba socialiniame tinkle (ji gali paplisti).

Norėdami atpažinti ir pranešti apie ESET prenumeratą, apsilankykite mūsų žinių bazės straipsnyje, kuriame pateikiami nurodymai.

Jei dvejojate, ar įsigyti ESET saugos produktą, galite pasinaudoti bandomąja versija, kuri padės apsispręsti:

1. Aktyvinkite „ESET Internet Security“ naudodami nemokamą bandomąją versiją
2. Dalyvaukite ESET Beta programoje
3. Jei naudojate „Android“ mobilųjį įrenginį, įdiekite „ESET Mobile Security“ – ji nemokama.

Norėdami gauti nuolaidą / pratęsti licenciją, Atnaujinkite savo ESET.

Aktyvinti nepavyko – dažniausi scenarijai

Jei ESET Internet Security aktyvinimas nesėkmingas, dažniausiai pasitaikantys scenarijai yra tokie:

- Aktyvinimo raktas jau naudojamas.

- Įvedėte netinkamą aktyvinimo raktą.
- Trūksta informacijos aktyvinimo formoje arba ji negalioja.
- Ryšys su aktyvinimo serveriu nutrūko.
- Nėra ryšio su ESET aktyvinimo serveriais arba ryšys išjungtas.

Patikrinkite, ar įvedėte tinkamą aktyvinimo raktą ir ar jūsų interneto ryšys aktyvus. Pabandykite suaktyvinti „ESET Internet Security“ dar kartą. Jei aktyvinimui naudojate ESET HOME paskyrą, žr. ESET HOME prenumerata ir prenumeratos valdymas – žinynas internete.

Jei gaunate konkretų klaidos pranešimą (pvz., sulaikyta arba Pereikvota prenumerata), vadovaukitės prenumeratos būsenos nurodymais.

Jei vis tiek negalite aktyvinti ESET Internet Security, ESET aktyvinimo trikčių diagnostikos priemonė padės išspręsti dažniausius aktyvinimo ir licencijavimo klausimus, klaidas ir problemas (pateikiama anglų ir keliomis kitomis kalbomis).

Prenumeratos būsena

Jūsų prenumeratos būsena gali skirtis. Prenumeratos būseną galite rasti ESET HOME. Norėdami pridėti prenumeratą prie savo ESET HOME paskyros, žr. Pridėti prenumeratą.

Jei neturite ESET HOME paskyros, galite Sukurti naują „ESET HOME“ paskyrą.

Jei prenumeratos būsena skiriasi nuo **aktyvios**, aktyvinimo metu gausite klaidą arba pranešimą pagrindiniame programos lange.

Norėdami išjungti prenumeratos būsenos pranešimus, atidarykite Išplėstinis nustatymas > **Pranešimai** > **Programos būsenos**. Spustelėkite **Redaguoti** šalia **Programos būsenos**, išplėskite **Licencijavimas** ir panaikinkite žymės langelio, esančio šalia pranešimo, kurį norite išjungti, žymėjimą. Išjungus pranešimą problema neišsprendžiama.

Peržiūrėkite įvairių prenumeratų būsenų aprašymus ir rekomenduojamus sprendimus toliau pateiktoje lentelėje:

Prenumeratos būsena	Aprašymas	Sprendimas
Aktyvi	Prenumerata galioja ir be jūsų sąveikos. „ESET Internet Security“ galima aktyvinti, o išsamią prenumeratos informaciją rasite pasirinkę pagrindinis programos langas > **Žinynas ir palaikymas**.	
Pereikvota	Ši prenumerata naudojama daugiau įrenginių, nei leidžiama. Gausite aktyvinimo klaidą.	Daugiau informacijos rasite skiltyje Aktyvinti nepavyko dėl pereikvotos prenumeratos.

Prenumeratos būsena	Aprašymas	Sprendimas
Sulaikyta	Jūsų prenumerata buvo sulaikyta dėl mokėjimo problemų. Jei norite naudoti prenumeratą, įsitikinkite, kad jūsų mokėjimo informacija ESET HOME yra atnaujinta, arba susisiekite su prenumeratos pardavėju. Šią klaidą galite matyti aktyvinimo metu arba pagrindiniame programos lange.	Įdiegtas produktas – jei turite ESET HOME paskyrą, pagrindiniame programos lange rodomame pranešime spustelėkite **Tvarkyti prenumeratą ESET HOME** ir peržiūrėkite išsamią mokėjimo informaciją. Kitu atveju susisiekite su prenumeratos pardavėju. Aktyvinimo klaida – jei turite „ESET HOME“ paskyrą, aktyvinimo klaidos lange spustelėkite **Atidaryti „ESET HOME“** ir peržiūrėkite išsamią mokėjimo informaciją. Kitu atveju susisiekite su prenumeratos pardavėju.
Nebegalioja	Jūsų prenumeratos galiojimas baigėsi ir jūs negalite naudoti šios prenumeratos „ESET Internet Security“ aktyvinti. Šią klaidą galite matyti aktyvinimo metu arba pagrindiniame programos lange. Jei „ESET Internet Security“ jau įdiegėte, jūsų kompiuteris nėra apsaugotas ir atnaujintas.	Įdiegtas produktas – pagrindiniame programos lange rodomame pranešime spustelėkite **Atnaujinti prenumeratą** ir vykdykite nurodymus, pateiktus skiltyje Kaip atnaujinti prenumeratą?, arba spustelėkite **Aktyvinti produktą** ir pasirinkite aktyvinimo būdą. Aktyvinimo klaida – aktyvinimo klaidos lange spustelėkite **Atnaujinti prenumeratą** ir vykdykite nurodymus, pateiktus skiltyje Kaip atnaujinti prenumeratą?, arba įveskite naują arba atnaujintą aktyvinimo raktą ir spustelėkite **Atnaujinti prenumeratą**.
Atšaukta	Jūsų prenumeratą atšaukė ESET arba prenumeratos pardavėjas.	Jei gaunate klaidos pranešimą: Atšaukta prenumerata pagrindiniame programos lange arba aktyvinimo metu, bet jūsų prenumerata turėtų veikti tinkamai, susisiekite su prenumeratos pardavėju.

Aktyvinti nepavyko dėl pereikvotos prenumeratos

Problema

- Jūsų prenumerata gali būti pereikvota arba ja gali būti piktnaudžiaujama
- Aktyvinti nepavyko dėl pereikvotos prenumeratos

Sprendimas

Yra daugiau įrenginių, kuriems naudojama ši prenumerata, nei leidžiama. Jūs galite būti programinės įrangos piratavimo ar padirbinėjimo auka. Prenumeratos negalima naudoti jokiam kitam ESET produktui aktyvinti. Šią problemą galite išspręsti tiesiogiai, jei jums leidžiama valdyti prenumeratą savo ESET HOME paskyroje arba įsigijote prenumeratą iš teisėto šaltinio. Jei dar neturite paskyros, sukurkite ją.

Jei esate prenumeratos savininkas ir nebuvote paraginti įvesti savo el. pašto adreso:

1. Norėdami tvarkyti savo ESET prenumeratą, atidarykite saityno naršyklę ir eikite į https://home.eset.com. Eikite į ESET License Manager ir pašalinkite arba išjunkite įrenginius. Daugiau informacijos žr. skiltyje Ką daryti, jei prenumerata pereikvota.

2. Norėdami atpažinti ir pranešti apie piratinę ESET prenumeratą, nurodymus žr. straipsnyje Kaip atpažinti ir pranešti apie piratinę ESET prenumeratą.

3. Jei nesate tikri, spustelėkite **Atgal** ir el. paštu kreipkitės į ESET techninės pagalbos tarnybą.

Jei nesate prenumeratos savininkas, susisiekite su šios prenumeratos savininku ir praneškite jam, kad negalite aktyvinti ESET produkto, nes prenumerata pereikvota. Savininkas gali išspręsti šią problemą naudodamas ESET HOME portalą.

Jei esate paraginami patvirtinti savo el. pašto adresą (tik keli atvejai), įveskite el. pašto adresą, kurį naudojote pirkdami arba aktyvindami savo ESET Internet Security.

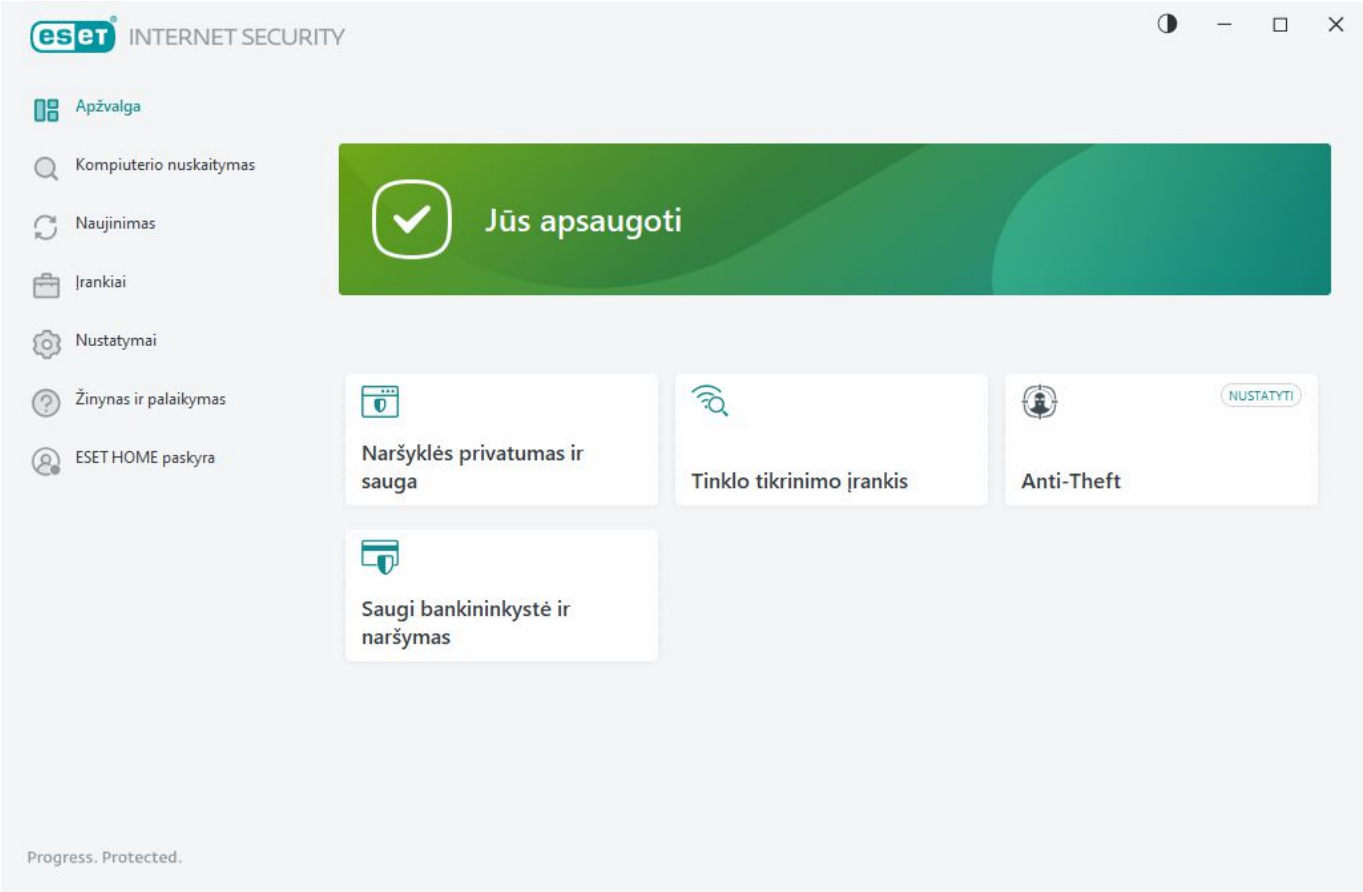
Darbas su ESET Internet Security

„ESET Internet Security“ pagrindinis programos langas padalytas į dvi dalis. Dešinėje esantis pagrindinis langas rodo informaciją, kuri atitinka kairėje esančiame pagrindiniame meniu pasirinktą parinktį.

> **Iliustruotos instrukcijos**
> Peržiūrėkite iliustruotas instrukcijas anglų ir keliomis kitomis kalbomis, kaip Atidaryti pagrindinį ESET „Windows“ produktų langą.

„ESET Internet Security“ GUI spalvų schemą galite pasirinkti viršutiniame dešiniajame pagrindinio programos lango kampe. Spustelėkite piktogramą **Spalvų schema** (piktograma kinta pagal šiuo metu pasirinktą spalvų schemą) šalia piktogramos **Minimizuoti** ir pasirinkite spalvų schemą išskleidžiamajame meniu:

- **Tas pats, kas sistemos spalva** – nustato „ESET Internet Security“ spalvų schemą pagal operacinės sistemos nustatymus.
- **Tamsus** – „ESET Internet Security“ turės tamsią spalvų schemą (tamsusis režimas).
- **Šviesus** – „ESET Internet Security“ turės standartinę, šviesią spalvų schemą.



Pagrindinio meniu parinktys:

Apžvalga – pateikia informaciją apie ESET Internet Security apsaugos būseną.

Kompiuterio nuskaitymas – sukonfigūruokite ir paleiskite kompiuterio nuskaitymą arba sukurkite pasirinktinį nuskaitymą.

Naujinimas – rodo informaciją modulį apie aptikimo modulio atnaujinimus.

Įrankiai – suteikia prieigą prie Tinklo tikrinimo įrankis ir kitų funkcijų, kurios padeda palengvinti programos administravimą ir siūlo papildomas parinktis patyrusiems naudotojams.

Nustatymai – pateikia ESET Internet Security apsaugos funkcijų (Kompiuterių apsauga, Interneto apsauga, tinklo apsauga ir saugumo priemonės) ir prieigos prie Išplėstinis nustatymas konfigūravimo parinktis.

Žinynas ir palaikymas – rodoma informacija apie jūsų prenumeratą, įdiegtą ESET produktą ir pateikiamos nuorodos į žinyną internete, ESET žinių bazę ir techninę pagalbą.

„ESET HOME“ paskyra – prijunkite įrenginį prie „ESET HOME“ arba peržiūrėkite „ESET HOME“ paskyros ryšio būseną. Naudokite ESET HOME, norėdami peržiūrėti ir tvarkyti savo Anti-Theft nustatymus ir aktyvintą ESET prenumeratą bei įrenginius.

Apžvalga

Lange **Apžvalga** rodoma informacija apie dabartinę kompiuterio apsaugą kartu su sparčiaisiais saitais į saugos funkcijas, esančias „ESET Internet Security“.

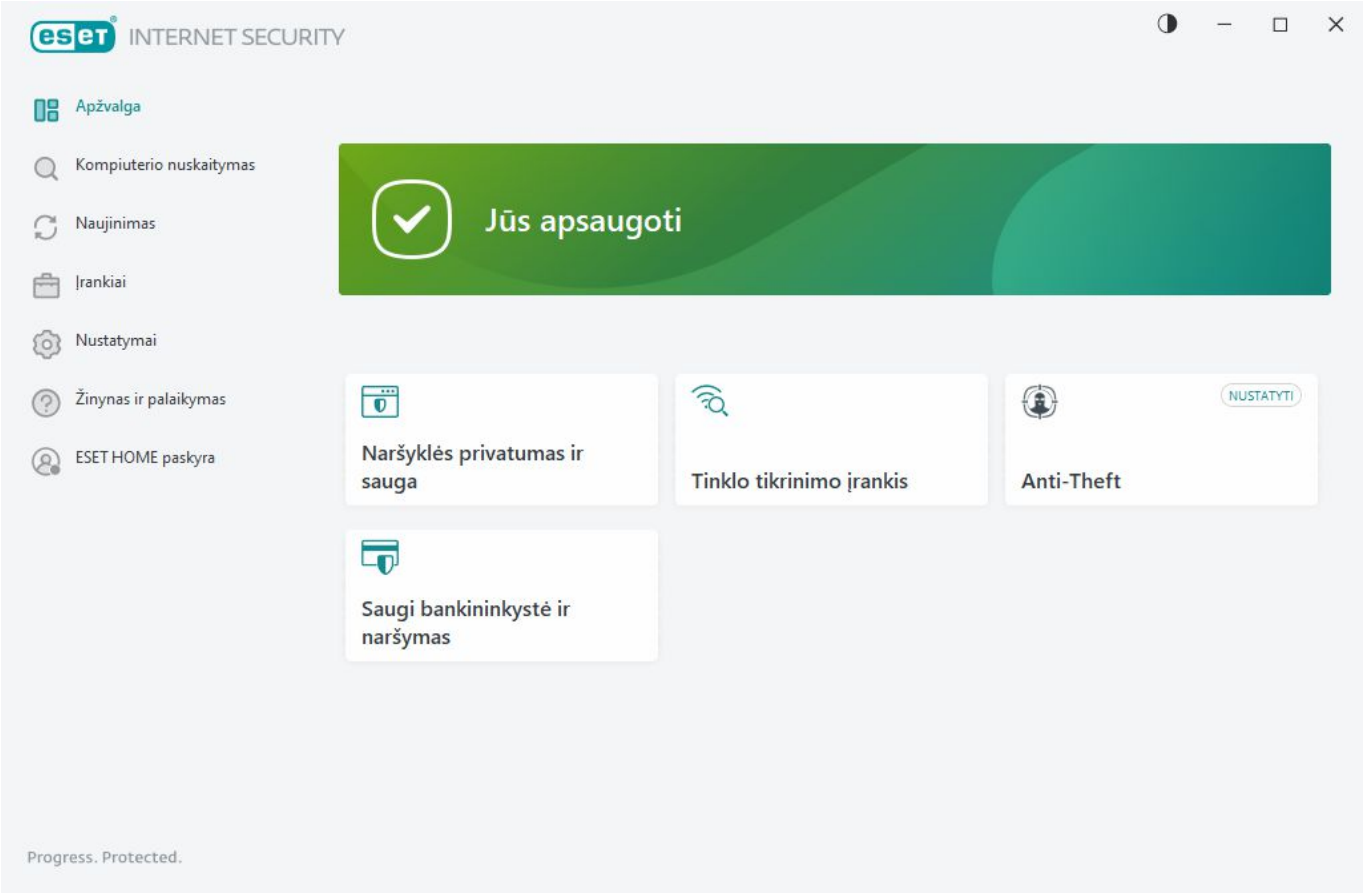
Lange **Apžvalga** rodomi pranešimai su išsamia informacija ir rekomenduojamais sprendimais, kaip pagerinti „ESET

Internet Security“ saugumą, įjungti papildomas funkcijas arba užtikrinti maksimalią apsaugą. Jei pranešimų yra daugiau, spustelėkite **X daugiau pranešimų**, kad išplėstumėte viską.

Tinklo tikrinimo įrankis – Patikrinkite savo tinklo saugumą

Saugi bankininkystė ir naršymas – saugiuoju režimu paleidžiama naršyklė, „Windows“ nustatyta kaip numatytoji.

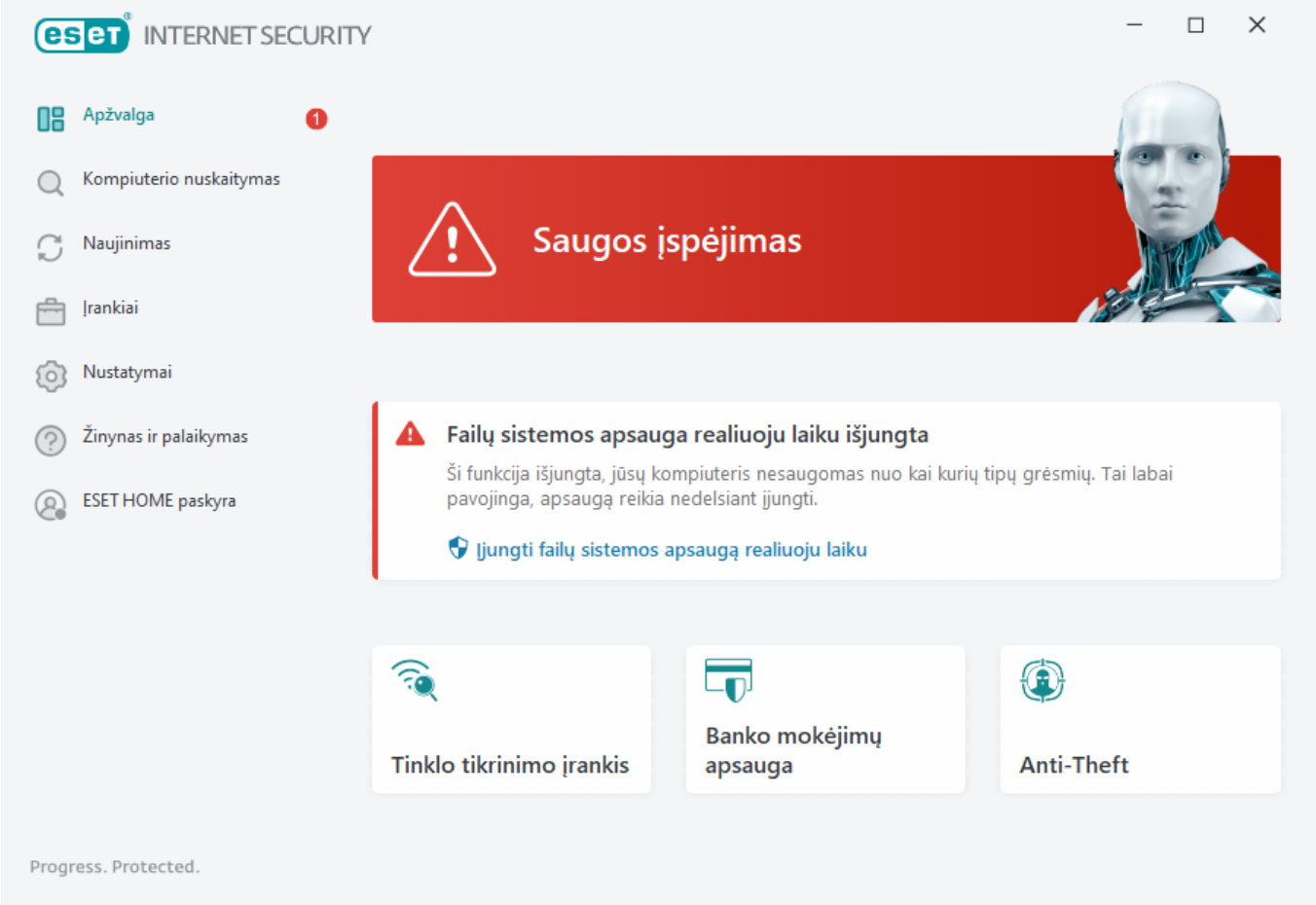
Anti-Theft – pradedamas Anti-Theft nustatymas. Jei jau nustatėte Anti-Theft, greitąja nuoroda atidaromas Anti-Theft puslapis.



Žalia piktograma ir žalia būsena **Esate apsaugoti** rodo, kad užtikrinama didžiausia apsauga.

Ką daryti, jei programa neveikia tinkamai

Jei aktyvus apsaugos modulis veikia tinkamai, jo apsaugos būsenos piktograma bus žalia. Raudonas šauktukas arba oranžinė pranešimo piktograma rodo, kad maksimali apsauga nėra užtikrinta. Papildoma informacija apie kiekvieno modulio apsaugos būseną bei siūlomi sprendimai, kaip atkurti geriausią apsaugą, rodomi lange **Apžvalga**, kaip pranešimas. Norėdami pakeisti atskirų modulių būseną, spustelėkite **Nustatymai** ir pasirinkite norimą modulį.



Raudona piktograma ir raudona **saugos įspėjimo** būsena rodo, kad yra kritinių problemų.
Ši būsena gali būti rodoma dėl kelių priežasčių, pavyzdžiui:

- **Produktas nesuaktyvintas** arba **Prenumeratos galiojimas baigėsi** – apie tai praneša raudona apsaugos būsenos piktograma. Kai baigiasi prenumeratos galiojimas, programos negalima atnaujinti. Laikydamiesi įspėjimo lange pateikiamų nurodymų, atnaujinkite prenumeratą.
- **Aptikimo modulis pasenęs** – ši klaida bus parodoma po keleto nesėkmingų bandymų atnaujinti aptikimo modulį. Rekomenduojame patikrinti naujinimo parametrus. Dažniausiai pasitaikanti šios klaidos priežastis yra neteisingai įvesti atpažinimo duomenys arba neteisingai sukonfigūruoti ryšio parametrai.
- **Failų sistemos apsauga realiuoju laiku išjungta** – apsaugą realiuoju laiku išjungė naudotojas. Jūsų kompiuteris neapsaugotas nuo grėsmių. Tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti failų sistemos apsaugą realiuoju laiku**.
- **Apsauga nuo virusų ir šnipinėjimo programų išjungta** – apsaugą nuo virusų ir šnipinėjimo programų galite vėl įjungti spustelėdami **Įjungti apsaugą nuo virusų ir šnipinėjimo programų**.
- **ESET užkarda išjungta** – apie šią problemą praneša saugos pranešimas šalia darbalaukio elemento **Tinklas**. Tinklo apsaugą galite vėl įjungti spustelėdami **Įjungti užkardą**.

Oranžinė piktograma rodo, kad apsauga yra ribota. Pavyzdžiui, kilo problemų atnaujinant programą arba jūsų prenumeratos galiojimas eina į pabaigą.
Ši būsena gali būti rodoma dėl kelių priežasčių, pavyzdžiui:

- **„Anti-Theft“ optimizavimo įspėjimas** – šis įrenginys nėra optimizuotas sistemai Anti-Theft. Pavyzdžiui, gali būti, kad kompiuteryje nesukurta fiktyvi paskyra (saugos funkcija, kuri suaktyvinama

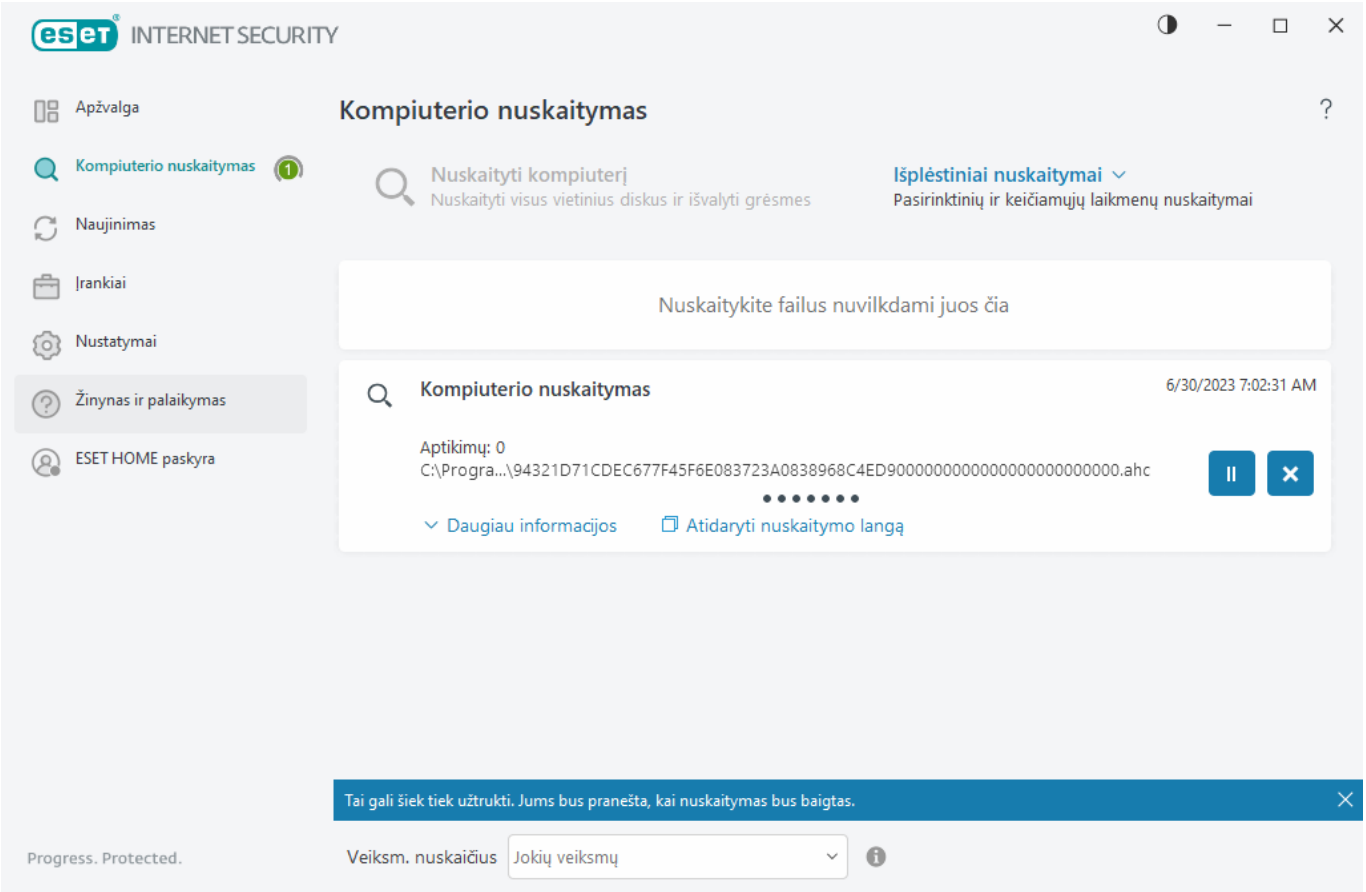
automatiškai, kai įrenginį pažymite kaip pamestą. Fiktyvią paskyrą galite sukurti naudodamiesi funkcija Optimizavimas, kurią rasite Anti-Theft saityno sąsajoje.

- **Žaidimų režimas aktyvus** – įjungtas Žaidimų režimas gali kelti pavojų kompiuterio saugumui. Įjungus šią funkciją išjungiami visi pranešimai / perspėjimo langai ir sustabdomos visos suplanuotos užduotys.
- **Jūsų prenumerata netrukus baigs galioti/Jūsų prenumerata baigia galioti šiandien** – apie tai praneša apsaugos būsenos piktograma, rodoma kaip šauktukas šalia sistemos laikrodžio. Kai jūsų prenumeratos galiojimas pasibaigia, programos negalima atnaujinti ir apsaugos būsenos piktograma tampa raudona.

Jei nepavyksta išspręsti problemos naudojant siūlomus sprendimus, spustelėkite **Žinynas ir palaikymas**, kad galėtumėte pasinaudoti žinyno failais arba ieškoti ESET žinių bazėje. Jei vis dar reikia pagalbos, galite pateikti pagalbos prašymą. ESET techninės pagalbos tarnyba greitai atsakys į jūsų klausimus ir padės rasti sprendimą.

Kompiuterio nuskaitymas

Nuskaitymo pareikalavus modulis yra svarbi jūsų antivirusinio sprendimo dalis. Jis naudojamas failams ir katalogams jūsų kompiuteryje nuskaityti. Saugai užtikrinti svarbu, kad kompiuterio nuskaitymai būtų atliekami reguliariai kaip įprastos saugos priemonės, o ne tik tuomet, kai įtariamas užkratas. Rekomenduojame reguliariai vykdyti sistemos išsamaus nuskaitymo procedūras, kad aptiktumėte virusus, kurių neranda Failų sistemos apsauga realiuoju laiku, kai jie įrašomi į diską. Taip gali nutikti, jei failų sistemos apsauga realiuoju laiku kažkuriuo metu buvo išjungta, paseno aptikimo modulis arba failas neaptiktas kaip virusas, kai jis buvo įrašomas į diską.



Yra du **kompiuterio nuskaitymo** tipai. **Nuskaityti kompiuterį** leidžia greitai nuskaityti sistemą nenurodant nuskaitymo parametrų. **Pasirinktinis nuskaitymas** (išplėstinių nuskaitymų skiltyje) leidžia pasirinkti kurį nors iš anksto nustatytų nuskaitymo profilių, skirtų konkrečioms vietoms, ir leidžia pasirinkti konkrečius nuskaitymo

tikslus.

Žiūrėkite Nuskaitymo eiga, kur pateikiama daugiau informacijos apie nuskaitymo procesą.

> Pagal numatytuosius nustatymus ESET Internet Security bandoma automatiškai išvalyti arba pašalinti aptikimus, rastus kompiuterio nuskaitymo metu. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, gaunate interaktyvų įspėjimą ir turite pasirinkti valymo veiksmą (pvz., šalinti arba nepaisyti). Norėdami pakeisti valymo lygį ir gauti išsamesnės informacijos, žr. Valymas. Norėdami peržiūrėti ankstesnius nuskaitymus, žr. Žurnalo failai.

Nuskaityti jūsų kompiuterį

Kompiuterio nuskaitymas suteikia galimybę greitai paleisti kompiuterio nuskaitymą ir išvalyti užkrėstus failus vartotojui neatliekant jokių veiksmų. **Kompiuterio nuskaitymo** privalumai yra paprastas naudojimas ir tai, kad jam nereikalinga išsami nuskaitymo konfigūracija. Kompiuterio nuskaitymas tikrina visus failus vietiniuose įrenginiuose ir automatiškai išvalo arba panaikina aptiktus įsiskverbimus. Valymo lygis automatiškai nustatomas į numatytąjį. Išsamesnės informacijos apie valymo tipus rasite skyriuje Valymas.

Be to, failui ar aplankui nuskaityti rankiniu būdu galite naudoti funkciją **Nuvilkti ir nuskaityti** – tiesiog spustelėkite failą ar palanką ir laikydami nuspaudę pelės mygtuką perkelkite pelės žymeklį į pažymėtą sritį, tada mygtuką atleiskite. Tada programa perkeliama į pirmą planą.

Šios nuskaitymo parinktys galimos atliekant **išplėstinius nuskaitymus**:

Pasirinktinis nuskaitymas

Naudodami **pasirinktinį nuskaitymą** galėsite nurodyti nuskaitymo parametrus, tokius kaip nuskaitymo tikslai ir metodai. **Pasirinktinio nuskaitymo** pranašumas yra tas, kad galite išsamiai konfigūruoti parametrus. Konfigūracijos gali būti išsaugotos vartotojo apibrėžtuose nuskaitymo profiliuose, kurie gali būti naudingi, jeigu nuskaitymas yra pakartotinai atliekamas su tais pačiais parametrais.

Nešiojamosios laikmenos nuskaitymas

Panašus į **kompiuterio nuskaitymą** – greitai paleidžia šiuo metu prie kompiuterio prijungtos nešiojamosios laikmenos nuskaitymą (pavyzdžiui, CD/DVD/USB). Tai gali būti naudinga, kai prie kompiuterio prijungiate USB atmintuką ir norite nuskaityti jo turinį ieškodami kenkimo programinės įrangos ir kitų galimų grėsmių.

Šio tipo nuskaitymą galima paleisti ir spustelėjus **Pasirinktinis nuskaitymas**, pasirenkant **Nešiojamoji laikmena** iš išskleidžiamojo meniu **Nuskaitymo tikslai** ir spustelėjus **Nuskaityti**.

Kartoti paskutinį nuskaitymą

Galite greitai paleisti anksčiau atliktą nuskaitymą, kuriam bus naudojami tie patys nustatymai.

Veiksmas po nuskaitymo išplečiamajame meniu leidžia nustatyti veiksmą, kuris turi būti atliekamas automatiškai, kai nuskaitymas bus baigtas:

- **Jokių veiksmų** – užbaigus nuskaitymą nebus atliekami jokie veiksmai.
- **Išjungti** – pasibaigus nuskaitymui kompiuteris išjungiamas.

• **Prireikus paleisti iš naujo** – kompiuteris paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.

• **Paleisti iš naujo** – užbaigus nuskaitymą uždaromos visos atidarytos programos, o kompiuteris paleidžiamas iš naujo.

• **Prireikus priversti paleisti iš naujo** – kompiuteris priverstinai paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.

• **Priversti paleisti iš naujo** – priverstinai uždaro visas atidarytas programas nelaukiant naudotojo sąveikos ir iš naujo paleidžia kompiuterį baigus nuskaitymą.

• **Miego režimas** – įrašomas jūsų seansas ir įjungiamas kompiuterio energijos taupymo režimas, kurį išjungę galite greitai tęsti darbą.

• **Sulaikytosios veiksenos režimas** – visus RAM vykdomus procesus perkelia į specialų failą standžiajame diske. Kompiuteris išjungiamas, tačiau kitą kartą įjungę galite tęsti darbą nuo ten, kur baigėte.

Veiksmai **Miego režimas** arba **Sulaikytosios veiksenos režimas** pasiekiami atsižvelgiant į jūsų kompiuterio operacinės sistemos maitinimo ir miego režimo nustatymus arba jūsų stalinio / nešiojamojo kompiuterio galimybes. Atminkite, kad miego režimu veikiantis kompiuteris nėra išjungtas. Jame toliau veikia pagrindinės funkcijos ir vartojama elektros energija, jei kompiuteris veikia naudodamas akumuliatorių. Jei norite pailginti akumuliatoriaus veikimo laiką, pavyzdžiui, išvykę iš biuro, rekomenduojame naudoti sulaikytosios veiksenos režimą.

Pasirinktas veiksmas bus pradėtas užbaigus visus vykdomus nuskaitymus. Pasirinkus **Išjungti** arba **Perkrauti**, patvirtinimo dialogo lange bus rodomas 30 sekundžių atgalinis skaičiavimas (spustelėkite **Atšaukti**, kad išjungtumėte reikalaujamą veiksmą).

Mes rekomenduojame atlikti kompiuterio nuskaitymą mažiausiai kartą per mėnesį. Nuskaitymas gali būti sukonfigūruotas kaip suplanuota užduotis, pasirenkant **Įrankiai** > **Planuoklė**. Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą?

Pasirinktinio nuskaitymo paleidimo priemonė

Naudodami pasirinktinį nuskaitymą galite nuskaityti operacinę atmintį, tinklą ar konkrečias disko dalis, o ne visą diską. Tai galite padaryti spustelėdami **Išplėstiniai nuskaitymai** > **Pasirinktinis nuskaitymas** pasirinkdami konkrečias paskirties vietas aplankų (medžio) struktūroje.

Galite pasirinkti profilį iš išplečiamojo meniu **Profilis**, kuris bus naudojamas nuskaitant konkrečius tikslus. Numatytasis profilis yra **Išmanusis nuskaitymas**. Yra dar trys iš anksto nustatyti nuskaitymo profiliai: **Giluminis nuskaitymas**, **Kontekstinio meniu nuskaitymas** ir **Kompiuterio nuskaitymas**. Šie nuskaitymo profiliai naudoja skirtingus „ThreatSense“ parametrus. Pasiekiamos parinktys aprašytos dalyje Išplėstinis nustatymai > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymas** > **Nuskaitymas pareikalavus** > „ThreatSense“.

Aplanko (medžio) struktūroje taip pat yra konkrečių tikslinių nuskaitymo objektų.

• **Operacinė atmintis** – nuskaito visus procesus ir duomenis, kuriuos šiuo metu naudoja operacinė atmintis.

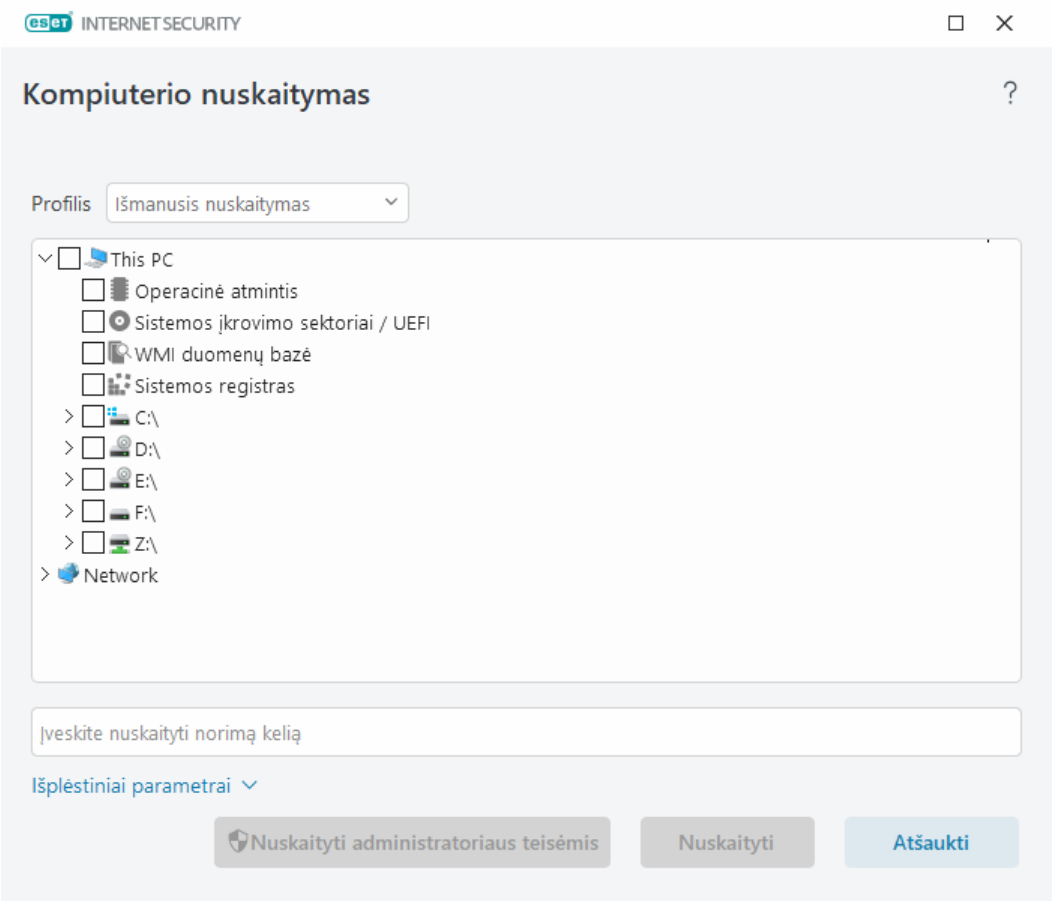
• **Įkrovos sektoriai / UEFI** – nuskaito įkrovos sektorius ir UEFI, siekiant aptikti kenkėjišką programinę įrangą. Daugiau apie UEFI skaitytuvą skaitykite žodynėlėje.

• **WMI duomenų bazė** – nuskaito visą Windows Management Instrumentation WMI duomenų bazę, visus pavadinimus, visus klasės egzempliorius ir visas ypatybes. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis.

• **Sistemos registras** – nuskaito visą sistemos registrą, visus raktus ir antrinius raktus. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis. Valant aptiktus elementus, nuoroda lieka registre, kad įsitikintumėte, jog nebus prarasti svarbūs duomenys.

Norėdami greitai pereiti prie nuskaitymo paskirties vietos (failo ar aplanko), įveskite jo kelią į teksto lauką po medžio struktūra. Kelio pavadinime skiriamos didžiosios ir mažosios raidės. Norėdami įtraukti paskirties vietą į nuskaitymą, pažymėkite jos žymės langelį medžio struktūroje.

> **Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą**
> Norėdami suplanuoti reguliarią užduotį, skaitykite skyrių Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą.



Nuskaitymo valymo parametrus galite sukonfigūruoti dalyje Išplėstiniai nustatymai > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nuskaitymas pareikalavus** >**ThreatSense** > **Valymas**. Norėdami paleisti nuskaitymą be valymo veiksmo, spustelėkite **Išplėstiniai nustatymai** ir pasirinkite **Nuskaityti be valymo**. Nuskaitymo istorija išsaugoma nuskaitymo žurnale.

Kai pasirenkama **Nepaisyti išimčių**, bus be išimčių nuskaitomi ir failai su anksčiau neįtrauktais plėtiniais.

Spustelėkite **Nuskaityti**, kad būtų vykdomas nuskaitymas, naudojant jūsų nustatytus pasirinktinius parametrus.

Mygtuku **Nuskaityti administratoriaus teisėmis** galima vykdyti nuskaitymą iš administratoriaus paskyros. Jį spustelėkite, jei dabartinis vartotojas neturi teisės pasiekti failus, kuriuos norite nuskaityti. Šis mygtukas

nepasiekiamas, jei dabartinis vartotojas negali iškviesti UAC operacijų kaip administratorius.

Pasibaigus nuskaitymui kompiuterio nuskaitymo žurnalą galite peržiūrėti spustelėdami Rodyti žurnalą.

Nuskaitymo eiga

Nuskaitymo eigos lange rodoma esama nuskaitymo būsena ir informacija apie failų, kuriuose buvo rastas kenkėjiškas kodas, kiekį.

Įprasta, kad kai kurių failų, tokių kaip slaptažodžiu apsaugoti failai arba failai, kuriuos išskirtinai naudoja tik sistema (paprastai *pagefile.sys* ir tam tikri žurnalo failai), negalima nuskaityti. Daugiau informacijos rasite mūsų Žinių bazės straipsnyje.

Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą
Norėdami suplanuoti reguliarią užduotį, skaitykite skyrių Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą.

Nuskaitymo eiga – eigos juostoje rodoma vykdomo nuskaitymo būsena.

Tikslas – šiuo metu nuskaitomo objekto pavadinimas ir jo vieta.

Yra aptikimų – rodo, kiek iš viso nuskaityta failų, rasta grėsmių ir išvalyta grėsmių nuskaitant.

Spustelėkite „Daugiau informacijos“, kad būtų rodoma ši informacija:

- **Naudotojas** – naudotojo, kuris pradėjo nuskaitymą, paskyros pavadinimas.
- **Nuskaityti objektai** – jau nuskaitytų objektų skaičius.
- **Trukmė** – praėjęs laikas.

„Pristabdyti“ piktograma – pristabdo nuskaitymą.

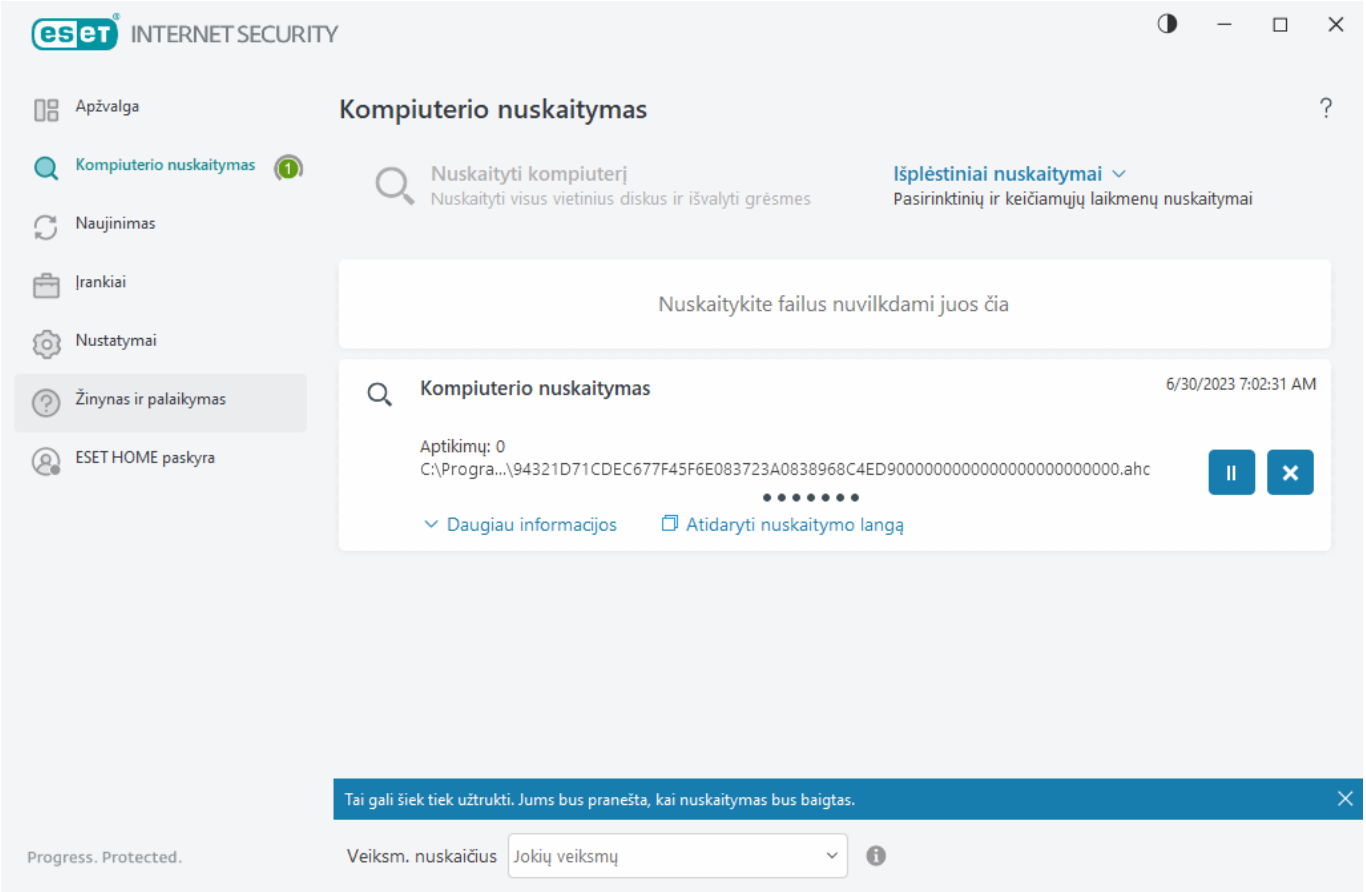
„Tęsti“ piktograma – ši parinktis matoma, kai nuskaitymo eiga buvo pristabdyta. Spustelėkite piktogramą, kad tęstumėte nuskaitymą.

„Sustabdyti“ piktograma – nutraukiamas nuskaitymas.

Spustelėkite **Atidaryti nuskaitymo langą**, kad atidarytumėte kompiuterio nuskaitymo žurnalą su daugiau informacijos apie nuskaitymą.

Slinkti nuskaitymo žurnalą – jeigu įjungta, pridėjus naujų įrašų nuskaitymo žurnalas bus automatiškai slenkamas žemyn, todėl bus matomi naujausi įrašai.

Spustelėkite didinamąjį stiklą arba rodyklę, kad būtų rodoma išsami informacija apie šiuo metu vykdomą nuskaitymą. Spustelėdami **Nuskaityti kompiuterį** arba **Išplėstiniai nuskaitymai** > **Pasirinktinis nuskaitymas** galite vykdyti kitą lygiagretų nuskaitymą.



Veiksmas po nuskaitymo išplečiamajame meniu leidžia nustatyti veiksmą, kuris turi būti atliekamas automatiškai, kai nuskaitymas bus baigtas:

- **Jokių veiksmų** – užbaigus nuskaitymą nebus atliekami jokie veiksmai.
- **Išjungti** – pasibaigus nuskaitymui kompiuteris išjungiamas.
- **Prireikus paleisti iš naujo** – kompiuteris paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.
- **Paleisti iš naujo** – užbaigus nuskaitymą uždaromos visos atidarytos programos, o kompiuteris paleidžiamas iš naujo.
- **Prireikus priversti paleisti iš naujo** – kompiuteris priverstinai paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.
- **Priversti paleisti iš naujo** – priverstinai uždaro visas atidarytas programas nelaukiant naudotojo sąveikos ir iš naujo paleidžia kompiuterį baigus nuskaitymą.
- **Miego režimas** – įrašomas jūsų seansas ir įjungiamas kompiuterio energijos taupymo režimas, kurį išjungę galite greitai tęsti darbą.
- **Sulaikytosios veiksenos režimas** – visus RAM vykdomus procesus perkelia į specialų failą standžiajame diske. Kompiuteris išjungiamas, tačiau kitą kartą įjungę galite tęsti darbą nuo ten, kur baigėte.

Veiksmai **Miego režimas** arba **Sulaikytosios veiksenos režimas** pasiekiami atsižvelgiant į jūsų kompiuterio operacinės sistemos maitinimo ir miego režimo nustatymus arba jūsų stalinio / nešiojamojo kompiuterio galimybes. Atminkite, kad miego režimu veikiantis kompiuteris nėra išjungtas. Jame toliau veikia pagrindinės funkcijos ir vartojama elektros energija, jei kompiuteris veikia naudodamas akumuliatorių. Jei norite pailginti akumuliatoriaus veikimo laiką, pavyzdžiui, išvykę iš biuro, rekomenduojame naudoti sulaikytosios veiksenos režimą.

Pasirinktas veiksmas bus pradėtas užbaigus visus vykdomus nuskaitymus. Pasirinkus **Išjungti** arba **Perkrauti**, patvirtinimo dialogo lange bus rodomas 30 sekundžių atgalinis skaičiavimas (spustelėkite **Atšaukti**, kad išjungtumėte reikalaujamą veiksmą).

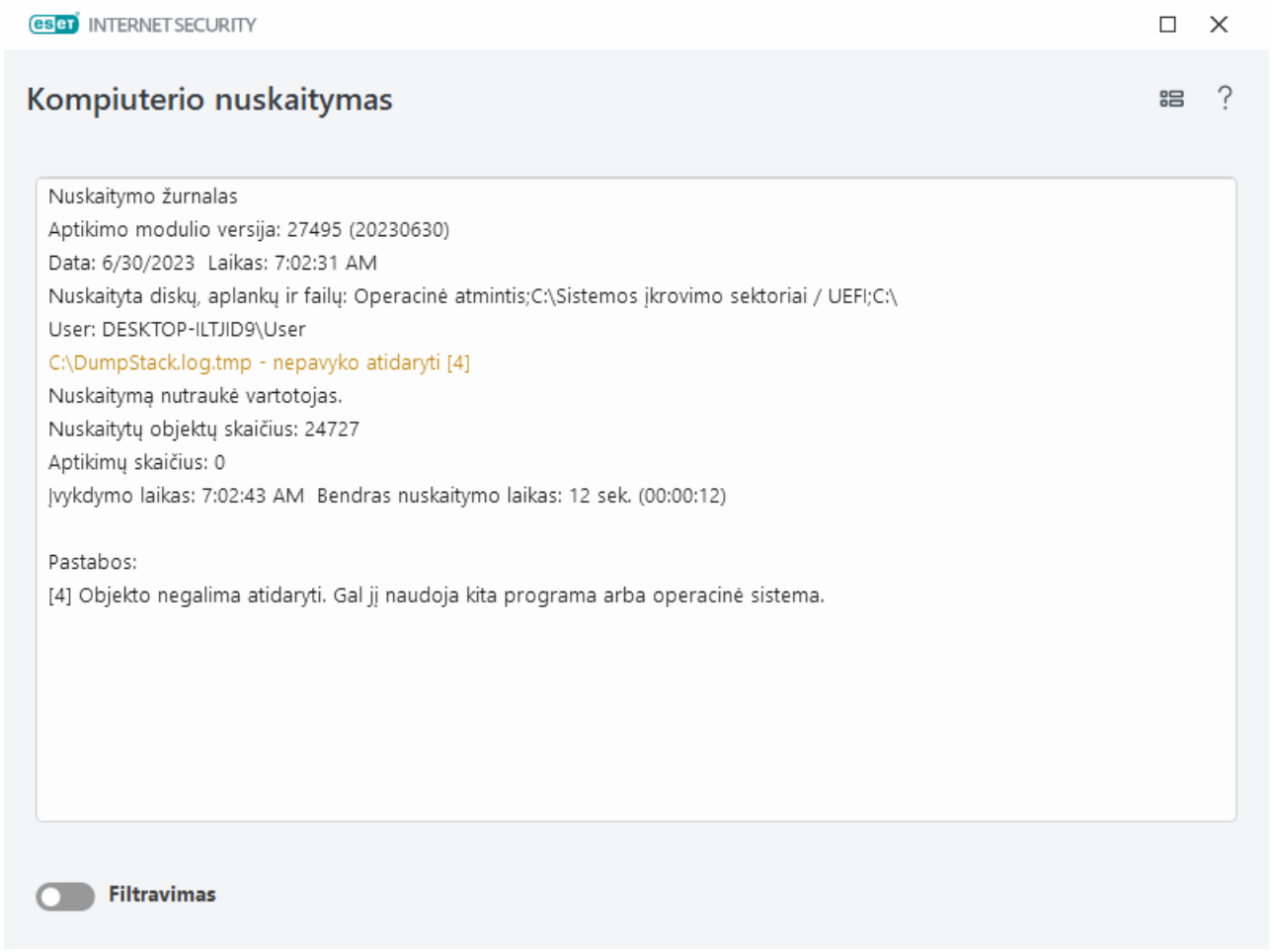
Kompiuterio nuskaitymo žurnalas

Išsamią informaciją, susijusią su konkrečiu nuskaitymu, galite peržiūrėti parinktyje Žurnalo failai. Nuskaitymo žurnale yra ši informacija:

- Aptikimo modulio versija
- Pradžios data ir laikas
- Nuskaitytų diskų, aplankų ir failų sąrašas
- Suplanuoto nuskaitymo pavadinimas (tiksuplanuotas nuskaitymas)
- Naudotojas, kuris pradėjo nuskaitymą.
- Nuskaitymo būsena
- Nuskaitytų objektų skaičius
- Rastų aptikimų skaičius
- Įvykdymo laikas
- Bendras nuskaitymo laikas

Nauja suplanuoto kompiuterio nuskaitymo užduoties pradžia praleidžiama, jei ta pati suplanuota užduotis, kuri buvo atlikta anksčiau, vis dar vykdoma. Praleista suplanuoto nuskaitymo užduotis sukurs kompiuterio nuskaitymo žurnalą su 0 nuskaitytų objektų, o **nuskaitymas nebuvo paleistas, nes ankstesnis nuskaitymas vis dar buvo vykdomas**.

Norėdami rasti ankstesnių nuskaitymų žurnalus, pagrindiniame programos lange pasirinkite **Įrankiai** > **Žurnalo failai**. Išskleidžiamajame meniu pasirinkite **Kompiuterio nuskaitymas** ir du kartus spustelėkite pageidaujamą įrašą.



Norėdami sužinoti daugiau apie įrašus „neįmanoma atidaryti", „atidarant įvyko klaida“ ir (arba) „archyvas sugadintas“, peržiūrėkite mūsų ESET žinių bazės straipsnį.

Spustelėkite perjungiklio piktogramą **Filtravimas**, kad atidarytumėte langą Žurnalo filtravimas, kuriame galite susiaurinti iešką pagal pasirinktinius kriterijus. Norėdami peržiūrėti kontekstinį meniu, dešiniuoju pelės klavišu spustelėkite žurnalo įrašą:

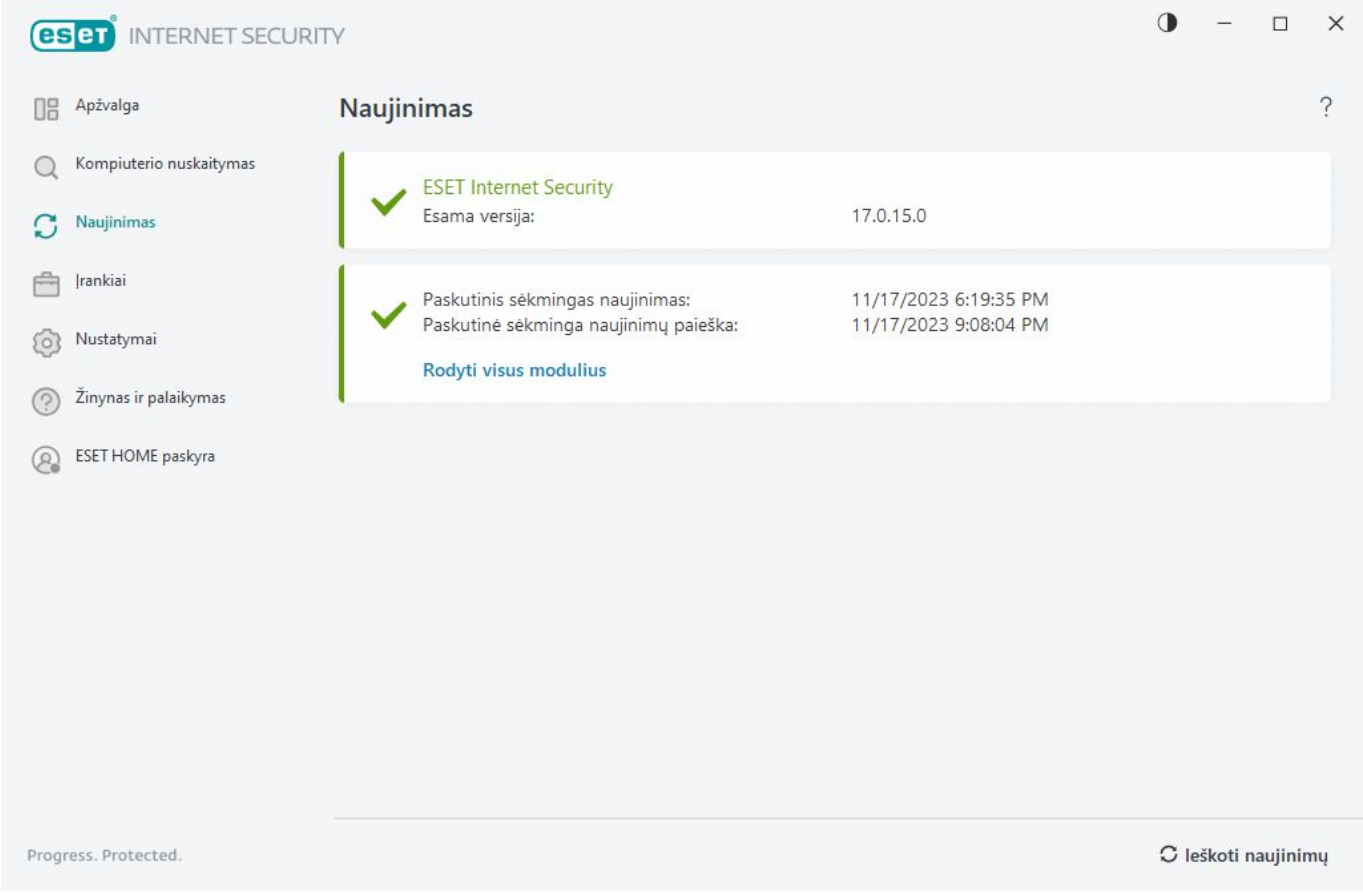
Veiksmas	Naudojimas
Filtruoti tokius pat įrašus	Suaktyvina žurnalo filtravimą. Žurnale bus rodomi tik to paties tipo kaip ir pasirinktas įrašai.
Filtruoti	Pasirinkus šią parinktį, atidaromas žurnalo filtravimo langas ir galite nustatyti konkrečių žurnalo įrašų kriterijus. Nuoroda: `Ctrl+Shift+F`
Įjungti filtrą	Aktyvinami filtro nustatymai. Jei filtrą aktyvinate pirmą kartą, turite nustatyti nustatymus, tada atidaromas žurnalo filtravimo langas.
Išjungti filtrą	Išjungia filtrą (taip pat kaip spustelėjus jungiklį apačioje).
Kopijuoti	Nukopijuoja paryškintą (-us) įrašą (-us) į iškarpinę. Nuoroda: `Ctrl+C`
Kopijuoti viską	Nukopijuoja visus įrašus į langą.
Eksportuoti	Eksportuoja paryškintą (-us) įrašą (-us) į iškarpinę į XML failą.
Eksportuoti viską	Įjungus šią parinktį, visi įrašai eksportuojami į langą į XML failą.
Aptikimo aprašas	Atidaroma ESET grėsmių enciklopedija, kurioje pateikiama išsami informacija apie pažymėto įsiskverbimo pavojus ir požymius.

Naujinti

Reguliariai naujinti ESET Internet Security yra geriausias būdas užtikrinti maksimalų saugos lygį jūsų kompiuteryje. Naujinimo modulis užtikrina, kad programų moduliai ir sistemos komponentai visada būtų atnaujinti.

Spustelėję **Naujinimas** pagrindiniame programos lange, galite rasti esamą naujinimo būseną, įskaitant paskutinio sėkmingo naujinimo datą ir laiką ir ar reikalingas naujinimas.

Be automatinių naujinimų, galite spustelėti **Tikrinti, ar yra naujinimų**, kad suaktyvintumėte neautomatinį naujinimą. Programų modulius ir komponentus reguliariai atnaujinti labai svarbu, kad būtų išlaikyta visapusiška apsauga nuo kenkėjiško kodo. Atkreipkite dėmesį į produkto modulių konfigūraciją ir veikimą. Jei norite gauti atnaujinimus, turite aktyvinti produktą naudodami aktyvinimo raktą. Jei to nepadarėte diegdami, galite suaktyvinti ESET Internet Security, kad galėtumėte pasiekti ESET naujinimo serverius. Aktyvinimo raktas jums išsiųstas el. laišku nuo ESET įsigijus ESET Internet Security.



Dabartinė versija – parodomas dabartinės produkto versijos, kurią esate įdiegę, numeris.

Paskutinis sėkmingas naujinimas – rodoma paskutinio sėkmingo naujinimo data. Jei nematote vėliausios datos, jūsų produkto moduliai gali būti pasenę.

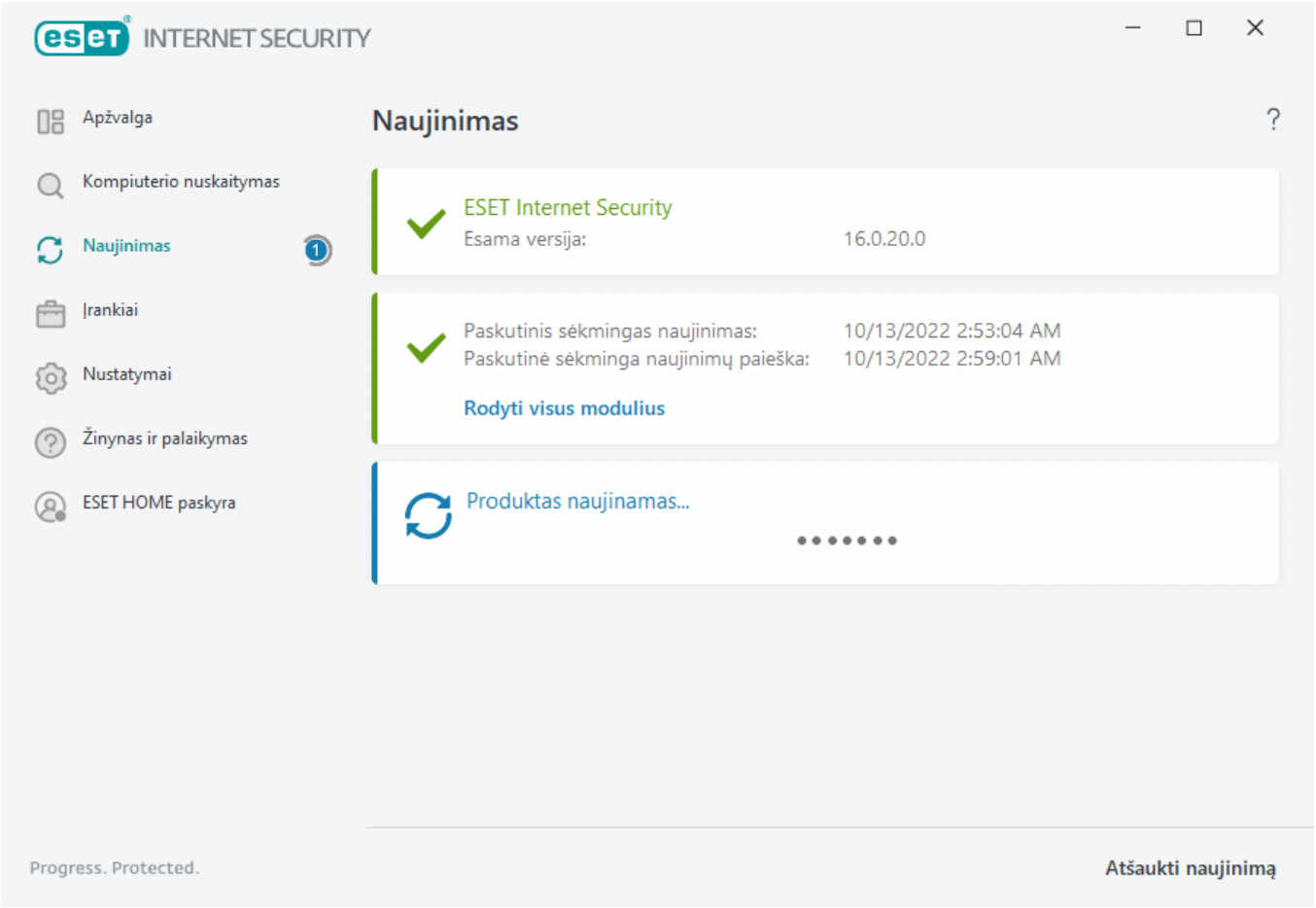
Paskutinis sėkmingas naujinimų tikrinimas – rodoma paskutinės sėkmingos naujinimų paieškos data.

Rodyti visus modulius – rodomas įdiegtų programų modulių sąrašas.

Spustelėkite **Ieškoti naujinimų**, kad aptiktumėte naujausią galimą ESET Internet Security versiją.

Naujinimo procesas

Spustelėję **Ieškoti naujinimų** pradedamas atsisiuntimas. Bus rodoma atsisiuntimo eigos juosta ir likęs atsisiuntimo laikas. Jei norite nutraukti naujinimą, spustelėkite **Atšaukti naujinimą**.



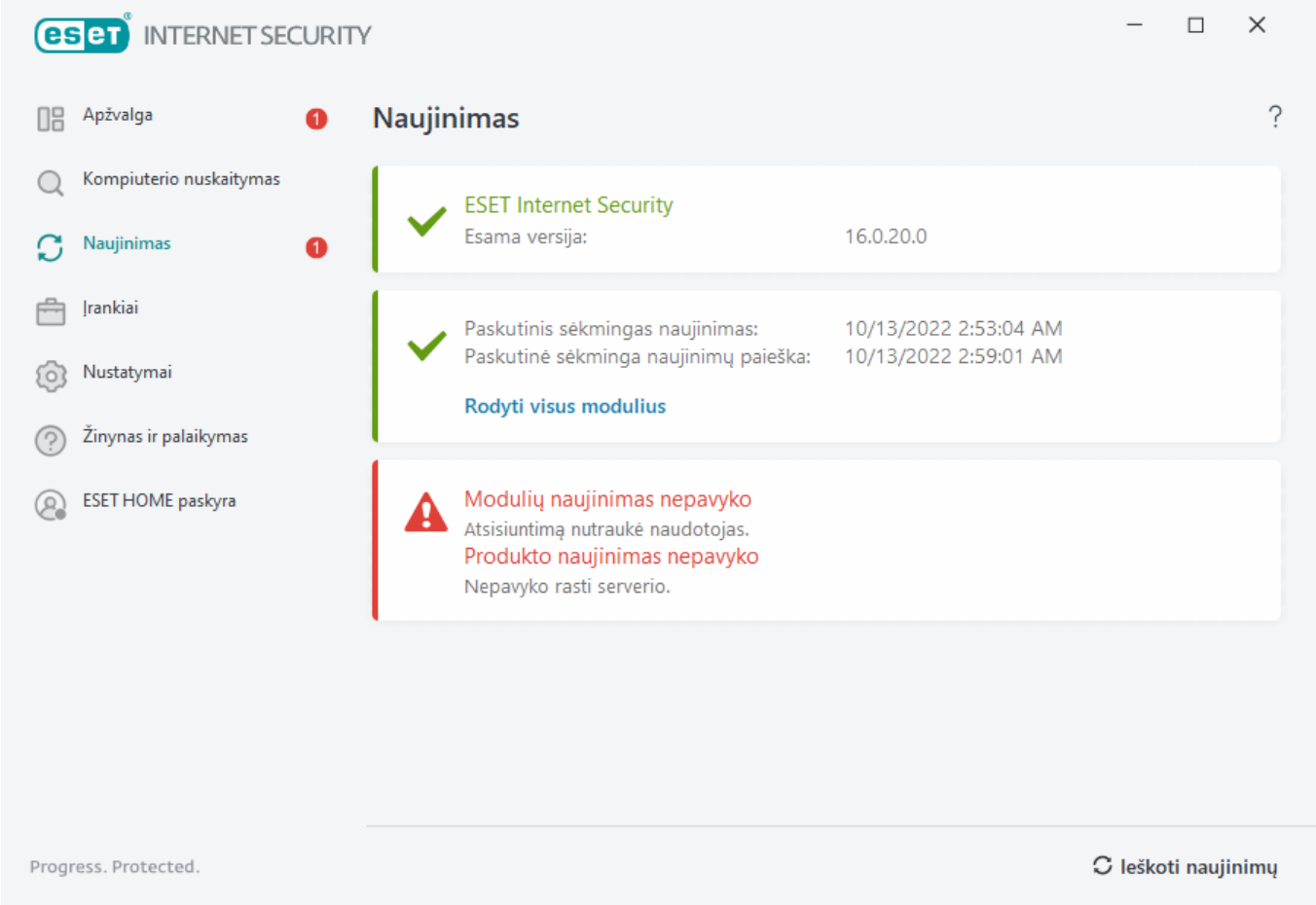
Esant normalioms sąlygoms **Naujinimo** lange rodoma žalia varnelė, kuri nurodo, kad programa yra atnaujinta. Jeigu nematote žalios varnelės, programa yra pasenusi ir labiau pažeidžiama užkrato. Atnaujinkite programos modulius kuo greičiau.

Nesėkmingas naujinimas:

Jei gavote pranešimą apie nepavykusį modulių naujinimą, taip galėjo nutikti dėl šių priežasčių:

1. **Negaliojanti prenumerata** – aktyvinti naudojama prenumerata yra netinkama arba nebegalioja. Pagrindiniame programos lange spustelėkite **Žinynas ir palaikymas** > **Keisti prenumeratą** ir aktyvinkite produktą.

2. **Atsisiunčiant naujinimo failus įvyko klaida** – galima šios klaidos priežastis yra neteisingi interneto ryšio parametrai. Rekomenduojame patikrinti savo interneto ryšį (atidarant bet kokią svetainę savo žiniatinklio naršyklėje). Jeigu svetainė neatsidaro, gali būti, kad nėra interneto ryšio arba yra jūsų kompiuterio prisijungimo problemų. Susisiekite su savo interneto paslaugų teikėju (ISP), jeigu nėra aktyvaus interneto ryšio.



Po sėkmingo ESET Internet Security atnaujinimo į naujesnę produkto versiją rekomenduojame iš naujo paleisti kompiuterį, kad visi programų moduliai būtų tinkamai atnaujinti. Kompiuterio nebūtina paleisti iš naujo po įprastinio modulių atnaujinimo.

Papildomos informacijos rasite šiame Pranešimo „Modulių naujinimas nepavyko“ trikčių šalinimas.

Dialogo langas – būtina paleisti iš naujo

Atnaujinus ESET Internet Security į naują versiją, reikia iš naujo paleisti kompiuterį. Naujos ESET Internet Security versijos išleidžiamos siekiant įgyvendinti patobulinimus arba išspręsti problemas, kurių negalima išspręsti automatiškai atnaujinant programos modulius.

Naują ESET Internet Security versiją galima įdiegti automatiškai, atsižvelgiant į programos naujinimo nustatymus, arba rankiniu būdu , atsisiunčiant ir įdiegiant naujesnę versiją vietoj ankstesnės.

Spustelėkite **Paleisti iš naujo dabar**, kad paleistumėte kompiuterį iš naujo. Jei planuojate vėliau paleisti kompiuterį iš naujo, spustelėkite **Priminti vėliau**. Vėliau galite paleisti kompiuterį iš naujo rankiniu būdu iš pagrindinio programos lango skilties **Apžvalga**.

Kaip sukurti naujinimo užduotis

Naujinimus galima paleisti rankiniu būdu spustelėjus **Ieškoti naujinimų** pradiniame lange, kuris parodomas pagrindiniame meniu spustelėjus **Naujinimas**.

Naujinimus galima vykdyti ir kaip suplanuotas užduotis. Norėdami konfigūruoti suplanuotą užduotį, spustelėkite **Įrankiai** > **Planuoklė**. Pagal numatytuosius nustatymus ESET Internet Security yra suaktyvintos šios naujinimo užduotys:

- **Reguliarus automatinis naujinimas**
- **Automatinis naujinimas prisiregistravus vartotojui**

Kiekvieną naujinimo užduotį galima pakeisti pagal savo poreikius. Šalia numatytųjų naujinimo užduočių galite kurti naujas naujinimo užduotis su vartotojo apibrėžta konfigūracija. Daugiau informacijos apie naujinimo užduočių kūrimą ir konfigūravimą rasite skyriuje Planuoklė.

Įrankiai

Meniu **Įrankiai** yra funkcijų, kurios suteikia papildomos saugos ir padeda supaprastinti „ESET Internet Security“ administravimą. Galimi šie įrankiai:

 Žurnalo failai

 Vykdomi procesai (jei ESET LiveGrid® yra įjungtas produkte ESET Internet Security)

 Saugumo ataskaita

 Tinklo ryšiai (jei Užkarda įjungta ESET Internet Security)

 ESET SysInspector

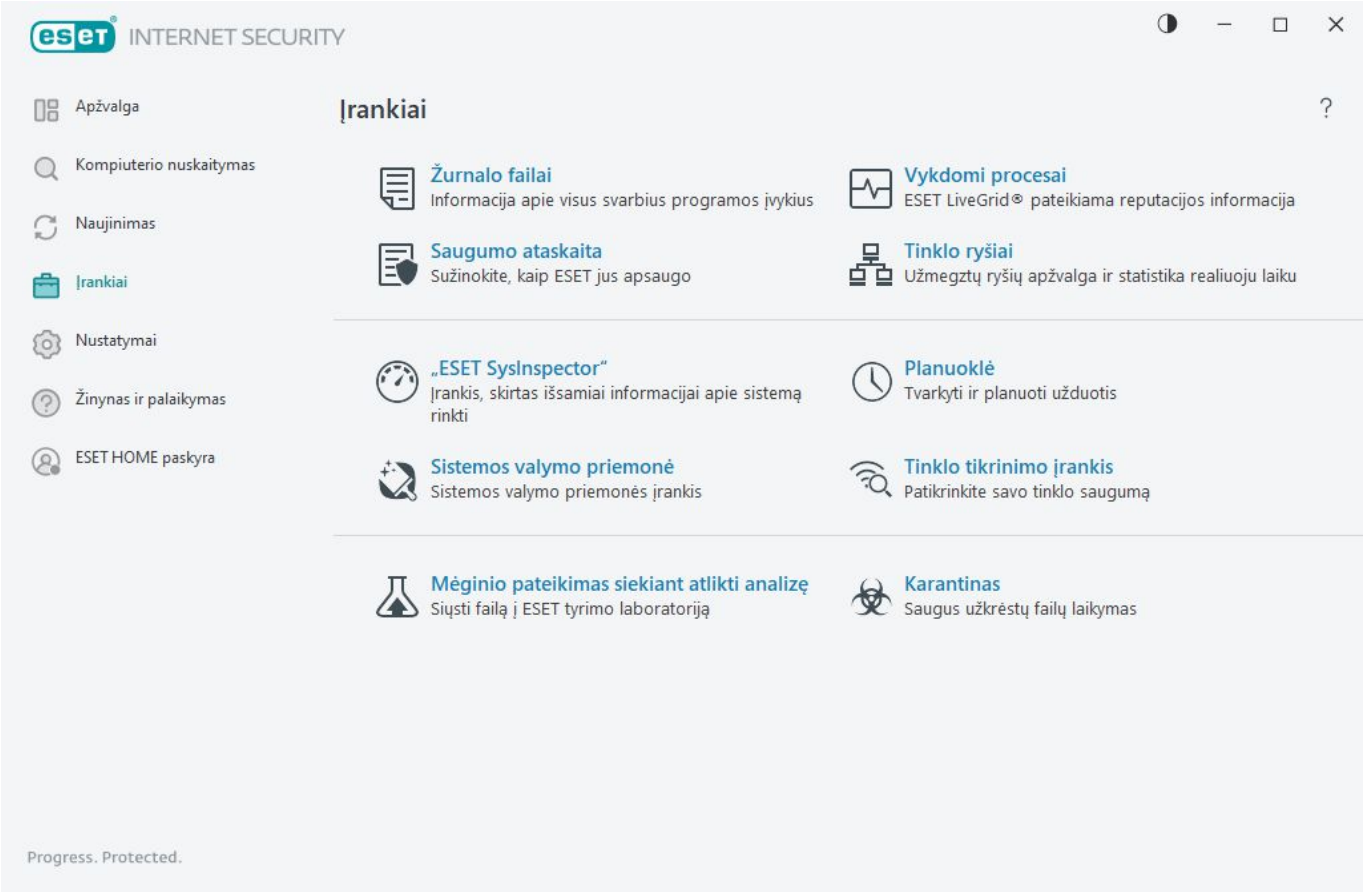
 Planuoklė

 Sistemos valymo priemonė

 Tinklo tikrinimo įrankis

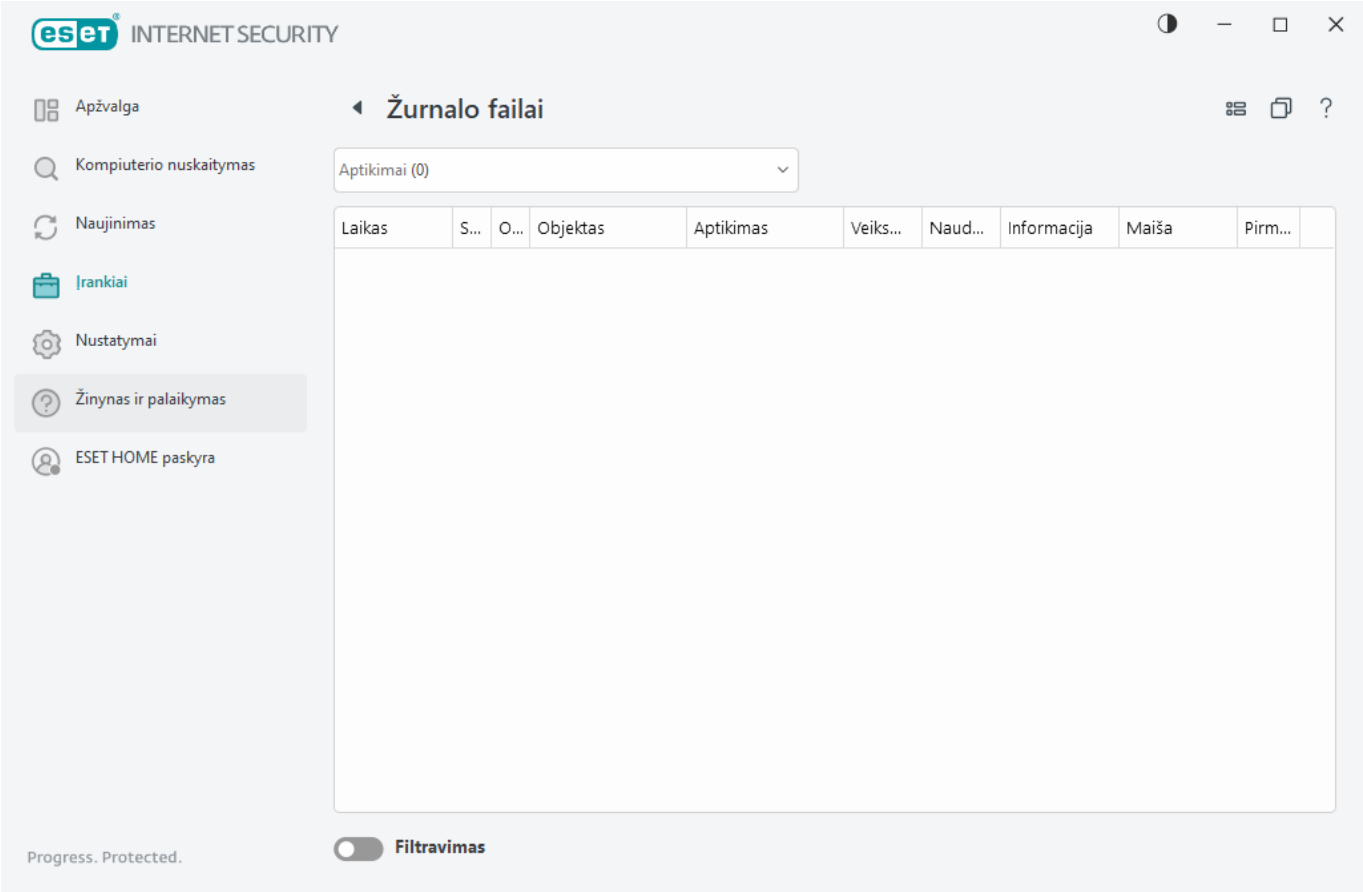
 Pateikti pavyzdį analizei (gali būti nepasiekiama, atsižvelgiant į jūsų ESET LiveGrid® konfigūraciją).

 Karantinas



Žurnalo failai

Žurnalų failuose pateikiama informacija apie svarbius programos įvykius ir aptiktų grėsmių apžvalga. Registravimas yra svarbi sistemos analizės, grėsmių aptikimo ir sutrikimų šalinimo dalis. Registravimas aktyviai atliekamas foniniu režimu, be vartotojo veiksmų. Informacija įrašoma remiantis esamais žurnalas daugiažodiškumo parametrais. Galima peržiūrėti teksto pranešimus ir žurnalo įrašus tiesiai iš ESET Internet Security aplinkos bei archyvuoti žurnalus.



Žurnalo failus galima pasiekti programos lange spustelėjus **Įrankiai** > **Žurnalo failai**. Pasirinkite norimą žurnalo tipą iš išskleidžiamojo meniu Žurnalas.

- **Aptikimai** – šiame žurnale pateikiama išsami informacija apie aptikimus ir įsiskverbimus, kuriuos aptiko ESET Internet Security. Žurnalo informaciją sudaro aptikimo laikas, skaitytuvo tipas, objekto tipas, objekto vieta, aptikimo pavadinimas, atliktas veiksmas, naudotojo, kuris buvo prisijungęs, kai įsiskverbimas buvo aptiktas, vardas, maiša ir pirmasis atvejis. Neišvalyti įsiskverbimai visada pažymimi raudonu tekstu šviesiai raudoname fone. Išvalyti įsiskverbimai pažymimi geltonu tekstu baltame fone. Neišvalytos PUA arba neišvalytos galimos nesaugios taikomosios programos pažymimos geltonu tekstu baltame fone.

- **Įvykiai** – visi svarbūs veiksmai, kuriuos atliko ESET Internet Security, įrašomi įvykių žurnaluose. Įvykių žurnale pateikiama informacija apie įvykius ir klaidas, kurios įvyko programoje. Jis yra skirtas sistemos administratoriams ir vartotojams, kad galėtų spręsti problemas. Dažnai čia esanti informacija gali padėti rasti programoje iškilusios problemos sprendimą.

- **Kompiuterio nuskaitymas** – šiame lange rodomi visi ankstesnių nuskaitymų rezultatai. Kiekviena eilutė atitinka vieną kompiuterio nuskaitymas. Dukart spustelėję bet kurį įrašą, galite peržiūrėti pasirinkto nuskaitymo išsamią informaciją.

- **HIPS** – jį sudaro konkrečių HIPS taisyklių, kurios yra nurodytos registruoti, įrašai. Protokole nurodyta taikomoji programa, kuri paleido operaciją, rezultatas (ar taisyklė buvo leidžiama, ar draudžiama) ir taisyklės pavadinimas.

- **Naršyklės apsauga** – nepatvirtintų / nepatikimų failų, įkeltų į naršyklę, įrašai.

- **Tinklo apsauga** – tinklo apsaugos žurnale rodomos visos užkardos, apsaugos nuo tinklo atakų (IDS) ir apsaugos nuo įtraukimo į užgrobtų kompiuterių tinklą aptiktos nuotolinės atakos. Čia jūs rasite informacijos apie visas atakas, vykdytas prieš jūsų kompiuterį. Stulpelyje Įvykis pateikiamos aptiktos atakos. Skiltyje

Šaltinis pateikiama daugiau informacijos apie įsilaužėlį. Skiltyje Protokolas nurodomas ryšio protokolas, kuris buvo naudojamas atakuojant. Tinklo apsaugos žurnalo analizė gali padėti laiku aptikti įsiskverbimų į sistemą bandymus ir užkirsti kelią neįgaliotai prieigai prie jūsų sistemos. Norėdami gauti daugiau informacijos apie tinklo atakas žr. skyrių IDS ir išplėstinės parinktys.

- **Filtruojamos svetainės** – Šis sąrašas naudingas, jei norite peržiūrėti svetainių, kurias užblokavo Prieigos prie saityno apsauga arba Tėvų kontrolė, sąrašą. Kiekviename iš šių žurnalų nurodytas laikas, URL adresas, vartotojas ir programa, kuri užmezgė ryšį su konkrečia svetaine.

- **El. pašto programos apsauga nuo brukalo** – ją sudaro įrašai, susiję su el. laiškais, kurie buvo pažymėti kaip brukalas.

- **Tėvų kontrolė** – rodo tinklalapius, kuriuos blokuoja arba leidžia tėvų kontrolė. Skiltys Atitikimo tipas ir Atitikimo reikšmės nurodys, kaip buvo taikomos filtravimo taisyklės.

- **Įrenginio kontrolė** – turi įrašus apie nešiojamąsias laikmenas arba įrenginius, kurie buvo prijungti prie kompiuterio. Į žurnalo failą bus įrašyti tik įrenginiai, kuriems taikomos atitinkamos įrenginio kontrolės taisyklės. Jeigu taisyklė neatitinka prijungto įrenginio, žurnalo įrašas apie prijungtą įrenginį nebus sukurtas. Be to, galite peržiūrėti tokią išsamią informaciją kaip įrenginio tipas, serijos numeris, tiekėjo pavadinimas ir laikmenos dydis (jei yra).

- **Interneto kameros apsauga** – pateikiami įrašai apie interneto kameros apsaugos funkcijos užblokuotos programos.

Pasirinkite žurnalo turinį ir paspauskite **CTRL + C** , kad nukopijuotumėte jį į iškarpinę. Laikydami **CTRL** arba **SHIFT** pasirinkite kelis elementus.

Spustelėkite **Filtravimas**, kad būtų atidarytas langas Žurnalo filtravimas, kuriame galima apibrėžti filtravimo kriterijus.

Dešiniuoju pelės mygtuku spustelėkite įrašą, kad būtų atidarytas kontekstinis meniu. Galimos šios parinktys kontekstiniame meniu:

- **Rodyti** – naujame lange pateikia išsamesnės informacijos apie pasirinktą žurnalą.

- **Filtruoti tuos pačius įrašus** – suaktyvinę šį filtrą, matysite tik to paties tipo įrašus (diagnostika, įspėjimai, ...).

- **Filtruoti** – spustelėję šią parinktį, lange Žurnalo filtravimas galėsite apibrėžti konkrečių žurnalo įrašų filtravimo kriterijus.

- **Įjungti filtrą** – suaktyvina filtro parametrus.

- **Išjungti filtrą** – panaikina visus filtro nustatymus (kaip aprašyta anksčiau).

- **Kopijuoti / Kopijuoti viską** – kopijuoja informaciją apie pasirinktus įrašus lange.

- **Kopijuoti langelį** – nukopijuoja dešiniuoju pelės mygtuku spustelėto langelio turinį.

- **Šalinti / Šalinti viską** – šalina pasirinktus įrašus arba visus rodomus įrašus. Šiam veiksmui reikalingos administratoriaus teisės.

- **Eksportuoti / Eksportuoti viską** – eksportuoja informaciją apie pasirinktus įrašus arba visus įrašus XML

formatu.

• **Rasti / Rasti kitą / Rasti ankstesnį** – spustelėję šią parinktį, lange „Žurnalo filtravimas“ galėsite apibrėžti filtravimo kriterijus, kad būtų pažymėtas konkretus įrašas.

• **Aptikimo aprašymas** – atidaroma ESET grėsmių enciklopedija, kurioje pateikiama išsami informacija apie užregistruoto įsiskverbimo pavojus ir požymius.

• **Kurti išimtį** – sukurti naują aptikimo išimtį, naudojant vedlį (negalima kenkėjiškos programinės įrangos aptikimui).

• **Įtraukti į naršyklės apsaugos leidimų sąrašą** – atidaromas naršyklės apsaugos leidimų sąrašo langas ir elementas įtraukiamas į sąrašą.

Žurnalo filtravimas

Spustelėkite **Filtravimas** dalyje **Įrankiai** > **Žurnalo failai** filtravimo kriterijams apibrėžti.

Žurnalo filtravimo funkcija padės rasti ieškomos informacijos, ypač, kai turite daugybę įrašų. Ji padeda susiaurinti žurnalo įrašų paiešką, pvz., jei ieškote konkretaus tipo įvykio, būsenos arba laikotarpio. Galite filtruoti žurnalo įrašus nurodydami konkrečias paieškos parinktis, kad lange žurnalo failai būtų rodomi tik aktualūs įrašai (atsižvelgiant į paieškos parinktis).

Įveskite ieškomą raktažodį į laukelį **Rasti tekstą**. Paieškai susiaurinti naudokite išskleidžiamąjį meniu **Ieškoti stulpeliuose**. Pasirinkite bent vieną įrašą išskleidžiamajame meniu **Įrašų žurnalų tipai**. Nurodykite **Laikotarpį** kurio rezultatus norite matyti. Taip pat galite naudoti kitas paieškos parinktis, pvz., **Ieškoti tik viso žodžio** arba **Skirti didžiąsias ir mažąsias raides**.

Rasti tekstą

Įveskite eilutę (žodį arba žodžio dalį). Bus rodomi tik įrašai, kuriuose yra ši eilutė. Kiti įrašai nebus rodomi.

Ieškoti stulpeliuose

Pasirinkite, kuriuos stulpelius įtraukti į paiešką. Galite pažymėti vieną ar daugiau stulpelių, kad jie būtų naudojami paieškoje.

Įrašų tipai

Pasirinkite vieną arba daugiau žurnalų įrašų tipų iš išskleidžiamojo meniu:

• **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.

• **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.

• **Įspėjimai** – įrašo kritines klaidas ir įspėjimo pranešimus.

• **Klaidos** – įrašomos klaidos, pvz., „Klaida atsiunčiant failą“, ir kritinės klaidos.

- **Kritinės** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų

Laikotarpis

apibrėžkite laikotarpį, kurio rezultatus norite peržiūrėti:

- **Nenurodytas** (numatytasis) – neieškoma konkretaus laikotarpio, ieškoma visame žurnale.
- **Paskutinė diena**
- **Paskutinė savaitė**
- **Paskutinis mėnuo**
- **Laikotarpis** – galite nurodyti konkretų laikotarpį (Nuo: ir Iki:), kad filtruotumėte tik konkretaus laikotarpio įrašus.

Ieškoti tik viso žodžio

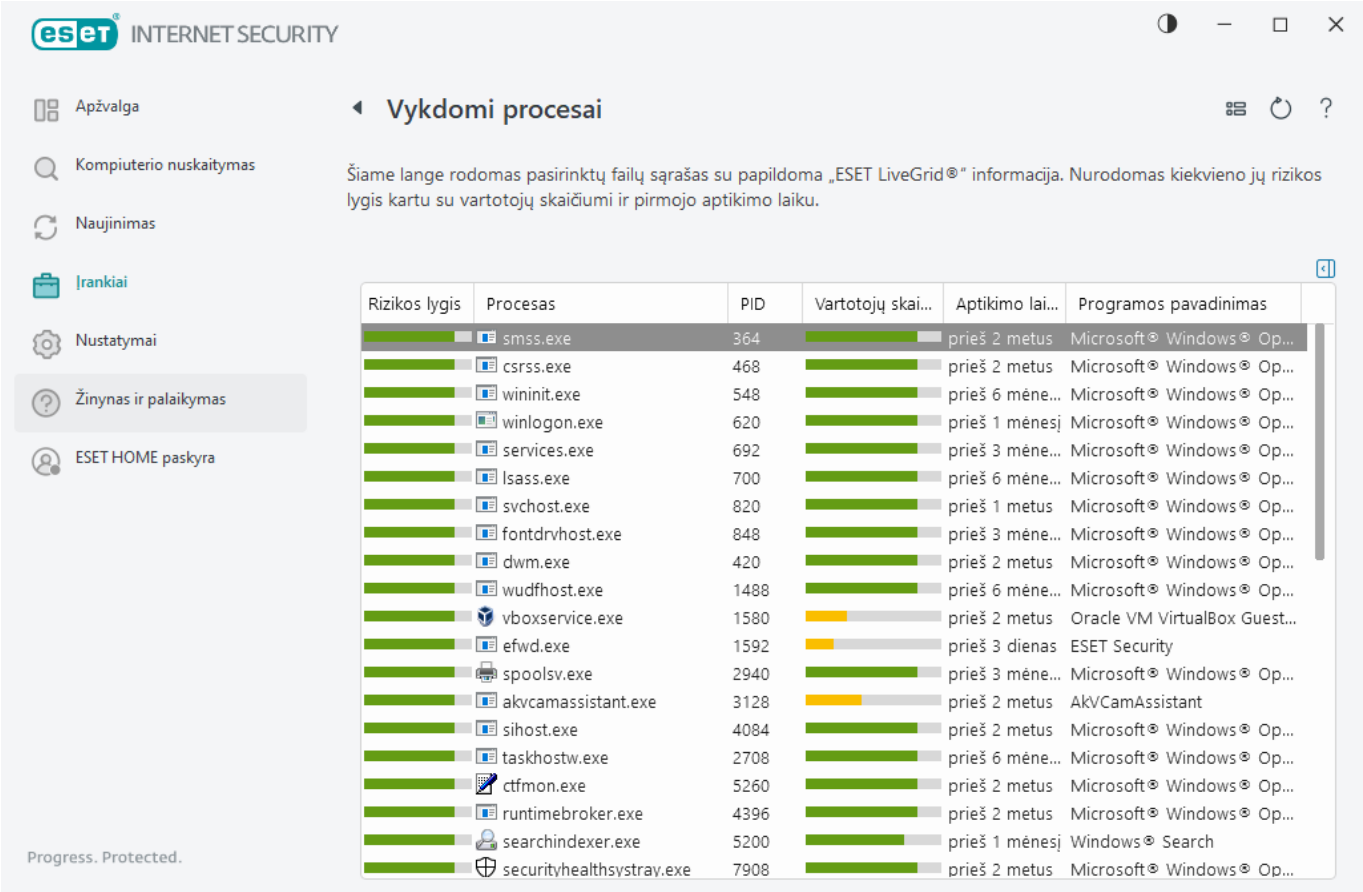
Jei norite ieškoti viso žodžio, pasirinkite šį žymės langelį, kad būtų parodyti tikslesni rezultatai.

Skirti didžiąsias ir mažąsias raides

Įjunkite šią parinktį, jei jums svarbu skirti didžiąsias ir mažąsias raides filtruojant. Kai sukonfigūruosite savo filtravimo / paieškos parinktis, spustelėkite **Gerai**, kad būtų rodomi filtruojami žurnalo įrašai arba **Rasti**, kad pradėtumėte paiešką. Žurnalo failų ieškoma nuo viršaus į apačią, pradedant nuo dabartinės vietos (paryškinto įrašo). Paieška sustoja, kai randamas pirmasis atitinkamas įrašas. Paspauskite **F3**, kad ieškotumėte kito įrašo arba spustelėkite dešiniuoju pelės mygtuku ir pasirinkite **Rasti**, kad patikslintumėte paieškos parinktis.

Vykdomi procesai

Vykdomi procesai rodo vykdomas programas arba procesus jūsų kompiuteryje ir iškart bei nuolatos informuoja ESET apie naujus įsiskverbimus. ESET Internet Security suteikia išsamią informaciją apie vykdomus procesus, kad vartotojai būtų apsaugoti naudodami ESET LiveGrid® technologiją.



Reputacija – daugeliu atvejų ESET Internet Security ir ESET LiveGrid® technologija priskiria rizikos lygius objektams (failams, procesams, registrų raktams ir t. t.) naudodama euristikos taisyklių sekas, kurios tikrina kiekvieno objekto charakteristikas, ir įvertina jų kenkėjiškos veiklos galimybę. Remiantis šiomis euristikomis, objektai priskiriami rizikos lygiams nuo 1 – gero (žalia spalva) iki 9 – rizikingo (raudona spalva).

Procesas – šiuo metu jūsų kompiuteryje vykdomos programos arba proceso atvaizdo pavadinimas. Norėdami matyti visus savo kompiuteryje vykdomus procesus galite naudoti ir „Windows" užduočių tvarkytuvą. Jei norite atidaryti užduočių tvarkytuvą, dešiniuoju pelės mygtuku spustelėkite tuščią sritį užduočių juostoje, tada spustelėkite **Užduočių tvarkytuvas** arba klaviatūroje paspauskite **Ctrl**+**Shift**+**Esc**.

Žinomos programos, pažymėtos kaip Geros (žaliai), tikrai yra švarios (įtrauktos į baltąjį sąrašą) ir jos nebus įtrauktos į nuskaitymą veikimui pagerinti.

PID – proceso identifikacinis numeris gali būti naudojamas kaip parametras įvairioms funkcijoms iškviesti, pvz., procesų pirmenybei koreguoti.

Vartotojų skaičius – vartotojų, naudojančių duotą taikomąją programą, skaičius. Šią informaciją renka ESET LiveGrid® technologija.

Atskleidimo laikas – laikotarpis, praėjęs nuo tada, kai taikomąją programą aptiko ESET LiveGrid® technologija.

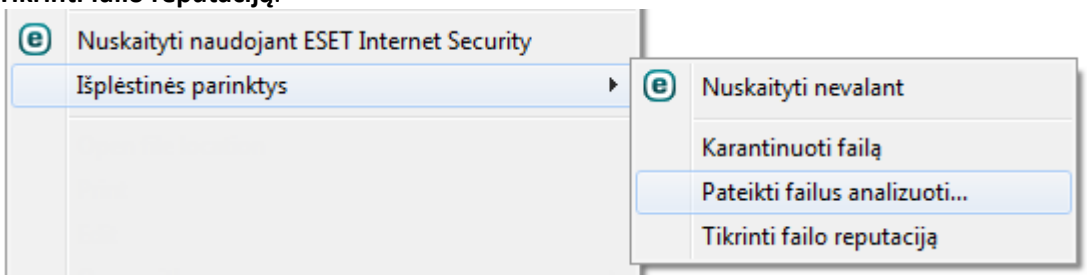
Programa, pažymėta kaip Nežinoma (oranžine spalva), nebūtinai yra kenkėjiška programinė įranga. Paprastai tai naujesnė taikomoji programa. Jei nesate tikri dėl failo, galite pateikti failą analizei į ESET tyrimų laboratoriją. Jei failas pasirodys esantis kenkėjiška programa, jo aptikimas bus įtrauktas į būsimą naujinimą.

Programos pavadinimas – duotas programos arba proceso pavadinimas.

Spustelėkite programą, kad būtų parodyti tokie programos duomenys:

- **Kelias** – programos vieta jūsų kompiuteryje.
- **Dydis** – failo dydis kB (kilobaitais) arba MB (megabaitais).
- **Aprašymas** – failo charakteristikos pagal aprašą operacinėje sistemoje.
- **Įmonės** – tiekėjo arba programos proceso pavadinimas.
- **Versija** – programos leidėjo informacija.
- **Produktas** – programos pavadinimas ir (arba) įmonės pavadinimas.
- **Sukūrimo / modifikavimo data** – sukūrimo (modifikavimo) data ir laikas.

Be to, galite patikrinti failų, kurie neveikia kaip veikiančios programos / procesai, reputaciją. Tai galite padaryti spustelėdami juos dešiniuoju pelės mygtuku failų naršyklėje ir pasirinkdami **Išplėstinės parinktys** > **Tikrinti failo reputaciją**.



Saugumo ataskaita

Ši funkcija leidžia peržiūrėti šių kategorijų statistiką:

- **Užblokuoti tinklalapiai** – rodo užblokuotų tinklalapių skaičių (į juodąjį sąrašą įtrauktus PUA, sukčiavimo apsimetant, maršrutizatoriaus, į kurį įsibrauta, URL, IP arba sertifikatą).
- **Aptikta užkrėstų el. pašto objektų** – rodo užkrėstų el. pašto objektų, kurie buvo aptikti, skaičių.
- **Tinklalapiai naudojant paslaugą „Tėvų kontrolė“ užblokuoti** – rodo užblokuotų tinklalapių, naudojant paslaugą „Tėvų kontrolė“, skaičių.
- **Aptikta PUA** – rodo galimai nepageidaujamų programų (PUA) skaičių.
- **Aptikta el. pašto brukalo** – rodo aptiktų el. pašto brukalų skaičių.
- **Užblokuota prieiga prie internetinės vaizdo kameros** – rodo užblokuotų jungimosi prie internetinės vaizdo kameros skaičių.
- **Nuskaityti dokumentai** – rodomas nuskaitytų dokumentų objektų skaičius.
- **Patikrinta programų** – rodo nuskaitytų vykdomųjų objektų skaičių.
- **Patikrinta kitų objektų** – rodo kitų nuskaitytų objektų skaičių.

- **Patikrinta tinklalapių objektų** – rodo nuskaitytų tinklalapių objektų skaičių.
- **Nuskaityta el. pašto objektų** – rodo nuskaitytų el. pašto objektų skaičių.

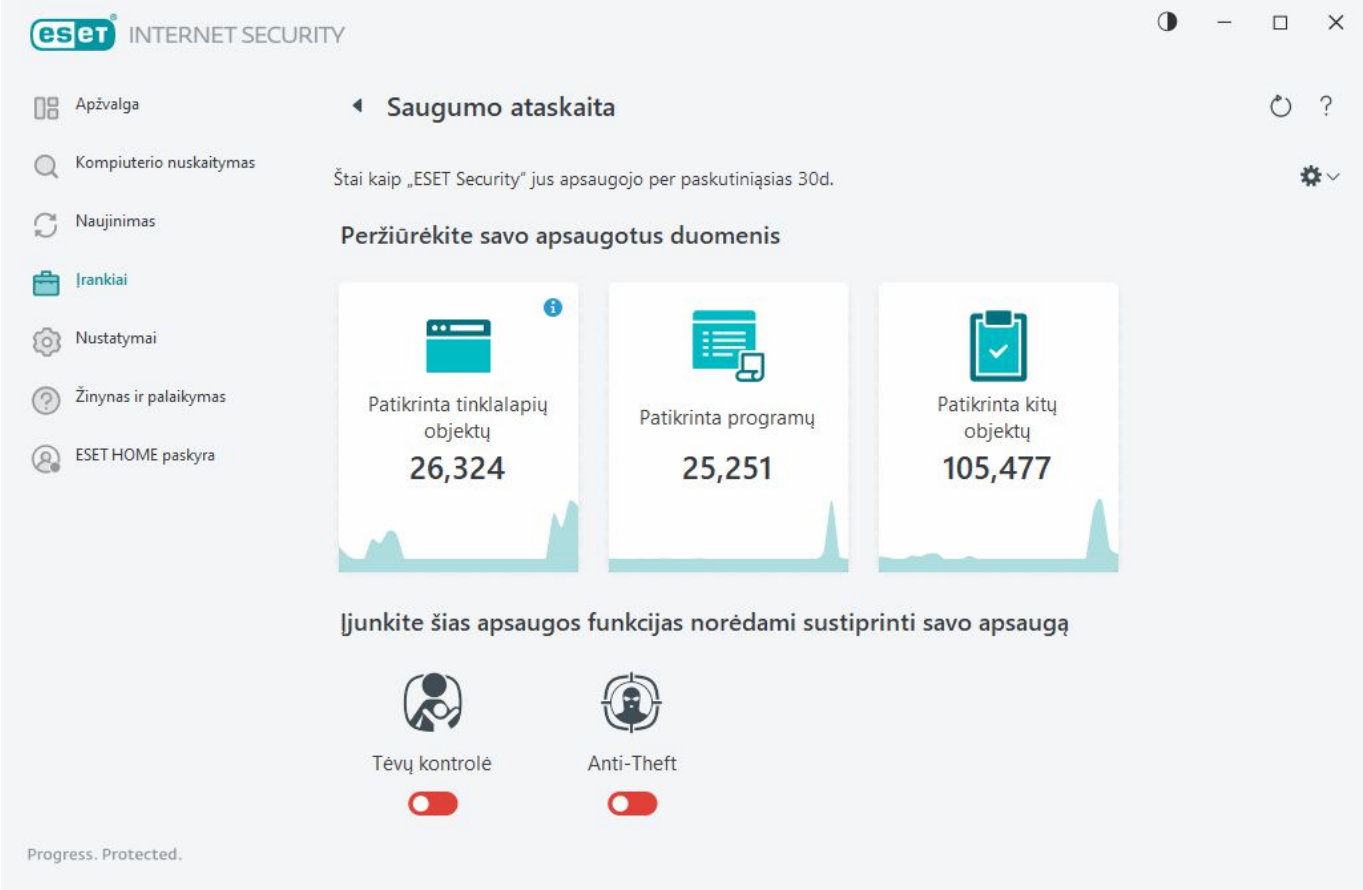
Šių kategorijų tvarka yra pagrįsta skaitine verte nuo didžiausios iki mažiausios. Kategorijos su nuline verte nėra rodomos. Paspauskite „**Rodyti daugiau**“, kad būtų išplėstos ir rodomos paslėptos kategorijos.

Paskutinėje saugumo ataskaitos dalyje siūloma galimybė aktyvinti šias funkcijas:

- Tėvų kontrolė
- Anti-Theft

Kai funkcija įjungta, saugumo ataskaitoje ji neberodoma kaip neveikianti.

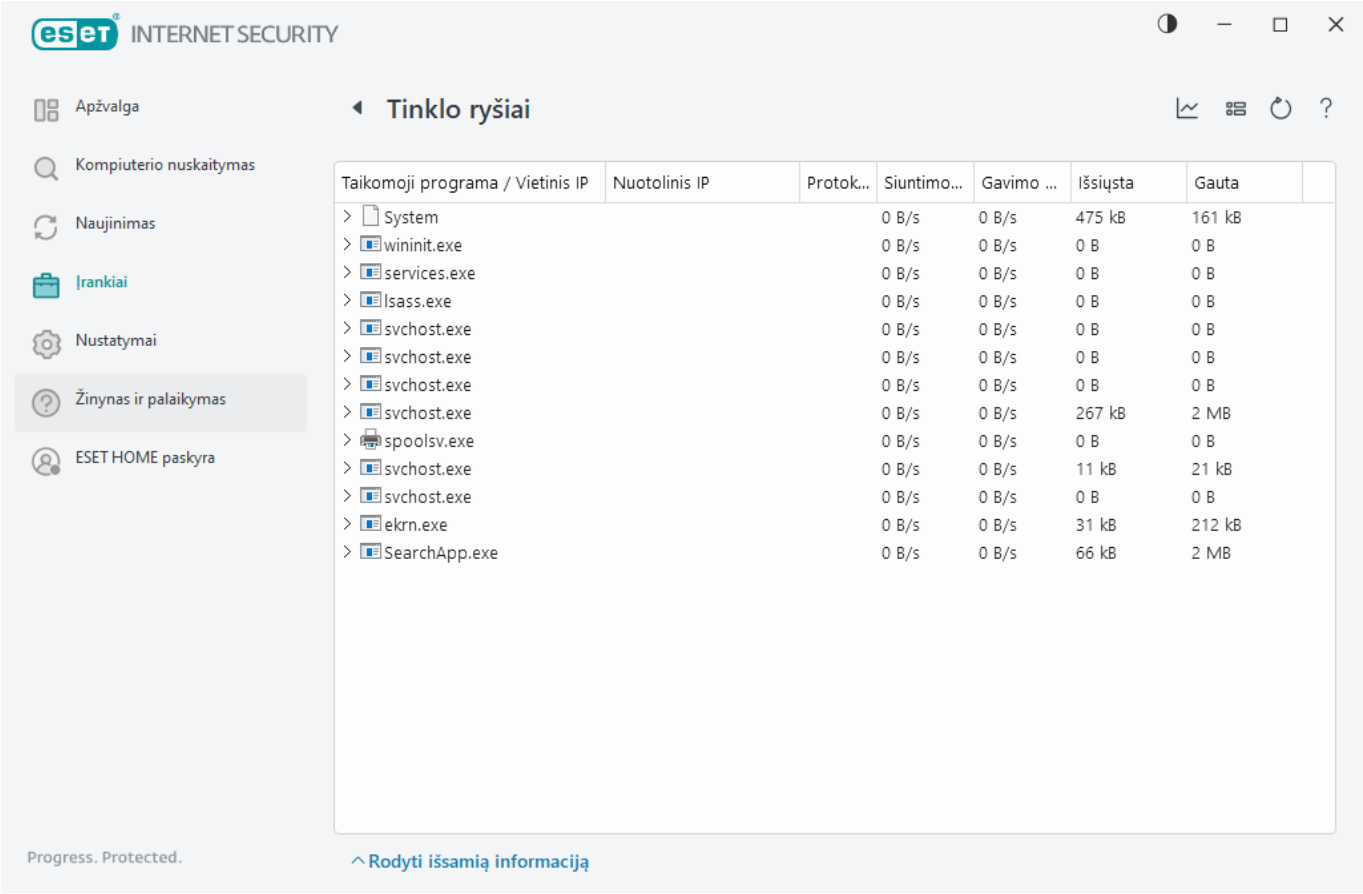
Paspauskite krumpliaračio piktogramą viršutiniame dešiniajame kampe ir galėsite **Įjungti / išjungti saugumo ataskaitos pranešimus** arba pasirinkti, ar rodyti paskutinių 30 dienų duomenis ar nuo to laiko, kai produktas buvo suaktyvintas. Jei ESET Internet Security buvo įdiegtas mažiau nei prieš 30 dienų, galima pasirinkti tik tą dienų skaičių, kuris praėjo nuo įdiegimo. 30 dienų laikotarpis nustatytas kaip numatytasis nustatymas.



Įjungus funkciją **Iš naujo nustatyti duomenis**, bus išvalyta visa statistika ir iš saugumo ataskaitos pašalinti visi joje esantys duomenys. Šį veiksmą reikia patvirtinti, išskyrus, jei atsisakysite parinkties **Klausti prieš atkuriant statistiką** (Išplėstinis nustatymas > **Pranešimai** > **Interaktyvūs įspėjimai** > **Patvirtinimo pranešimai** > **Redaguoti**).

Tinklo ryšiai

Tinklo ryšių skyriuje galite matyti aktyvių ir laukiamų ryšių sąrašą. Tai padeda kontroliuoti visų programų palaikomus siunčiamus ryšius.



Spustelėkite diagramos piktogramą , kad atidarytumėte Tinklo veikla.

Pirmoje eilutėje rodomas programos pavadinimas ir jos duomenų perdavimo greitis. Norėdami matyti programos užmegztų ryšių sąrašą (ir išsamesnę informaciją), spustelėkite **>**.

Stulpeliai

Programa / vietinis IP – programos pavadinimas, vietiniai IP adresai ir ryšio prievadai.

Nuotolinis IP – konkretaus nuotolinio kompiuterio IP adresas ir prievado numeris.

Protokolas – naudojamas siuntimo protokolas.

Siuntimo greitis / gavimo greitis – esamas siunčiamų ir gaunamų duomenų greitis.

Išsiųsta / gauta – duomenų kiekis, apsikeistas ryšio metu.

Rodyti išsamią informaciją – nurodykite šią parinktį, kad būtų pateikta išsamios informacijos apie pasirinktą ryšį.

Spustelėkite dešiniuoju pelės klavišu ryšį, norėdami matyti papildomas parinktis:

Pasirinkti pagrindinio kompiuterio pavadinimus – jeigu įmanoma, visi tinklo adresai rodomi DNS formatu, o ne

skaitiniu IP adreso formatu.

Rodyti tik TCP ryšius – sąraše rodomi tik tie ryšiai, kurie priklauso TCP protokolo programų paketui.

Rodyti klausomus ryšius – nurodžius šią parinktį, pateikiami tik tie ryšiai, kuriems ryšys šiuo metu nėra užmegztas, tačiau sistema yra atidariusi prievadą ir laukia ryšio.

Rodyti ryšius kompiuteryje – nurodykite šią parinktį, kad būtų rodomi tik tie ryšiai, kurių nuotolinė pusė yra vietinė sistema – vadinamieji localhost kompiuterio ryšiai.

Atnaujinti greitį – pasirinkite, kokiu dažnumu atnaujinti aktyvius ryšius.

Atnaujinti dabar – iš naujo įkelia **Tinklo ryšių** langą.

Šios parinktys pasiekiamos tik spustelėjus programą arba procesą, o ne aktyvią jungtį:

Laikinai uždrausti proceso ryšį – atmeta esamus duotosios programos ryšius. Jeigu užmezgamas naujas ryšys, užkarda naudoja iš anksto nustatytą taisyklę. Nustatymų aprašą rasite skyriuje Užkardos taisyklės.

Laikinai leisti proceso ryšį – leidžia esamus duotosios programos ryšius. Jeigu užmezgamas naujas ryšys, užkarda naudoja iš anksto nustatytą taisyklę. Nustatymų aprašą rasite skyriuje Užkardos taisyklės.

Tinklo veikla

Norėdami peržiūrėti dabartinę **Tinklo veiklą** diagramos forma, spustelėkite **Įrankiai** > **Tinklo ryšiai** ir spustelėkite diagramos piktogramą . Diagramos apačioje yra laiko planavimo juosta, kuri registruoja tinklo veiklą realiuoju laiku pagal pasirinktą laiko tarpą. Norėdami pakeisti laiko tarpą, išplečiamajame meniu **Atnaujinimo dažnis** pasirinkite taikomą reikšmę.

Galimos šios parinktys:

- **1 sekundė** – diagrama bus atnaujinama kas sekundę, o laiko linija apims paskutines 4 minučių.
- **1 minutė (paskutinės 24 valandos)** – diagrama bus atnaujinama kas minutę ir laiko linija apims paskutines 24 valandas.
- **1 valanda (paskutinis mėnuo)** – diagrama bus atnaujinama kas valandą ir laiko intervalas apims paskutinį mėnesį.

Vertikalioji diagramos ašis rodo gautų arba išsiųstų duomenų kiekį. Užveskite pelės žymiklį ant diagramos, kad matytumėte tikslų gautų / išsiųstų duomenų kiekį tam tikru laiku.

ESET SysInspector

ESET SysInspector yra programa, kuri nuodugniai tikrina jūsų kompiuterį, surenka išsamią informaciją apie sistemos komponentus (tvarkykles ir programas, tinklo ryšius ar svarbius registrų įrašus) ir įvertina kiekvieno komponento rizikos lygį. Ši informacija gali padėti nustatyti įtartino sistemos veikimo priežastis dėl programinės įrangos ar aparatūros nesuderinamumo arba užsikrėtus kenkėjiška programa. Norėdami sužinoti, kaip naudoti ESET SysInspector, žr. ESET SysInspector Internetinis žinynas.

ESET SysInspector lange rodoma ši informacija apie žurnalus:

- **Laikas** – žurnalo sukūrimo laikas.
- **Komentaras** – trumpas komentaras.
- **Vartotojas** – vartotojo, sukūrusio žurnalą, vardas.
- **Būsena** – žurnalo kūrimo būsena.

Galimi šie veiksmai:

- **Rodyti** – atidaro pasirinktą prisijungimą ESET SysInspector. Be to, galite dešiniuoju pelės klavišu spustelėti reikiamą žurnalo failą ir kontekstiniame meniu pasirinkti **Rodyti**.
- **Kurti** – sukuriamas naujas žurnalas. Palaukite, kol ESET SysInspector bus sugeneruotas (būsena **Sukurta**), prieš bandydami pasiekti žurnalą. Žurnalas įrašomas į C:\ProgramData\ESET\ESET Security\SysInspector.
- **Naikinti** – iš sąrašo pašalinamas pasirinktas žurnalas (-ai).

Kai pasirenkamas vienas ar keli žurnalo failai, kontekstiniame meniu pateikiami tokie elementai:

- **Rodyti** – atidaro pasirinktą žurnalą ESET SysInspector lange (ta pati funkcija, kaip dukart spustelėjus žurnalą).
- **Kurti** – sukuriamas naujas žurnalas. Palaukite, kol ESET SysInspector bus sugeneruotas (būsena **Sukurta**), prieš bandydami pasiekti žurnalą.
- **Naikinti** – iš sąrašo pašalinamas pasirinktas žurnalas (-ai).
- **Naikinti viską** – panaikina visus žurnalus.

- **Eksportuoti** – eksportuoja žurnalą į .xml failą arba zip formatu suglaudintą .xml.

Planuoklė

Planuoklė tvarko ir paleidžia planuotas užduotis su iš anksto nustatyta konfigūracija ir ypatybėmis.

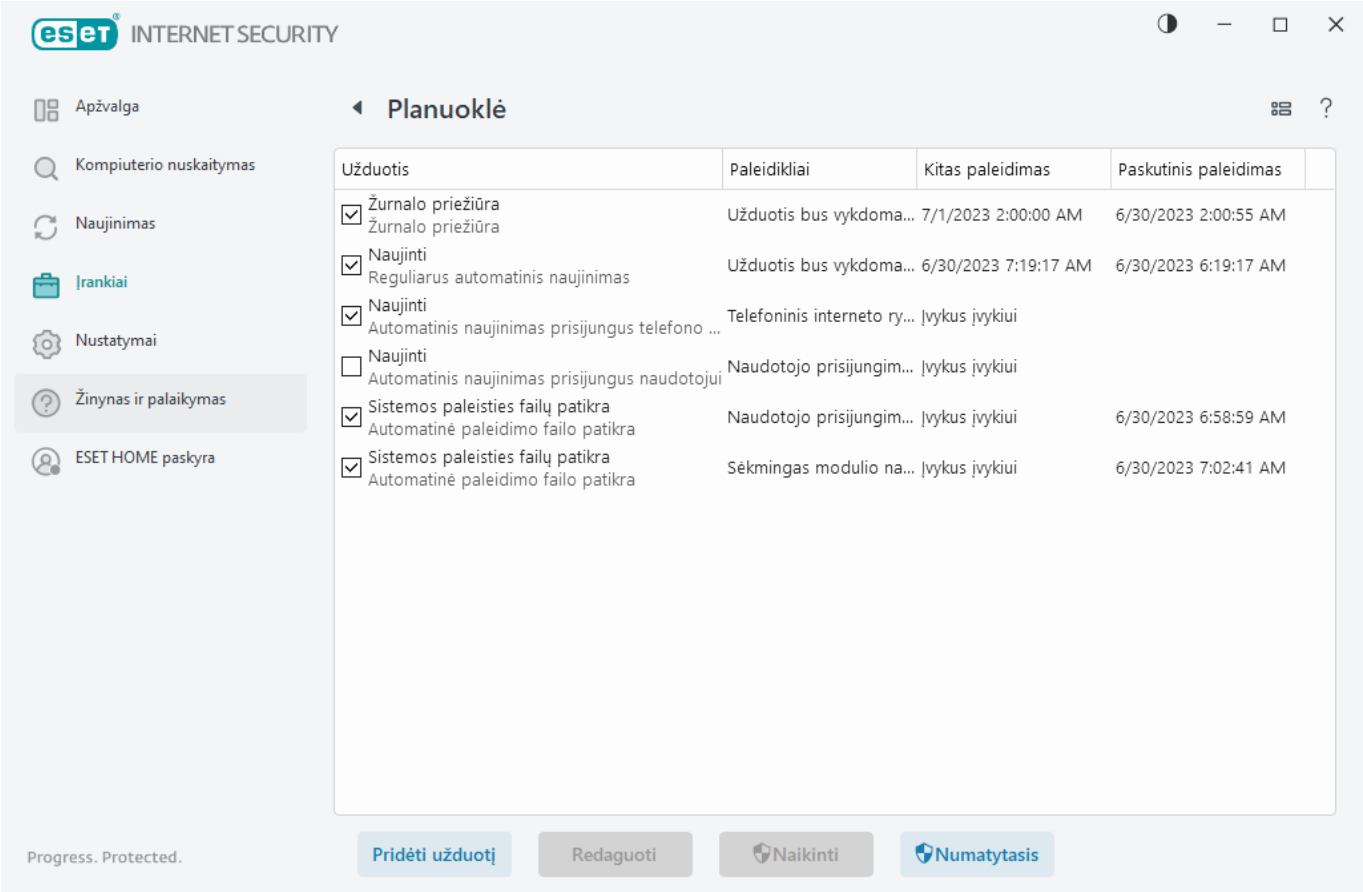
Planuoklę galima pasiekti iš ESET Internet Security pagrindinio programos lango spustelėjus **Įrankiai** > **Planuoklė**. **Planuoklėje** yra visų planuotų užduočių ir konfigūracijos ypatybių sąrašas – iš anksto nustatyta data, laikas ir naudojamas nuskaitymo profilis.

Planuoklė skirta planuoti šias užduotis: naujinimo moduliai, nuskaitymo užduotis, sistemos paleidimo failo patikra ir žurnalo priežiūra. Galite pridėti arba panaikinti užduotis tiesiog pagrindiniame planuoklės lange (spustelėkite **Pridėti užduotį...** arba **Naikinti** apačioje). Galite atkurti numatytąjį suplanuotų užduočių sąrašą ir panaikinti visus pakeitimus spustelėdami **Numatytoji**. Dešiniuoju pelės klavišu spustelėkite bet kur planuoklės lange, kad galėtumėte atlikti šiuos veiksmus: rodyti išsamią informaciją, atlikti užduotį iškart, pridėti naują užduotį ir panaikinti esamą. Naudodami žymės langelius kiekvieno įrašo pradžioje galite aktyvinti / deaktyvinti užduotis.

Pagal numatytuosius nustatymus **planuoklėje** rodomos šios suplanuotos užduotys:

- **Žurnalo priežiūra**
- **Reguliarus automatinis naujinimas**
- **Automatinis naujinimas prisiregistravus vartotojui**
- **Automatinė paleidimo failo patikra** (prisiregistravus vartotojui)
- **Automatinė paleidimo failo patikra** (sėkmingai atnaujinus aptikimo modulį)

Norėdami redaguoti esamos suplanuotos užduoties konfigūraciją (tiek numatytąją, tiek apibrėžtą vartotojo), dešiniuoju pelės klavišu spustelėkite užduotį ir tada **Redaguoti** arba pasirinkite užduotį, kurią norite keisti, ir spustelėkite **Redaguoti**.



Pridėti naują užduotį

1. Spustelėkite **Pridėti užduotį** lango apačioje.

2. Įveskite užduoties pavadinimą.

3. Pasirinkite norimą užduotį iš išskleidžiamojo meniu:

   • **Vykdyti išorinę taikomąją programą** – leidžia planuoti išorinės taikomosios programos vykdymą.

   • **Žurnalo priežiūra** – žurnalo failuose taip pat gali būti panaikintų įrašų likučių. Ši užduotis reguliariai optimizuoja įrašus žurnalo failuose, kad darbas būtų efektyvus.

   • **Sistemos paleidimo failo patikra** – tikrina failus, kurie leidžiami vykdyti paleidžiant sistemą arba registruojantis.

   • **Sukurti kompiuterio būsenos momentinę kopiją** – sukuria ESET SysInspector kompiuterio momentinę kopiją – surenka išsamią informaciją apie sistemos dalis (pvz., tvarkykles, programas) ir įvertina kiekvienos dalies rizikos lygį.

   • **Kompiuterio nuskaitymas pareikalavus** – atlieka kompiuterio failų ir katalogų nuskaitymą.

   • **Naujinti** – atnaujinant modulius suplanuojama naujinimo užduotis.

4. Įjunkite perjungiklį šalia **Įjungta**, jei norite suaktyvinti užduotį (tai galite padaryti vėliau, pažymėdami langelį ar nuimdami jo žymą planinių užduočių sąraše), spustelėkite **Toliau** ir nurodykite vieną iš laiko parinkčių:

   • **Vieną kartą** – užduotis bus atlikta iš anksto nustatyta data ir laiku.

- **Pakartotinai** – užduotis bus atliekama nurodytais intervalais.
- **Kasdien** – užduotis bus pakartotinai vykdoma kasdien nurodytu laiku.
- **Kas savaitę** – užduotis bus vykdoma pasirinktą dieną ir laiku.
- **Įvykus įvykiui** – užduotis bus vykdoma įvykus nurodytam įvykiui.

5. Nurodykite **Praleisti užduotį, kai naudojama akumuliatoriaus energija**, kad maksimaliai apribotumėte energijos sąnaudas, kai nešiojamasis kompiuteris veikia maitinamas akumuliatoriaus. Užduotis bus vykdoma laukuose **Užduoties vykdymas** nurodytą datą ir laiku. Jeigu užduotis negali būti atlikta iš anksto nustatytu laiku, galite nurodyti, kada ji bus vėl vykdoma:

- **Kitu suplanuotu laiku**
- **Kaip įmanoma greičiau**
- **Nedelsiant, jei laikas nuo paskutinio vykdymo viršija (valandas)** – tai laikas, praėjęs nuo pirmojo praleisto užduoties vykdymo. Jei šis laikas bus viršytas, užduotis bus vykdoma iš karto. Nustatykite laiką naudodami toliau pateiktą suktuką.

Norėdami peržiūrėti planinę užduotį, spustelėkite ją dešiniuoju pelės klavišu ir pasirinkite **Rodyti užduoties informaciją**.

Suplanuotos nuskaitymo parinktys

Šiame lange galite nurodyti išplėstines suplanuotos kompiuterio nuskaitymo užduoties parinktis.

Norėdami paleisti nuskaitymą be valymo veiksmo, spustelėkite **Išplėstiniai nustatymai** ir pasirinkite **Nuskaityti be valymo**. Nuskaitymo retrospektyva įrašoma į nuskaitymo žurnalą.

Kai pasirenkama **Nepaisyti išimčių**, bus nuskaitomi ir failai su išimtimis, kurie anksčiau nebuvo įtraukti į nuskaitymą.

Veiksmas po nuskaitymo išplečiamajame meniu leidžia nustatyti veiksmą, kuris turi būti atliekamas automatiškai, kai nuskaitymas bus baigtas:

- **Jokių veiksmų** – užbaigus nuskaitymą nebus atliekami jokie veiksmai.
- **Išjungti** – pasibaigus nuskaitymui kompiuteris išjungiamas.
- **Prireikus paleisti iš naujo** – kompiuteris paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.
- **Paleisti iš naujo** – užbaigus nuskaitymą uždaromos visos atidarytos programos, o kompiuteris paleidžiamas iš naujo.
- **Prireikus priversti paleisti iš naujo** – kompiuteris priverstinai paleidžiamas iš naujo tik jei reikia užbaigti aptiktų grėsmių valymą.
- **Priversti paleisti iš naujo** – priverstinai uždaro visas atidarytas programas nelaukiant naudotojo sąveikos ir iš naujo paleidžia kompiuterį baigus nuskaitymą.

• **Miego režimas** – įrašomas jūsų seansas ir įjungiamas kompiuterio energijos taupymo režimas, kurį išjungę galite greitai tęsti darbą.

• **Sulaikytosios veiksenos režimas** – visus RAM vykdomus procesus perkelia į specialų failą standžiajame diske. Kompiuteris išjungiamas, tačiau kitą kartą įjungę galite tęsti darbą nuo ten, kur baigėte.

Veiksmai **Miego režimas** arba **Sulaikytosios veiksenos režimas** pasiekiami atsižvelgiant į jūsų kompiuterio operacinės sistemos maitinimo ir miego režimo nustatymus arba jūsų stalinio / nešiojamojo kompiuterio galimybes. Atminkite, kad miego režimu veikiantis kompiuteris nėra išjungtas. Jame toliau veikia pagrindinės funkcijos ir vartojama elektros energija, jei kompiuteris veikia naudodamas akumuliatorių. Jei norite pailginti akumuliatoriaus veikimo laiką, pavyzdžiui, išvykę iš biuro, rekomenduojame naudoti sulaikytosios veiksenos režimą.

Pasirinktas veiksmas bus pradėtas užbaigus visus vykdomus nuskaitymus. Pasirinkus **Išjungti** arba **Perkrauti**, patvirtinimo dialogo lange bus rodomas 30 sekundžių atgalinis skaičiavimas (spustelėkite **Atšaukti**, kad išjungtumėte reikalaujamą veiksmą).

Pasirinkite **Nuskaitymo atšaukti negalima**, kad uždraustumėte neįgaliotiems naudotojams sustabdyti veiksmus, kurie atliekami užbaigus nuskaitymą.

Jei ribotų teisių vartotojui norite leisti nurodytam laikui pristabdyti kompiuterio nuskaitymą, pasirinkite parinktį **Vartotojas nuskaitymą gali pristabdyti (min.)**.

Taip pat žr. Nuskaitymo eiga.

Suplanuotų užduočių apžvalga

Dukart spustelėjus pasirinktinę užduotį arba dešiniuoju pelės klavišu spustelėjus pasirinktinę planuoklės užduotį ir tada spustelėjus **Rodyti užduoties informaciją**, šiame dialogo lange pateikiama išsamios informacijos apie pasirinktą planinę užduotį.

Užduoties informacija

Įveskite **Užduoties pavadinimą**, pasirinkite vieną iš parinkčių **Užduoties tipas**, tada spustelėkite **Pirmyn**:

• **Vykdyti išorinę taikomąją programą** – leidžia planuoti išorinės taikomosios programos vykdymą.

• **Žurnalo priežiūra** – žurnalo failuose taip pat gali būti panaikintų įrašų likučių. Ši užduotis reguliariai optimizuoja įrašus žurnalo failuose, kad darbas būtų efektyvus.

• **Sistemos paleidimo failo patikra** – tikrina failus, kurie leidžiami vykdyti paleidžiant sistemą arba registruojantis.

• **Sukurti kompiuterio būsenos momentinę kopiją** – sukuria ESET SysInspector kompiuterio momentinę kopiją – surenka išsamią informaciją apie sistemos dalis (pvz., tvarkykles, programas) ir įvertina kiekvienos dalies rizikos lygį.

• **Kompiuterio nuskaitymas pareikalavus** – atlieka kompiuterio failų ir katalogų nuskaitymą.

• **Naujinti** – atnaujinant modulius suplanuojama naujinimo užduotis.

Užduočių sinchronizacija

Užduotis bus kartojama nurodytu laiko intervalu. Nurodykite vieną iš laiko parinkčių:

- **Vieną kartą** – užduotis bus atlikta tik vieną kartą, iš anksto nustatytą datą ir laiku.
- **Pakartotinai** – užduotis bus atliekama nurodytais intervalais (valandomis).
- **Kasdien** – užduotis bus vykdoma kasdien nurodytu laiku.
- **Kas savaitę** – užduotis bus vykdoma vieną arba daugiau kartų per savaitę, pasirinktą dieną ar dienomis ir laiku.
- **Įvykus įvykiui** – užduotis bus vykdoma įvykus nurodytam įvykiui.

Praleisti užduotį, kai naudojama akumuliatoriaus energija – užduotis nebus paleidžiama, jei planiniu užduoties vykdymo metu jūsų kompiuteris bus maitinamas iš akumuliatoriaus. Tai taikoma ir kompiuteriams, maitinamiems iš UPS.

Užduoties laikas – vieną kartą

Užduoties vykdymas – nurodyta užduotis bus vykdoma tik vieną kartą, nurodytą datą ir laiku.

Užduoties laikas – kasdien

Užduotis bus vykdoma kasdien nurodytu laiku.

Užduoties laikas – kas savaitę

Užduotis bus pakartotinai vykdoma kiekvieną savaitę pasirinktą (-omis) dieną (-omis) ir laiku.

Užduoties laikas – suaktyvintas įvykis

Užduotis bus paleista vieno šių įvykių:

- **Kaskart paleidus kompiuterį**
- **Pirmą kartą paleidžiant kompiuterį kasdien**
- **Telefoninis interneto ryšys / VPN**
- **Sėkmingas modulio naujinimas**
- **Sėkmingas produkto naujinimas**
- **Vartotojo registravimas**

- **Grėsmių aptikimas**

Kai planuojama įvykio paleidžiama užduotis, galima nurodyti minimalų intervalą tarp dviejų užduoties vykdymų. Pavyzdžiui, jeigu prisijungiate prie kompiuterio kelis kartus per dieną, pasirinkite 24 valandas, kad užduotis būtų vykdoma tik tą dieną prisijungiant pirmą kartą, o paskui – kitą dieną.

Praleista užduotis

Užduotį galima praleisti, jei kompiuteris maitinamas akumuliatoriaus energija arba išjungtas. Nurodydami vieną iš šių parinkčių, pasirinkite, kada užduotis turi būti vykdoma, ir spustelėkite **Toliau**:

- **Kitu suplanuotu laiku** – užduotis bus vykdoma, jei kompiuteris bus įjungtas kitu suplanuotu laiku.
- **Kuo greičiau** – užduotis bus vykdoma, jei kompiuteris bus įjungtas.
- **Nedelsiant, jei laikas nuo paskutinio suplanuoto vykdymo viršija (valandas)** – tai laikas, praėjęs nuo pirmojo praleisto užduoties vykdymo. Jei šis laikas bus viršytas, užduotis bus vykdoma iš karto.

Iškart, jei laikas nuo paskutinio suplanuoto vykdymo viršija (valandos) – pavyzdžiai

Pavyzdinė užduotis nustatyta pakartotinai vykdyti kas valandą. Pasirenkama parinktis **jei laikas nuo paskutinio suplanuoto vykdymo viršija (valandas)** ir viršytas laikas yra dvi valandos. Užduotis vykdoma 13.00 val., o užbaigus kompiuteris užmigs:

- Kompiuteris atsibunda 15.30 val. Pirmasis praleistas užduoties vykdymas buvo 14.00 val. Nuo 14.00 val. praėjo tik 1,5 valandos, todėl užduotis bus vykdoma 16.00 val.
- Kompiuteris atsibunda 16.30 val. Pirmasis praleistas užduoties vykdymas buvo 14.00 val. Nuo 14.00 val. praėjo 2,5 valandos, todėl užduotis bus vykdoma nedelsiant.

Išsami užduoties informacija – naujinti

Jeigu norite naujinti programą iš dviejų naujinimo serverių, būtina sukurti du skirtingus naujinimų profilius. Jeigu iš pirmojo nepavyksta atsisiųsti naujinimų failų, programa automatiškai pereina prie alternatyvaus serverio. Tai tinka, pavyzdžiui, nešiojamiesiems kompiuteriams, kurie paprastai naujinami iš vietinio LAN naujinimo serverio, tačiau jų savininkai dažnai prisijungia prie interneto naudodami kitus tinklus. Todėl jeigu pirmasis profilis negali atsisiųsti, antrasis automatiškai atsisiųs naujinimų failus iš ESET naujinimo serverių.

Išsami užduoties informacija – Vykdyti taikomąją programą

Šis užduotis suplanuoja išorinės taikomosios programos vykdymą.

Vykdomasis failas – pasirinkite vykdomąjį failą iš katalogo medžio, spustelėkite parinktį **...** arba įveskite kelią rankiniu būdu.

Darbo aplankas – nurodykite išorinės taikomosios programos darbinį katalogą. Visi laikinieji pasirinkto **vykdomojo failo** failai bus kuriami šiame kataloge.

Parametrai – taikomosios programos komandos eilutės parametrai (nebūtini).

Spustelėkite **Baigti**, kad priskirtumėte užduotį.

Sistemos valymo priemonė

Sistemos valymo priemonė – tai įrankis, padedantis atkurti tokią kompiuterio būseną, kad juo būtų galima naudotis pašalinus grėsmę. Kenkėjiškos programos galima išjungti sistemos pagalbines programas, pvz., registrų rengyklę, užduočių tvarkytuvę ar „Windows“ naujinimus. Sistemos valymo priemonė atkuria konkrečios sistemos numatytąsias reikšmes ir nustatymus vienu spustelėjimu.

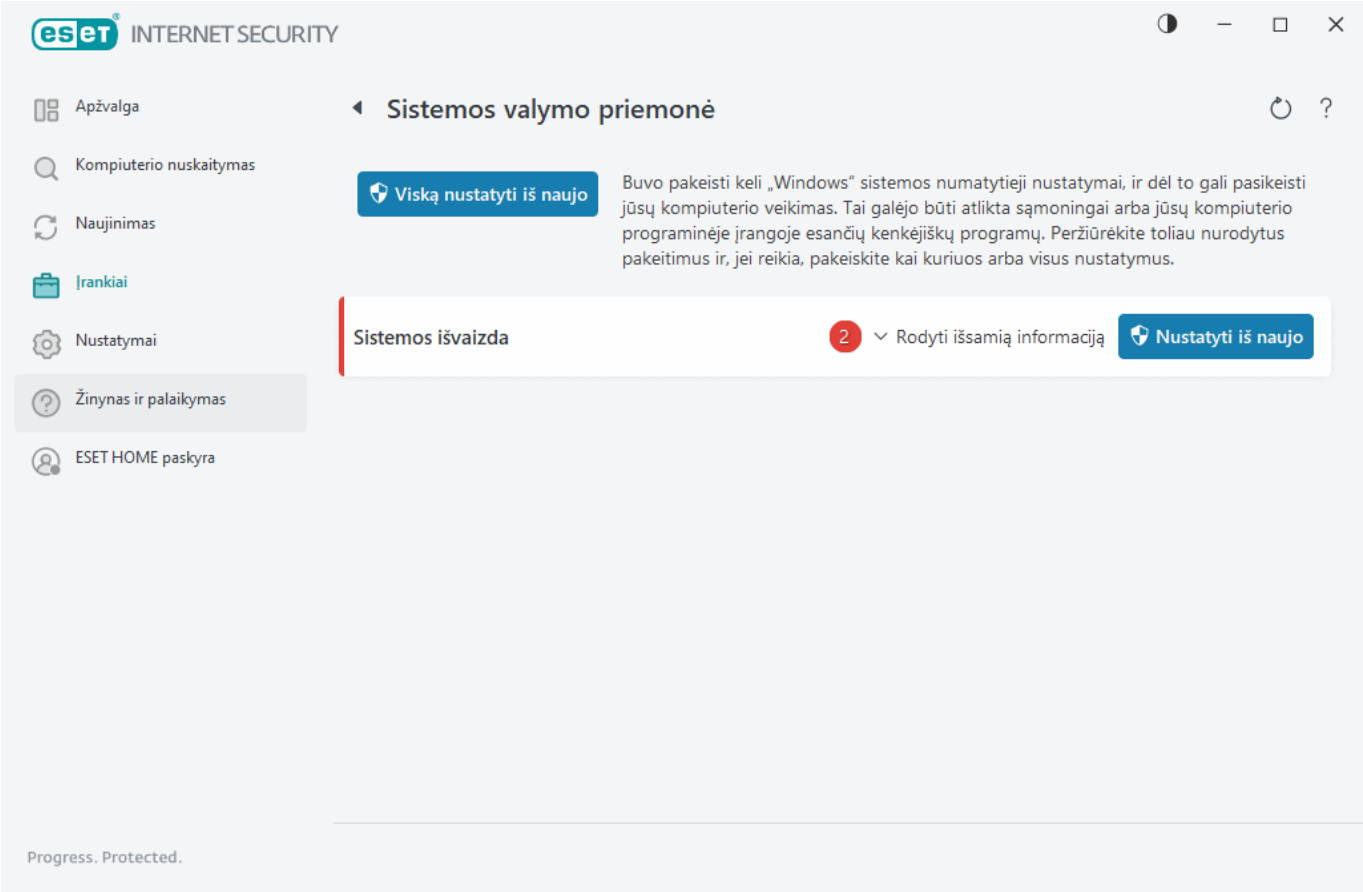
Sistemos valymo priemonė praneša apie problemas penkiose nustatymų kategorijose:

- **Apsaugos nustatymai**: nustatymų pakeitimai, dėl kurių gali padidėti jūsų kompiuterio pažeidžiamumas, pvz., „Windows“ naujinimo
- **Sistemos nustatymai**: sistemos nustatymų pakeitimai, kurie gali pakeisti jūsų kompiuterio veikimą, pvz., failų asociacijas
- **Sistemos išvaizda**: nustatymai, kurie keičia sistemos išvaizdą, pvz., darbalaukio foną
- **Išjungtos funkcijos**: svarbios funkcijos ir programos, kurios gali būti išjungtos
- **„Windows“ sistemos atkūrimas**: „Windows“ sistemos atkūrimo funkcijos nustatymai, kurie leidžia atkurti ankstesnę sistemos būseną

Sistemos valymas gali būti atliekamas, kai:

- aptinkama grėsmė;
- vartotojas spusteli **Nustatyti iš naujo**.

Jei norite galite peržiūrėti pakeitimus ir iš naujo nustatyti parametrus.



Veiksmus su sistemos valymo priemone gali atlikti tik vartotojas, kuriam suteiktos administratoriaus teisės.

Tinklo tikrinimo įrankis

Tinklo tikrinimo įrankis gali padėti nustatyti silpnąsias jūsų patikimo (namų arba biuro) tinklo vietas (pvz., atvirus prievadus ar silpną maršruto parinktuvo slaptažodį). Jis taip pat suteikia prijungtų įrenginių sąrašą, kuriame įrenginiai suskirstyti pagal tipą (pvz., spausdintuvas, maršruto parinktuvas, mobilusis įrenginys ir pan.) – taip galite aiškiai matyti, kas yra prijungta prie tinklo (pvz., žaidimų konsolė, IoT ar kiti išmanieji namų įrenginiai).

Tinklo tikrinimo įrankis padeda nustatyti silpnąsias maršruto parinktuvo vietas ir sustiprina apsaugą, kai prisijungiama prie tinklo.

Tinklo tikrinimo įrankis iš naujo nekonfigūruoja jūsų maršruto parinktuvo. Pakeitimus atliksite patys naudodamiesi specializuota maršruto parinktuvo sąsaja. Maršrutų parinktuvai namuose gali būti lengvai panaudoti kenkėjiškų programų, kuriomis paleidžiamos paskirstytosios aptarnavimo perkrovos atakoms (DDoS). Jei naudotojas nepakeitė numatytojo maršruto parinktuvo slaptažodžio, įsilaužėliams lengva jį atspėti, o tada prisijungti prie jūsų maršruto parinktuvo ir perkonfigūruoti jį arba pakenkti jūsų tinklui.

Primygtinai rekomenduojame sukurti sudėtingą slaptažodį, kuris būtų pakankamai ilgas, ir jame būtų skaitmenų, simbolių ar didžiųjų raidžių. Kad slaptažodį būtų sunkiai „nulaužti“, naudokite skirtingų simbolių derinį.

Jei tinklas, prie kurio esate prisijungę, sukonfigūruotas kaip patikimas, tinklą galite pažymėti kaip „Mano tinklas“. Spustelėkite **Žymėti kaip „Mano tinklas“**, kad prie tinklo pridėtumėte žymą „Mano tinklas“. Ši žyma bus rodoma šalia tinklo visame ESET Internet Security, kad būtų galima geriau nustatyti ir peržiūrėti saugą. Norėdami pašalinti žymą, spustelėkite **Pašalinti žymą „Mano tinklas“**.

Kiekvienas įrenginys, prijungtas prie jūsų tinklo, rodomas sąrašo rodinyje su pagrindine informacija. Spustelėkite konkretų įrenginį, jei norite redaguoti įrenginį arba peržiūrėti išsamią informaciją apie įrenginį.

Išskleidžiamajame meniu **Tinklai** galite filtruoti įrenginius pagal šiuos kriterijus:

- Įrenginiai, prijungti prie konkretaus tinklo
- Įrenginiai, prijungti prie **Visų tinklų**
- Įrenginiai be kategorijų

Spustelėkite įrenginio piktogramą, jei norite redaguoti įrenginį arba peržiūrėti išsamią informaciją apie įrenginį. Neseniai prijungti įrenginiai rodomi arčiau maršrutizatoriaus, kad juos būtų lengviau pamatyti.

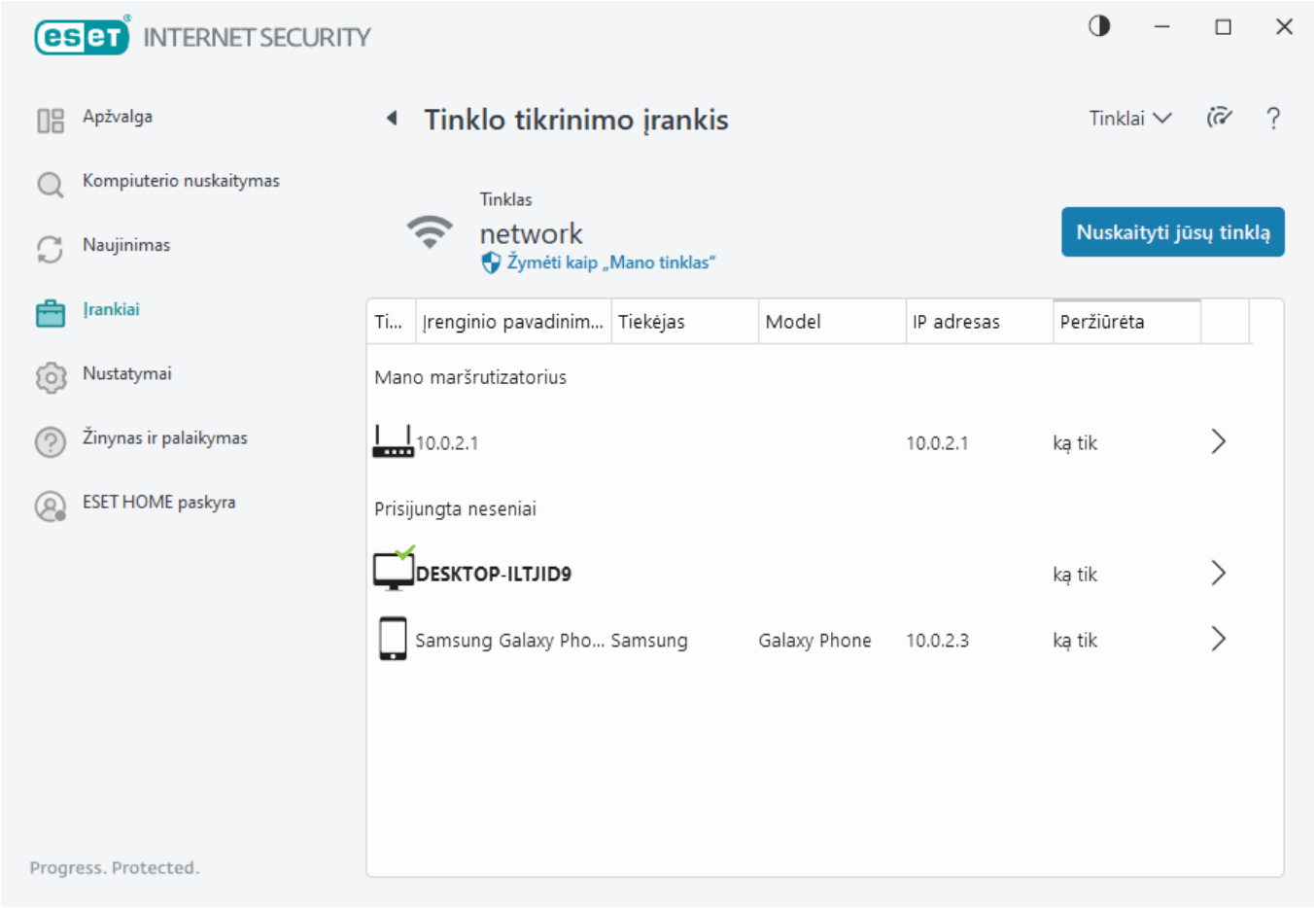
Viršutiniame dešiniajame kampe spustelėkite krumpliaratį ⚙ ir pasirinkite, ar pranešti, kai tinkle aptinkamas naujas įrenginys.

Jei norite rankiniu būdu nuskaityti tinklą, prie kurio šiuo metu esate prisijungę, spustelėkite **Nuskaityti tinklą**. **Nuskaityti tinklą** galima tik patikimo tinklo atveju. Žr. Tinklo ryšio profiliai, norėdami peržiūrėti arba redaguoti tinklo nustatymus.

Galite rinktis iš šių nuskaitymo parinkčių:

- Nuskaityti viską
- Nuskaityti tik kelvedį
- Nuskaityti tik įrenginius

⚠ Tinklo nuskaitymus atlikite tik patikimame tinkle! Jei ketinate tai atlikti nepatikimuose tinkluose, saugokitės galimo pavojaus.



Pasibaigus nuskaitymui parodomas pranešimas su saitu į bendrąją informaciją apie įrenginį arba galite dukart spustelėti įtartiną įrenginį sąraše ar sonaro rodinyje. Jei norite peržiūrėti pastaruoju metu užblokuotus ryšius, spustelėkite **Trikčių diagnostika**. Daugiau informacijos apie užkardos trikčių šalinimą.

Tinklo tikrinimo įrankio modulyje rodomi dviejų tipų pranešimai:

- **Prie tinklo prijungtas naujas įrenginys** – rodomas, jei vartotojui esant prisijungus prie tinklo prisijungia anksčiau nematytas įrenginys.
- **Aptiktas naujas tinklo įrenginys** – rodoma, jei iš naujo prisijungiate prie savo patikimo tinklo ir jame yra anksčiau nematytas įrenginys.

Abiejų tipų pranešimai informuoja jus, jei neįgaliotas įrenginys bando prisijungti prie jūsų tinklo. Spustelėkite **rodyti įrenginį**, kad matytumėte išsamią informaciją apie įrenginį.

Ką reiškia piktogramos tinklo tikrinimo įrankio įrenginiuose?

	Geltonos žvaigždutės piktograma nurodomi įrenginiai, kurie tinkle yra nauji arba kuriuos ESET aptiko pirmą kartą.
	Geltona perspėjimo piktograma nurodoma, kad maršruto parinktuve gali būti pažeidžiamų vietų. Norėdami gauti išsamesnės informacijos apie problemą, spustelėkite produkto piktogramą.
	Raudona įspėjimo piktograma nurodomi įrenginiai, dėl kurių maršruto parinktuve gali būti pažeidžiamų vietų ir kurie gali būti užkrėsti. Norėdami gauti išsamesnės informacijos apie problemą, spustelėkite produkto piktogramą.

Mėlyna piktograma gali atsirasti, kai ESET produktas turi papildomos informacijos jūsų maršruto parinktuvui, tačiau nereikalauja skubaus dėmesio, nes nėra rizikos saugai. Norėdami gauti išsamesnės informacijos, spustelėkite produkto piktogramą.

Tinklo įrenginys Tinklo tikrinimo įrankyje

Išsami informacija apie įrenginį pateikiama čia, įskaitant:

- Įrenginio pavadinimas
- Įrenginio tipas
- Pastarąjį kartą matytas
- Tinklo pavadinimas
- IP adresas
- MAC adresas
- Operacinės sistemos

Pieštuko piktograma rodo, kad galite modifikuoti įrenginio pavadinimą arba tipą.

Šalinti iš retrospektyvos – pašalinkite įrenginį iš įrenginių sąrašo. Ši parinktis galima tik įrenginiams, kurie šiuo metu nėra prijungti prie jūsų tinklo.

Galimi šie su kiekvienu įrenginio tipu susiję veiksmai:

Maršrutizatoriaus

Maršruto parinktuvo nustatymai – maršruto parinktuvo nustatymus galite pasiekti žiniatinklio sąsajoje, mobiliojoje programoje arba spustelėję **Atidaryti maršruto parinktuvo sąsają**. Jei turite interneto paslaugų teikėjo teikiamą maršruto parinktuvą, gali tekti susisiekti su interneto paslaugų teikėjo palaikymo ištekliais arba maršruto parinktuvo gamintoju, kad būtų galima išspręsti aptiktas saugos problemas. Visuomet laikykitės tinkamų saugos priemonių, nurodytų maršruto parinktuvo naudotojo vadove.
Apsauga – Norėdami apsaugoti kelvedį ir tinklą nuo kibernetinio saugumo atakų, vadovaukitės toliau pateiktomis pagrindinėmis rekomendacijomis.

Tinklo įrenginys

Įrenginio identifikacija – jei nesate tikri dėl įrenginio, prijungto prie jūsų tinklo, patikrinkite po įrenginio pavadinimu esantį pardavėjo ar gamintojo vardą. Tai gali padėti nustatyti, koks tai yra įrenginys. Galite pakeisti įrenginio pavadinimą, kad ateityje nekiltų neaiškumų.
Įrenginio atjungimas – jei nesate tikri, kad prijungtas įrenginys nekenkia jūsų tinklui ar kitiems įrenginiams, tvarkykite šio įrenginio tinklo prieigą maršruto parinktuvo nustatymuose arba pakeiskite tinklo slaptažodį.
Apsauga – norėdami apsaugoti savo įrenginį nuo atakų ir kenkėjiškos programinės įrangos, savo įrenginyje įdiekite kibernetinio saugumo apsaugą ir visuomet užtikrinkite, kad jūsų operacinė sistema ir įdiegta programinė įranga būtų atnaujinta. Siekdami neprarasti apsaugos, nesijunkite prie nesaugių „Wi-Fi“ tinklų.

Šis įrenginys

Šis įrenginys nurodo jūsų kompiuterį tinkle.
Tinklo adapteriai – rodoma informacija apie jūsų tinklo adapterius.

Pranešimai | Tinklo tikrinimo įrankis

Toliau pateikiami keli pranešimai, kurie gali būti parodyti, kai ESET Internet Security aptinka kokią nors kelvedžio pažeidžiamumo problemą. Kiekviename pranešime pateikiamas trumpas aprašymas ir koks nors sprendimas ar veiksmai, kuriuos reikia atlikti norint sumažinti kelvedžio pažeidžiamumo pavojų. Jei neišmanote kelvedžio nuostatų keitimo, rekomenduojame kreiptis į kelvedžio gamintoją arba interneto ryšio tiekėją.

Aptiktas galimas pažeidžiamumas
Jūsų kelvedyje gali būti žinomų pažeidžiamų vietų, kurios gali padėti surengti ataką ar juo pasinaudoti. Atnaujinkite kelvedžio programinę aparatinę įrangą.

Aptiktas pažeidžiamumas
Jūsų kelvedyje yra pažeidžiamų vietų, kurios leidžia surengti ataką arba jį išnaudoti. Atnaujinkite kelvedžio programinę aparatinę įrangą.

Rasta grėsmė
Jūsų kelvedis yra užkrėstas kenkėjiška programa. Paleiskite kelvedį iš naujo ir pakartokite nuskaitymą.

Silpnas kelvedžio slaptažodis
Jūsų kelvedžio slaptažodis yra silpnas, todėl kiti jį gali lengvai atspėti. Pakeiskite slaptažodį kelvedyje.

Kenkėjiškas tinklo srauto nukreipimas
Jūsų interneto duomenų srautas nukreipiamas į kenkėjiškas svetaines. Tai gali reikšti, kad į kelvedį buvo įsilaužta. Pakeiskite DNS serverio nustatymą kelvedyje.

Atvirojo tinklo paslaugos
Jūsų kelvedyje veikia tinklo tarnybos, kurios gali būti naudojamos kitų. Taip gali nutikti dėl prastos konfigūracijos arba įsilaužimo į kelvedį. Patikrinkite kelvedžio konfigūraciją.

Jautrios atvirojo tinklo paslaugos
Jūsų kelvedyje veikia jautrios tinklo tarnybos, kurios gali būti naudojamos kitų. Taip gali nutikti dėl prastos konfigūracijos arba įsilaužimo į kelvedį. Patikrinkite kelvedžio konfigūraciją.

Pasenusi programinė aparatinė įranga
Kelvedžio programinė aparatinė įranga pasenusi, todėl joje gali būti pažeidžiamų vietų. Atnaujinkite kelvedžio programinę aparatinę įrangą.

Kenkėjiškas kelvedžio nustatymai
Šis jūsų naudojamas DNS serveris gali būti kenkėjiškas ir gali nukreipti jus į pavojingas svetaines. Tai gali reikšti, kad į kelvedį buvo įsilaužta. Pakeiskite DNS serverio nustatymą kelvedyje.

Tinklo paslaugos
Jūsų kelvedyje veikia bendrosios tinklo tarnybos. Jos reikalingos tinklui ir tikriausiai yra saugios. Patikrinkite kelvedžio konfigūraciją.

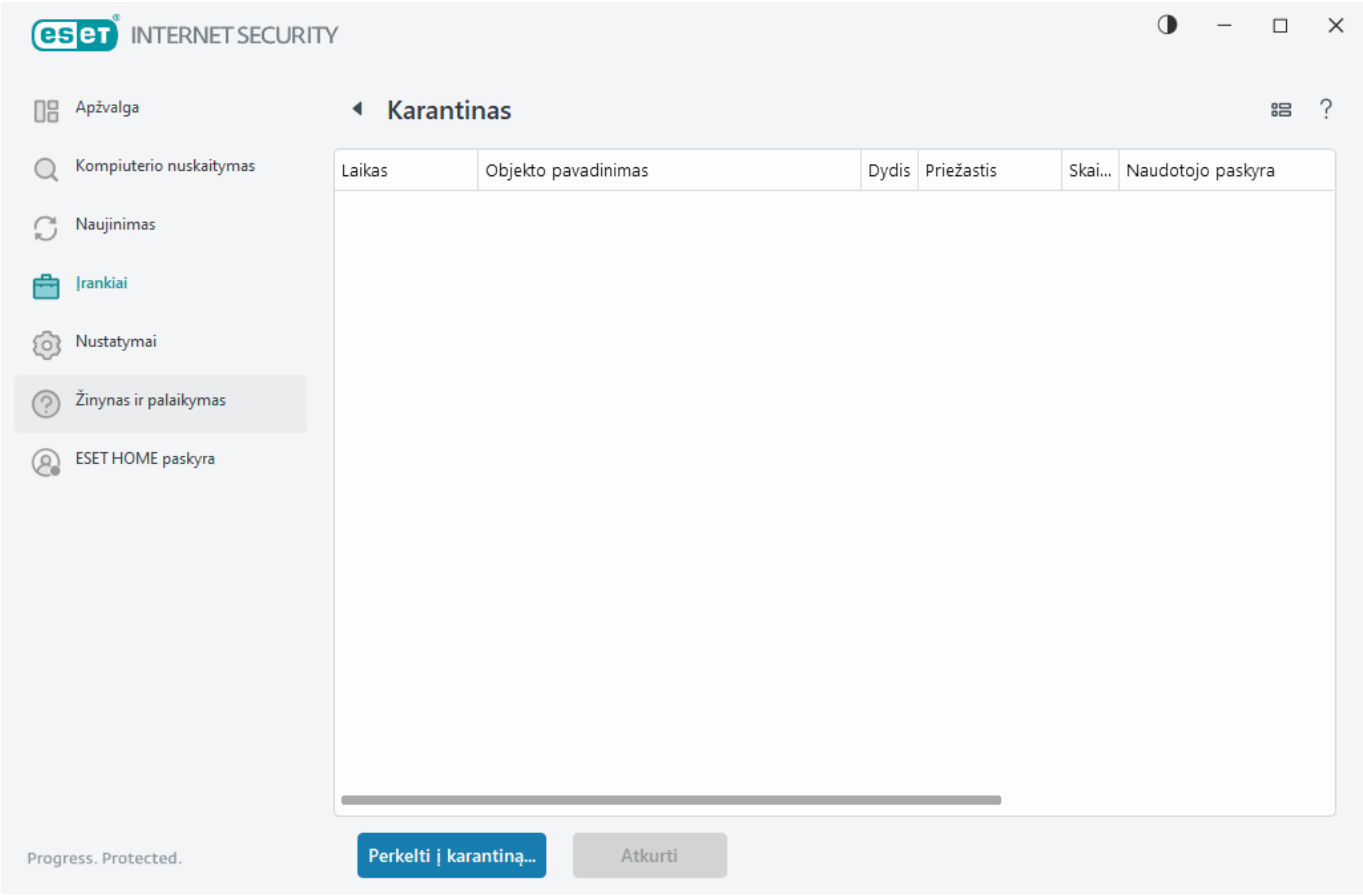
Karantinas

Pagrindinė karantino funkcija – saugiai saugoti objektus, apie kuriuos pranešta (pvz., kenkėjišką programinę įrangą, užkrėstus failus arba galimas nepageidaujamas taikomąsias programas).

Karantiną galima pasiekti ESET Internet Security pagrindiniame programos lange spustelėjus **Įrankiai** > **Karantinas**.

Karantino aplanke laikomus failus galima peržiūrėti lentelėje, kurioje rodoma:

- karantinavimo data ir laikas,
- kelias į originalią failo vietą,
- failo dydis baitais,
- priežastis (pvz., objektą pridėjo naudotojas),
- aptikimų skaičius (pvz., pasikartojantys to paties failo aptikimai arba archyvas, kuriame yra keli įsiskverbimai).



Failų karantinavimas

ESET Internet Security automatiškai karantinuoja pašalintus failus (jei neatšaukėte šios parinkties įspėjimų lange).

Papildomus failus reikėtų karantinuoti, jeigu:

a.jų negalima išvalyti,

b.nesaugu arba nepatartina jų pašalinti,

c.juos klaidingai aptiko ESET Internet Security,

d.failai įtartinai atrodo, tačiau jų neaptinka Apsaugos priemonės.

Norėdami karantinuoti failą, galite rinktis iš šių galimybių:

a.Failui karantinuoti rankiniu būdu galite naudoti funkciją „Nuvilkti“ – tiesiog spustelėkite failą ir laikydami nuspaudę pelės mygtuką perkelkite pelės žymeklį į pažymėtą sritį, tada mygtuką atleiskite. Tada programa perkeliama į pirmą planą.

b.Dešiniuoju pelės mygtuku spustelėkite failą, tada spustelėkite **Išplėstinės parinktys** > **Karantinuoti failą**.

c.Lange **Karantinas** spustelėkite **Perkelti į karantiną**.

d.Tam galima naudoti ir kontekstinį meniu – spustelėkite dešiniuoju pelės klavišu langą **Karantinas** ir pasirinkite **Karantinuoti**.

Atkūrimas iš karantino

Karantinuotus failus taip pat galima atkurti į jų originalią vietą:

- Šiuo tikslu naudokite funkciją **Atkurti**, kuri pasiekiama kontekstiniame meniu, dešiniuoju pelės klavišu spustelėjus nurodytą karantinuotą failą.
- Jei failas pažymėtas kaip galima nepageidaujama taikomoji programa, aktyvinta parinktis **Atkurti ir neįtraukti į nuskaitymą**. Taip pat žr. skiltį Išimtys.
- Be to, kontekstiniame meniu siūloma parinktis **Atkurti į**, kuri leidžia atkurti failą į kitą vietą (ne į tą, iš kurios jis buvo pašalintas).
- Atkūrimo funkcija kai kuriais atvejais nepasiekiama, pvz., failams, esantiems tik skaitomoje tinklo dalyje.

Pašalinimas iš karantino

Spustelėkite dešiniuoju pelės klavišu pateiktą elementą ir pasirinkite **Naikinti iš karantino** arba pasirinkite norimą naikinti elementą ir klaviatūroje paspauskite klavišą **Delete**. Jei norite pažymėti ir pašalinti visus karantino elementus, galite paspausti klaviatūroje **Ctrl + A**, o tuomet **Delete**. Panaikinti elementai bus visam laikui pašalinti iš jūsų įrenginio ir karantino.

Failų pateikimas iš karantino

Jeigu karantinavote įtartiną failą, kurio neaptiko programa, arba jeigu failas buvo neteisingai nustatytas kaip užkrėstas (pvz., atliekant kodo euristikos analizę) ir todėl izoliuotas karantinui, nusiųskite pavyzdį išanalizuoti ESET tyrimų laboratorijai. Norėdami pateikti failą, spustelėkite jį dešiniuoju pelės klavišu ir pasirinkite **Pateikti analizuoti** iš kontekstinio meniu.

Aptikimo aprašas

Dešiniuoju pelės mygtuku spustelėkite elementą ir spustelėkite **Aptikimo aprašymas**, kad atidarytumėte ESET grėsmių enciklopediją, kurioje pateikiama išsami informacija apie užregistruoto įsiskverbimo pavojus ir požymius.

> **Iliustruotos instrukcijos**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Atkurti karantinuotą failą ESET Internet Security
> - Pašalinti karantinuotą failą ESET Internet Security
> - Mano ESET produktas pranešė apie aptikimą. Ką man daryti?

Karantinuoti nepavyko

Priežastys, kodėl tam tikrų failų negalima perkelti į karantiną:

- **Jūs neturite skaitymo leidimų** – reiškia, kad negalite peržiūrėti failo turinio.
- **Jūs neturite rašymo leidimų** – reiškia, kad negalite modifikuoti failo turinio, t. y. įtraukti naujo turinio ar panaikinti esamą turinį.
- **Failas, kurį bandote karantinuoti, yra per didelis** – turite sumažinti failo dydį.

Jei gaunate klaidos pranešimą „Karantinas nepavyko“, spustelėkite **Daugiau informacijos**. Parodomas karantino klaidų sąrašas ir matysite failo pavadinimą bei priežastį, kodėl failo negalima karantinuoti.

Pasirinkti mėginį analizei

Jeigu radote įtartiną failą savo kompiuteryje arba įtartiną svetainę internete, galite pateikti jį analizuoti ESET tyrimų laboratorijai (gali būti neprieinama atsižvelgiant į ESET LiveGrid® konfigūraciją).

Prieš pateikiant pavyzdžius ESET

Pateikite tik šiuos reikalavimus atitinkančius pavyzdžius:
- Pavyzdžio visiškai neaptinka jūsų ESET produktas
- Pavyzdys klaidingai aptiktas kaip grėsmė
- Nepriimame jūsų asmeninių failų (kad pati ESET patikrintų, ar juose nėra kenkėjiškų programų ESET) kaip pavyzdžių (ESET tyrimų laboratorija netikrina vartotojų failų pagal pageidavimą)
- Aiškiai aprašykite temą ir pateikti kuo daugiau informacijos apie šį failą (pavyzdžiui, ekrano kopiją arba svetainę, iš kurios jis atsisiųstas)

Pavyzdį (failą arba svetainę) ESET analizei galite atsiųsti vienu iš šių būdų:

1. Naudokite savo produkto pavyzdžio pateikimo formą. Ji yra dalyje **Įrankiai** > **Pavyzdžio pateikimas siekiant atlikti analizę**. Maksimalus pateikto pavyzdžio dydis yra 256 MB.

2. Arba galite pateikti failą el. paštu. Jeigu pasirenkate šį būdą, supakuokite failą (-us) WinRAR/WinZIP programa, apsaugokite archyvą slaptažodžiu „infected“ (užkrėstas) ir siųskite jį adresu samples@eset.com.

3. Norėdami pranešti apie brukalą, klaidingai teigiamą brukalą arba svetaines, kurioms tėvų kontrolės modulis priskyrė klaidingą kategoriją, žr. ESET žinių bazės straipsnį.

Formoje **Pasirinkti pavyzdį analizei** pasirinkite aprašą iš išskleidžiamojo meniu **Failo pateikimo priežastis**, kuris geriausiai atitinka jūsų tikslą:

- Įtartinas failas
- Įtartina svetainė (svetainė, užkrėsta bet kokia kenkėjiška programa),
- Klaidingai teigiama svetainė
- Klaidingai teigiamas failas (failas, kuris buvo aptiktas kaip užkrėstas, bet nėra užkrėstas),
- Kita

Failas / svetainė – kelias į failą arba svetainę, kurį norite pateikti.

Kontaktinis el. paštas – šis kontaktinis el. pašto adresas yra siunčiamas kartu su įtartinais failais į ESET ir gali būti naudojamas norint susisiekti su jumis, jeigu analizei reikalinga papildoma informacija. Įvesti kontaktinį el. pašto adresą nebūtina. Norėdami palikti tuščią, pasirinkite **Pateikti anonimiškai**.

> **Galite gauti ESET atsakymą**
> Jūs negausite atsakymo iš ESET, jeigu nereikės daugiau informacijos. Kasdien mūsų serveriai gauna dešimtis tūkstančių failų, todėl neįmanoma atsakyti visiems juos pateikusiems.
> Jeigu pavyzdys pasirodys esantis kenkėjiška programa arba svetainė, jo aptikimas bus įtrauktas į būsimą ESET naujinimą.

Pasirinkti pavyzdį analizei – įtartinas failas

Pastebėti užkrėtimo kenkėjiška programa ženklai ir požymiai – įveskite savo kompiuteryje pastebėto įtartino failo veikimo aprašymą.

Failo kilmė (URL adresas arba tiekėjas) – įveskite failo kilmę (šaltinį) ir kaip jūs susidūrėte su šiuo failu.

Pastabos ir papildoma informacija – čia galite pridėti papildomos informacijos arba aprašymą, kuris padėtų apdorojant įtartiną failą.

> Pirmasis parametras – **pastebėti užkrėtimo kenkėjiška programa ženklai ir požymiai** – yra būtinas, tačiau pateikdami papildomą informaciją labai padėsite mūsų laboratorijoms identifikuojant ir apdorojant pavyzdžius.

Pasirinkti pavyzdį analizei – įtartinas svetainė

Pasirinkite vieną iš šių parinkčių išskleidžiamajame meniu **Kas negerai su šia svetaine?**:

- **Užkrėsta** – svetainė, kurioje yra įvairiai platinamų virusų arba kenkėjiškų programų.
- **Sukčiavimas apsimetant** naudojamas norint gauti prieigą prie slaptų duomenų, tokių kaip banko sąskaitų numeriai, PIN kodai ir t. t. Išsamiau apie šio tipo atakas skaitykite terminų žodyne.
- **Apsimestinė svetainė** – apgaulinga svetainė, kuri siekia greito pelno.
- Pasirinkite **Kita**, jei anksčiau pateiktos parinktys nenurodo svetainės, kurią pateiksite.

Pastabos ir papildoma informacija – galite įvesti papildomą informaciją arba aprašą, kuris padės analizuoti įtartiną svetainę.

Pasirinkti pavyzdį analizei – klaidingai aptiktas failas

Mes prašome pateikti failus, kurie buvo aptikti kaip užkrėsti, bet nėra užkrėsti, kad galėtume patobulinti apsaugos nuo virusų ir šnipinėjimo programų modulį ir geriau apsaugotume kitus. Klaidingai teigiami (KT) rezultatai gali būti gaunami, kai failo dalis sutampa su tokia pat dalimi aptikimo modulyje.

Programos pavadinimas ir versija – programos pavadinimas ir jos versija (pavyzdžiui, numeris, alternatyvusis vardas arba kodo pavadinimas).

Failo kilmė (URL adresas arba tiekėjas) – įveskite failo kilmę (šaltinį) ir nurodykite, kaip jūs susidūrėte su šiuo failu.

Programos paskirtis – bendras programos aprašas, jos tipas (pvz., naršyklė, medijos leistuvas...) ir jos funkcionalumas.

Pastabos ir papildoma informacija – čia galite pridėti papildomos informacijos arba aprašymą, kuris padėtų apdorojant įtartiną failą.

> Pirmieji trys parametrai yra būtini, kad būtų galima nustatyti teisėtas programas ir atskirti jas nuo kenkėjiško kodo. Pateikdami papildomos informacijos, jūs labai padėsite mūsų laboratorijoms identifikuojant ir apdorojant pavyzdžius.

Pasirinkti pavyzdį analizei – klaidingai aptikta svetainė

Mes prašome pateikti svetaines, kurios aptinkamos kaip užkrėstos arba apgaulingos, bet tokios nėra. Klaidingai teigiami (KT) rezultatai gali būti gaunami, kai failo dalis sutampa su tokia pat dalimi aptikimo modulyje. Prašome pateikti šią svetainę, kad galėtume pagerinti apsaugos nuo virusų ir šnipinėjimo programų modulį ir geriau apsaugoti kitus.

Pastabos ir papildoma informacija – čia galite pridėti papildomos informacijos arba aprašymą, kuris padėtų tvarkant įtartiną svetainę.

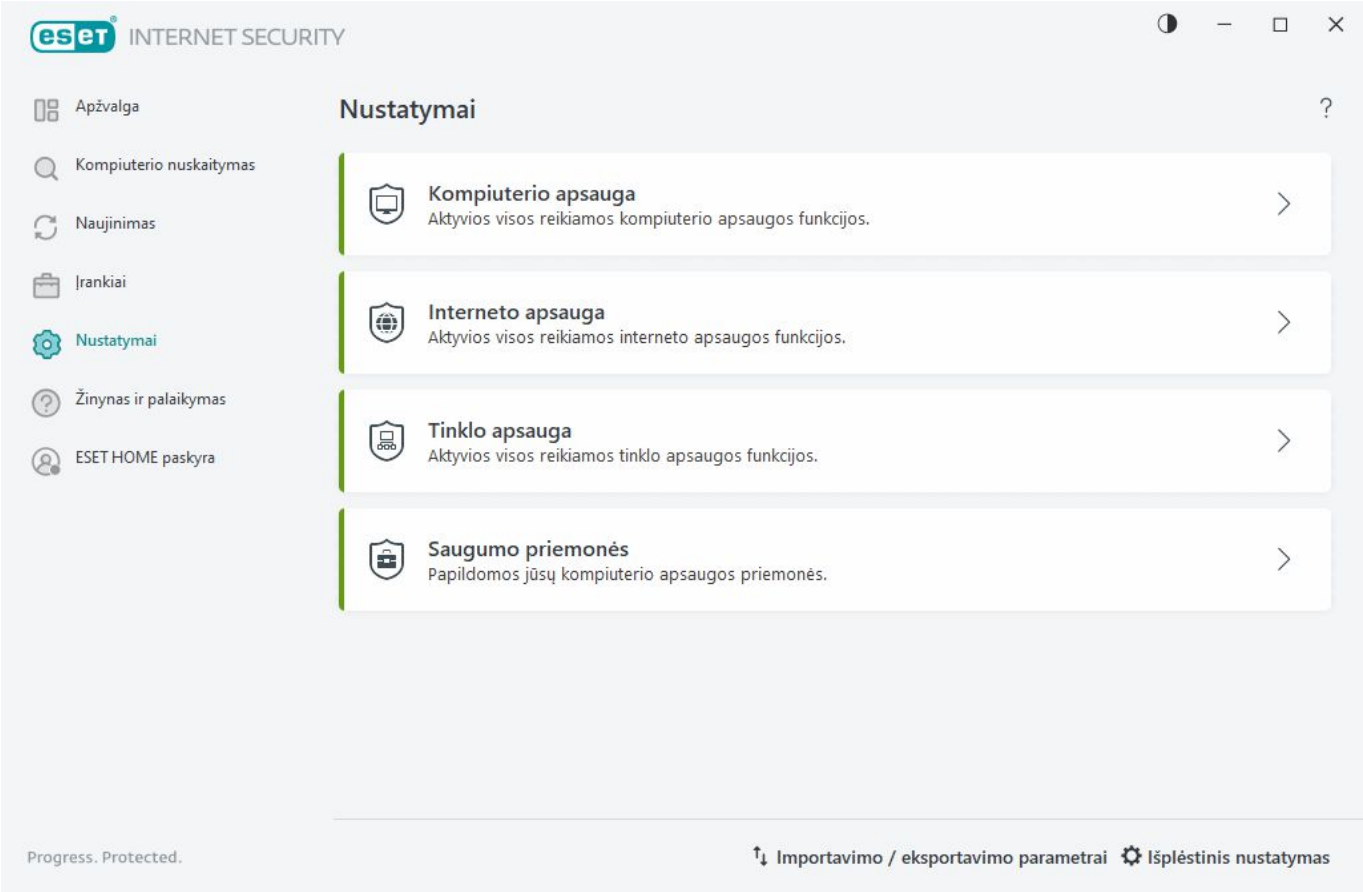
Pasirinkti pavyzdį analizei – kitas

Naudokite šią formą, jeigu failas negali būti priskirtas **įtartinų failų** arba **klaidingai teigiamų** kategorijai.

Failo pateikimo priežastis – įveskite išsamų aprašymą ir failo siuntimo priežastį.

Nustatymai

Galimų apsaugos funkcijų grupes galite rasti pagrindiniame programos lange > **Nustatymai**.



Meniu **Nustatymai** yra suskirstytas į šiuos skyrius:

Kompiuterio apsauga

Interneto apsauga

Tinklo apsauga

Saugumo priemonės

Nustatymo lango apačioje yra pateikiamos papildomos parinktys. Jei norite nustatyti išsamesnius kiekvieno modulio parametrus, pasinaudokite Išplėstinio nustatymo nuoroda. Pasinaudokite Importuoti / eksportuoti parametrus, kad įkeltumėte nustatymo parametrus iš .xmll konfigūravimo failo, arba įrašykite dabartinius nustatymo parametrus konfigūravimo faile.

Kompiuterio apsauga

Spustelėkite parinktį **Kompiuterio apsauga**, kurią rasite pagrindiniame programos lange > **Nustatymai**, kad pamatytumėte visų apsaugos modulių apžvalgą:

- Failų sistemos apsauga realiuoju laiku – visi failai atidarant, kuriant ar vykdant juos yra nuskaitomi tikrinant, ar nėra kenkėjiškų kodų.

- Įrenginio kontrolė – šis modulis leidžia nuskaityti, blokuoti nešiojamąją laikmeną arba pakeisti jos išplėstinius filtrus / teises ir pasirinkti, kaip vartotojas gali pasiekti ir naudotis konkrečiu įrenginiu (CD / DVD /

USB ir pan.).

• HIPS – HIPS sistema stebi įvykius operacinėje sistemoje ir į juos reaguoja pagal pasirinktinių taisyklių rinkinį.

• Žaidimų režimas – įjungia arba išjungia žaidimų režimą. Įjungę žaidimų režimą, gausite įspėjamąjį pranešimą (galima saugos rizika), o pagrindinis langas pasidarys oranžinis.

• Interneto kameros apsauga – valdo procesus ir programas, kurios pasiekia prie prijungtą kamerą.

Norėdami pristabdyti arba išjungti atskirus apsaugos modulius, spustelėkite perjungiklio piktogramą  .

⚠ Išjungus apsaugos modulius gali sumažėti jūsų kompiuterio apsaugos lygis.

Spustelėkite krumpliaračio piktogramą šalia apsaugos modulio, kad pereitumėte prie išplėstinių šio modulio parametrų.

Norėdami **apsaugoti failų sistemą realiuoju laiku,** spustelėkite krumpliaračio piktogramą ir pasirinkite iš šių parinkčių:

• **Konfigūruoti** – atidaromas failų sistemos apsaugos realiuoju laiku išplėstinis nustatymas.

• **Redaguoti išskyrimus** – atidaromas langas Išskyrimo nustatymas, kad būtų galima neįtraukti failų ir aplankų į nuskaitymą.

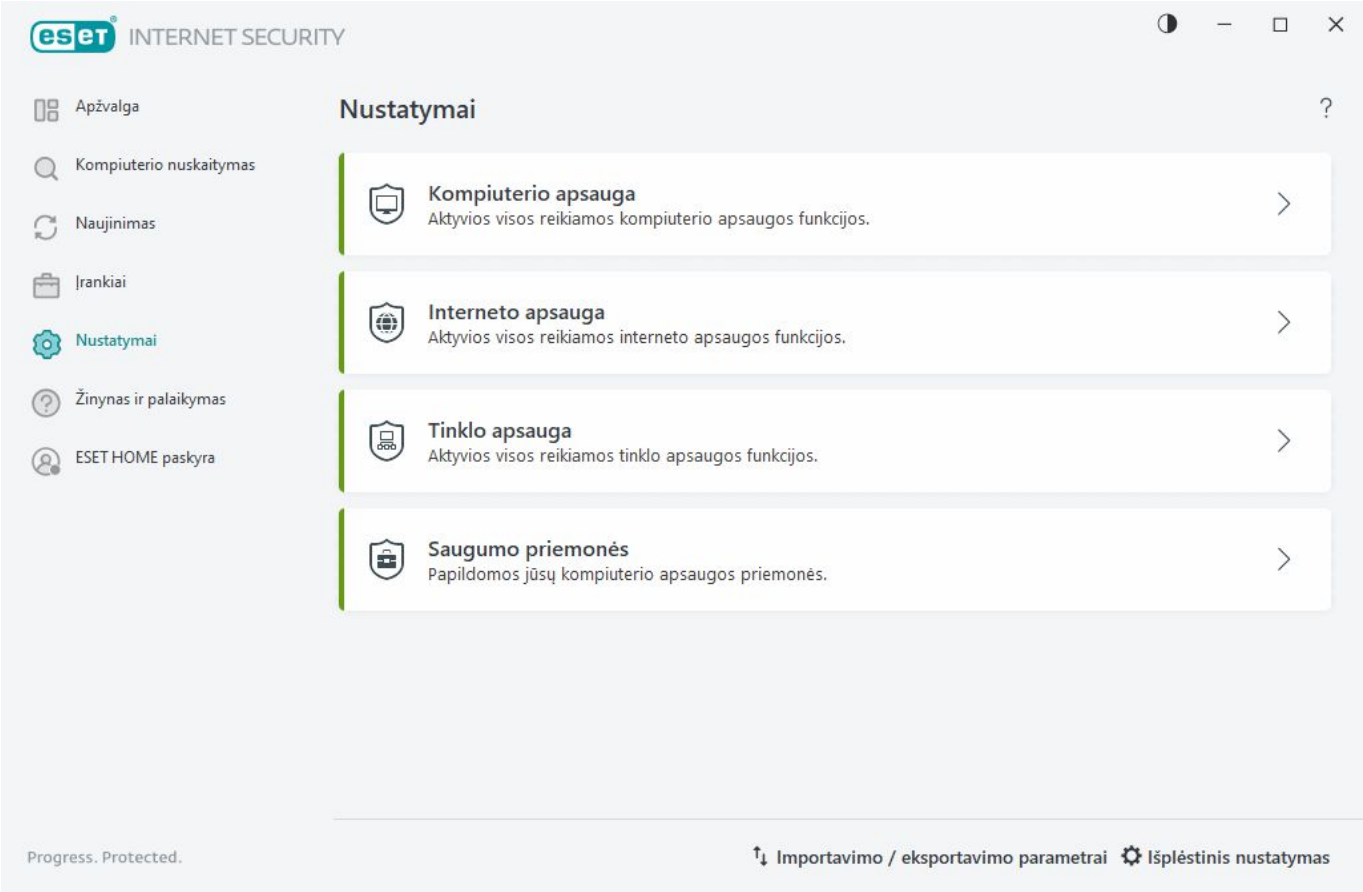
Norėdami **Interneto kameros apsaugos**, spustelėkite ir pasirinkite iš šių parinkčių:

• **Konfigūruoti** – atidaromas interneto kameros apsaugos išplėstinis nustatymas.

• **Blokuoti visą prieigą, kol bus paleista iš naujo** – blokuojama visa prieiga prie interneto kameros, kol kompiuteris bus paleistas iš naujo.

• **Blokuoti visą prieigą visam laikui** – blokuojama visa prieiga prie interneto kameros, kol šis nustatymas bus išjungtas.

• **Stabdyti visos prieigos blokavimą** – išjungiama galimybė blokuoti prieigą prie interneto kameros. Ši parinktis galima tik tuo atveju, jei prieiga prie interneto kameros užblokuota.



Pristabdyti apsaugą nuo virusų ir šnipinėjimo programų – išjungiami visi apsaugos nuo virusų ir šnipinėjimo programų moduliai. Išjungus apsaugą pasirodys langas, kuriame galėsite nustatyti, kiek laiko apsauga bus išjungta – pasinaudokite išskleidžiamuoju meniu **Laiko intervalas**. Naudokite, tik jei esate patyręs vartotojas arba vadovaudamiesi ESET techninės pagalbos nurodymais.

Aptiktas įsiskverbimas

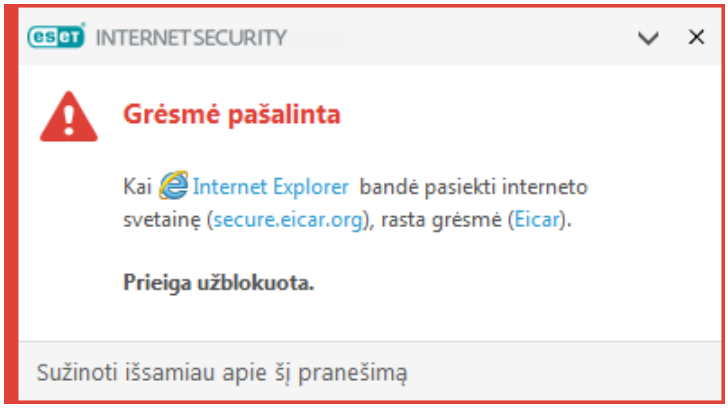
Įsiskverbimai gali patekti į sistemą per įvairius įsiskverbimo taškus: iš tinklalapių, bendrinamų aplankų, el. paštu arba iš nešiojamųjų įrenginių (USB, išorinių diskų, CD, DVD ir t. t.).

Standartinis veikimas

Bendras pavyzdys, kaip įsiskverbimus apdoroja ESET Internet Security, gali būti įsiskverbimų aptikimas, kai naudojama:

- Failų sistemos apsauga realiuoju laiku
- Prieigos prie saityno apsauga
- El. pašto programų apsauga
- Kompiuterio nuskaitymas pareikalavus

Kiekvienas jų naudoja standartinį valymo lygį ir bandys išvalyti failą bei perkelti jį į Karantiną arba nutraukti ryšį. Pranešimo langas rodomas informacinių pranešimų srityje, apatiniame dešiniajame lango kampe. Išsamią informaciją apie aptiktus / išvalytus objektus rasite dalyje Žurnalo failai. Daugiau informacijos apie valymo lygius ir veiksmus rasite skyriuje Valymo lygis.



Kompiuterio nuskaitymas ieškant užkrėstų failų

Jeigu jūsų kompiuteryje atsiranda užsikrėtimo kenkėjiška programa požymių, pvz., jis pradeda lėčiau veikti, dažnai sustoja ir t. t., rekomenduojame atlikti šiuos veiksmus:

1.Atidarykite ESET Internet Security ir spustelėkite **„Kompiuterio nuskaitymas“**.

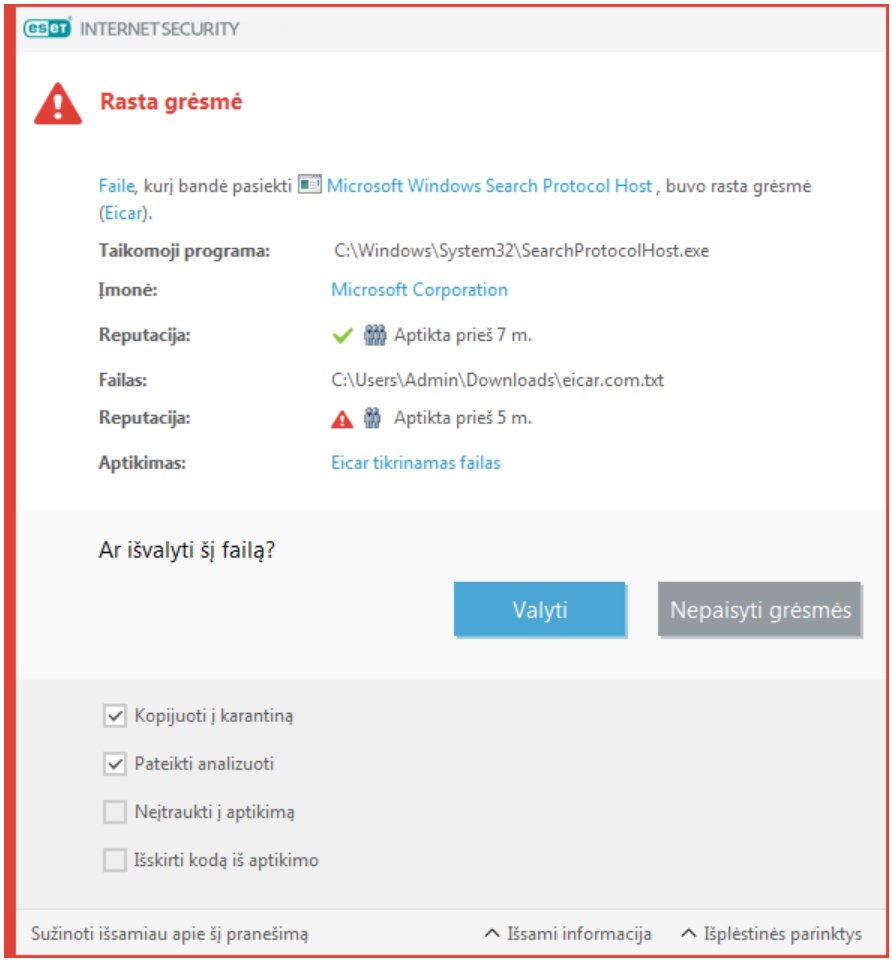
2.Spustelėkite **Nuskaityti kompiuterį** (daugiau informacijos rasite Kompiuterio nuskaitymas).

3.Kai nuskaitymas bus baigtas, peržiūrėkite žurnalą, kuriame pateikiamas nuskaitytų, užkrėstų ir išvalytų failų skaičius.

Jeigu norite nuskaityti tik tam tikrą disko dalį, spustelėkite **Pasirinktinis nuskaitymas** ir pasirinkite tikslus, kuriuos reikia nuskaityti ieškant virusų.

Valymas ir naikinimas

Jeigu nėra iš anksto nustatyto veiksmo, kurį turi vykdyti failų sistemos apsauga realiuoju laiku, jūsų paprašys pasirinkti parinktį perspėjimo lange. Paprastai siūlomos parinktys **Valyti**, **Naikinti** ir **Nieko nedaryti**. Pasirinkti **Nieko nedaryti** nerekomenduojama, nes taip užkrėsti failai liks neišvalyti. Išimtis gali būti, kai esate tikri, jog failas yra nekenksmingas ir buvo aptiktas klaidingai.



Naudokite valymą, jeigu failą atakavo virusas ir prie jo prijungė kenkėjišką kodą. Tokiu atveju pirmiausia bandykite išvalyti užkrėstą failą ir atkurti jo originalią būseną. Jeigu failą sudaro tik kenkėjiškas kodas, jis bus panaikintas.

Jei užkrėstas failas yra „užrakintas“ arba naudojamas sistemos proceso, jis bus panaikintas, tik kai atsilaisvins (paprastai paleidus sistemą iš naujo).

Atkūrimas iš karantino

Karantiną galima pasiekti ESET Internet Security pagrindiniame programos lange spustelėjus **Įrankiai** > **Karantinas**.

Karantinuotus failus taip pat galima atkurti į jų originalią vietą:

- Šiuo tikslu naudokite funkciją **Atkurti**, kuri pasiekiama kontekstiniame meniu, dešiniuoju pelės klavišu spustelėjus nurodytą karantinuotą failą.
- Jei failas pažymėtas kaip galima nepageidaujama taikomoji programa, aktyvinta parinktis **Atkurti ir neįtraukti į nuskaitymą**. Taip pat žr. skiltį Išimtys.
- Be to, kontekstiniame meniu siūloma parinktis **Atkurti į**, kuri leidžia atkurti failą į kitą vietą (ne į tą, iš kurios jis buvo pašalintas).
- Atkūrimo funkcija kai kuriais atvejais nepasiekiama, pvz., failams, esantiems tik skaitomoje tinklo dalyje.

Keletas grėsmių

Jei kurie nors užkrėsti failai nebuvo išvalyti nuskaitant kompiuterį (arba buvo parinkta parametro Valymo lygis vertė **Nevaloma**), bus pateiktas perspėjimo langas, kuriame raginama pasirinkti, ką daryti su šiais failais. Pasirinkite, ką daryti su failais (veiksmai yra nustatyti atskirai kiekvienam sąraše esančiam failui), tada spustelėkite **Baigti**.

Failų naikinimas archyvuose

Numatytuoju valymo režimu visas archyvas bus panaikintas, tik jeigu jame visi failai yra užkrėsti ir nėra švarių. Kitaip tariant, archyvai nebus panaikinami, jeigu juose yra ir nekenksmingų švarių failų. Būkite atsargūs, kai atliekate nuskaitymą naudodami griežtą valymą – įjungtas griežtas valymas, neatsižvelgdamas į kitų archyvo failų būseną, archyvą panaikins, jeigu jame yra bent vienas užkrėstas failas.

Interneto apsauga

Galimybė jungtis prie interneto yra standartinė asmeninio kompiuterio funkcija. Deja, internetas taip pat tapo pagrindine kenkėjiško kodo persiuntimo terpe. Atidarykite pagrindinį programos langą > **Nustatymai** > **interneto apsauga**, kad sukonfigūruotumėte funkcijas ESET Internet Security, kurios padidina jūsų interneto apsaugą.

Norėdami pristabdyti arba išjungti atskirus apsaugos modulius, spustelėkite perjungiklio piktogramą .

Išjungus apsaugos modulius gali sumažėti jūsų kompiuterio apsaugos lygis.

Spustelėkite krumpliaračio piktogramą šalia apsaugos modulio, kad pereitumėte prie išplėstinių šio modulio

parametrų.

Tėvų kontrolės modulis apsaugo jūsų vaikus, blokuodamas netinkamą arba žalingą turinį internete.

Prieigos prie saityno apsauga nuskaito HTTP/HTTPS ryšį ir nustato, ar nėra kenkėjiškų programų ir sukčiavimo apsimetant atvejų. Prieigos prie saityno apsauga turėtų būti išjungta tik atliekant trikčių diagnostiką.

Apsauga nuo sukčiavimo apsimetant leidžia blokuoti žinomas svetaines, kurios platina apgaulingą turinį. Primygtinai rekomenduojame palikti apsaugą nuo sukčiavimo apsimetant įjungtą.

Pranešti apie sukčiavimo apsimetant svetainę – praneškite apie sukčiavimo apsimetant / kenkėjišką svetainę ESET analizei.

> Prieš pateikdami svetainę ESET įsitikinkite, kad ji atitinka vieną ar daugiau iš šių kriterijų:
> • Svetainė visiškai nebuvo aptikta.
> • Svetainė klaidingai aptikta kaip grėsmė. Tokiu atveju galite Pranešti apie netinkamai užblokuotą puslapį.

El. pašto programos apsauga kontroliuoja el. pašto ryšius, priimamus naudojant POP3(S) ir IMAP(S) protokolus. Naudodama jūsų el. pašto programos papildinį, ESET Internet Security užtikrina visų ryšių iš el. pašto programos kontrolę.

El. pašto programos apsauga nuo brukalo filtruoja nepageidaujamus el. laiškus.

Norėdami atlikti pakeitimus parinktyje **El. pašto programos apsauga nuo brukalo**, spustelėkite krumpliaračio piktogramą ir pasirinkite iš šių parinkčių:

- **Konfigūruoti** – atveria išplėstinius el. pašto programos apsaugos nuo brukalo nustatymus.
- **Naudotojo adresų sąrašas** (jei įgalintas) – atidaro dialogo langą, kuriame galite pridėti, redaguoti arba pašalinti adresus, kad nustatytumėte apsaugos nuo brukalo taisykles. Šio sąrašo taisyklės bus taikomos dabartiniam naudotojui.
- **Visuotinis adresų sąrašas** (jei įgalintas) – atidaro dialogo langą, kuriame galite pridėti, redaguoti arba pašalinti adresus, kad nustatytumėte apsaugos nuo brukalo taisykles. Šio sąrašo taisyklės bus taikomos visiems naudotojams.

Apsauga nuo sukčiavimo apsimetant

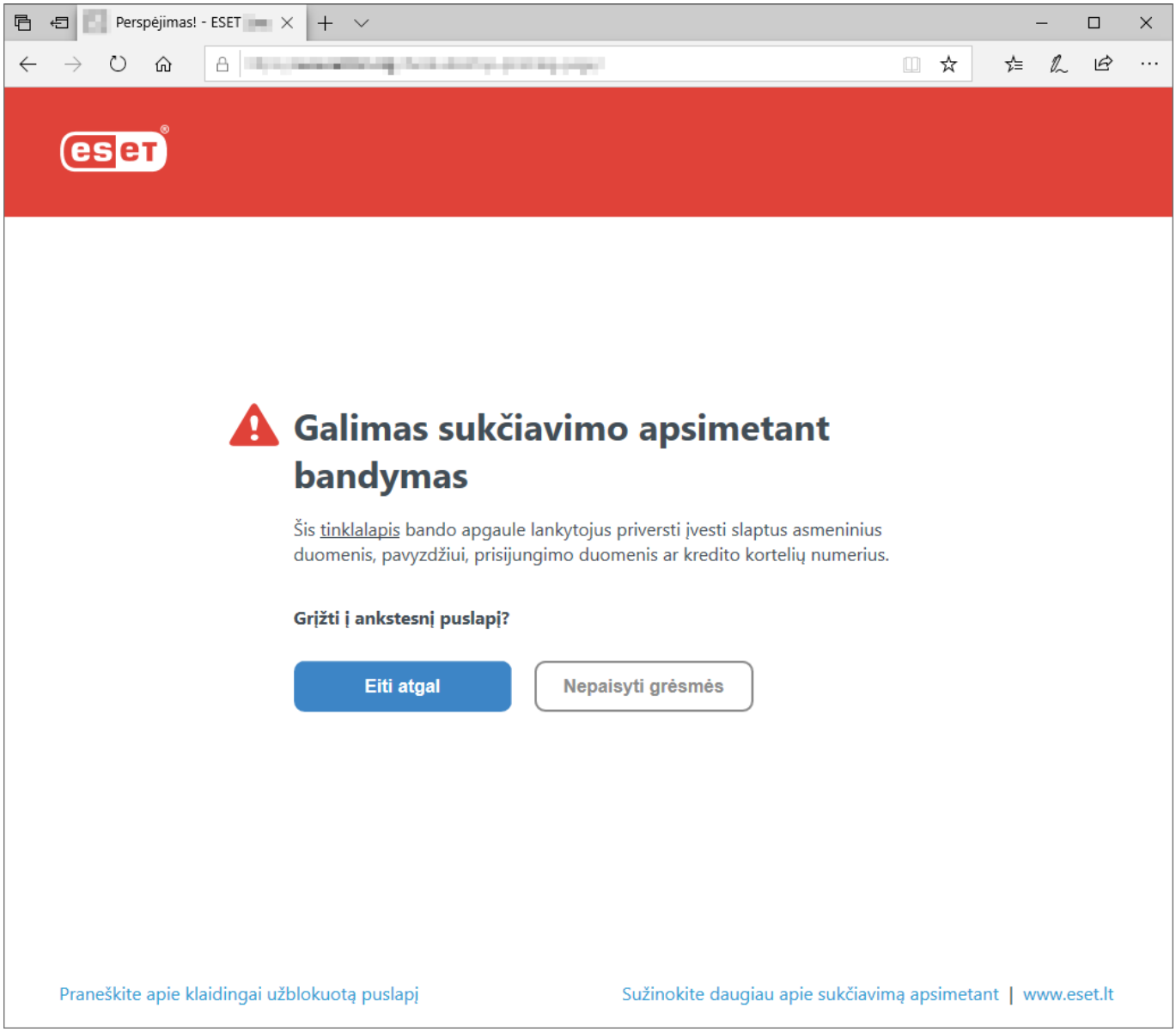
Sukčiavimas apsimetant yra nusikalstama veikla, kurioje naudojama socialinė inžinerija (manipuliavimas naudotojais, siekiant gauti konfidencialią informaciją). Sukčiavimas apsimetant naudojamas norint pasiekti neskelbtinus duomenis, pvz., banko sąskaitų numerius, PIN kodus ir kt. Daugiau informacijos rasite terminų žodyne. ESET Internet Security yra apsaugos nuo sukčiavimo apsimetant funkcija, kuri blokuoja tinklalapius, platinančius šio tipo turinį.

Apsauga nuo sukčiavimo apsimetant įgalinta pagal numatytuosius nustatymus. Šį parametrą galima konfigūruoti, pasirinkus Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga**.

Apsilankę mūsų žinių bazės straipsnyje rasite daugiau informacijos apie ESET Internet Security apsaugą nuo sukčiavimo apsimetant.

Prieiga prie apsimestinės svetainės

Kai pasiekiate atpažintą sukčiavimo apsimetant svetainę, jūsų saityno naršyklėje bus rodomas šis dialogo langas. Jei svetainėje vis tiek norėsite apsilankyti, spustelėkite **Nepaisyti grėsmės** (nerekomenduojama).



Galimos sukčiavimo apsimetant svetainės, kurios buvo įtrauktos į baltąjį sąrašą, pagal numatytuosius nustatymus nustos galioti po keleto valandų. Kad leistumėte naudoti interneto svetainę nuolat, naudokite URL adresų valdymo įrankį. Dalyje Išplėstinis nustatymai > **Apsaugos priemonės** > **Prieigos prie saityno apsauga** > **URL adresų valdymas** > **Adresų sąrašas** > **Redaguoti** įtraukite į sąrašą svetainę, kurią norite redaguoti.

Pranešti apie sukčiavimo apsimetant svetainę

Naudodami saitą **Pranešti apie neteisingai užblokuotą puslapį** galite pranešti apie svetainę, kuri klaidingai aptikta kaip grėsmė.

Arba galite pateikti svetainę el. paštu. Siųskite el. laišką adresu samples@eset.com. Būtinai nurodykite aprašomąją temą ir pridėkite kuo daugiau informacijos apie svetainę (pvz., svetainę, iš kurios čia patekote, kaip sužinojote apie šią svetainę ir pan.).

Tėvų kontrolė

Tėvų kontrolės modulyje galima sukonfigūruoti tėvų kontrolės parametrus, kurie pateikia tėvams automatinius įrankius, padedančius apsaugoti jų vaikus ir nustatyti apribojimus įrenginiams ir paslaugoms. Jų tikslas – neleisti vaikams ir jaunuoliams pasiekti puslapių su netinkamu arba žalingu turiniu.

Tėvų kontrolė leidžia blokuoti interneto puslapius, kuriuose gali būti galimos žalingos informacijos. Be to, tėvai gali uždrausti prieigą prie daugiau nei 40 iš anksto nustatytų svetainių kategorijų ir daugiau nei 140 pogrupių.

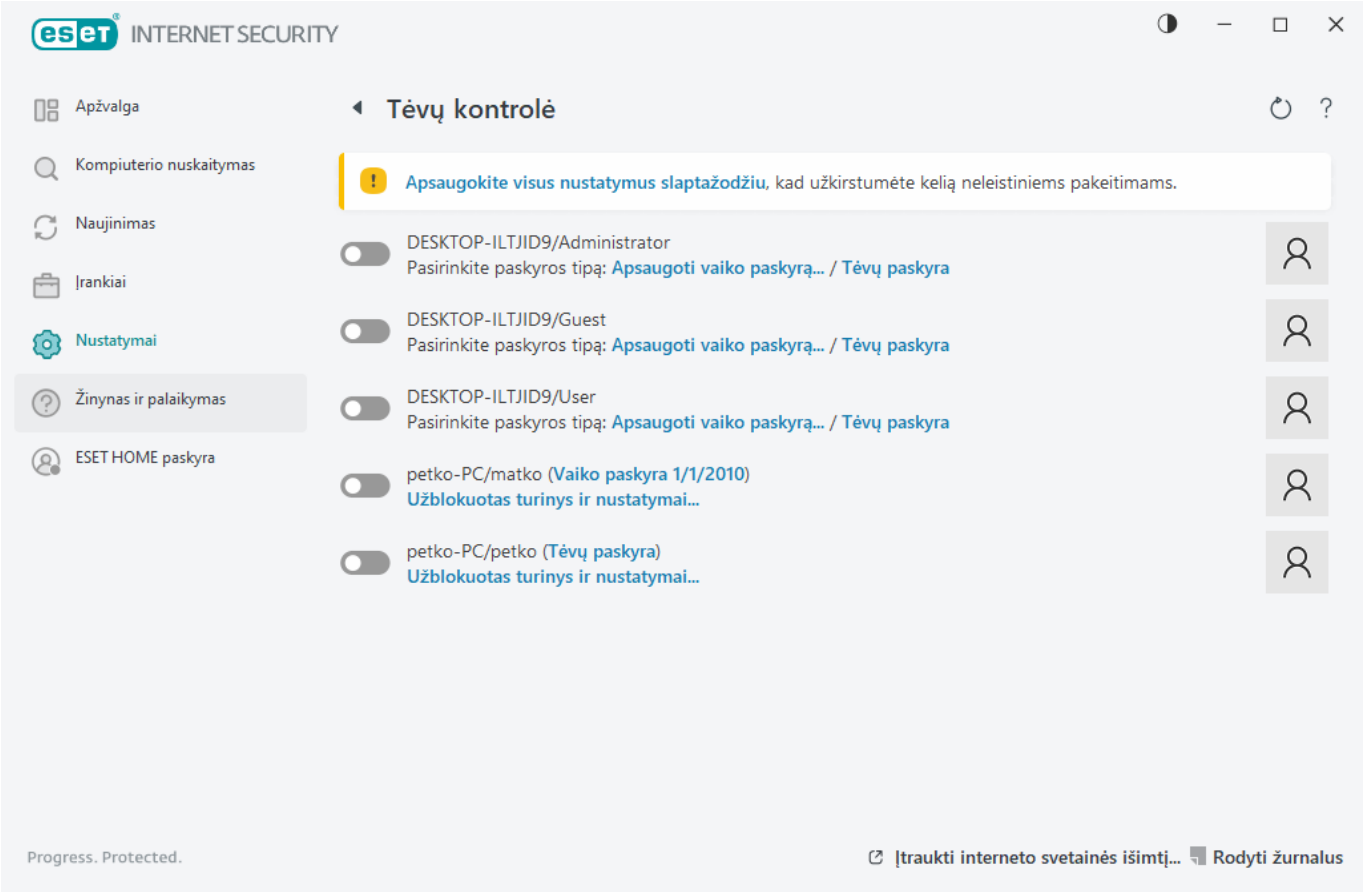
Norėdami aktyvinti konkrečios vartotojo paskyros tėvų kontrolę, atlikite žemiau pateiktus veiksmus:

1. Pagal numatytuosius nustatymus ESET Internet Security tėvų kontrolė yra išjungta. Yra du tėvų kontrolės aktyvinimo būdai:

   • Pagrindiniame programos lange spustelėkite perjungimo piktogramą, esančią **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė** ir pakeiskite tėvų kontrolės būseną į „Įjungta“.

   • Atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga** > **Tėvų kontrolė** ir įjunkite perjungiklį šalia parinkties **Įgalinti tėvų kontrolę**.

2. Pagrindiniame programos lange spustelėkite **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė**. Nors prie funkcijos **Tėvų kontrolė** rodomas užrašas **Įjungta**, spustelėdami rodyklės simbolį ir kitame lange pasirinkdami **Apsaugoti vaiko paskyrą** arba **Tėvų paskyra** turite sukonfigūruoti tėvų kontrolę reikiamai paskyrai. Kitame lange pasirinkite gimimo datą, pagal kurią nustatomas prieigos lygis ir rekomenduojami pagal amžių tinkami tinklalapiai. Tada nurodytoje naudotojo paskyroje įjungiama tėvų kontrolė. Spustelėkite **Blokuojamas turinys ir nustatymai** po paskyros pavadinimu, kad galėtumėte tinkinti kategorijas, kurias norite leisti arba blokuoti skirtuke Kategorijos. Norėdami leisti arba blokuoti pasirinktinius tinklalapius, kurie neatitinka kategorijos, spustelėkite skirtuką Išimtys.



Jei spustelėsite **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė** pagrindiniame ESET Internet Security produkto lange, tada pagrindiniame lange pamatysite:

„Windows“ vartotojų paskyros

Jeigu sukūrėte esamos paskyros vaidmenį, jis bus rodomas čia. Spustelėkite perjungiklį , kad prie paskyros „Tėvų kontrolė“ pasirodytų žalia varnelė . Prie aktyvios paskyros spustelėkite Blokuojamas turinys ir parametrai ir peržiūrėkite šioje paskyroje leistinų tinklalapių sąrašą bei blokuojamus ir leidžiamus tinklalapius.

Apatinėje lango dalyje rasite

Pridėti svetainės išimtį – galima leisti arba uždrausti konkrečią svetainę pagal kiekvienos tėvų paskyros nuostatas atskirai.

Rodyti žurnalus – bus parodytas išsamus tėvų kontrolės veiklos žurnalas (užblokuotus puslapius, paskyrą, kuriai puslapis buvo užblokuotas, kategoriją ir t. t.). Be to, spustelėdami **Filtravimas** galite filtruoti šį žurnalą pagal pasirinktus kriterijus.

Tėvų kontrolė

Išjungus tėvų kontrolę pasirodys langas **Išjungti tėvų kontrolę**. Čia galite nustatyti laiko intervalą, kuriam apsauga bus išjungta. Tada parinktis pasikeičia į **Pristabdyta** arba **Išjungta visam laikui**.

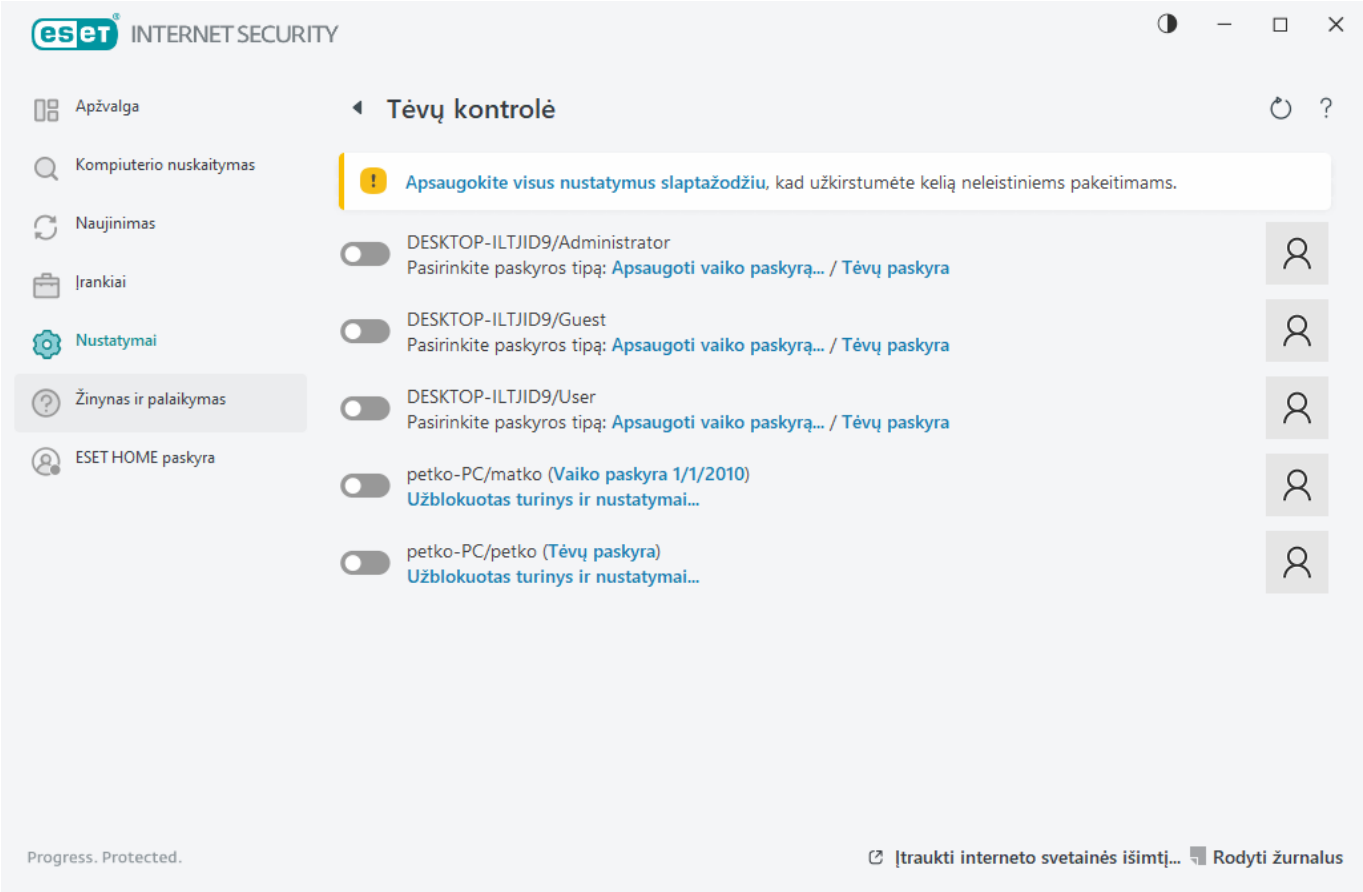
Svarbu apsaugoti ESET Internet Security parametrus slaptažodžiu. Šis slaptažodis gali būti nustatytas dalyje Prieigos nustatymai. Jei nėra nustatytas slaptažodis, pasirodys toliau nurodytas įspėjimas – **Apsaugokite visus parametrus slaptažodžiu**, kad išvengtumėte neleistinų pakeitimų. Ribojimai, nustatyti tėvų kontrolėje, veikia tik

standartines vartotojų paskyras. Kadangi administratorius gali apeiti visus ribojimus, jie neturės jokios įtakos.

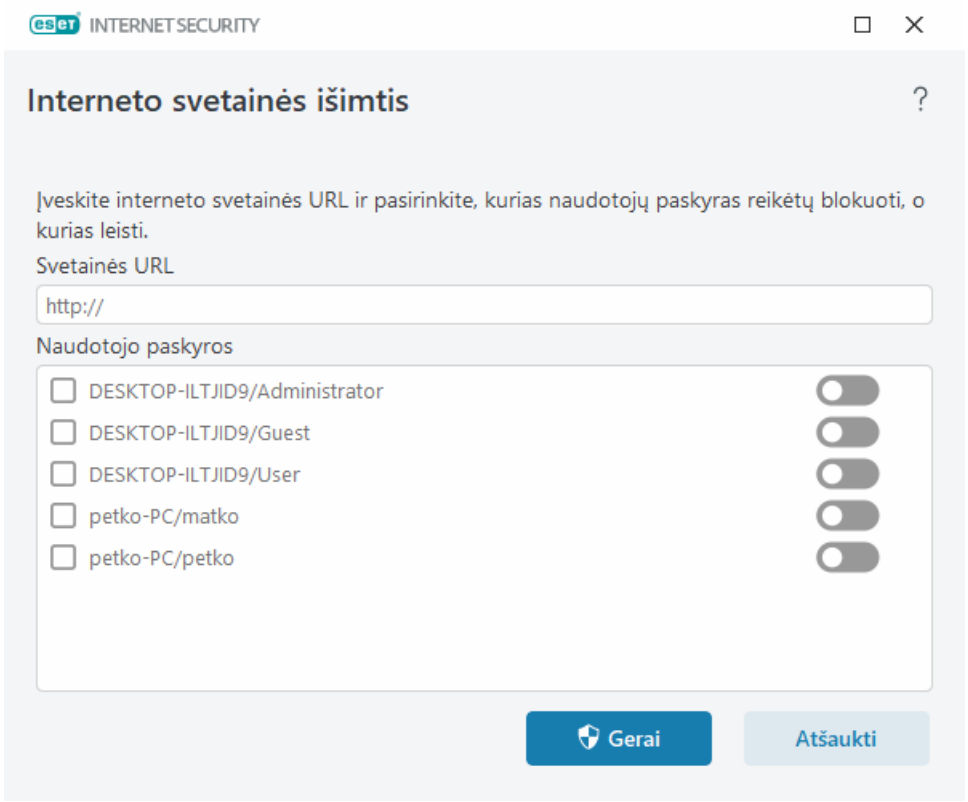
> Tėvų kontrolei reikia, kad tinkamai veiktų tinklo duomenų srauto skaitytuvas, HTTP(S) srauto nuskaitymas ir užkarda. Visos šios funkcijos yra įjungtos pagal numatytuosius nustatymus.

Svetainių išimtys

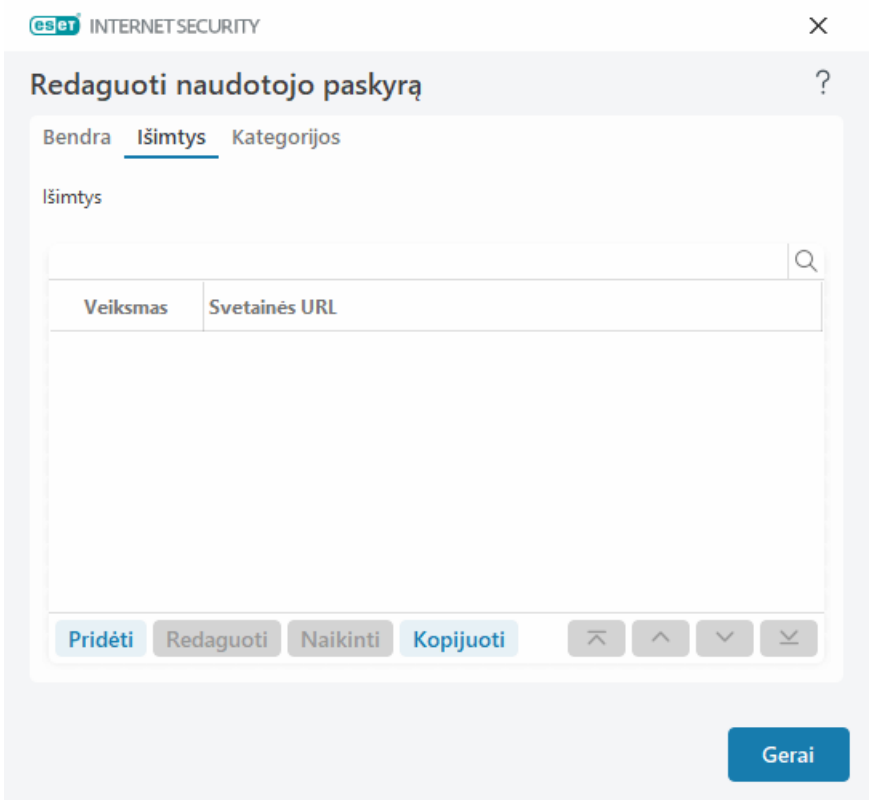
Jei norite pridėti svetainės išimtį, spustelėkite **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė**, tada spustelėkite **Pridėti svetainės išimtį**.



Įveskite URL lauke **Svetainės URL**, pasirinkite (leidžiama) arba (blokuojama) kiekvienai vartotojo paskyrai, tada spustelėkite **Gerai**, kad įtrauktumėte į sąrašą.



Jei iš sąrašo norite panaikinti URL adresą, spustelėkite **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė**, prie reikiamos vartotojo paskyros spustelėkite **Blokuojamas turinys ir parametrai**, spustelėkite skirtuką **Išimtis**, pasirinkite išimtį ir spustelėkite **Pašalinti**.



URL adresų sąraše negalima naudoti specialiųjų simbolių „*“ (žvaigždutės) ir „?“ (klaustuko). Pavyzdžiui, tinklalapio adresai su keletu TLD turi būti įvedami rankiniu būdu (*examplepage.com*, *examplepage.sk* ir t. t.). Kai pridedate prie sąrašo domeną, visas šio domeno ir visų padomenių turinys (pvz., *sub.examplepage.com*) bus blokuojamas arba leidžiamas, atsižvelgiant į jūsų pasirinktą veiksmą pagal URL.

Blokuoti arba leisti konkrečius tinklalapius gali būti tiksliau, nei blokuoti arba leisti tinklalapių kategoriją. Būkite atsargūs keisdami šiuos parametrus ir įtraukdami kategoriją / tinklalapį į sąrašą.

Kopijuoti išimtį iš naudotojo

Išskleidžiamajame meniu, iš kurio norite kopijuoti sukurtą išimtį, pasirinkite vartotoją.

Kopijuoti kategorijas iš paskyros

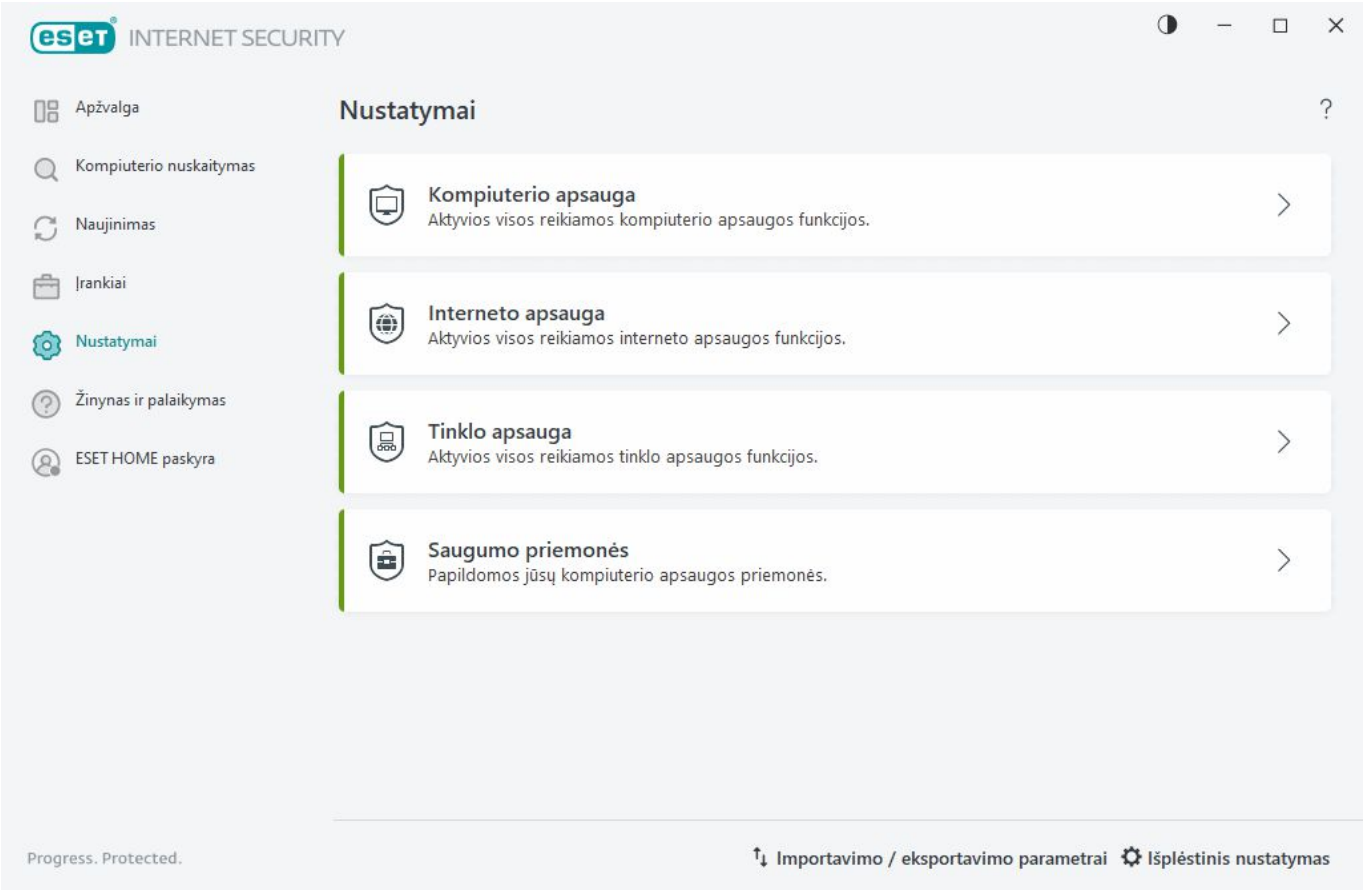
Leidžia kopijuoti užblokuotų arba leidžiamų kategorijų sąrašą iš esamos pakeistos paskyros.

Tinklo apsauga

Atidarykite pagrindinį programos langą > **Nustatymai** > **Tinklo apsauga**, kad sukonfigūruotumėte pagrindinius tinklo apsaugos nustatymus arba pašalintumėte tinklo ryšio triktis.

Norėdami pristabdyti arba išjungti atskirus apsaugos modulius, spustelėkite perjungiklio piktogramą .

Išjungus apsaugos modulius gali sumažėti jūsų kompiuterio apsaugos lygis.



Spustelėkite krumpliaračio piktogramą šalia apsaugos modulio, kad pereitumėte prie išplėstinių šio modulio parametrų.

Užkarda – filtruoja visus tinklo ryšius pagal ESET Internet Security konfigūraciją.

Konfigūruoti – atveria langą Užkardos išplėstinis nustatymas, kuriame galima apibrėžti, kaip užkarda tvarkys tinklo ryšį.

Pristabdyti užkardą (leisti visus duomenų srautus) – Pasirinkus visos užkardos filtravimo parinktys bus išjungtos ir visi gaunami ir siunčiami ryšiai bus leidžiami. Spustelėkite **Įjungti užkardą**, kad vėl įjungtumėte užkardą, kol veikia šis tinklo srauto filtravimo režimas.

Blokuoti visą srautą – užkarda užblokuos visus gaunamus ir siunčiamus ryšius. Naudokite šią parinktį tik tada, jei įtariate kritinį saugumo pavojų, dėl kurio sistemą būtina atjungti nuo tinklo. Kai tinklo srauto filtravimo funkcija veikia režimu **Blokuoti visą srautą**, spustelėkite **Stabdyti visų duomenų srautų blokavimą**, kad atkurtumėte įprastą užkardos veikimą.

Automatinis režimas – (kai įjungtas kitas filtravimo režimas) – spustelėkite norėdami pakeisti filtravimo režimą į automatinį (su vartotojo apibrėžtomis taisyklėmis).

Interaktyvusis režimas – (kai įjungtas kitas filtravimo režimas) – spustelėkite norėdami pakeisti filtravimo režimą į interaktyvųjį.

Apsauga nuo atakos iš tinklo (IDS) – analizuoja tinklo duomenų srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas visas duomenų srautas, kuri laikomas žalingu. ESET Internet Security informuos jus, kai prisijungsite prie neapsaugoto belaidžio tinklo arba silpnai apsaugoto tinklo.

Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą – sistemoje greitai ir tiksliai aptinka kenkimo programinę įrangą.

Tinklo ryšiai – pateikiami tinklai, prie kurių prisijungę tinklo adapteriai ir išsami informacija apie juos.

Užblokuoto ryšio problemos sprendimas – padeda išspręsti jungiamumo problemas, kurias sukelia ESET užkarda. Išsamesnės informacijos skaitykite čia: Trikčių šalinimo vediklis.

Laikinai užblokuotų IP adresų problemos sprendimas – Peržiūrėti sąrašą IP adresų, kurie buvo aptikti kaip atakų šaltiniai ir pridėti prie juodojo sąrašo, kad tam tikrą laiką būtų blokuojamas prisijungimas.

Rodyti žurnalus – atidaromas tinklo apsaugos Žurnalo failas.

Tinklo ryšiai

Pateikiami tinklai, prie kurių prisijungę tinklo adapteriai. Norėdami pamatyti tinklo ryšius, atidarykite pagrindinį programos langą > **Nustatymai** > **Tinklo apsauga** > **Tinklo ryšiai**.

Dukart spustelėkite ant ryšio įtraukto į sąrašą, kad būtų rodoma išsami informacija apie jį ir Tinklo adapterį.

Užveskite pelės žymeklį virš konkretaus tinklo ryšio ir spustelėkite meniu piktogramą ⋮ stulpelyje **Patikima**, kad pasirinktumėte vieną iš šių parinkčių:

- **Redaguoti** – atidaromas langas Konfigūruoti tinklo apsauga, kuriame galite priskirti tinklo apsaugos profilį konkrečiam tinklui
- **Pamiršti** – iš naujo nustatoma numatytoji tinklo ryšio konfigūracija
- **Nuskaityti tinklą naudojant tinklo tikrinimo įrankį** – atidaro tinklo tikrinimo įrankį, kad būtų galima

nuskaityti tinklą

• **Žymėti kaip „Mano tinklas“** – prie tinklo prideda žymą „Mano tinklas“; ši žyma bus rodoma šalia tinklo visame ESET Internet Security, kad būtų galima geriau nustatyti ir peržiūrėti saugą

• **Panaikinti žymėjimą „Mano tinklas“** – pašalina žymę „Mano tinklas“; leidžiama tik tuo atveju, jei tinklas jau pažymėtas

Išsami tinklo ryšio informacija

Dukart spustelėkite ant ryšio nurodyto Tinklo ryšių sąraše, kad būtų pateikiama išsami informacija apie tinklo ryšius ir adapterį. Išsami informacija apie tinklo ryšį ir adapterį gali padėti nustatyti tinklą, kurį bandote konfigūruoti per Tinklo prieigos apsauga.

Išsami tinklo ryšio informacija:

- Tinklo ryšio būsena
- Pirmojo tinklo aptikimo data ir laikas
- Paskutinis kartas, kai tinklas buvo aktyvus
- Bendras laikas, praleistas prisijungus prie šio tinklo
- Tinklo ryšio profilis
- Tinklo ryšio profilis, apibrėžtas sistemoje „Windows“
- Tinklo apsaugos konfigūracija (ar tinklas patikimas)

Tinklo adapterio informacija:

- Ryšio tipas (laidinis, virtualusis ir kt.)
- Tinklo adapterio pavadinimas
- Adapterio aprašymas
- IP adresas su MAC adresu
- Tinklo IPv4 ir IPv6 adresas su potinkliu
- DNS plėtinys
- DNS serverio IP
- DHCP serverio IP
- Numatytojo šliuzo IP ir MAC adresas
- Adapterio MAC adresas

Tinklo prieigos trikčių šalinimas

Trikčių diagnostikos vedlys padeda išspręsti ryšio problemas, kurias sukelia užkarda. Parinktį **Tinklo prieigos trikčių šalinimas** galite rasti pagrindiniame programos lange > **Nustatymai** > **Tinklo apsauga** > **Užblokuoto ryšio problemos sprendimas**.

Pasirinkite, jei norite rodyti ryšį užblokuotą **vietinėms programoms** arba užblokuotą ryšį iš **nuotolinių įrenginių**.

Išskleidžiamajame meniu pasirinkite laikotarpį, kurį ryšys buvo blokuojamas. Pastaruoju metu užblokuotų ryšių sąraše nurodomas programos ar įrenginio tipas, reputacija bei bendras programų ir įrenginių, kurie buvo užblokuoti per šį laikotarpį, skaičius. Jei reikia išsamesnės informacijos apie užblokuotus ryšius, spustelėkite **Išsami informacija**. Tada reikės atblokuoti programą ar įrenginį, dėl kurio kyla ryšio problemų.

Kai spustelėsite **Atblokuoti**, anksčiau užblokuoti ryšiai taps leidžiami. Jei problemų su programa kils ir toliau arba įrenginys neveiks kaip turėtų, spustelėkite **Kitos taisyklės sukūrimas** ir visi anksčiau šiam įrenginiui užblokuoti ryšiai taps leidžiami. Jei problema išlieka, paleiskite kompiuterį iš naujo.

Spustelėkite **Atidaryti užkardos taisykles**, kad pamatytumėte vedlio sukurtas taisykles. Be to, vedlio sukurtas taisykles galite peržiūrėti ir eidami Išplėstiniai nustatymai > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda** > **Taisyklės** > **Redaguoti**.

> Jei taisyklės sukurti nepavyks, gausite klaidos pranešimą. Spustelėkite **Bandyti dar kartą** ir pakartokite procesą, kad atblokuotumėte ryšį, arba sukurkite kitą taisyklę iš užblokuotų ryšių sąrašo.

Laikinas IP adresų juodasis sąrašas

Norėdami peržiūrėti IP adresus, kurie buvo aptikti kaip atakų šaltiniai ir įtraukti į juodąjį sąrašą, kad kuriam laikui būtų uždraustas ryšys, atidarykite pagrindinį programos langą eikite į **Nustatymai** > **Tinklo apsauga** > **Laikinai užblokuotų IP adresų problemos sprendimas**. Laikinai užblokuoti IP adresai blokuojami 1 valandą.

Stulpeliai

IP adresas – rodo užblokuotą IP adresą.

Blokavimo pagrindas – rodo atakos tipą, kuriam buvo sutrukdyta pasiekti adresą (pavyzdžiui, TCP prievadų nuskaitymo ataka).

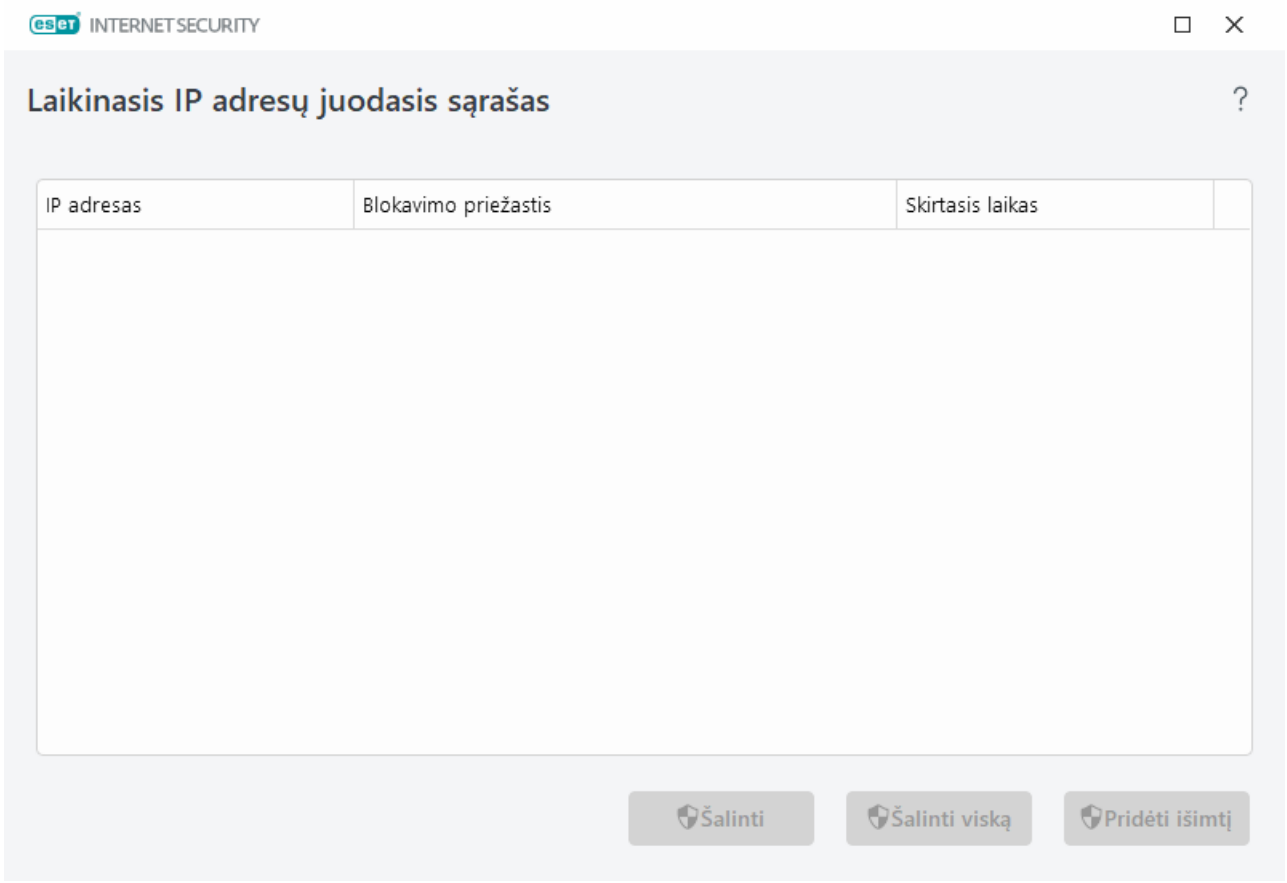
Skirtasis laikas – rodo datą ir laiką, kada adresas bus pašalintas iš juodojo sąrašo.

Valdymo elementai

Šalinti – spustelėkite norėdami pašalinti adresą iš juodojo sąrašo nesibaigus skirtajam laikui.

Šalinti visus – spustelėkite norėdami nedelsiant pašalinti visus adresus iš juodojo sąrašo.

Add exception – spustelėkite norėdami pridėti užkardos išimtį prie IDS filtravimo.



Tinklo apsaugos žurnalai

ESET Internet Security Tinklo apsauga įrašo visus svarbius įvykius į žurnalo failą. Norėdami peržiūrėti žurnalo failą, atidarykite pagrindinį programos langą > **Nustatymai** > **Tinklo apsauga** > **Rodyti žurnalus**.

Žurnalo failus galima naudoti klaidoms aptikti ir įsiskverbimams į jūsų sistemą atskleisti. Tinklo apsaugos žurnaluose yra šie duomenys:

- Įvykio data ir laikas
- Įvykio pavadinimas
- Šaltinis
- Tikslo tinklo adresas
- Tinklo ryšio protokolas
- Taikyta taisyklė arba kirmino pavadinimas, jeigu nustatytas
- Programos kelias ir pavadinimas
- Maiša
- Vartotojas
- Programos pasirašiusysis (leidėjas)

- Paketo pavadinimas
- Paslaugos pavadinimas

Išsami šių duomenų analizė gali padėti aptikti bandymus kėsintis į sistemos saugą. Daugelis kitų faktorių rodo galimą saugos riziką ir leidžia sumažinti jų poveikį: dažni ryšiai iš nežinomų vietų, daug bandymų užmegzti ryšius, nežinomos programos ryšiai arba naudojami neįprasti prievadų numeriai.

> **Saugos pažeidžiamumo išnaudojimas**
> Pranešimas apie saugumo pažeidžiamumą registruojamas net ir tuo atveju, jei konkretus pažeidžiamumas jau pašalintas, nes aptinkamas naudojimo bandymas ir jis blokuojamas tinklo lygmeniu prieš faktiškai naudojant.

Užkardos problemų sprendimas

Jei patiriate jungiamumo problemų, kai įdiegta ESET Internet Security, yra keli būdai nustatyti, ar užkarda yra jų priežastis. Be to, užkarda gali padėti sukurti naujas taisykles ar išimtis jungiamumo problemoms spręsti.

Žr. toliau pateiktas temas, kuriose rasite priemonių, padedančių spręsti užkardos problemas:

- Tinklo prieigos trikčių šalinimas
- Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo
- Išimčių kūrimas iš užkardos pranešimų
- Tinklo apsaugos išplėstinį registravimą
- Tinklo duomenų srauto skaitytuvo problemų sprendimas

Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo

Pagal numatytąją parinktį ESET užkarda neregistruoja visų užblokuotų ryšių. Jei norite pamatyti, ką užblokavo tinklo apsauga, atidarykite Išplėstinis nustatymas > **Įrankiai** > **Diagnostika** > **Išplėstinis prisijungimas** ir įjunkite **Įgalinti tinklo apsaugos išplėstinį prisijungimą**. Jei žurnale pastebėsite ką nors, ko nenorite, kad jūsų užkarda blokuotų, galite sukurti taisyklę arba IDS taisyklę, dešiniuoju pelės klavišu spustelėdami tą elementą ir pasirinkdami **Ateityje neblokuoti panašių įvykių**. Atminkite, kad visų užblokuotų ryšių žurnale gali būti tūkstančiai punktų, tarp kurių bus sunku surasti konkretų ryšį. Išsprendę problemą, galite išjungti registravimo funkciją.

Papildomos informacijos apie žurnalą rasite čia: Žurnalo failai.

> Naudokite registravimo funkciją, kad pamatytumėte tvarką, pagal kurią tinklo apsauga blokuoja konkrečius ryšius. Be to, taisyklių kūrimo iš žurnalo funkcija leis sukurti taisykles, kurios darys tiksliai tai, ko jūs norėsite.

Sukurti taisyklę iš žurnalo

Naujoji ESET Internet Security versija leidžia sukurti taisyklę iš žurnalo. Pagrindiniame meniu spustelėkite **Įrankiai** > **Žurnalo failai**. Išskleidžiamajame meniu pasirinkite **Tinklo apsauga**, dešiniuoju pelės klavišu spustelėkite pageidaujamą žurnalo įrašą ir iš kontekstinio meniu pasirinkite **Ateityje neblokuoti panašių įvykių**. Pranešimo lange bus parodyta jūsų naujoji taisyklė.

Kad būtų galima iš žurnalo sukurti naujas taisykles, ESET Internet Security turi būti sukonfigūruota tokiais parametrais:

1. Nustatykite minimalų registravimo daugiažodiškumo lygį **Diagnostika**, pasirinkdami Išplėstiniai nustatymai > **Įrankiai** > **Žurnalo failai**.

2. Įjungti parinktį **Pranešti apie gaunamas atakas prieš saugumo spragas**, kurią rasite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Apsauga nuo atakos iš tinklo (IDS)** > **Išplėstinės parinktys** > **Įsilaužimo aptikimas**.

Išimčių kūrimas iš užkardos pranešimų

ESET užkardai aptikus kenkimo veiklą tinkle, pateikiamas įvykį apibūdinantis pranešimo langas. Šiame pranešime yra saitas, kurį paspaudus galima sužinoti išsamiau apie įvykį ir pageidaujant nustatyti jam taisyklę.

Jei tinklo programa ar įrenginys tinkamai neįgyvendina tinklo standartų, jis gali sužadinti pasikartojančius užkardos IDS pranešimus. Galite sukurti išimtį tiesiogiai iš pranešimo, kad ESET užkarda nebeaptiktų šios programos ar įrenginio.

Tinklo apsaugos išplėstinį registravimą

Šia funkcija siekiama vesti sudėtingesnius žurnalo failus ESET techninei pagalbai teikti. Šią funkciją naudokite tik to paprašius ESET techninės pagalbos tarnybai, nes ji gali sukurti didžiulį žurnalo failą ir sulėtinti jūsų kompiuterio darbą.

1. Pereikite prie Išplėstinis nustatymai > **Įrankiai** > **Diagnostika** > **Išplėstinis prisijungimas** ir įjunkite **Įjungti tinklo apsaugos išplėstinį registravimą**.

2. Pamėginkite atkurti problemą, su kuria susiduriate.

3. Išjunkite tinklo apsaugos išplėstinį registravimą.

4. Tinklo apsaugos išplėstinio registravimo sukurtą PCAP žurnalo failą rasite tame pačiame aplanke, kuriame generuojamos diagnostinės atminties išklotinės: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Tinklo duomenų srauto skaitytuvo problemų

sprendimas

Jei kyla problemų su naršykle ar el. pašto programa, pirmiausia reikia išsiaiškinti, ar už jas neatsakingas tinklo duomenų srauto skaitytuvo funkcija. Norėdami tai padaryti, pabandykite laikinai išjungti tinklo duomenų srauto skaitytuvą pasirinkę Išplėstinis nustatymas > **Aptikimo modulis** > **Tinklo duomenų srauto skaitytuvas** (nepamirškite jo vėl įjungti, kai baigsite, kitaip jūsų naršyklė ir el. pašto programa liks neapsaugota). Jei išjungus problema dingsta, peržvelkite toliau pateiktą dažniausiai pasitaikančių problemų sąrašą su jų sprendimais:

Naujinimo arba saugaus ryšio problemos

Jei jūsų programa praneša, kad negali atsinaujinti arba ryšio kanalas nesaugus:

- Jei įjungta SSL/TLS funkcija, pabandykite ją laikinai išjungti. Jei tai padeda, galite ir toliau naudoti SSL / TLS funkciją ir leisti veikti naujinimo funkcijai, neįtraukdami probleminių ryšių:
  Išjungti SSL/TLS. Paleiskite naujinimo procesą iš naujo. Turi pasirodyti dialogo langas, informuojantis apie šifruojamą tinklo srautą. Užtikrinkite, kad programa atitiktų tą, kurios triktį šalinate, o sertifikatas būtų atsiunčiamas iš serverio, kuris tiekia jai naujinimus. Tada pasirinkite įsiminti veiksmą su šiuo sertifikatu ir spustelėkite „Nepaisyti“. Jei daugiau nerodoma susijusių dialogo langų, galite perjungti filtravimo režimą atgal į automatinį ir problema turėtų būti išspręsta.

- Jei konkreti programa nėra naršyklė arba el. pašto programa, galite jos visai neįtraukti į Prieigos prie saityno apsauga (jei tai padarysite su naršykle ar el. pašto programa, jūsų kompiuteris taps pažeidžiamas). Visos programos, kurių ryšiai buvo filtruojami praeityje, turi jau būti įtrauktos į jums pateiktą sąrašą, kai buvo pridedama išimtis, tad rankiniu būdu jų įtraukti turbūt nereikės.

Jūsų tinkle veikiančio įrenginio pasiekimo problema

Jei negalite naudotis savo tinkle esančio įrenginio funkcijomis (pvz., atverti internetinės kameros tinklalapį ar leisti vaizdo įrašą namų medijos leistuvu), pamėginkite pridėti jo IPv4 ir IPv6 adresus į neįtrauktų adresų sąrašą.

Problemos su konkrečia interneto svetaine

Galite išskirti konkrečioms svetainėms prieigos prie saityno apsaugą naudodami URL adresų valdymą. Pavyzdžiui, jei negalite pasiekti https://www.gmail.com/intl/en/mail/help/about.html, pamėginkite pridėti *gmail.com* į neįtrauktų adresų sąrašą.

Klaida „Vis dar vykdomos kai kurios programos, galinčios importuoti šakninį sertifikatą“

Jums įjungus SSL/TLS, ESET Internet Security pasirūpina, kad įdiegtos programos pasikliautų būdu, kuriuo ji filtruoja SSL protokolą, importuodama sertifikatą į jų sertifikatų saugyklą. Kai kurias programas gali reikėti paleisti iš naujo, kad būtų importuotas sertifikatas. Tai taikoma „Firefox“ ir „Opera“. Įsitikinkite, kad nė viena iš jų neveikia (geriausias būdas tai padaryti – atverti užduočių tvarkytuvą ir patikrinti, ar jo kortelėje „Procesai“ nėra veikiančių failų „firefox.exe“ arba „opera.exe“), tada spustelėkite „Kartoti“.

Nepatikimo leidėjo arba negaliojančio sertifikato klaida

Tai dažniausiai reiškia, kad įvyko pirmiau nurodyto aprašyto importo proceso triktis. Pirmiausia įsitikinkite, kad neveikia nė viena iš paminėtų programų. Tada išjunkite SSL/TLS ir vėl įjunkite. Taip pakartotinai įvykdysite importo

procedūrą.

Žr. žinių bazės straipsnius, kad sužinotumėte Kaip valdyti tinklo duomenų srauto skaitytuvą ESET „Windows“ pagrindiniame produkte.

Užblokuota tinklo grėsmė

Taip gali nutikti, kai kompiuteryje įdiegta programa bando perduoti kenkimo duomenis į kitą tinklo įrenginį, panaudojamos saugumo spragos arba net kai sistemoje aptinkamas bandymas nuskaityti prievadus.

Pranešime galite rasti grėsmės tipą ir susijusio įrenginio IP adresą. Spustelėkite **Keisti šios grėsmės valdymą**, kad būtų rodomos šios parinktys:

Tęsti blokavimą – užblokuoja aptiktą grėsmę. Jei nebenorite gauti pranešimų apie tokio tipo grėsmę iš konkretaus nuotolinio adreso, pasirinkite išrinkimo mygtuką šalia **Nepranešti** prieš spustelėdami **Tęsti blokavimą**. Taip bus sukurta įsibrovimo aptikimo tarnybos (IDS) taisyklė su tokia konfigūracija: **Blokuoti** – numatytoji, **Pranešti** – ne, **Žurnalas** – ne.

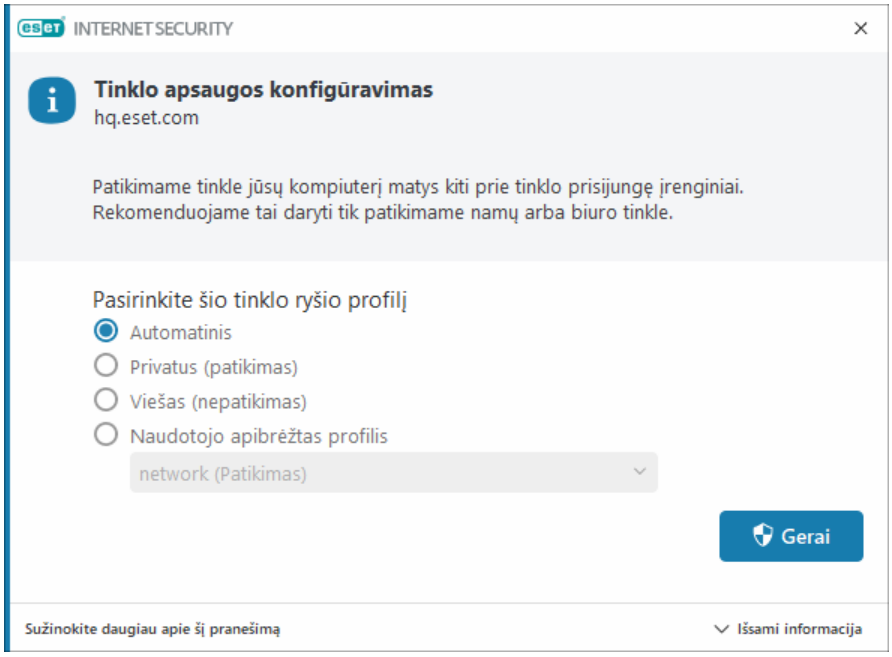
Leisti – sukuria įsibrovimo aptikimo tarnybos (IDS) taisyklę, leidžiančią aptiktą grėsmę. Pasirinkite vieną iš šių parinkčių prieš spustelėdami **Leisti**, kad nurodytumėte taisyklės nustatymus:

- **Pranešti tik kai grėsmė užblokuojama** – taisyklės konfigūracija: **Blokuoti** – ne, **Pranešti** – ne, **Žurnalas** – ne.
- **Pranešti kaskart nustačius šią grėsmę** – taisyklės konfigūracija: **Blokuoti** – ne, **Pranešti** – numatytoji, **Žurnalas** – numatytoji.
- **Nepranešti** – taisyklės konfigūracija: **Blokuoti** – ne, **Pranešti** – ne, **Žurnalas** – ne.

Pranešimo lange pateikiama informacija priklauso nuo aptiktos grėsmės tipo.
Daugiau informacijos apie grėsmes ir kitas susijusias sąvokas rasite skyriuose Nuotolinių atakų tipai arba Aptikimų tipai.
Norėdami išspręsti **Tinkle yra IP adresų dublikatų** įvykį, žr. ESET žinių bazės straipsnį.

Aptiktas naujas tinklas

Pagal numatytuosius nustatymus, ESET Internet Security naudoja „Windows“ nustatymus, kai aptinkamas naujas tinklas. Norėdami, kad aptikus naują tinklą būtų rodomas dialogo langas, pakeiskite Tinklo apsaugos profilio priskyrimas į **Klausti**. Tinklo apsauga konfigūruojama visada, kai jūsų kompiuteris jungiasi prie naujo tinklo.



Galite pasirinkti iš šių tinklo ryšio profilių:

Automatinis – ESET Internet Security profilį parinks automatiškai, pagal kiekvienam profiliui sukonfigūruotus aktyvatorius.

Asmeninis – patikimam tinklui (namų arba biuro tinklui). Kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuteryje saugomus failus bei pasiekti sistemos išteklius (suteikta prieiga prie bendrinamų failų ir spausdintuvų, gaunamas RPC ryšys yra įgalintas ir leidžiama bendrinti nuotolinį darbalaukį). Rekomenduojame naudoti šį parametrą jungiantis prie saugaus vietinio tinklo. Šis profilis automatiškai priskiriamas tinklo ryšiui, jei jis sukonfigūruotas kaip domenas arba privatus tinklas Windows.

Viešasis – nepatikimam tinklui (viešajam tinklui). Failai ir aplankai jūsų sistemoje nėra bendrinami su kitais tinklo vartotojais arba nematomi kitiems vartotojams, o sistemos išteklių bendrinimas išjungiamas. Rekomenduojame naudoti šį parametrą, kai naudojatės belaidžiais tinklais. Šis profilis automatiškai priskiriamas bet kokiam tinklo ryšiui, kuris nesukonfigūruotas kaip domenas arba privatus tinklas Windows.

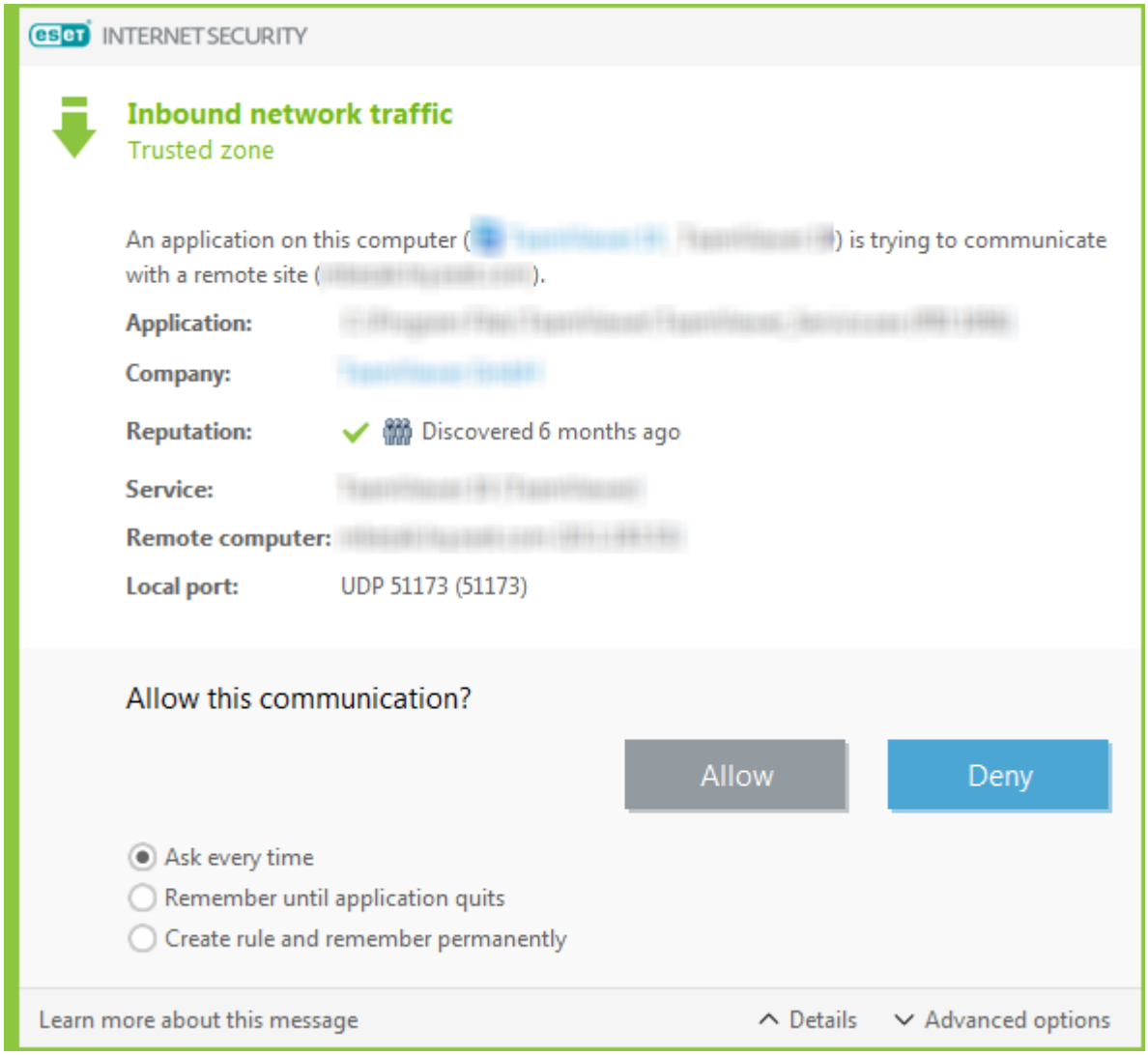
Naudotojo apibrėžtas profilis – išplečiamajame meniu galite pasirinkti vieną iš jūsų sukurtų profilių. Ši parinktis galima tik tuo atveju, jei sukūrėte bent vieną pasirinktinį profilį.

⚠ Neteisingai sukonfigūravus tinklą jūsų kompiuterio saugai gali iškilti grėsmė.

Ryšio nustatymas – aptikimas

Užkarda aptinka kiekvieną naujai sukurtą tinklo ryšį. Aktyvusis užkardos režimas nustato, kokie veiksmai atliekami pagal naują taisyklę. Jei aktyvinamas **Automatinis režimas** arba **Politika pagrįstas režimas**, užkarda atliks iš anksto nustatytus veiksmus nesikišant vartotojui.

Interaktyvusis režimas rodo informacinį langą, kuriame pranešama apie naujo tinklo ryšio aptikimą ir pateikiama išsami informacija apie šį sujungimą. Galite pasirinkti **leisti** arba **neleisti** (blokuoti) ryšį. Jeigu pakartotinai leisite tą patį ryšį dialogo lange, rekomenduojame sukurti naują taisyklę šiam ryšiui. Tai galite padaryti pasirinkę **Kurti taisyklę ir įsiminti visam laikui** ir įrašę veiksmą kaip naują užkardos taisyklę. Jeigu užkarda vėliau atpažins tą patį ryšį, ji taikys esamą taisyklę be vartotojo veiksmų.



Kurdami naujas taisykles leiskite tik tikrai saugius ryšius. Jei visi ryšiai yra leidžiami, užkarda netenka prasmės. Tai svarbūs ryšių parametrai:

Programa – vykdomojo failo vieta ir proceso ID. Neleiskite nežinomų programų ir procesų ryšių.

Pasirašantis asmuo – programos leidėjo vardas / pavadinimas. Spustelėkite tekstą, kad būtų rodomas įmonės saugos sertifikatas.

Reputacija – ryšio rizikos lygis. Ryšiams priskiriamas rizikos lygis: Geras (žalia), Nežinomas (oranžinė) arba Rizikingas (raudona), naudojant keletą euristinių taisyklių, kuriose nagrinėjamos kiekvieno ryšio savybės, naudotojų skaičius ir atradimo laikas. Šią informaciją renka ESET LiveGrid® technologija.

Paslauga – paslaugos pavadinimas, jei programa yra „Windows“ paslauga.

Nuotolinis kompiuteris – nuotolinio įrenginio adresas. Leiskite ryšius tik su patikimais ir žinomais adresais.

Nuotolinis prievadas – ryšių prievadas. Ryšys su bendraisiais prievadais (pvz., saityno srautas – prievado numeris 80.443) įprastomis aplinkybėmis gali būti leidžiamas.

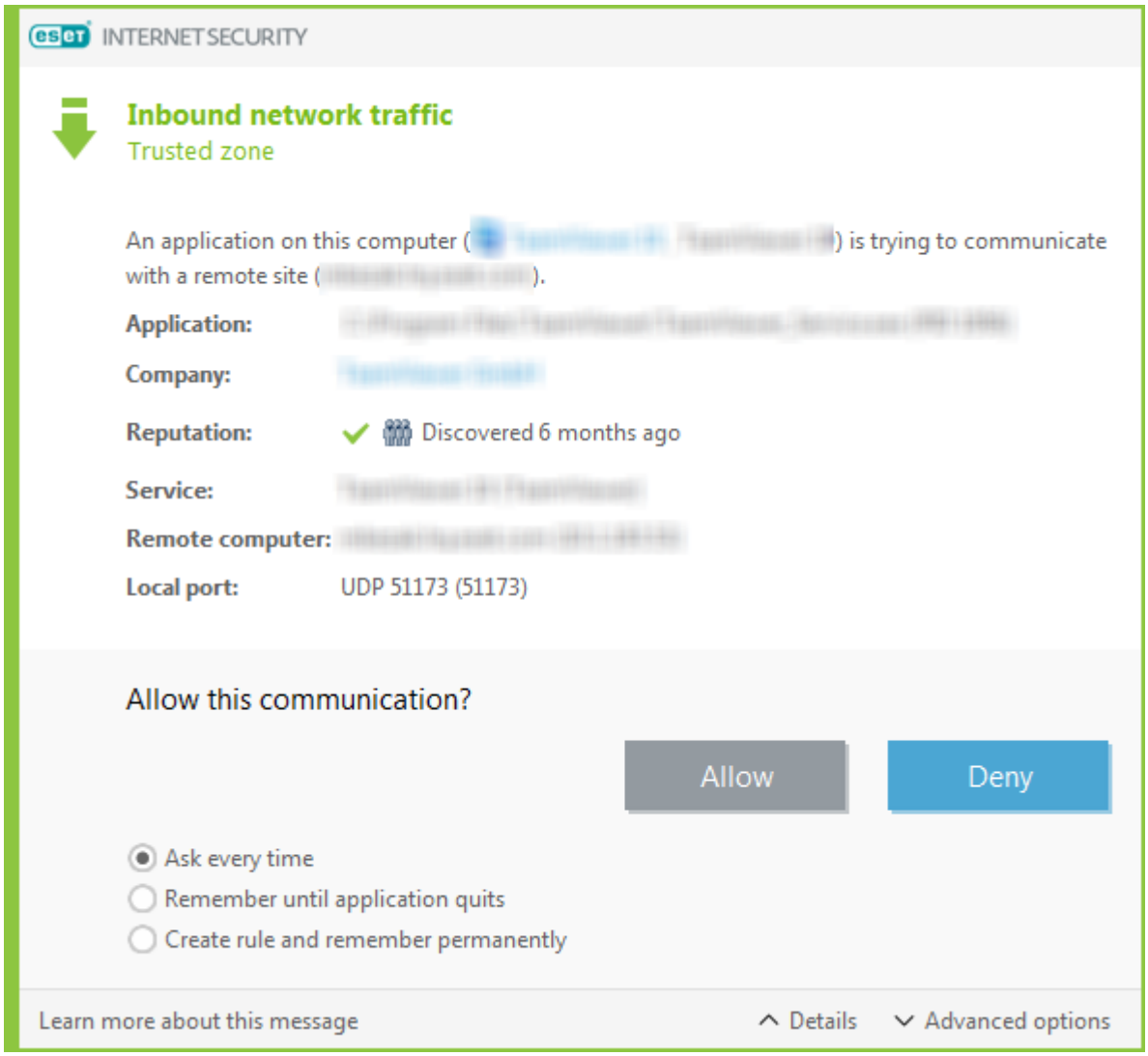
Kompiuterio įsiskverbimai dažnai naudoja internetą ir paslėptus ryšius, kad užkrėstų nuotolines sistemas. Jeigu taisyklės yra tinkamai sukonfigūruotos, užkarda tampa naudingu įrankiu apsisaugant nuo įvairių kenkėjiškų kodų atakų.

Programos keitimas

Užkarda aptiko keitimą taikomojoje programoje, kuri naudojama siunčiamiems ryšiams iš jūsų kompiuterio. Gali būti, kad taikomoji programa paprasčiausiai buvo atnaujinta į naują versiją. Tačiau gali būti, kad modifikavimą atliko kenkėjiška programa. Jeigu neturite informacijos apie kokius nors teisėtus modifikavimus, rekomenduojame uždrausti ryšį ir nuskaityti kompiuterį naudojant naujausią virusų kodų duomenų bazę.

Gaunamas patikimas ryšys

Gaunamo ryšio patikimoje zonoje pavyzdys:
Nuotolinis kompiuteris iš patikimos zonos bando užmegzti ryšį su jūsų kompiuteryje vykdoma vietine taikomąją programa.



Programa – programa, palaikanti ryšį su nuotoliniu įrenginiu.

Programos kelias – programos vieta.

„Microsoft store“ programa – „Microsoft store“ programos pavadinimas.

Pasirašantis asmuo – programos leidėjo pavadinimas. Spustelėkite tekstą, kad būtų rodomas įmonės saugos sertifikatas.

Reputacija – programos reputacija, nustatyta taikant technologiją ESET LiveGrid®.

Tarnyba – šiuo metu kompiuteryje veikianti tarnyba.

Nuotolinis kompiuteris – nuotolinis kompiuteris, bandantis užmegzti ryšį su taikomąja programa jūsų kompiuteryje.

Nuotolinis prievadas – ryšiui naudojamas prievadas.

Kiekvienąkart klausti – jei numatytasis taisyklės veiksmas yra nustatytas kaip **Klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas.

Prisiminti, kol programa baigs darbą – ESET Internet Security įsimins pasirinktą veiksmą iki kito sistemos paleidimo iš naujo.

Kurti taisyklę ir įsiminti visam laikui – jei pasirenkate šią parinktį prieš leisdami arba uždrausdami ryšį, ESET Internet Security įsimins šį veiksmą ir naudos jį, jei nuotolinis kompiuteris vėl bandys prisijungti prie programos.

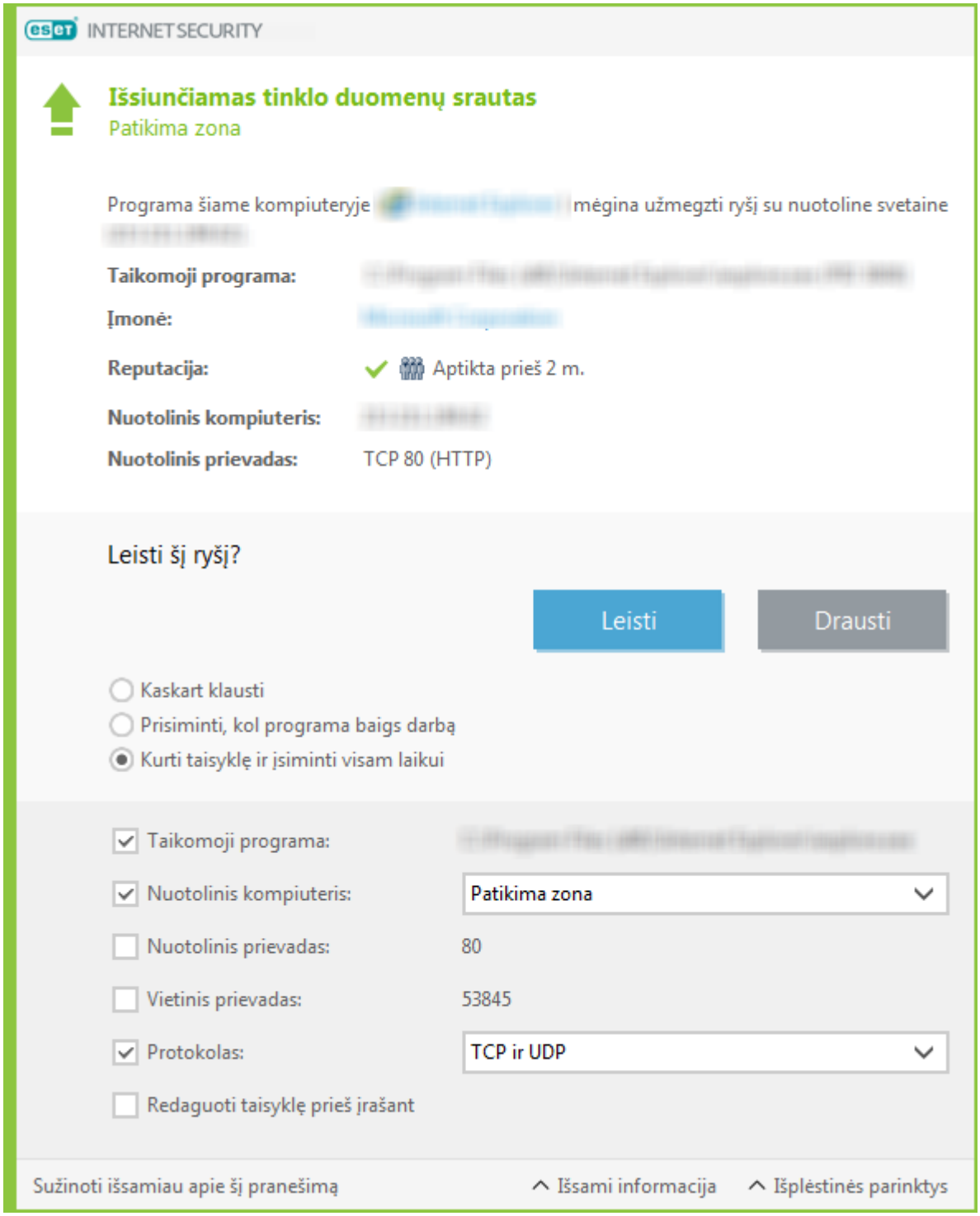
Leisti – leisti gaunamą ryšį.

Uždrausti – drausti gaunamą ryšį.

Redaguoti taisyklę – leidžia tinkinti taisyklės ypatybes naudojant užkardos taisyklių rengyklę.

Siunčiamas patikimas ryšys

Siunčiamo ryšio patikimoje zonoje pavyzdys:
Vietinė taikomoji programa, bandanti užmegzti ryšį su kitu kompiuteriu, esančiu vietiniame tinkle arba tinkle patikimoje zonoje.



Programa – programa, palaikanti ryšį su nuotoliniu įrenginiu.

Programos kelias – programos vieta.

„Microsoft store“ programa – „Microsoft store“ programos pavadinimas.

Pasirašantis asmuo – programos leidėjo pavadinimas. Spustelėkite tekstą, kad būtų rodomas įmonės saugos sertifikatas.

Reputacija – programos reputacija, nustatyta taikant technologiją ESET LiveGrid®.

Tarnyba – šiuo metu kompiuteryje veikianti tarnyba.

Nuotolinis kompiuteris – nuotolinis kompiuteris, bandantis užmegzti ryšį su taikomąja programa jūsų kompiuteryje.

Nuotolinis prievadas – ryšiui naudojamas prievadas.

Kiekvienąkart klausti – jei numatytasis taisyklės veiksmas yra nustatytas kaip **Klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas.

Prisiminti, kol programa baigs darbą – ESET Internet Security įsimins pasirinktą veiksmą iki kito sistemos paleidimo iš naujo.

Kurti taisyklę ir įsiminti visam laikui – jei pasirenkate šią parinktį prieš leisdami arba uždrausdami ryšį, ESET Internet Security įsimins šį veiksmą ir naudos jį, jei nuotolinis kompiuteris vėl bandys prisijungti prie programos.

Leisti – leisti gaunamą ryšį.

Uždrausti – drausti gaunamą ryšį.

Redaguoti taisyklę – leidžia tinkinti taisyklės ypatybes naudojant užkardos taisyklių rengyklę.

Gaunamas ryšys

Gaunamo interneto ryšio pavyzdys:
Nuotolinis kompiuteris, bandantis palaikyti ryšį su kompiuteryje veikiančia taikomąja programa.

Programa – programa, palaikanti ryšį su nuotoliniu įrenginiu.

Programos kelias – programos vieta.

„Microsoft store“ programa – „Microsoft store“ programos pavadinimas.

Pasirašantis asmuo – programos leidėjo pavadinimas. Spustelėkite tekstą, kad būtų rodomas įmonės saugos sertifikatas.

Reputacija – programos reputacija, nustatyta taikant technologiją ESET LiveGrid®.

Tarnyba – šiuo metu kompiuteryje veikianti tarnyba.

Nuotolinis kompiuteris – nuotolinis kompiuteris, bandantis užmegzti ryšį su taikomąja programa jūsų kompiuteryje.

Nuotolinis prievadas – ryšiui naudojamas prievadas.

Kiekvienąkart klausti – jei numatytasis taisyklės veiksmas yra nustatytas kaip **Klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas.

Prisiminti, kol programa baigs darbą – ESET Internet Security įsimins pasirinktą veiksmą iki kito sistemos paleidimo iš naujo.

Kurti taisyklę ir įsiminti visam laikui – jei pasirenkate šią parinktį prieš leisdami arba uždrausdami ryšį, ESET Internet Security įsimins šį veiksmą ir naudos jį, jei nuotolinis kompiuteris vėl bandys prisijungti prie programos.

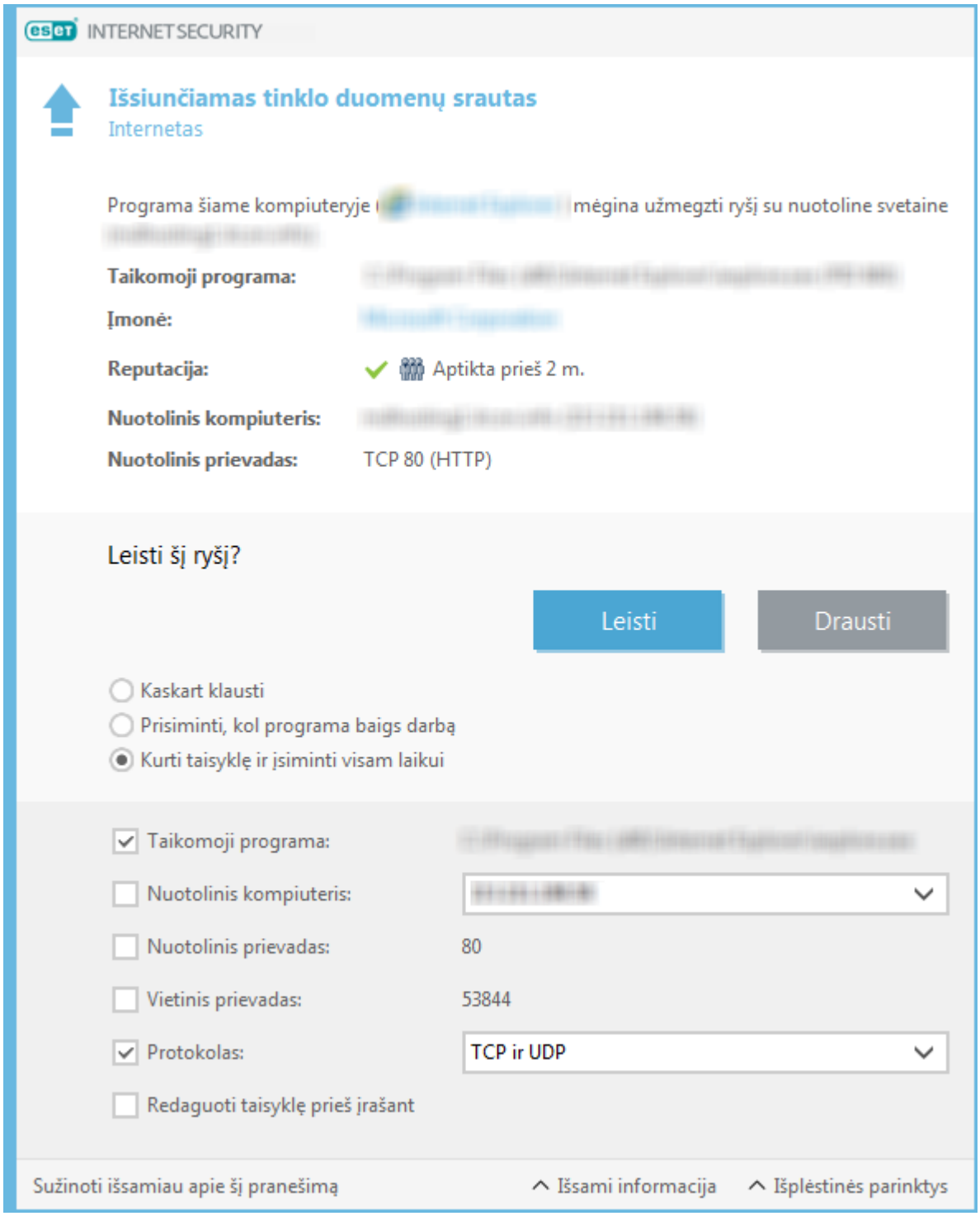
Leisti – leisti gaunamą ryšį.

Uždrausti – drausti gaunamą ryšį.

Redaguoti taisyklę – leidžia tinkinti taisyklės ypatybes naudojant užkardos taisyklių rengyklę.

Siunčiamas ryšys

Siunčiamo interneto ryšio pavyzdys:
Vietinė taikomoji programa bando užmegzti interneto ryšį.



Programa – programa, palaikanti ryšį su nuotoliniu įrenginiu.

Programos kelias – programos vieta.

„Microsoft store“ programa – „Microsoft store“ programos pavadinimas.

Pasirašantis asmuo – programos leidėjo pavadinimas. Spustelėkite tekstą, kad būtų rodomas įmonės saugos sertifikatas.

Reputacija – programos reputacija, nustatyta taikant technologiją ESET LiveGrid®.

Tarnyba – šiuo metu kompiuteryje veikianti tarnyba.

Nuotolinis kompiuteris – nuotolinis kompiuteris, bandantis užmegzti ryšį su taikomąja programa jūsų kompiuteryje.

Nuotolinis prievadas – ryšiui naudojamas prievadas.

Kiekvienąkart klausti – jei numatytasis taisyklės veiksmas yra nustatytas kaip **Klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas.

Prisiminti, kol programa baigs darbą – ESET Internet Security įsimins pasirinktą veiksmą iki kito sistemos paleidimo iš naujo.

Kurti taisyklę ir įsiminti visam laikui – jei pasirenkate šią parinktį prieš leisdami arba uždrausdami ryšį, ESET Internet Security įsimins šį veiksmą ir naudos jį, jei nuotolinis kompiuteris vėl bandys prisijungti prie programos.

Leisti – leisti gaunamą ryšį.

Uždrausti – drausti gaunamą ryšį.

Redaguoti taisyklę – leidžia tinkinti taisyklės ypatybes naudojant užkardos taisyklių rengyklę.

Ryšio rodinio nustatymas

Spustelėkite dešiniuoju pelės klavišu ryšį, norėdami matyti papildomas parinktis:

Pasirinkti pagrindinio kompiuterio pavadinimus – jeigu įmanoma, visi tinklo adresai rodomi DNS formatu, o ne skaitiniu IP adreso formatu.

Rodyti tik TCP ryšius – sąraše rodomi tik tie ryšiai, kurie priklauso TCP protokolo programų paketui.

Rodyti klausomus ryšius – nurodžius šią parinktį, pateikiami tik tie ryšiai, kuriems ryšys šiuo metu nėra užmegztas, tačiau sistema yra atidariusi prievadą ir laukia ryšio.

Rodyti ryšius kompiuteryje – nurodykite šią parinktį, kad būtų rodomi tik tie ryšiai, kurių nuotolinė pusė yra vietinė sistema – vadinamieji localhost kompiuterio ryšiai.

Atnaujinti greitį – pasirinkite, kokiu dažnumu atnaujinti aktyvius ryšius.

Atnaujinti dabar – iš naujo įkelia **Tinklo ryšių** langą.

Saugumo priemonės

Atidarykite pagrindinį programos langą > **Nustatymai** > **Saugumo priemonės**, kad sureguliuotumėte šiuos modulius:

Saugi bankininkystė ir naršymas – tai papildomas naršyklės apsaugos lygis, skirtas finansiniams duomenims apsaugoti, kai atliekate operacijas internetu. Įgalinkite parinktį **Apsaugoti visas naršykles** skiltyje Saugios bankininkystės ir naršymo išplėstinis nustatymas, kad paleistumėte visas palaikomas saityno naršykles saugiuoju režimu.

Naršyklės privatumas ir sauga – išlaiko jūsų veiklą internete privačią ir saugią nepaliekant skaitmeninio pėdsako.

„Anti-Theft“ – įjunkite Anti-Theft, kad apsaugotumėte pamestą arba pavogtą kompiuterį.

Saugi bankininkystė ir naršymas

Saugi bankininkystė ir naršymas – tai papildomas apsaugos lygis, skirtas finansiniams duomenims apsaugoti, kai atliekate operacijas internetu.

Pagal numatytuosius nustatymus, visos palaikomos interneto naršyklės paleidžiamos saugiuoju režimu. Tai leidžia naršyti internete, naudotis internetine bankininkyste ir pirkti bei atlikti operacijas internetu viename apsaugotos naršyklės lange automatiškai.

„ESET LiveGrid®“ reputacijos sistema turi būti įgalinta (įgalinta pagal numatytuosius nustatymus), siekiant užtikrinti, kad saugi bankininkystė ir naršymas veiktų tinkamai.

Norėdami sukonfigūruoti apsaugotos naršyklės veikimą, žr. Saugios bankininkystės ir naršymo išplėstinis nustatymas. Jei išjungsite **Apsaugoti visas naršykles**, apsaugotą naršyklę galėsite pasiekti pagrindiniame programos lange > **Apžvalga** > **Saugi bankininkystė ir naršymas** arba spustelėdami darbalaukio piktogramą **Saugi bankininkystė ir naršymas**. Windows numatytoji naršyklė paleidžiama saugiuoju režimu.

HTTPS šifruotasis ryšys yra būtina apsaugoto naršymo sąlyga. Saugią bankininkystę ir naršymą palaiko šios naršyklės:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Tik Firefox ir Microsoft Edge yra palaikomos įrenginiuose su ARM procesoriais.

Norėdami gauti daugiau informacijos apie saugios bankininkystės ir naršymo funkcijas, perskaitykite toliau nurodytus ESET žinių bazės straipsnius anglų ir kai kuriomis kitomis kalbomis:

- Kaip naudotis ESET saugia bankininkyste ir naršymu?
- Saugios bankininkystės ir naršymo pristabdymas arba išjungimas ESET „Windows“ namų produktuose

- ESET saugi bankininkystė ir naršymas – dažnos klaidos
- ESET žodynėlis | Saugi bankininkystė ir naršymas

Naršyklės pranešimas

Apsaugota naršyklė informuoja apie dabartinę būseną naršyklės pranešimu ir naršyklės rėmelio spalva.

Naršyklės pranešimai rodomi dešinėje pusėje esančiame skirtuke.

Norėdami išplėsti pranešimą naršyklėje, spustelėkite ESET piktogramą . Norėdami sumažinti pranešimą, spustelėkite pranešimo tekstą. Norėdami atmesti pranešimą ir žalią naršyklės rėmelį, spustelėkite uždarymo piktogramą .

Galima atmesti tik informacinį pranešimą ir žalią naršyklės rėmelį.

Naršyklės pranešimai

Pranešimo tipas	Būsena
Informacinis pranešimas ir žalia naršyklės rėmelis	Užtikrinama maksimali apsauga ir pagal numatytuosius nustatymus sumažinamas naršyklės pranešimas. Išplėskite pranešimą naršyklėje ir spustelėkite **Nustatymai**, kad atidarytumėte saugos įrankių sąranką.
Įspėjimas ir oranžinis naršyklės rėmelis	Apsaugota naršyklė reikalauja jūsų dėmesio dėl nekritinės problemos. Norėdami gauti daugiau informacijos apie problemą ar sprendimą, vadovaukitės naršyklės pranešime pateiktomis instrukcijomis.
Saugos įspėjimas ir raudonas naršyklės rėmelis	Naršyklė nėra apsaugota naudojant ESET saugią bankininkystę ir naršymą. Paleiskite naršyklę iš naujo, kad įsitikintumėte, jog apsauga yra aktyvi. Norėdami išspręsti konfliktą su į naršyklę įkeltais failais, atidarykite Žurnalo failai > **Saugi bankininkystė ir naršymas** ir įsitikinkite, kad užregistruoti failai nebus įkelti, kai kitą kartą paleisite naršyklę. Jei problema išlieka, kreipkitės į ESET techninę pagalbą vadovaudamiesi mūsų žinių bazės straipsnyje pateiktomis instrukcijomis.

Naršyklės privatumas ir sauga

Naršyklės privatumo ir saugos funkciją galite įgalinti naudodami pasirinktinį plėtinį, pasiekiamą palaikomose naršyklėse (tik „Google Chrome“, „Mozilla Firefox“ ir „Microsoft Edge“).

Norėdami įdiegti ir įgalinti plėtinį:

1. Įsitikinkite, kad naudojate naujausią „ESET Internet Security“ versiją ir po atnaujinimo sėkmingai iš naujo paleiskite kompiuterį.
2. Atidarykite naršyklę.
3. Plėtinys yra įdiegtas jūsų naršyklėje.

4. Įgalinkite plėtinį, kad būtų parodytas naršyklės puslapis su plėtinio informacija.

Pagrindinis naršyklės privatumo ir saugos plėtinio meniu suskirstytas į šias skiltis:

Apžvalga

Saugi paieška

Spustelėkite perjungimo piktogramą  šalia parinkties **Nuskaityti paieškos rezultatus**, kad įgalintumėte funkciją ir pamatytumėte, kuriuos rezultatus saugu spustelėti. Saugi paieška įvertins išvardytų nuorodų adresus, tačiau tai nebūtinai reikš, kad svetainėje nėra kenkėjiškos programinės įrangos. Tada mūsų aptikimo modulis aptiks bet kokią svetainėje esančią kenkėjišką programinę įrangą.

Naršyklės valymas

Ištrinkite naršymo duomenis arba nustatykite reguliarius valymus. Galite pridėti svetaines, kuriose norite priimti slapukus ir likti prisijungę net ir atlikę naršyklės valymą, **įtraukdami jas į sąrašą**.

- **Vienkartinis valymas –**išplečiamajame meniu pasirinkite laiko intervalą ir duomenų tipą, kurį norite ištrinti. Galite rinktis iš parinkčių „Visi duomenys“, „Privatūs duomenys“ ir „Pasirinktiniai duomenys“.

- **Reguliarus valymas** – spustelėkite perjungimo piktogramą  šalia parinkties **Reguliarus valymas**, kad įgalintumėte funkciją. Išskleidžiamajame meniu pasirinkite laiko intervalą ir duomenų tipą, kurį norite reguliariai ištrinti. Galite rinktis iš parinkčių „Visi duomenys“, „Privatūs duomenys“ ir „Pasirinktiniai duomenys“.

Pasirinktinių duomenų parinktyje yra šios kategorijos:

- Naršymo istorija
- Atsisiuntimų istorija
- Slapukai ir svetainių duomenys
- Talpykloje laikomi vaizdai ir failai
- Slaptažodžiai ir prisijungimo duomenys
- Formų automatinio pildymo duomenys

Svetainės nustatymų peržiūra

Lengvai pasiekite ir tvarkykite svetainės leidimus, kad galėtumėte valdyti, kokią informaciją gali naudoti svetainės.

- **Pranešimai** – peržiūrėkite, kuriose svetainėse norite **leisti / blokuoti** pranešimus arba norite, kad naršyklės plėtinys **kaskart jūsų paklaustų**.

išplėstinis nustatymas

Naršyklės valymas

Išplėstiniai slapukų nustatymai

Svetainių, kuriose norite priimti slapukus ir likti prisijungę net ir atlikę naršyklės valymą, sąrašas. Teksto lauke įveskite URL adresą ir spustelėkite **Pridėti**. Galite bet kada pašalinti jį iš sąrašo spustelėdami minuso piktogramą  šalia konkrečios svetainės.

Puslapio apačioje yra siūlomų domenų, šiuo metu atidarytų naršyklėje, sąrašas. Jei nematote konkrečios svetainės, spustelėkite **Atnaujinti sąrašą** ir pridėkite jį prie priimtinų slapukų sąrašo spustelėdami pliuso piktogramą  .

Svetainės nustatymų peržiūra

Lengvai pasiekite ir tvarkykite svetainės leidimus, kad galėtumėte valdyti, kokią informaciją gali naudoti svetainės.

- **Pranešimai** – peržiūrėkite, kuriose svetainėse norite **leisti / blokuoti** pranešimus arba norite, kad naršyklės plėtinys **kaskart jūsų paklaustų**.

Išvaizda

Tinkinkite sąsajos spalvų schemą, kad ji atitiktų jūsų pageidavimus. Galite pasirinkti pageidaujamą spalvų schemą pažymėdami žymės langelį **Šviesus** arba **Tamsus**.

Anti-Theft

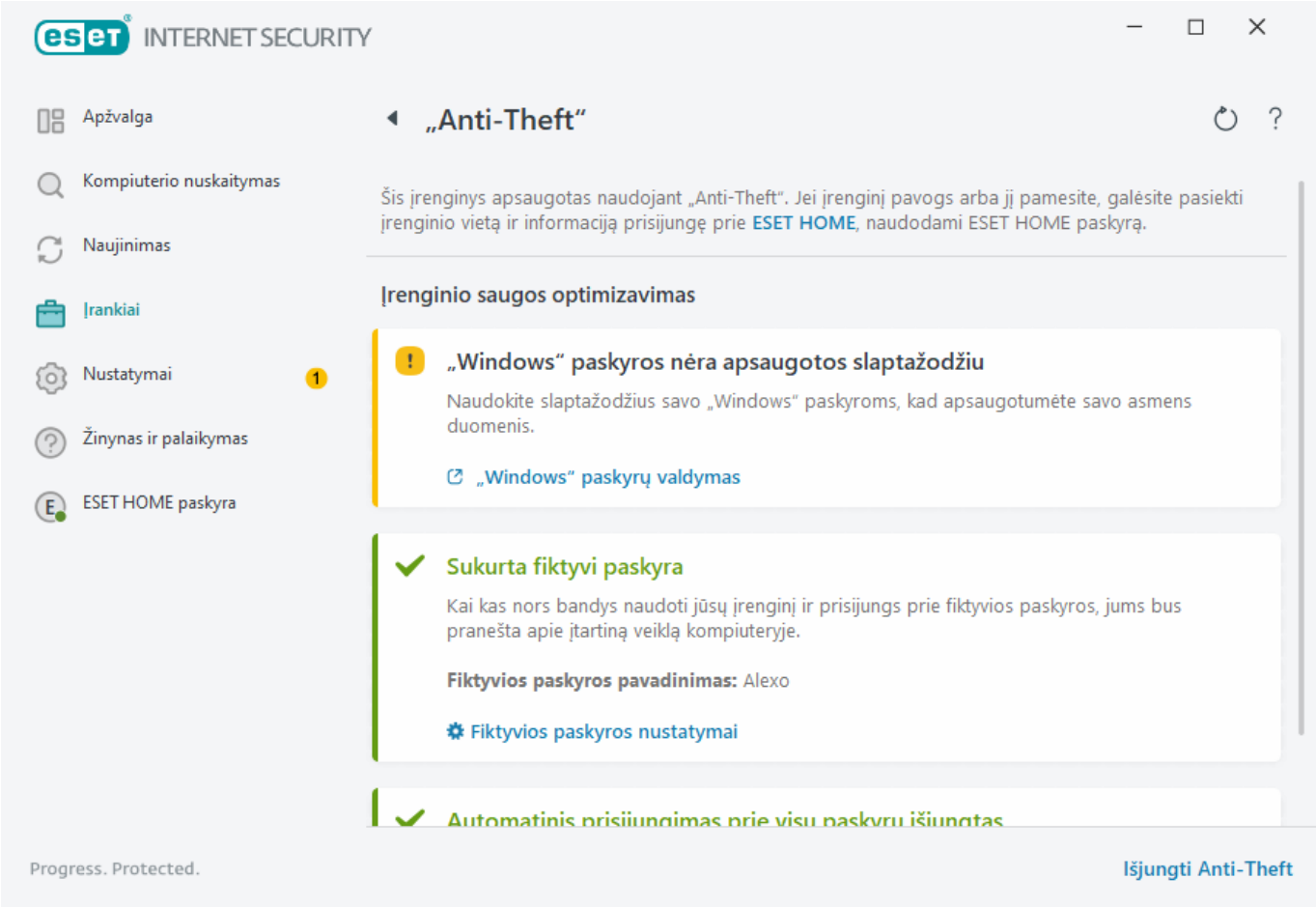
Kasdien iš namų vykstant į darbą ar kitose viešose vietose nuolat kyla pavojus, kad savo asmeninius įrenginius pamesite arba juos pavogs. Anti-Theft – funkcija, leidžianti padidinti naudotojo lygio apsaugą pamesto arba pavogto įrenginio atveju. Anti-Theft suteikia galimybę stebėti įrenginio naudojimą ir nustatyti jūsų pamesto įrenginio vietą nustatant IP adresą ESET HOME – tai padės įrenginį atgauti ir apsaugoti asmens duomenis.

Tokios modernios Anti-Theft technologijos kaip geografinė IP adresų paieška, vaizdo fiksavimas saityno kamera, naudotojo paskyros apsauga ir įrenginio stebėjimas gali padėti jums ir teisėsaugos organizacijoms surasti jūsų kompiuterį ar įrenginį, jei jį pamestumėte ar pavogtų. ESET HOME galite matyti, kokia veikla vykdoma kompiuteryje arba įrenginyje.

Norėdami sužinoti daugiau apie Anti-Theft programoje ESET HOME, žr. ESET HOME Internetinis žinynas.

„Anti-Theft“ gali netinkamai veikti domenų kompiuteriuose dėl naudotojų paskyrų valdymo apribojimų.

Įgalinę Anti-Theft, galite optimizuoti įrenginio saugą pagrindiniame programos lange > **Nustatymai** > **Saugumo priemonės** > **Anti-Theft**.



Optimizavimo parinktys

Fiktyvi paskyra nesukurta

Sukūrus fiktyvią paskyrą, padidėja tikimybė rasti pamestą ar pavogtą įrenginį. Jei pažymėsite įrenginį kaip pamestą, Anti-Theft užblokuos prieigą prie aktyvių naudotojo paskyrų, kad apsaugotų slaptus duomenis. Visiems, kurie bandys naudotis įrenginiu, bus leidžiama naudoti tik fiktyvią paskyrą. Fiktyvi paskyra yra svečio paskyros forma su ribotomis teisėmis. Ji bus naudojama kaip numatytoji sistemos paskyra, kol įrenginys nebus pažymėtas kaip susigrąžintas, neleidžiant niekam prisijungti prie kitų naudotojų paskyrų ar pasiekti naudotojo duomenų.

Kaskart kam nors prisijungus prie fiktyvios paskyros, kai jūsų kompiuteris yra įprastos būsenos, jums bus išsiųstas pranešimas su informacija apie įtartiną veiklą kompiuteryje. Gavę pranešimą el. paštu, galite nuspręsti, ar norite pažymėti, kad kompiuteris yra dingęs.

Norėdami sukurti fiktyvią paskyrą, spustelėkite **Kurti fiktyvią paskyrą**, teksto lauke įveskite **fiktyvios paskyros pavadinimą** ir spustelėkite **Kurti**.

Sukūrę fiktyvią paskyrą, spustelėkite **Fiktyvios paskyros nustatymai**, kad pervardytumėte arba pašalintumėte paskyrą.

Windows paskyrų slaptažodžių apsauga

Jūsų naudotojo paskyra nėra apsaugota slaptažodžiu. Šį optimizavimo įspėjimą gausite, jei bent viena naudotojo paskyra nebus apsaugota slaptažodžiu. Sukūrus slaptažodį visiems naudotojams (išskyrus **fiktyvią paskyrą**) kompiuteryje, ši problema bus išspręsta.

Norėdami sukurti naudotoj paskyros slaptažodį, spustelėkite **Tvarkyti Windows paskyras** ir pakeiskite slaptažodį arba vykdykite toliau pateiktus nurodymus:

1. Klaviatūroje paspauskite CTRL+Alt+Delete.

2. Spustelėkite **Keisti slaptažodį**.

3. Lauką **Senas slaptažodis** palikite tuščią.

4. Įveskite slaptažodį į laukus **Naujas slaptažodis** ir **Patvirtinti slaptažodį** ir paspauskite **Įvesti**.

Automatinis prisijungimas prie Windows paskyrų

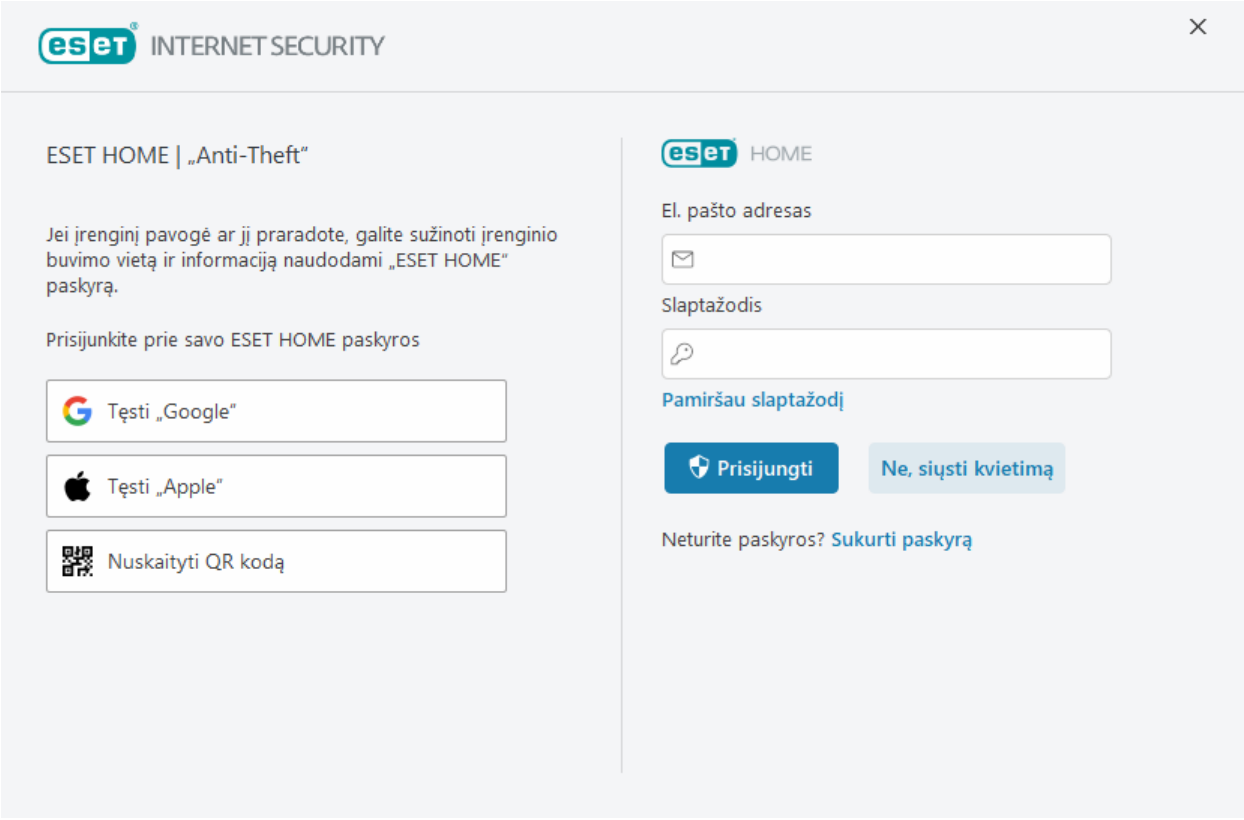
Jūsų naudotojo paskyroje įgalintas automatinis prisijungimas, todėl jūsų paskyra nėra apsaugota nuo neteisėtos prieigos. Šį optimizavimo įspėjimą gausite, jei bent vienoje naudotojo paskyroje įjungtas automatinis prisijungimas. Norėdami išspręsti šią optimizavimo problemą, spustelėkite **Išjungti automatinį prisijungimą**.

Automatinis prisijungimas prie fiktyvios paskyros

Automatinis prisijungimas įgalintas **fiktyviai paskyrai** jūsų įrenginyje. Kai įrenginys yra įprastoje būsenoje, nerekomenduojame naudoti automatinio prisijungimo, nes tai gali sukelti problemų dėl prieigos prie jūsų tikrosios naudotojo paskyros arba siųsti klaidingus pavojaus signalus apie trūkstamą kompiuterio būseną. Norėdami išspręsti šią optimizavimo problemą, spustelėkite **Išjungti automatinį prisijungimą**.

Prisijungti prie savo ESET HOME paskyros.

Norėdami įgalinti / išjungti Anti-Theft ir pasiekti įrenginio vietą ir informaciją ESET HOME, prisijunkite prie savo ESET HOME paskyros.



Yra keli prisijungimo prie ESET HOME paskyros būdai:

• **Naudokite savo ESET HOME el. pašto adresą ir slaptažodį** – įveskite **el. pašto adresą** ir **slaptažodį,** kuriuos naudojote kurdami ESET HOME paskyrą, ir spustelėkite **Prisijungti**.

• **Naudokite savo Google paskyrą /AppleID** – spustelėkite **Tęsti Google** arba **Tęsti Apple** ir prisijunkite prie atitinkamos paskyros. Po sėkmingo prisijungimo būsite nukreipti į ESET HOME patvirtinimo tinklalapį. Norėdami tęsti, grįžkite į ESET produkto langą. Daugiau informacijos apie prisijungimą naudojant Google paskyrą / AppleID rasite ESET HOME internetiniame žinyne.

• **Nuskaitykite QR kodą** – spustelėkite **Nuskaityti QR kodą**, kad būtų rodomas QR kodas. Atidarykite ESET HOME programą mobiliesiems ir nuskaitykite QR kodą arba nukreipkite įrenginio kamerą į QR kodą. Daugiau informacijos ieškokite ESET HOME internetiniame žinyne.

Prisijungti nepavyko – dažniausios klaidos.

Jeigu dar neturite ESET HOME paskyros, spustelėkite **Sukurti paskyrą**, kad užsiregistruotumėte arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.
Jei pamiršote slaptažodį, spustelėkite **Pamiršau savo slaptažodį** ir atlikite ekrane pateikiamus veiksmus arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.

Anti-Theft nepalaiko Microsoft Windows Home Server.

Nustatyti įrenginio pavadinimą

Lauke **Įrenginio pavadinimas** pateikiamas jūsų kompiuterio (įrenginio) pavadinimas, kuris bus rodomas kaip identifikatorius visose ESET HOME paslaugose. Kompiuterio pavadinimas naudojamas pagal numatytuosius nustatymus. Įveskite įrenginio pavadinimą arba naudokite numatytąjį pavadinimą ir spustelėkite **Tęsti**.

Anti-Theft įgalinta / išjungta

Šiame lange yra patvirtinimo pranešimas, kai įgalinate / išjungiate Anti-Theft:

• Įgalinta – jūsų įrenginį dabar saugo Anti-Theft, o jo saugą galite valdyti nuotoliniu būdu ESET HOME portale naudodami savo paskyrą.

• Išjungta – Anti-Theft šiame įrenginyje išjungta, o visi su <%ESET_ANTTHEFT%> susiję šio įrenginio duomenys pašalinami iš ESET HOME portalo.

Nepavyko pridėti naujo įrenginio

Įvyko klaida aktyvinant Anti-Theft.

Dažniausi scenarijai yra šie:

• Klaida prisijungiant prie ESET HOME

• Nėra interneto ryšio (arba šiuo metu neveikia internetas)

Jei negalite išspręsti problemos, kreipkitės į ESET techninę pagalbą.

Parametrų importavimas ir eksportavimas

Galite importuoti arba eksportuoti pasirinktinius ESET Internet Security .xml konfigūracijos failus iš **Nustatymų** meniu.

> **Iliustruotos instrukcijos**
> Peržiūrėkite mūsų iliustruotas instrukcijas anglų ir keliomis kitomis kalbomis apie ESET konfigūracijos nustatymų importavimas arba eksportavimas, naudojant .xml failą.

Konfigūravimo failų importavimas ir eksportavimas yra naudingas, jeigu reikia padaryti ESET Internet Security dabartinės konfigūracijos atsarginę kopiją, kurią galėtumėte naudoti vėliau. Be to, parametrų eksportavimo parinktis yra patogi, jei norite pageidautiną konfigūraciją naudoti keliose sistemose. Galite lengvai importuoti .xml failą ir perkelti šiuos nustatymus.

Norėdami importuoti konfigūraciją, pagrindiniame programos lange spustelėkite **Nustatymai** > **Parametrų importavimas / eksportavimas** ir pasirinkite **Importuoti parametrus**. Įveskite kelią į konfigūracijos failą arba spustelėkite mygtuką **...**, kad galėtumėte naršydami rasti konfigūracijos failą, kurį norite importuoti.

Norėdami eksportuoti konfigūraciją, pagrindiniame programos lange spustelėkite **Nustatymai** > **Parametrų importavimas / eksportavimas**. Pasirinkite **Eksportuoti parametrus** ir įveskite visą failo kelią su pavadinimu. Spustelėkite **...** ir susiraskite vietą kompiuteryje, kur norite įrašyti konfigūracijos failą.

> Eksportuojant parametrus gali įvykti klaida, jeigu neturite visų teisių rašyti eksportuojamą failą į nurodytą katalogą.

Žinynas ir palaikymas

Pagrindiniame programos lange spustelėkite **Žinynas ir palaikymas**, kad būtų rodoma palaikymo informacija ir trikčių šalinimo įrankiai, padedantys išspręsti problemas, su kuriomis galite susidurti.

Prenumerata

- Prenumeratos trikčių diagnostika – spustelėkite šią nuorodą, kad rastumėte aktyvinimo arba prenumeratos keitimo problemų sprendimus.

- Keisti prenumeratą – spustelėkite, kad būtų atidarytas aktyvinimo langas, kuriame galėsite aktyvinti produktą. Jei jūsų įrenginys prijungtas prie ESET HOME, pasirinkite prenumeratą iš savo ESET HOME paskyros arba pridėkite naują.

Įdiegtas produktas

- Kas nauja – spustelėkite, kad atidarytumėte informacijos langą apie naujas ir patobulintas funkcijas.

- Apie ESET Internet Security – rodo informaciją apie jūsų ESET Internet Security kopiją.

- Produkto trikčių diagnostika – spustelėkite šią nuorodą, kad rastumėte dažniausiai pasitaikančių problemų sprendimus.

- **Keisti produktą** – spustelėkite ir sužinosite, ar „ESET Internet Security“ galima pakeisti į kitą produktų liniją naudojant dabartinę prenumeratą.

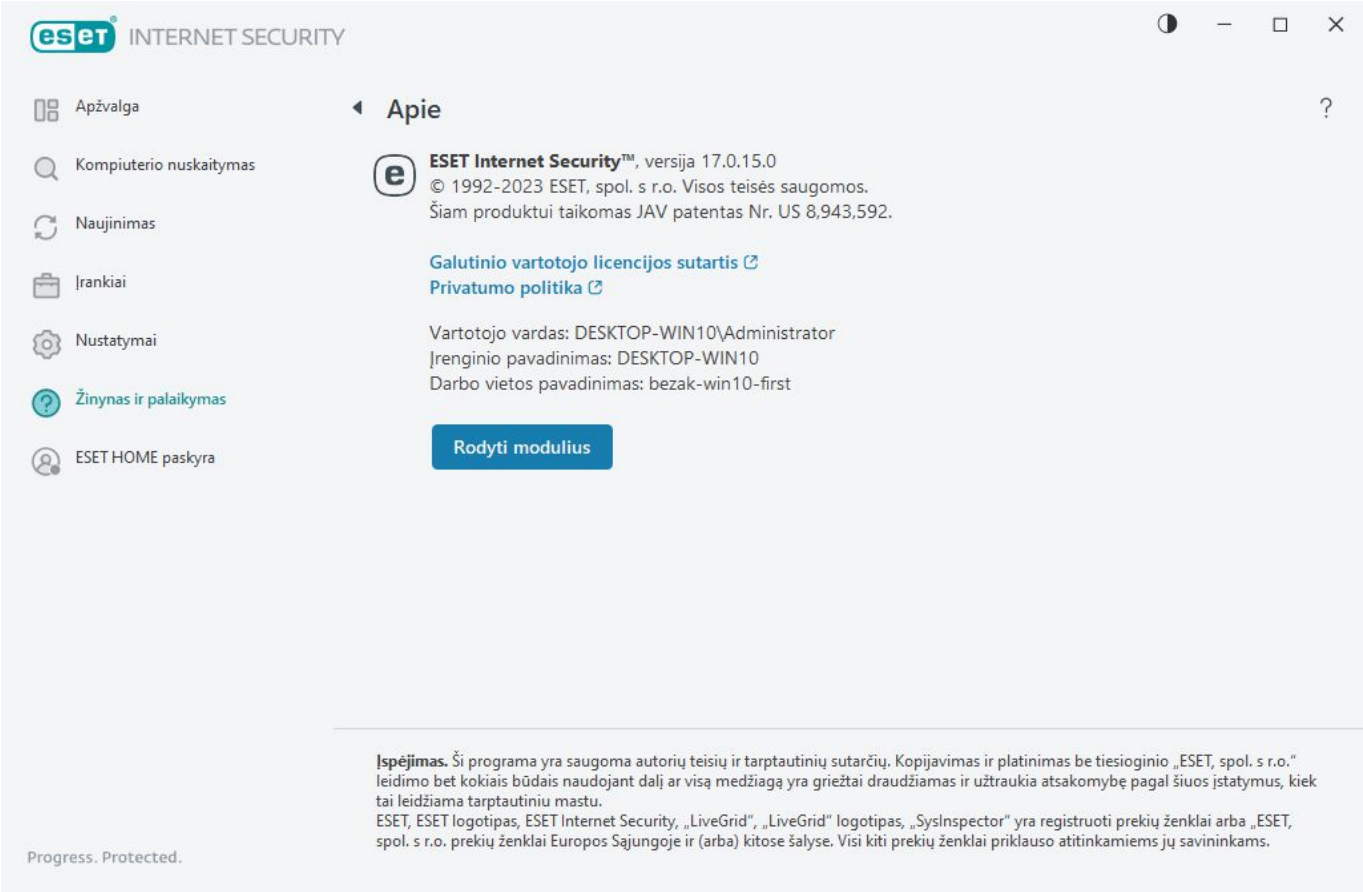
Žinyno puslapis – spustelėkite šią nuorodą norėdami patekti į ESET Internet Security žinyno puslapius.

Techninė pagalba

Žinių bazė – ESET žinių bazėje yra pateikiami atsakymai į dažniausiai užduodamus klausimus ir rekomenduojami įvairių problemų sprendimai. Reguliariai ESET techninių specialistų naujinama žinių bazė yra galingiausias įrankis sprendžiant įvairiausias problemas.

Apie ESET Internet Security

Šiame lange pateikiama išsami informacija apie įdiegtą ESET Internet Security versiją ir jūsų kompiuterį.



Spustelėkite **Rodyti modulius**, kad pamatytumėte informaciją apie įkeltų programų modulių sąrašą.

- Informaciją apie modulius galite nukopijuoti į mainų sritį spustelėdami **Kopijuoti**. Tai gali būti naudinga diagnozuojant sutrikimus arba kreipiantis į techninę pagalbą.

- Lange „Moduliai“ spustelėkite **Aptikimo modulis,** kad atidarytumėte ESET virusų radarą, kuriame pateikiama informacija apie kiekvieną ESET aptikimo modulio versiją.

ESET naujienos

Šiame lange ESET Internet Security reguliariai pateikia jums ESET naujienas.

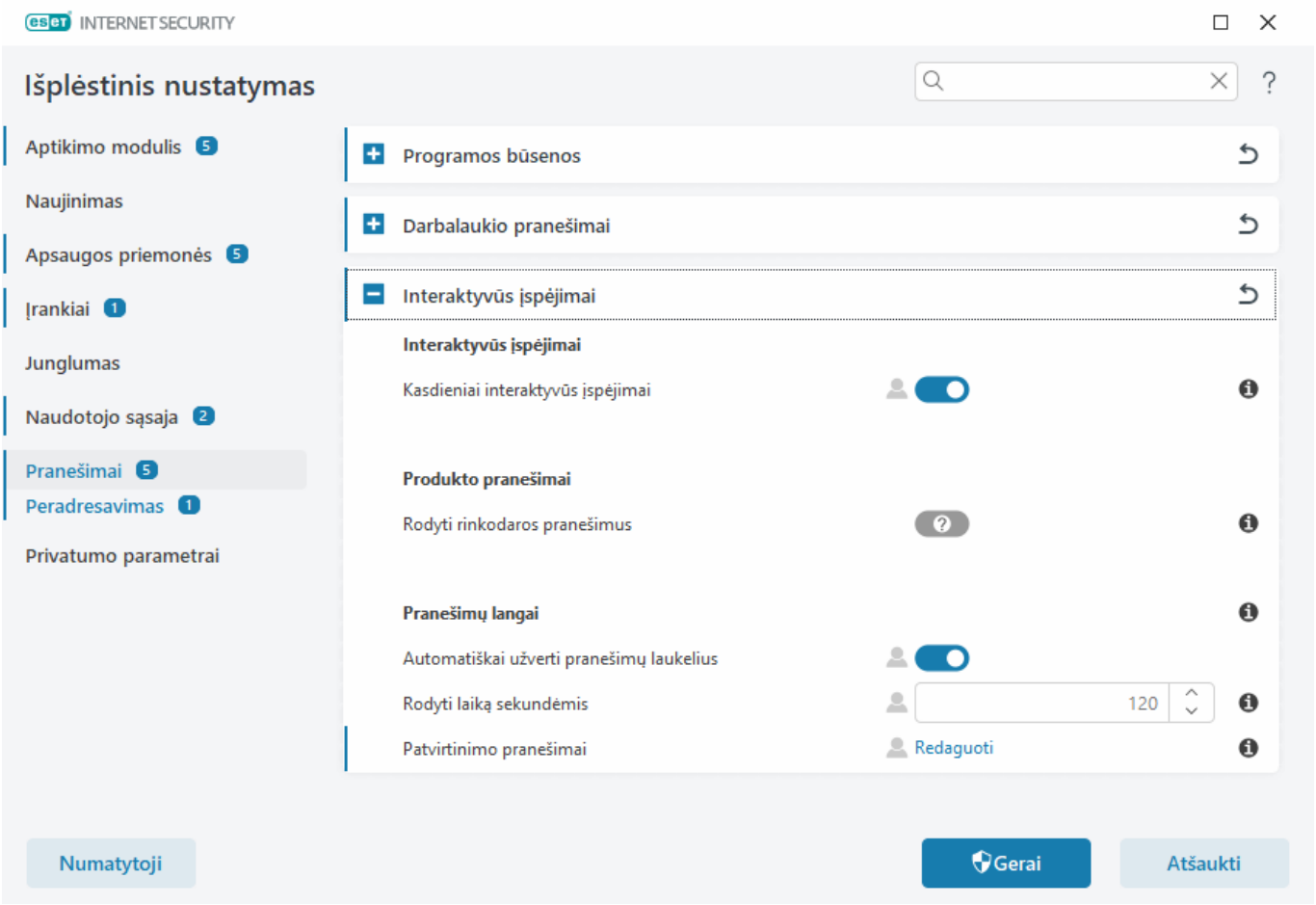
Produkto pranešimai, teikiami tam, kad naudotojai gautų ESET naujienas bei kitą informaciją. Rinkodaros pranešimų siuntimui reikia vartotojo sutikimo. Todėl rinkodaros pranešimai pagal numatytuosius nustatymus vartotojui nesiunčiami (rodoma kaip klaustukas). Įjungdami šią parinktį, sutinkate gauti ESET rinkodaros pranešimus. Jei nesate suinteresuoti gauti ESET rinkodaros medžiagos, išjunkite parinktį **Rodyti rinkodaros pranešimus**.

Norėdami įjungti ar išjungti rinkodaros pranešimų gavimą pranešimo lange, vadovaukitės toliau pateiktais nurodymais.

1. Atidaro išplėstinį nustatymą.

2. Spustelėkite **Pranešimai** > **Interaktyvūs įspėjimai**.

3. Modifikuokite parinktį **Rodyti rinkodaros pranešimus**.



Sistemos konfigūracijos duomenų pateikimas

Kad pagalbą galėtų suteikti kuo greičiau ir tiksliau, ESET reikalauja informacijos apie ESET Internet Security konfigūraciją, išsamios sistemos informacijos ir vykdomų procesų („ESET SysInspector“ žurnalo failas) bei registro duomenų. ESET šiuos duomenis naudos tik norėdama suteikti klientui techninę pagalbą.

Pateikus žiniatinklio formą jūsų sistemos konfigūracijos duomenys pateikiami ESET. Jei norite šį veiksmą įsiminti ir toliau taikyti šiam procesui, pasirinkite **Visada pateikti šią informaciją**. Pateikti žiniatinklio formą nesiųsdami jokių duomenų, spustelėkite **Neteikti duomenų** ir tęskite.

Sistemos konfigūracijos duomenų pateikimą galite konfigūruoti pasirinkę Išplėstinis nustatymas > **Įrankiai** > **Diagnostika** > Techninė pagalba.

Jei nusprendėte pateikti sistemos konfigūracijos duomenis, būtina užpildyti ir pateikti žiniatinklio formą. Priešingu atveju jūsų bilietas nebus sukurtas, o sistemos konfigūracijos duomenys bus prarasti. Jei sistemos konfigūracijos duomenų pateikti negalima, užpildykite žiniatinklio formą ir palaukite nurodymų iš techninės pagalbos.

Techninė pagalba

Pagrindiniame programos lange spustelėkite **Žinynas ir palaikymas** > **Techninė pagalba**.

Susisiekti su technine pagalba

Prašyti pagalbos – jei nepavyksta rasti savo problemos sprendimo, galite naudoti ir šią formą, esančią ESET svetainėje, kad galėtumėte greitai susisiekti su ESET techninės pagalbos skyriumi. Atsižvelgiant į jūsų nustatymus, prieš pildant saityno formą rodomas sistemos konfigūracijos duomenų pateikimo langas.

Gaukite informacijos apie techninę pagalbą

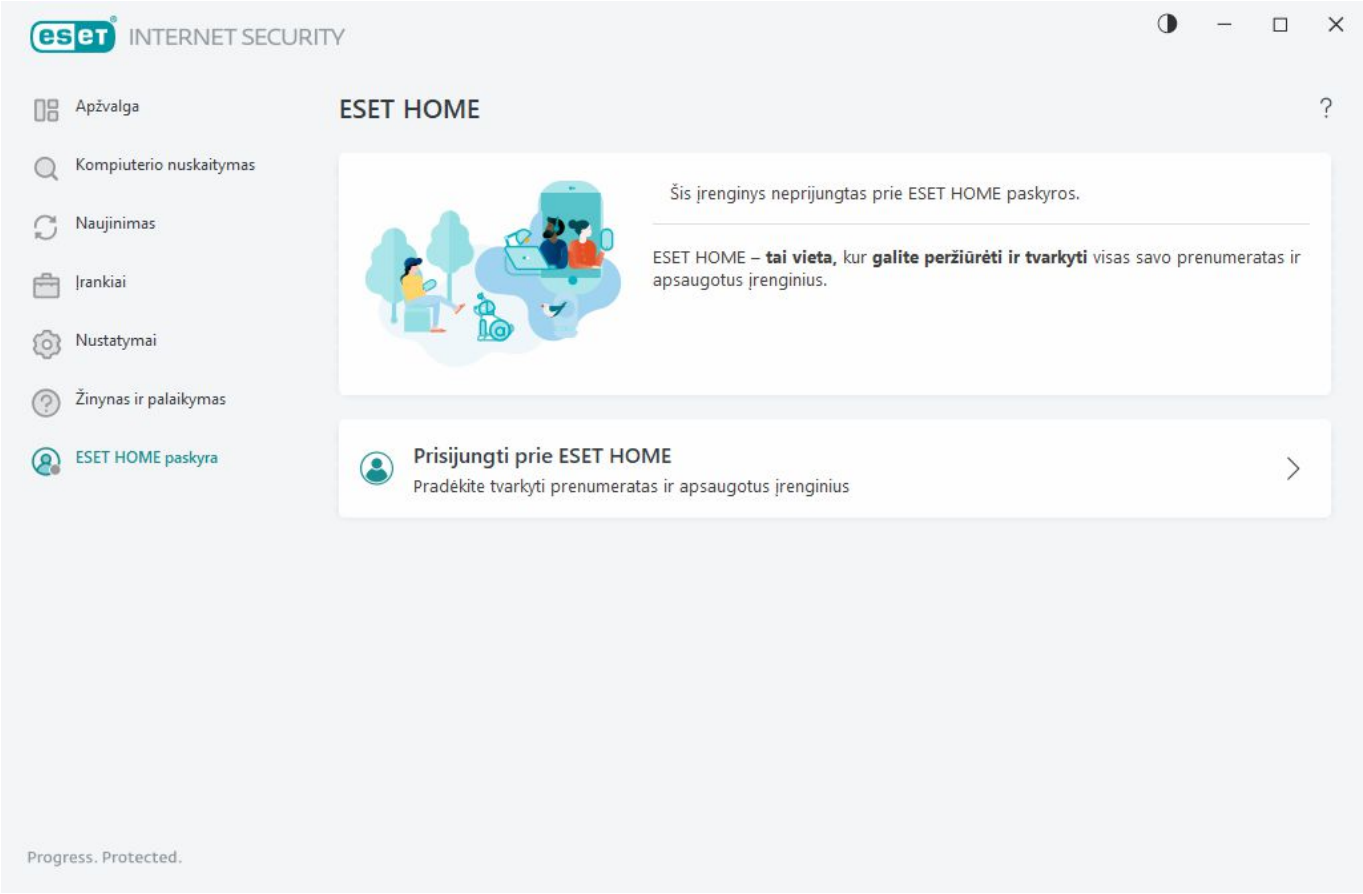
Išsami informacija apie techninę pagalbą – kai prašoma, galite nukopijuoti ir nusiųsti informaciją ESET techninės pagalbos tarnybai (pvz., išsamią prenumeratos informaciją, produkto pavadinimą, produkto versiją, operacinę sistemą ir kompiuterio informaciją).

ESET Log Collector – saitai į ESET žinių bazės straipsnį, iš kurio galima atsisiųstiESET Log Collector – programą, kuri iš kompiuterio automatiškai renka informaciją ir žurnalus, kad padėtų greičiau spręsti kylančias problemas. Jei pageidaujate daugiau informacijos, žr. ESET Log Collector internetinį vartotojo vadovą.

Spustelėkite Įjungti išplėstinį registravimą, kad sukurtumėte išplėstinius visų galimų funkcijų žurnalus ir padėtumėte kūrėjams nustatyti ir išspręsti problemas. Nustatytas **Diagnostinis** minimalaus registravimo daugiažodiškumo lygis. Išplėstinis registravimas bus išjungtas po dviejų valandų, nebent jį sustabdytumėte paspausdami **Stabdyti išplėstinį registravimą**. Kai visi žurnalai sukurti, pranešimų lange pateikta tiesioginė prieiga prie diagnostikos aplanko, kuriame yra sukurti žurnalai.

„ESET HOME“ paskyra

ESET HOME Paskyros ryšio būseną galite peržiūrėti pagrindinis programos lango > **„ESET HOME“ paskyra**.



Šis įrenginys neprijungtas prie „ESET HOME“ paskyros.

Spustelėkite Prijungti prie ESET HOME, kad prijungtumėte įrenginį prie ESET HOME ir tvarkytumėte savo prenumeratas ir apsaugotus įrenginius. Galite atnaujinti, naujovinti ar pratęsti prenumeratą bei peržiūrėti svarbią informaciją. ESET HOME valdymo portale arba mobiliojoje programėlėje galite pridėti kitų prenumeratų, atsisiųsti produktus į savo įrenginius, patikrinti produkto saugos būseną ar bendrinti prenumeratą el. paštu. Daugiau informacijos rasite apsilankę ESET HOME internetiniame žinyne.

Šis įrenginys prijungtas prie „ESET HOME“ paskyros

Įrenginio saugą galite valdyti nuotoliniu būdu naudodami „ESET HOME“ portalą arba programą mobiliesiems. Spustelėkite **„App Store“** arba **„Google Play“**, kad būtų rodomas QR kodas, kurį galite nuskaityti mobiliuoju telefonu ir atsisiųsti „ESET HOME“ programą mobiliesiems iš „App Store“ arba „Google Play“.

„ESET HOME“ paskyra – jūsų „ESET HOME“ paskyros pavadinimas.

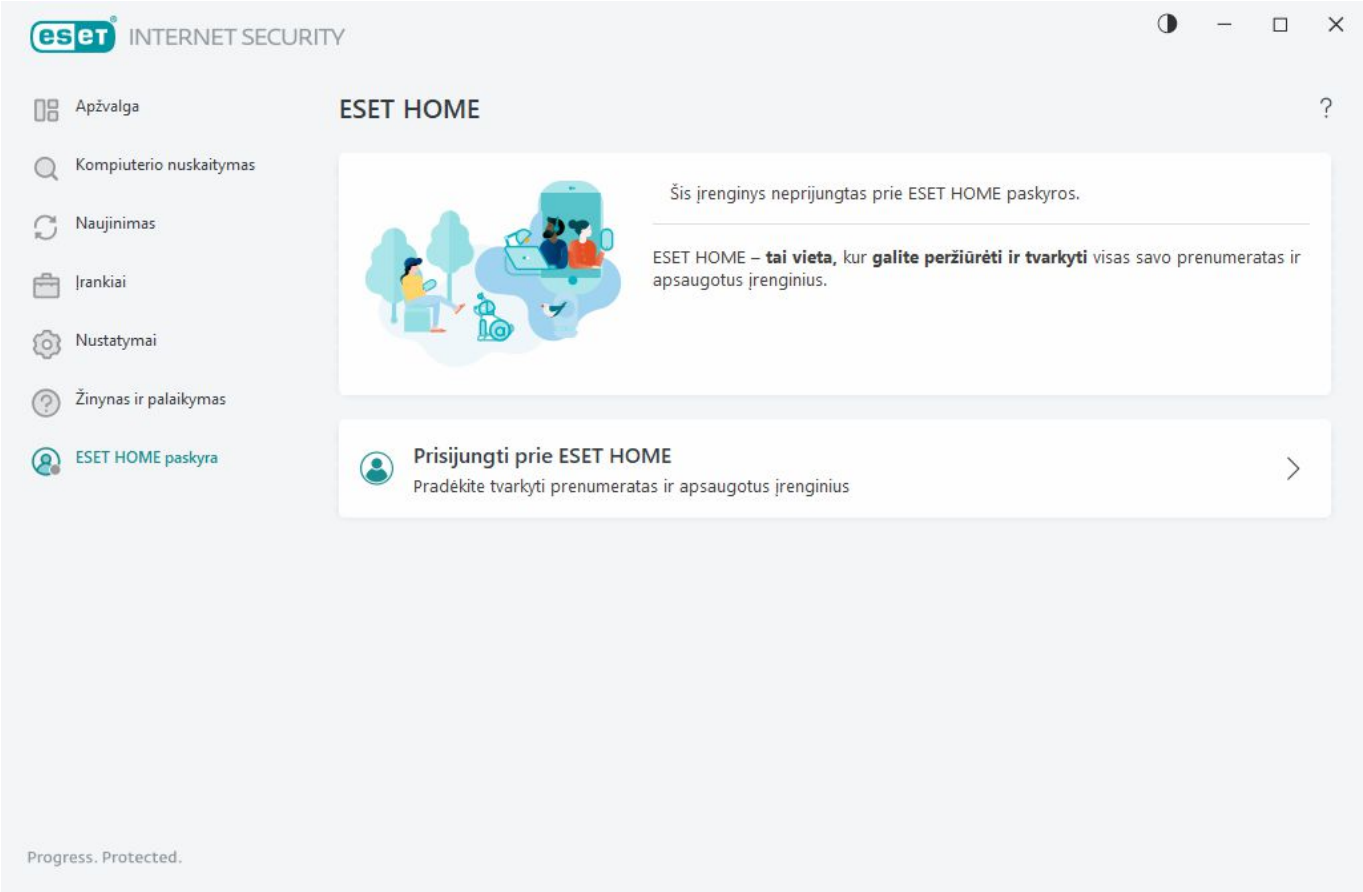
Įrenginio pavadinimas – „ESET HOME“ paskyroje rodomas šio įrenginio pavadinimas.

Atidaryti „ESET HOME“ – atidaro „ESET HOME“ valdymo portalą.

Norėdami atjungti įrenginį nuo „ESET HOME“ paskyros, spustelėkite **Atjungti nuo „ESET HOME“** > **Atjungti**. Aktyvinimui naudojama prenumerata išliks aktyvi, o jūsų įrenginys bus apsaugotas.

Prisijunkite prie „ESET HOME“

Susiekite įrenginį su ESET HOME, kad peržiūrėtumėte ir valdytumėte visas savo aktyvintas ESET prenumeratas ir įrenginius. Galite atnaujinti, naujovinti ar pratęsti prenumeratą bei peržiūrėti svarbią prenumeratos informaciją. ESET HOME valdymo portale arba mobiliojoje programėlėje galite pridėti kitų prenumeratų, atsisiųsti produktus į savo įrenginius, patikrinti produkto saugos būseną ar bendrinti prenumeratas el. paštu. Daugiau informacijos rasite apsilankę ESET HOME internetiniame žinyne.



Įrenginio prijungimas prie ESET HOME:

> Jei jungiatės prie ESET HOME diegdami arba pasirinkdami **Naudoti ESET HOME paskyrą** kaip aktyvinimo būdą, vadovaukitės nurodymais temoje Naudoti ESET HOME paskyrą.
> Jei jau įdiegėte ir aktyvinote „ESET Internet Security“ naudodami prie ESET HOME paskyros pridėtą prenumeratą, galite susieti įrenginį su ESET HOME, naudodamiesi ESET HOME portalu. Vadovaukitės ESET HOME internetinio žinyno instrukcijomis ir leiskite prisijungti ESET Internet Security.

1. Pagrindiniame programos lange spustelėkite **ESET HOME paskyra** > **Prisijungti prie ESET HOME** arba spustelėkite **Prisijungti prie ESET HOME** pranešime **Susiekite šį įrenginį su ESET HOME paskyra**.

2. Prisijungti prie savo ESET HOME paskyros.

> Jeigu dar neturite ESET HOME paskyros, spustelėkite **Sukurti paskyrą**, kad užsiregistruotumėte arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.
> Jei pamiršote slaptažodį, spustelėkite **Pamiršau savo slaptažodį** ir atlikite ekrane pateikiamus veiksmus arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.

3. Nustatykite **įrenginio pavadinimą** ir spustelėkite **Tęsti**.

4. Sėkmingai užmezgus ryšį rodomas išsamios informacijos langas. Spustelėkite **Atlikta**.

Prisijungti prie ESET HOME

Yra keli prisijungimo prie ESET HOME paskyros būdai:

- **Naudokite savo ESET HOME el. pašto adresą ir slaptažodį** – įveskite **el. pašto adresą** ir **slaptažodį,** kuriuos

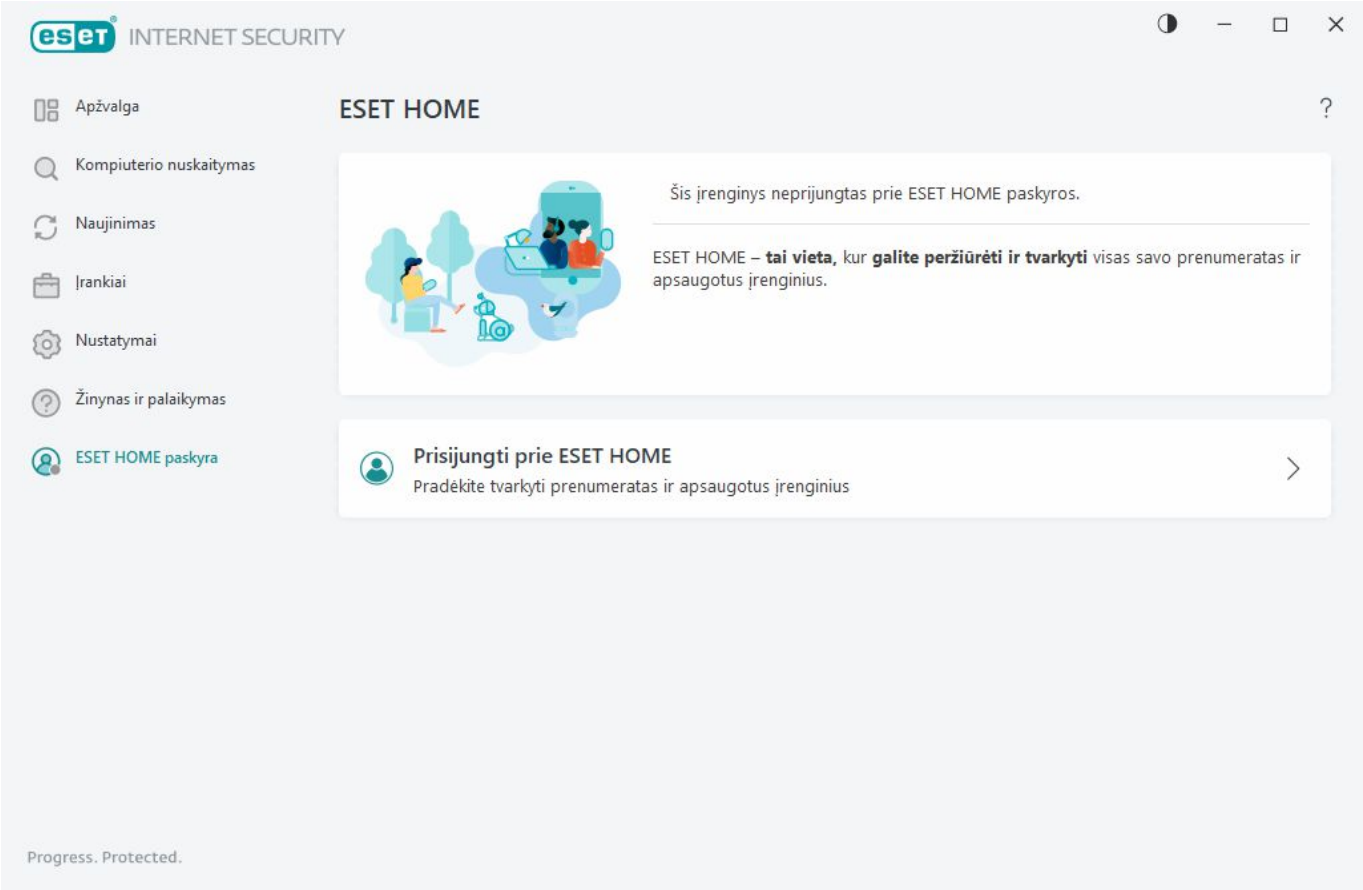
naudojote kurdami ESET HOME paskyrą, ir spustelėkite **Prisijungti**.

• **Naudokite savo Google paskyrą /AppleID** – spustelėkite **Tęsti Google** arba **Tęsti Apple** ir prisijunkite prie atitinkamos paskyros. Po sėkmingo prisijungimo būsite nukreipti į ESET HOME patvirtinimo tinklalapį. Norėdami tęsti, grįžkite į ESET produkto langą. Daugiau informacijos apie prisijungimą naudojant Google paskyrą / AppleID rasite ESET HOME internetiniame žinyne.

• **Nuskaitykite QR kodą** – spustelėkite **Nuskaityti QR kodą**, kad būtų rodomas QR kodas. Atidarykite ESET HOME programą mobiliesiems ir nuskaitykite QR kodą arba nukreipkite įrenginio kamerą į QR kodą. Daugiau informacijos ieškokite ESET HOME internetiniame žinyne.

Jeigu dar neturite ESET HOME paskyros, spustelėkite **Sukurti paskyrą**, kad užsiregistruotumėte arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.
Jei pamiršote slaptažodį, spustelėkite **Pamiršau savo slaptažodį** ir atlikite ekrane pateikiamus veiksmus arba peržiūrėkite instrukcijas ESET HOME internetiniame žinyne.

Prisijungti nepavyko – dažniausios klaidos.



Prisijungti nepavyko – dažniausios klaidos

Nepavyko rasti paskyros, atitinkančios įvestą el. pašto adresą

Įvestas el. pašto adresas nesutampa su jokia ESET HOME paskyra. Spustelėkite **Atgal** ir įveskite teisingą el. pašto adresą ir slaptažodį.

Norėdami prisijungti, turite sukurti ESET HOME paskyrą. Jei neturite ESET HOME paskyros, spustelėkite **Atgal** >

Sukurti paskyrą arba žr. Sukurti naują ESET HOME paskyrą.

Naudotojo vardas ir slaptažodis nesutampa

Įvestas slaptažodis neatitinka įvesto el. pašto adreso. Spustelėkite **Atgal**, įveskite teisingą slaptažodį ir patikrinkite, ar įvestas el. pašto adresas yra teisingas. Jei vis tiek negalite prisijungti, spustelėkite **Atgal** > **Pamiršau slaptažodį,** kad iš naujo nustatytumėte slaptažodį ir atlikite ekrane pateikiamus veiksmus arba žr. Pamiršau savo ESET HOME slaptažodį.

Pasirinkta prisijungimo parinktis neatitinka jūsų paskyros

Jūsų paskyra yra susieta su jūsų socialinio tinklo paskyra. Norėdami prisijungti prie ESET HOME, spustelėkite **Tęsti „Google“** arba **Tęsti Apple** ir prisijunkite prie atitinkamos paskyros. Po sėkmingo prisijungimo būsite nukreipti į ESET HOME patvirtinimo tinklalapį. Galite atjungti savo socialinio tinklo paskyrą nuo ESET HOME savo paskyros ESET HOME portale.

Neteisingas slaptažodis

Ši klaida gali įvykti, jei jūsų ESET Internet Security jau susietas ir jūs atliekate ESET HOME pakeitimus, kurie reikalauja prisijungti (pvz., išjungti „Anti-Theft“), bet slaptažodis, kurį įvedėte neatitinka jūsų paskyros. Spustelėkite **Atgal** ir įveskite teisingą slaptažodį. Jei vis tiek negalite prisijungti, spustelėkite **Atgal** > **Pamiršau slaptažodį,** kad iš naujo nustatytumėte slaptažodį ir atlikite ekrane pateikiamus veiksmus arba žr. Pamiršau savo ESET HOME slaptažodį.

Įtraukti įrenginį į ESET HOME

Jei jau įdiegėte ir aktyvinote „ESET Internet Security“ naudodami prie ESET HOME paskyros pridėtą prenumeratą, galite susieti įrenginį su ESET HOME, naudodamiesi ESET HOME portalu:

1. Išsiųskite užklausą susieti jūsų įrenginį.

2. ESET Internet Security rodomas dialogo langas **Susieti šį įrenginį su ESET HOME paskyra** su ESET HOME paskyros pavadinimu. Spustelėkite **Leisti**, kad susietumėte įrenginį su minėta ESET HOME paskyra.

Jei neatliekama jokių veiksmų, susiejimo užklausa bus automatiškai atšaukta maždaug po 30 minučių.

Išplėstiniai nustatymai

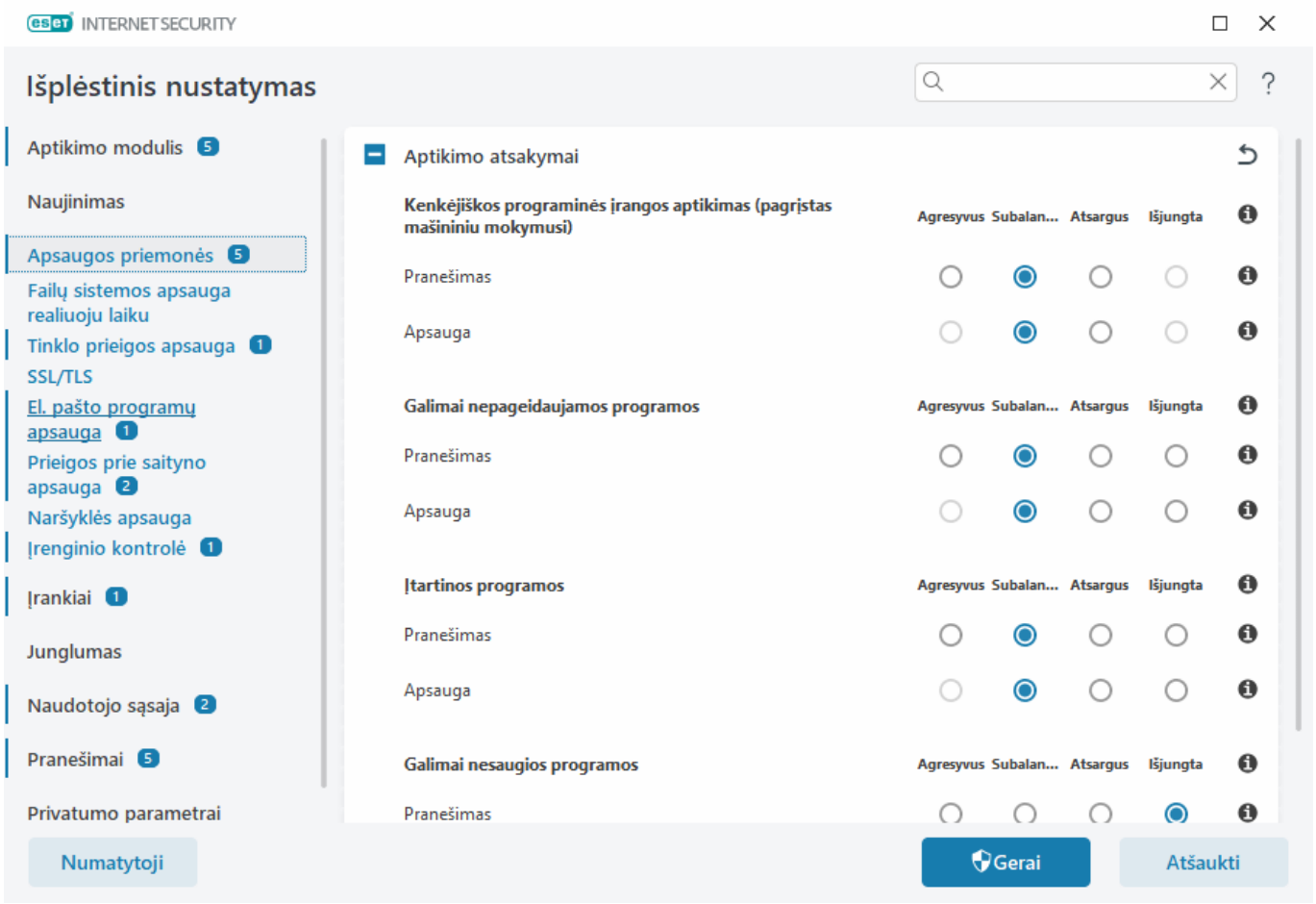
Išplėstinis nustatymas leidžia konfigūruoti išsamius ESET Internet Security nustatymus, kad jie atitiktų jūsų poreikius.

Norėdami atidaryti „Išplėstinį nustatymą“, pirmiausia atidarykite pagrindinį programos langą ir paspauskite klaviatūros klavišą **F5** arba spustelėkite **Nustatymai** > **Išplėstinis nustatymas**.

Atsižvelgiant į Prieigos sąranką, galite būti paraginti įvesti slaptažodį, kad galėtumėte atidaryti išplėstinius nustatymus.

Išplėstiniame nustatyme galite konfigūruoti šiuos parametrus:

- Aptikimo modulis
- Naujinti
- Apsaugos priemonės
- Įrankiai
- Junglumas
- Vartotojo sąsaja
- Pranešimai
- Privatumo parametrai



Aptikimo modulis

Išplėstinis nustatymas > **Aptikimo modulis** leidžia konfigūruoti šias parinktis:

- Išimtys
- Išplėstinės parinktys
- Tinklo duomenų srauto skaitytuvas

Išimtys

Išimtys leidžia neįtraukti objektų į aptikimo modulį. Kad būtų nuskaityti visi objektai, išimtis rekomenduojame kurti tik kai tai visiškai būtina. Atskiri atvejai, kai gali reikėti neįtraukti tam tikro objekto: didelės duomenų bazės įrašai, kurie lėtina kompiuterio darbą nuskaitant, ar programinė įranga, kuri konfliktuoja su nuskaitymo procesu.

Našumo išimtys – neįtraukti failų ir aplankų į nuskaitymą. Našumo išimtys yra naudingos neįtraukiant žaidimų į failų lygmens nuskaitymą arba jei sukeliamas nenormalus sistemos veikimas arba didinant našumą.

Aptikimo išimtys suteikia galimybę neįtraukti objektų į aptikimą, naudojant aptikimo pavadinimą, kelią arba maišą. Aptikimo išimtys nepašalina failams ir aplankams taikomo nuskaitymo, tai atlieka našumo išimtys. Aptikimo išimtys taikomos objektams tik kai juos aptinka aptikimo modulis ir išimčių sąraše yra atitinkama taisyklė.

Nesupainiokite jų su kitų tipų išimtimis:

- Proceso išimtys – į nuskaitymą neįtraukiamos visos failų operacijos, priskiriamos neįtrauktos programos procesams (gali būti būtina, norint pagerinti atsarginių kopijų kūrimo greitį ir paslaugų prieinamumą),
- Neįtraukti failų plėtiniai,
- HIPS išimtys,
- Debesimi paremtos apsaugos išimčių filtras.

Našumo išimtys

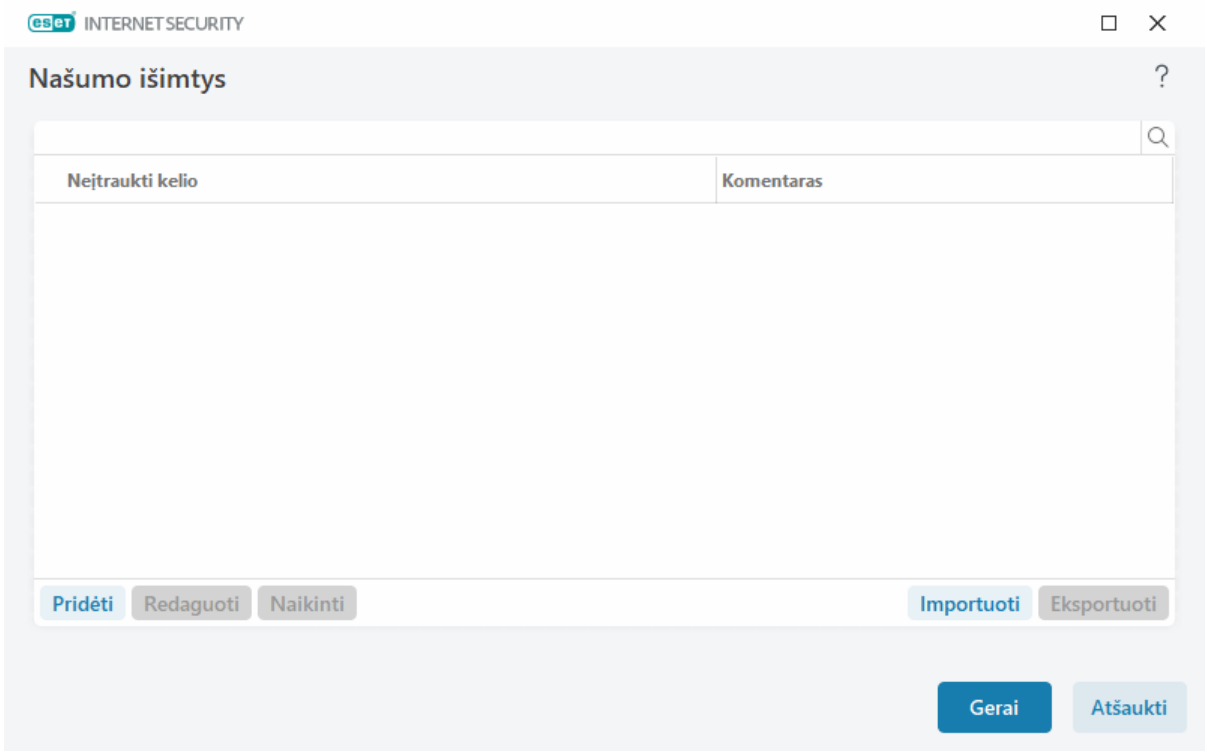
Našumo išimtys leidžia neįtraukti failų ir aplankų į nuskaitymą.

Kad visi objektai būtų nuskaityti ieškant grėsmių, išimtis rekomenduojame kurti tik kai tai visiškai būtina. Vis dėlto yra situacijų, kai reikia neįtraukti tam tikro objekto, pavyzdžiui, didelių duomenų bazės įrašų, kurie lėtintų kompiuterio darbą nuskaitant, ar programinės įrangos, kuri nesuderinama su nuskaitymu.

Galite įtraukti failus ir aplanką į nuskaitymo išimčių sąrašą dalyje Išplėstinis nustatymai > **Aptikimo modulis** > **Išimtys** > **Našumo išimtys** > **Redaguoti**.

Nesupainiokite su Aptikimo išimtys, Neįtraukti failų plėtiniai, HIPS išskyrimai arba Procesų išimtys.

Norėdami neįtraukti objekto (kelio, failo arba aplanko) į nuskaitymą, spustelėkite **Pridėti** ir įveskite taikytiną kelią į arba pasirinkite jį medžio struktūroje.



Jei failas atitinka nuskaitymo išimties kriterijus, jame esančios grėsmės **failų sistemos apsaugos realiuoju laiku** modulis ar **kompiuterio nuskaitymo** modulis neaptiks.

Valdymo elementai

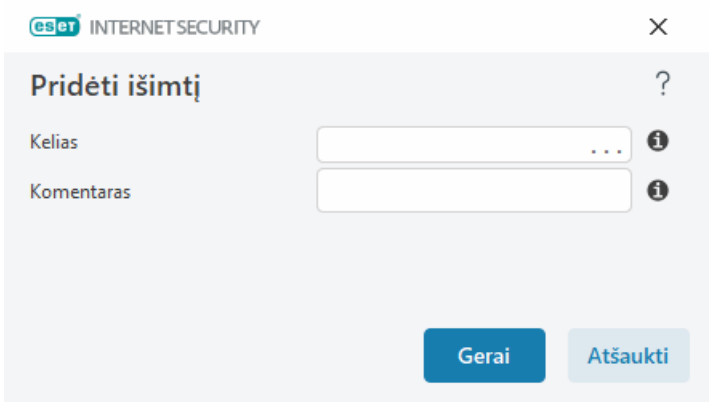
- **Pridėti** – neįtraukia objektų į aptikimą.
- **Redaguoti** – leidžia redaguoti pasirinktus įrašus.
- **Šalinti** – pašalinami pasirinkti įrašai (paspauskite CTRL ir spustelėkite norėdami pasirinkti kelis įrašus).

Pridėti arba redaguoti našumo išimtis

Šis dialogo langas neįtraukia konkretaus kelio (failo arba katalogo) šiame kompiuteryje.

Pasirinkite kelią arba įveskite ranka

Norėdami pasirinkti tinkamą kelią, spustelėkite **...** lauke **Kelias**.
Įrašydami rankiniu būdu, daugiau išskyrimų formatų pavyzdžių žr. toliau.



Galite naudoti pakaitos simbolius norėdami neįtraukti failų grupės. Klaustukas (*?*) reiškia vieną simbolį, o žvaigždutė (***) reiškia eilutę iš nulio ar daugiau simbolių.

Išimties formatas

- Norėdami neįtraukti visų aplanke esančių failų ir antrinių aplankų, įveskite kelią į aplanką ir naudokite kaukę **.*
- Norėdami neįtraukti tik „doc“ failų, naudokite kaukę **.doc*.
- Jei vykdomojo failo pavadinimas turi konkretų simbolių skaičių (su skirtingais simboliais) ir žinote tik pirmąjį simbolį (pavyzdžiui, „D“), naudokite šį formatą:

D????.exe (klaustukai pakeičia trūkstamus / nežinomus simbolius)

Pavyzdžiai:

- *C:\Tools** – Kelias turi baigtis kairiniu brūkšniu (\) ir žvaigždute (*), kad būtų nurodyta, jog tai aplankas ir visas aplanko turinys (failai ir antriniai aplankai) nebus įtrauktas.
- *C:\Tools*.** – Toks pat elgesys kaip ir *C:\Tools**
- *C:\Tools* – *Tools* aplankui nebus taikoma išimtis. Skaitytuvui *Tools* gali atrodyti ir kaip failo pavadinimas.
- *C:\Tools*.dat* – tai neįtrauks .dat failų, esančių *Tools* aplanke.
- *C:\Tools\sg.dat* – neįtrauks šio konkretaus failo, į kurį veda konkretus kelias.

Sistemos kintamieji išskyrimuose

Galite naudoti sistemos kintamuosius kaip %PROGRAMFILES% norėdami nustatyti nuskaitymo išskyrimus.

- Jei norite neįtraukti aplanko Programiniai failai naudodami šį sistemos kintamąjį, naudokite kelią *%PROGRAMFILES%** (nepamirškite kelio gale pridėti įžambaus kairinio brūkšnio ir žvaigždutės) pridedami jį į išskyrimus.
- Jei norite neįtraukti visų pakatalogio *%PROGRAMFILES%* failų ir aplankų, naudokite kelią *%PROGRAMFILES%\Excluded_Directory**

Išskleiskite palaikomų sistemos kintamųjų sąrašą

Toliau pateikti kintamieji gali būti naudojami kelio išskyrimo formate:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Nuo naudotojų priklausantys sistemos kintamieji (pavyzdžiui, *%TEMP%* arba *%USERPROFILE%*) arba aplinkos kintamieji (pavyzdžiui, *%PATH%*) nepalaikomi.

Pakaitos simboliai kelio viduryje nepalaikomi

Pakaitos simbolių naudojimas kelio viduryje (pvz., *C:\Tools*\Data\file.dat*) gali veikti, bet nėra oficialiai palaikomas veiklos išskyrimų atveju.

Nėra jokių pakaitos simbolių naudojimo kelio viduryje apribojimų, kai naudojate aptikimo išimtis.

Išskyrimų tvarka

- Taisyklių pirmenybės lygio negalima reguliuoti mygtukais aukštyn / žemyn (kaip Užkardos taisyklių, kurias galima vykdyti iš viršaus į apačią).
- Kai pirma taikoma taisyklė yra suderinta skaitytuvo, antra taikoma taisyklė nebus vertinama.
- Kuo mažiau taisyklių, tuo geresnis nuskaitymų rezultatas.
- Venkite kurti jau esamas taisykles.

Kelio išskyrimo formatas

Galite naudoti pakaitos simbolius norėdami neįtraukti failų grupės. Klaustukas (*?*) reiškia vieną simbolį, o žvaigždutė (***) reiškia eilutę iš nulio ar daugiau simbolių.

Išimties formatas

• Norėdami neįtraukti visų aplanke esančių failų ir antrinių aplankų, įveskite kelią į aplanką ir naudokite kaukę ***.
• Norėdami neįtraukti tik „doc“ failų, naudokite kaukę **.doc*.
• Jei vykdomojo failo pavadinimas turi konkretų simbolių skaičių (su skirtingais simboliais) ir žinote tik pirmąjį simbolį (pavyzdžiui, „D“), naudokite šį formatą:
D????.exe (klaustukai pakeičia trūkstamus / nežinomus simbolius)
Pavyzdžiai:
• *C:\Tools** – Kelias turi baigtis kairiniu brūkšniu (\) ir žvaigždute (*), kad būtų nurodyta, jog tai aplankas ir visas aplanko turinys (failai ir antriniai aplankai) nebus įtrauktas.
• *C:\Tools*.** – Toks pat elgesys kaip ir *C:\Tools**
• *C:\Tools* – *Tools* aplankui nebus taikoma išimtis. Skaitytuvui *Tools* gali atrodyti ir kaip failo pavadinimas.
• *C:\Tools*.dat* – tai neįtrauks .dat failų, esančių *Tools* aplanke.
• *C:\Tools\sg.dat* – neįtrauks šio konkretaus failo, į kurį veda konkretus kelias.

Sistemos kintamieji išskyrimuose

Galite naudoti sistemos kintamuosius kaip %PROGRAMFILES% norėdami nustatyti nuskaitymo išskyrimus.
• Jei norite neįtraukti aplanko Programiniai failai naudodami šį sistemos kintamąjį, naudokite kelią *%PROGRAMFILES%** (nepamirškite kelio gale pridėti įžambaus kairinio brūkšnio ir žvaigždutės) pridedami jį į išskyrimus.
• Jei norite neįtraukti visų pakatalogio *%PROGRAMFILES%* failų ir aplankų, naudokite kelią *%PROGRAMFILES%\Excluded_Directory**

Išskleiskite palaikomų sistemos kintamųjų sąrašą

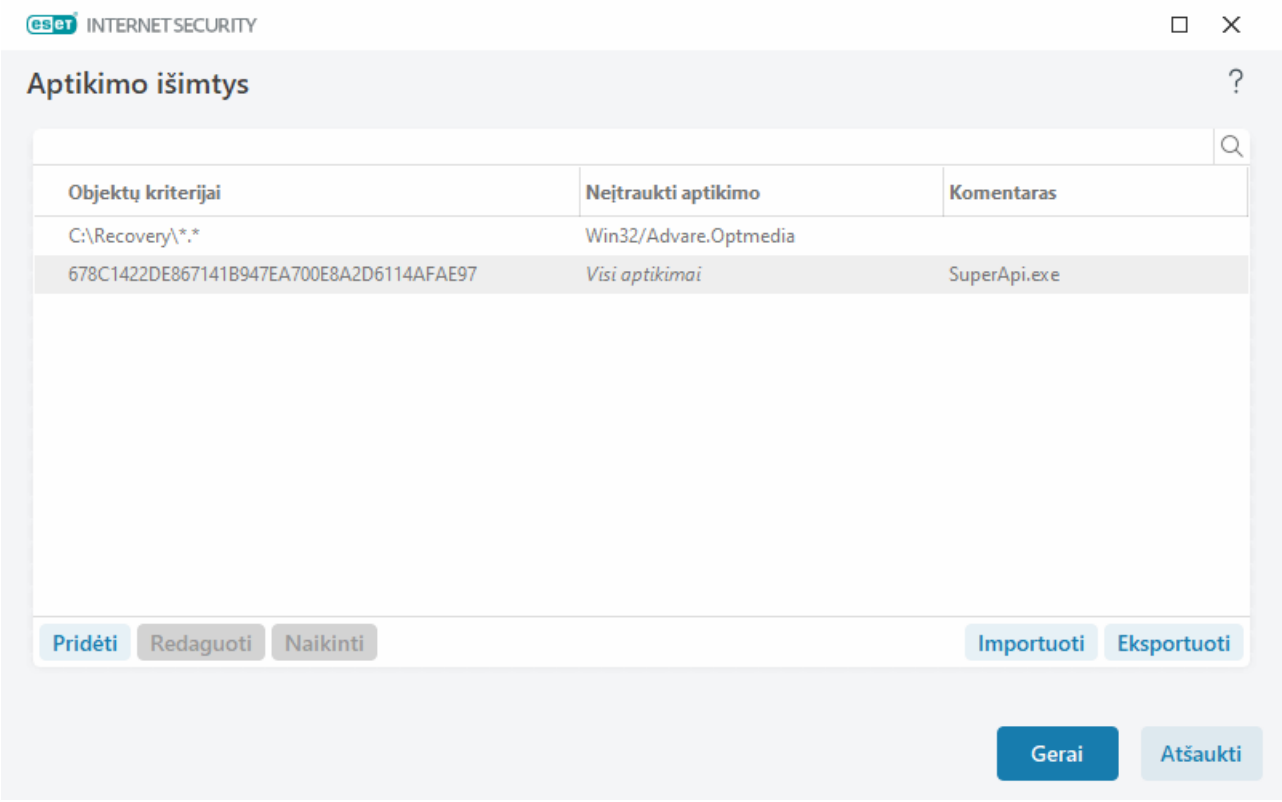
Toliau pateikti kintamieji gali būti naudojami kelio išskyrimo formate:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Nuo naudotojų priklausantys sistemos kintamieji (pavyzdžiui, *%TEMP%* arba *%USERPROFILE%*) arba aplinkos kintamieji (pavyzdžiui, *%PATH%*) nepalaikomi.

Aptikimo išimtys

Aptikimo išimtys suteikia galimybę neįtraukti objektų į aptikimą, filtruojant aptikimo pavadinimą, objekto kelią arba maišą.

Kaip veikia aptikimo išimtys

Aptikimo išimtys nepašalina failams ir aplankams taikomo nuskaitymo, tai atlieka Našumo išimtys. Aptikimo išimtys taikomos objektams tik kai juos aptinka aptikimo modulis ir išimčių sąraše yra atitinkama taisyklė. Pavyzdžiui, (žr. toliau pateiktos iliustracijos pirmą eilutę), kai objektas aptinkamas kaip Win32/Adware.Optmedia ir aptiktas failas yra *C:\Recovery\file.exe*. Antroje eilutėje kiekvienam failui su tinkama SHA-1 maiša visada bus taikoma išimtis, nepaisant aptikimo pavadinimo.



Norint užtikrinti visų grėsmių aptikimą, rekomenduojame kurti aptikimo išimtis tik kai tai būtina.

Norėdami įtraukti failus ir aplankus į išimčių sąrašą, pasirinkite Išplėstinis nustatymai > **Aptikimo modulis** > **Išimtys** > **Aptikimo išimtys** > **Redaguoti**.

Nesupainiokite su Našumo išimtys, Neįtraukti failų plėtiniai, HIPS išskyrimai arba Procesų išimtys.

Kad objektas būtų neįtraukiamas (pagal aptikimo pavadinimą arba maišą) į aptikimo modulį, spustelėkite **Pridėti**.

Potencialiai nepageidaujamoms programoms ir potencialiai nesaugioms programoms taip pat galima sukurti išskyrimą pagal aptikimo pavadinimą:

- Įspėjimo lange, kuriame pranešama apie aptikimą (spustelėkite **Rodyti išplėstines parinktis,** tada pasirinkite **Neįtraukti į aptikimą**).
- Žurnalo failų kontekstiniame meniu, naudojant Aptikimo išimčių kūrimo vedlį.
- Spustelėję **Įrankiai** > **Karantinas**, dešiniuoju mygtuku spustelėję karantinuotą failą ir kontekstiniame meniu pasirinkę **Atkurti ir neįtraukti į nuskaitymą**.

Aptikimo išimčių kriterijai objektams

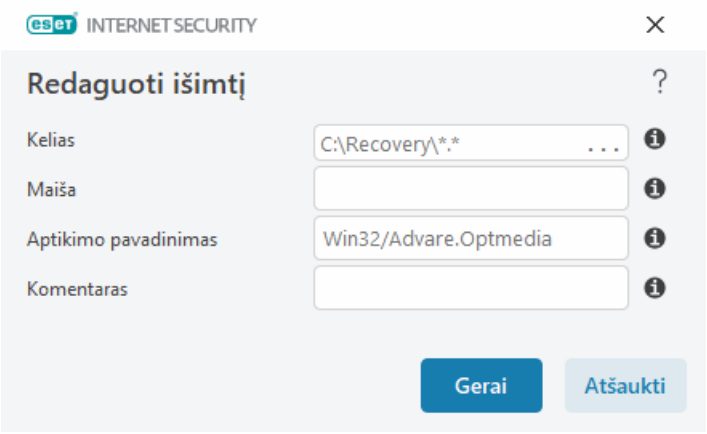
- **Kelias** – riboti aptikimo išimtį nurodytam keliui (arba bet kokiam).
- **Aptikimo pavadinimas** – jei šalia neįtraukto failo yra aptikimo pavadinimas, tai reiškia, kad failas neįtraukiamas tik nurodytam aptikimui, o ne visiškai. Jei vėliau šis failas bus užkrėstas kitomis kenkėjiškomis programomis, jis bus aptiktas.
- **Maiša** – neįtraukia failo pagal konkrečią maišą SHA-1, nepaisant failo tipo, vietos, pavadinimo ar jo plėtinio.

Pridėti arba redaguoti aptikimo išimtį

Neįtraukti aptikimo

Turi būti pateiktas teisingas ESET aptikimo pavadinimas. Norėdami sužinoti teisingą aptikimo pavadinimą, žr. sritį Žurnalo failai ir tada išskleidžiamame žurnalo failų meniu pasirinkite **Aptikimai**. Tai yra naudinga, kai ESET Internet Security aptinkamas klaidingai teigiamas pavyzdys. Tikrų grėsmių išskyrimai yra labai pavojingi, pagalvokite apie tai, kad turėtumėte neįtraukti tik paveiktų failų / katalogų, lauke **Kelio kaukė** spustelėdami **...**, ir (arba) tik laikinai. Išimtys apima ir galimas nepageidaujamas taikomąsias programas, galimas nesaugias taikomąsias programas ir įtartinas programas.

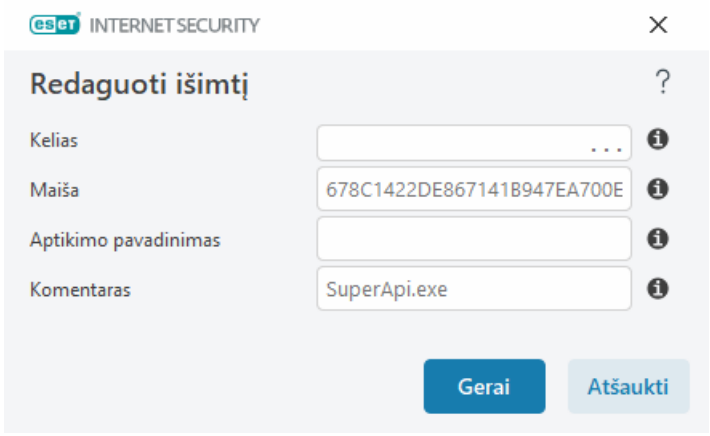
Taip pat skaitykite Kelio išskyrimo formatas.



Žr. Aptikimo išimčių pavyzdys toliau.

Išskirti maišą

Neįtraukia failo pagal konkrečią maišą SHA-1, nepaisant failo tipo, vietos, pavadinimo ar jo plėtinio.



Išimtys pagal aptikimo pavadinimą
Norėdami pašalinti konkretų aptikimą pagal jo pavadinimą, įveskite teisingą aptikimo pavadinimą: Win32/Adware.Optmedia
Taip pat galite naudoti toliau nurodytus formatus, kai pašalinate aptikimą iš ESET Internet Security perspėjimo lango:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Valdymo elementai

- **Pridėti** – neįtraukia objektų į aptikimą.
- **Redaguoti** – leidžia redaguoti pasirinktus įrašus.
- **Šalinti** – pašalinami pasirinkti įrašai (paspauskite CTRL ir spustelėkite norėdami pasirinkti kelis įrašus).

Aptikimo išimčių kūrimo vedlys vedlį

Aptikimo išimtį taip pat galima sukurti kontekstiniame meniu Žurnalo failai (netaikoma kenkėjiškos programinės įrangos aptikimui):

1. Pagrindiniame programos lange spustelėkite **Įrankiai** > **Žurnalo failai**.
2. Dešiniuoju pelės mygtuku spustelėkite aptikimą **Aptikimų žurnale**.
3. Spustelėkite **Kurti išimtį**.

Norėdami išskirti vieną arba daugiau aptikimų pagal **Išimčių kriterijus**, spustelėkite **Keisti kriterijus**:

- **Tikslūs failai** – išskirti kiekvieną failą pagal jo SHA-1 maišą.
- **Aptikimas** – išskirti kiekvieną failą pagal jo aptikimo pavadinimą.
- **Kelias ir aptikimas** – išskirti kiekvieną failą pagal jo aptikimo pavadinimą ir kelią, įskaitant failo pavadinimą (pvz., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Rekomenduojama parinktis yra iš anksto pasirinkta pagal aptikimo tipą.

Pasirinktinai galite pridėti **Komentarą**, prieš spustelėdami **Kurti išimtį**.

Aptikimo modulio išplėstinės parinktys

Įgalinti išplėstinį nuskaitymą per AMSI yra „Microsoft“ apsaugos nuo kenkėjiškų programų nuskaitymo sąsajos įrankis, kuris leidžia nuskaityti „Powershell“ scenarijus, „Windows Script Host“ vykdomus scenarijus ir AMSI SDK nuskaitomus duomenis.

Tinklo duomenų srauto skaitytuvas

Tinklo duomenų srauto skaitytuvas suteikia programų protokolų apsaugą nuo kenkėjiškų programinių įrangų, kurios integruoja keletą pažangių kenkėjiškų programinių įrangų nuskaitymo metodų. Tinklo duomenų srauto skaitytuvas automatiškai nuskaito HTTP(S), POP3(S) ir IMAP(S) protokolus, nepriklausomai nuo interneto naršyklės ar el. pašto programos. Tinklo duomenų srauto skaitytuvą galite įjungti / išjungti, pasirinkę Išplėstinis nustatymas > **Aptikimo modulis** > **Tinklo duomenų srauto skaitytuvas**.

Įgalinti tinklo duomenų srauto skaitytuvą – jei išjungsite šią parinktį, HTTP(S), POP3(S) ir IMAP(S) protokolai nebus nuskaityti. Atminkite, kad ESET Internet Security šioms funkcijoms aktyvuoti, reikia įjungti tinklo duomenų srauto skaitytuvą:

- Prieigos prie saityno apsauga
- Tėvų kontrolė
- Naršyklės privatumas ir sauga
- Saugi bankininkystė ir naršymas
- SSL/TLS
- Apsauga nuo sukčiavimo apsimetant
- El. pašto programų apsauga

Debesimi paremta apsauga

ESET LiveGrid® (pagal ESET ThreatSense.Net išplėstinę ankstyvojo įspėjimo sistemą) naudoja duomenis, kuriuos ESET pateikia vartotojai iš viso pasaulio ir siunčia juos į ESET tyrimų laboratoriją. Pateikdama įtartinus pavyzdžius ir metaduomenis iš pasaulio ESET LiveGrid® suteikia mums galimybę greitai prisitaikyti prie klientų poreikių ir padeda ESET reaguoti į naujausias grėsmes.

Galimos šios parinktys:

Įjungti ESET LiveGrid® reputacijos sistemą

ESET LiveGrid® reputacijos sistema teikia debesų technologija pagrįstą baltąjį ir juodąjį sąrašą.

Jūs galite patikrinti Vykdomų procesų ir failų reputaciją tiesiog naudodamiesi programos sąsaja arba kontekstiniu meniu su papildoma informacija, gauta iš ESET LiveGrid®.

Įjungti ESET LiveGrid® atsiliepimų sistemą

Be ESET LiveGrid® reputacijos sistemos, ESET LiveGrid® grįžtamojo ryšio sistema surinks informaciją apie naujai aptiktas grėsmes, susijusias su jūsų kompiuteriu. Šią informaciją gali sudaryti toliau nurodyti duomenys.

- Failo, kuriame atsirado grėsmė, pavyzdys arba kopija
- Failo maršrutas
- Failo pavadinimas
- Data ir laikas
- Procesas, kurio metu grėsmė atsirado jūsų kompiuteryje
- Informacija apie kompiuterio operacinę sistemą

Pagal numatytuosius nustatymus ESET Internet Security yra sukonfigūruotas pateikti įtartinus failus ESET virusų laboratorijai, kad būtų atlikta išsami jų analizė. Failai su konkrečiais plėtiniais, pavyzdžiui, *.doc* ar *.xls*, niekada neįtraukiami. Taip pat galite pridėti kitų plėtinių, jei yra konkrečių failų, kurių jūs ar jūsų organizacija nenori siųsti.

Skaitykite apie susijusių duomenų siuntimą Privatumo politikoje.

Galite pasirinkti įjungti ESET LiveGrid®

Neprarasite jokių programinės įrangos funkcijų, tačiau atskirais atvejais ESET Internet Security gali sparčiau reaguoti į naujas grėsmes, kai įjungta ESET LiveGrid®. Jei anksčiau naudojote ESET LiveGrid® ir ją išjungėte, gali būti likę paruoštų siųsti duomenų paketų. Tokie paketai bus išsiųsti į ESET net ir išaktyvinus funkciją. Išsiuntus visą dabartinę informaciją, daugiau paketų kuriama nebus.

Išsamiau apie šių ESET LiveGrid® skaitykite terminų žodyne.
Peržiūrėkite mūsų iliustruotas instrukcijas anglų ir keliomis kitomis kalbomis, kaip įgalinti arba išjungti ESET LiveGrid® ESET Internet Security.

Debesimi paremta konfigūracija išplėstiniame nustatyme

Norėdami pasiekti ESET LiveGrid® nustatymus, atidarykite Išplėstinis nustatymas > **Aptikimo modulis** > **Apsauga, veikianti debesų technologijos pagrindu**.

• **Įjungti ESET LiveGrid® reputacijos sistemą (rekomenduojama)** – ESET LiveGrid® reputacijos sistema pagerina ESET apsaugos nuo kenkimo programinės įrangos sprendimų efektyvumą, nes nuskaitytų failų duomenis palygina su debesies saugykloje esančiais duomenų bazės įrašais baltajame ir juodajame sąrašuose.

• **Įjungti ESET LiveGrid® atsiliepimų sistemą** – siunčia atitinkamus pateikimo duomenis (aprašytus toliau esančiame skyriuje **Pavyzdžių pateikimas**) kartu su strigčių ataskaitomis ir statistiniais duomenimis į ESET tyrimo laboratoriją tolesnei analizei.

• **Pateikti strigčių ataskaitas ir diagnostinius duomenis** – pateikti ESET LiveGrid® susijusius diagnostinius

duomenis, pavyzdžiui, strigčių ataskaitas ir modulių atminties išklotines. Rekomenduojame laikyti įjungtą, nes tai padeda ESET diagnozuoti problemas, gerinti produktus ir užtikrinti geresnę galutinio naudotojo apsaugą.

• **Pateikti anoniminius statistinius duomenis** – leiskite ESET rinkti informaciją apie naujai aptiktas grėsmes, pvz., grėsmės pavadinimą, aptikimo datą ir laiką, aptikimo metodą ir susijusius metaduomenis, produkto versiją ir konfigūraciją, įskaitant informaciją apie jūsų sistemą.

• **Kontaktinis el. paštas (nebūtinas)** – jūsų kontaktinis el. pašto adresas gali būti įtrauktas su visais įtartinais failais ir gali būti naudojamas su jumis susisiekti, jeigu analizuojant reikės papildomos informacijos. Jūs negausite atsakymo iš ESET, jei neprireiks daugiau informacijos.

Pavyzdžių pateikimas

Rankinis pavyzdžių pateikimas – Leidžia rankiniu būdu pateikti pavyzdžius ESET iš kontekstinio meniu, pasirinkus Karantinas arba Įrankiai.

Automatinis aptiktų pavyzdžių pateikimas

Pasirinkite kokius pavyzdžius pateikti ESET analizei, kad būtų pagerintas grėsmių aptikimas (the numatytoji maximum pavyzdys size is 64MB) ateityje. Galimos šios parinktys:

• **Visi aptikti pavyzdžiai** – visi objektai, kuriuos aptiko aptikimo modulis (įskaitant galimas nepageidaujamas taikomąsias programas, kai įjungti skaitytuvo nustatymai).

• **Visi pavyzdžiai, išskyrus dokumentus** – visi aptikti pavyzdžiai, išskyrus **Dokumentai** (žr. toliau).

• **Nepateikti** – aptikti objektai nebus siunčiami ESET.

Automatinis įtartinų mėginių pateikimas

Šie pavyzdžiai taip pat bus siunčiami ESET, jei aptikimo modulis jų neaptinka. Pvz., pavyzdžiai, kurių vos neaptiko, arba vienas iš ESET Internet Security apsauginių modulių laiko šiuos pavyzdžius įtartinais arba jie neaiškiai elgiasi (numatytasis maksimalus pavyzdžių dydis yra 64 MB).

• **Vykdomieji failai** – sudaro vykdomieji failai, pavyzdžiui .exe, .dll, .sys.

• **Archyvai** – sudaro archyvo failų tipai, pavyzdžiui, .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Scenarijai** – sudaro scenarijaus failų tipai, pavyzdžiui, .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Kita** – įeina failų tipai, tokie kaip .jar, .reg, .msi, .sfw, .lnk.

• **Galimi brukalo el. laiškai** – funkcija leidžia siųsti galimas brukalo dalis ar visus el. laiškus su priedais tolesnei ESET analizei. Šios parinkties įgalinimas gerina visuotinį brukalų aptikimą, įskaitant efektyvesnį jūsų gaunamo brukalo aptikimą.

• **Dokumentai** – sudaro Microsoft Office arba PDF dokumentai su arba be aktyvaus turinio.

Išplėsti visų įtrauktų dokumentų failų tipų sąrašui

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Išimtys

Išimties filtras leidžia į pateikimo sąrašą neįtraukti failų ar aplankų (pvz., gali būti naudinga neįtraukti failų su konfidencialia informacija, tarkime, dokumentų ar skaičiuoklių). Sąraše esantys failai niekada nebus siunčiami analizuoti į ESET laboratoriją, net jei juose bus įtartino kodo. Dažniausiai naudojami failų tipai neįtraukti pagal numatytuosius nustatymus (.doc, ir t. t.). Jeigu norite, galite įtraukti į nesiunčiamų failų sąrašą.

Norėdami neįtraukti failų, atsisiųstų iš `download.domain.com`, eikite Išplėstinis nustatymas > **Aptikimo modulis** > **Debesimi pagrįsta apsauga** > **Pavyzdžių pateikimas** ir šalia **Išskyrimai** spustelėkite **Redaguoti**. Įtraukite išskyrimą `.download.domain.com`.

Maksimalus pavyzdžių dydis (MB) – nustato maksimalų automatiškai pateiktų pavyzdžių dydį (1-64 MB).

Debesimi paremtos apsaugos išimčių filtras

Išimčių filtras leidžia atsisakyti pateikti kai kuriuos failus ar aplankus kaip pavyzdžius. Sąraše esantys failai niekada nebus siunčiami analizuoti į ESET laboratoriją, net jei juose bus įtartino kodo. Dažniausi failų tipai (pvz., .doc ir pan.) neįtraukiami pagal numatytuosius nustatymus.

Ši funkcija praverčia, kai reikia neįtraukti failų, kuriuose gali būti konfidencialios informacijos, pvz., dokumentų arba skaičiuoklių.

Norėdami neįtraukti failų, atsisiųstų iš download.domain.com, spustelėkite Išplėstinis nustatymas > **Aptikimo modulis** > **Debesimi pagrįsta apsauga** > **Pavyzdžių pateikimas** > **Išskyrimai** ir įtraukite išskyrimą *download.domain.com*.

Kenkėjiškų programų nuskaitymai

Skyrių **Kenkėjiškų programų nuskaitymai** galima pasiekti pasirinkus Išplėstinis nustatymas > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** ir tai leidžia konfigūruoti nuskaitymo profilių nuskaitymo parametrus.

Nuskaitymas pareikalavus

Pasirinktas profilis – konkretus nustatymų rinkinys, kurį naudoja skaitytuvas pagal pareikalavimą. Kad sukurtumėte naują profilį, spustelėkite **Redaguoti** šalia **Profilių sąrašo**. Jei reikia daugiau informacijos, žr. Nuskaitymo profiliai.

Pasirinkę nuskaitymo profilį, galite konfigūruoti šias parinktis:

Nuskaitymo paskirties vietos – jei norite nuskaityti tik konkrečią paskirties vietą arba grupę paskirties vietų, spustelėkite **Redaguoti** šalia **Nuskaitymo paskirties vietos** ir pažymėkite parinktį aplankų (medžio) struktūroje. Jei reikia daugiau informacijos, žr. Nuskaitymo paskirties vietos.

Apsauga pareikalavus ir naudojant mašininį mokymąsi – galite konfigūruoti kiekvieno nuskaitymo profilio

ataskaitų teikimo ir apsaugos lygius. Pagal numatytuosius nustatymus nuskaitymo profiliai naudoja tą pačią sąranką, kaip apibrėžta Failų sistemos apsauga realiuoju laiku. Išjunkite perjungiklį šalia **Apsaugos realiuoju laiku nuostatų naudojimas**, kad sukonfigūruotumėte pasirinktinius ataskaitų teikimo ir apsaugos lygius. Žr. Apsaugos priemonės, kad gautumėte išsamų ataskaitų teikimo ir apsaugos lygių paaiškinimą.

ThreatSense – išplėstinio nustatymo parinktys, pvz., failų plėtiniai, kuriuos norite valdyti, ir naudojami aptikimo metodai. Daugiau informacijos ieškokite ThreatSense.

Nuskaitymo profiliai

ESET Internet Security yra 4 iš anksto apibrėžti nuskaitymo profiliai:

- **Išmanusis nuskaitymas** – tai numatytasis išplėstinis nuskaitymo profilis. Išmaniojo nuskaitymo profilyje naudojama išmaniojo optimizavimo technologija, kuri neapima failų, kurie ankstesnio nuskaitymo metu buvo rasti švarūs ir po šio nuskaitymo nebuvo pakeisti. Tai leidžia sutrumpinti nuskaitymo laiką ir daro mažiausią poveikį sistemos saugumui.

- **Kontekstinio meniu nuskaitymas** – pagal poreikį galite pradėti bet kurio failo nuskaitymą iš kontekstinio meniu. Kontekstinio meniu nuskaitymo profilis leidžia nustatyti nuskaitymo konfigūraciją, kuri bus naudojama paleidus nuskaitymą tokiu būdu.

- **Giluminis nuskaitymas** – giluminio nuskaitymo profilyje pagal numatytuosius parametrus išmanusis optimizavimas nenaudojamas, todėl naudojant šį profilį nuskaitomi visi failai.

- **Kompiuterio nuskaitymas** – numatytasis profilis, naudojamas įprastai nuskaitant kompiuterį.

Jūsų pasirinkti nuskaitymo parametrai gali būti išsaugoti, kad galėtumėte juos panaudoti nuskaitydami kitą kartą. Rekomenduojame susikurti skirtingus profilius (su skirtingais nuskaitymo tikslais, nuskaitymo metodais ir kitais parametrais) kiekvienam reguliariai atliekamam nuskaitymui.

Norėdami sukurti naują profilį, atidarykite langą Išplėstinis nustatymas > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nuskaitymas pareikalavus** > **Profilių sąrašas** > **Redaguoti**. **Profilių tvarkytuvės** lange yra **Pasirinkto profilio** išskleidžiamasis meniu, kuriame pateikti nuskaitymo profiliai ir naujo profilio kūrimo parinktis. Norėdami sukurti nuskaitymo profilį, kuris atitiktų jūsų poreikius, žiūrėkite skyrių ThreatSense, kuriame aprašytas kiekvienas nuskaitymo nustatymų parametras.

> Tarkime, norite sukurti savo nuskaitymo profilį ir jums iš dalies tinka **kompiuterio nuskaitymo** konfigūracija, tačiau nenorite nuskaityti pakavimo programos arba galimas nesaugias taikomąsias programas, be to, norite taikyti **Visada ištaisyti aptikimą**. Įveskite savo naujojo profilio pavadinimą į langą **Profilių tvarkytuvas** ir spustelėkite **Pridėti**. **Pasirinkto profilio** išskleidžiamajame meniu pasirinkite naująjį profilį ir pakeiskite likusius parametrus pagal savo reikalavimus, tada spustelėkite **Gerai**, kad naująjį profilį įrašytumėte.

Nuskaitymo tikslai

Išskleidžiamajame meniu **Nuskaitymo tikslai** galite pasirinkti iš anksto nustatytus nuskaitymo tikslus.

- **Pagal profilio parametrus** – pasirenkami paskirties tikslai, nustatyti pagal pasirinktą nuskaitymo profilį.
- **Nešiojamoji laikmena** – pasirenka diskelius, USB atminties įrenginius, CD/DVD.

- **Vietiniai įrenginiai** – pasirenka visus sistemos standžiuosius diskus.
- **Tinklo diskų įrenginiai** – pasirenka visus susietus tinklo diskus.
- **Tinkintaspasirinkimas** – atšaukia visus ankstesnius pasirinkimus.

Aplanko (medžio) struktūroje taip pat yra konkrečių tikslinių nuskaitymo objektų.

- **Operacinė atmintis** – nuskaito visus procesus ir duomenis, kuriuos šiuo metu naudoja operacinė atmintis.
- **Įkrovos sektoriai / UEFI** – nuskaito įkrovos sektorius ir UEFI, siekiant aptikti kenkėjišką programinę įrangą. Daugiau apie UEFI skaitytuvą skaitykite žodynėlėje.
- **WMI duomenų bazė** – nuskaito visą Windows Management Instrumentation WMI duomenų bazę, visus pavadinimus, visus klasės egzempliorius ir visas ypatybes. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis.
- **Sistemos registras** – nuskaito visą sistemos registrą, visus raktus ir antrinius raktus. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis. Valant aptiktus elementus, nuoroda lieka registre, kad įsitikintumėte, jog nebus prarasti svarbūs duomenys.

Norėdami greitai pereiti prie nuskaitymo paskirties vietos (failo ar aplanko), įveskite jo kelią į teksto lauką po medžio struktūra. Kelio pavadinime skiriamos didžiosios ir mažosios raidės. Norėdami įtraukti paskirties vietą į nuskaitymą, pažymėkite jos žymės langelį medžio struktūroje.

Nuskaitymas laukimo būsenoje

Galite įjungti laukimo būsenos skaitytuvą dalyje Išplėstiniai nustatymai > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nuskaitymas laukimo būsenoje**.

Nuskaitymas laukimo būsenoje

Kad įjungtumėte šią funkciją, įjunkite perjungiklį, esantį šalia **Įjungti laukimo būsenos nuskaitymą**. Kai kompiuteris yra laukimo būsenos, tylusis kompiuterio nuskaitymas yra atliekamas visuose vietiniuose įrenginiuose.

Kaip numatyta, laukimo būsenos aptikimo skaitytuvas neveiks (nešiojamajam) kompiuteriui veikiant akumuliatoriaus energija. Šį parametrą galite apeiti, išplėstiniame nustatyme suaktyvinę perjungiklį šalia **Vykdyti, net jei kompiuteris veikia naudodamas akumuliatoriaus energiją**.

Išplėstiniame nustatyme įgalinkite perjungiklį šalia **Įjungti registravimą**, kad kompiuterio nuskaitymo išvestis būtų registruojama Žurnalo failuose (pagrindiniame programos lange spustelėkite **Įrankiai** > **Žurnalo failai** ir išplečiamajame meniu **Žurnalas** pasirinkite **Kompiuterio nuskaitymas**).

Laukimo būsenos aptikimas

Išsamaus sąlygų, būtinų įjungti laukimo būsenos skaitytuvui, sąrašą žr. Laukimo būsenos aptikimo paleidimo sąlygos.

ThreatSense – išplėstinio nustatymo parinktys, pvz., failų plėtiniai, kuriuos norite valdyti, ir naudojami aptikimo

metodai. Daugiau informacijos rasite ThreatSense.

Laukimo būsenos aptikimas

Laukimo būsenos aptikimo parametrus galima konfigūruoti pasirinkus Išplėstiniai nustatymai > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Laukimo būsenos nuskaitymas** > **Laukimo būsenos aptikimas**. Šie parametrai nurodo Laukimo būsenos nuskaitymo paleidimo sąlygas:

- **Išjungtas ekranas arba ekrano užsklanda**
- **Kompiuterio užraktas**
- **Naudotojo atsijungimas**

Naudokite kiekvienos atitinkamos būsenos perjungiklius skirtingų laukimo būsenų aptikimo paleidimo sąlygoms įjungti arba išjungti.

Nuskaitymas paleidžiant

Pagal numatytąją parinktį automatinė failų patikra paleidimo metu bus atliekama paleidus sistemą arba atnaujinus aptikimo modulį. Šis nuskaitymas priklauso nuo Planuoklės konfigūracijos ir užduočių.

Nuskaitymo paleidžiant parinktys yra **Sistemos paleidimo failo patikros** planuoklės užduoties dalis. Norėdami pakeisti jos nustatymus, eikite į **Įrankiai** > **Planuoklė**, spustelėkite **Automatinė paleidimo failo patikra**, tada – **Redaguoti**. Atliekant paskutinį veiksmą pasirodys langas Automatinė paleidimo failo patikra. Norėdami rasti išsamias instrukcijas apie planuoklės užduoties kūrimą ir tvarkymą, žiūrėkite Naujų užduočių kūrimas.

ThreatSense – išplėstinio nustatymo parinktys, pvz., failų plėtiniai, kuriuos norite valdyti, ir naudojami aptikimo metodai. Daugiau informacijos rasite ThreatSense.

Automatinė paleidimo failo patikra

Kurdami suplanuotą sistemos paleidimo failo patikros užduotį toliau pateikiamus parametrus galite pakeisti įvairiai:

Išskleidžiamajame meniu **Nuskaitymo tikslas** pasitelkus slaptą modernų algoritmą nurodomas nuskaitymo išsamumas failams, kurie vykdomi paleidžiant sistemą. Failai išdėstomi mažėjimo tvarka pagal šiuos kriterijus:

- **Visi registruotieji failai** (daugiausia nuskaitytų failų)
- **Retai naudojami failai**
- **Įprastai naudojami failai**
- **Dažnai naudojami failai**
- **Tik dažniausiai naudojami failai** (nuskaitoma mažiausiai failų)

Įtraukiamos ir dvi konkrečios grupės:

- **Failai, paleidžiami prieš prisijungiant vartotojui** – failai iš tokių vietų, kurias galima pasiekti vartotojui neprisijungus (tai beveik visos paleidimo vietos, pavyzdžiui, paslaugos, naršyklės pagalbos objektai, „winlogon“ pranešimai, „Windows“ planuoklės įrašai, žinomi dll ir pan.).

- **Failai, paleidžiami vartotojui prisijungus** – failai iš tokių vietų, kurias galima pasiekti tik vartotojui prisijungus (tai failai, kuriuos paleidžia konkretus vartotojas, paprastai šie failai yra saugomi *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Nuskaitomų failų sąrašai nustatomi kiekvienai pirmiau nurodytai grupei. Jei pasirinksite mažesnį failų, vykdomų paleidžiant sistemą, nuskaitymo gylį, nenuskaityti failai bus nuskaityti atidarius arba vykdant.

Nuskaitymo prioritetas – prioriteto lygis, naudojamas nustatant, kada prasidės skenavimas:

- **Kai laisva** – užduotis bus atliekama, tik kai sistema veiks laukimo režimu,

- **Žemiausias** – esant pačiai mažiausiai sistemos apkrovai,

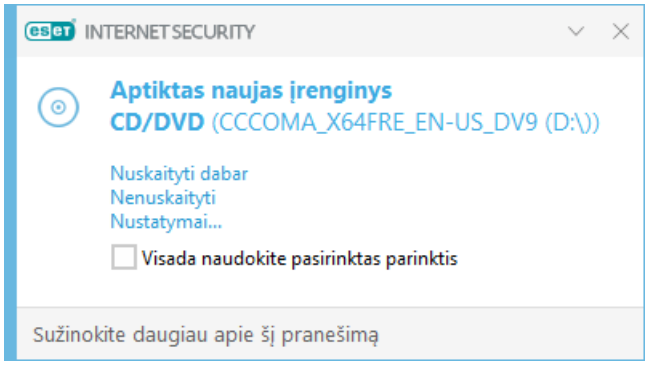
- **Žemesnis** – esant mažai sistemos apkrovai,

- **Įprastas** – esant vidutinei sistemos apkrovai.

Nešiojamoji laikmena

„ESET Internet Security“ atlieka automatinį nešiojamųjų laikmenų (CD / DVD / USB /...) nuskaitymą prijungus prie kompiuterio. Tai gali būti naudinga, jeigu kompiuterio administratorius nenori, kad naudotojai naudotų nešiojamąsias laikmenas su nepageidaujamu turiniu.

Kai prijungiama nešiojamoji laikmena ir nustatoma parinktis **Rodyti nuskaitymo parinktis**, pasirinkus Išplėstinis nustatymas > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nešiojamoji laikmena**, parodomas toks dialogo langas:



Šio dialogo parinktys:

- **Nuskaityti dabar** – galite paleisti nešiojamosios laikmenos nuskaitymą.

- **Nenuskaityti** – nešiojamoji laikmena nebus nuskaitoma.

- **Nustatymas** – atidaromas išplėstinis nustatymas.

- **Pasirinktą parinktį naudoti visada** – jei pasirinksite, tas pats veiksmas bus atliekamas kaskart prijungus nešiojamąją laikmeną.

Be to, ESET Internet Security turi įrenginių kontrolės funkciją, kurią naudojant galima apibrėžti išorinių įrenginių naudojimo taisykles konkrečiame kompiuteryje. Daugiau informacijos apie įrenginio kontrolę galima rasti skyriuje Įrenginių kontrolė.

Norėdami pasiekti nešiojamosios laikmenos nuskaitymo nustatymus, atidarykite Išplėstinis nustatymai > **Aptikimo modulis** > **Kenkėjiškos programinės įrangos nuskaitymai** > **Nešiojamoji laikmena**.

Veiksmas, atliekamas įdėjus nešiojamąją laikmeną – pasirinkite numatytąjį veiksmą, kuris bus atliekamas, kai nešiojamoji laikmena įdedama į kompiuterį (CD / DVD / USB). Pasirinkite pageidaujamą veiksmą įdėjus nešiojamąją laikmeną į kompiuterį:

- **Nenuskaityti** – jokie veiksmai nebus atliekami, o langas **Aptiktas naujas įrenginys** nebus atidarytas.
- **Automatinis įrenginio nuskaitymas** – bus atliktas kompiuterio, į kurį įdėta nešiojamoji laikmena, nuskaitymas.
- **Rodyti nuskaitymo parinktis** – atidaro **nešiojamosios laikmenos** nustatymų skyrių.

Dokumentų apsauga

Dokumentų apsaugos funkcija prieš atidarant nuskaito „Microsoft Office“ dokumentus, kaip ir „Internet Explorer“ automatiškai atsisiųstus failus, pavyzdžiui, „Microsoft ActiveX“ elementus. Dokumentų apsauga pateikia papildomą apsaugos lygmenį šalia failų sistemos apsaugos realiuoju laiku ir gali būti išjungta, siekiant pagerinti efektyvumą sistemose, kuriose neapdorojamas didelis „Microsoft Office“ dokumentų kiekis.

Norėdami aktyvuoti dokumentų apsaugą, atidarykite Išplėstinis nustatymas > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Dokumentų apsauga** ir spustelėkite perjungiklį, esantį šalia **Įjungti dokumentų apsaugą**.

ThreatSense – išplėstinio nustatymo parinktys, pvz., failų plėtiniai, kuriuos norite valdyti, ir naudojami aptikimo metodai. Daugiau informacijos rasite ThreatSense.

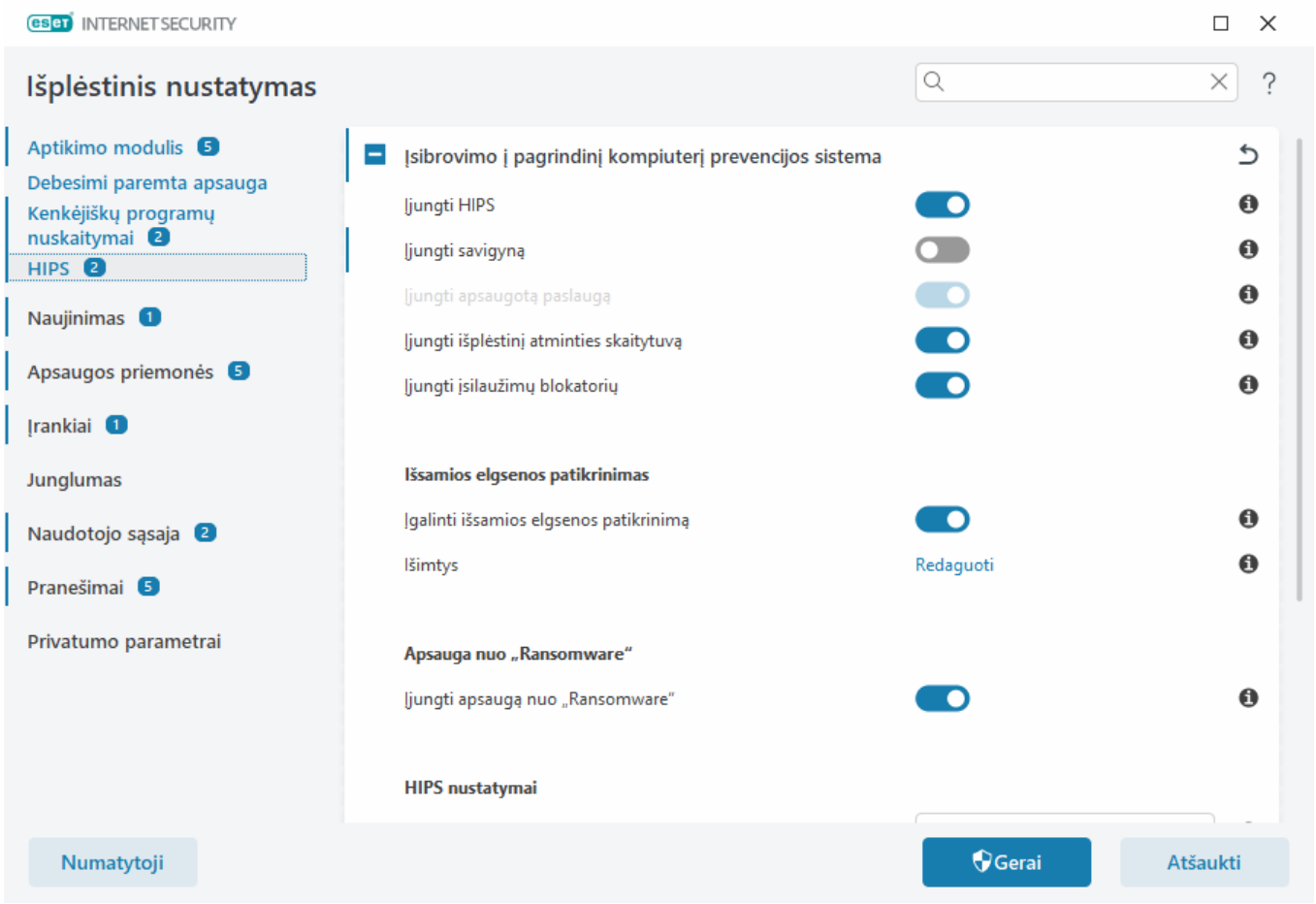
Šią funkciją suaktyvina programos, kurios naudoja „Microsoft Antivirus API““ (pvz., „Microsoft Office 2000“ ir naujesnės versijos arba „Microsoft Internet Explorer 5.0“ ir naujesnės versijos).

HIPS – Įsibrovimo į pagrindinį kompiuterį prevencijos sistema

HIPS parametrų keitimus gali atlikti tik patyręs vartotojas. Netinkamai sukonfigūravus HIPS parametrus gali būti paveiktas sistemos veikimo stabilumas.

Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS) saugo jūsų sistemą nuo kenkimo programinės įrangos ir nepageidaujamų veiksmų, bandančių neigiamai paveikti jūsų kompiuterį. HIPS naudoja išplėstinę veikimo analizę, suderintą su tinklo filtravimo aptikimo galimybėmis, kad būtų galima stebėti vykdomus procesus, failus ir registrų raktus. HIPS veikia atskirai nuo failų sistemos apsaugos realiuoju laiku ir nėra užkarda; ji tik stebi operacinėje sistemoje vykdomus procesus.

HIPS parametrus galite konfigūruoti pasirinkę Išplėstinis nustatymas > **Aptikimo modulis** > **HIPS** > **Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS)**. HIPS būsena (įjungta / išjungta) rodoma ESET Internet Security pagrindiniame programos lange > **Nustatymai** > **Kompiuterio apsauga**.



Įsibrovimo į pagrindinį kompiuterį prevencijos sistema

Įjungti HIPS – programoje ESET Internet Security HIPS yra įjungta pagal numatytuosius nustatymus. Išjungus HIPS išjungiamos visos kitos HIPS funkcijos, pvz., Įsilaužimų blokatorius.

Įjungti savigyną – ESET Internet Security yra integruota **Savigynos** technologija (HIPS funkcijos dalis), kuri neleidžia kenkėjiškai programinei įrangai sugadinti arba išjungti jūsų apsaugos nuo virusų ir šnipinėjimo programų. Savigynos technologija saugo svarbiausią sistemą ir ESET procesus, registrų raktus ir failus nuo sugadinimo.

Įjungti apsaugotą paslaugą – įjungia ESET tarnybos (ekrn.exe) apsaugą. Ją įjungus tarnyba paleidžiama kaip apsaugotas „Windows“ procesas apsaugai nuo kenkėjiškos programinės įrangos.

Įjungti išplėstinį atminties skaitytuvą – veikia kartu su spragų išnaudojimo blokatoriumi ir sustiprina apsaugą nuo kenkimo programinės įrangos, kuri buvo sukurta siekiant išvengti apsaugos nuo kenkimo programinės įrangos aptikimo, pasitelkiant klaidinimo arba šifravimo priemones. Išplėstinis atminties skaitytuvas būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Įjungti įsilaužimų blokatorių – sustiprina programas, į kurias įsilaužiama dažniausiai, pavyzdžiui, saityno naršykles, PDF skaitymo programas, el. pašto programas ir „MS Office“ komponentus. Įsilaužimų blokatorius būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Išsamios elgsenos patikrinimas

Įgalinti išsamios elgsenos patikrinimą – kitas apsaugos lygis, naudojamas kaip HIPS funkcija. Šis HIPS plėtinys analizuoja visų kompiuteryje veikiančių programų elgseną ir įspėja jus, jei proceso elgsena yra kenkėjiška.

HIPS išskyrimai iš išsamaus elgsenos patikrinimo leidžia į nuskaitymą neįtraukti procesų. Kad visi procesai būtų nuskaityti ieškant galimų grėsmių, išimtis rekomenduojame kurti tik kai tai visiškai būtina.

Apsauga nuo išpirkos reikalaujančių programų

Įjungti apsaugą nuo „Ransomware“ – tai dar vienas apsaugos lygmuo, kuris veikia kaip HIPS funkcijos dalis. Jei norite, kad apsauga nuo „Ransomware“ veiktų tinkamai, turite įjungti ESET LiveGrid® reputacijos sistemą. Skaitykite daugiau apie šio tipo apsaugą.

Įjungti Intel® Threat Detection Technology – padeda aptikti išpirkos reikalaujančių kenkėjų atakas naudodama išskirtinę „Intel“ procesoriaus telemetriją, kad padidintų aptikimo efektyvumą, sumažintų klaidingai teigiamų įspėjimų skaičių ir išplėstų matomumą, kad užfiksuotų pažangius vengimo metodus. Peržiūrėkite palaikomus procesorius.

HIPS nustatymai

Filtravimo režimas gali būti atliekamas vienu iš toliau nurodytų režimų:

Filtravimo režimas	Aprašymas
Automatinis režimas	operacijos yra leidžiamos, išskyrus blokuojamas iš anksto nustatytomis taisyklėmis, kurios apsaugo jūsų sistemą.
Išmanusis režimas	Vartotojas informuojamas tik apie labai įtartinus įvykius.
Interaktyvusis režimas	Vartotojas bus raginamas patvirtinti operacijas.
Politika pagrįstas režimas	blokuoja visas operacijas, kurios nėra apibrėžtos konkrečia ją leidžiančia taisykle.
Mokymosi režimas	Operacijos įjungiamos ir taisyklė sukuriama po kiekvienos operacijos. Šiuo režimu sukurtas taisykles galima peržiūrėti **HIPS taisyklių** rengyklėje, tačiau jų prioritetas yra mažesnis nei rankiniu būdu arba automatiniu režimu sukurtų taisyklių prioritetas. **Filtravimo režimo** išskleidžiamajame meniu pasirinkus **mokymosi režimą** atsiranda nustatymas **Mokymosi režimas bus išjungtas**. Pasirinkite laikotarpį, kuriam norite įjungti mokymosi režimą (ilgiausia trukmė yra 14 d.). Kai nurodytas laikotarpis pasibaigia, jūsų prašoma pakeisti taisykles, sukurtas HIPS veikiant mokymosi režimu. Galite pasirinkti ir kitą filtravimo režimą arba atidėti šį pasirinkimą ir toliau naudoti mokymosi režimą.

Režimas įjungiamas pasibaigus mokymosi režimo laikui – pasirinkite filtravimo režimą, kuris bus naudojamas pasibaigus mokymosi režimo laikui. Pasibaigus, parinktis **Teirautis naudotojo** prašo administratoriaus teisių, kad galėtų atlikti HIPS filtravimo režimo pakeitimą.

HIPS sistema stebi įvykius operacinėje sistemoje ir atitinkamai reaguoja, atsižvelgdama į taisykles, kurios yra panašios į užkardos naudojamas taisykles. Spustelėkite **Redaguoti** šalia **taisyklių**, kad būtų atidaryta **HIPS taisyklės HIPS** rengyklė. HIPS taisyklių lange galite pasirinkti, pridėti, redaguoti arba šalinti taisykles. Daugiau informacijos apie taisyklių kūrimą ir HIPS operacijas rasite skyriuje HIPS taisyklės redagavimas.

HIPS išskyrimai

Išskyrimai leidžia neįtraukti procesų iš HIPS išsamaus elgsenos patikrinimo.

Norėdami redaguoti HIPS išimtis, atidarykite Išplėstinis nustatymas > **Aptikimo modulis** > **HIPS** > **Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS)** > **Išimtys** > **Redaguoti**.

Nesupainiokite su Neįtraukti failų plėtiniai, Aptikimo išimtys, Našumo išimtys arba Procesų išimtys.

Norėdami neįtraukti objekto, spustelėkite **Pridėti** ir įveskite kelią į objektą arba pasirinkite jį medžio struktūroje. Taip pat galite redaguoti arba šalinti pasirinktus įrašus.

HIPS išplėstinis nustatymai

Šios parinktys naudingos derinant ir analizuojant programos veikimą:

Tvarkyklės, kurias leidžiama įkelti visada – pasirinktas tvarkykles įkelti leidžiama visada, neatsižvelgiant į sukonfigūruotą filtravimo režimą, nebent naudotojo taisyklė aiškiai tai užblokuotų.

Registruoti visas užblokuotas operacijas – visos užblokuotos operacijos bus įrašytos į HIPS žurnalą. Naudokite šią funkciją tik šalinant triktis arba paprašius ESET techninio palaikymo tarnybai, nes ji gali generuoti didžiulį žurnalo failą ir sulėtinti kompiuterį.

Pranešti, kai įvyksta pakeitimai paleidimo programose – rodo darbalaukio pranešimą kaskart, kai taikomoji programa įtraukiama arba pašalinama iš sistemos paleidimo.

Tvarkyklės, kurias leidžiama įkelti visada

Jei jos nėra aiškiai blokuojamos pagal vartotojo nustatytą taisyklę, šiame sąraše pateikiamas tvarkykles leidžiama įkelti visada, nesvarbu, koks naudojamas HIPS filtravimo režimas.

Pridėti – pridedama nauja tvarkyklė.

Redaguoti – redaguojama pasirinkta tvarkyklė.

Šalinti – tvarkyklė pašalinama iš sąrašo.

Nustatyti iš naujo – iš naujo įkeliamas sistemos tvarkyklių rinkinys.

Spustelėkite **Nustatyti iš naujo**, kad nebūtų įtrauktos rankiniu būdu jūsų pridėtos tvarkyklės. Tai gali būti naudinga, jei esate pridėję kelias tvarkykles ir negalite jų panaikinti iš sąrašo rankiniu būdu.

Po diegimo tvarkyklių sąrašas yra tuščias. „ESET Internet Security“ ilgainiui automatiškai užpildo sąrašą.

HIPS interaktyvusis langas

HIPS pranešimo lange galite sukurti taisyklę, paremtą naujais veiksmais, kuriuos aptinka HIPS, ir tada apibrėžti sąlygas, kuriomis leidžiamas arba uždraudžiamas šis veiksmas.

Pranešimo lange sukurtos taisyklės laikomos prilygstančiomis taisyklėms, sukurtoms rankiniu būdu. Taisyklė, sukurta pranešimo lange, gali būti ne tokia konkreti kaip šį dialogo langą suaktyvinusi taisyklė. Tai reiškia, kad, sukūrus taisyklę dialogo lange, tokia pati operacija gali suaktyvinti tą patį langą. Jei reikia daugiau informacijos, žr. HIPS taisyklių pirmenybė.

Jei numatytasis taisyklės veiksmas yra **Kaskart klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas. Galite pasirinkti **Uždrausti** arba **Leisti** operaciją. Jei per skirtą laiką nepasirinksite veiksmo, naujas veiksmas bus pasirinktas pagal taisykles.

Parinktis **Prisiminti, kol programa baigs darbą** leidžia naudoti veiksmą (**Leisti / drausti**) tol, kol bus pakeistos taisyklės ar filtravimo režimas, bus atnaujintas HIPS modulis ar sistema bus paleista iš naujo. Atlikus bet kuriuos iš šių trijų veiksmų laikinosios taisyklės bus panaikintos.

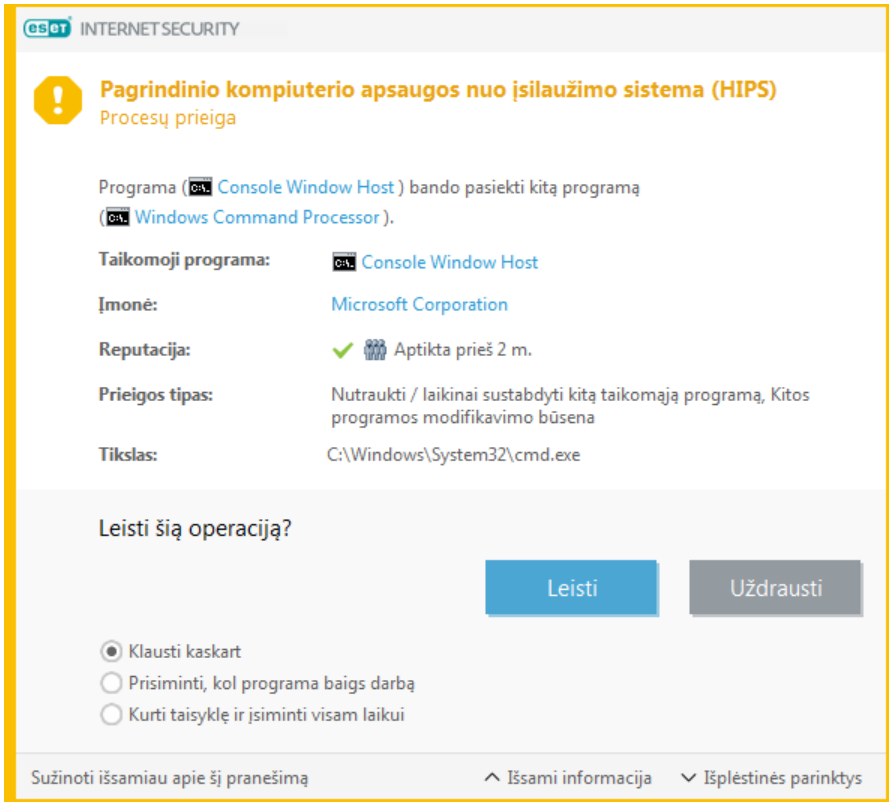
Parinktis **Kurti taisyklę ir įsiminti visam laikui** sukurs naują HIPS taisyklę, kurią vėliau galima pakeisti dalyje HIPS taisyklių tvarkymas (būtinos administratoriaus teisės).

Apačioje spustelėkite **Išsami informacija**, kad pamatytumėte kuri programa aktyvina operaciją, kokia failo reputacija arba kokią operaciją prašoma leisti arba drausti.

Išsamesnius taisyklės parametrų nustatymus pasieksite spustelėję **Išplėstinės parinktys**. Tolesnės parinktys pasiekiamos pasirinkus **Kurti taisyklę ir įsiminti visam laikui**:

- **Sukurti taisyklę, galiojančią tik šiai programai** – jei išvalote šį žymės langelį, taisyklė bus sukurta visoms šaltinio programoms.
- **Tik šiai operacijai** – pasirinkite taisyklės failą / programą / registro operaciją (-as). Žr. visų HIPS operacijų aprašus.
- **Tik šiam tikslui** – pasirinkite taisyklės failą / programą / registro tikslą (-us).

> **Nesibaigiantys HIPS pranešimai?**
> Norėdami, kad pranešimai nebebūtų rodomi, pakeiskite filtravimo režimą į **Automatinis režimas** dalyje Išplėstinis nustatymas > **Aptikimo modulis** > **HIPS** > **HIPS**.



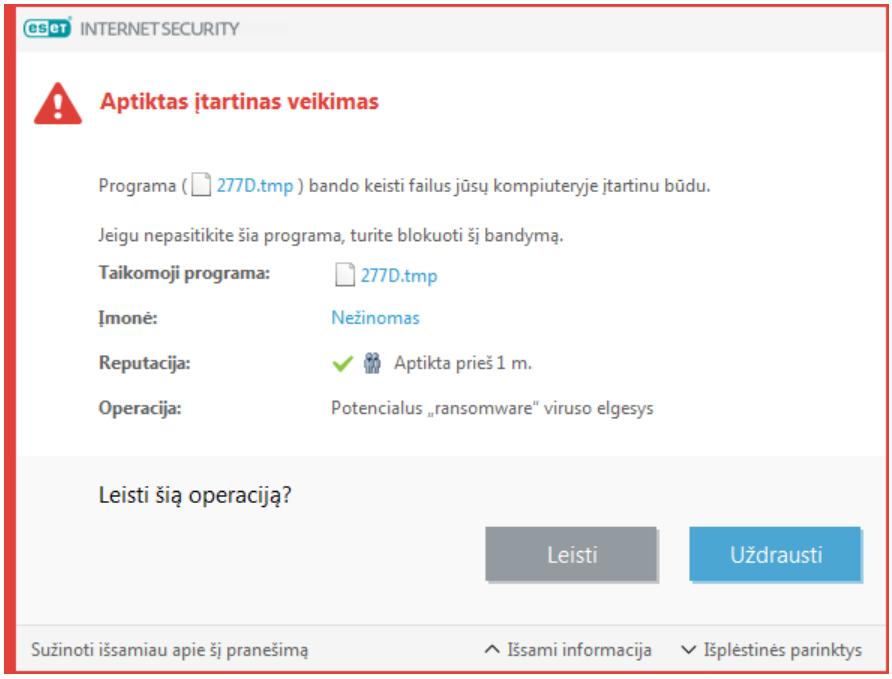
Mokymosi režimas užbaigtas

Mokymosi režimas automatiškai sukuria ir išsaugo taisykles. Visas sukurtas taisykles galite patikrinti HIPS taisyklių nustatymuose. Šį režimą geriausia naudoti pradinei HIPS konfigūracijai, tačiau jį reikia įjungti tik trumpą laiką. Nereikalingi jokie vartotojo veiksmai, nes ESET Internet Security įrašo taisykles pagal iš anksto nustatytus parametrus. Perjunkite į **interaktyvųjį** arba **politika pagrįstą režimą**, kai bus sukurtos visos būtinų operacinėje sistemoje veikiančių procesų taisyklės, kad būtų išvengta saugos pavojų.

Galite atidėti šį sprendimą, jei nenorite keisti nustatymų.

Aptiktas potencialus „Ransomware“ viruso elgesys

Šis interaktyvusis langas pasirodys, kai bus aptiktas „Ransomware“ viruso elgesys. Galite pasirinkti **Uždrausti** arba **Leisti** operaciją.



Spustelėkite **Išsami informacija** ir peržiūrėkite konkrečius aptikimo parametrus. Šiame dialogo lange galite **pateikti failą analizei** ar **neįtraukti į aptikimą**.

kad apsauga nuo „Ransomware“ viruso veiktų tinkamai, būtina įjungti ESET LiveGrid®.

HIPS taisyklių tvarkymas

Naudotojo apibrėžtų ir automatiškai įtrauktų taisyklių iš HIPS sistemos sąrašas. Daugiau informacijos apie taisyklių kūrimą ir HIPS operacijas galima rasti skyriuje HIPS taisyklių nustatymai. Taip pat žr. Bendrieji HIPS principai.

Stulpeliai

Taisyklė – vartotojo pasirinktas arba automatiškai sukurtas taisyklės pavadinimas.

Įjungta – išjunkite perjungiklį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos naudoti.

Veiksmas – taisykle apibrėžiamas veiksmas – **Leisti**, **Blokuoti** arba **Klausti** – kuris turi būti atliekamas esant tinkamoms sąlygoms.

Šaltiniai – taisyklė bus naudojama, tik jei įvykis suaktyvinamas šios (šių) taikomosios (-ųjų) programos (-ų).

Paskirtis – taisyklė bus naudojama tik tada, jei operacija yra susijusi su konkrečiu failu, programa ar registro įrašu.

Registravimo svarbumas – jei suaktyvinsite šią parinktį, informacija apie šią taisyklę bus įrašyta į HIPS žurnalą.

Pranešti – suaktyvinus veiksmą apatiniame dešiniajame kampe pasirodys mažas pranešimo langas.

Valdymo elementai

Pridėti – sukuriama nauja taisyklė.

Redaguoti – leidžia redaguoti pasirinktus įrašus.

Šalinti – pašalinami pasirinkti įrašai.

HIPS taisyklių pirmenybė

HIPS taisyklių pirmenybės lygio negalima reguliuoti mygtukais aukštyn / žemyn (kaip Užkardos taisyklių, kurias galima vykdyti iš viršaus į apačią).

- Visos sukurtos taisyklės yra lygiavertės
- Kuo konkretesnė taisyklė, tuo didesnė pirmenybė (pvz., konkrečios programos taisyklė turi didesnę pirmenybę, nei taisyklė visoms programoms)
- HIPS turi didesnės pirmenybės vidinių taisyklių, kurios nėra jums pasiekiamos (pvz., negalite apeiti savigynos taisyklių)
- Jūsų sukurtos taisyklės, dėl kurių gali užstrigti operacinė sistema, nebus taikomos (jų pirmenybė bus mažiausia).

HIPS taisyklės redagavimas

Pirmiausia perskaitykite HIPS taisyklių valdymas.

Taisyklės pavadinimas – vartotojo pasirinktas arba automatiškai sukurtas taisyklės pavadinimas.

Veiksmas – nurodomas veiksmas – **Leisti**, **Blokuoti** arba **Klausti** – kuris turi būti atliekamas, kai tenkinamos nustatytos sąlygos.

Susijusios operacijos – turite pasirinkti operacijų tipą, kuriam bus taikoma taisyklė. Taisyklė bus naudojama tik šio tipo operacijoms ir pasirinktam tikslui.

Įjungta – išjunkite perjungiklį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos taikyti.

Registravimo svarbumas – jei suaktyvinsite šią parinktį, informacija apie šią taisyklę bus įrašyta į HIPS žurnalą.

Pranešti naudotojui – suaktyvinus veiksmą apatiniame dešiniajame kampe pasirodys mažas pranešimo langas.

Taisyklė sudaryta iš dalių, kurios apibūdina sąlygas, įjungiančias šią taisyklę:

Šaltinio programos– taisyklė bus naudojama, tik jei įvykį paleidžia ši (šios) programa (-os). Išskleidžiamajame meniu pasirinkite **Konkrečios programos** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visos programos** ir pridėti visas programas.

Tiksliniai failai – taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkretūs failai** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visi failai** ir pridėti visus failus.

Programos– taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkrečios programos** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visos programos** ir pridėti visas programas.

Registro įrašai– taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkretūs įrašai** ir spustelėkite **Pridėti**, kad įvestumėte rankiniu būdu, arba spustelėkite **Atidaryti registro rengyklę**, kad pasirinktumėte raktą iš registro. Be to, išskleidžiamajame meniu galite pasirinkti **Visi įrašai**, kad pridėtumėte visas programas.

> Kai kurios tam tikrų taisyklių iš anksto HIPS nustatytos operacijos negali būti užblokuotos ir yra leidžiamos pagal numatytuosius nustatymus. Be to, ne visos sistemos operacijos yra stebimos HIPS. HIPS stebi operacijas, kurios gali būti laikomos nesaugiomis.

Svarbių operacijų aprašai:

Failų operacijos

- **Naikinti failą** – taikomoji programa prašo leidimo naikinti tikslo failą.
- **Rašyti į failą** – programa prašo leidimo rašyti į tikslo failą.
- **Tiesioginė prieiga prie disko** – programa bando skaityti arba rašyti į diską nestandartiniu būdu, apeidama įprastas Windows procedūras. Taip gali būti modifikuojami failai netaikant atitinkamų taisyklių. Šią operaciją galima atlikti, kai kenkėjiška programa bando išvengti aptikimo, atsarginio saugojimo programinė įranga bando padaryti tikslią disko kopiją arba skaidinių tvarkyklė bando pertvarkyti disko tomus.
- **Diegti visuotinę trikčių gaudyklę** – susijusi su funkcija SetWindowsHookEx iš MSDN bibliotekos.
- **Įkelti tvarkyklę** – tvarkyklių diegimas ir įkėlimas į sistemą.

Programų operacijos

- **Derinti kitą programą** – derinimo modulis prijungiamas prie proceso. Derinant taikomąją programą galima peržiūrėti ir pakeisti daugelį jos veikimo detalių ir prieiti prie jos duomenų.
- **Sustabdyti kitų programų įvykiai** – šaltinio programa bando perimti įvykius, nukreiptus į konkrečią programą (pavyzdžiui, klaviatūros paspaudimų registravimo programa bando įrašyti naršyklės įvykius).
- **Nutraukti / laikinai sustabdyti kitą taikomąją programą** – laikinai sustabdo, tęsia arba nutraukia procesą (galima prieiga tiesiai iš „Process Explorer“ arba iš procesų polangio).
- **Pradėti naują taikomąją programą** – naujų programų arba procesų paleidimas.
- **Modifikuoti kitos programos būseną** – šaltinio programa bando rašyti į tikslo programos atmintį arba vykdyti kodą jos vardu. Ši funkcija gali būti naudinga norint apsaugoti svarbią programą konfigūruojant ją kaip tikslo programą taisyklėje, blokuojančioje šios operacijos naudojimą.

Registrų operacijos

- **Modifikuoti paleidimo parametrus** – visi parametrų, nurodančių, kurios programos bus vykdomos paleidžiant „Windows“, keitimai. Jie gali būti aptikti, pavyzdžiui, ieškant Run rakto „Windows“ registre.
- **Naikinti iš registro** – registro rakto arba jo reikšmės naikinimas.
- **Pervardyti registro raktą** – registrų raktų pervardijimas.

• **Keisti registrą** – kuriamos naujos registro rakto reikšmės, keičiamos esamos reikšmės, duomenys perkeliami į duomenų bazės medį arba nustatomos vartotojo ar grupės teisės registro raktams.

Įvesdami tikslą galite su tam tikrais ribojimais naudoti pakaitos simbolius. Vietoje konkretaus rakto registro kelyje galima naudoti simbolį „*“ (žvaigždutę). Pavyzdžiui, *HKEY_USERS*\software* gali reikšti *HKEY_USER\.default\software*, bet ne *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** yra negaliojantis registro rakto kelias. Registro rakto kelias, turintis „*“, reiškia „šis kelias arba bet koks kelias bet kuriame lygyje už šio simbolio“. Tai vienintelis būdas naudoti failų tikslų pakaitos simbolius. Pirmiausia bus įvertinama konkreti kelio dalis, tada kelias už pakaitos simbolio (*).

Jei sukursite labai bendrą taisyklę, bus parodytas įspėjimas apie šio tipo taisyklę.

Šiame pavyzdyje parodysime, kaip uždrausti nepageidaujamus konkrečios programos veiksmus:

1. Pavadinkite taisyklę ir pasirinkite **Blokuoti** (arba **Klausti**, jei norite pasirinkti vėliau) išskleidžiamajame meniu **Veiksmas**.

2. Įjunkite perjungiklį prie **Pranešti naudotojui**, kad pranešimas būtų rodomas kaskart pritaikius taisyklę.

3. Pasirinkite bent vieną operaciją dalyje **Aktualios operacijos**, kurioms bus taikoma taisyklė.

4. Spustelėkite **Kitas**.

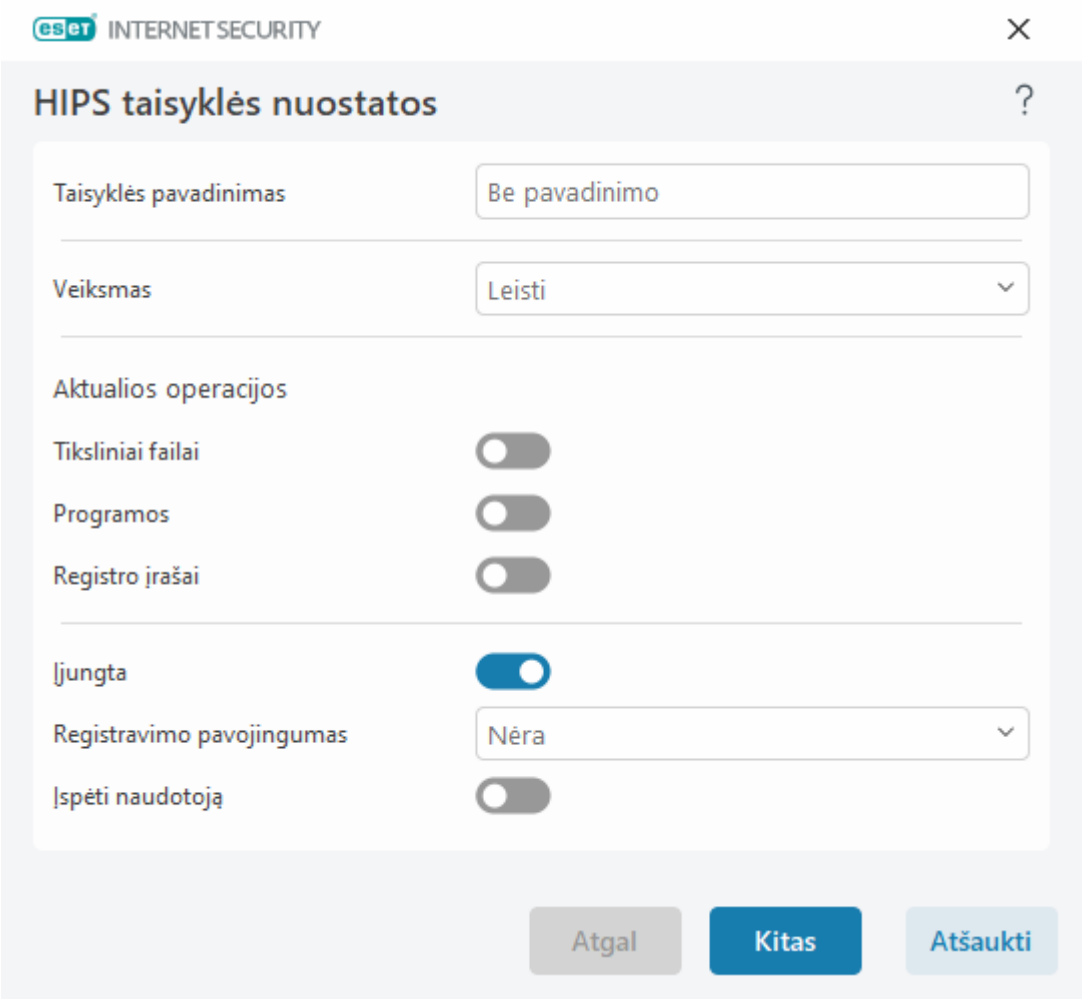
5. Lango **Šaltinio programos** išskleidžiamajame meniu pasirinkite **Konkrečios programos**, kad naują taisyklę pritaikytumėte visoms programoms, kurios bandys atlikti kurią nors iš pasirinktų programų operacijų.

6. Spustelėkite **Pridėti** ir **...**, kad pasirinktumėte konkrečios programos kelią, ir paspauskite **Gerai**. Jei norite, įtraukite daugiau programų.
Pavyzdžiui: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Pasirinkite operaciją **Rašyti į failą**.

8. Išskleidžiamajame meniu pasirinkite **Visi failai**. Taip užblokuosite ankstesniu veiksmu pasirinktos programos (-ų) bandymus įrašyti į failus.

9. Spustelėkite **Baigti**, kad naują taisyklę įrašytumėte.



Pridėti programos / registro kelią HIPS

Pasirinkite taikomosios programos failo kelią spustelėdami parinktį **...**. Pasirinkus aplanką, bus įtrauktos visos jame esančios programos.

Parinktis **Atverti registro rengyklę** paleis „Windows“ registrų rengyklę („RegEdit“). Pridėdami registro kelią, įveskite teisingą vietą į lauką **Reikšmė**.

Failo arba registro kelio pavyzdžiai:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Naujinti

Naujinimo nustatymų parinktys pasiekiamos pasirinkus Išplėstinis nustatymas > **Naujinimas**. Šiame skyriuje nurodoma naujinimo šaltinio informacija, tokia kaip naudojami naujinimo serveriai ir šių serverių autentiškumo patvirtinimo duomenys.

Naujinti

Šiuo metu naudojamas naujinimo profilis rodomas išskleidžiamajame meniu**Pasirinkti numatytąjį naujinimo profilį**.

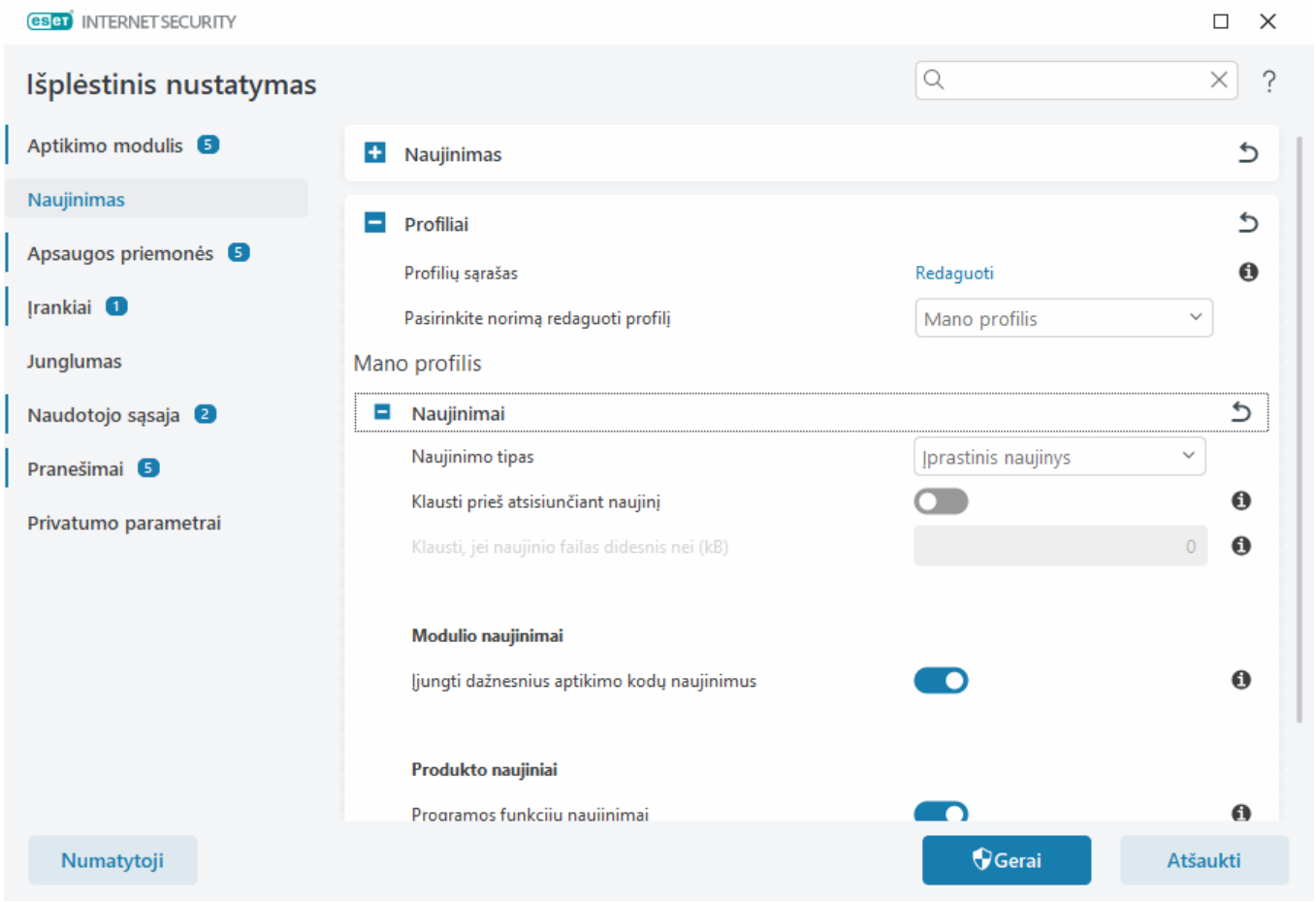
Norėdami sukurti naują profilį, žr. skyrių Profilių naujinimas.

Automatinis profilio perjungimas – leidžia priskirti naujinimo profilį konkrečiam tinklo ryšio profiliui.

Jei mėgindami atsisiųsti aptikimo modulį arba modulių naujinimus patiriate sunkumų, spustelėkite **Išvalyti** šalia **Išvalyti naujinimo podėlį**, kad išvalytumėte laikinuosius naujinimo failus / podėlį.

Modulio atšaukimas

Jei įtariate, kad naujas aptikimo modulio ir (arba) programos modulio naujinimas gali būti nestabilus arba sugadintas, galite atšaukti keitimus į ankstesnę versiją ir išjungti visus pasirinkto laikotarpio naujinimus.



Kad naujinimai būtu atsisiunčiami tinkamai, labai svarbu teisingai įvesti visus naujinimo parametrus. Jei naudojate užkardą, įsitikinkite, kad jūsų ESET programai leidžiama jungtis prie interneto (t. y. leidžiamas HTTP ryšys).

Profiliai

Naujinimų profiliai gali būti sukurti įvairioms naujinimų konfigūracijoms ir užduotims. Kurti naujinimų profilius yra labai naudinga mobiliųjų vartotojams, kuriems reikalingas alternatyvus profilis, atitinkantis nuolat besikeičiančias interneto ryšio ypatybes.

Išskleidžiamajame meniu **Pasirinkti redaguojamą profilį** rodomas šiuo metu pasirinktas profilis, kuris pagal numatytuosius nustatymus nustatomas kaip **Mano profilis**. Jei norite sukurti naują profilį, šalia **Profilių sąrašas** spustelėkite **Redaguoti**, įveskite savo **Profilio pavadinimą** ir spustelėkite **Pridėti**.

Naujinimai

Pagal numatytuosius nustatymus nustatyta parinkties **Naujinimo tipas** vertė yra **Reguliarus naujinimas**, kad naujinimo failai būtų automatiškai atsisiunčiami iš ESET serverio, kai tinklo srautas mažiausias. Išankstinio leidimo naujinimai (parinktis **Išankstinio leidimo naujinimas**) yra naujinimai, kuriems atliktas vidinis tikrinimas ir kurie bus greitai pateikti viešai. Įjungę išankstinio leidimo naujinimus galite pasinaudoti jų privalumais, gavę prieigą prie naujausių aptikimo metodų ir taisymų. Tačiau išankstinio leidimo naujinimai gali būti nepakankamai stabilūs visą laiką ir NETURĖTŲ būti naudojami gamybos serveriuose ir kompiuteriuose, kur reikalingas maksimalus prieinamumas ir stabilumas.

Klausti prieš atsisiunčiant naujinimą – programoje bus rodomas pranešimas, kuriame galėsite patvirtinti arba atsisakyti naujinimų failų atsisiuntimo.

Klausti, jei naujinimo failo dydis viršija (kB) – jei naujinimo failo dydis viršija nurodytą vertę, programa rodys patvirtinimo dialogo langą. Jei naujinimo failo dydis yra nustatytas į 0 kB, programa visada rodys patvirtinimo dialogo langą.

Modulių naujinimai

Įjungti dažnesnius aptikimo parašų naujinimus – aptikimo parašai bus naujinami trumpesniais intervalais. Šio parametro išjungimas gali neigiamai paveikti aptikimo spartą.

Produkto naujinimai

Programos funkcijų atnaujinimai – automatiškai įdiekite naujas ESET Internet Security versijas.

Ryšio parinktys

Norėdami naudoti tarpinį serverį naujinimams atsisiųsti, žr. dalį Ryšio parinktys.

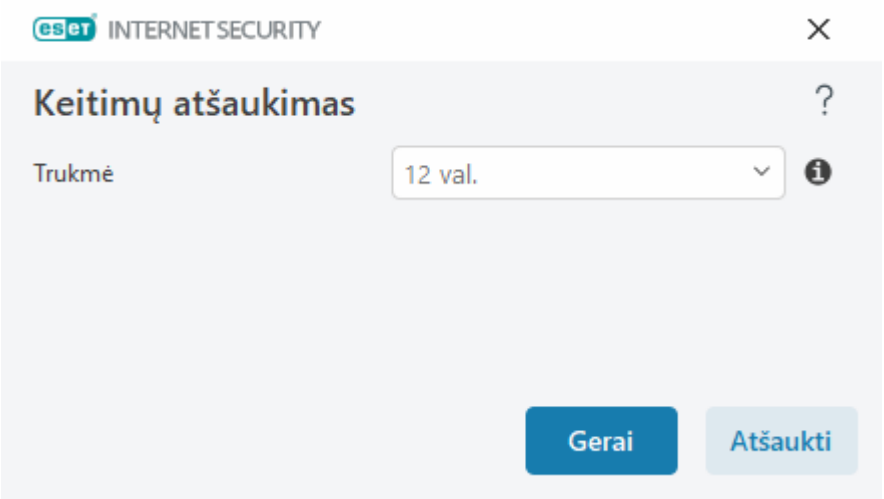
Naujinimo atšaukimas

Jei įtariate, kad naujas aptikimo modulio naujinimas arba programos moduliai gali būti nestabilūs arba sugadinti, galite atšaukti keitimus į ankstesnę versiją ir laikinai išjungti naujinimus. Arba galite įjungti anksčiau išjungtus naujinimus, jeigu atidėjote juos neapibrėžtam laikui.

ESET Internet Security įrašo aptikimo modulio ir programos modulių, naudojamų su keitimų atšaukimo funkcija, momentines kopijas. Norėdami sukurti virusų duomenų bazės momentines kopijas, **įjunkite modulių momentines kopijas.** Įgalinus **modulių momentinių kopijų kūrimą,** pirmojo naujinimo metu sukuriama pirmoji momentinė kopija. Kita sukuriama po 48 valandų. Lauke **Vietoje saugomų momentinių kopijų skaičius** apibrėžiamas išsaugotų aptikimo modulio momentinių kopijų skaičius.

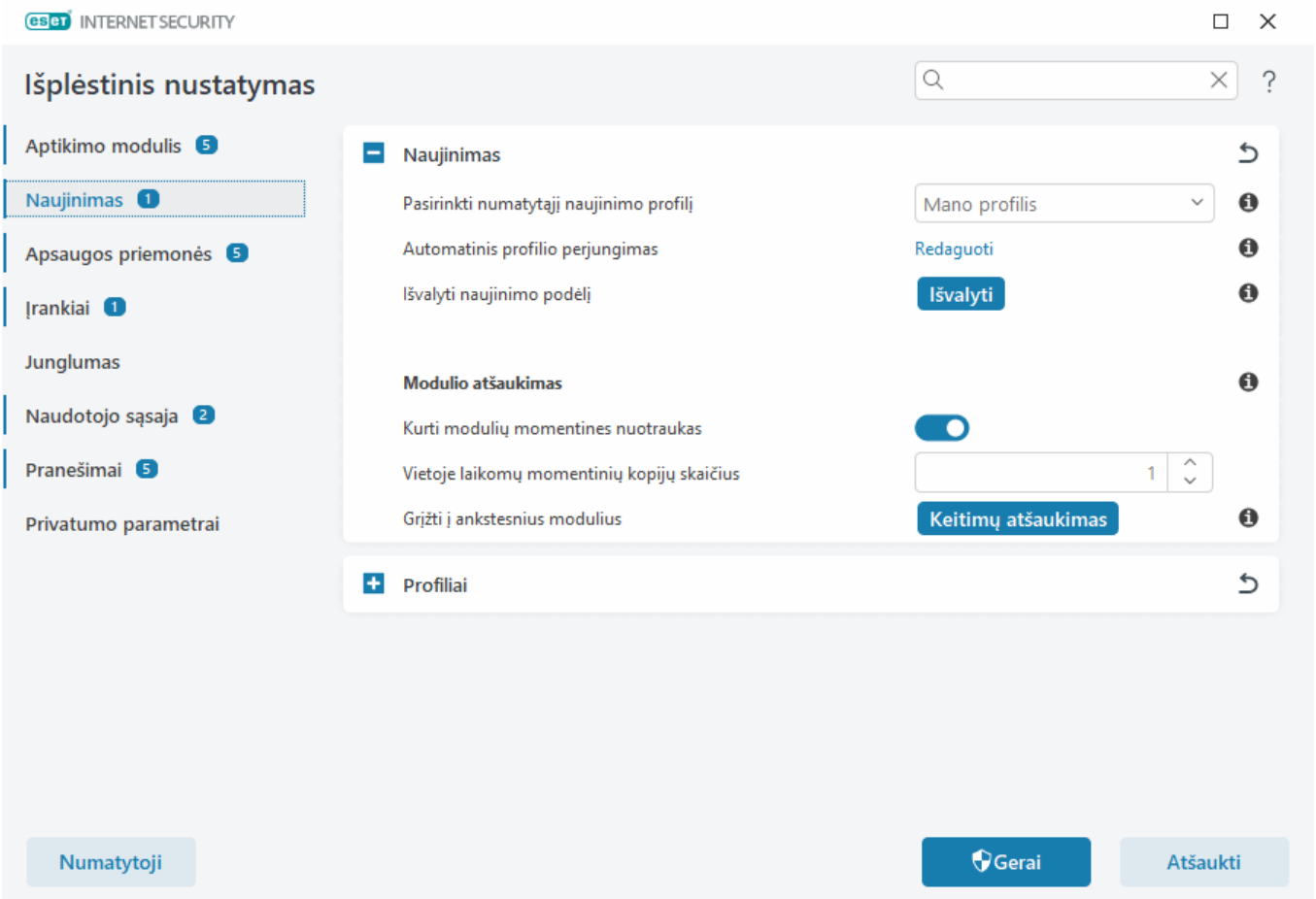
> Pasiekus maksimalų momentinių kopijų kiekį (pvz., tris), seniausia momentinė kopija kas 48 valandas pakeičiama nauja momentinė kopija. ESET Internet Security grąžina aptikimo modulio ir programos modulio naujinimo versijas į seniausią momentinę kopiją.

Jei spustelėsite **Atšaukti pakeitimus** (Išplėstinis nustatymas > **Naujinimas** > **Naujinimas**), išskleidžiamajame meniu **Trukmė** turėsite pasirinkti laiko intervalą, nurodantį laikotarpį, kuriuo aptikimo modulio ir programos modulio naujinimai bus pristabdyti.



Pasirinkite **Kol bus atšaukta**, norėdami atidėti reguliarius naujinimus neribotam laikui, kol atkursite naujinimų funkcionavimą rankiniu būdu. Kadangi iškyla galima saugos rizika, ESET nerekomenduoja pasirinkti šios parinkties.

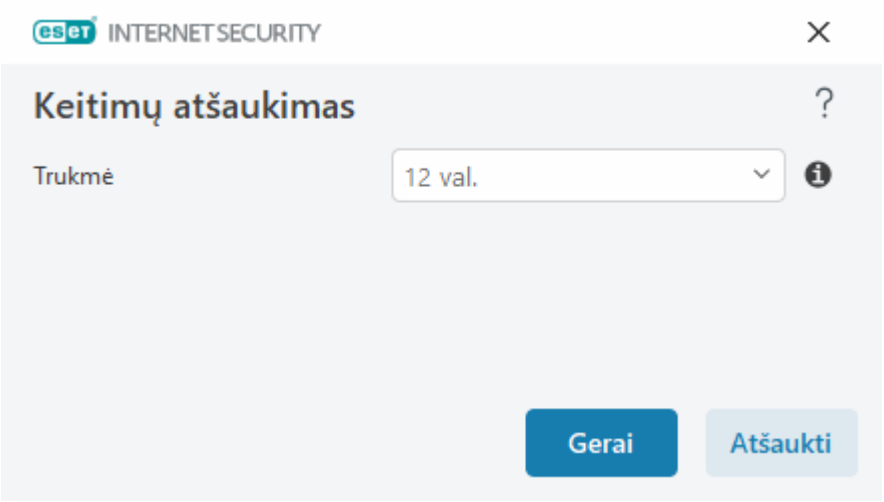
Atlikus keitimų atšaukimą, mygtukas **Atšaukti keitimus** pasikeičia į **Leisti naujinimus**. Naujinimai neleidžiami laikotarpiu, kuris buvo pasirinktas iš išskleidžiamojo meniu **Laikinai sustabdyti naujinimai**. Aptikimo modulio versija pakeista į seniausią galimą versiją ir saugoma kaip momentinė kopija vietinio kompiuterio failų sistemoje.



Tarkime, 22700 yra naujausias aptikimo modulio versijos numeris, o 22698 ir 22696 saugomos kaip aptikimo modulio momentinės kopijos. Atminkite, kad 22697 nepasiekiamas. Šiame pavyzdyje kompiuteris buvo išjungtas 22697 naujinimo metu, o naujesnis naujinimas buvo prieinamas prieš atsisiunčiant 22697. Jei lauko vertė **vietoje saugomos momentinės kopijos** yra du ir spustelite **Atšaukti keitimus**, aptikimo modulis (įskaitant programos modulius) atkuriamas į versijos numerį 22696. Šis procesas gali šiek tiek užtrukti. Patikrinkite, ar aptikimo modulio versija sumažinta ekrane Naujinimas.

Grąžinimo laiko intervalas

Jei spustelėsite **Atšaukti pakeitimus** (Išplėstinis nustatymas > **Naujinimas** > **Naujinimas**), išskleidžiamajame meniu **Trukmė** turėsite pasirinkti laiko intervalą, nurodantį laikotarpį, kuriuo aptikimo modulio ir programos modulio naujinimai bus pristabdyti.



Pasirinkite **Kol bus atšaukta**, norėdami atidėti reguliarius naujinimus neribotam laikui, kol atkursite naujinimų funkcionavimą rankiniu būdu. Kadangi iškyla galima saugos rizika, ESET nerekomenduoja pasirinkti šios parinkties.

Produkto naujinimai

Skiltyje **Produkto naujiniai** galite įdiegti naujus funkcijų atnaujinimus, kai jie pasiekiami automatiškai.

Programos funkcijų atnaujinimai suteikia naujų funkcijų arba pakeičia tas, kurios jau yra iš ankstesnių versijų. Tai gali būti atliekama automatiškai vartotojui neatliekant jokių veiksmų arba galite pasirinkti, kad jums apie tai praneštų. Įdiegus programos funkcijos atnaujinimą, gali reikėti iš naujo paleisti kompiuterį.

Programos funkcijų atnaujinimai – įgalinus programos funkcijų atnaujinimai bus atliekami automatiškai.

Ryšio parinktys

Norėdami pasiekti konkretaus naujinimo profilio įgaliotojo serverio sąrankos parinktis, atidarykite Išplėstinis nustatymas > **Naujinimas** > **Profiliai** > **Naujinimai** > **Ryšio parinktys**. Spustelėkite išskleidžiamąjį meniu **Įgaliotojo serverio režimas** ir nurodykite vieną iš šių trijų parinkčių:

- Nenaudoti įgaliotojo serverio
- Jungtis per įgaliotąjį serverį

- Naudoti visuotinius įgaliotojo serverio parametrus

Pasirinkite **Naudoti visuotinius įgaliotojo serverio nustatymus**, kad būtų naudojamos įgaliotojo serverio konfigūracijos parinktys, kurios jau nurodytos skiltyje Išplėstinis nustatymas > **Ryšys** > **Įgaliotasis serveris**.

Pasirinkite **Nenaudoti įgaliotojo serverio** ir nurodykite, kad įgaliotasis serveris nebus naudojamas naujinant ESET Internet Security.

Parinktį **Jungtis per įgaliotąjį serverį** reikia pasirinkti, jeigu:

- Kitas įgaliotasis serveris nei nurodytas Išplėstinis nustatymas > **Junglumas** naudojamas naujinant ESET Internet Security. Esant šiai konfigūracijai naujo įgaliojo serverio informaciją reikia nurodyti įvedant **Įgaliotojo serverio** adresą, ryšio **Prievadą** (pagal numatytuosius nustatymus – 3128) ir **Vartotojo vardą** bei **Slaptažodį** (jei reikia).

- Įgaliotojo serverio parametrai nėra nustatyti visuotinai, tačiau ESET Internet Security jungsis prie įgaliotojo serverio atliekant naujinimus.

- Jūsų kompiuteris yra prijungtas prie interneto per įgaliotąjį serverį. Parametrai paimami iš „Internet Explorer, kai diegiama programa, tačiau jei jie pakeičiami (pvz., jei pakeičiate interneto paslaugų teikėją), patikrinkite, ar šiame lange išvardyti įgaliotojo serverio parametrai yra teisingi. Kitaip programa negalės prisijungti prie naujinimo serverių.

Numatytasis įgaliotojo serverio nustatymas yra **Naudoti visuotinius įgaliotojo serverio parametrus**.

Jei įgaliotasis serveris nepasiekiamas, naudoti tiesioginį prisijungimą – jei įgaliotasis serveris nepasiekiamas, atliekant naujinimą jis bus apeinamas.

Šio skyriaus laukai **Vartotojo vardas** ir **Slaptažodis** yra skirti įgaliotajam serveriui. Užpildykite šiuos laukus, tik jei įgaliotajam serveriui pasiekti reikalingas vartotojo vardas ir slaptažodis. Šiuos laukus reikia pildyti, tik jei žinote, jog jums reikalingas slaptažodis jungiantis prie interneto per įgaliotąjį serverį.

Apsaugos priemonės

Apsauga nuo virusų saugo nuo kenkėjiškų sistemos atakų kontroliuodama failus, el. laiškus ir interneto ryšį. Pavyzdžiui, jei aptinkamas objektas, klasifikuojamas kaip kenkėjiška programinė įranga, prasidės valymas. Aptikimo priemonės gali pašalinti ją pirmiausiai užblokuodamos, tada valydamos, pašalindamos arba perkeldamos į karantiną.

Norėdami išsamiai sukonfigūruoti apsaugos priemones, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės**.

Apsaugos priemonių keitimus gali atlikti tik patyręs naudotojas. Netinkamai sukonfigūravus nustatymus gali sumažėti apsaugos lygis.

Šiame skyriuje:

- Aptikimo atsakymai
- Pranešimų nustatymai
- Apsaugos nustatymai

Aptikimo atsakymai

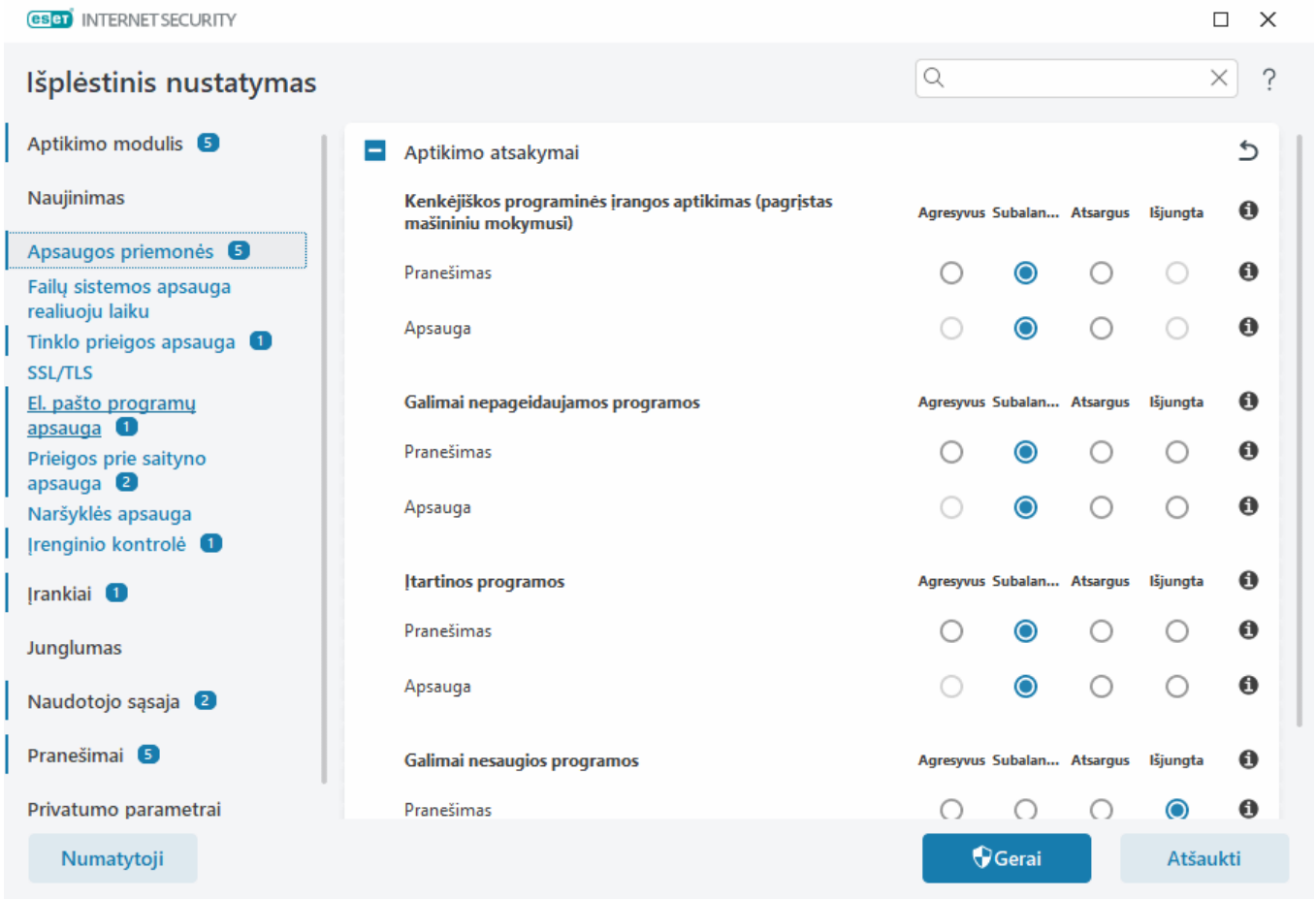
Aptikimo atsakymai leidžia konfigūruoti ataskaitų ir apsaugos lygius šioms kategorijoms:

- **Kenkėjiškos programinės įrangos aptikimas (pagrįstas mašininiu mokymusi)** – Kompiuterinis virusas yra kenkėjiško kodo dalis, kuri pridedama prie jūsų kompiuteryje esančių failų. Tačiau terminas „virusas“ dažnai naudojamas netinkamai. Tikslesnis terminas yra „kenkėjiška programinė įranga“. Kenkėjiškos programinės įrangos aptikimą vykdo aptikimo modulis kartu su mašininio mokymosi komponentu. Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.

- **Galimos nepageidaujamos programos** – „Grayware“ arba potencialiai nepageidaujamos programos (PUA) yra plati programinės įrangos kategorija, kurios tikslas nėra vienareikšmiškai kenkėjiškas, kaip kitų tipų kenkėjiškos programinės įrangos, pvz., virusų ar Trojos arklių. Visgi ji gali įdiegti nepageidaujamą papildomą programinę įrangą, pakeisti skaitmeninio įrenginio veikimo būdą ar atlikti veiksmus, kurių naudotojas nepatvirtino arba nesitiki. Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.

- **Įtartinomis programomis** – gali būti palaikytos pakavimo arba apsauginėmis programomis suglaudintos programos. Šio tipo apsaugos programas yra dažnai naudojamos kenkėjiškos programinės įrangos kūrėjų, siekiant išvengti aptikimo.

- **Galimai nesaugios programos**– yra teisėta komercinė programinė įranga, kuri gali būti netinkamai panaudota kenkimo tikslais. Galimai nesaugių programų (PUA) pavyzdžiais gali būti nuotolinės prieigos įrankiai, slaptažodžio iššifravimo ir klavišų registravimo programos (programos, įrašančios kiekvieną naudotojo klaviatūros klavišo paspaudimą). Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.



> **Pagerinta apsauga**
> Išplėstinis mašininis mokymasis dabar yra apsaugos priemonių dalis, kaip išplėstinis apsaugos sluoksnis, kuriuo pagerinamas aptikimas, grindžiamas mašininiu mokymusi. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Pranešimų nustatymai

Aptikimo atveju (pvz, aptinkama grėsmė, klasifikuojama kaip kenkėjiška programinė įranga), informacija užfiksuojama aptikimų žurnale ir pateikiami darbalaukio pranešimai, jei sukonfigūruota ESET Internet Security.

Pranešimų ribinė reikšmė konfigūruojama kiekvienai kategorijai (vadinamai „KATEGORIJA“):

1.Kenkėjiškų programų aptikimas

2.Galimai nepageidaujamos programos

3.Galimai nesaugu

4.Įtartinos programos

Pranešimus teikia aptikimo modulis, įskaitant mašininio mokymosi komponentą. Galite nustatyti aukštesnę pranešimo ribinę reikšmę, nei dabartinė apsaugos ribinė reikšmė. Šie pranešimo nustatymai nedaro įtakos objektų blokavimui, valymui arba naikinimui.

Prieš keisdami KATEGORIJOS pranešimų ribinę reikšmę (arba lygį), perskaitykite toliau pateiktą informaciją:

Ribinė reikšmė	Paaiškinimas
Agresyvi	Sukonfigūruotas didžiausias pranešimo apie KATEGORIJĄ jautrumas. Pranešama apie daugiau aptikimų. Esant **agresyviai** nuostatai, objektai gali būti klaidingai identifikuojami kaip KATEGORIJA.
Subalansuota	Sukonfigūruotas subalansuotas pranešimas apie KATEGORIJĄ. Ši nuostata leidžia subalansuoti našumą ir aptikimo tikslumą bei klaidingai praneštų objektų skaičių.
Atsargi	Pranešimas apie KATEGORIJĄ sukonfigūruotas taip, kad sumažintų klaidingai nustatytų objektų kiekį išlaikant pakankamą apsaugos lygį. Apie objektus pranešama tik tada, kai tikimybė yra didelė ir kai atitinka KATEGORIJOS veikimo kriterijus.
Išjungta	Pranešimas apie KATEGORIJĄ neaktyvus, o šio tipo aptikimų nėra ieškoma, apie juos nepranešama ir jie nėra valomi. Todėl ši nuostata išjungia apsaugą nuo šio aptikimo tipo. Pranešimo apie kenkėjišką programinę įrangą išjungti negalima ir tai yra numatytoji reikšmė galimai nesaugioms programoms.

ESET Internet Security apsaugos modulių galimumas

Apsaugos modulio galimumas (įjungta arba išjungta) pasirinktai KATEGORIJOS ribinei reikšmei yra:

	Agresyvi	Subalansuota	Atsargi	Išjungta*
Išplėstinis mašininio mokymosi modulis	✔ (agresyvus režimas)	✔ (atsargus režimas)	X	X
Aptikimo modulis	✔	✔	✔	X
Kiti apsaugos moduliai	✔	✔	✔	X

* Nerekomenduojama.

Nustatykite programos versiją, programos modulio versijas ir kompiliavimo datas

1. Spustelėkite **Žinynas ir palaikymas** > **Apie ESET Internet Security**.
2. Ekrane **Apie** pirmoje teksto eilutėje rodomas jūsų ESET produkto versijos numeris.
3. Spustelėkite **Įdiegti komponentai**, norėdami peržiūrėti konkrečių modulių informaciją.

Svarbiausios pastabos

Kelios svarbiausios pastabos apie atitinkamų ribinių reikšmių nustatymą jūsų aplinkai:

- **Subalansuota** ribinė reikšmė rekomenduojama daugumai sąrankų.
- Kuo aukštesnė pranešimo ribinė reikšmė, tuo daugiau aptikimų, tačiau kartu didėja klaidingo objektų identifikavimo tikimybė.
- Neįmanoma užtikrinti 100 % aptikimų dažnio ir 0 % tikimybės išvengti nepavojingų objektų kategorizavimo kaip kenkėjiškos programinės įrangos.
- Naudokite naujausias ESET Internet Security ir jo modulių versijas, siekdami geriausios pusiausvyros tarp našumo bei aptikimo dažnių ir klaidingų pranešimų apie objektus.

Apsaugos nustatymai

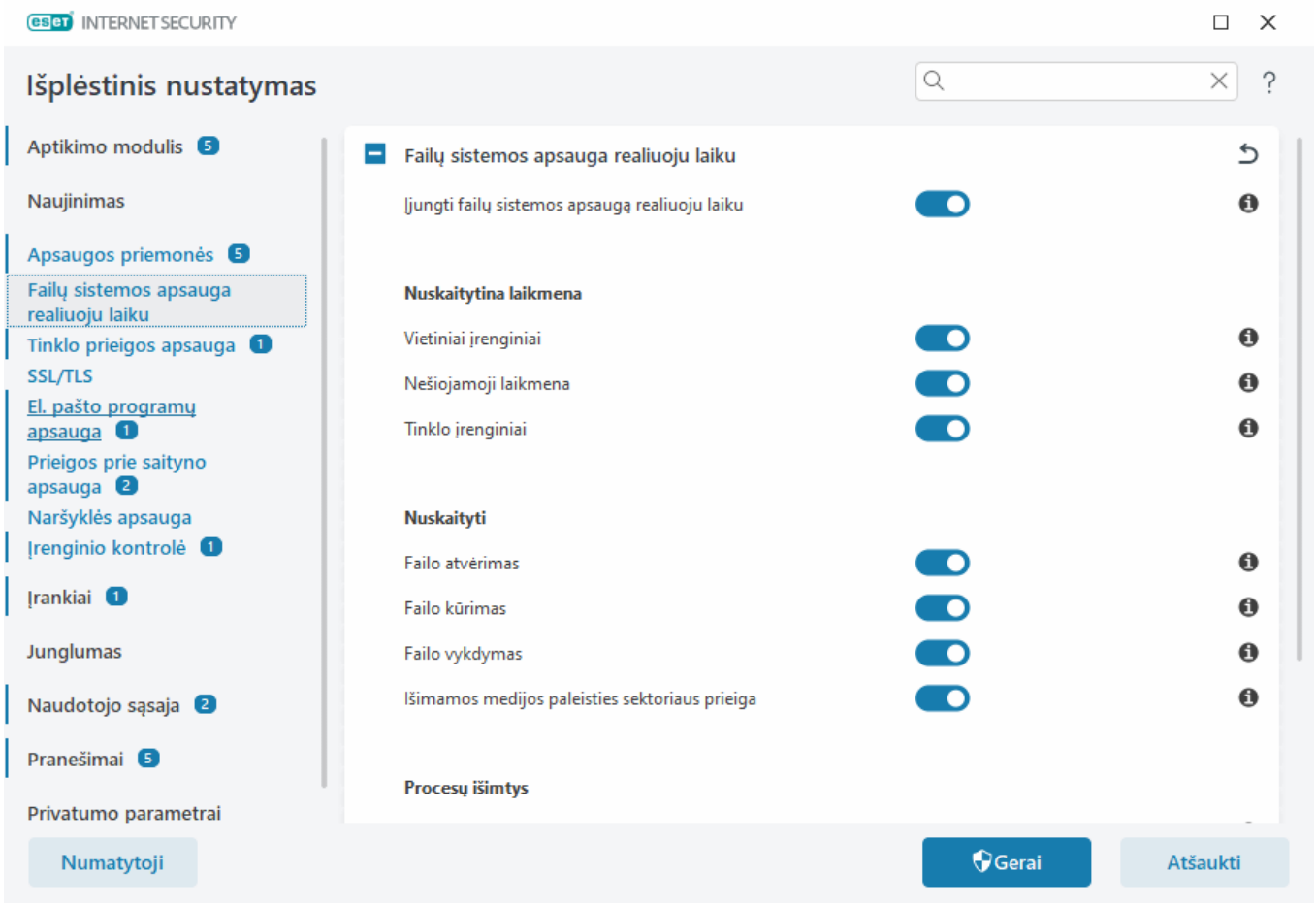
Jei pranešama apie objektą, klasifikuotą kaip KATEGORIJA, programa užblokuoja objektą ir išvalo, panaikina arba perkelia jį į karantiną.

Prieš keisdami KATEGORIJOS apsaugos ribinę reikšmę (arba lygį), perskaitykite toliau pateiktą informaciją:

Ribinė reikšmė	Paaiškinimas
Agresyvi	Pranešimai apie agresyvaus (arba žemesnio) lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas). Ši nuostata rekomenduojama, kai visi įrenginiai buvo nuskaityti taikant agresyvias nuostatas ir klaidingai pranešti objektai buvo pridėti prie aptikimo išimčių.
Subalansuota	Pranešimai apie subalansuoto (arba žemesnio) lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas).
Atsargi	Pranešimai apie atsargaus lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas).
Išjungta	Naudinga identifikuojant ir išskiriant klaidingai praneštus objektus. Apsaugos nuo kenkėjiškos programinės įrangos išjungti negalima ir tai yra numatytoji reikšmė galimai nesaugioms programoms.

Failų sistemos apsauga realiuoju laiku

Failų sistemos apsauga realiuoju laiku tikrina, ar nėra kenkėjiško kodo, atidarant, kuriant arba paleidžiant visus sistemos failus.



Pagal numatytuosius nustatymus failų sistemos apsauga realiuoju laiku įjungiama paleidžiant sistemą ir atlieka nepertraukiamą nuskaitymą. Nerekomenduojame išjungti **Įjungti failų sistemos apsauga realiuoju laiku**, kurią rasite Išplėstinis nustatymas > **Apsaugos priemonės** > **Failų sistemos apsauga realiuoju laiku** > **Failų sistemos apsauga realiuoju laiku**.

Nuskaitoma laikmena

Pagal numatytuosius nustatymus visų tipų laikmenos nuskaitomos ieškant galimų grėsmių:

- **Vietiniai įrenginiai** – nuskaito visus sisteminius ir fiksuotus standžiuosius diskus (pvz.: *C:*\, *D:*\).
- **Nešiojamoji laikmena** – nuskaito CD/DVD, USB laikmenas, atminties korteles ir pan.
- **Tinklo diskų įrenginiai** – nuskaito visus susietus tinklo diskų įrenginius (pvz.: *H:*\ kaip *store04*) arba tiesioginės prieigos tinklo diskų įrenginius (pvz.: *store08*).

Rekomenduojame naudoti numatytuosius parametrus ir keisti juos tik tam tikrais atvejais, pvz., jei kurios nors laikmenos nuskaitymas labai sulėtina duomenų persiuntimą.

Nuskaitymas įjungtas

Pagal numatytąją parinktį nuskaitomi visi atidaromi, sukuriami arba vykdomi failai. Rekomenduojame palikti numatytuosius nustatymus, nes jie užtikrina geriausią jūsų kompiuterio apsaugos realiuoju laiku lygį:

- **Failo atidarymas** – nuskaitoma failą atidarant.

- **Failo kūrimas** – nuskaitoma kuriant arba modifikuojant failą.
- **Failo vykdymas** – nuskaitoma vykdant arba paleidžiant failą.
- **Nešiojamosios laikmenos paleidimo sektoriaus prieiga** – kai prie įrenginio prijungiama nešiojamoji laikmena su paleidimo sektoriumi, iškart nuskaitomas paleidimo sektorius. Ši parinktis neįjungia nešiojamosios laikmenos failų nuskaitymo. Nešiojamosios laikmenos failų nuskaitymą rasite **Nuskaitoma laikmena** > **Nešiojamoji laikmena**. Kad **Nešiojamosios laikmenos paleidimo sektoriaus prieiga** veiktų tinkamai, **Paleidimo sektoriai / UEFI** turi būti įjungta „ThreatSense“.

Procesų išimtys

Žr. Procesų išimtys.

ThreatSense

Failų sistemos apsauga realiuoju laiku tikrina visų tipų laikmenas ir yra paleidžiama įvairių sistemos įvykių, pavyzdžiui, kai norima pasiekti failą. Naudojant „**ThreatSense**“ technologijos aptikimo metodus (kaip aprašyta skyriuje „ThreatSense“), failų sistemos apsauga realiuoju laiku gali būti sukonfigūruota skirtingai tvarkyti naujai sukurtus failus ir esamus failus. Pavyzdžiui, galite konfigūruoti failų sistemos apsaugą realiuoju laiku atidžiau stebėti naujai sukuriamus failus.

Kad būtų užtikrinta mažiausia įtaka sistemos našumui naudojant apsaugą realiuoju laiku, kartą nuskaityti failai pakartotinai nenuskaitomi (jeigu jie nebuvo pakeisti). Failai nuskaitomi dar kartą iškart po kiekvieno aptikimo modulio naujinimo. Šie veiksmai valdomi naudojant **Išmanųjį optimizavimą**. Jei funkcija **Išmanusis optimizavimas** išjungta, visi failai nuskaitomi kaskart juos pasiekiant. Norėdami pakeisti šį parametrą, atidarykite Išplėstiniai nustatymai > **Apsaugos priemonės** > **Failų sistemos apsauga realiuoju laiku**. Spustelėkite „**ThreatSense“** > **Kita** ir pažymėkite arba panaikinkite žymėjimą prie **Įjungti išmanųjį optimizavimą**.

Failų sistemos apsauga realiuoju laiku taip pat leidžia konfigūruoti Papildomus „ThreatSense“ parametrus.

Procesų išimtys

Procesų išimčių funkcija suteikia galimybę neįtraukti programos procesų į failų sistemos apsaugą realiuoju laiku. Kad būtų sparčiau kuriamos atsarginės kopijos, pagerintas procesų patikimumas ir paslaugų pasiekiamumas, atsarginių kopijų kūrimo metu naudojamos kai kurios technikos, kurios sukelia konfliktus su failų lygmens apsauga nuo kenkėjiškų programų. Vienintelis veiksmingas būdas išvengti šių situacijų yra išjungti apsaugos nuo kenkėjiškų programų programinę įrangą. Sukuriant konkrečių procesų išimtis (pavyzdžiui, išsprendžiančias atsarginės kopijos kūrimo problemas), nepaisoma visų su neįtrauktais procesais susijusių failų operacijų ir jos laikomos saugiomis, taip sumažinant trukdžius atsarginės kopijos kūrimo procesui. Rekomenduojame išimtis kurti atsargiai – į išimčių sąrašą įtrauktas atsarginių kopijų kūrimo įrankis gali pasiekti užkrėstus failus ir sukelti pavojaus signalą. Būtent todėl išplėstiniai leidimai leidžiami tik apsaugos realiuoju laiku moduliui.

> Nesupainiokite su Neįtraukti failų plėtiniai, HIPS išskyrimai, Aptikimo išimtys arba Našumo išimtys.

Procesų išimtys padeda sumažinti galimų konfliktų riziką ir padidina išimtinių programų našumą, o tai padidina bendrą operacinės sistemos našumą ir stabilumą. Proceso / programos išimtis yra jos vykdomojo failo (*.exe*) įtraukimas į išskyrimų sąrašą.

Galite įtraukti vykdomuosius failus į neįtrauktų procesų sąrašą pasirinkę Išplėstinis nustatymas > **Apsaugos**

priemonės > **Failų sistemos apsaugos realiuoju laiku** > **Failų sistemos apsaugos realiuoju laiku** > **Procesų išimtys**.

Ši funkcija buvo sukurta atsarginių kopijų kūrimo įrankių išimtims kurti. Neįtraukiant atsarginių kopijų kūrimo įrankio proceso į nuskaitymą ne tik užtikrinamas sistemos stabilumas, bet it nekenkiama atsarginių kopijų kūrimo našumui, nes vykdomas atsarginių kopijų kūrimas nestabdomas.

Spustelėkite **Redaguoti**, kad atidarytumėte valdymo langą **Procesų išimtys**, kuriame galite Pridėti išimtis ir ieškoti vykdomųjų failų (pvz., *Backup-tool.exe*), kurie nebus įtraukti į nuskaitymą.
Kai tik *.exe* failas įtraukiamas į išimtis, šio proceso veiklos nebestebi ESET Internet Security ir nebenuskaitomos jokios šio proceso vykdomos failų operacijos.

Jei pasirinkdami vykdomąjį proceso failą nesinaudojate naršymo funkcija, turite patys įvesti visą vykdomojo failo kelią. Antraip išimtis bus sukurta netinkamai ir HIPS gali pranešti apie klaidas.

Taip pat galite **Redaguoti** esamus procesus arba **Naikinti** juos išimčių sąraše.

Į šias išimtis neatsižvelgia saityno prieigos apsauga, todėl į išimčių sąrašą įtraukus saityno naršyklės vykdomąjį failą, atsisiųsti failai vistiek nuskaitomi. Taip apsaugoma nuo įsibrovimo. Tai tik pavyzdinis scenarijus ir mes nerekomenduojame kurti saityno naršyklių išimčių.

Pridėti arba redaguoti procesų išskyrimus

Šiame dialogo lange leidžiama **pridėti** procesus, neįtraukus į aptikimo modulį. Procesų išimtys padeda sumažinti galimų konfliktų riziką ir padidina išimtinių programų našumą, o tai padidina bendrą operacinės sistemos našumą ir stabilumą. Proceso / programos išimtis yra jos vykdomojo failo (*.exe*) įtraukimas į išskyrimų sąrašą.

Pasirinkite išskirtos programos failo kelią spustelėdami ... (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮRAŠYKITE programos pavadinimo.
Kai tik *.exe* failas įtraukiamas į išimtis, šio proceso veiklos nebestebi ESET Internet Security ir nebenuskaitomos jokios šio proceso vykdomos failų operacijos.

Jei pasirinkdami vykdomąjį proceso failą nesinaudojate naršymo funkcija, turite patys įvesti visą vykdomojo failo kelią. Antraip išimtis bus sukurta netinkamai ir HIPS gali pranešti apie klaidas.

Taip pat galite **Redaguoti** esamus procesus arba **Naikinti** juos išimčių sąraše.

Kada keisti apsaugos realiuoju laiku konfigūraciją

Apsauga realiuoju laiku yra svarbiausias komponentas, užtikrinantis sistemos saugą. Visada būkite atidūs keisdami jos parametrus. Rekomenduojame keisti jos parametrus tik tam tikrais atvejais.

Įdiegus ESET Internet Security, visi parametrai optimizuojami, kad būtų užtikrinamas maksimalus vartotojo sistemos saugumo lygis. Norėdami atkurti numatytuosius nustatymus, spustelėkite šalia Išplėstinis nustatymas > **Apsaugos priemonės** > **Aptikimo atsakymai**.

Apsaugos realiuoju laiku tikrinimas

Norėdami įsitikinti, kad apsauga realiuoju laiku veikia ir aptinka virusus, naudokite tikrinimo failą iš *www.eicar.com*. Šis tikrinimo failas yra nekenksmingas failas, kurį aptinka visos antivirusinės programos. Šį failą

sukūrė EICAR bendrovė (Europos kompiuterių antivirusinių programų tyrimo institutas – European Institute for Computer Antivirus Research), kad būtų galima patikrinti antivirusinių programų funkcionalumą.

Failą galima atsisiųsti čia http://www.eicar.org/download/eicar.com
Naršyklėje įvedę šį URL, turėtumėte pamatyti pranešimą, kad grėsmė pašalinta.

Ką daryti, jeigu apsauga realiuoju laiku neveikia

Šiame skyriuje apibūdiname problemas, kurių gali kilti naudojant apsaugą realiuoju laiku, ir kaip jas spręsti.

Apsauga realiuoju laiku išjungta

Jei naudotojas netyčia išjungia apsaugą realiuoju laiku, turėtumėte iš naujo aktyvinti šią funkciją. Norėdami iš naujo aktyvinti apsaugą realiuoju laiku, pagrindiniame programos lange eikite į **Nustatymas** ir spustelėkite **Kompiuterio apsauga** > **Failų sistemos apsauga realiuoju laiku**.

Jei apsauga realiuoju laiku nepaleidžiama paleidžiant sistemą, paprastai taip yra dėl to, kad išjungta parinktis **Paleisti failų sistemos apsaugą realiuoju laiku**. Norėdami užtikrinti, kad ši parinktis įjungta, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Failų sistemos apsauga realiuoju laiku**.

Jeigu apsauga realiuoju laiku neaptinka ir neišvalo įsiskverbimų

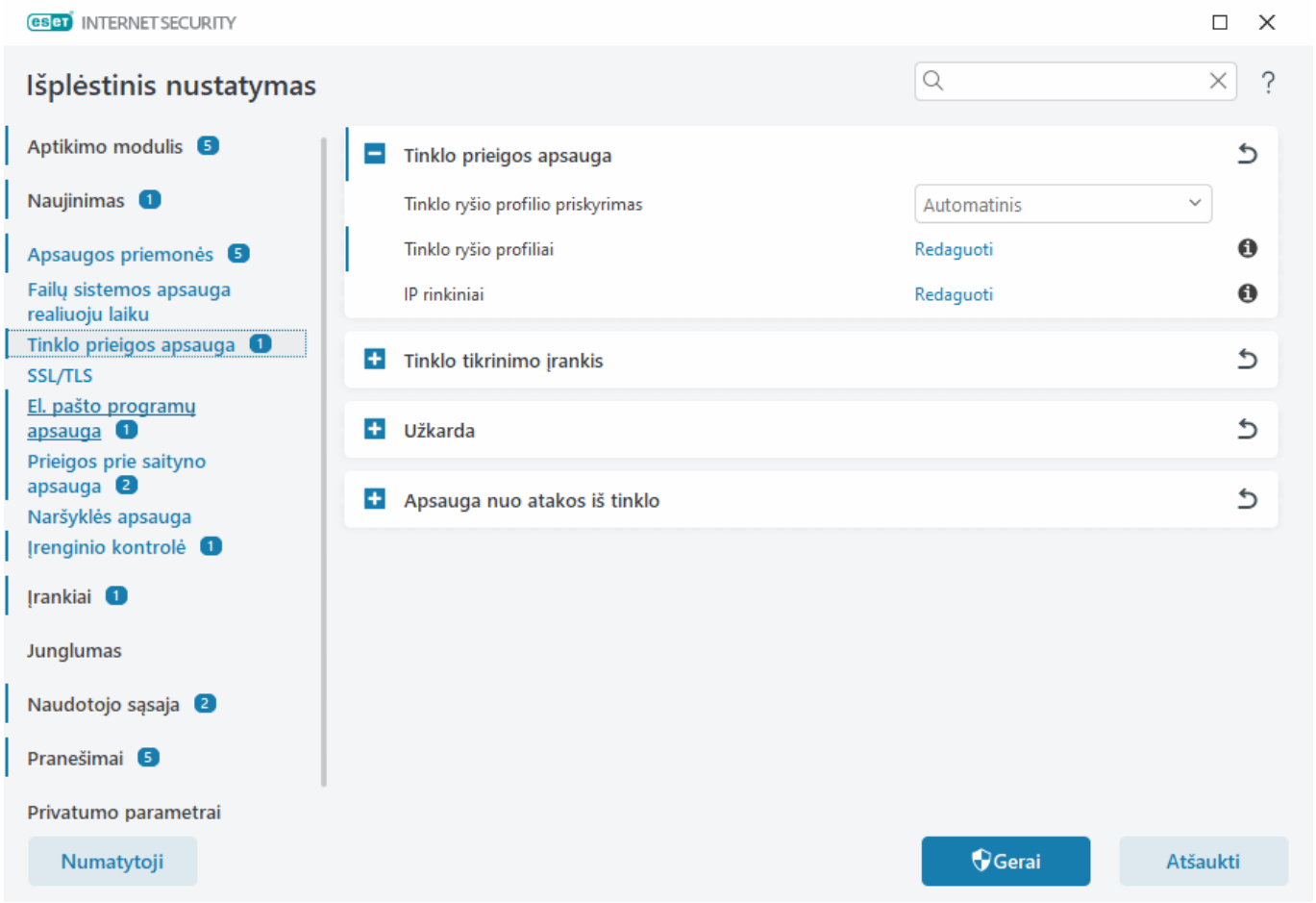
Įsitikinkite, kad kompiuteryje nėra įdiegta jokių kitų antivirusinių programų. Jei vienu metu yra įdiegtos dvi antivirusinės programos, jos gali būti nesuderinamos viena su kita. Rekomenduojame prieš įdiegiant ESET išdiegti visas kitas antivirusines programas savo sistemoje.

Apsauga realiuoju laiku nepaleidžiama

Jeigu apsauga realiuoju laiku nepaleidžiama paleidžiant sistemą (ir parinktis **Įjungti failų sistemos apsaugą realiuoju laiku** yra įjungta), gali būti, kad ji yra nesuderinama su kitomis programomis. Šiai problemai išspręsti sukurkite „ESET SysInspector“ žurnalą ir pateikite jį ESET techninės pagalbos tarnybai, kad ji atliktų analizę.

Tinklo prieigos apsauga

Tinklo prieigos apsauga leidžia išsamiai konfigūruoti visus tinklo ryšius. Galite leisti / uždrausti prieigą prie kompiuterio konkrečiuose tinkluose, leisti / uždrausti prieigą prie tinklo įrenginių iš savo kompiuterio ir dar daugiau, atsižvelgdami į konfigūraciją. Pagal numatytuosius nustatymus ESET Internet Security iš anksto sukonfigūravo užkardos taisykles ir tinklo prieigos apsaugą, kad būtų užtikrintas maksimalus saugumas. Tačiau konkrečioms aplinkoms gali reikėti pasirinktinės konfigūracijos. Numatytųjų nustatymų keitimą turėtų atlikti tik patyręs naudotojas.



Šiuos nustatymus galite konfigūruoti pasirinkę Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** (spustelėkite toliau pateiktus saitus, kad gautumėte išsamų kiekvienos tinklo prieigos apsaugos parinkties aprašą):

Tinklo prieigos apsauga

Tinklo ryšio profiliai – galite naudoti profilius, kad valdytumėte užkardos veikimą konkrečiuose tinklo ryšiuose.

IP rinkiniai – galite apibrėžti IP adresų rinkinius, kurie sukuria vieną loginę IP adresų grupę, kurią galite naudoti užkardos taisyklėms.

Tinklo tikrinimo įrankis

Užkarda

Tinklo apsauga nuo atakų

Tinklo ryšio profiliai

Profilius galima naudoti konkrečių tinklo ryšių ESET Internet Security tinklo apsaugos elgsenai valdyti. Kurdami arba redaguodami užkardos taisyklę, IDS taisyklę arba Apsaugos nuo grubios jėgos atakų taisyklę, galite priskirti ją konkrečiam profiliui arba taikyti visiems profiliams. Kai tinklo ryšyje aktyvus konkretus profilis, jam taikomos tik visuotinės taisyklės (taisyklės, nepriskirtos konkrečiam profiliui) ir taisyklės, kurios priskirtos tam profiliui. Norėdami paprastai keisti užkardos elgseną, galite sukurti įvairius profilius su įvairiomis taisyklėmis, priskirtomis tinklo ryšiams.

Tinklo ryšių profilius ir priskyrimus galite konfigūruoti dalyje Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Tinklo prieigos apsauga**.

Tinklo ryšio profilio priskyrimas – leidžia jums pasirinkti, ar naujai aptiktiems tinklo ryšiams yra automatiškai (išplečiamajame meniu pasirinkite **Automatinis**) priskiriamas iš anksto nustatytas arba pasirinktinis profilis, atsižvelgiant į aktyvatorius, sukonfigūruotus tinklo ryšio profiliuose, ar norite būti paprašyti (išplečiamajame meniu pasirinkite **Klausti**) atlikti tinklo apsaugos konfigūravimą ir priskirti profilį rankiniu būdu kiekvieną kartą, kai aptinkamas naujas tinklo ryšys.

Taip pat galite rankiniu būdu priskirti konkretų tinklo ryšio profilį pagrindiniame programos lange > **Nustatymai** > **Tinklo apsauga** > **Tinklo ryšiai**. Užveskite pelės žymeklį virš konkretaus tinklo ryšio ir spustelėkite meniu piktogramą ⋮ > **Redaguoti**, kad atidarytumėte langą Tinklo apsaugos konfigūravimas ir tada galite pasirinkti profilį.

Tinklo ryšio profiliai – spustelėkite **Redaguoti**, kad galėtumėte įtraukti arba redaguoti tinklo ryšio profilius.

Šie profiliai yra iš anksto apibrėžti ir jų negalima redaguoti / pašalinti:

Asmeninis – patikimam tinklui (namų arba biuro tinklui). Kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuteryje saugomus failus bei pasiekti sistemos išteklius (suteikta prieiga prie bendrinamų failų ir spausdintuvų, gaunamas RPC ryšys yra įgalintas ir leidžiama bendrinti nuotolinį darbalaukį). Rekomenduojame naudoti šį parametrą jungiantis prie saugaus vietinio tinklo. Šis profilis automatiškai priskiriamas tinklo ryšiui, jei jis sukonfigūruotas kaip domenas arba privatus tinklas Windows.

Viešasis – nepatikimam tinklui (viešajam tinklui). Failai ir aplankai jūsų sistemoje nėra bendrinami su kitais tinklo vartotojais arba nematomi kitiems vartotojams, o sistemos išteklių bendrinimas išjungiamas. Rekomenduojame naudoti šį parametrą, kai naudojatės belaidžiais tinklais. Šis profilis automatiškai priskiriamas bet kokiam tinklo ryšiui, kuris nesukonfigūruotas kaip domenas arba privatus tinklas Windows.

Kai tinklo ryšys persijungia į kitą profilį, apatiniame dešiniajame ekrano kampe pateikiamas pranešimas.

Tinklo ryšio profilių pridėjimas arba redagavimas

Tinklo ryšio profilius galite pridėti arba redaguoti pasirinkę Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Tinklo prieigos apsauga** > **Tinklo ryšio profiliai** > **Redaguoti**. Norėdami redaguoti profilį, turite jį pasirinkti iš lango **Tinklo ryšio profiliai** sąrašo.

Šie profiliai yra iš anksto nustatyti ir jų negalima redaguoti / ištrinti:

Asmeninis – patikimam tinklui (namų arba biuro tinklui). Kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuteryje saugomus failus bei pasiekti sistemos išteklius (suteikta prieiga prie bendrinamų failų ir spausdintuvų, gaunamas RPC ryšys yra įgalintas ir leidžiama bendrinti nuotolinį darbalaukį). Rekomenduojame naudoti šį parametrą jungiantis prie saugaus vietinio tinklo. Šis profilis automatiškai priskiriamas tinklo ryšiui, jei jis sukonfigūruotas kaip domenas arba privatus tinklas Windows.

Viešasis – nepatikimam tinklui (viešajam tinklui). Failai ir aplankai jūsų sistemoje nėra bendrinami su kitais tinklo vartotojais arba nematomi kitiems vartotojams, o sistemos išteklių bendrinimas išjungiamas. Rekomenduojame naudoti šį parametrą, kai naudojatės belaidžiais tinklais. Šis profilis automatiškai priskiriamas bet kokiam tinklo ryšiui, kuris nesukonfigūruotas kaip domenas arba privatus tinklas Windows.

Iš viršaus / aukštyn / žemyn / apačioje  – leidžia koreguoti tinklo ryšio profilių prioriteto lygį (Tinklo ryšio profiliai vertinami ir taikomi pagal jų prioritetą. Visada taikomas pirmasis atitikimo profilis).

Profilio pridėjimas arba redagavimas

Pasirinktinis tinklo ryšio profilis leidžia taikyti užkardos taisykles ir apibrėžti papildomus nustatymus konkretiems tinklo ryšiams. Skyriuje Aktyvatoriai nurodysite, kuriems tinklo ryšiams bus priskirtas pasirinktinis profilis.

Norėdami atidaryti profilio rengyklę, lange **Tinklo ryšio profiliai**:

- Spustelėkite **Pridėti**.
- Pasirinkite vieną iš esamų profilių ir spustelėkite **Redaguoti**.
- Pasirinkite vieną iš esamų profilių ir spustelėkite **Kopijuoti**.

Pavadinimas – pasirinktinis profilio pavadinimas.

Aprašas – profilio aprašas, padedantis identifikuoti profilį.

Papildomi patikimi adresai – čia apibrėžti adresai įtraukiami į tinklo ryšio, kuriam taikomas šis profilis, patikimą zoną (neatsižvelgiant į tinklo apsaugos tipą).

Patikimas ryšys – kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuterį saugomus failus bei pasiekti sistemos išteklius (suteikta prieiga prie bendrinamų failų ir spausdintuvų, gaunamas RPC ryšys yra įgalintas ir leidžiama bendrinti nuotolinį darbalaukį). Rekomenduojame naudoti šį nustatymą kuriant saugaus vietinio tinklo ryšio profilį. Visi tiesiogiai prijungti tinklo potinkliai taip pat laikomi patikimais. Pavyzdžiui, jei prie šio tinklo prijungtas tinklo adapteris, kurio IP adresas yra 192.168.1.5, o potinklio kaukė yra 255.255.255.0, tuomet prie adapterio patikimosios zonos bus pridėtas potinklis 192.168.1.0/24. Jei adapteris turi daugiau adresų / potinklių, visi jie bus patikimi.

Pranešti apie silpną „WiFi“ šifravimą – ESET Internet Security pateiks darbalaukio pranešimą, kai prisijungsite prie neapsaugoto belaidžio tinklo arba tinklo su silpna apsauga.

Aktyvatoriai – pasirinktinės sąlygos, kurias reikia įvykdyti norint priskirti šį tinklo ryšio profilį tinklo ryšiui. Išsamų paaiškinimą žr. Aktyvatoriai.

Aktyvatoriai

Aktyvatoriai yra pasirinktinės sąlygos, kurios turi būti įvykdytos norint tinklo ryšio profilį priskirti tinklo ryšiui. Jei prijungtas tinklas turi tuos pačius duomenis, kurie nustatyti prijungto tinklo profilio aktyvatoriuose, profilis bus taikomas tinklui. Tinklo ryšio profilyje gali būti vienas arba keli aktyvatoriai. Jei yra keli aktyvatoriai, taikoma OR logika (turi būti įvykdyta bent viena sąlyga). Aktyvatorius galite nustatyti Tinklo ryšio profilio rengyklėje. Pasirinktinius tinklo ryšio profilius turėtų kurti patyręs naudotojas.

Galimi šie aktyvatoriai (jei norite sužinoti išsamią informaciją apie dabartinį tinklą, žr. Tinklo ryšiai):

Adapteris

Adapterio tipas – taikykite profilį, jei tinklo ryšys užmegztas pasirinktam adapterio tipui.
Adapterio pavadinimas – taikykite profilį, jei tinklo adapterio pavadinimas sutampa.
Adapterio IP – taikykite profilį, jei sutampa jūsų tinklo adapterio IP adresas.

DNS

DNS plėtinys – taikykite profilį, jei domeno pavadinimas sutampa.
DNS IP – taikykite profilį, jei DNS serverio IP adresas sutampa.

WINS

Taikykite profilį, jei susietasis Windows Internet Name Service (WINS) IP adresas sutampa.

DHCP

DHCP IP – sutampa su DHCP serverio IP adresu.

Numatytasis šliuzas

IP – taikykite profilį, jei sutampa numatytojo šliuzo IP adresas.
MAC adresas – taikykite profilį, jei sutampa numatytojo šliuzo MAC adresas.

„Wi-Fi“

SSID – taikykite profilį, jei SSID („Wi-Fi“ pavadinimas) sutampa.
Profilio pavadinimas – taikykite profilį, jei „Wi-Fi“ profilio pavadinimas sutampa.
Saugos tipas – taikykite profilį, jei saugos tipas sutampa su tuo, kuris pasirinktas išplečiamajame meniu. Jei norit, kad sutaptų su daugiau nei vienu, sukurkite kitą aktyvatorių.
Šifravimo tipas – taikykite profilį, jei šifravimo tipas sutampa su tuo, kuris pasirinktas išplečiamajame meniu. Jei norit, kad sutaptų su daugiau nei vienu, sukurkite kitą aktyvatorių.
Tinklo sauga – taikykite profilį, jei tinklas yra **Atidarytas** / **Apsaugotas**.

„Windows“ profilis

Taikyti profilį, jei tinklas sukonfigūruotas sistemoje „Windows“ kaip **Domenas** / **Privatus** / **Viešasis**.

Autentiškumo patvirtinimas

Tinklo autentiškumo patvirtinimo funkcija ieško konkretaus serverio tinkle ir to serverio autentiškumui patvirtinti naudoja asimetrinio šifravimo būdą (RSA). Autentifikuojamas tinklo pavadinimas turi sutapti su autentifikavimo serverio nustatymuose nustatytu pavadinimu. Pavadinime skiriamos didžiosios ir mažosios raidės. Serverio pavadinimą galima įvesti kaip IP adresą, DNS arba NetBios pavadinimą.
Atsisiųskite „ESET Authentication Server“
Viešasis raktas gali būti importuojamas naudojant bet kurį iš šių failų tipų:
• PEM šifruotas viešasis raktas (.pem); šį raktą galite sugeneruoti naudodami „ESET Authentication Server“
• Šifruotas viešasis raktas
• Viešojo rakto sertifikatas („.crt“)
Spustelėkite **Bandyti** , kad išbandytumėte savo parametrus. Jei autentiškumo patvirtinimas sėkmingas, rodoma Serverio autentiškumo patvirtinimas buvo sėkmingas. Jei atpažinimas nėra tinkamai sukonfigūruotas, bus parodytas vienas iš šių klaidos pranešimų:
Serverio atpažinimas nesėkmingas. Negalioja arba nesutampa parašas.
Serverio parašas neatitinka įvesto viešojo rakto.
Serverio atpažinimas nesėkmingas. Tinklo pavadinimas nesutampa.
Sukonfigūruoto tinklo pavadinimas neatitinka autentiškumo patvirtinimo serverio tinklo pavadinimo. Peržvelkite abu pavadinimus ir užtikrinkite, kad jie būtų identiški.
Serverio atpažinimas nesėkmingas. Negauta atsakymo iš serverio arba gautas negaliojantis atsakymas. Atsakymo negaunama, jei serveris neveikia arba yra nepasiekiamas. Negaliojantis atsakymas gali būti gautas, jei nurodytu adresu veikia kitas HTTP serveris.
Įvestas negaliojantis viešasis raktas.
Patikrinkite, ar jūsų įvestas viešasis raktas nėra sugadintas.

IP rinkiniai

IP rinkinys yra IP adresų rinkinys, sukuriantis vieną loginę IP adresų grupę, naudingas pakartotinai naudojant tą patį adresų rinkinį keliose užkardos taisyklėse arba apsaugos nuo grubios jėgos atakos taisyklėse. ESET Internet Security taip pat yra iš anksto nustatytų IP rinkinių, kuriems taikomos vidaus taisyklės. Vienas iš tokios grupės pavyzdžių yra **Patikima zona**. Patikima zona nurodo tinklo adresų grupę kiti tinklo naudotojai gali matyti jūsų kompiuterį ir jūsų kompiuteryje saugomus failus bei pasiekti sistemos išteklius.

Norėdami įtraukti IP rinkinį:

1. Atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **IP rinkiniai** > **Redaguoti**.

2. Spustelėkite **Įtraukti**, įveskite zonos **pavadinimą** ir **aprašymą** ir įveskite nuotolinį IP adresą laukelyje **Nuotolinio kompiuterio adresas (IPv4/IPv6, diapazonas, šablonas)**.

3. Spustelėkite **Gerai**.

Daugiau informacijos ieškokite IP rinkinių redagavimas.

IP rinkinių redagavimas

Daugiau informacijos apie IP rinkinius, rasite IP rinkiniai.

Stulpeliai

Pavadinimas – nuotolinių kompiuterių grupės pavadinimas.

Aprašas – bendras grupės aprašas.

IP adresai – nuotoliniai IP adresai, kurie priklauso IP rinkiniui.

Valdymo elementai

Pridėdami arba **redaguodami** IP rinkinį, galite naudotis šiais laukais:

Pavadinimas – nuotolinių kompiuterių grupės pavadinimas.

Aprašas – bendras grupės aprašas.

Nuotolinio kompiuterio adresas (IPv4, IPv6, intervalas, kaukė) – leidžia pridėti nuotolinį adresą, adresų intervalą arba potinklį.

Šalinti – zona pašalinama iš sąrašo.

Iš anksto nustatytų IP rinkinių pašalinti negalima.

IP adresų pavyzdžiai

Pridėti IPv4 adresą:
Vienas adresas – prideda atskiro kompiuterio IP adresą (pvz., *192.168.0.10*).
Adresų diapazonas – įveda pradinį ir galutinį IP adresus, kad būtų nurodytas keleto kompiuterių IP diapazonas (pavyzdžiui, *192.168.0.1 – 192.168.0.99*).
Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė). Pavyzdžiui, 255.255.255.0 yra 192.168.1.0 potinklio tinklo kaukė. Norėdami išskirti visą potinklį, įveskite *192.168.1.0/24*.
Pridėti IPv6 adresą:
Vienas adresas – prideda atskiro kompiuterio IP adresą, kuriam bus taikoma taisyklė (pavyzdžiui, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė) (pavyzdžiui, *2002:c0a8:6301:1::1/64*).

Tinklo tikrinimo įrankis

Tinklo tikrinimo įrankis gali padėti nustatyti silpnąsias jūsų patikimo (namų arba biuro) tinklo vietas (pvz., atvirus prievadus ar silpną maršruto parinktuvo slaptažodį). Jis taip pat suteikia prijungtų įrenginių sąrašą, kuriame įrenginiai suskirstyti pagal tipą (pvz., spausdintuvas, maršruto parinktuvas, mobilusis įrenginys ir pan.) – taip galite aiškiai matyti, kas yra prijungta prie tinklo (pvz., žaidimų konsolė, IoT ar kiti išmanieji namų įrenginiai). Tinklo tikrinimo įrankį galite konfigūruoti dalyje Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Tinklo tikrinimo įrankis**.

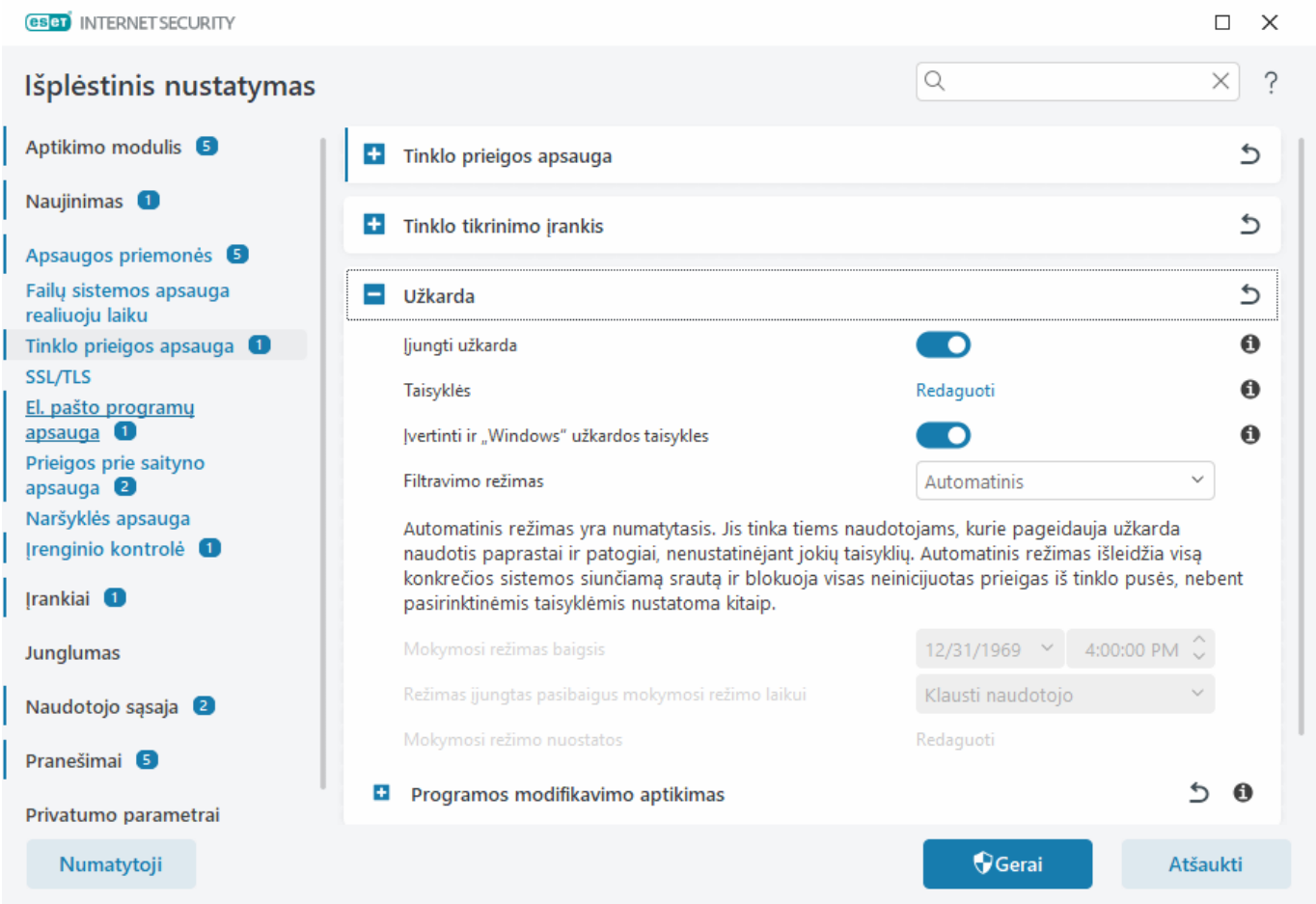
Įgalinti tinklo tikrinimo įrankį – Tinklo tikrinimo įrankisgali padėti nustatyti silpnąsias jūsų namų tinklo vietas, pvz., atvirus prievadus ar silpną maršruto parinktuvo slaptažodį. Jis taip pat suteikia prijungtų įrenginių sąrašą, kuriame įrenginiai suskirstyti pagal tipą.

Pranešti apie naujai aptiktus tinklo įrenginius – praneša, kai jūsų tinkle aptinkamas naujas įrenginys.

Užkarda

Užkarda valdo visą gaunamą ir išsiunčiamą tinklo duomenų srautą jūsų kompiuteryje pagal vidines taisykles ir jūsų nustatytas taisykles. Tai atliekama leidžiant arba draudžiant atskirus tinklo ryšius. Užkarda užtikrina apsaugą nuo atakų iš nuotolinių įrenginių ir gali užblokuoti galimai pavojingas tarnybas.

Norėdami sukonfigūruoti užkardą, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda**.



Užkarda

Įjungti užkarda

rekomenduojame šią funkciją palikti įjungtą, kad būtų užtikrintas sistemos saugumas. Įjungus užkardą, tinklo duomenų srautas nuskaitomas abiem kryptimis.

Taisyklės

Taisyklių nustatymas leidžia peržiūrėti ir redaguoti visas užkardos taisykles, taikomas srautui, kurį patikimame ryšyje ir Internete generuoja atskiros programos.

> Užgrobtų kompiuterių tinklui („Botnet“) surengus ataką prieš jūsų kompiuterį, galite sukurti IDS taisyklę. Taisyklė gali būti pakeista dalyje Išplėstiniai nustatymai > **Apsaugos priemonės** > **Tinklo apsauga** > **Apsauga nuo atakos iš tinklo** > **IDS taisyklės** spustelėję **Redaguoti**.

Įvertinti ir „Windows“ užkardos taisykles

Veikiant automatiniam filtravimo režimui bus leidžiamas ir gaunamas srautas, kuris yra leidžiamas pagal „Windows“ užkardos taisykles, nebent jis tiesiogiai blokuojamas pagal ESET taisykles.

Filtravimo režimas

Užkardos veikimas pasikeičia pagal filtravimo režimą. Be to, filtravimo režimai lemia, kiek reikia vartotojo veiksmų.

Galite pasirinkti toliau pateikiamus ESET Internet Security užkardos filtravimo režimus:

Filtravimo režimas	Aprašymas
Automatinis režimas	Numatytasis režimas. Šis režimas tinka vartotojams, kurie nori lengvai ir patogiai naudotis užkarda nenustatinėdami taisyklių. **Automatiniu režimu** galima kurti pasirinktines, vartotojo apibrėžtas taisykles, tačiau jos neprivalomos. Automatinis režimas leidžia išsiųsti visą konkrečios sistemos srautą ir blokuoja didžiąją dalį atsiunčiamo srauto (išskyrus srautą iš patikimos zonos, kuris apibrėžiamas IDS ir išplėstinėse parinktyse / leidžiamose paslaugose bei reaguoja į pastaruoju metu išsiųstą srautą).
Interaktyvusis režimas	Leidžia sukurti pasirinktinę konfigūraciją savo užkardai. Kai aptinkamas ryšys ir nėra šiam ryšiui taikomos taisyklės, parodomas dialogo langas, kuriame pranešama apie nežinomą ryšį. Dialogo langas suteikia galimybę leisti arba uždrausti ryšį, ir šis sprendimas leisti arba drausti gali būti įrašytas kaip nauja užkardos taisyklė. Jeigu pasirinksite sukurti naują taisyklę, visi vėlesni šio tipo ryšiai pagal tokią taisyklę bus leidžiami arba blokuojami.
Politika pagrįstas režimas	Blokuoja visus ryšius, kurie nėra apibrėžti konkrečios juos leidžiančios taisyklės. Šis režimas leidžia patyrusiems vartotojams apibrėžti taisykles, kurios leidžia tik norimus ir saugius ryšius. Visus kitus nenurodytus ryšius užkarda blokuos.
Mokymosi režimas	Automatiškai sukuriamos ir išsaugomos taisyklės; šis režimas itin naudingas pirminės užkardos konfigūracijos etape, tačiau jo nereikėtų palikti įjungto ilgam. Nereikalingi jokie vartotojo veiksmai, nes ESET Internet Security įrašo taisykles pagal iš anksto nustatytus parametrus. Mokymosi režimas turėtų būti naudojamas tik iki tol, kol sukuriamos visos reikiamų ryšių taisyklės, kad būtų išvengta saugumo pavojų.

Mokymosi režimas baigsis – nustatykite datą ir laiką, kada mokymosi režimas baigsis automatiškai. Taip pat galite išjungti mokymosi režimą rankiniu būdu, kada norite.

Režimas, nustatytas pasibaigus mokymosi režimui – nustatykite, kurį filtravimo režimą asmeninė užkarda vėl įjungs pasibaigus mokymosi režimo laikui. Daugiau apie filtravimo režimus skaitykite aukščiau esančioje lentelėje. Pasibaigus, parinktis **Teirautis naudotojo** prašo administratoriaus teisių, kad galėtų atlikti užkardos filtravimo režimo pakeitimą.

Mokymosi režimo nustatymai – spustelėkite **Redaguoti**, kad sukonfigūruotumėte mokymosi režimu sukurtų taisyklių įrašymo parametrus.

Programos modifikavimo aptikimas

Jei ryšį bando užmegzti modifikuotos programos, kurioms yra nustatyta užkardos taisyklė, programos modifikavimo aptikimo funkcija ima rodyti pranešimus.

Mokymosi režimo nuostatos

Mokymosi režimas automatiškai sukuria ir įrašo po taisyklę kiekvienam ryšiui, kuris buvo užmegztas sistemoje. Nereikalingi jokie vartotojo veiksmai, nes ESET Internet Security įrašo taisykles pagal iš anksto nustatytus parametrus.

Šis režimas gali kelti jūsų sistemai pavojų, todėl rekomenduojamas tik pradiniam užkardos konfigūravimui.

Pasirinkite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda** > **Užkarda** > **Filtravimo režimas**, tada išskleidžiamajame meniu pasirinkite **Mokymasis**, kad suaktyvintumėte mokymosi režimo parinktis. Spustelėkite parinktį **Redaguoti**, esančią šalia **Mokymosi režimo nustatymai**, kad galėtumėte konfigūruoti šias parinktis:

Mokymosi režimu užkarda nefiltruoja ryšio. Leidžiami visi siunčiami ir gaunami ryšiai. Šiuo režimu jūsų kompiuteris nėra visiškai apsaugotas užkardos.

Gaunamas srautas iš patikimos zonos – gaunamo ryšio pavyzdys patikimoje zonoje būtų nuotolinis kompiuteris iš patikimos zonos, bandantis užmegzti ryšį su vietine taikomąja programa, vykdoma jūsų įrenginyje.

Siunčiamas srautas į patikimą zoną – vietinė taikomoji programa, bandanti užmegzti ryšį su kitu įrenginiu, esančiu vietiniame tinkle arba tinkle patikimoje zonoje.

Gaunamas interneto duomenų srautas – nuotolinis įrenginys, bandantis susisiekti su kompiuteryje veikiančia taikomąja programa.

Siunčiamas interneto duomenų srautas – vietinė taikomoji programa bando užmegzti ryšį su kitu įrenginiu.

Kiekviename skyriuje galima apibrėžti parametrus, kurie bus pridedami prie naujai kuriamų taisyklių:

Pridėti vietinį prievadą – įtraukia tinklo ryšio vietinio prievado numerį. Siunčiamiems ryšiams paprastai generuojami atsitiktiniai numeriai. Dėl šios priežasties rekomenduojame įjungti šią parinktį tik gaunamiems ryšiams.

Pridėti taikomąją programą – įtraukia vietinės taikomosios programos pavadinimą. Ši parinktis tinka programos lygio taisyklėms ateityje (taisyklėms, kurios apibrėžia visos programos ryšį). Pavyzdžiui, galite leisti ryšį tik žiniatinklio naršyklei arba el. pašto programai.

Pridėti nuotolinį prievadą – įtraukia tinklo ryšio nuotolinio prievado numerį. Pavyzdžiui, galite leisti arba uždrausti konkrečias paslaugas, susijusias su standartiniu prievado numeriu (HTTP – 80, POP3 – 110 ir t. t.).

Pridėti nuotolinį IP adresą / patikimą zoną – nuotolinis IP adresas arba zona gali būti naudojami kaip parametrai naujoms taisyklėms, nustatančioms visus tinklo ryšius tarp vietinės sistemos ir to nuotolinio adreso / zonos. Ši parinktis tinka, jeigu norite nustatyti konkretaus įrenginio arba tinklo įrenginių grupės veiksmus.

Maksimalus skirtingų taisyklių taikomajai programai skaičius – jeigu taikomoji programa palaiko ryšius per skirtingus prievadus, su įvairiais IP adresais ir t. t., užkarda mokymosi režimu sukuria atitinkamą skaičių taisyklių šiai programai. Ši parinktis leidžia riboti taisyklių, kurios gali būti sukurtos vienai taikomajai programai, skaičių.

Užkardos taisyklės

Užkardos taisyklės – tai sąlygų rinkinys, naudojamas reikšmingai tikrinti visus šioms sąlygoms priskirtus tinklo ryšius ir veiksmus. Naudodamiesi užkardos taisyklėmis galite nurodyti veiksmą, kurį reikia atlikti užmezgus įvairius tinklo ryšius.

Taisyklės vertinamos iš viršaus į apačią, o jų prioritetą galite pamatyti pirmame stulpelyje. Kiekvienam vertinamam tinklo ryšiui naudojamas pirmosios atitinkančios taisyklės veiksmas.

Ryšius galima skirstyti į gaunamus ir siunčiamus ryšius. Gaunami ryšiai yra inicijuojami nuotolinio įrenginio, bandančio užmegzti ryšį su vietine sistema. Siunčiami ryšiai veikia atvirkščiai – vietinė sistema kreipiasi į nuotolinį įrenginį.

Jeigu aptinkamas naujas nežinomas ryšys, turite atsakingai nuspręsti, ar leisti jį, ar uždrausti. Neprašyti, nesaugūs arba nežinomi ryšiai kelia riziką sistemos saugai. Jeigu toks ryšys užmezgamas, rekomenduojame atkreipti dėmesį į nuotolinio įrenginio ir taikomosios programos bandymą prisijungti prie jūsų kompiuterio. Daugelis įsiskverbimų bando gauti ir išsiųsti asmeninius duomenis arba atsisiųsti kitas kenkėjiškas programas į pagrindinius kompiuterius. Užkarda leidžia aptikti ir nutraukti tokius ryšius.

Užkardos taisykles galite peržiūrėti ir redaguoti Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda** > **Taisyklės** > **Redaguoti**.

Jei turite daug užkardos taisyklių, galite naudoti filtrą, kad būtų rodomos tik konkrečios taisyklės. Norėdami filtruoti užkardos taisykles, virš užkardos taisyklių sąrašo spustelėkite **Daugiau filtrų**. Taisykles galite filtruoti pagal šiuos kriterijus:

- Kilmė
- Kryptis
- Veiksmas
- Pasiekiamumas

Pagal numatytuosius nustatymus iš anksto nustatytos užkardos taisyklės yra paslėptos. Norėdami pamatyti visas iš anksto nustatytas taisykles, išjunkite perjungiklį šalia **Slėpti įtaisytąsias (iš anksto apibrėžtas) taisykles**. Šias taisykles galite išjungti, tačiau iš anksto nustatytos taisyklės panaikinti negalima.

Spustelėkite paieškos piktogramą viršutiniame dešiniajame kampe ir ieškokite taisyklės (-ių).

Stulpeliai

Prioritetas – taisyklės vertinamos iš viršaus į apačią, o jų prioritetą galite matyti pirmame stulpelyje.

Įjungta – parodo, ar taisyklė įjungta, ar išjungta. Norint suaktyvinti taisyklę, reikia pažymėti atitinkamą žymimąjį langelį.

Programa – programa, kuriai taikoma taisyklė.

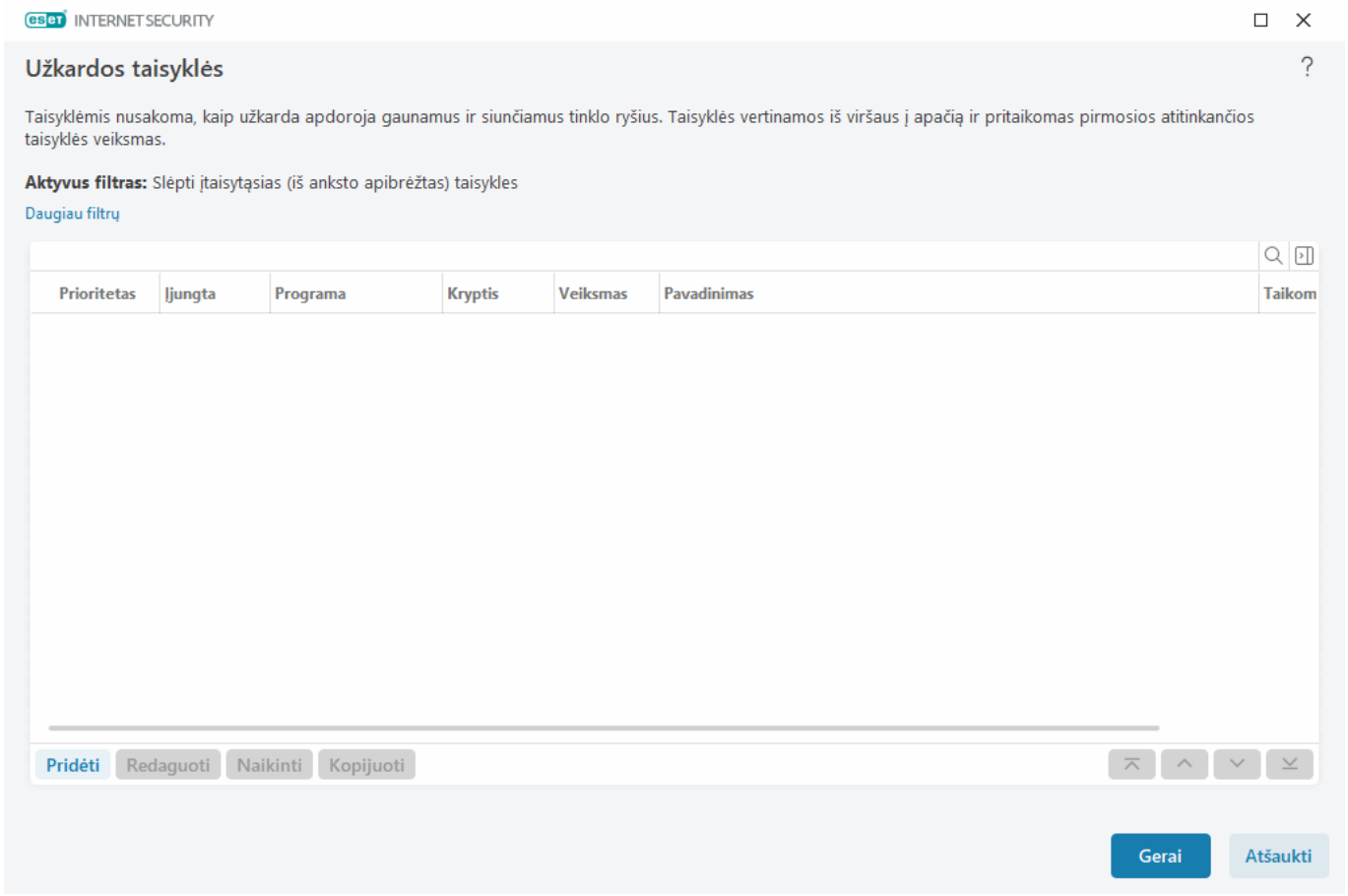
Kryptis – ryšio kryptis (įeinantis / išeinantis / abi).

Veiksmas – pateikiama ryšio būsena (blokuoti / leisti / klausti).

Pavadinimas – taisyklės pavadinimas. ESET piktograma nurodo iš anksto apibrėžtą taisyklę.

Taikytas laikas – bendras taisyklės taikymo kartų skaičius.

Spustelėkite išplėtimo piktogramą, kad būtų rodoma išsami informacija apie taisyklę.



Valdymo elementai

Pridėti – sukuriama nauja taisyklė.

Redaguoti – redaguokite esamą taisyklę.

Pašalinti – pašalinkite esamą taisyklę.

Kopijuoti – sukurkite pasirinktos taisyklės kopiją.

Į viršų / aukštyn / žemyn / į apačią – suteikia galimybę nustatyti taisyklių pirmumo lygį (taisyklės vykdomos iš viršaus žemyn).

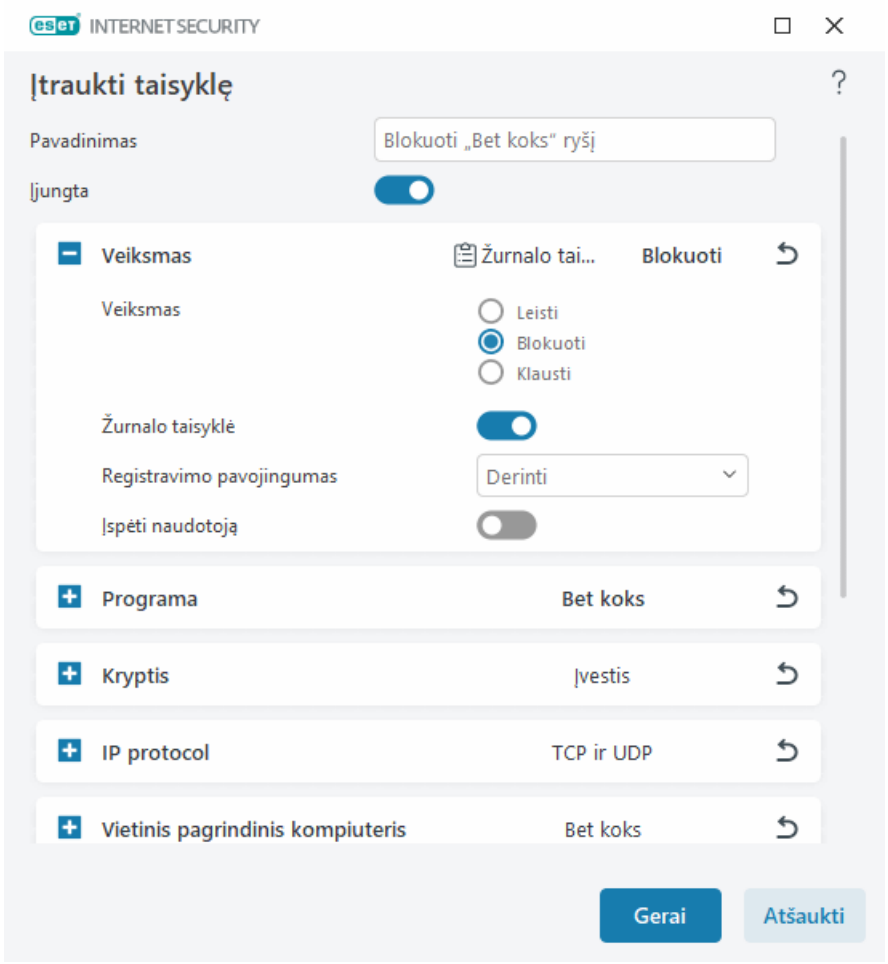
Užkardos taisyklių įtraukimas arba redagavimas

Užkardos taisyklės – tai sąlygų rinkinys, naudojamas reikšmingai tikrinti visus šioms sąlygoms priskirtus tinklo ryšius ir veiksmus. Gali reikėti redaguoti arba pridėti užkardos taisykles, kai pasikeičia tinklo nustatymai (pvz., pasikeitė nuotolinės pusės tinklo adresas arba prievado numeris), kad būtų užtikrintas tinkamas programos, kuriai

taikoma taisyklė, veikimas. Patyręs naudotojas turėtų sukurti pasirinktines užkardos taisykles.

> **Iliustruotos instrukcijos**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Atidarykite arba uždarykite (leiskite arba uždrauskite) konkretų prievadą naudodami užkardą
> - Sukurkite užkardos taisyklę ESET Internet Security žurnalo failų

Norėdami pridėti arba redaguoti užkardos taisyklę, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda** > **Taisyklės** > **Redaguoti**. Lange Užkardos taisyklės spustelėkite **Pridėti** arba **Redaguoti**.



Pavadinimas – įveskite taisyklės pavadinimą.

Įgalinta – spustelėkite perjungiklį, kad taisyklė būtų aktyvi.

Įtraukite užkardos taisyklės veiksmus ir sąlygas:

Veiksmas

Veiksmas – pasirinkite, ar norite **Leisti** / **Blokuoti** ryšį, kuris atitinka šioje taisyklėje apibrėžtas sąlygas, ar norite ESET Internet Security **Klausti** kiekvieną kartą, kai užmezgamas ryšys.
Žurnalo taisyklė – jei taisyklė pritaikyta, ji bus įrašyta į skiltį Žurnalo failai.
Registravimo svarbumas – pasirinkite šios taisyklės Žurnalo įrašo svarbą.
Parinktis **Įspėti naudotoją** rodo pranešimą, kai taisyklė yra taikoma.

Taikomoji programa

Nurodykite programą, kurioje bus taikoma ši taisyklė.
Programos kelias – spustelėkite **...** ir eikite į programą arba įveskite visą programos kelią (pvz., C:\Program Files\Firefox\Firefox.exe). NEĮRAŠYKITE vien tik programos pavadinimo.
Taikomosios programos parašas – taisyklę galite taikyti programoms pagal jų parašus (leidėjo vardą). Išskleidžiamajame meniu pasirinkite, jei norite taikyti taisyklę programoms su **bet kokiu galiojančiu parašu** arba programoms, **pasirašytoms konkretaus pasirašančio asmens**. Jei pasirenkate programas **Pasirašė konkretus pasirašantis asmuo**, lauke **Pasirašančio asmens vardas ir pavardė** turite apibrėžti pasirašantįjį.
„Microsoft Store“ programa – išskleidžiamajame meniu pasirinkite programą, įdiegtą iš „Microsoft Store“.
Paslauga – galite pasirinkti sistemos paslaugą, o ne programą. Atidarykite išskleidžiamąjį meniu, kad pasirinktumėte paslaugą.
Taikyti antriniams procesams – kai kurios programos gali vykdyti daugiau procesų, kai matote tik vieną programos langą. Spustelėkite perjungiklį, kad įjungtumėte taisyklę kiekvienam procesui nurodytoje programoje.

Kryptis

Pasirinkite šios taisyklės ryšio **kryptį**:
- **Abu** – gaunamas ir siunčiamas ryšys
- **Įeiti** – tik gaunamas ryšys
- **Išeiti** – tik siunčiamas ryšys

IP protokolas

Išplečiamajame meniu pasirinkite **Protokolas**, jei norite, kad ši taisyklė būtų taikoma tik konkrečiam protokolui.

Vietinis pagrindinis kompiuteris

Vietiniai adresai, adresų diapazonas arba potinklis, kuriame taikoma ši taisyklė. Jei adresas nenurodytas, taisyklė bus taikoma visiems ryšiams su vietiniais kompiuteriais. IP adresus, adresų diapazonus ar potinklius galite pridėti tiesiai į **IP** teksto lauką arba pasirinkti iš esamų IP rinkinių, spustelėdami **Redaguoti** šalia **IP rinkiniai**.

Vietinis prievadas

Prievadas – vietinio prievado numeris (-iai). Jei numeriai nepateikiami, taisyklė bus taikoma bet kuriam prievadui. Galite pridėti vieną ryšio prievadą arba jų intervalą.

Nuotolinis pagrindinis kompiuteris

Nuotolinis adresas, adresų diapazonas arba potinklis, kuriame taikoma ši taisyklė. Jei adresas nenurodytas, taisyklė bus taikoma visam ryšiui su nuotoliniais kompiuteriais. IP adresus, adresų diapazonus ar potinklius galite pridėti tiesiai į **IP** teksto lauką arba pasirinkti iš esamų IP rinkinių, spustelėdami **Redaguoti** šalia **IP rinkiniai**.

Nuotolinis prievadas

Nuotolinio **prievado** numeris (-iai). Jei numeriai nepateikiami, taisyklė bus taikoma bet kuriam prievadui. Galite pridėti vieną ryšio prievadą arba jų intervalą.

Profilis

Užkardos taisyklę galima taikyti konkretiems tinklo ryšio profiliams.
Bet koks – taisyklė bus taikoma bet kokiam tinklo ryšiui, nepriklausomai nuo naudojamo profilio.
Pasirinktas – taisyklė bus taikoma konkrečiam tinklo ryšiui pagal pasirinktą profilį. Pažymėkite žymės langelį šalia profilių, kuriuos norite pasirinkti.

Sukuriame naują taisyklę, kad interneto naršyklė Firefox galėtų prisijungti prie Internetas / vietinio tinklo svetainių:
1.Sekcijoje **Veiksmas** pasirinkite **Veiksmas** > **Leisti**.
2.Sekcijoje **Programa** nurodykite žiniatinklio naršyklės **programos kelią** (pvz., C:\Program Files\Firefox\Firefox.exe). NEĮRAŠYKITE vien tik programos pavadinimo.
3.Sekcijoje **Kryptis** pasirinkite **Kryptis** > **Išeiti**.
4.Sekcijoje **IP protokolas** išskleidžiamajame meniu **Protokolas** pasirinkite **TCP ir UDP**.
5.Sekcijoje **Nuotolinis prievadas** įtraukite **prievadų** numerius: *80 443*, kad būtų galima atlikti standartinį naršymą.

Programos modifikavimo aptikimas

Jei ryšį bando užmegzti modifikuotos programos, kurioms yra nustatyta užkardos taisyklė, programos modifikavimo aptikimo funkcija ima rodyti pranešimus. Programos modifikavimas yra mechanizmas, kai kitu vykdomuoju failu originali programa laikinai arba visam laikui pakeičiama kita programa (apsaugo nuo piktnaudžiavimo užkardos taisyklėmis).

Atminkite, kad šia savybe nesiekiama bendrai aptikti programų modifikavimo atvejų. Šiuo atveju tikslas – išvengti piktnaudžiavimo esamomis užkardos taisyklėmis ir stebimos tik tos programos, kurioms yra nustatytos konkrečios užkardos taisyklės.

Norėdami redaguoti parinktį **Programos modifikavimo aptikimas**, atidarykite išplėstinį nustatymą > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Užkarda** > **Programos modifikavimo aptikimas**.

Įjungti programos keitimų aptikimą – jeigu pasirinkta, sistema stebės, ar nekeičiamos programos (naujinimai, užkrėtimai, kitos modifikacijos). Kai modifikuota taikomoji programa bandys užmegzti ryšį, užkarda jums apie tai praneš.

Leisti modifikuoti pasirašytas (patikimas) programas – nepranešti, jei programa prieš ir po modifikavimo išlaiko tą patį galiojantį skaitmeninį parašą.

Neaptinkamų programų sąrašas – šiame lange galima pridėti arba pašalinti atskiras programas, kurias galima modifikuoti neparodant pranešimų.

Neaptinkamų programų sąrašas

ESET Internet Security užkarda aptinka pokyčius tose programose, kurioms yra sukurtos taisyklės (žr. Programų modifikavimo aptikimas).

Tam tikrais atvejais galite nenorėti taikyti šios funkcijos kai kurioms programoms ir galite norėti jų neįtraukti į užkardos vykdomas patikras.

Pridėti – atidaromas langas ir jame galima pasirinkti programą, kurią norite pridėti prie sąrašo programų, neįtrauktų į modifikavimo aptikimo procesą. Galima rinktis iš sąrašo veikiančių programų su atviru tinklo ryšiu, kurioms taikoma užkardos taisyklė, arba pridėti konkrečią programą.

Redaguoti – atidaromas langas ir jame galima pakeisti vietą programos, kuri priklauso sąrašui programų, neįtrauktų į modifikavimo aptikimo procesą. Galima rinktis iš sąrašo veikiančių programų su atviru tinklo ryšiu, kurioms taikoma užkardos taisyklė, arba pakeisti vietą rankiniu būdu.

Šalinti – šalina į modifikavimo aptikimo procesą neįtrauktų programų sąrašo įrašus.

Apsauga nuo atakos iš tinklo (IDS)

Tinklo apsauga nuo atakų (IDS) pagerina žinomų pažeidžiamumo atvejų nustatymą. Daugiau apie tinklo apsaugą nuo atakų skaitykite terminų žodyne. Norėdami konfigūruoti apsaugą nuo atakos iš tinklo (IDS), atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Apsauga nuo atakos iš tinklo (IDS)**.

Įjungti apsaugą nuo atakos iš tinklo (IDS) – Analizuoja tinklo srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas bet koks žalingu laikomas turinys.

Įjungti apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą – aptinka ir užblokuoja ryšį su kenkti skirtais komandų ir valdymo centrais, vadovaujantis simptomais, pasireiškiančiais kompiuterį užkrėtus ir botui mėginant užmegzti ryšį. Daugiau apie apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą skaitykite terminų žodyne.

IDS taisyklės – Ši parinktis jums leis sukonfigūruoti išplėstines filtravimo parinktis, kad aptiktumėte įvairių tipų atakas ir spragų išnaudojimus, kurie gali būti panaudoti pakenkti jūsų kompiuteriui.

> **Iliustruotos instrukcijos**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Nejtraukti IP adreso iš IDS į ESET Internet Security

Visi tinklo apsaugos aptikti svarbūs įvykiai saugomi žurnalo faile. Norėdami gauti daugiau informacijos, žr. tinklo apsaugos žurnalą.

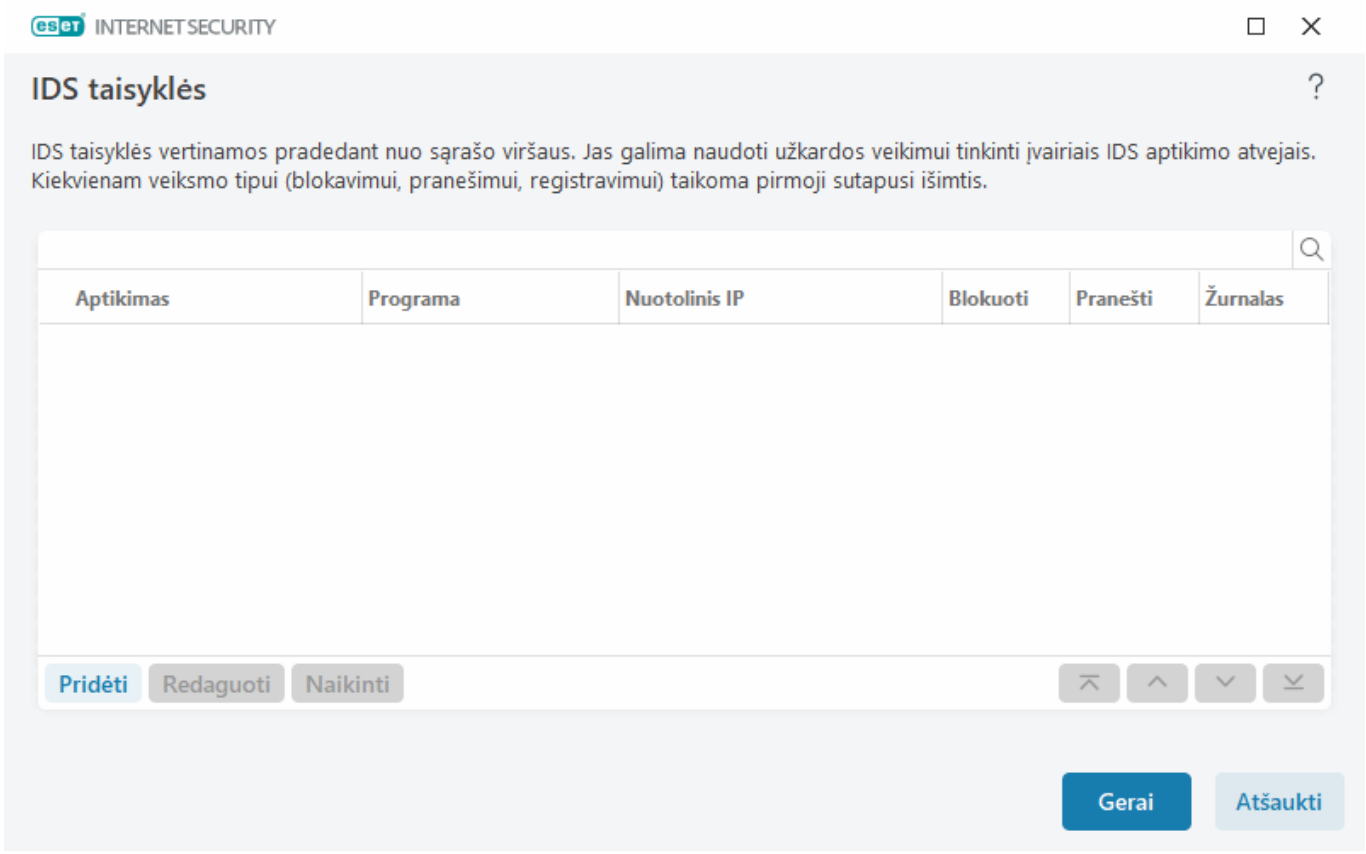
IDS taisyklės

Tam tikrais atvejais Įsilaužimo aptikimo tarnyba (IDS) gali nustatyti maršrutų parinktuvų ir kitų tarptautinių tinklų įrenginių ryšį kaip galimą ataką. Pavyzdžiui, kad būtų apeita IDS, galite pridėti žinomą saugų adresą prie adresų, neįtrauktų į IDS sritį.

> **Iliustruotos instrukcijos**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Nejtraukti IP adreso iš IDS į ESET Internet Security

IDS taisyklių valdymas

- **Pridėti** – spustelėkite, kad sukurtumėte naują IDS taisyklę.
- **Redaguoti** – spustelėkite, norėdami redaguoti esamą IDS taisyklę.
- **Šalinti** – pasirinkite ir spustelėkite, jei norite pašalinti esamą taisyklę iš IDS taisyklių sąrašo.
-  **Į viršų / aukštyn / žemyn / į apačią** – leidžia nustatyti taisyklių pirmumo lygį (išimtys vertinamos iš viršaus žemyn).



Taisyklių rengyklė

Aptikimas – aptikimo tipas.

Grėsmės pavadinimas – galite nurodyti kai kurių galimų aptikimų grėsmės pavadinimą.

Programa – pasirinkite išskirtos programos failo kelią spustelėdami ... (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮRAŠYKITE programos pavadinimo.

Nuotolinis IP adresas – nuotolinių IPv4 arba IPv6 adresų / ribų / potinklių sąrašas. Kelis adresus reikia atskirti kableliais.

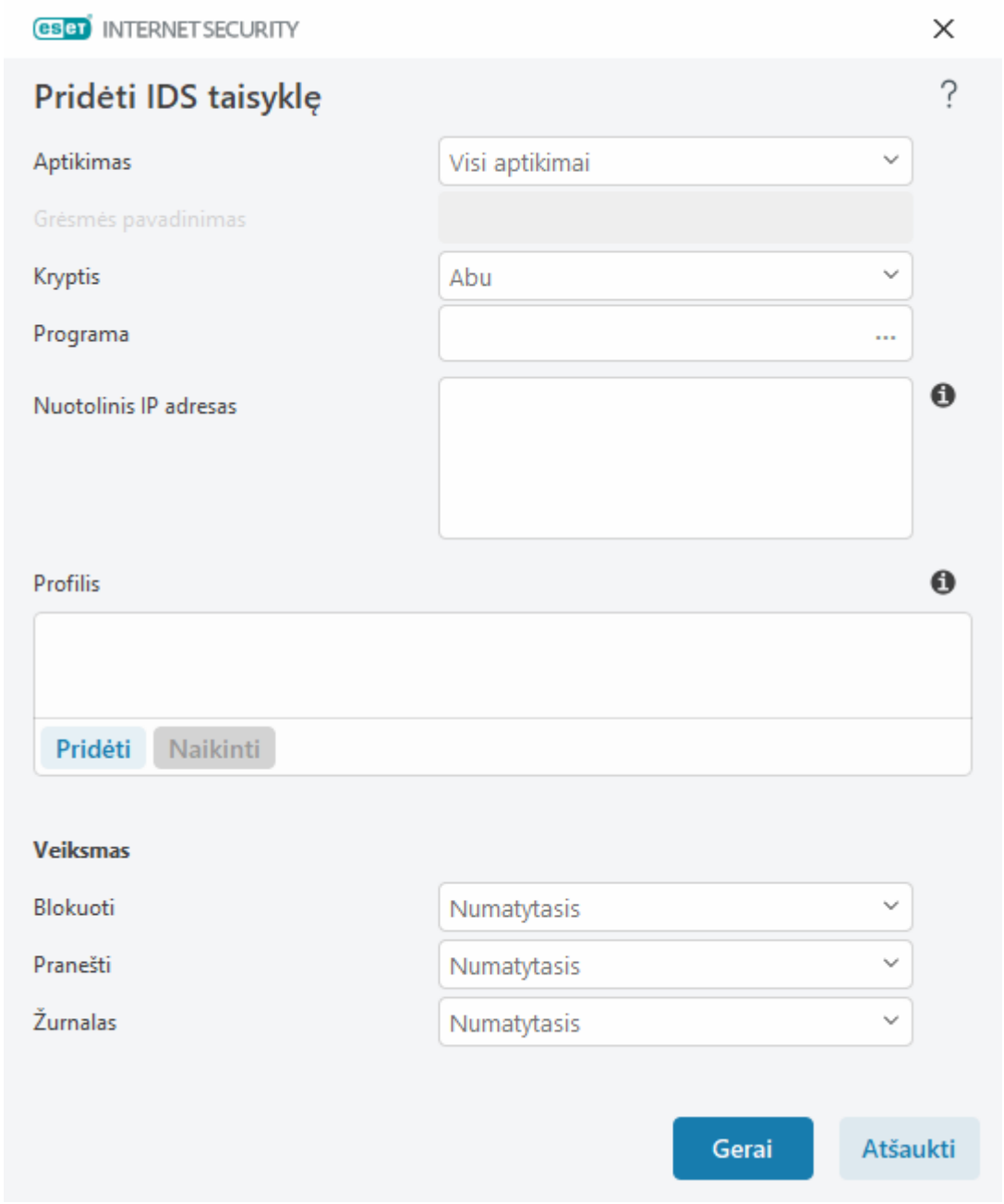
Profilis – galite pasirinkti tinklo ryšio profilį, kuriam bus taikoma ši taisyklė.

Veiksmas

Blokuoti – kiekvienas sistemos procesas turi savo numatytąją elgseną ir priskirtą veiksmą (blokuoti arba leisti). Norint apeiti ESET Internet Security numatytąją elgseną, pasirinkite ją blokuoti arba leisti, pasinaudojant išskleidžiamuoju meniu.

Pranešti – Pasirinkite Taip, kad rodytumėte Darbalaukio pranešimus savo kompiuteryje. Pasirinkite Ne, jei nepageidaujate kompiuterio pranešimų. Galimos parinktys yra Numatytoji/Taip/Ne.

Žurnalas – Pasirinkite **Taip**, kad fiksuotumėte įvykius žurnalo failuose. Pasirinkite **Ne**, jei nepageidaujate fiksuoti įvykių. Galimos parinktys yra **Numatytoji/Taip/Ne**.



Jei norite rodyti pranešimą ir fiksuoti visus įvykius:
1.Spustelėkite **Įtraukti**, kad įtrauktumėte naują IDS taisyklę.
2.Pasirinkite konkretų aptikimą išskleidžiamajame meniu **Aptikimas**.
3.Pasirinkite programos kelią spustelėdami **...**, kuriam norite pritaikyti šį pranešimą.
4.Palikite parinktį **Numatytoji** išskleidžiamajame meniu **Blokuoti**. Taip bus naudojamas numatytasis veiksmas, kurį taiko ESET Internet Security.
5.Išskleidžiamuosiuose meniu **Pranešti** ir **Žurnalas** pasirinkite **Taip**.
6.Įrašykite pranešimą spustelėdami **Gerai**.

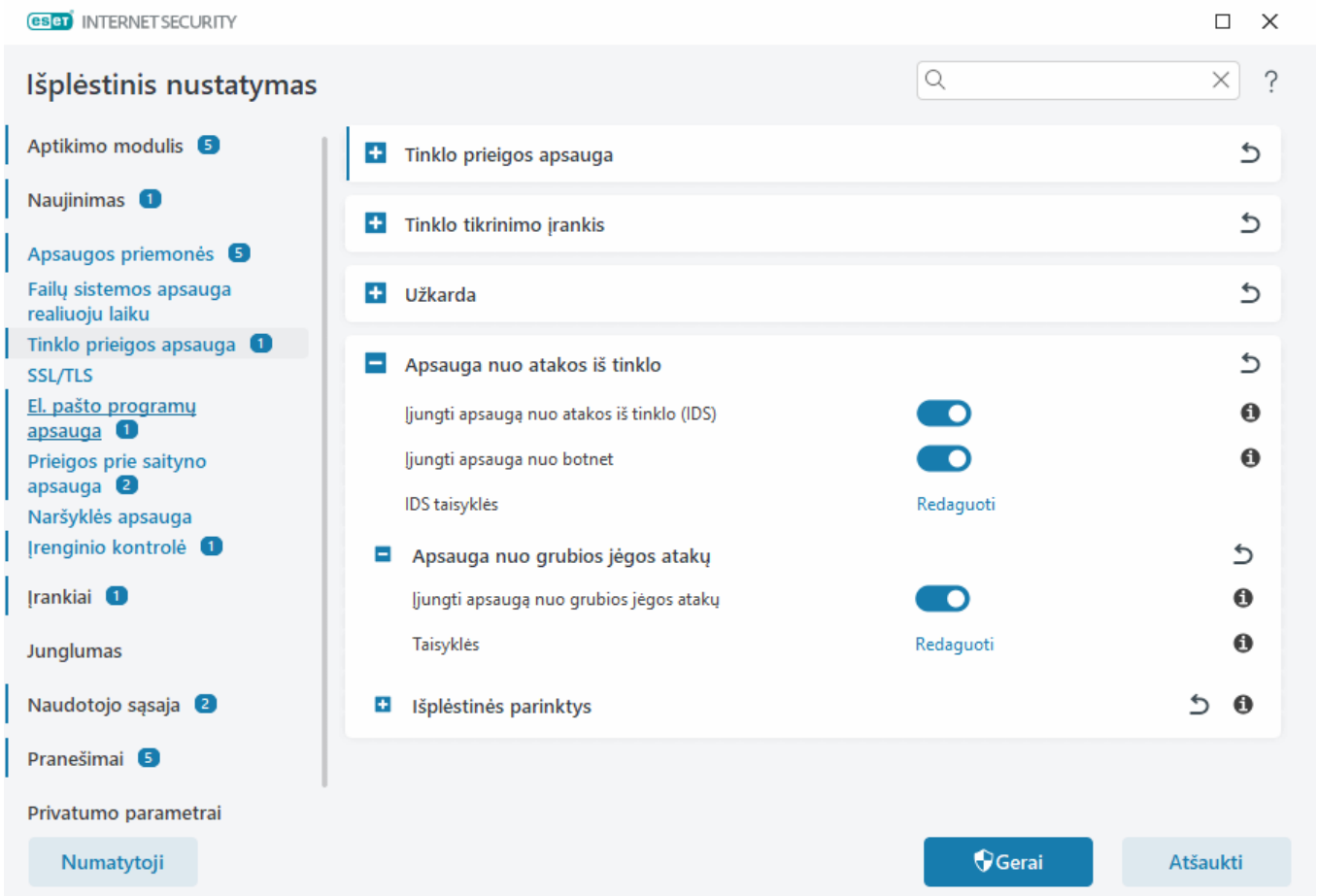
Jei nenorite, kad būtų rodomas pasikartojantis pranešimas, kurio nelaikote konkretaus **Aptikimas** tipo grėsme:
1.Spustelėkite **Įtraukti**, kad įtrauktumėte naują IDS taisyklę.
2.Išsirinkite konkretų aptikimą išskleidžiamajame meniu **Aptikimas**, pvz., **SMB seansas be saugumo plėtinių** arba **TCP prievadų nuskaitymo ataka**.
3.Išskleidžiamajame krypčių meniu pasirinkite **Įvestis**, jei įspėjimas skelbiamas dėl įeinančiojo ryšio.
4.Išskleidžiamajame meniu **Pranešti** pasirinkite **Ne**.
5.Išskleidžiamajame meniu **Žurnalas** pasirinkite **Taip**.
6.Palikite **Programa** tuščią.
7.Jei ryšys ateina ne iš konkretaus IP adreso, palikite **Nuotoliniai IP adresai** tuščią.
8.Įrašykite pranešimą spustelėdami **Gerai**.

Apsauga nuo grubios jėgos atakų

Apsauga nuo grubios jėgos atakų blokuoja RDP ir SMB tarnybų slaptažodžių spėliojimo atakas. Apsauga nuo grubios jėgos atakų yra būdas atrasti tikslinį slaptažodį, sistemingai bandant visus raidžių, skaičių ir simbolių derinius. Norėdami konfigūruoti apsaugą nuo grubios jėgos atakų, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Apsauga nuo atakos iš tinklo (IDS)** > **Apsauga nuo grubios jėgos atakų**.

Įjungti apsaugą nuo grubios jėgos atakų – ESET Internet Security tikrina tinklo srauto turinį ir blokuoja slaptažodžių spėliojimo atakų bandymus.

Taisyklės – leidžia kurti, redaguoti ir peržiūrėti gaunamų ir siunčiamų tinklo ryšių taisykles. Daugiau informacijos rasite skyriuje Taisyklės.



Taisyklės

Apsaugos nuo grubios jėgos atakų taisyklės leidžia kurti, redaguoti ir peržiūrėti gaunamų ir siunčiamų tinklo ryšių taisykles. Iš anksto apibrėžtų taisyklių negalima redaguoti arba naikinti.

Apsaugos nuo grubios jėgos atakų taisyklių valdymas

Pridėti – sukuriama nauja taisyklė.

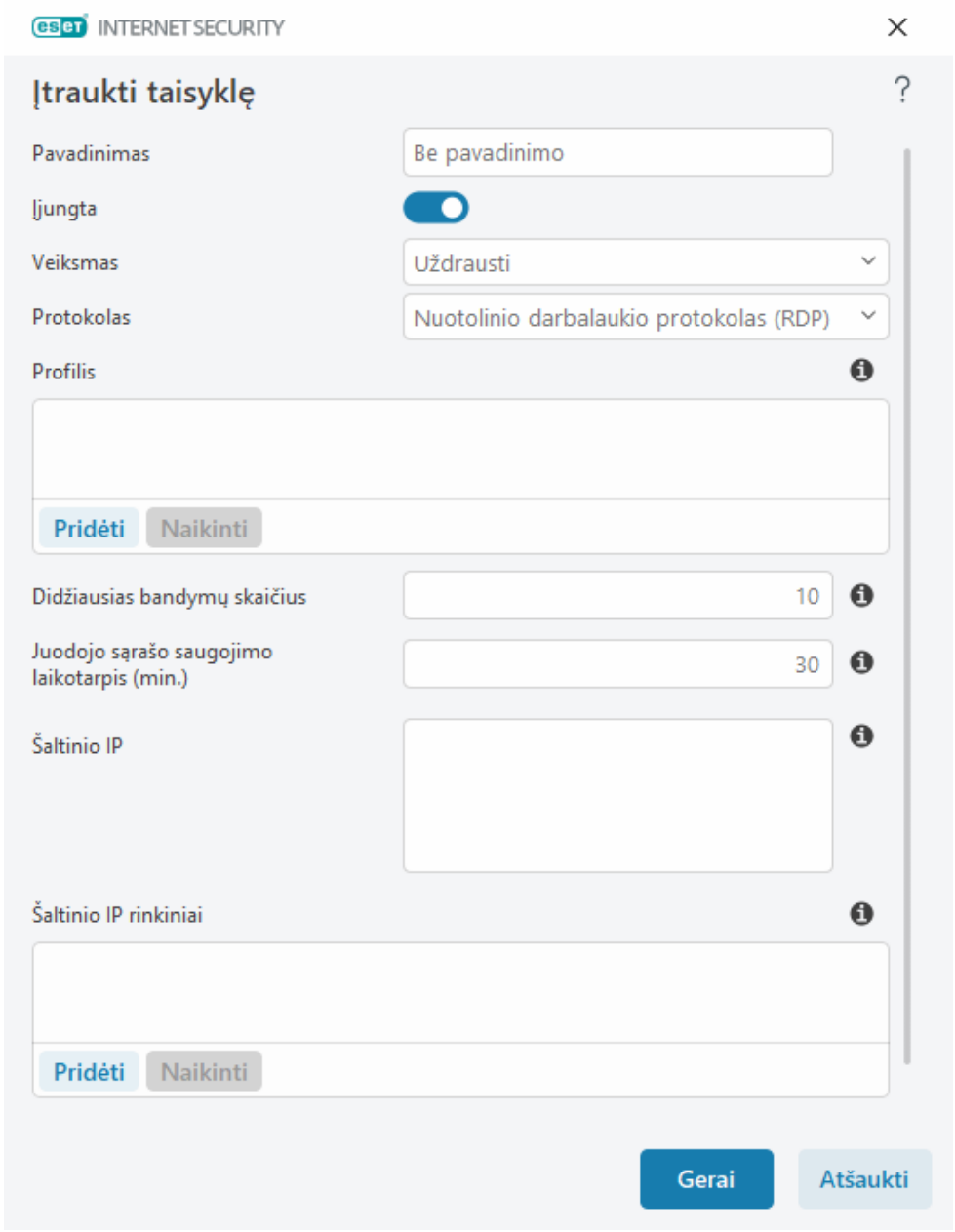
Redaguoti – redaguokite esamą taisyklę.

Naikinti – pašalinti esamą taisyklę iš taisyklių sąrašo.

 **Į viršų / aukštyn / žemyn / į apačią** – koreguokite taisyklių prioriteto lygį.

> Siekiant užtikrinti didžiausią įmanomą apsaugą, taikoma blokavimo taisyklė su mažiausia **didžiausio bandymų skaičiaus** reikšme, net jei taisyklė yra žemiau taisyklių sąraše, kai kelios blokavimo taisyklės atitinka aptikimo sąlygas.

Taisyklių rengyklė



Pavadinimas – taisyklės pavadinimas.

Įjungta – išjunkite perjungiklį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos taikyti.

Veiksmas – pasirinkite, ar **Drausti** arba **Leisti** ryšį, jei taisyklės parametrai įvykdyti.

Protokolas – ryšio protokolas, kurį tikrins ši taisyklė.

Profilis – tam tikriems profiliams galima nustatyti ir taikyti pasirinktines taisykles.

Didžiausias bandymų skaičius – Didžiausias leidžiamų bandymų pakartotinai atakuoti skaičius, kol IP adresas bus užblokuotas ir įtrauktas į juodąjį sąrašą.

Juodojo sąrašo saugojimo laikotarpis (min.) – nustato adreso buvimo juodajame sąraše pabaigos datą.

Šaltinio IP – IP adresų / diapazonų / potinklių sąrašas. Kelis adresus reikia atskirti kableliais.

Šaltinio IP rinkiniai – IP adresų, kuriuos jau apibrėžėte IP rinkiniuose, rinkinys.

Išplėstinės parinktys

Pasirinkę Išplėstinis nustatymas > **Apsaugos priemonės** > **Tinklo prieigos apsauga** > **Apsauga nuo atakos iš tinklo (IDS)** > **Išplėstinės parinktys**, galite įjungti arba išjungti naudojimosi ir kelių tipų atakų, kurie gali pakenkti jūsų kompiuteriui, aptikimą.

Kai kuriais atvejais negausite grėsmės pranešimo apie užblokuotus ryšius. Žr. skyrių Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo, kur rasite instrukcijų, kaip peržiūrėti visus užblokuotus ryšius užkardos žurnale.

Konkrečios parinktys šiame lange gali būti pateikiamos atsižvelgiant į jūsų ESET produkto ir užkardos modulio tipą arba versiją bei operacinės sistemos versiją.

Įsilaužimo aptikimas

Įsilaužimo aptikimas stebi, ar įrenginio tinklo ryšyje nėra kenkėjiškos veiklos.

- **Protokolo SMB** – aptinka ir užblokuota įvairias SMB protokolo saugumo problemas.
- **Protokolo RPC** – aptinka ir užblokuoja įvairius CVE nuotolinių procedūrų iškvietimo sistemoje, sukurtoje paskirstytųjų skaičiavimų aplinkai (DCE).
- **RDP Protokolas** – aptinka ir užblokuoja įvairius RDP protokole (žr. pirmiau).
- **ARP Nuodijimo atakos aptikimas** – tarpininko atakų sukeltų ARP nuodijimo atakų arba tinklo komutatoriaus šnipinėjimo aptikimas. ARP (adresų nustatymo protokolas) yra naudojamas tinklo programų ir įrenginių eterneto adresui nustatyti.
- **TCP/UDP prievadų nuskaitymo atakos aptikimas** – aptinka atakas, atliekamas prievadų nuskaitymo programine įranga – programomis, sukurtomis tikrinti atviriems pagrindinio kompiuterio prievadams siunčiant klientų užklausas įvairiais prievadų adresais, siekiant aptikti aktyvius prievadus ir išnaudoti tarnybos saugumo spragas. Išsamiau apie šio tipo atakas skaitykite terminų žodyne.
- **Blokuoti nesaugius adresus aptikus ataką** – IP adresai, kurie buvo aptikti kaip atakų šaltiniai, pridedami prie juodojo sąrašo ir kuriam laikui uždraudžiamas ryšys. Galite nustatyti **juodojo sąrašo saugojimo laikotarpį**, kuris nustato laiką, kiek laiko adresas bus užblokuotas aptikus ataką.
- **Rodyti pranešimą aptikus ataką** – įjungia „Windows“ pranešimų srities pranešimą apatiniame dešiniajame lango kampe.
- **Rodyti pranešimus ir apie atakas panaudojant saugumo spragas** – perspėja jus apie aptiktas atakas panaudojant saugumo spragas arba grėsmių bandymus tokiu būdu patekti į sistemą.

Paketo tikrinimas

Paketų analizės tipas, filtruojantis duomenis, perduodamus tinklu.

- **Leisti įeinantį ryšį su administratoriaus bendrinimais SMB protokolu** – administratoriaus bendrinimai yra numatytieji tinklo bendrinimai, bendrinantys standžiojo disko skaidinius (*C$*, *D$*, ...) sistemoje kartu su sisteminiu aplanku (*ADMIN$*). Išjungus įeinantį ryšį prie administratoriaus bendrinimų turi sumažėti daugelis saugos pavojų. Pavyzdžiui, kirminas „Conficker“ vykdo žodyno atakas, siekdamas prisijungti prie

administratoriaus bendrinimų.

- **Uždrausti senus (nepalaikomus) SMB dialektus** – draudžia SMB seansus, naudojančius seną SMB dialektą, kurio nepalaiko IDS. Šiuolaikinės „Windows“ operacinės sistemos palaiko senus SMB dialektus, kad būtų suderinamos su senomis operacinėmis sistemomis, pvz., „Windows 95“. Užpuolikas gali panaudoti seną dialektą SMB seansui, kad išvengtų duomenų srauto tikrinimo. Uždrauskite senus SMB dialektus, jei kompiuteriui nereikia bendrinti failų (ar naudoti SMB ryšį apskritai) su seną „Windows“ versiją turinčiu kompiuteriu.

- **Uždrausti SMB seansus be išplėstinės apsaugos** – SMB seanso pradžios metu galima naudoti išplėstinę apsaugą, siekiant užtikrinti saugesnį atpažinimo mechanizmą nei atpažinimas LAN tvarkytuvo iškvietimu / atsakymu (LM). LM schema laikoma silpna ir jos naudoti nerekomenduojama.

- **Uždrausti atidaryti SMB protokolu vykdomuosius failus iš serverio, kuris nėra patikimoje zonoje** – nutraukia ryšį, kai bandote atidaryti vykdomąjį failą (.exe, .dll, ...) iš bendrinamo aplanko serveryje, kuris nepriklauso patikimai zonai užkardoje. Atminkite, kad vykdomųjų failų kopijavimas iš patikimų šaltinių gali būti teisėtas. Atminkite: vykdomųjų failų kopijavimas iš patikimų šaltinių gali būti teisėtas, tačiau šis aptikimo būdas turėtų sumažinti pavojų nepageidaujamai atidaryti kenkimo serveryje esantį failą (pvz., atidaryti failą spustelint bendrinamo kenkimo vykdomojo failo saitą).

- **Uždrausti NTLM atpažinimą SMB protokole prisijungiant prie serverio, esančio arba nesančio patikimoje zonoje** – NTLM (abiejų versijų) atpažinimo schemas naudojantys protokolai yra pažeidžiami kredencialų persiuntimo atakomis (SMB protokolo atveju jos vadinamos „SMB relay“ atakomis). Uždraudžiant NTLM atpažinimą serveriams ne iš patikimos zonos turi sumažinti kredencialų persiuntimo atakos grėsmę iš kenkėjiškų serverių už patikimos zonos. Analogiškai NTLM atpažinimą galima uždrausti ir serveriams patikimoje zonoje.

- **Leisti ryšį su saugumo paskyrų tvarkytuvo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SAMR].

- **Leisti ryšį su vietinių saugumo institucijų tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-LSAD] ir [MS-LSAT].

- **Leisti ryšį su nuotolinio registravimo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-RRP].

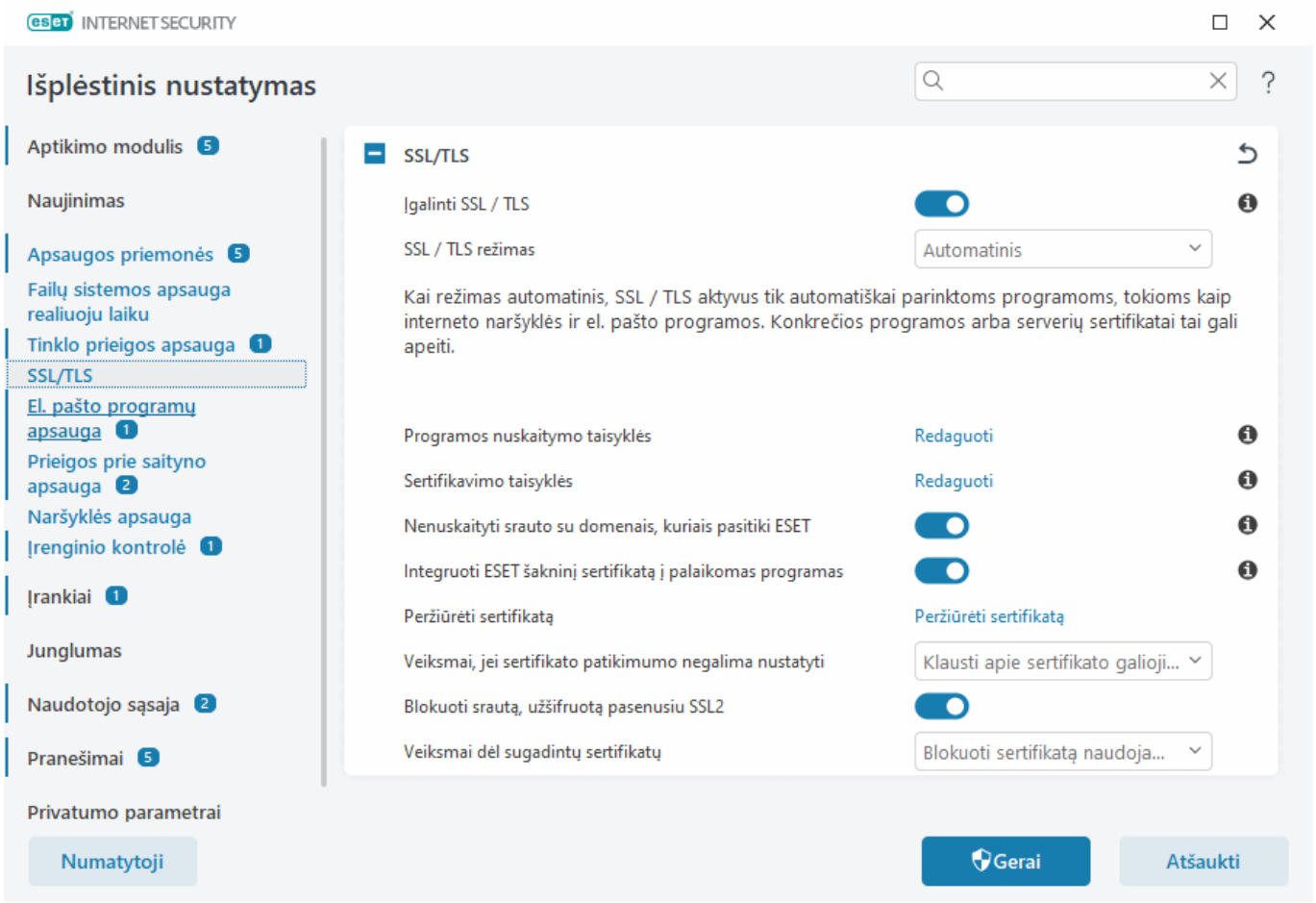
- **Leisti ryšį su tarnybų valdymo tvarkytuvo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SCMR].

- **Leisti ryšį su serverio tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SRVS].

- **Leisti ryšį su kitomis tarnybomis** – kitos MSRPC tarnybos. MSRPC yra „Microsoft“ būdas įdiegti DCE RPC mechanizmą. Be to, MSRPC dėl transportavimo gali naudoti įvardytuosius kanalus, perkeltus į SMB (tinklo failų bendrinimo) protokolą (ncacn_np transport). MSRPC paslaugos suteikia sąsajas nuotoliniu būdu pasiekti ir valdyti „Windows“ sistemoms. Buvo aptiktos kelios „Windows“ MSRPC sistemos saugumo spragos, kurias išnaudojo plintantys virusai (kirminai „Conficker“, „Sasser“…). Išjunkite nebūtiną ryšį su MSRPC tarnybomis daugeliui saugumo pavojų (tokių kaip nuotolinis kodo vykdymas ar tarnybų gedimo atakos) sumažinti.

SSL/TLS

ESET Internet Security gali patikrinti, ar nėra ryšio grėsmių, kurios naudoja SSL protokolą. Galite rinktis įvairius filtravimo režimus SSL apsaugotiems ryšiams ištirti, naudodami patikimus sertifikatus, nežinomus sertifikatus arba sertifikatus, kurie yra neįtraukti į SSL apsaugotų ryšių tikrinimo procesą. Norėdami redaguoti SSL/TLS nustatymus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **SSL/TLS.**



Įjungti SSL/TLS – jei išjungta, ESET Internet Security nenuskaitys ryšio per SSL/TLS.

SSL/TLS režimas siūlo tokias parinktis:

Filtravimo režimas	Aprašymas
Automatinis	Numatytasis režimas nuskaitys tik reikiamas programas, pavyzdžiui, saityno naršykles ir el. pašto programas. Galite jo nepaisyti pasirinkdami programas, kuriose nuskaitomas ryšys.
Interaktyvus	Jei įvesite naują SSL apsaugotą svetainę (su nežinomu sertifikatu), bus parodytas veiksmo pasirinkimo dialogo langas. Šis režimas leidžia sukurti SSL sertifikatų / programų, kurie nebus nuskaitomi, sąrašą.
Pagrįsta politika	Nurodykite šią parinktį norėdami nuskaityti visus SSL apsaugotus ryšius, išskyrus sertifikatų apsaugotus ryšius, kurie yra neįtraukti į tikrinimą. Jeigu užmezgamas naujas ryšys, naudojantis nežinomą pasirašytą sertifikatą, jums apie tai nebus pranešta ir ryšys bus automatiškai filtruojamas. Kai prisijungsite prie serverio su nepatikimu sertifikatu, kuris buvo pažymėtas kaip patikimas (jis yra patikimų sertifikatų sąraše), ryšys su šiuo serveriu bus leidžiamas, o šio ryšio kanalo turinys bus filtruojamas.

Programų nuskaitymo taisyklės – leidžia tinkinti ESET Internet Security konkrečių programų veikimą.

Sertifikavimo taisyklės – leidžia tinkinti ESET Internet Security konkrečių SSL sertifikatų veikimą.

Nenuskaityti srauto su domenais, kuriais pasitiki ESET – kai įjungta, ryšys su patikimais domenais nebus nuskaitomas. ESET valdomas įtaisytasis baltasis sąrašas nustato domeno patikimumą.

Integruoti ESET šakninį sertifikatą į palaikomas programas – tam, kad SSL ryšys veiktų tinkamai jūsų naršyklėse /

el. pašto programose, svarbu, kad ESET šakninis sertifikatas būtų įtrauktas į žinomų šakninių sertifikatų (leidėjų) sąrašą. Kai įjungta, ESET Internet Security automatiškai įtrauks ESET SSL Filter CA į žinomas naršykles (pvz., Opera). Naršyklėse, naudojančiose sistemos sertifikavimo saugyklą, sertifikatas yra pridedamas automatiškai. Pavyzdžiui, naršyklė Firefox yra automatiškai sukonfigūruota suteikti prieigą šakninėms organizacijoms sistemos sertifikavimo saugykloje.

Norėdami taikyti sertifikatą nepalaikomoms naršyklėms, spustelėkite **Peržiūrėti sertifikatą** > **Išsami informacija** > **Kopijuoti į failą** ir rankiniu būdu importuokite jį į naršyklę.

Veiksmai, jei sertifikato patikimumo negalima nustatyti – kai kuriais atvejais svetainės sertifikato negalima patikrinti naudojant patikimų šakninių sertifikavimo tarnybų (TRCA) saugyklą (pvz., nebegaliojantis sertifikatas, nepatikimas sertifikatas, sertifikatas negalioja konkrečiam domenui arba parašas, kurį galima išanalizuoti, bet sertifikatas nepasirašomas teisingai). Teisėtose svetainėse visada bus naudojami patikimi sertifikatai. Jei jie jo nepateikia, tai gali reikšti, kad atakuojanti programa iššifruoja jūsų ryšį arba svetainė patiria techninių sunkumų.

Jei punktas **Klausti apie sertifikato galiojimą** yra pažymėtas (pagal numatytąją parinktį), naudotojas raginamas pasirinkti, kokį veiksmą vykdyti, kai užmezgamas šifruotasis ryšys. Bus rodomas veiksmo pasirinkimo dialogas, kuriame galite nuspręsti pažymėti sertifikatą kaip patikimą arba neįtrauktą. Jeigu sertifikato nėra TRCA sąraše, langas yra raudonas. Jeigu sertifikatas yra TRCA sąraše, langas bus žalias.

Galite pasirinkti parinktį **Blokuoti sertifikatą naudojantį ryšį**, jeigu norite visada nutraukti šifruotąjį ryšį su svetaine, naudojančia nepatikimą sertifikatą.

Blokuoti srautą, užšifruotą pasenusiu SSL2 – ryšys naudojant ankstesnę SSL protokolo versiją bus automatiškai užblokuotas.

Veiksmai dėl sugadintų sertifikatų – sugadintas sertifikatas reiškia, kad sertifikate naudojamas formatas, kurio neatpažino ESET Internet Security arba kuris buvo gautas sugadintas (pvz., perrašytas atsitiktiniais duomenimis). Tokiu atveju rekomenduojame palikti punktą **Blokuoti sertifikatą naudojantį ryšį** pažymėtą. Jei pažymėtas punktas **Klausti apie sertifikato galiojimą**, naudotojas raginamas pasirinkti, kokį veiksmą vykdyti, kai užmezgamas šifruotasis ryšys.

> **Iliustruoti pavyzdžiai**
>
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Sertifikatų pranešimai ESET „Windows“ namų produktuose
> - „Šifruotas tinklo srautas: nepatikimas sertifikatas“ – Lankantis tinklalapiuose rodomas pranešimas

Programos nuskaitymo taisyklės

Pasirinkę **Programos nuskaitymo taisyklės** galite tinkinti ESET Internet Security veikimą konkrečiose programose ir veiksmams įsiminti, kai **SSL / TLS režime** pasirinkta parinktis **Interaktyvusis režimas**. Sąrašą galima peržiūrėti ir redaguoti pasirinkus Išplėstinis nustatymas > **Apsaugos priemonės SSL / TLS** > **Programos nuskaitymo taisyklės** > **Redaguoti**.

Programos nuskaitymo taisyklių langą sudaro:

Stulpeliai

Programa – pasirinkite vykdomąjį failą iš katalogo medžio, spustelėkite parinktį **...** arba įveskite kelią rankiniu būdu.

Nuskaitymo veiksmas – pasirinkite **Nuskaityti** arba **Nepaisyti**, kad ryšį nuskaitytumėte ar nepaisytumėte. Pasirinkite **Automatinis**, kad būtų nuskaitoma automatiniu režimu ir būtų klausiama interaktyviuoju režimu. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Valdymo elementai

Pridėti – pridėkite filtruojamą programą.

Redaguoti – pasirinkite programą, kurią norite konfigūruoti, ir spustelėkite **Redaguoti**.

Šalinti – pasirinkite programą, kurią norite pašalinti, ir spustelėkite **Šalinti**.

Importuoti / **Eksportuoti** – importuokite programas iš failo arba įrašykite dabartinį programų sąrašą į failą.

Gerai / **Atšaukti** – spustelėkite **Gerai**, jei norite įrašyti pakeitimus, arba spustelėkite **Atšaukti**, jei norite išeiti neįrašydami.

Sertifikavimo taisyklės

Sertifikavimo taisykles galima naudoti norint tinkinti konkrečių SSL ESET Internet Security sertifikatų veikimą ir prisiminti veiksmus, pasirinktus, kai **SSL / TLS režimas** veikia **interaktyviuoju režimu**. Sąrašą galima peržiūrėti ir redaguoti pasirinkus Išplėstinis nustatymas > **Apsaugos priemonės SSL / TLS** > **Sertifikavimo taisyklės** > **Redaguoti**.

Sertifikato taisyklių langą sudaro:

Stulpeliai

Pavadinimas – sertifikato pavadinimas.

Sertifikato išdavėjas – sertifikato kūrėjo pavadinimas.

Sertifikato tema – temos laukas identifikuoja įmonę, susijusią su viešuoju raktu, laikomu temos viešojo rakto lauke.

Prieiga – kaip **Prieigos veiksmą** pasirinkite **Leisti** arba **Blokuoti**, kad leistumėte / užblokuotumėte šio sertifikato saugomą ryšį neatsižvelgiant į jo patikimumą. Pasirinkite **Automatinis**, kad leistumėte naudoti patikimus sertifikatus ir būtų klausiama dėl nepatikimų. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Nuskaityti – kaip **Nuskaitymo veiksmą** pasirinkite **Nuskaityti** arba **Ignoruoti**, kad šiuo sertifikatu saugomą ryšį nuskaitytumėte arba ignoruotumėte. Pasirinkite **Automatinis**, kad būtų nuskaitoma automatiniu režimu ir būtų klausiama interaktyviuoju režimu. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Valdymo elementai

Pridėti – pridėkite naują sertifikatą ir reguliuokite jo nustatymus, susijusius su prieiga ir nuskaitymo parinktimis.

Redaguoti – pasirinkite sertifikatą, kurį norite konfigūruoti, ir spustelėkite **Redaguoti**.

Naikinti – pasirinkite sertifikatą, kurį norite panaikinti, ir spustelėkite **Šalinti**.

Gerai / atšaukti – spustelėkite **Gerai**, jei norite įrašyti pakeitimus, arba spustelėkite **Atšaukti**, jei norite išeiti neįrašydami.

Šifruotas tinklo srautas

Jei jūsų sistema sukonfigūruota naudoti SSL/TLS nuskaitymo procedūrą, toliau nurodytais dviem atvejais pasirodys dialogo langas, raginantis pasirinkti veiksmą:

Pirmiausia, jei svetainėje naudojamas nepatikrinamas arba negaliojantis sertifikatas, o ESET Internet Security yra sukonfigūruotas tokiais atvejais klausti naudotojo (pagal numatytuosius parametrus atsakymas yra „Taip“ dėl nepatikrinamų sertifikatų ir „Ne“ dėl negaliojančių sertifikatų), dialogo lange jūsų bus paklausta, ar tokį ryšį **Leisti**, ar **Blokuoti**. Jei sertifikatas nerandamas Trusted Root Certification Authorities store (TRCA), jis laikomas nepatikimu.

Antra, jei **SSL/TLS režimas** yra nustatytas kaip **Interaktyvusis režimas**, dialogo lange, pateikiamame prie kiekvienos svetainės, jūsų bus paklausta, ar srautą **Nuskaityti**, ar **Ignoruoti**. Kai kurios programos tikrina, ar jų SSL srautas nėra kieno nors modifikuotas ar tikrintas: tokiais atvejais ESET Internet Security turi **Ignoruoti** tą srautą, kad programa ir toliau veiktų normaliai.

> **Iliustruoti pavyzdžiai**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> - Sertifikatų pranešimai ESET „Windows“ namų produktuose
> - „Šifruotas tinklo srautas: nepatikimas sertifikatas“ – Lankantis tinklalapiuose rodomas pranešimas

Abiem atvejais vartotojas gali nurodyti įsiminti pasirinktą veiksmą. Įrašyti veiksmai saugomi Sertifikavimo taisyklės.

El. pašto programų apsauga

Norėdami sukonfigūruoti el. pašto programų apsaugą, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** ir pasirinkite iš šių konfigūravimo parinkčių:

- Pašto perdavimo apsauga
- Pašto dėžutės apsauga
- Adresų sąrašų tvarkymas
- ThreatSense

Pašto perdavimo apsauga

IMAP(S) ir POP3(S) yra populiariausi protokolai, naudojami el. pašto ryšiams priimti el. pašto programoje. Interneto pranešimų prieigos protokolas (IMAP) yra dar vienas el. pašto interneto protokolas. IMAP turi kai kurių privalumų prieš POP3, pavyzdžiui, keletas klientų gali vienu metu prisijungti prie tos pačios pašto dėžutės ir tvarkyti laiško būsenos informaciją (pvz., ar pranešimas buvo perskaitytas, atsakytas arba panaikintas). Apsaugos modulis, atliekantis šią kontrolę, automatiškai inicijuojamas paleisties metu ir tada yra aktyvus atmintyje.

ESET Internet Security užtikrina šių protokolų apsaugą neatsižvelgiant į naudojamą el. pašto klientą ir nereikalaujant el. pašto kliento perkonfigūravimo. Pagal numatytuosius nustatymus, visas ryšys, einantis per POP3 ir IMAP protokolus, yra nuskenuojamas nepaisant numatytųjų POP3 / IMAP prievadų skaičių.
MAPI protokolas nenuskaitytas. Tačiau ryšį su Microsoft Exchange serveriu gali nuskaityti integracijos modulis el. pašto kliente, pavyzdžiui, „Microsoft Outlook“.

ESET Internet Security papildomai dera su IMAPS (585, 993) ir POP3S (995) protokolų nuskaitymo funkcija. Šie protokolai informacijai tarp serverio ir kliento siųsti naudoja šifruotą kanalą. ESET Internet Security tikrina ryšius naudodama SSL (saugaus lizdo lygmens) ir TLS (transportavimo lygmens saugumo) protokolus. Šifruotas ryšys bus nuskaitytas pagal numatytuosius nustatymus. Norėdami peržiūrėti skaitytuvo nustatymus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > SSL / TLS.

Norėdami sukonfigūruoti pašto perdavimo apsaugą, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** > **Pašto perdavimo apsauga**.

Įjungti pašto perdavimo apsaugą – kai ši funkcija įjungta, pašto perdavimo ryšį nuskaitys ESET Internet Security.

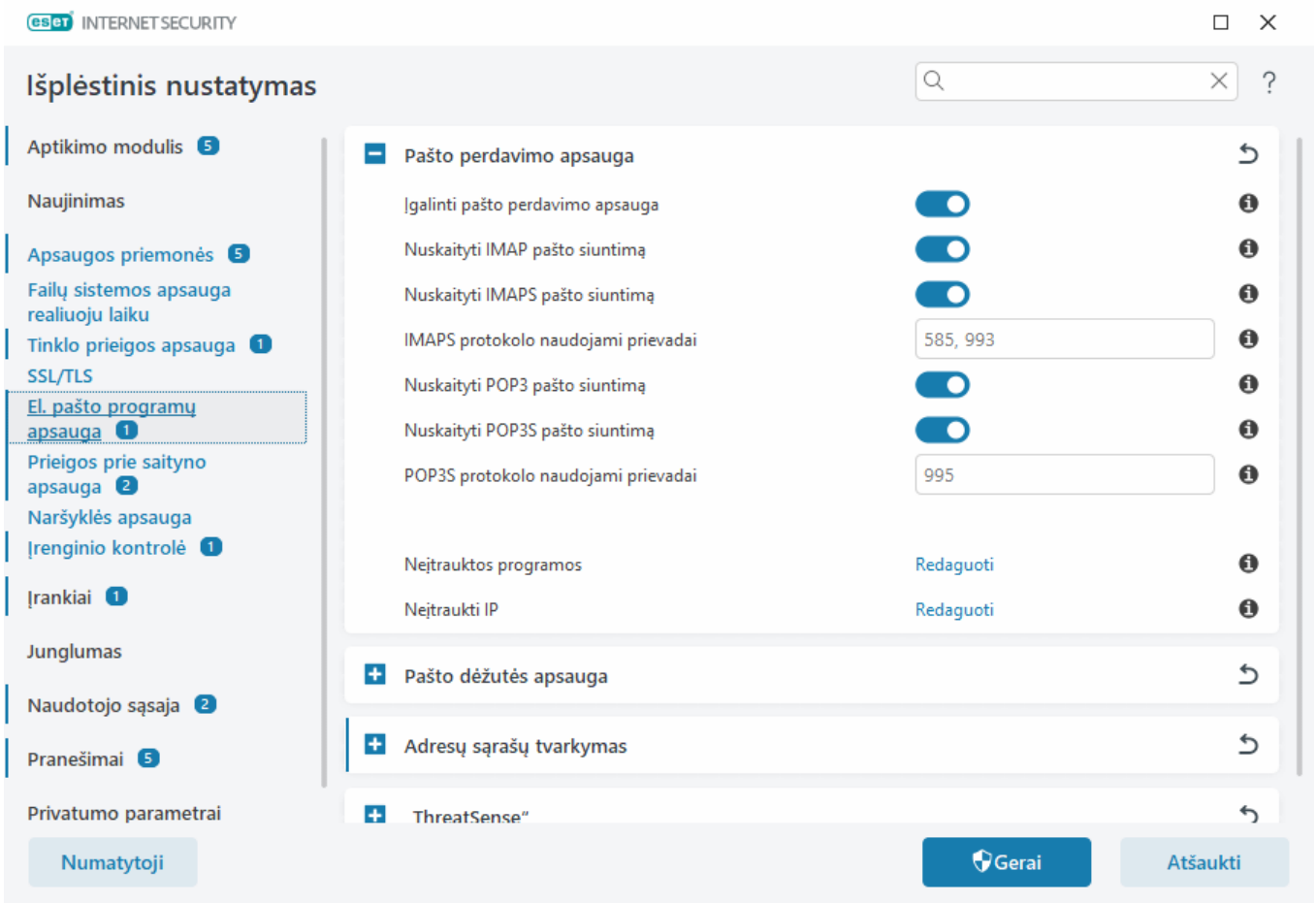
Galite pasirinkti, kurie pašto perdavimo protokolai bus nuskaityti, spustelėdami perjungiklį šalia šių parinkčių (pagal numatytuosius nustatymus įjungtas visų protokolų nuskaitymas):

- **Nuskaityti IMAP pašto siuntimą**
- **Nuskaityti IMAPS pašto siuntimą**
- **Nuskaityti POP3 pašto siuntimą**
- **Nuskaityti POP3S pašto siuntimą**

Pagal numatytuosius nustatymus ESET Internet Security nuskaitys IMAPS ir POP3S ryšį standartiniuose prievaduose. Norėdami įtraukti pasirinktinius IMAPS ir POP3S protokolų prievadus, įtraukite juos į teksto lauką, esantį šalia **IMAPS protokolo naudojami prievadai** arba **POP3S protokolo naudojami prievadai**. Kelių prievadų numerius reikia atskirti kableliais.

Nejtrauktos programos – leidžia pašalinti konkrečias programas, kurių negalima nuskaityti naudojant pašto perdavimo apsaugą. Tai naudinga, kai prieigos prie saityno apsauga sukelia suderinamumo problemų.

Nejtraukti IP – leidžia pašalinti konkrečius nuotolinius adresus, kad jie nebūtų nuskaitomi naudojant pašto perdavimo apsaugą. Tai naudinga, kai prieigos prie saityno apsauga sukelia suderinamumo problemų.



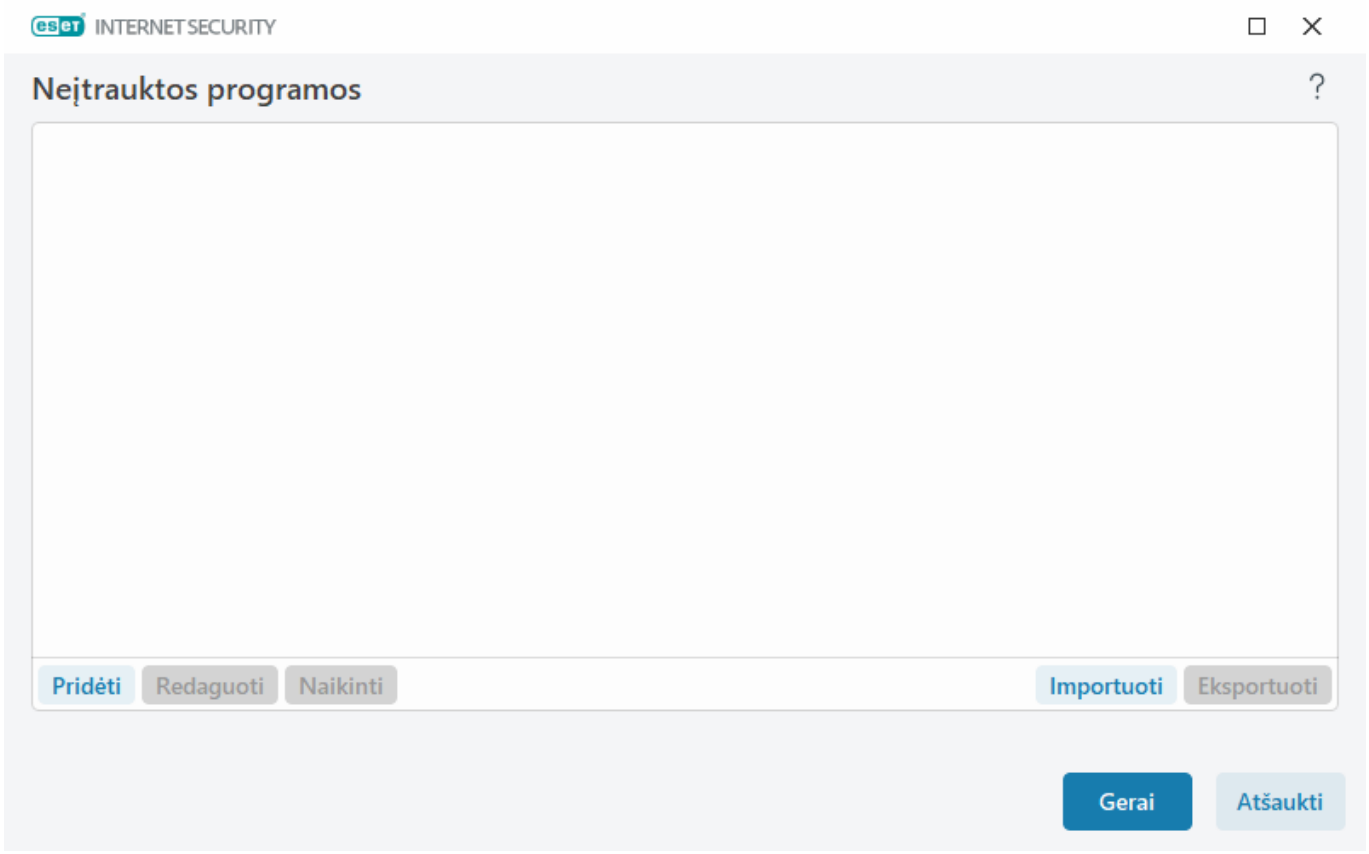
Neįtrauktos programos

Norėdami neįtraukti ryšių nuskaitymo konkrečioms programoms, įtraukite jas į sąrašą. Pasirinktų programų HTTP(S) / POP3(S) / IMAP(S) ryšys nebus tikrinamas ieškant grėsmių. Šią parinktį rekomenduojame naudoti tik programoms, kurios tinkamai neveikia, kai tikrinamas jų ryšys.

Veikiančios programos ir paslaugos čia bus automatiškai pasiekiamos, kai spustelėsite **Pridėti**. Spustelėkite **...** ir eikite į programą, kad rankiniu būdu pridėtumėte išimtį.

Redaguoti – suredaguokite pasirinktus sąrašo įrašus.

Šalinti – šalina pasirinktus įrašus iš sąrašo.



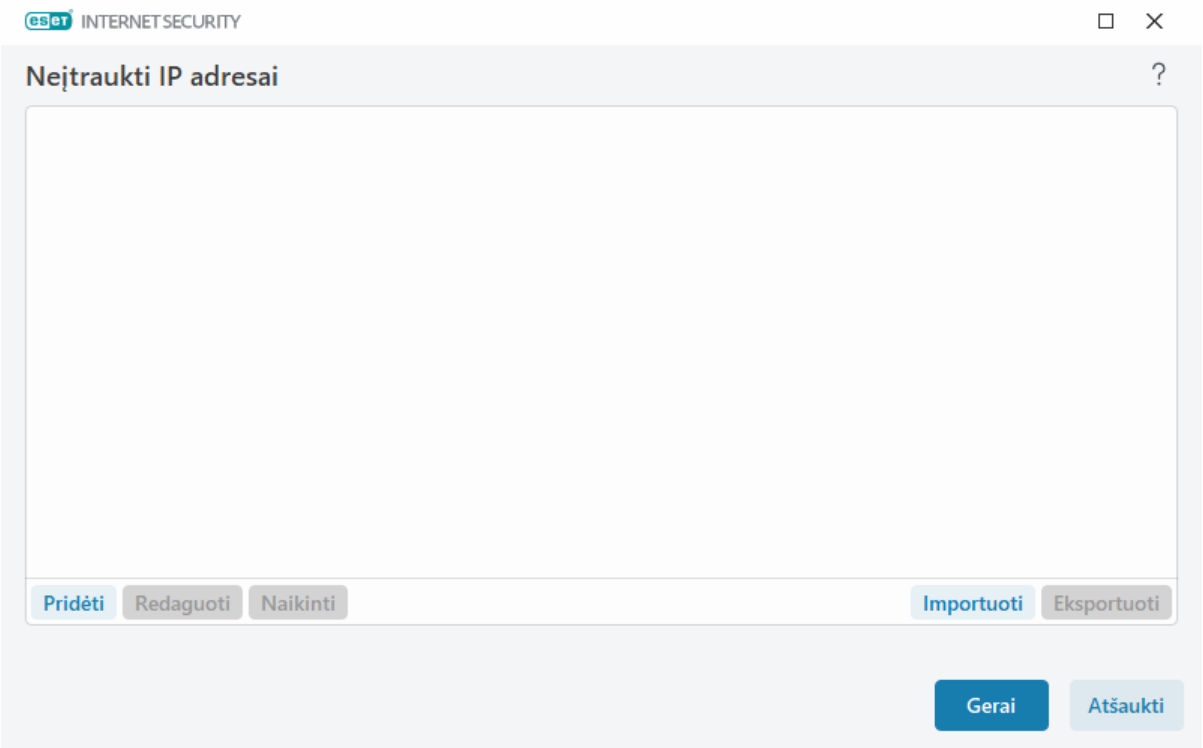
Nejtraukti IP

Įrašai sąraše bus neįtraukti į nuskaitymą. HTTP(S) / POP3(S) / IMAP(S) ryšys į pasirinktus adresus ir iš jų nebus tikrinamas ieškant grėsmių. Rekomenduojame naudoti šias parinktis tik adresams, kurie žinomi kaip patikimi.

Spustelėkite **Pridėti**, jei nenorite įtraukti nuotolinio taško IP adreso / adresų diapazono / potinklio.

Spustelėkite **Redaguoti**, jei norite pakeisti pasirinktą IP adresą.

Spustelėkite **Šalinti** ir pašalinkite pasirinktus įrašus iš sąrašo.



IP adresų pavyzdžiai

Pridėti IPv4 adresą:

Vienas adresas – prideda atskiro kompiuterio IP adresą (pvz., *192.168.0.10*).

Adresų diapazonas – įveda pradinį ir galutinį IP adresus, kad būtų nurodytas keleto kompiuterių IP diapazonas (pavyzdžiui, *192.168.0.1 – 192.168.0.99*).

Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė). Pavyzdžiui, 255.255.255.0 yra 192.168.1.0 potinklio tinklo kaukė. Norėdami išskirti visą potinklį, įveskite *192.168.1.0/24*.

Pridėti IPv6 adresą:

Vienas adresas – prideda atskiro kompiuterio IP adresą, kuriam bus taikoma taisyklė (pavyzdžiui, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė) (pavyzdžiui, *2002:c0a8:6301:1::1/64*).

Pašto dėžutės apsauga

Integravimas ESET Internet Security su jūsų pašto dėžute padidina el. laiškų aktyviosios apsaugos nuo kenkėjiškų kodų lygį.

Norėdami sukonfigūruoti pašto dėžutės apsaugą, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** > **Pašto dėžutės apsauga**.

Įjungti el. pašto apsaugą naudojant pašto programos papildinius – kai išjungta, apsauga naudojant el. pašto kliento papildinius yra išjungta.

Pasirinkite el. laiškus, kuriuos norite nuskaityti:

- **Gauti el. laiškai**
- **Išsiųsti el. laiškai**
- **Perskaityti el. laiškai**

- **Modifikuotas el. paštas**

Rekomenduojame laikyti **Įjungti el. pašto apsaugą naudojant pašto programos papildinius** įjungtą. Net jei integracija neįjungta ar neveikia, bendravimas el. paštu vis tiek saugomas Pašto perdavimo apsauga (IMAP/IMAPS ir POP3/POP3S).

Nuskaityti ieškant brukalo

Nepageidaujami el. laiškai, vadinami brukalu, yra viena didžiausių elektroninių ryšių problemų. Brukalas užima iki 30 procentų visų el. pašto ryšių. El. pašto programos apsauga nuo brukalo padeda apsisaugoti nuo šios problemos. Suderindamas keletą el. pašto saugos principų, el. pašto programos apsauga nuo brukalo užtikrina nepalyginamai pranašesnį filtravimą, kad jūsų pašto dėžutė išliktų švari. Norint aptikti brukalą, vienas svarbus principas yra nepageidaujamų el. laiškų atpažinimas pagal iš anksto nustatytus patikimus adresus (leidžiamus) ir brukalo adresus (užblokuotus).

Pagrindinis metodas, taikomas brukalui aptikti, yra el. laiškų ypatybių nuskaitymas. Gauti laiškai yra nuskaitomi remiantis pagrindiniais apsaugos nuo brukalo kriterijais (laiško apibrėžtys, statistinė euristika, atpažinimo algoritmai ir kiti unikalūs metodai) ir gauta indekso reikšmė nusako, ar laiškas yra brukalas, ar ne.

Įgalinti el. pašto programos apsaugą nuo brukalo – kai ši funkcija įjungta, gauti pranešimai bus nuskaitomi ieškant pašto šiukšlių.

Naudokite išplėstinį pašto šiukšlių skaitytuvą – periodiškai atsisiunčiami papildomi apsaugos nuo brukalo duomenys leidžia padidinti apsaugą nuo brukalo ir tokiu būdu pasiekti geresnių rezultatų.

Brukalo rezultatų registravimas – ESET Internet Security apsaugos nuo brukalo modulis priskiria brukalo tikimybę kiekvienam nuskaitytam laiškui. Laiškas bus įrašytas į apsaugos nuo brukalo žurnalą (Pagrindinis programos langas > **Įrankiai** > **Žurnalo failai** > **El. pašto programos apsauga nuo brukalo**).

- **Nėra** – apsaugos nuo brukalo nuskaitymo nustatytas tikimybės lygis nėra registruojamas.
- **Perskirstyta ir pažymėta kaip brukalas** – pasirinkite šią parinktį, jei norite užregistruoti laiškų, pažymėtų kaip SPAM, brukalo tikimybės lygį.
- **Viskas** – visi laiškai bus įrašyti į žurnalą nurodant brukalo tikimybės lygį.

Nepageidaujamų laiškų aplanke spustelėję laišką galite pasirinkti **Perskirstyti pasirinktus laiškus ir nepriskirti brukalui**, kad laiškas būtų perkeltas į gautų laiškų aplanką. Gautų laiškų aplanke spustelėję laišką, kurį laikote brukalu, pasirinkite **Perskirstyti laiškus ir priskirti brukalui**, kad laiškas būtų perkeltas į nepageidaujamų laiškų aplanką. Galite pasirinkti kelis laiškus, kad vienu metu su jais visais atliktumėte veiksmą.

Priedų tvarkymo optimizavimas – jei optimizavimas išjungtas, visi priedai nuskaitomi iš karto. Gali būti, kad el. pašto programos našumas sulėtėja.

Integravimo priemonės – leidžia integruoti pašto dėžutės apsaugą į el. pašto programą. Norėdami gauti daugiau informacijos, žiūrėkite Integravimo priemonės.

Atsakas – leidžia tinkinti pašto šiukšlių pranešimų tvarkymą. Norėdami gauti daugiau informacijos, žiūrėkite Atsakas.

Integravimo priemonės

ESET Internet Security Integravimas el. pašto programoje padidina aktyvios apsaugos nuo kenkimo kodų lygį el. laiškuose. Jeigu jūsų el. pašto programa yra palaikoma, integravimą galite įjungti programoje „ESET Internet Security“. Integravus į el. pašto programą ESET Internet Security įrankių juosta įterpiama tiesiai į šią programą, kad būtų efektyviau saugomas el. paštas. Norėdami redaguoti integravimo nustatymus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** > **Pašto dėžutės apsauga** > **Integracija**.

Integruoti į „Microsoft Outlook“ – „Microsoft Outlook“ šiuo metu yra vienintelė palaikoma el. pašto programa. El. pašto apsauga veikia kaip papildinys. Pagrindinis papildinio privalumas yra tas, kad jis nepriklauso nuo naudojamo protokolo. Kai el. pašto programa gauna šifruotą laišką, jis iššifruojamas ir siunčiamas į virusų skaitytuvą. Šiame ESET žinių bazės straipsnyje rasite išsamų palaikomų „Microsoft Outlook“ versijų sąrašą.

Išplėstinis el. pašto programos apdorojimas – apdorojami papildomi Outlook Messaging API (MAPI) įvykiai: Objektas modifikuotas (`fnevObjectModified`) ir objektas sukurtas (`fnevObjectCreated`). Jei dirbdami su savo el. pašto programa pastebite, kad sistema sulėtėjo, išjunkite šią parinktį.

„Microsoft Outlook“ įrankių juosta

„Microsoft Outlook“ apsauga veikia kaip papildinio modulis. Įdiegus ESET Internet Security, ši įrankių juosta, kurioje yra apsaugos nuo virusų antivirusinės programos ir el. pašto programos apsaugos nuo brukalo parinktys, įtraukiama į „Microsoft Outlook“:

Brukalas – pažymi pasirinktus laiškus kaip brukalą. Pažymėjus laiško „kontroliniai kodai“ siunčiami į centrinį serverį, kaupiantį brukalo kodus. Jeigu serveris gauna daugiau panašių „kontrolinių kodų“ iš keleto vartotojų, pranešimas ateityje bus klasifikuojamas kaip brukalas.

Ne brukalas – pažymi pasirinktus laiškus kaip ne brukalą.

Brukalo adresas (užblokuotas, brukalo adresų sąrašas) – įtraukia naują siuntėjo adresą kaip užblokuotą į adresų sąrašą. Visi laiškai, gauti iš šio sąrašo, bus automatiškai klasifikuojami kaip brukalas.

> Saugokitės apsimetinėjimo – siuntėjo adreso klastojimo el. laiškuose, siekiant suklaidinti el. laiško gavėjus, kad jie perskaitytų laišką ir atsakytų į jį.

Patikimas adresas (leidžiamas, patikimų adresų sąrašas) – įtraukia naują siuntėjo adresą kaip leidžiamą į adresų sąrašą. Visi laiškai, gauti iš leidžiamų adresų, niekada automatiškai nebus klasifikuojami kaip brukalas.

ESET Internet Security Dukart spustelėkite piktogramą, kad atidarytumėte pagrindinį ESET Internet Security langą.

Nuskaityti iš naujo laiškus – leidžia paleisti el. pašto tikrinimą rankiniu būdu. Galite nurodyti laiškus, kurie bus tikrinami, ir galite aktyvinti pakartotinį gautų el. laiškų nuskaitymą. Daugiau informacijos žr. Pašto dėžutės apsauga.

Skaitytuvo nustatymas – rodomos pašto dėžutės apsaugos nustatymo parinktys.

Apsaugos nuo brukalo nustatymas – rodomos pašto dėžutės apsaugos nustatymo parinktys.

Adresų knygos – atidaro langą Adresų sąrašų tvarkymas, kuriame galite rasti neįtrauktų, patikimų ir brukalo adresų sąrašus.

Patvirtinimo dialogas

Šis pranešimas leidžia įsitikinti, kad vartotojas tikrai nori atlikti pasirinktą veiksmą, kuris padėtų išvengti galimų klaidų.

Kita vertus, dialogas siūlo galimybę atsisakyti patvirtinimų.

Nuskaityti iš naujo laiškus

ESET Internet Security įrankių juosta, integruota į el. pašto programas, leidžia vartotojams nurodyti keletą el. laiškų tikrinimo parinkčių. Parinktis **Nuskaityti iš naujo laiškus** siūlo du nuskaitymo režimus:

Visus laiškus esamame aplanke – nuskaito laiškus šiuo metu rodomame aplanke.

Tik pasirinktus laiškus – nuskaito tik vartotojo pažymėtus laiškus.

Žymės langelis **Nuskaityti iš naujo jau nuskaitytus laiškus** suteikia vartotojui galimybę paleisti dar kartą nuskaityti laiškus, kurie buvo nuskaityti anksčiau.

Atsakas

Atsižvelgdami į pranešimų nuskaitymo rezultatus, ESET Internet Security galite perkelti nuskaitytus pranešimus arba pridėti pasirinktinį tekstą prie temos. Šiuos parametrus galite konfigūruoti dalyje Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programos apsauga** > **Pašto dėžutės apsauga** > **Atsakas**.

El. pašto programos apsauga nuo brukalo ESET Internet Security leidžia konfigūruoti šiuos pranešimų parametrus:

Pridėti tekstą prie el. pašto temos – leidžia įtraukti pasirinktinę prefikso eilutę į laiško, kuris buvo klasifikuotas kaip brukalas, temos eilutę. **Numatytasis tekstas** yra „[SPAM]“.

Perkelti į brukalo aplanką – įjungus brukalo laiškai bus perkeliami į numatytąjį nepageidaujamų el. laiškų aplanką, laiškai identifikuoti kaip ne brukalas bus perkelti į gautų laiškų aplanką. Dešiniuoju pelės klavišu spustelėdami el. laišką ir kontekstiniame meniu pasirinkdami ESET Internet Security galite pasirinkti taikytinas parinktis.

Perkelti į pasirinktinį aplanką – kai įjungta, brukalo pranešimai bus perkelti į toliau nurodytą aplanką.

Aplankas – nurodykite pasirinktinį aplanką, į kurį pageidaujate perkelti aptiktus užkrėstus el. laiškus.

Jei yra pranešimas, kuriame yra aptikimas, pagal numatytuosius nustatymus ESET Internet Security bando išvalyti pranešimą. Jei pranešimo negalima išvalyti, galite pasirinkti **Veiksmai, kurių reikia imtis, jei išvalyti neįmanoma**:

- **Nieko nedaryti** – jeigu įjungta, programa identifikuos užkrėstus priedus, tačiau paliks el. laiškus neatlikdama jokių veiksmų.
- **Naikinti el. laišką** – programa praneš vartotojui apie įsiskverbimą (-us) ir panaikins laišką.

- ***Perkelti el. laiškus į panaikintų elementų aplanką** – užkrėsti el. laiškai bus automatiškai perkeliami į Panaikintų elementų aplanką.

- **Perkelti el. laiškus į aplanką** (numatytasis veiksmas) – užkrėsti el. laiškai bus automatiškai perkeliami į nurodytą aplanką.

Aplankas – nurodykite pasirinktinį aplanką, į kurį pageidaujate perkelti aptiktus užkrėstus el. laiškus.

Pažymėti brukalo laiškus kaip perskaitytus – įjunkite šią parinktį, jeigu norite automatiškai pažymėti brukalą kaip perskaitytą. Tai padės patogiau atkreipti dėmesį į „švarius“ laiškus.

Pažymėti perklasifikuotus pranešimus kaip neskaitytus – laiškai, kurie iš pradžių buvo klasifikuoti kaip brukalas, tačiau vėliau pažymėti kaip „švarūs“, bus rodomi kaip neskaityti.

Patikrinus el. laišką, pranešimas su nuskaitymo rezultatais gali būti prijungiamas prie laiško. Galite nuspręsti **Prijungti gairės pranešimus prie gautų ir perskaitytų el. laiškų** arba **Prijungti gairės pranešimus prie išsiųstų el. laiškų**. Atminkite, kad retais atvejais gairių pranešimai probleminiuose HTML pranešimuose gali būti praleisti arba suklastoti kenkimo programinės įrangos. Gairės pranešimai gali būti pridėti prie gautų ir perskaitytų el. laiškų, prie išsiųstų el. laiškų arba prie abiejų. Galimos šios parinktys:

- **Niekada** – gairės pranešimai nebus pridedami.

- **Aptikus** – tik kenkėjiškas programas turintys laiškai bus pažymėti kaip patikrinti (numatytoji parinktis).

- **Visiems nuskaitytiems el. laiškams** – programa prijungs pranešimus prie visų nuskaitytų el. laiškų.

Atnaujinti gauto ir perskaityto el. laiško temą / **Atnaujinti išsiųsto el. laiško temą** – įjunkite šią parinktį, kad prie pranešimo pridėtumėte toliau nurodytą pasirinktinį tekstą.

Tekstas pridėtas prie užkrėsto el. laiško temos – redaguokite šį šabloną, jeigu norite pakeisti užkrėsto el. laiško temos prefikso formatą. Ši funkcija pakeis pranešimo temą „Sveiki“ tokiu formatu: „[aptikimas %APTIKIMO PAVADINIMAS%] Sveiki“. Kintamasis %DETECTIONNAME% nurodo aptikimą.

Adresų sąrašų tvarkymas

El. pašto programos apsaugos nuo brukalo funkcija ESET Internet Security leidžia konfigūruoti įvairius adresų sąrašų parametrus. Norėdami konfigūruoti adresų sąrašus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** > **Adresų sąrašų tvarkymas**.

Įgalinti naudotojo adresų sąrašą – įgalinkite šią parinktį, kad aktyvintumėte naudotojo adresų sąrašą.

Naudotojo adresų sąrašas – el. pašto adresų sąrašas, kuriame galite pridėti, redaguoti arba šalinti adresus, kad nustatytumėte apsaugos nuo brukalo taisykles. Šio sąrašo taisyklės bus taikomos dabartiniam naudotojui.

Įgalinti visuotinį adresų sąrašą – įgalinkite šią parinktį norėdami aktyvinti visuotinį adresų sąrašą, kurį bendrina visi naudotojai šiame įrenginyje.

Visuotinis adresų sąrašas – el. pašto adresų sąrašas, kuriame galite pridėti, redaguoti arba šalinti adresus, kad nustatytumėte apsaugos nuo brukalo taisykles. Šio sąrašo taisyklės bus taikomos visiems naudotojams.

Automatiškai leisti ir įtraukti į naudotojo adresų sąrašą

Adresų knygelėje esančius adresatus laikyti patikimais – Jūsų adresatų sąraše esantys adresai bus laikomi patikimais neįtraukiant jų į naudotojo adresų sąrašą.

Pridėti siunčiamų laiškų gavėjų adresus – pridėkite išsiųstų laiškų gavėjų adresus prie naudotojo adresų sąrašo, kaip leidžiama.

Pridėti adresus iš laiškų, kurie buvo perklasifikuoti kaip NE brukalas – pridėkite prie naudotojo adresų sąrašo siuntėjų adresus iš laiškų, kurie buvo perklasifikuoti kaip NE brukalas, kaip leidžiama.

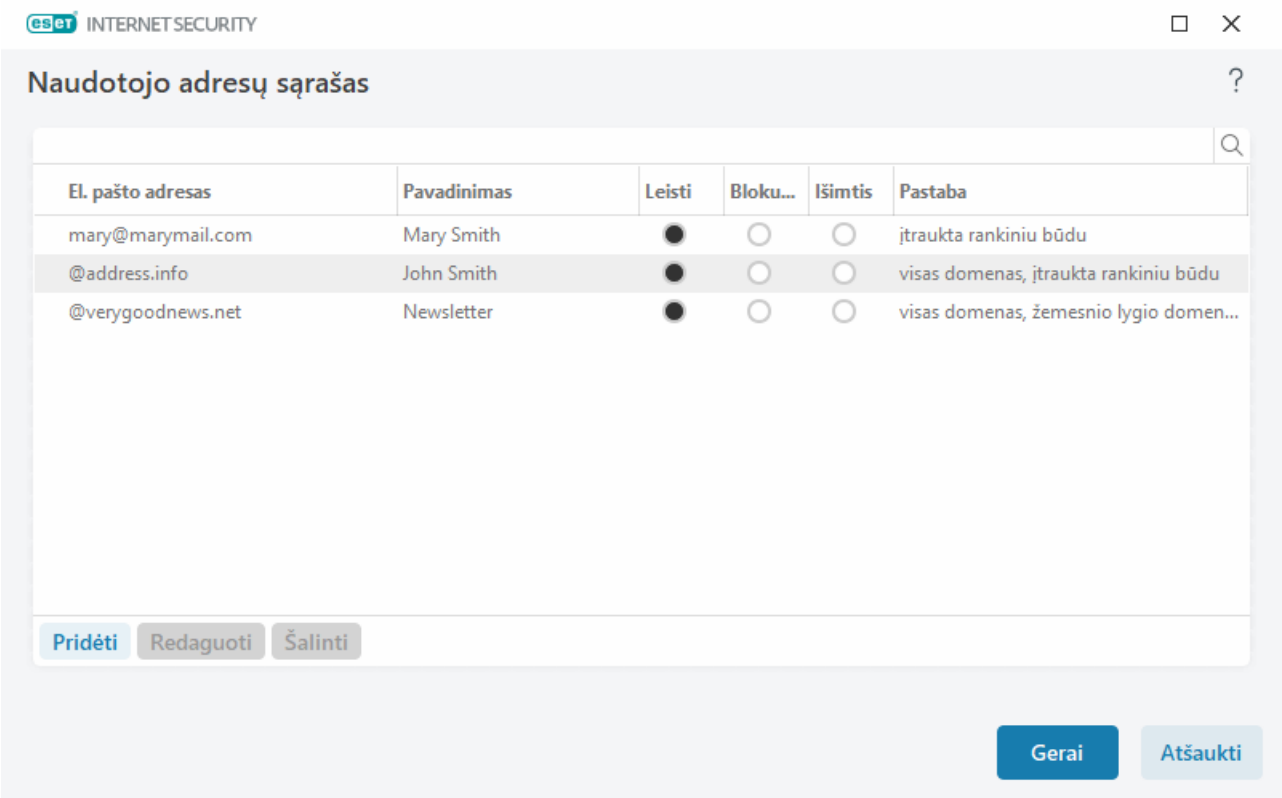
Automatiškai įtraukti į naudotojo adresų sąrašą kaip išimtį

Pridėti adresus iš savo paskyrų – pridėkite prie naudotojo adresų sąrašo adresus iš esamų el. pašto programos paskyrų kaip išimtį.

Adresai sąrašas

Norėdami apsisaugoti nuo nepageidaujamų el. laiškų, ESET Internet Security galite klasifikuoti el. pašto adresus adresų sąrašuose.

Norėdami redaguoti adresų sąrašus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **El. pašto programų apsauga** > **Adresų sąrašų tvarkymas** ir spustelėkite **Redaguoti** šalia **Naudotojo adresų sąrašas** arba **Visuotinis adresų sąrašas**.



Stulpeliai

El. pašto adresas – adresas, kuriam bus taikoma taisyklė. Pakaitos simboliai nepalaikomi.

Pavadinimas – pasirinktinis taisyklės pavadinimas.

Leisti / blokuoti / išimtis – radijo mygtukai, naudojami nustatyti, kokių veiksmų imtis el. pašto adresui (spustelėkite norimo stulpelio radijo mygtuką, kad greitai pakeistumėte veiksmą):

- **Leisti** – adresai, kurie laikomi saugiais ir iš kurių norite gauti laiškus.
- **Blokuoti** – adresai, kurie laikomi nesaugiais / brukalu ir iš kurių nenorite gauti laiškų.
- **Išimtis** - adresai, kurie visada tikrinami dėl brukalo ir kurie gali būti suklastoti ir naudojami brukalui siųsti.

Pastaba – informacija apie tai, kaip taisyklė buvo sukurta ir ar ji taikoma visam domenui / žemesnio lygio domenams.

Adresų tvarkymas

- **Pridėti** – spustelėkite, jei norite pridėti taisyklę naujam adresui.
- **Redaguoti** – pasirinkite ir spustelėkite, jei norite redaguoti esamą taisyklę.
- **Pašalinti** – pasirinkite ir spustelėkite, jei norite pašalinti taisyklę iš adresų sąrašo.

Adreso pridėjimas / redagavimas

Šis langas leidžia pridėti arba redaguoti adresą, įtrauktą į Adresų sąrašų tvarkymas ir konfigūruoti atliktą veiksmą:

El. pašto adresas – adresas, kuriam bus taikoma taisyklė.

Pavadinimas – pasirinktinis taisyklės pavadinimas.

Veiksmas – veiksmas, kurio reikia imtis, jei kontakto el. pašto adresas atitinka adresą, nurodytą lauke **El. pašto adresas**:

- **Leisti** – adresai, kurie laikomi saugiais ir iš kurių norite gauti laiškus.
- **Blokuoti** – adresai, kurie laikomi nesaugiais / brukalu ir iš kurių nenorite gauti laiškų.
- **Išimtis** - adresai, kurie visada tikrinami dėl brukalo ir kurie gali būti suklastoti ir naudojami brukalui siųsti.

Visas domenas – pasirinkite šią parinktį, kad taisyklė būtų taikoma visam kontakto domenui (ne tik adresui, nurodytam lauke **El. pašto adresas**, bet ir visiems el. pašto adresams domene *address.info*).

Žemesnio lygio domenai – pasirinkite šią parinktį, kad taisyklė būtų taikoma kontakto žemesnio lygio domenams (*address.info* nurodo domeną, o *my.address.info* – padomenį).

Adreso apdorojimo rezultatas

Pridedant naujus adresus arba keičiant el. pašto adresui skirtą veiksmą, ESET Internet Security rodomi pranešimai. Pranešimų turinys skiriasi atsižvelgiant į veiksmą, kurį bandote atlikti.

Pasirinkite žymės langelį **Daugiau neklausti**, kad kitą kartą veiksmas būtų atliekamas automatiškai, nerodant pranešimo.

ThreatSense

„ThreatSense“ sudaro įvairūs sudėtiniai grėsmių aptikimo metodai. Ši technologija yra iniciatyvi, o tai reiškia, kad ji užtikrina apsaugą, vos tik pradeda plisti nauja grėsmė. Joje kartu naudojama kodų analizė, kodų imitavimas, bendrieji kodai ir virusų kodai, kurie darniai veikia ir gerokai padidina sistemos saugumą. Nuskaitymo modulis gali vienu metu kontroliuoti keletą duomenų srautų – tai padidina efektyvumą ir aptikimo greitį. Be to, „ThreatSense“ technologija sėkmingai panaikina kenkėjiškas prieigos programas.

„ThreatSense“ modulio nustatymų parinktys leidžia nurodyti keletą nuskaitymo parametrų:

- failų, kurie turi būti nuskaityti, tipai ir plėtiniai;
- įvairių aptikimo metodų derinys;
- valymo lygiai ir t. t.

Norėdami patekti į nustatymo langą, išplėstinio nustatymo lange spustelėkite **„ThreatSense**“ parametrai, kad būtų parodyti moduliai, kuriems naudojama ThreatSense technologija (žr. toliau). Skirtingiems saugumo scenarijams gali reikėti skirtingų konfigūracijų. Atsižvelgiant į tai, „ThreatSense“ yra atskirai konfigūruojama šiems apsaugos moduliams:

- Failų sistemos apsauga realiuoju laiku
- Laukimo būsenos nuskaitymas
- Nuskaitymas paleidžiant
- Dokumentų apsauga
- El. pašto programų apsauga
- Prieigos prie saityno apsauga
- Kompiuterio nuskaitymas

„ThreatSense“ parametrai yra optimizuoti kiekvienam moduliui ir jų keitimas gali labai paveikti sistemos veikimą. Pavyzdžiui, pakeitus parametrus, kad visada būtų nuskaitomos momentinio pakavimo programos, arba įjungus išplėstinę euristiką failų sistemos apsaugos realiuoju laiku modulyje, sistemos darbas gali sulėtėti (paprastai naudojant šiuos metodus nuskaitomi tik naujai sukurti failai). Rekomenduojame palikti numatytuosius „ThreatSense“ parametrus nepakeistus visuose moduliuose, išskyrus kompiuterio nuskaitymą.

Nuskaitytini objektai

Šiame skyriuje galite nurodyti, kurie kompiuterio komponentai ir failai bus nuskaityti ieškant įsiskverbimų.

Operacinė atmintis – nuskaitomos grėsmės, kurios atakuoja sistemos operacinę atmintį.

Paleidimo sektorius / UEFI – nuskaitomi sistemos įkrovimo sektoriai tikrinant, ar nėra kenkėjiškos programinės įrangos pagrindiniame sistemos įkrovimo įraše. Daugiau apie UEFI skaitykite terminų žodyne.

El. laiškų failai – programa palaiko šiuos plėtinius: DBX („Outlook Express“) ir EML.

Archyvai – programa palaiko šiuos plėtinius: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ir daugelį kitų.

Išsiskleidžiantieji archyvai – išsiskleidžiantieji archyvai (SFX) yra archyvai, kurie gali išsiskleisti patys.

Momentiniai pakuotuvai – įvykdytos momentinio išpakavimo programos (skirtingai nei standartinių tipų archyvai) vėl suglaudinamos atmintyje. Be standartinių statinių pakavimo programų (UPX, yoda, ASPack, FSG ir t. t.), naudodamas kodų imitavimo principą skaitytuvas gali atpažinti kelis papildomus pakuotuvų tipus.

Nuskaitymo parinktys

Pasirinkite metodus, kurie bus naudojami nuskaitant sistemą ir ieškant įsiskverbimų. Galimos šios parinktys:

Euristika – euristika yra algoritmas, analizuojantis programų (kenkimo programinės įrangos) veiklą. Pagrindinis šios technologijos privalumas yra gebėjimas identifikuoti kenkimo programinę įrangą, kurios nebuvo ankstesnėje aptikimo modulio versijoje arba ji nebuvo žinoma. Trūkumas yra klaidingų pavojaus pranešimų (labai maža) tikimybė.

Išplėstinė euristika / DNA kodai – išplėstinė euristika yra unikalus ESET sukurtas algoritmas, optimizuotas aptikti kompiuterio kirminus bei Trojos arklius ir yra parašytas aukšto lygio programavimo kalbomis. Naudojant išplėstinę euristiką, gerokai padidėja ESET produktų grėsmių aptikimo galimybės. Kodai gali patikimai aptikti ir identifikuoti virusus. Naudojant automatinę naujinimo sistemą, nauji kodai tampa pasiekiami per kelias valandas nuo grėsmės atskleidimo. Kodų trūkumas yra tai, kad jie aptinka tik jiems žinomus virusus (arba šiek tiek modifikuotas jų versijas).

Valymas

Valymo parametrai apibrėžia ESET Internet Security veiksmus valant objektus. Yra 4 valymo lygiai:

ThreatSense siūlo šiuos atkūrimo (t. y. valymo) lygius.

Atkūrimas programoje ESET Internet Security

Valymo lygis	Aprašymas
Visada valyti objektą	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais retais atvejais (pvz., esant sisteminiams failams), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.

Valymo lygis	Aprašymas
Jei saugu, valyti objektą, priešingu atveju palikti	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais atvejais (pvz., esant sisteminiams failams arba archyvams, kuriuose yra ir švarūs, ir užkrėsti failai), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju paklausti	Valant objektus, bandoma atkurti aptikimą. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, galutiniam naudotojui rodomas interaktyvus įspėjimas ir jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Daugeliu atveju ši nuostata yra rekomenduojama.
Visada klausti galutinio naudotojo	Valant objektus, galutiniam naudotojui rodomas interaktyvus langas, kuriame jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Šis lygis skirtas labiau patyrusiems naudotojams, kurie žino, kokį veiksmą atlikti aptikimo atveju.

Išimtys

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis „ThreatSense“ parametrų nustatymo skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

Kita

Konfigūruojant „ThreatSense“ modulio kompiuterio užsakomojo nuskaitymo parametrų nustatymus, papildomai pasiekiamos ir šios parinktys, pateikiamos skyriuje **Kita**:

Nuskaityti kintamuosius duomenų srautus (ADS) – NTFS failų sistemos naudojami kintamieji duomenų srautai yra failų ir aplankų ryšiai, kurie nematomi įprastoms nuskaitymo priemonėms. Daugelis įsiskverbimų bando išvengti aptikimo apsimesdami kintamaisiais duomenų srautais.

Vykdyti mažo prioriteto foninius nuskaitymus – kiekviena nuskaitymo seka naudoja tam tikrą kiekį sistemos išteklių. Jeigu dirbate su programomis, kurios intensyviai naudoja sistemos išteklius, galite suaktyvinti mažo prioriteto foninį nuskaitymą ir taupyti išteklius savo programoms.

Registruoti visus objektus – nuskaitymo žurnale bus rodomi visi nuskaityti failai išsiskleidžiančiuosiuose archyvuose, net neužkrėsti (gali būti generuojama daug nuskaitymo žurnalo duomenų ir padidės nuskaitymo žurnalo failo dydis).

Įjungti išmanųjį optimizavimą – įjungus išmanųjį optimizavimą, naudojami optimaliausi parametrai, leidžiantys užtikrinti efektyviausią nuskaitymo lygį ir kartu palaikyti didžiausią nuskaitymo greitį. Įvairūs apsaugos moduliai išmaniai atlieka nuskaitymą, naudodami įvairius nuskaitymo metodus ir taikydami juos konkretiems failų tipams. Jei išmanusis optimizavimas išjungtas, atliekant nuskaitymą taikomi tik vartotojo apibrėžti parametrai tam tikrų modulių ThreatSense šerdyje.

Saugoti paskutinį prieigos laiką – nurodykite šią parinktį, norėdami išlaikyti nuskaitytų failų originalius prieigos laikus, o ne naujinti juos (pavyzdžiui, naudojant su duomenų atsarginio kopijavimo sistemomis).

Ribos

Ribų skyriuje galima nurodyti maksimalius nuskaitomų objektų dydžius ir archyvų įdėties lygius:

Objekto parametrai

Maksimalus objekto dydis – apibrėžia maksimalų nuskaitomų objektų dydį. Antivirusinės programos modulis nuskaitys tik mažesnius nei nurodytas dydis objektus. Šią parinktį turėtų keisti tik patyrę vartotojai, kurie gali turėti tam tikrų priežasčių neįtraukti didelių objektų į nuskaitymą. Numatytoji reikšmė: neribota.

Maksimali objekto nuskaitymo trukmė (sek.) – apibrėžia maksimalią objekto failų (pvz., esančių RAR / ZIP archyve arba el. laiške su keliais priedais) nuskaitymo trukmę. Šis nustatymas netaikomas pavieniams failams. Jei įvesta naudotojo apibrėžta vertė ir tas laikas praėjo, nuskaitymas bus sustabdytas kuo greičiau, neatsižvelgiant į tai, ar kiekvieno failo nuskaitymas objekte yra užbaigtas.
Archyvo su dideliais failais atveju nuskaitymas bus sustabdytas išskleidus failą iš archyvo (pvz., kai naudotojo apibrėžtas kintamasis yra 3 sekundės, bet failo išskleidimas užtrunka 5 sekundes). Praėjus nurodytam laikui, likę archyvo failai nebus nuskaitomi.
Norėdami apriboti nuskaitymo trukmę, taip pat ir didesnių archyvų atveju, naudokite parinktis **Maksimalus objekto dydis** ir **Maksimalus failo archyve dydis** (nerekomenduojama dėl galimos rizikos saugai).
Numatytoji reikšmė: neribota.

Archyvo nuskaitymo nustatymai

Archyvo įdėties lygis – nurodo maksimalų archyvų nuskaitymo gylį. Numatytoji vertė: 10.

Maksimalus failo archyve dydis – ši parinktis leidžia nurodyti, kokio maksimalaus dydžio (kai jie išskleidžiami) archyve esantys failai bus nuskaitomi. Maksimali reikšmė: **3 GB**.

> Mes nerekomenduojame keisti numatytųjų verčių: dirbant įprastai, jų keisti nėra priežasties.

Prieigos prie saityno apsauga

Prieigos prie saityno apsauga leidžia konfigūruoti išplėstinius interneto apsaugos modulio parametrus. Galimos šios parinktys Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga** > **Prieigos prie saityno apsauga**:

Įjungti prieigos prie saityno apsaugą – kai ši parinktis išjungta, prieigos prie saityno apsauga ir apsauga nuo sukčiavimo apsimetant nebus paleista.

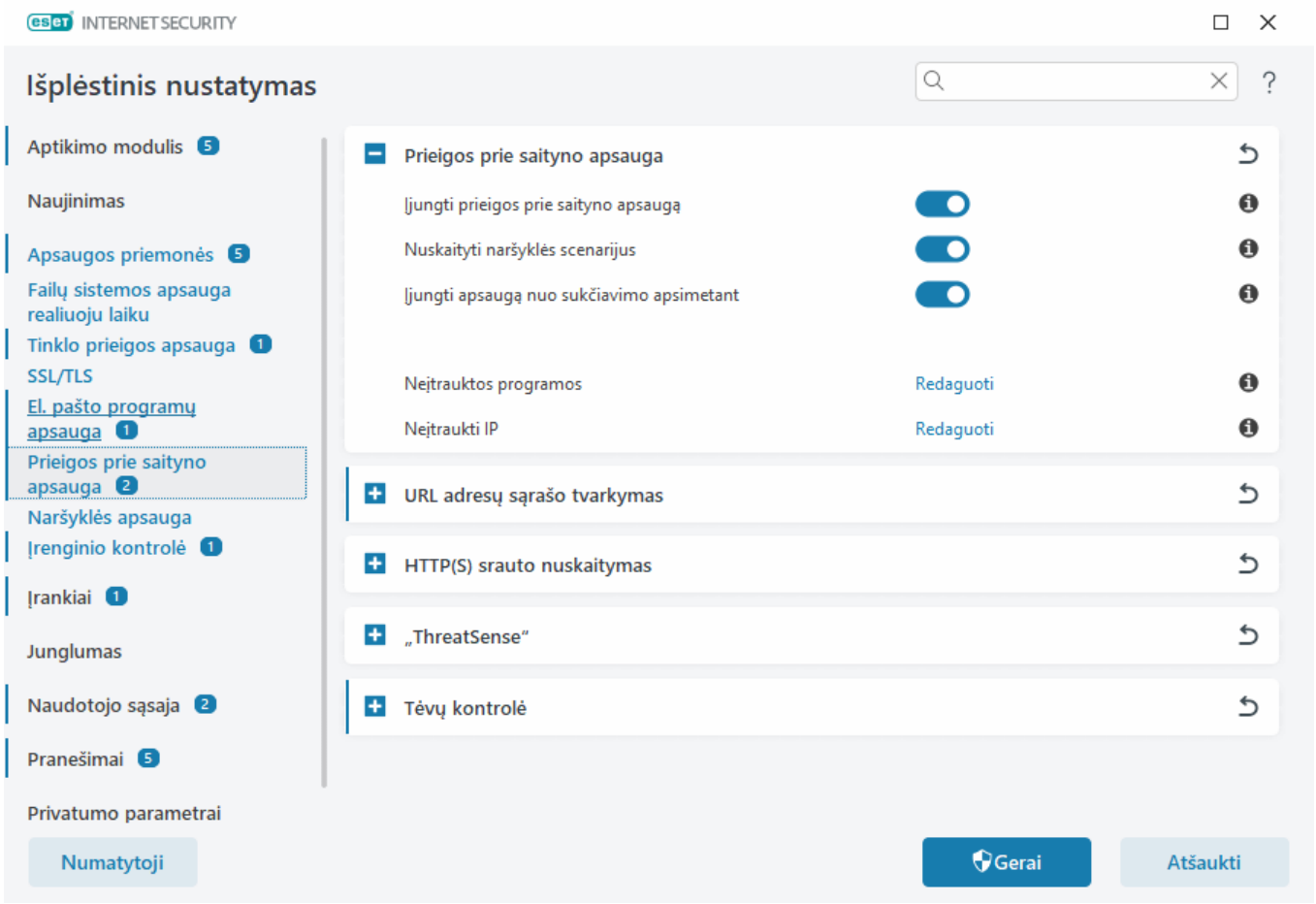
> Primygtinai rekomenduojame palikti prieigos prie saityno apsaugą įjungtą ir pagal numatytuosius nustatymus neišskirti jokių programų ar IP adresų.

Nuskaityti naršyklės scenarijus – kai įjungta, aptikimo modulis tikrina visas JavaScript žiniatinklio naršyklių vykdomas programas.

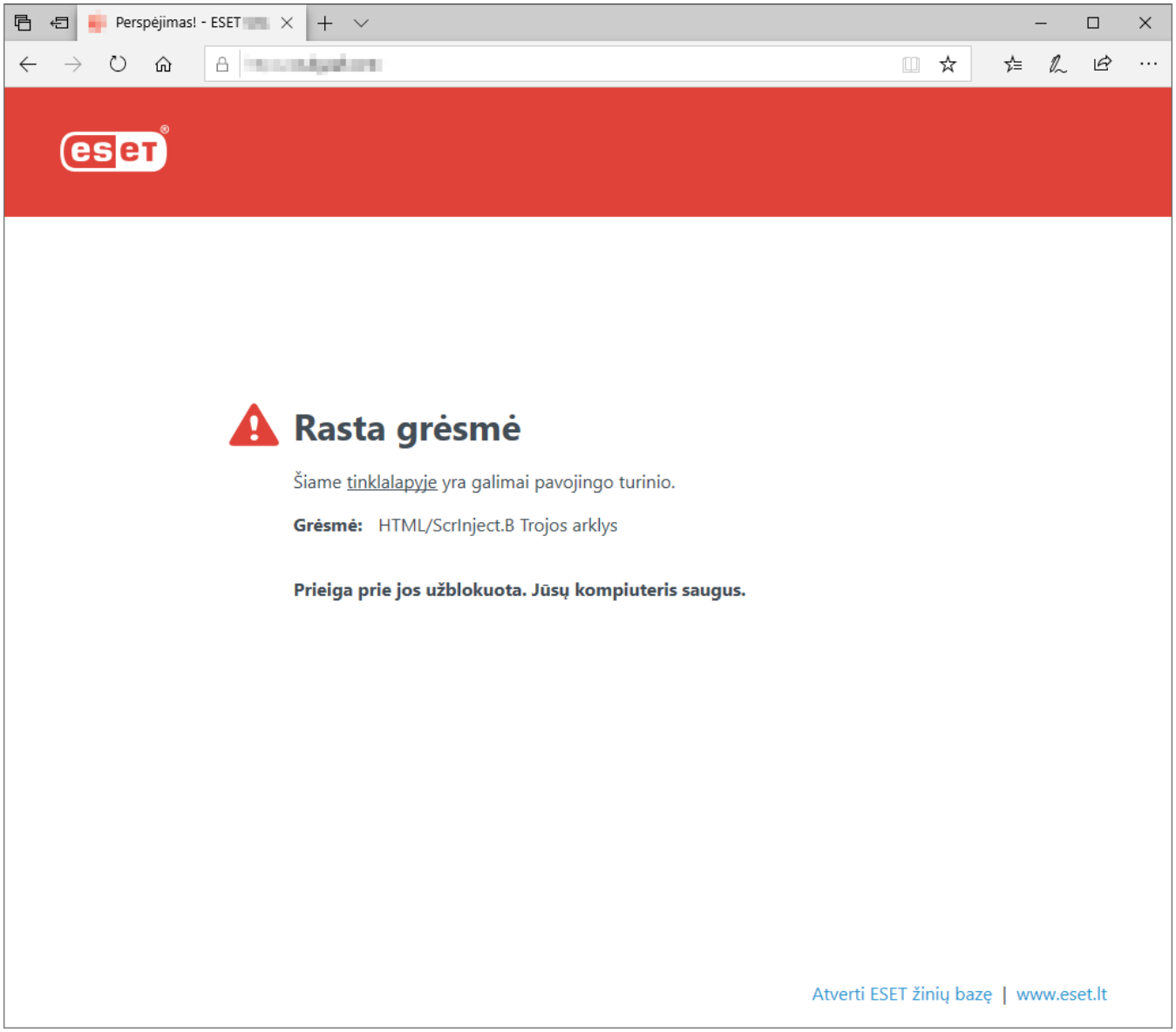
Įjungti apsaugą nuo sukčiavimo apsimetant – kai įjungta, apsimestiniai tinklalapiai blokuojami. Žr. Apsauga nuo sukčiavimo apsimetant, kur rasite papildomos informacijos.

Neįtrauktos programos – leidžia išskirti konkrečias programas, kurių negalima nuskaityti naudojant prieigos prie saityno apsaugą. Naudinga, kai prieigos prie saityno apsauga sukelia suderinamumo problemų.

Neįtraukti IP – leidžia išskirti konkrečius nuotolinius adresus, kad jų nebūtų galima nuskaityti naudojant prieigos prie saityno apsaugą. Naudinga, kai prieigos prie saityno apsauga sukelia suderinamumo problemų.



Prieigos prie saityno apsauga naršyklėje rodys toliau nurodytą pranešimą, kai svetainė užblokuota:



Iliustruotos instrukcijos

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:

- Neleisti blokuoti saugios interneto svetainės, kai taikoma prieigos prie saityno apsauga
- Blokuoti interneto svetainę naudojant ESET Internet Security

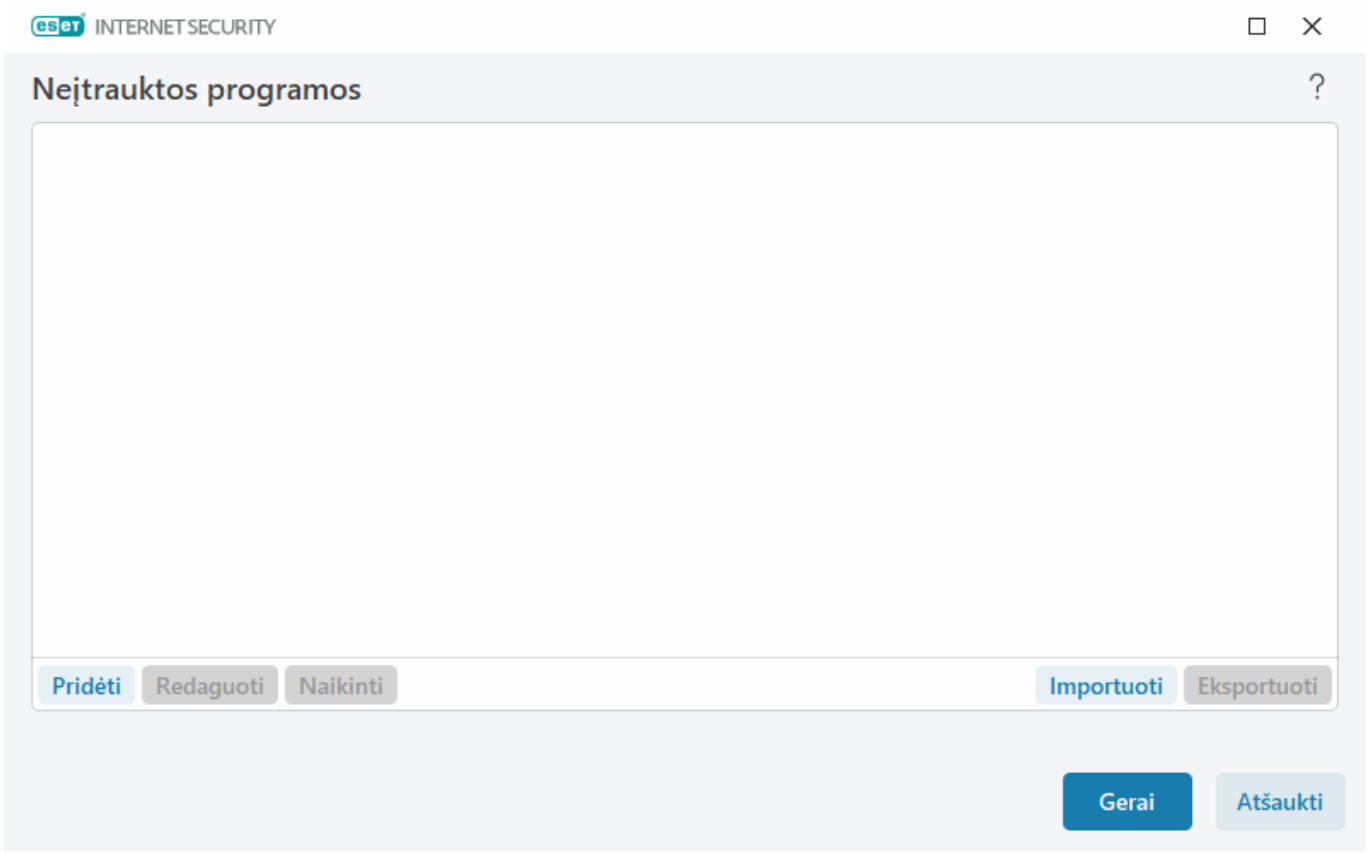
Neįtrauktos programos

Norėdami neįtraukti ryšių nuskaitymo konkrečioms programoms, įtraukite jas į sąrašą. Pasirinktų programų HTTP(S) / POP3(S) / IMAP(S) ryšys nebus tikrinamas ieškant grėsmių. Šią parinktį rekomenduojame naudoti tik programoms, kurios tinkamai neveikia, kai tikrinamas jų ryšys.

Veikiančios programos ir paslaugos čia bus automatiškai pasiekiamos, kai spustelėsite **Pridėti**. Spustelėkite **...** ir eikite į programą, kad rankiniu būdu pridėtumėte išimtį.

Redaguoti – suredaguokite pasirinktus sąrašo įrašus.

Šalinti – šalina pasirinktus įrašus iš sąrašo.



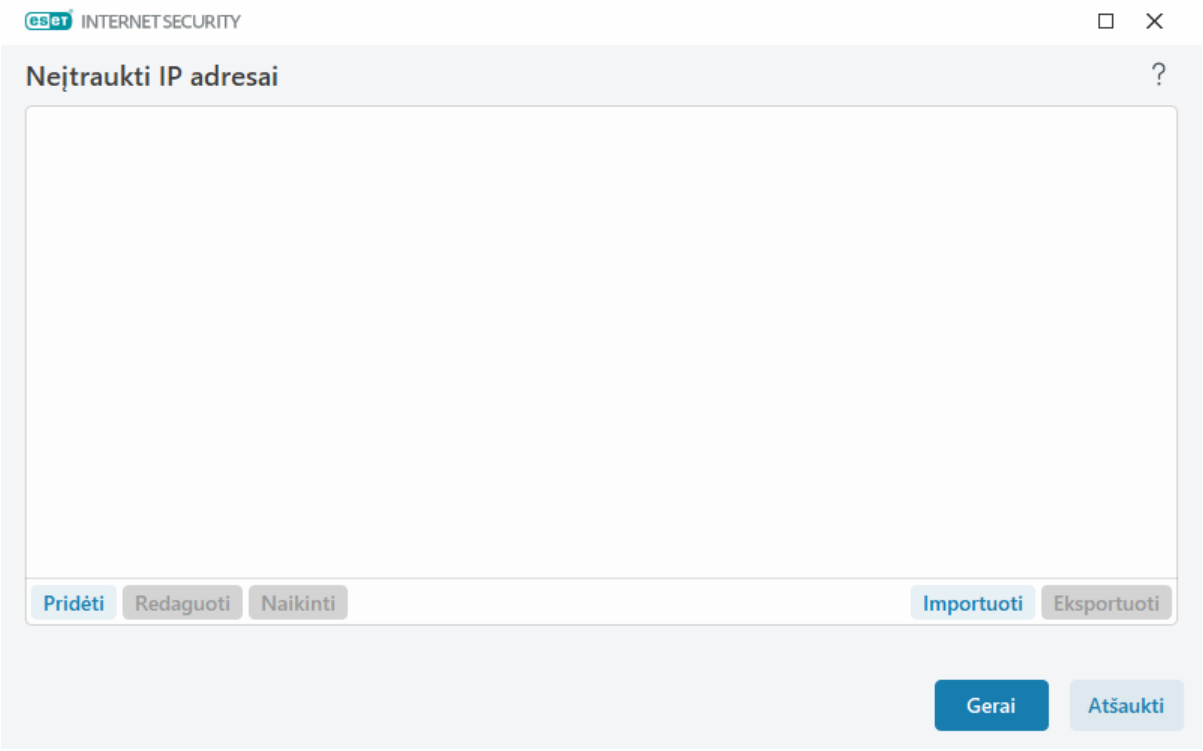
Nejtraukti IP

Įrašai sąraše bus neįtraukti į nuskaitymą. HTTP(S) / POP3(S) / IMAP(S) ryšys į pasirinktus adresus ir iš jų nebus tikrinamas ieškant grėsmių. Rekomenduojame naudoti šias parinktis tik adresams, kurie žinomi kaip patikimi.

Spustelėkite **Pridėti**, jei nenorite įtraukti nuotolinio taško IP adreso / adresų diapazono / potinklio.

Spustelėkite **Redaguoti**, jei norite pakeisti pasirinktą IP adresą.

Spustelėkite **Šalinti** ir pašalinkite pasirinktus įrašus iš sąrašo.



IP adresų pavyzdžiai

Pridėti IPv4 adresą:

Vienas adresas – prideda atskiro kompiuterio IP adresą (pvz., *192.168.0.10*).

Adresų diapazonas – įveda pradinį ir galutinį IP adresus, kad būtų nurodytas keleto kompiuterių IP diapazonas (pavyzdžiui, *192.168.0.1 – 192.168.0.99*).

Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė). Pavyzdžiui, 255.255.255.0 yra 192.168.1.0 potinklio tinklo kaukė. Norėdami išskirti visą potinklį, įveskite *192.168.1.0/24*.

Pridėti IPv6 adresą:

Vienas adresas – prideda atskiro kompiuterio IP adresą, kuriam bus taikoma taisyklė (pavyzdžiui, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Potinklis – IP adreso ir kaukės apibrėžtas potinklis (kompiuterių grupė) (pavyzdžiui, *2002:c0a8:6301:1::1/64*).

URL adresų sąrašo tvarkymas

URL adresų sąrašo valdymas, kurį rasite Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga**, leidžia nurodyti HTTP adresus, kuriuos norite blokuoti, leisti arba neįtraukti į turinio nuskaitymą.

SSL / TLS turi būti įjungtas, jei norite filtruoti HTTPS adresus kartu su HTTP. Kitaip bus pridėti tik jūsų aplankytų HTTPS svetainių domenai, o visas URL – ne.

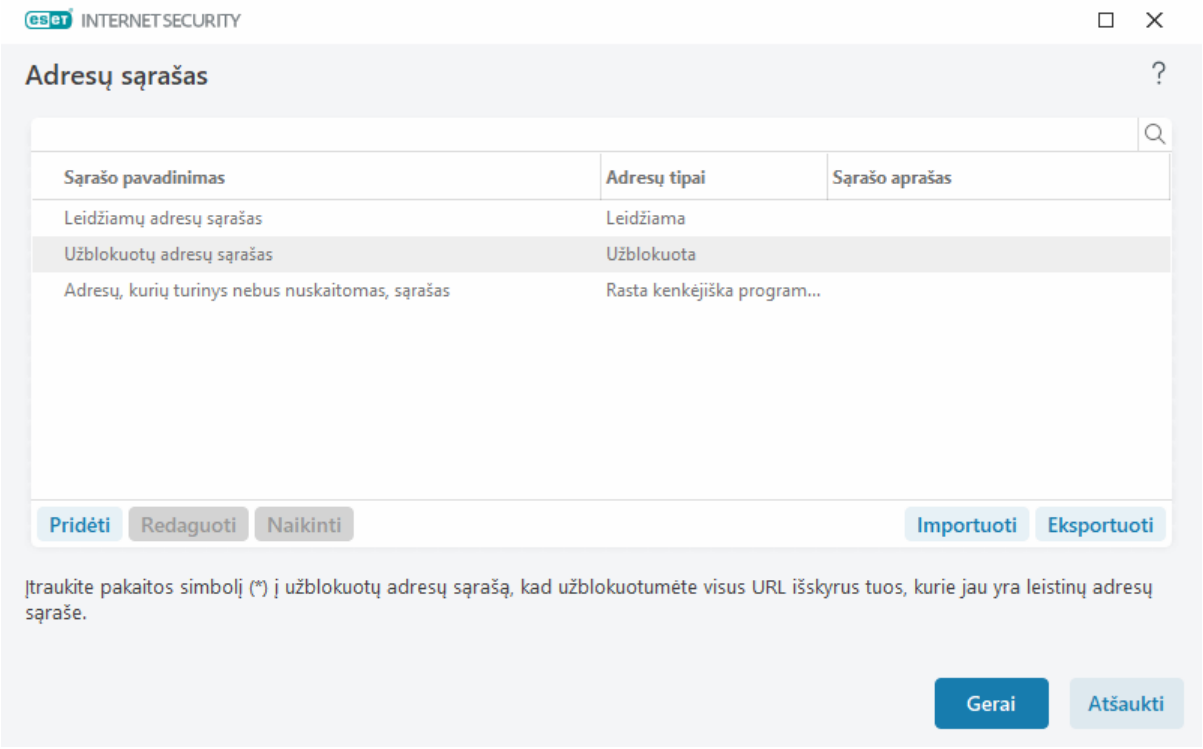
Blokuojamų adresų sąrašas nebus pasiekiamas svetainėse, jei jos bus įtrauktos ir į **Leidžiamų adresų sąrašą**. **Adresų, kurie nebus įtraukiami į turinio tikrinimą, sąrašas** nėra nuskaitomas ieškant kenkėjiško kodo.

Jei norite užblokuoti visus HTTP adresus, išskyrus esančius aktyviame **Leidžiamųjų adresų sąraše**, pridėkite * prie aktyvaus **Blokuojamųjų adresų sąrašo**.

Sąrašuose galima naudoti specialiuosius simbolius „*“ (žvaigždutes) ir „?“ (klaustukus). Žvaigždutė pakeičia bet kokią simbolių eilutę, o klaustukas – bet kokį simbolį. Būkite atidūs nurodydami neįtrauktus adresus, nes šiame sąraše turi būti tik patikimi ir saugūs adresai. Be to, būtina užtikrinti, kad šiame sąraše būtų tinkamai naudojami

simboliai „*“ ir „?“. Žr. Pridėti HTTP adresą / domeno kaukę, kur aprašoma, kaip gali būti saugiai sutapdintas visas domenas su visais padomeniais. Jei norite suaktyvinti sąrašą, pasirinkite **Sąrašas aktyvus**. Jei norite gauti pranešimą, kai patenkate į adresą iš esamo sąrašo, pasirinkite **Pranešti, kai naudojama**.

> **Adresai, kuriais pasitiki ESET**
>
> Jei funkcija **Nenuskaityti srauto su domenais, kuriais pasitiki ESET** įjungta, reiškia, kad yra SSL/TLS, ir ESET valdomiems baltajame sąraše esantiems domenams URL adresų sąrašo valdymo konfigūracija įtakos neturės.



Valdymo elementai

Pridėti – šalia iš anksto apibrėžtų sukuria naują sąrašą. Tai gali būti naudinga, jei norite logiškai išskaidyti atskiras adresų grupes. Pavyzdžiui, viename blokuojamųjų adresų sąraše gali būti adresai iš tam tikro išorinio viešo juodojo sąrašo, o kitame – jūsų sudarytas juodasis sąrašas: taip bus lengviau atnaujinti išorinį sąrašą išlaikant savąjį nepakeistą.

Redaguoti – modifikuoja esamus sąrašus. Šią parinktį galite naudoti norėdami įtraukti adresų arba jų pašalinti.

Naikinti – panaikinami esami sąrašai. Galima naudoti tik sąrašuose, sukurtuose naudojant parinktį **Pridėti**, bet ne su numatytaisiais sąrašais.

Adresų sąrašas

Šiame skyriuje galite sudaryti sąrašus iš HTTP(S) adresų, kurie bus blokuojami, leidžiami arba netikrinami.

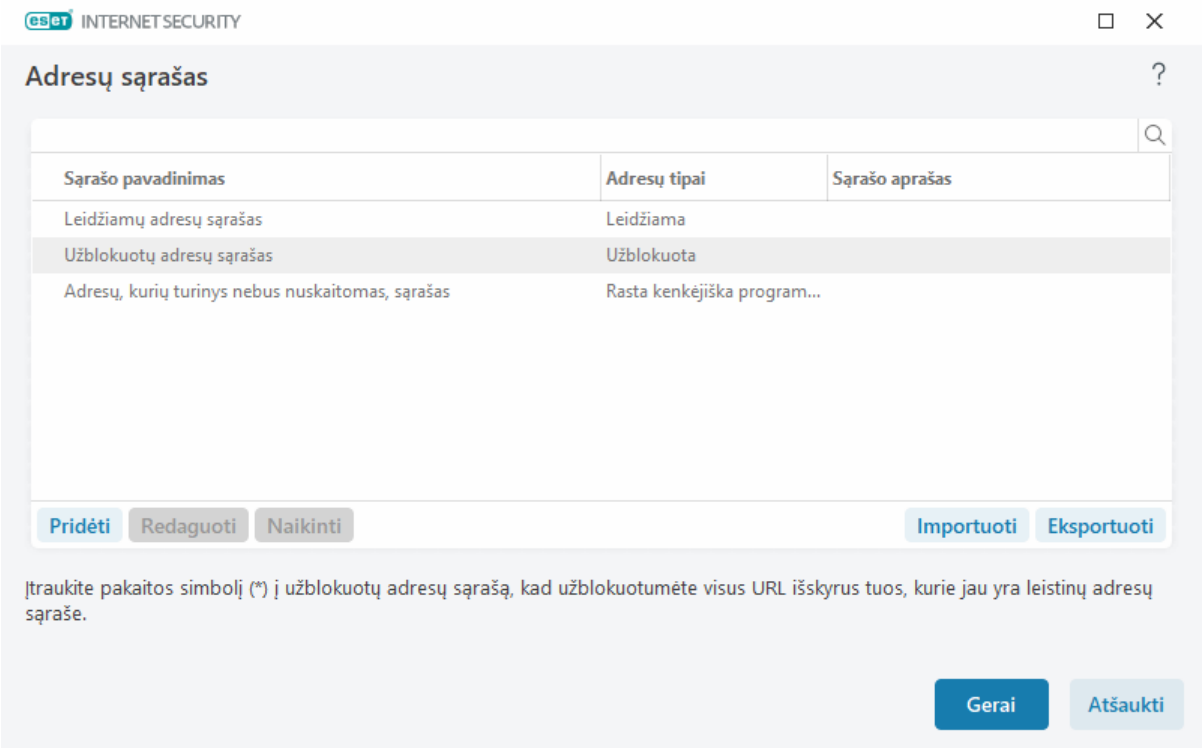
Pagal numatytuosius nustatymus galimi trys sąrašai:

- **Adresų, kurių turinys nebus tikrinamas, sąrašas** – jokie į šį sąrašą įtraukti adresai nebus tikrinami ieškant kenkėjiško kodo.

• **Leidžiamų adresų sąrašas** – jei įjungta parinktis Leisti prieigą tik prie leidžiamų adresų sąraše nurodytų HTTP adresų, o blokuojamų adresų sąraše yra „*“ (tinka viskas), vartotojui bus suteikta prieiga tik prie šiame sąraše nurodytų adresų. Šiame sąraše adresai yra leidžiami, net jei jie įtraukti į blokuojamų adresų sąrašą.

• **Užblokuotų adresų sąrašas** – vartotojui nebus leidžiama prieiga prie adresų, nurodytų šiame sąraše, nebent šie adresai yra įtraukti ir į leidžiamų adresų sąrašą.

Spustelėkite **Pridėti**, norėdami sukurti naują sąrašą. Norėdami panaikinti pasirinktus sąrašus, spustelėkite **Šalinti**.



> **Iliustruotos instrukcijos**
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> • Neleisti blokuoti saugios interneto svetainės, kai taikoma prieigos prie saityno apsauga
> • Blokuoti svetainę naudojant ESET „Windows“ namų produktus

Daugiau informacijos ieškokite URL adresų sąrašo tvarkymas.

Naujo adresų sąrašo kūrimas

Šis dialogo langas leidžia konfigūruoti naują URL adresų / kaukių, kurie bus blokuojami, leidžiami arba neįtraukti į tikrinimą, sąrašą.

Galite konfigūruoti šias parinktis:

Adresų sąrašo tipas – galimi trys sąrašo tipai:

• **Rasta kenkėjiška programinė įranga ignoruojama** – ieškant kenkėjiško kodo jokie į šį sąrašą įtraukti adresai nebus tikrinami.

• **Blokuojama** - prieiga prie šiame sąraše nurodytų adresų bus blokuojama.

• **Leidžiama** – bus leidžiama pasiekti šiame sąraše nurodytus adresus. Šiame sąraše nurodyti adresai yra

leidžiami, net jei sutampa su blokuojamų adresų sąraše esančiais adresais.

Sąrašo pavadinimas – nurodykite sąrašo pavadinimą. Šis laukas bus nepasiekiamas redaguojant vieną iš sąrašų, nustatytų iš anksto.

Sąrašo aprašas – įveskite trumpą sąrašo aprašymą (nebūtina). Nepasiekiama redaguojant vieną iš sąrašų, nustatytų iš anksto.

Norint suaktyvinti sąrašą, reikia pasirinkti punktą **Sąrašas aktyvus**, esantį šalia to sąrašo. Jei norite, kad jums būtų pranešta, kai prisijungiant prie svetainių naudojamas konkretus sąrašas, pasirinkite **Pranešti, kai teikiama paraiška**. Pavyzdžiui, jei interneto svetainė yra blokuojama arba leidžiama, nes yra įtraukta į blokuojamų arba leidžiamų adresų sąrašą, gausite pranešimą. Pranešime bus pateiktas pavadinimas sąrašo.

Registravimo rimtumas – informacija apie konkretų sąrašą, naudojamą prisijungiant prie svetainių, gali būti įrašyta į žurnalo failus.

Valdymo elementai

Pridėti – pridėkite prie sąrašo naują URL adresą (kelias vertes atskirkite skyrikliais).

Redaguoti – modifikuoja sąraše esamą adresą. Pasiekiama tik adresams, sukurtiems naudojant funkciją **Pridėti**.

Šalinti – panaikina iš sąrašo jame esančius adresus. Pasiekiama tik adresams, sukurtiems naudojant funkciją **Pridėti**.

Importuoti – importuokite failą su URL adresais (atskirkite reikšmes eilučių skirtukais, pvz., „*.txt“ faile, naudojančiame koduotę UTF-8).

Kaip pridėti URL kaukę

Peržiūrėkite instrukcijas šiame dialoge prieš įvesdami norimą adresą / domeno kaukę.

ESET Internet Security leidžia vartotojui blokuoti prieigą prie nurodytos svetainės ir neleisti interneto naršyklei rodyti jų turinio. Be to, ji leidžia vartotojui nurodyti adresus, kurie turi būti netikrinami. Jeigu nuotolinio serverio visas pavadinimas yra nežinomas arba vartotojas nori nurodyti visą nuotolinių serverių grupę, tokiai grupei identifikuoti gali būti naudojami vadinamieji šablonai. Kaukėje naudojami simboliai „?“ ir „*“:

- naudokite „?“ norėdami pakeisti simbolį
- naudokite „*“ norėdami pakeisti teksto eilutę.

Pavyzdžiui, *.c?m taikoma visiems adresams, kuriuose paskutinė dalis prasideda raide c, baigiasi raide m, o tarp jų yra nežinomas simbolis (.com, .cam ir t. t.)

Priekyje esanti seka „*.“ apdorojama ypatingai, jei yra naudojama domeno vardo pradžioje. Pirmiausia šiuo atveju pakaitos simbolis „*“ neatitinka pasvirojo brūkšnio („/“). Tuo siekiama išvengti kaukės apėjimo, pvz., kaukė **.domenas.com* neatitiks *http://betkoksdomenas.com/betkokskelias#.domenas.com* (tokia priesaga gali būti pridedama prie bet kokio URL nepaveikiant atsisiuntimo). Be to, antrasis „*.“ šiuo ypatinguoju atveju taip pat atitinka tuščią eilutę. Tuo siekiama leisti naudojant vieną kaukę sutapdinti visą domeną, įskaitant padomenius. Pavyzdžiui, kaukė **.domenas.com* taip pat atitinka *http://domenas.com*. Naudoti kaukę **domenas.com* būtų neteisinga, nes ji taip pat atitiktų ir *http://kitasdomenas.com*.

HTTP(S) srauto nuskaitymas

Pagal numatytuosius nustatymus ESET Internet Security yra sukonfigūruotas nuskaityti HTTP ir HTTPS srautą, kurį naudoja interneto naršyklės ir kitos programos. Srauto nuskaitymą turėtumėte išjungti tik tuo atveju, jei kyla problemų dėl 3-iosios šalies programinės įrangos ir norite sužinoti, ar problemą sukėlė ESET Internet Security.

Įgalinti HTTP srauto nuskaitymą – HTTP srautas, siunčiamas per visus prievadus, yra visada stebimas.

Įgalinti HTTPS srauto nuskaitymą – HTTPS srautas naudoja šifruotą kanalą informacijai tarp serverio ir kliento siųsti. ESET Internet Security tikrina ryšius naudodama SSL (saugaus sujungimo sluoksnio) ir TLS (transportavimo lygmens saugos) protokolus. Programa nuskaito srautą tik per prievadus, kurie nustatyti parinktyje **HTTPS protokolo naudojami prievadai**, nepriklausomai nuo to, kokią operacinės sistemos versiją naudojate (galite pridėti prievadus į iš anksto nustatytą 443 arba 0-65535).

ThreatSense

„ThreatSense“ sudaro įvairūs sudėtiniai grėsmių aptikimo metodai. Ši technologija yra iniciatyvi, o tai reiškia, kad ji užtikrina apsaugą, vos tik pradeda plisti nauja grėsmė. Joje kartu naudojama kodų analizė, kodų imitavimas, bendrieji kodai ir virusų kodai, kurie darniai veikia ir gerokai padidina sistemos saugumą. Nuskaitymo modulis gali vienu metu kontroliuoti keletą duomenų srautų – tai padidina efektyvumą ir aptikimo greitį. Be to, „ThreatSense“ technologija sėkmingai panaikina kenkėjiškas prieigos programas.

„ThreatSense“ modulio nustatymų parinktys leidžia nurodyti keletą nuskaitymo parametrų:

- failų, kurie turi būti nuskaityti, tipai ir plėtiniai;
- įvairių aptikimo metodų derinys;
- valymo lygiai ir t. t.

Norėdami patekti į nustatymo langą, išplėstinio nustatymo lange spustelėkite **„ThreatSense**“ parametrai, kad būtų parodyti moduliai, kuriems naudojama ThreatSense technologija (žr. toliau). Skirtingiems saugumo scenarijams gali reikėti skirtingų konfigūracijų. Atsižvelgiant į tai, „ThreatSense“ yra atskirai konfigūruojama šiems apsaugos moduliams:

- Failų sistemos apsauga realiuoju laiku
- Laukimo būsenos nuskaitymas
- Nuskaitymas paleidžiant
- Dokumentų apsauga
- El. pašto programų apsauga
- Prieigos prie saityno apsauga
- Kompiuterio nuskaitymas

„ThreatSense“ parametrai yra optimizuoti kiekvienam moduliui ir jų keitimas gali labai paveikti sistemos veikimą. Pavyzdžiui, pakeitus parametrus, kad visada būtų nuskaitomos momentinio pakavimo programos, arba įjungus

išplėstinę euristiką failų sistemos apsaugos realiuoju laiku modulyje, sistemos darbas gali sulėtėti (paprastai naudojant šiuos metodus nuskaitomi tik naujai sukurti failai). Rekomenduojame palikti numatytuosius „ThreatSense“ parametrus nepakeistus visuose moduliuose, išskyrus kompiuterio nuskaitymą.

Nuskaitytini objektai

Šiame skyriuje galite nurodyti, kurie kompiuterio komponentai ir failai bus nuskaityti ieškant įsiskverbimų.

Operacinė atmintis – nuskaitomos grėsmės, kurios atakuoja sistemos operacinę atmintį.

Paleidimo sektorius / UEFI – nuskaitomi sistemos įkrovimo sektoriai tikrinant, ar nėra kenkėjiškos programinės įrangos pagrindiniame sistemos įkrovimo įraše. Daugiau apie UEFI skaitykite terminų žodyne.

El. laiškų failai – programa palaiko šiuos plėtinius: DBX („Outlook Express“) ir EML.

Archyvai – programa palaiko šiuos plėtinius: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ir daugelį kitų.

Išsiskleidžiantieji archyvai – išsiskleidžiantieji archyvai (SFX) yra archyvai, kurie gali išsiskleisti patys.

Momentiniai pakuotuvai – įvykdytos momentinio išpakavimo programos (skirtingai nei standartinių tipų archyvai) vėl suglaudinamos atmintyje. Be standartinių statinių pakavimo programų (UPX, yoda, ASPack, FSG ir t. t.), naudodamas kodų imitavimo principą skaitytuvas gali atpažinti kelis papildomus pakuotuvų tipus.

Nuskaitymo parinktys

Pasirinkite metodus, kurie bus naudojami nuskaitant sistemą ir ieškant įsiskverbimų. Galimos šios parinktys:

Euristika – euristika yra algoritmas, analizuojantis programų (kenkimo programinės įrangos) veiklą. Pagrindinis šios technologijos privalumas yra gebėjimas identifikuoti kenkimo programinę įrangą, kurios nebuvo ankstesnėje aptikimo modulio versijoje arba ji nebuvo žinoma. Trūkumas yra klaidingų pavojaus pranešimų (labai maža) tikimybė.

Išplėstinė euristika / DNA kodai – išplėstinė euristika yra unikalus ESET sukurtas algoritmas, optimizuotas aptikti kompiuterio kirminus bei Trojos arklius ir yra parašytas aukšto lygio programavimo kalbomis. Naudojant išplėstinę euristiką, gerokai padidėja ESET produktų grėsmių aptikimo galimybės. Kodai gali patikimai aptikti ir identifikuoti virusus. Naudojant automatinę naujinimo sistemą, nauji kodai tampa pasiekiami per kelias valandas nuo grėsmės atskleidimo. Kodų trūkumas yra tai, kad jie aptinka tik jiems žinomus virusus (arba šiek tiek modifikuotas jų versijas).

Valymas

Valymo parametrai apibrėžia ESET Internet Security veiksmus valant objektus. Yra 4 valymo lygiai:

ThreatSense siūlo šiuos atkūrimo (t. y. valymo) lygius.

Atkūrimas programoje ESET Internet Security

Valymo lygis	Aprašymas
Visada valyti objektą	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais retais atvejais (pvz., esant sisteminiams failams), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju palikti	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais atvejais (pvz., esant sisteminiams failams arba archyvams, kuriuose yra ir švarūs, ir užkrėsti failai), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju paklausti	Valant objektus, bandoma atkurti aptikimą. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, galutiniam naudotojui rodomas interaktyvus įspėjimas ir jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Daugeliu atveju ši nuostata yra rekomenduojama.
Visada klausti galutinio naudotojo	Valant objektus, galutiniam naudotojui rodomas interaktyvus langas, kuriame jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Šis lygis skirtas labiau patyrusiems naudotojams, kurie žino, kokį veiksmą atlikti aptikimo atveju.

Išimtys

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis „ThreatSense“ parametrų nustatymo skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

Kita

Konfigūruojant „ThreatSense“ modulio kompiuterio užsakomojo nuskaitymo parametrų nustatymus, papildomai pasiekiamos ir šios parinktys, pateikiamos skyriuje **Kita**:

Nuskaityti kintamuosius duomenų srautus (ADS) – NTFS failų sistemos naudojami kintamieji duomenų srautai yra failų ir aplankų ryšiai, kurie nematomi įprastoms nuskaitymo priemonėms. Daugelis įsiskverbimų bando išvengti aptikimo apsimesdami kintamaisiais duomenų srautais.

Vykdyti mažo prioriteto foninius nuskaitymus – kiekviena nuskaitymo seka naudoja tam tikrą kiekį sistemos išteklių. Jeigu dirbate su programomis, kurios intensyviai naudoja sistemos išteklius, galite suaktyvinti mažo prioriteto foninį nuskaitymą ir taupyti išteklius savo programoms.

Registruoti visus objektus – nuskaitymo žurnale bus rodomi visi nuskaityti failai išsiskleidžiančiuosiuose archyvuose, net neužkrėsti (gali būti generuojama daug nuskaitymo žurnalo duomenų ir padidės nuskaitymo žurnalo failo dydis).

Įjungti išmanųjį optimizavimą – įjungus išmanųjį optimizavimą, naudojami optimaliausi parametrai, leidžiantys užtikrinti efektyviausią nuskaitymo lygį ir kartu palaikyti didžiausią nuskaitymo greitį. Įvairūs apsaugos moduliai išmaniai atlieka nuskaitymą, naudodami įvairius nuskaitymo metodus ir taikydami juos konkretiems failų tipams. Jei išmanusis optimizavimas išjungtas, atliekant nuskaitymą taikomi tik vartotojo apibrėžti parametrai tam tikrų modulių ThreatSense šerdyje.

Saugoti paskutinį prieigos laiką – nurodykite šią parinktį, norėdami išlaikyti nuskaitytų failų originalius prieigos laikus, o ne naujinti juos (pavyzdžiui, naudojant su duomenų atsarginio kopijavimo sistemomis).

Ribos

Ribų skyriuje galima nurodyti maksimalius nuskaitomų objektų dydžius ir archyvų įdėties lygius:

Objekto parametrai

Maksimalus objekto dydis – apibrėžia maksimalų nuskaitomų objektų dydį. Antivirusinės programos modulis nuskaitys tik mažesnius nei nurodytas dydis objektus. Šią parinktį turėtų keisti tik patyrę vartotojai, kurie gali turėti tam tikrų priežasčių neįtraukti didelių objektų į nuskaitymą. Numatytoji reikšmė: neribota.

Maksimali objekto nuskaitymo trukmė (sek.) – apibrėžia maksimalią objekto failų (pvz., esančių RAR / ZIP archyve arba el. laiške su keliais priedais) nuskaitymo trukmę. Šis nustatymas netaikomas pavieniams failams. Jei įvesta naudotojo apibrėžta vertė ir tas laikas praėjo, nuskaitymas bus sustabdytas kuo greičiau, neatsižvelgiant į tai, ar kiekvieno failo nuskaitymas objekte yra užbaigtas.
Archyvo su dideliais failais atveju nuskaitymas bus sustabdytas išskleidus failą iš archyvo (pvz., kai naudotojo apibrėžtas kintamasis yra 3 sekundės, bet failo išskleidimas užtrunka 5 sekundes). Praėjus nurodytam laikui, likę archyvo failai nebus nuskaitomi.
Norėdami apriboti nuskaitymo trukmę, taip pat ir didesnių archyvų atveju, naudokite parinktis **Maksimalus objekto dydis** ir **Maksimalus failo archyve dydis** (nerekomenduojama dėl galimos rizikos saugai).
Numatytoji reikšmė: neribota.

Archyvo nuskaitymo nustatymai

Archyvo įdėties lygis – nurodo maksimalų archyvų nuskaitymo gylį. Numatytoji vertė: 10.

Maksimalus failo archyve dydis – ši parinktis leidžia nurodyti, kokio maksimalaus dydžio (kai jie išskleidžiami) archyve esantys failai bus nuskaitomi. Maksimali reikšmė: **3 GB**.

> Mes nerekomenduojame keisti numatytųjų verčių: dirbant įprastai, jų keisti nėra priežasties.

Tėvų kontrolė

Parinktis **Įgalinti tėvų kontrolę** integruoja tėvų kontrolę į ESET Internet Security. Spustelėkite **Redaguoti** šalia Naudotojo paskyros, jei norite susieti „Windows“ naudotojų paskyras, kurios naudojamos tėvų kontrolei, su konkrečiais vartotojais ir apriboti jų prieigą prie netinkamo ar žalingo turinio internete.

Vartotojo paskyros

Pasirinkę Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga** > **Tėvų kontrolė** > **Naudotojo paskyros** > **Redaguoti**, galite susieti „Windows“ naudotojų paskyras, kurias naudoja tėvų kontrolė, su konkrečiais naudotojais, kad apribotumėte jų prieigą prie netinkamo ar žalingo turinio internete.

Stulpeliai

„Windows“ paskyra – vartotojo naudojamas vardas.

Įjungta – jei įjungta, suaktyvinama konkrečios vartotojo paskyros tėvų kontrolė.

Domenas – domeno, kuriam priklauso vartotojas, pavadinimas.

Gimimo data – šios paskyros vartotojo amžius.

Valdymo elementai

Pridėti – bus parodytas dialogo langas Darbas su vartotojo paskyromis.

Redaguoti – galima redaguoti pasirinktas paskyras.

Šalinti – naikinti pasirinktą paskyrą.

Atnaujinti – jei pridėjote vartotojo paskyrą, ESET Internet Security gali atnaujinti vartotojo paskyrų sąrašą neatidarant šio lango iš naujo.

Naudotojo paskyros nustatymai

Lange yra trys skirtukai:

Bendra

Įgalinkite perjungiklį šalia **Įjungta**, norėdami įjungti toliau pasirinktos Windows paskyros tėvų kontrolę.

Pirmiausia **pasirinkite** Windows paskyrą savo kompiuteryje. Ribojimai, nustatyti tėvų kontrolėje, veikia tik standartines „Windows“ paskyras. Administravimo paskyros apribojimų gali nepaisyti.

Jei paskyrą naudoja vienas iš tėvų, pasirinkite **Tėvų paskyra**.

Nustatykite paskyros **Vaiko gimimo datą**, kad būtų nustatytas atitinkamas prieigos lygis ir nustatytos prieigos prie pagal amžių tinkamus tinklalapius taisyklės.

Registravimo pavojingumas

ESET Internet Security įrašo visus svarbius įvykius į žurnalo failą, kurį galima peržiūrėti tiesiai iš pagrindinio meniu. Spustelėkite **Įrankiai** > **Žurnalo failai**, tada išskleidžiamajame meniu **Žurnalas** pasirinkite **Tėvų kontrolė**.

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą.
- **Informacija** – įrašo informacinius pranešimus, įskaitant leidžiamas ir užblokuotas išimtis, ir visus pirmiau nurodytus įrašus.
- **Įspėjimas** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Nėra** – žurnalai nekuriami.

Išimtys

Sukūrus išimtį galima leisti ar uždrausti vartotojo prieigą prie svetainių, kurios nėra įtrauktos į išimčių sąrašą. Tai naudinga, jei norite kontroliuoti prieigą prie konkrečių svetainių, kad nereikėtų naudoti kategorijų. Vienai paskyrai sukurtas išimtis galima nukopijuoti ir panaudoti kitai paskyrai. Tai gali padėti, jei norite sukurti identiškas taisykles panašaus amžiaus vaikams.

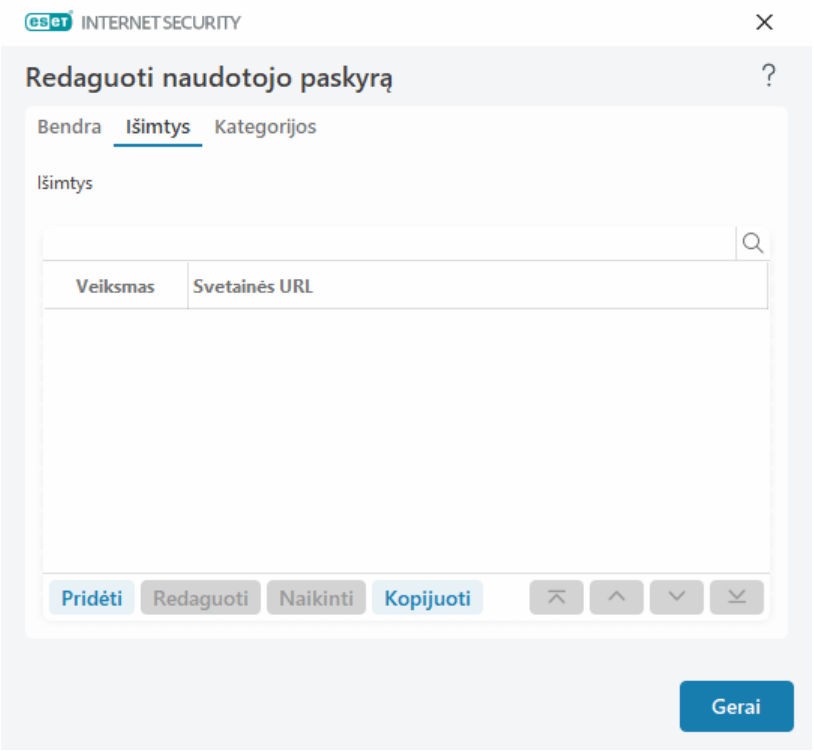
Spustelėkite **Pridėti** ir sukurkite naują išimtį. Naudodamiesi išskleidžiamuoju meniu nurodykite **Veiksmą** (pvz., **Blokuoti**), įveskite **Svetainės URL**, kuriam taikoma ši išimtis ir spustelėkite **Gerai**. Išimtis bus pridėta prie esamų išimčių sąrašo, o prie jos bus nurodyta būsena.

Pridėti – sukuriama nauja išimtis.

Redaguoti – pasirinktos išimties **Svetainės URL** arba **Veiksmą** galite redaguoti.

Šalinti – pašalina pasirinktą išimtį.

Kopijuoti – išskleidžiamajame meniu pasirinkite vartotoją, iš kurio norite kopijuoti sukurtą išimtį.

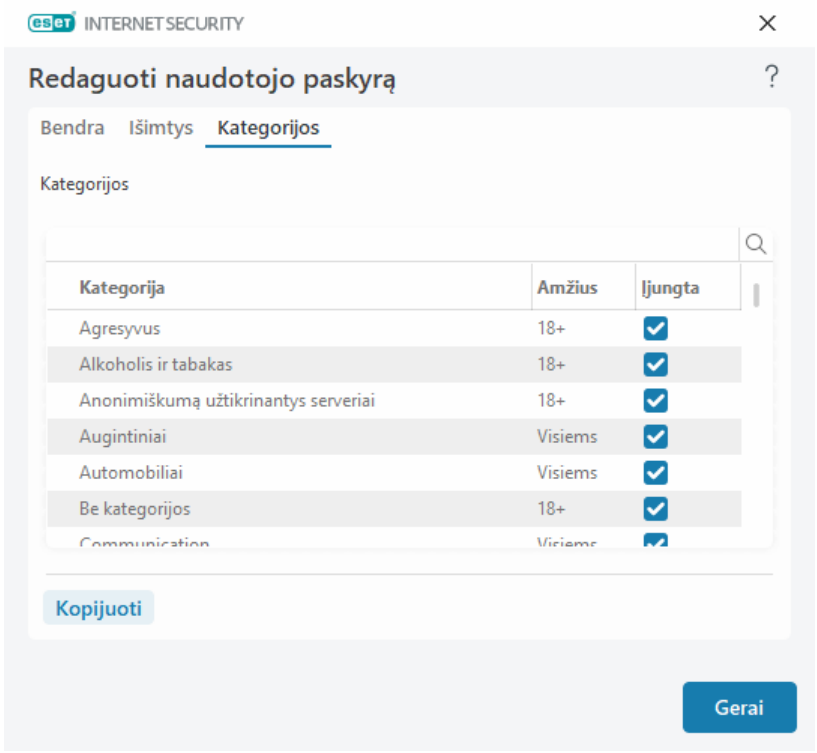


Apibrėžtos išimtys leidžia nepaisyti pasirinktoje paskyroje (-ose) apibrėžtų kategorijų. Pavyzdžiui, jei paskyroje blokuojama kategorija **Naujienos**, tačiau naujienų tinklalapį apibrėžėte kaip leidžiamą išimtį, paskyrai suteikiama prieiga prie leidžiamo tinklalapio. Visus atliktus pakeitimus galite peržiūrėti skyriuje Išimtys.

Kategorijos

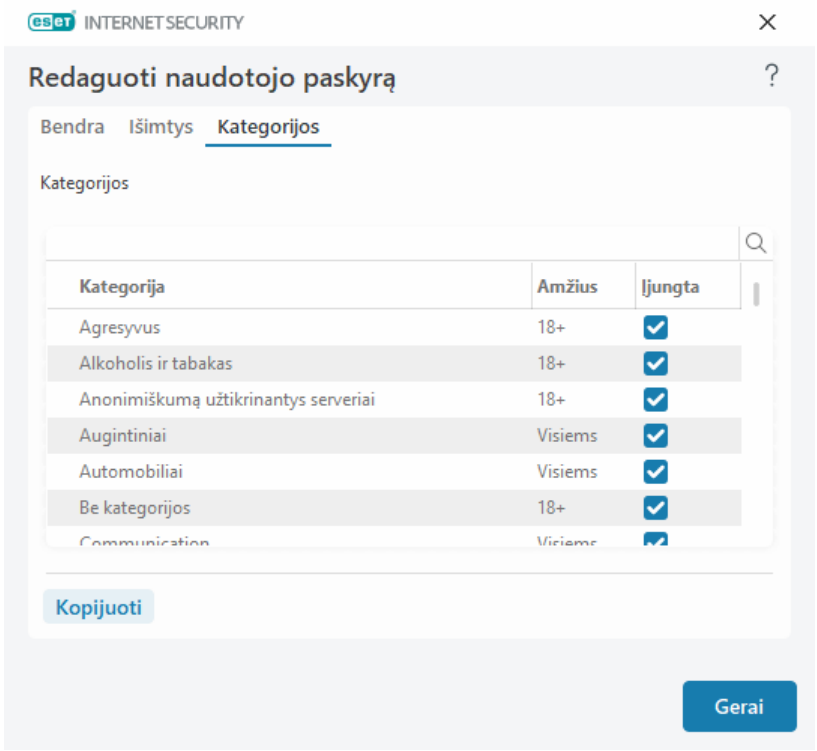
Skirtuke **Kategorijos** galite apibrėžti bendras svetainių, kurias norite blokuoti arba leisti kiekvienai paskyrai, kategorijas. Jei norite leisti kategoriją, pažymėkite prie jos esantį langelį. Jei paliksite langelį tuščią, kategorija šioje paskyroje nebus leidžiama.

Kopijuoti – leidžia kopijuoti užblokuotų arba leidžiamų kategorijų sąrašą iš esamos pakeistos paskyros.



Kategorijos

Norėdami leisti kategoriją, pažymėkite žymės langelį **Įjungta** stulpelyje šalia kategorijos. Jei nepažymėsite žymės langelio, šiai paskyrai kategorija nebus leidžiama.



Čia pateikiami keli kategorijų (grupių) pavyzdžiai, kurie vartotojams gali būti nepažįstami:

- **Įvairūs** – paprastai asmeniniai (vietiniai) IP adresai, tokie kaip intranetas, 127.0.0.0/8, 192.168.0.0/16 ir t. t. Kai gausite klaidos kodą Nr. 403 arba 404, interneto svetainė taip pat atitiks šią kategoriją.

- **Neišspręsta** – į šią kategoriją įeina tinklalapiai, kurie yra neišspręsti dėl klaidos jungiantis prie tėvų kontrolės duomenų bazės modulio.
- **Be kategorijos** – nežinomi tinklalapiai, kurių dar nėra tėvų kontrolės duomenų bazėje.
- **Dinamiški** – tinklalapiai, nukreipiantys į kitus puslapius kitose svetainėse.

Naršyklės apsauga

Naršyklės apsauga – tai dar vienas jūsų saugumo ir privatumo apsaugos sluoksnis, apsaugantis naršyklės atmintį nuo tikrinimo pagal kitus procesus, padidinantis apsaugą nuo klavišų paspaudimų registravimo programų ir neleidžiantis įklijuoti su internetiniais mokėjimais susijusių duomenų, modifikuotų kenkėjiškos programos, iš mainų srities į apsaugotą naršyklę. Norėdami sukonfigūruoti naršyklės apsaugą, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Naršyklės apsauga** ir pasirinkite iš šių konfigūravimo parinkčių:

- Saugi bankininkystė ir naršymas
- Naršyklės apsaugos leidimų sąrašas
- Naršyklės rėmelis

Saugi bankininkystė ir naršymas

Parinktį Saugi bankininkystė ir naršymas galite konfigūruoti pasirinkę Išplėstinis nustatymas > **Apsaugos priemonės** > **Naršyklės apsauga** > **Saugi bankininkystė ir naršymas**.

Saugi bankininkystė ir naršymas

Įgalinti saugią bankininkystę ir naršymą – kai įgalinta saugi bankininkystė ir naršymas, pagal numatytuosius nustatymus visos palaikomos saityno naršyklės bus paleistos saugiuoju režimu.

Naršyklės apsauga

Įjunkite **Apsaugoti visas naršykles**, kad paleistumėte visas palaikomas naršykles saugiuoju režimu.

Plėtinių diegimo režimas – išskleidžiamajame meniu galite pasirinkti, kuriuos plėtinius bus leidžiama diegti ESET saugomoje naršyklėje:

- **Esminiai plėtiniai** – gali būti diegiami tik svarbiausi plėtiniai, kuriuos sukūrė konkretus naršyklės gamintojas.
- **Visi plėtiniai** – visus plėtinius, kuriuos palaiko konkreti naršyklė.

> Plėtinio diegimo režimo keitimas neturi įtakos anksčiau įdiegtiems naršyklės plėtiniams:

Apsaugota naršyklė

Išplėsta atminties apsauga – jei įjungta, saugios naršyklės atmintis bus apsaugota nuo kitų procesų vykdomo

tikrinimo.

Klaviatūros apsauga – jei įgalinta, apsaugotoje naršyklėje klaviatūra įvesta informacija bus paslėpta nuo kitų programų. Tai padidina apsaugą nuo registravimo programų.

Mainų srities apsauga – jei įgalinta, „ESET Internet Security“ neleis įklijuoti jokių su mokėjimais susijusių internetinių duomenų, kuriuos pakeitė kenkėjiška programinė įranga, iš mainų srities į apsaugotą naršyklę. Tai užtikrina apsaugą nuo galimų kenkėjiškos programinės įrangos atliekamų pakeitimų.

Naršyklės rėmelis – Suasmeninkite naršyklės rėmelio rodymo nustatymus apsaugotose naršyklėse.

Naršyklės apsaugos leidimų sąrašas – Tvarkykite failus, įtrauktus į naršyklės apsaugos leidimų sąrašą.

Naršyklės privatumas ir sauga

Įgalinti naršyklės privatumą ir saugą – jei išjungta, naršyklės privatumo ir saugos plėtinys bus pašalintas iš visų palaikomų naršyklių visose „Windows“ paskyrose.

Rodyti naršyklės privatumo saugos pranešimus – jei įgalinta, „ESET Internet Security“ bus rodomi naršyklės privatumo ir saugos pranešimai.

Naršyklės scenarijų skaitytuvas

Įgalinti išplėstinį naršyklės scenarijų nuskaitymą – jei įgalinta, apsaugos nuo virusų skaitytuvas patikrins visas „JavaScript“ programas, kurias vykdo interneto naršyklės.

00

Įrenginio kontrolė

ESET Internet Security leidžia atlikti automatinį įrenginio (CD / DVD / USB ir kt.) valdymą. Šis modulis leidžia blokuoti arba koreguoti išplėstinius filtrus / teises ir pasirinkti, kaip vartotojas gali naudotis ir dirbti su nurodytais įrenginiais. Tai gali būti naudinga, jei kompiuterio administratorius nori neleisti naudotis įrenginiais, kuriuose yra nepageidaujamo turinio.

Palaikomi išoriniai įrenginiai:

- Diskų atminties įrenginys (HDD, USB atjungiamasis diskas)
- CD / DVD
- Spausdintuvas USB
- FireWire kaupiklis
- Bluetooth Įrenginys
- Lustinių kortelių skaitytuvas
- Vaizdavimo įrenginys

- Modemas
- LPT/COM prievadas
- Nešiojamasis įrenginys (baterijomis maitinami įrenginiai, pvz., medijos leistuvai, išmanieji telefonai, „prijungti ir leisti“ įrenginiai ir kt.)
- Visi įrenginių tipai

Įrenginių kontrolės nustatymų parinktys gali būti keičiamos per Išplėstiniai nustatymai **Apsaugos priemonės** > **Įrenginio kontrolė**.

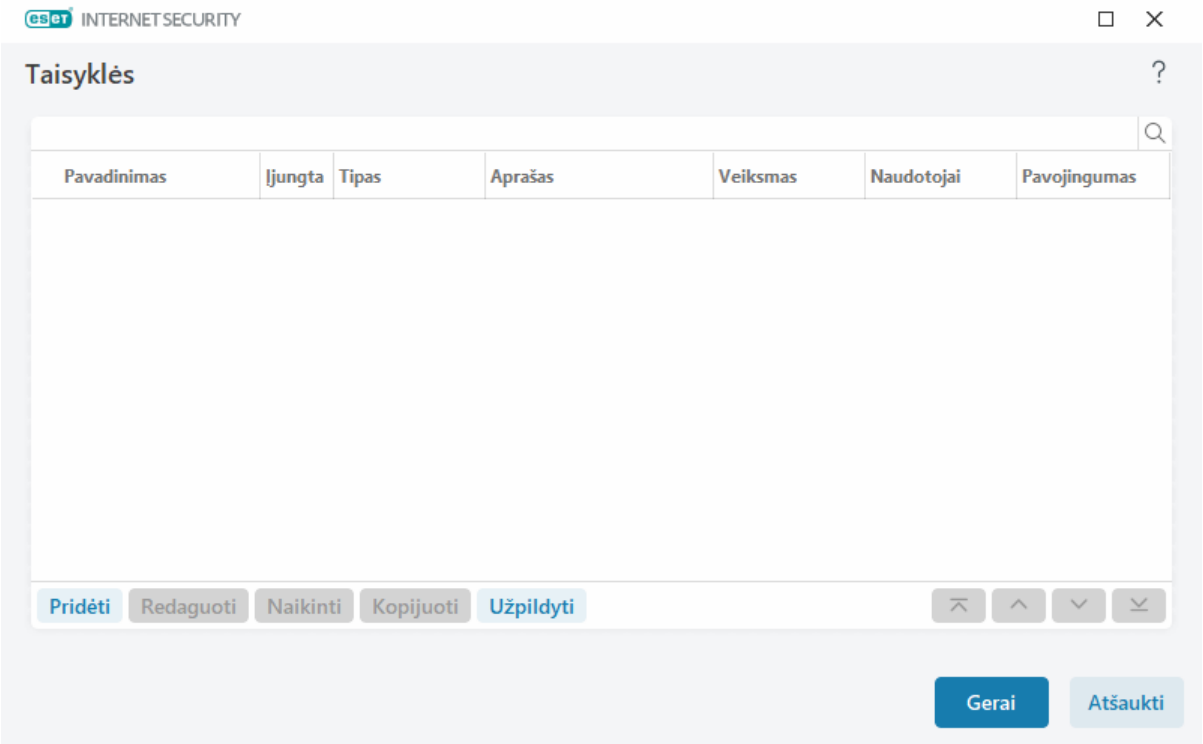
Spustelėkite perjungiklį **Įjungti įrenginio kontrolę**, kad įjungtumėte įrenginio valdymo funkciją ESET Internet Security; turite iš naujo paleisti kompiuterį, kad šis pakeitimas įsigaliotų. Įjungę įrenginio valdymą, taisyklių rengyklės lange galite apibrėžti **taisykles**.

> Galite sukurti įvairias įrenginių grupes, kurioms bus taikomos skirtingos taisyklės. Be to, galite sukurti tik vieną įrenginių grupę, kuriai bus taikoma taisyklė su veiksmu **Leisti** arba **Blokuoti rašymą**. Taip užtikrinama, kad bus blokuojami įrenginių valdymo neatpažinti įrenginiai, kai juos prijungiate prie kompiuterio.

Jei bus prijungtas įrenginys, kurį blokuoja esama taisyklė, pasirodys pranešimo langas ir prieiga prie įrenginio suteikta nebus.

Įrenginio kontrolės taisyklių rengyklė

Lange **Įrenginio kontrolės taisyklių rengyklė** rodomos esančios taisyklės ir jame galima tiksliai kontroliuoti išorinius įrenginius, kuriuos vartotojai prijungia prie kompiuterio.



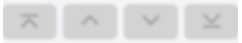
Tam tikri naudotojo arba naudotojų grupės įrenginiai gali būti leidžiami arba užblokuojami, atsižvelgiant į papildomus įrenginio parametrus, kuriuos galima nurodyti taisyklės konfigūracijoje. Taisyklių sąraše yra keletas taisyklės aprašymų, tokių kaip išorinio įrenginio pavadinimas, tipas, veiksmas, kurį reikia atlikti po to, kai išorinis

įrenginys prijungiamas prie jūsų kompiuterio, ir žurnalo svarba. Taip pat žr. Įrenginio valdymo taisyklių įtraukimas.

Spustelėkite **Pridėti** arba **Redaguoti** norėdami tvarkyti taisyklę. Jei norite sukurti naują taisyklę su iš anksto nustatytomis parinktimis, naudojamomis kitai pasirinktai taisyklei, spustelėkite **Kopijuoti**. XML eilutės, rodomos paspaudus taisyklę, gali būti nukopijuotos į iškarpinę ir padėti sistemos administratoriams eksportuoti / importuoti šiuos duomenis bei naudoti juos, pavyzdžiui, .

Paspaudus **CTRL** ir pelės mygtuką, galima pasirinkti keletą taisyklių ir taikyti veiksmus, tokius kaip naikinimas arba perkėlimas aukštyn ar žemyn sąraše, visoms pasirinktoms taisyklėms. Žymės langelis **Įjungta** išjungia ar įjungia šią taisyklę. Tai gali būti naudinga, jei norite palikti taisyklę.

Spustelėkite parinktį **Susieti**, kad automatiškai susietumėte nešiojamosios laikmenos įrenginio parametrus, skirtus prie kompiuterio prijungtiems įrenginiams.

Taisyklės sąraše išdėstomos pagal prioritetus: kuo aukštesnis prioritetas, tuo arčiau viršaus yra taisyklė. Taisykles galite perkelti spustelėdami  **Viršus / aukštyn / žemyn / apačia**; jas galite perkelti po vieną arba grupėmis.

Žurnalo įrašus galima peržiūrėti pagrindiniame programos lange > **Įrankiai** > Žurnalo failai.

Įrenginio kontrolės žurnale registruojami visi įvykiai, kai buvo suaktyvinta įrenginio kontrolė.

Aptikti įrenginiai

Mygtukas **Pateikti** parodo visų šiuo metu prijungtų įrenginių apžvalgą su informacija apie įrenginio tipą, įrenginio tiekėją, modelį ir serijos numerį (jei toks yra). Jei norite matyti visus paslėptus įrenginius, pasirinkite **Rodyti paslėptus įrenginius**.

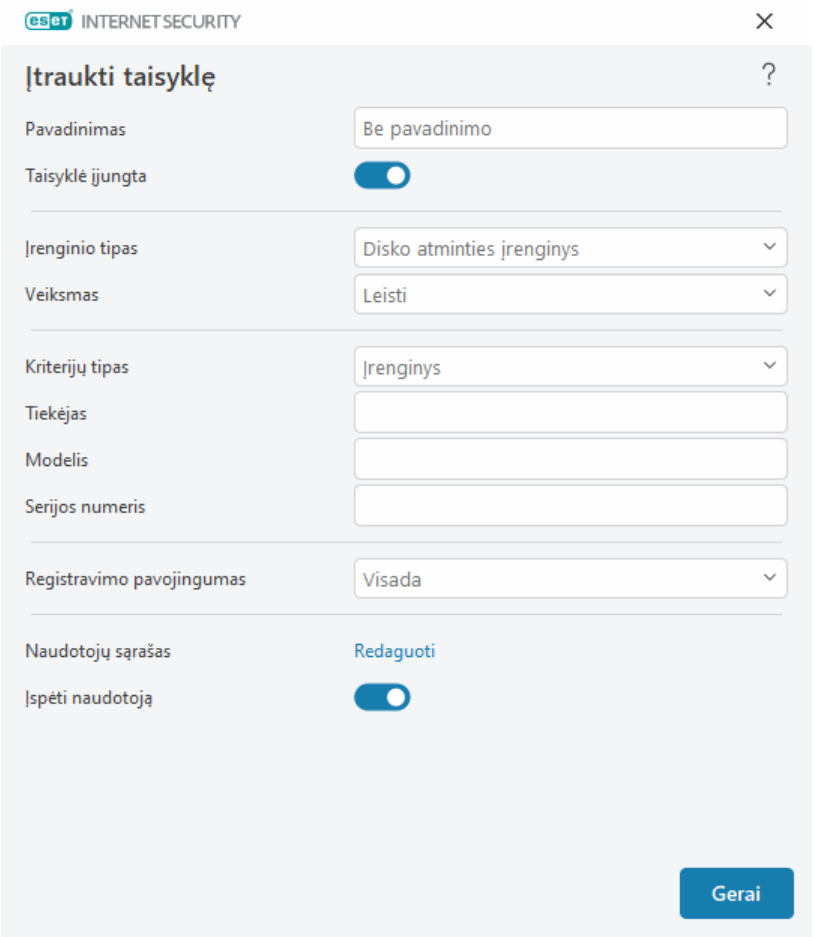
Pasirinkite įrenginį iš aptiktų įrenginių sąrašo ir spustelėkite **Gerai**, kad įtrauktumėte įrenginio kontrolės taisyklę su iš anksto nustatyta informacija (visus nustatymus galima koreguoti).

Mažos galios (miego) režimu veikiantys įrenginiai pažymėti įspėjamąja piktograma . Norėdami įgalinti mygtuką **Gerai** ir įtraukti šio įrenginio taisyklę, atlikite šiuos veiksmus:

- Iš naujo prijunkite įrenginį
- Naudokitės įrenginiu (pvz., paleiskite „Windows“ programą „Kamera“, kad pažadintumėte internetinę kamerą)

Įrenginio kontrolės taisyklių pridėjimas

Įrenginio valdymo taisyklė apibrėžia veiksmą, atliktiną, kai įrenginys, atitinkantis taisyklės kriterijų, bus prijungtas prie kompiuterio.



Kad būtų patogiau nustatyti, įveskite taisyklės aprašymą į lauką **Pavadinimas**. Spustelėkite perjungiklį, esantį šalia **Taisyklė įjungta**, kad uždraustumėte arba įgalintumėte šią taisyklę. Tai gali būti naudinga, jei nenorite taisyklės panaikinti visam laikui.

Įrenginio tipas

Iš išskleidžiamojo meniu pasirinkite išorinio įrenginio tipą (diskų atminties įrenginys / nešiojamasis įrenginys „Bluetooth“ / „FireWire“ / ...). Įrenginių tipų informacija gaunama iš operacinės sistemos, o jei įrenginys prijungtas prie kompiuterio, ją galima peržiūrėti sistemos įrenginių tvarkytuvėje. Atminties įrenginiai gali būti išoriniai diskai arba įprasti atminties kortelių skaitytuvai, prijungti per USB arba „FireWire“. Lustinių kortelių skaitytuvai – tai visi skaitytuvai, nuskaitantys lustines korteles su lustu, pvz., SIM arba atpažinimo korteles. Vaizdo įrenginių pavyzdžiai yra skaitytuvai arba kameros. Kadangi šie įrenginiai pateikia informaciją tik apie savo veiksmus, o ne apie vartotojus, juos galima užblokuoti tik visuotinai.

Veiksmas

Prieiga prie ne atminties įrenginių gali būti leidžiama arba blokuojama. Tuo tarpu atminties įrenginių taisyklės leidžia pasirinkti vieną šių teisių parametrų:

- **Leisti** – bus leidžiama visa prieiga prie įrenginio.
- **Blokuoti** – prieiga prie įrenginio bus blokuojama.
- **Rašymo blokavimas** – bus leidžiama įrenginį tik skaityti.
- **Įspėti** – kaskart prijungus įrenginį, vartotojui pranešama, ar jis leidžiamas / blokuojamas, ir sukuriamas žurnalo įrašas. Įrenginiai neįsimenami, o kitą kartą prijungus tą patį įrenginį vis tiek parodomas pranešimas.

Atminkite, kad ne visos teisės (veiksmai) suteikiamos visų tipų įrenginiams. Jei naudojate atminties įrenginį,

leidžiami visi keturi veiksmai. Ne atminties įrenginiuose leidžiami tik trys veiksmai (pavyzdžiui, veiksmas **Rašymo blokavimas** negali būti taikomas „Bluetooth“, todėl „Bluetooth“ įrenginys gali būti tik leidžiamas, užblokuotas arba dėl jo pateikiamas įspėjimas).

Kriterijų tipas

Pasirinkite **Įrenginių grupė** arba **Įrenginys**.

Toliau pateikiami papildomi parametrai, kurie gali būti naudojami taisyklėms pakoreguoti ir pritaikyti jas įvairiems įrenginiams. Visiems parametrams yra svarbios didžiosios ar mažosios raidės bei visi jie palaiko pakaitos simbolius (*, ?):

- **Tiekėjas** – filtruokite pagal tiekėjo pavadinimą arba ID.
- **Modelis** – duotas įrenginio pavadinimas.
- **Serijos numeris** – išoriniai įrenginiai dažniausiai turi savo serijos numerį. CD / DVD tai yra duotos laikmenos, o ne CD įrenginio serijos numeris.

Jei šie parametrai nenustatomi, taisyklė ieškodama atitikmenų šios taisyklės nepaisys. Filtravimo parametrams visuose teksto laukuose yra svarbios didžiosios ir mažosios raidės bei palaikomi pakaitos simboliai (klaustukas (?) reiškia vieną simbolį, o žvaigždutė (*) reiškia eilutę iš nulio ar daugiau simbolių).

Jei norite peržiūrėti informaciją apie įrenginį, sukurkite šio tipo įrenginiui taisyklę, prijunkite įrenginį prie kompiuterio, tada patikrinkite išsamią įrenginio informaciją, kuri pateikiama Įrenginių valdymo žurnale.

Registravimo pavojingumas

ESET Internet Security įrašo visus svarbius įvykius į žurnalo failą, kurį galima peržiūrėti tiesiai iš pagrindinio meniu. Spustelėkite **Įrankiai** > **Žurnalo failai**, tada išskleidžiamajame meniu **Žurnalas** pasirinkite **Įrenginio kontrolė**.

- **Visada** – registruojami visi įvykiai.
- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimas** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Nėra** – žurnalai nekuriami.

Vartotojų sąrašas

Taisyklės gali būti ribojamos tam tikriems naudotojams arba naudotojų grupėms, įtraukiant juos į naudotojų sąrašą, spustelėjus šalia **naudotojų sąrašo** esantį mygtuką **Redaguoti**.

- **Pridėti** – atidaro **objekto tipus: Vartotojų arba grupių** dialogo langas leidžia pasirinkti norimus vartotojus.
- **Šalinti** – šalina pasirinktą vartotoją iš filtro.

Naudotojų sąrašo apribojimai

Naudotojų sąrašo negalima apibrėžti taisyklėms, taikomoms konkretiems įrenginių tipams:

- USB spausdintuvas
- „Bluetooth“ įrenginys
- Lustinių kortelių skaitytuvas
- Vaizdavimo įrenginys
- Modemas
- LPT / COM prievadas

Pranešti naudotojui – jei bus prijungtas įrenginys, kurį blokuoja esama taisyklė, bus rodomas pranešimo langas.

Įrenginių grupės

Prie kompiuterio prijungtas įrenginys gali kelti saugumo pavojų.

Įrenginių grupių langas yra padalytas į dvi dalis. Dešinėje lango pusėje yra įrenginių, kurie priklauso atitinkamai grupei, sąrašas, o kairėje – sukurtos grupės. Pasirinkite grupę su reikiamu įrenginių sąrašu, kad ji būtų parodyta dešiniajame polangyje.

Atidarę įrenginių grupių langą ir pasirinkę grupę galite į sąrašą pridėti įrenginių arba jų pašalinti. Kita būdas pridėti įrenginių prie grupės – importuoti juos iš failo. Arba galite spustelėti mygtuką **Surinkti**, kad visi prie kompiuterio prijungti įrenginiai būtų pateikti lange **Aptikti įrenginiai**. Spustelėdami **Gerai** sudarytame sąraše pasirinkite įrenginius, kuriuos norite pridėti prie grupės.

Valdymo elementai

Pridėti – galite pridėti grupę įrašydami jos pavadinimą, arba pridėti įrenginį prie esamos grupės – tai priklauso nuo to, kurioje lango dalyje spustelite mygtuką.

Redaguoti – jums leidžiama keisti pasirinktos grupės pavadinimą ar įrenginio parametrus (teikėją, modelį, serijos numerį).

Naikinti – atsižvelgiant į tai, kurioje lango dalyje spustelėjote mygtuką, panaikinama pasirinkta grupė ar įrenginys.

Importuoti – importuojamas įrenginių sąrašas iš tekstinio failo. Norint importuoti įrenginius iš tekstinio failo, reikalingas tinkamas formatavimas.

- Kiekvienas įrenginys pateikiamas naujoje eilutėje.
- **Tiekėjas ,** Modelis **ir Serijos numeris** turi būti pateikti kiekvienam įrenginiui ir atskirti kableliu.

Tekstinių failų turinio pavyzdys:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Eksportuoti – eksportuoja įrenginių sąrašą į failą.

Mygtukas **Pateikti** parodo visų šiuo metu prijungtų įrenginių apžvalgą su informacija apie įrenginio tipą, įrenginio tiekėją, modelį ir serijos numerį (jei toks yra).

Pridėti įrenginį

Spustelėkite **Pridėti** dešiniajame lange, kad įtrauktumėte įrenginį į esamą grupę. Toliau pateikiami papildomi parametrai, kurie gali būti naudojami taisyklėms pakoreguoti ir pritaikyti jas įvairiems įrenginiams. Visiems parametrams yra svarbios didžiosios ar mažosios raidės bei visi jie palaiko pakaitos simbolius (*, ?):

- **Tiekėjas** – filtruokite pagal tiekėjo pavadinimą arba ID.
- **Modelis** – duotas įrenginio pavadinimas.
- **Serijos numeris** – išoriniai įrenginiai dažniausiai turi savo serijos numerį. CD / DVD tai yra duotos laikmenos, o ne CD įrenginio serijos numeris.
- **Aprašas** – jūsų įrenginio aprašas, kad būtų lengviau sisteminti.

> Jei šie parametrai nenustatomi, taisyklė ieškodama atitikmenų šios taisyklės nepaisys. Filtravimo parametrams visuose teksto laukuose yra svarbios didžiosios ir mažosios raidės bei palaikomi pakaitos simboliai (klaustukas [?] reiškia vieną simbolį, o žvaigždutė [*] reiškia eilutę iš nulių ar daugiau simbolių).

Spustelėkite **Gerai**, kad būtų įrašyti keitimai. Spustelėkite **Atšaukti**, jei langą **Įrenginių grupės** norite uždaryti neįrašę pakeitimų.

> Sukūrę įrenginių grupę, turite pridėti naują sukurtos įrenginių grupės įrenginio valdymo taisyklę ir pasirinkti veiksmą, kurio reikia imtis.

Atminkite, kad ne visos teisės (veiksmai) suteikiamos visų tipų įrenginiams. Jei naudojate atminties įrenginį, leidžiami visi keturi veiksmai. Ne atminties įrenginiuose leidžiami tik trys veiksmai (pavyzdžiui, veiksmas **Rašymo blokavimas** negali būti taikomas „Bluetooth“, todėl „Bluetooth“ įrenginys gali būti tik leidžiamas, užblokuotas arba dėl jo pateikiamas įspėjimas).

Interneto kameros apsauga

Interneto kameros apsauga praneša apie procesus ir programas, kurie pasiekia jūsų kompiuterio interneto kamerą. Kai programa bando pasiekti kamerą, pasirodo pranešimas, kuriame galite **leisti** arba **blokuoti** prieigą. Perspėjimo lango spalva priklauso nuo programos reputacijos.

Interneto kameros apsaugos nustatymų parinktys gali būti keičiamos per Išplėstiniai nustatymai > **Apsaugos priemonės** > **Įrenginio kontrolė** > **Interneto kameros apsauga**.

Norėdami aktyvinti žiniatinklio kameros apsaugos funkciją ESET Internet Security, įjunkite perjungiklį šalia **Įjungti žiniatinklio kameros apsaugą**.

Kai įjungsite interneto kameros apsaugą, parinktis **Taisyklės** taps aktyvi ir galėsite atidaryti langą Taisyklių rengyklė.

Norėdami išjungti įspėjimus taisyklę turinčioms programoms, kurios buvo modifikuotos, bet vis dar turi galiojantį skaitmeninį parašą (pvz., programos naujinimą), įjunkite perjungiklį šalia **Išjungti modifikuotų programų žiniatinklio kameros prieigos įspėjimus**.

Interneto kameros apsaugos taisyklių rengyklė

Šiame lange parodomos esamos taisyklės ir leidžiama kontroliuoti programas bei procesus, kurie pasiekia kompiuterio interneto kamerą pagal jūsų atliekamus veiksmus.

Galimi šie veiksmai:

- **Leisti prieigą**
- **Blokuoti prieigą**

- **Prašyti** (prašo naudotojo kaskart, kai programa bando pasiekti internetinę kamerą)

Jei nebenorite gauti pranešimų, kai programos bando pasiekti internetinę kamerą, pašalinkite žymą iš žymės laukelio šalia stulpelio **Pranešti**.

> **Iliustruotos instrukcijos**
> Kaip sukurti ir redaguoti interneto kameros taisykles programoje ESET Internet Security.

ThreatSense

„ThreatSense“ sudaro įvairūs sudėtiniai grėsmių aptikimo metodai. Ši technologija yra iniciatyvi, o tai reiškia, kad ji užtikrina apsaugą, vos tik pradeda plisti nauja grėsmė. Joje kartu naudojama kodų analizė, kodų imitavimas, bendrieji kodai ir virusų kodai, kurie darniai veikia ir gerokai padidina sistemos saugumą. Nuskaitymo modulis gali vienu metu kontroliuoti keletą duomenų srautų – tai padidina efektyvumą ir aptikimo greitį. Be to, „ThreatSense“ technologija sėkmingai panaikina kenkėjiškas prieigos programas.

„ThreatSense“ modulio nustatymų parinktys leidžia nurodyti keletą nuskaitymo parametrų:

- failų, kurie turi būti nuskaityti, tipai ir plėtiniai;
- įvairių aptikimo metodų derinys;
- valymo lygiai ir t. t.

Norėdami patekti į nustatymo langą, išplėstinio nustatymo lange spustelėkite **„ThreatSense**“ parametrai, kad būtų parodyti moduliai, kuriems naudojama ThreatSense technologija (žr. toliau). Skirtingiems saugumo scenarijams gali reikėti skirtingų konfigūracijų. Atsižvelgiant į tai, „ThreatSense“ yra atskirai konfigūruojama šiems apsaugos moduliams:

- Failų sistemos apsauga realiuoju laiku
- Laukimo būsenos nuskaitymas
- Nuskaitymas paleidžiant
- Dokumentų apsauga
- El. pašto programų apsauga
- Prieigos prie saityno apsauga

- Kompiuterio nuskaitymas

„ThreatSense“ parametrai yra optimizuoti kiekvienam moduliui ir jų keitimas gali labai paveikti sistemos veikimą. Pavyzdžiui, pakeitus parametrus, kad visada būtų nuskaitomos momentinio pakavimo programos, arba įjungus išplėstinę euristiką failų sistemos apsaugos realiuoju laiku modulyje, sistemos darbas gali sulėtėti (paprastai naudojant šiuos metodus nuskaitomi tik naujai sukurti failai). Rekomenduojame palikti numatytuosius „ThreatSense“ parametrus nepakeistus visuose moduliuose, išskyrus kompiuterio nuskaitymą.

Nuskaitytini objektai

Šiame skyriuje galite nurodyti, kurie kompiuterio komponentai ir failai bus nuskaityti ieškant įsiskverbimų.

Operacinė atmintis – nuskaitomos grėsmės, kurios atakuoja sistemos operacinę atmintį.

Paleidimo sektorius / UEFI – nuskaitomi sistemos įkrovimo sektoriai tikrinant, ar nėra kenkėjiškos programinės įrangos pagrindiniame sistemos įkrovimo įraše. Daugiau apie UEFI skaitykite terminų žodyne.

El. laiškų failai – programa palaiko šiuos plėtinius: DBX („Outlook Express“) ir EML.

Archyvai – programa palaiko šiuos plėtinius: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ir daugelį kitų.

Išsiskleidžiantieji archyvai – išsiskleidžiantieji archyvai (SFX) yra archyvai, kurie gali išsiskleisti patys.

Momentiniai pakuotuvai – įvykdytos momentinio išpakavimo programos (skirtingai nei standartinių tipų archyvai) vėl suglaudinamos atmintyje. Be standartinių statinių pakavimo programų (UPX, yoda, ASPack, FSG ir t. t.), naudodamas kodų imitavimo principą skaitytuvas gali atpažinti kelis papildomus pakuotuvų tipus.

Nuskaitymo parinktys

Pasirinkite metodus, kurie bus naudojami nuskaitant sistemą ir ieškant įsiskverbimų. Galimos šios parinktys:

Euristika – euristika yra algoritmas, analizuojantis programų (kenkimo programinės įrangos) veiklą. Pagrindinis šios technologijos privalumas yra gebėjimas identifikuoti kenkimo programinę įrangą, kurios nebuvo ankstesnėje aptikimo modulio versijoje arba ji nebuvo žinoma. Trūkumas yra klaidingų pavojaus pranešimų (labai maža) tikimybė.

Išplėstinė euristika / DNA kodai – išplėstinė euristika yra unikalus ESET sukurtas algoritmas, optimizuotas aptikti kompiuterio kirminus bei Trojos arklius ir yra parašytas aukšto lygio programavimo kalbomis. Naudojant išplėstinę euristiką, gerokai padidėja ESET produktų grėsmių aptikimo galimybės. Kodai gali patikimai aptikti ir identifikuoti virusus. Naudojant automatinę naujinimo sistemą, nauji kodai tampa pasiekiami per kelias valandas nuo grėsmės atskleidimo. Kodų trūkumas yra tai, kad jie aptinka tik jiems žinomus virusus (arba šiek tiek modifikuotas jų versijas).

Valymas

Valymo parametrai apibrėžia ESET Internet Security veiksmus valant objektus. Yra 4 valymo lygiai:

ThreatSense siūlo šiuos atkūrimo (t. y. valymo) lygius.

Atkūrimas programoje ESET Internet Security

Valymo lygis	Aprašymas
Visada valyti objektą	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais retais atvejais (pvz., esant sisteminiams failams), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju palikti	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais atvejais (pvz., esant sisteminiams failams arba archyvams, kuriuose yra ir švarūs, ir užkrėsti failai), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju paklausti	Valant objektus, bandoma atkurti aptikimą. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, galutiniam naudotojui rodomas interaktyvus įspėjimas ir jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Daugeliu atveju ši nuostata yra rekomenduojama.
Visada klausti galutinio naudotojo	Valant objektus, galutiniam naudotojui rodomas interaktyvus langas, kuriame jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Šis lygis skirtas labiau patyrusiems naudotojams, kurie žino, kokį veiksmą atlikti aptikimo atveju.

Išimtys

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis „ThreatSense“ parametrų nustatymo skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

Kita

Konfigūruojant „ThreatSense“ modulio kompiuterio užsakomojo nuskaitymo parametrų nustatymus, papildomai pasiekiamos ir šios parinktys, pateikiamos skyriuje **Kita**:

Nuskaityti kintamuosius duomenų srautus (ADS) – NTFS failų sistemos naudojami kintamieji duomenų srautai yra failų ir aplankų ryšiai, kurie nematomi įprastoms nuskaitymo priemonėms. Daugelis įsiskverbimų bando išvengti aptikimo apsimesdami kintamaisiais duomenų srautais.

Vykdyti mažo prioriteto foninius nuskaitymus – kiekviena nuskaitymo seka naudoja tam tikrą kiekį sistemos išteklių. Jeigu dirbate su programomis, kurios intensyviai naudoja sistemos išteklius, galite suaktyvinti mažo prioriteto foninį nuskaitymą ir taupyti išteklius savo programoms.

Registruoti visus objektus – nuskaitymo žurnale bus rodomi visi nuskaityti failai išsiskleidžiančiuosiuose archyvuose, net neužkrėsti (gali būti generuojama daug nuskaitymo žurnalo duomenų ir padidės nuskaitymo žurnalo failo dydis).

Įjungti išmanųjį optimizavimą – įjungus išmanųjį optimizavimą, naudojami optimaliausi parametrai, leidžiantys užtikrinti efektyviausią nuskaitymo lygį ir kartu palaikyti didžiausią nuskaitymo greitį. Įvairūs apsaugos moduliai išmaniai atlieka nuskaitymą, naudodami įvairius nuskaitymo metodus ir taikydami juos konkretiems failų tipams. Jei išmanusis optimizavimas išjungtas, atliekant nuskaitymą taikomi tik vartotojo apibrėžti parametrai tam tikrų modulių ThreatSense šerdyje.

Saugoti paskutinį prieigos laiką – nurodykite šią parinktį, norėdami išlaikyti nuskaitytų failų originalius prieigos laikus, o ne naujinti juos (pavyzdžiui, naudojant su duomenų atsarginio kopijavimo sistemomis).

Ribos

Ribų skyriuje galima nurodyti maksimalius nuskaitomų objektų dydžius ir archyvų įdėties lygius:

Objekto parametrai

Maksimalus objekto dydis – apibrėžia maksimalų nuskaitomų objektų dydį. Antivirusinės programos modulis nuskaitys tik mažesnius nei nurodytas dydis objektus. Šią parinktį turėtų keisti tik patyrę vartotojai, kurie gali turėti tam tikrų priežasčių neįtraukti didelių objektų į nuskaitymą. Numatytoji reikšmė: neribota.

Maksimali objekto nuskaitymo trukmė (sek.) – apibrėžia maksimalią objekto failų (pvz., esančių RAR / ZIP archyve arba el. laiške su keliais priedais) nuskaitymo trukmę. Šis nustatymas netaikomas pavieniams failams. Jei įvesta naudotojo apibrėžta vertė ir tas laikas praėjo, nuskaitymas bus sustabdytas kuo greičiau, neatsižvelgiant į tai, ar kiekvieno failo nuskaitymas objekte yra užbaigtas.
Archyvo su dideliais failais atveju nuskaitymas bus sustabdytas išskleidus failą iš archyvo (pvz., kai naudotojo apibrėžtas kintamasis yra 3 sekundės, bet failo išskleidimas užtrunka 5 sekundes). Praėjus nurodytam laikui, likę archyvo failai nebus nuskaitomi.
Norėdami apriboti nuskaitymo trukmę, taip pat ir didesnių archyvų atveju, naudokite parinktis **Maksimalus objekto dydis** ir **Maksimalus failo archyve dydis** (nerekomenduojama dėl galimos rizikos saugai).
Numatytoji reikšmė: neribota.

Archyvo nuskaitymo nustatymai

Archyvo įdėties lygis – nurodo maksimalų archyvų nuskaitymo gylį. Numatytoji vertė: 10.

Maksimalus failo archyve dydis – ši parinktis leidžia nurodyti, kokio maksimalaus dydžio (kai jie išskleidžiami) archyve esantys failai bus nuskaitomi. Maksimali reikšmė: **3 GB**.

Mes nerekomenduojame keisti numatytųjų verčių: dirbant įprastai, jų keisti nėra priežasties.

Valymo lygiai

Norėdami pakeisti norimo apsaugos modulio valymo lygio nustatymus, išplėskite **ThreatSense** (pavyzdžiui, **Failų sistemos apsauga realiuoju laiku**) ir išskleidžiamajame meniu pasirinkite **Valymo lygis**.

ThreatSense siūlo šiuos atkūrimo (t. y. valymo) lygius.

Atkūrimas programoje ESET Internet Security

Valymo lygis	Aprašymas
Visada valyti objektą	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais retais atvejais (pvz., esant sisteminiams failams), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.
Jei saugu, valyti objektą, priešingu atveju palikti	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais atvejais (pvz., esant sisteminiams failams arba archyvams, kuriuose yra ir švarūs, ir užkrėsti failai), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.

Valymo lygis	Aprašymas
Jei saugu, valyti objektą, priešingu atveju paklausti	Valant objektus, bandoma atkurti aptikimą. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, galutiniam naudotojui rodomas interaktyvus įspėjimas ir jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Daugeliu atveju ši nuostata yra rekomenduojama.
Visada klausti galutinio naudotojo	Valant objektus, galutiniam naudotojui rodomas interaktyvus langas, kuriame jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Šis lygis skirtas labiau patyrusiems naudotojams, kurie žino, kokį veiksmą atlikti aptikimo atveju.

Failų plėtiniai, kurie nebus nuskaitomi

Neįtraukti failų plėtiniai yra ThreatSense dalis. Norėdami konfigūruoti neįtrauktus failų plėtinius, spustelėkite **ThreatSense**, kurį rasite pasirinkę Išplėstinis nustatymas bet kuriame modulyje, naudojančiame ThreatSense technologiją.

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis ThreatSense nustatymų skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

> Nesupainiokite su Procesų išimtys, HIPS išskyrimai arbaFailo / aplanko išimtys.

Pagal numatytąją parinktį nuskaitomi visi failai. Bet kurį plėtinį galima įtraukti į failų, kurie nebus nuskaitomi, sąrašą.

Neįtraukti failų kartais būtina, jeigu nuskaitant tam tikro tipo failus blogai veikia programa, kuri naudoja failus su tam tikro tipo plėtiniais. Pavyzdžiui, gali tekti neįtraukti `.edb`, `.eml` ir `.tmp` plėtinių, kai naudojami „Microsoft Exchange“ serveriai.

> Norėdami įtraukti plėtinį į sąrašą, spustelėkite **Pridėti**. Įveskite plėtinį į tuščią laukelį (pvz., tmp) ir spustelėkite **Gerai**. Kai pasirinksite **Įvesti kelias vertes**, galėsite įtraukti kelis failų plėtinius, atskirtus eilutėmis, kableliais arba kabliataškiais (pvz., išskleidžiamajame meniu kaip skirtuką pasirinkite **Kabliataškis** ir įveskite `edb;eml;tmp`).
> Galite naudoti specialų simbolį „?“ (klaustuką). Klaustukas reiškia bet kurį simbolį (pvz., `?db`).

> Norėdami pamatyti tikslų failo plėtinį (jei toks yra) „Windows“ operacinėje sistemoje, turite pažymėti žymės langelį **Failo vardo plėtiniai** skiltyje **Windows Explorer** > **Rodyti** (skirtukas).

Papildomi ThreatSense parametrai

Norėdami redaguoti šiuos parametrus, atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Failų sistemos apsauga realiuoju laiku** > **Papildomi ThreatSense parametrai**.

Papildomi naujai sukurtų ir pakeistų failų „ThreatSense“ parametrai

Naujai sukurtų ar modifikuotų failų užkrėtimo tikimybė yra palyginti didesnė nei esamų failų. Dėl šios priežasties programa tikrina šiuos failus su papildomais nuskaitymo parametrais. ESET Internet Security naudoja išplėstinę euristiką, kuri gali aptikti naujas grėsmes prieš išleidžiant aptikimo modulio atnaujinimą kartu su parašu pagrįstais nuskaitymo metodais.

Be naujai sukurtų failų, taip pat atliekamas **Išsiskleidžiančiųjų archyvų** (.sfx) ir **Momentinio išpakavimo programų**

(viduje suglaudintų vykdomųjų failų) nuskaitymas. Pagal numatytuosius nustatymus archyvai nuskaitomi iki 10-ojo įdėjimo lygio ir yra tikrinami neatsižvelgiant į jų faktinį dydį. Norėdami modifikuoti archyvo nuskaitymo nustatymus, atšaukite parinkties **Numatytieji archyvo nuskaitymo nustatymai** pasirinkimą.

Papildomi vykdomųjų failų „ThreatSense“ parametrai

Išplėstinė euristika vykdant failą – pagal numatytąją parinktį vykdant failus naudojama Išplėstinė euristika. Įjungus funkciją, primygtinai rekomenduojame palikti punktus Išmanusis optimizavimas ir ESET LiveGrid® įjungtus, kad būtų minimaliai paveiktas sistemos našumas.

Išplėstinė euristika vykdomiesiems failams iš keičiamosios laikmenos – išplėstinė euristika imituoja kodus virtualioje aplinkoje ir įvertina jų veikimą prieš leidžiant kodą vykdyti iš keičiamosios laikmenos.

Įrankiai

Pasirinkę Išplėstinis nustatymas > **Įrankiai**, galite konfigūruoti funkcijų, kurios suteikia papildomą saugą ir padeda supaprastinti ESET Internet Security administravimą, išplėstinius nustatymus.

- „Microsoft Windows®“ naujinimas
- ESET CMD
- Žurnalo failai
- Žaidimų režimas
- Diagnostika

„Microsoft Windows®“ naujinimas

„Windows“ naujinimo funkcija yra svarbus komponentas apsaugant vartotojus nuo kenkėjiškų programų. Todėl labai svarbu, kad įdiegtumėte „Microsoft Windows“ naujinimus, kai tik jie atsiranda. ESET Internet Security įspėja jus apie trūkstamus naujinimus, atsižvelgiant į jūsų nurodytą lygį skiltyje Išplėstinis nustatymas > **Įrankiai**. Galimi šie lygiai:

- **Naujinimų nėra** – nebus siūloma atsisiųsti jokių sisteminių naujinimų.
- **Pasirinktiniai naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip žemo prioriteto ir aukštesnius.
- **Rekomenduojami naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip įprastus ir aukštesnius.
- **Svarbūs naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip svarbius ir aukštesnius.
- **Kritiniai naujinimai** – bus siūloma atsisiųsti tik kritinius naujinimus.

Dialogo langas – sistemos naujinimai

Jei yra jūsų operacinės sistemos atnaujinimų, „ESET Internet Security“ pagrindiniame programos lange > **Apžvalga** rodomas pranešimas. Spustelėkite **Daugiau informacijos**, kad atidarytumėte sistemos naujinimų langą.

Sistemos naujinimų lange rodomas paruoštų atsisiųsti ir įdiegti naujinimų sąrašas. Naujinimo tipas rodomas šalia naujinimo pavadinimo.

Kad būtų parodytas langas Naujinimo informacija, kuriame pateikiama papildomos informacijos, dukart spustelėkite bet kurią naujinimo eilutę.

Spustelėkite **Vykdyti sistemos naujinimą**, kad atsisiųstumėte ir įdiegtumėte visus išvardytus operacinės sistemos naujinimus.

Naujinimo informacija

Sistemos naujinimų lange rodomas paruoštų atsisiųsti ir įdiegti naujinimų sąrašas. Naujinimo prioriteto lygis rodomas šalia naujinimo pavadinimo.

Spustelėkite **Vykdyti sistemos naujinimą**, kad prasidėtų operacinės sistemos naujinimų atsiuntimas ir diegimas.

Dešiniuoju pelės klavišu spustelėkite bet kurią atnaujinimo eilutę ir spustelėkite **Rodyti informaciją**, kad būtų rodomas naujas langas su papildoma informacija.

ESET CMD

Tai – funkcija, kuri įjungia išplėstines „ecmd“ komandas. Ji leidžia eksportuoti ir importuoti parametrus naudojantis komandos eilute (ecmd.exe). Iki šiol parametrus buvo galima eksportuoti tik naudojant GUI. ESET Internet Security konfigūraciją galima eksportuoti į *.xml* failą.

Kai įjungiate ESET CMD, galimi du įgaliojimo būdai:

- **Nėra** – įgaliojimo nėra. Šio būdo nerekomenduojame, nes jis suteikia galimybę importuoti bet kokią nepasirašytą konfigūraciją, o tai gali būti rizikinga.

- **Išplėstinių nustatymų slaptažodis** – reikalingas slaptažodis, norint importuoti konfigūraciją iš .xml failo; šis failas turi būti pasirašytas (žr. toliau apie .xml konfigūracijos failo pasirašymą). Slaptažodis, nurodytas dalyje Prieigos nustatymai turi būti pateiktas prieš importuojant naują konfigūraciją. Jei prieigos nustatymo nesate įjungę, slaptažodis neteisingas arba .xml formato konfigūracijos failas nepasirašytas, konfigūracija nebus importuojama.

Įjungę ESET CMD, galite importuoti ar eksportuoti ESET Internet Security konfigūracijas naudodami komandos eilutę. Galite tai daryti rankiniu būdu arba automatizuotai, naudodami susikurtą scenarijų.

Jei norite naudotis išplėstinėmis „ecmd“ komandomis, jas reikia paleisti turint administratoriaus privilegijas arba „Windows“ komandinę eilutę (cmd) atidaryti naudojantis funkcija **Paleisti administratoriaus teisėmis**. Kitaip jums bus parodytas pranešimas **Error executing command**. Be to, kai eksportuojate konfigūraciją, paskirties aplankas turi būti egzistuojantis. Kai ESET CMD nustatymai yra išjungtas, eksportavimo komanda vis dar veikia.

Parametrų eksportavimo komanda:
`ecmd /getcfg c:\config\settings.xml`

Parametrų importavimo komanda:
`ecmd /setcfg c:\config\settings.xml`

Išplėstines „ecmd“ komandas leisti galima tik vietoje.

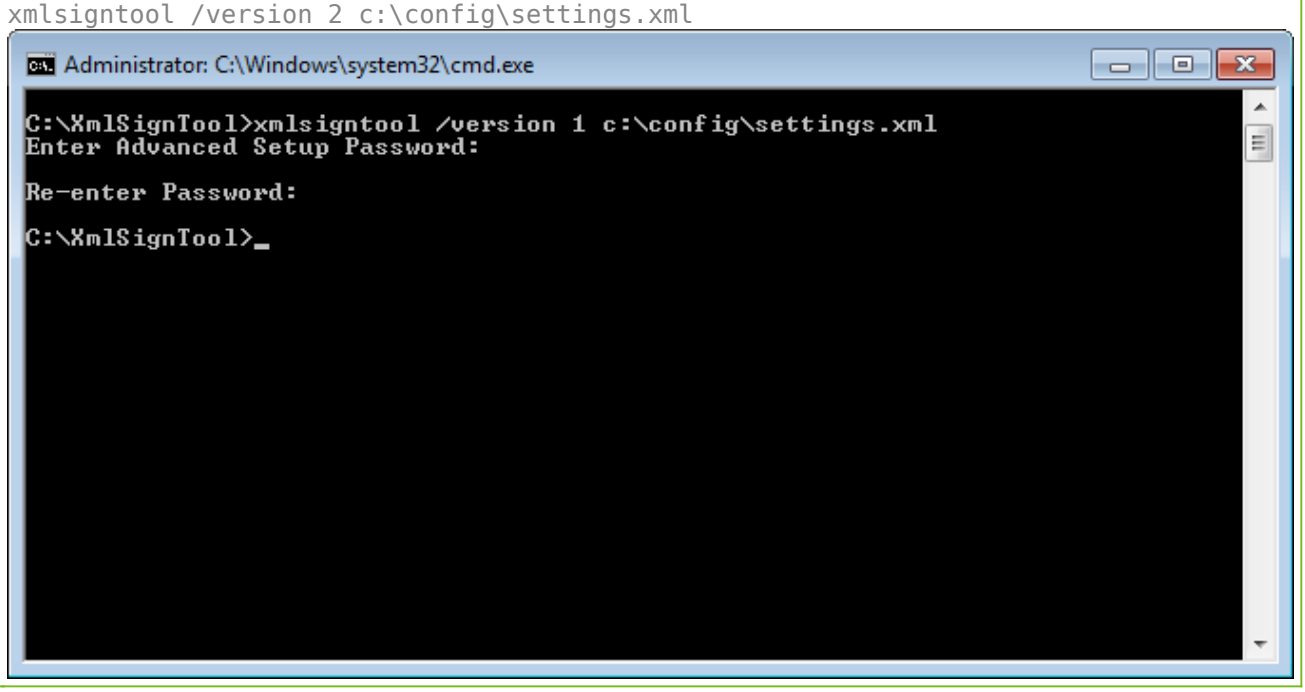
.xml formato konfigūracijos failo pasirašymas:

1. Atsisiųskite „XmlSignTool“ vykdomąjį failą.
2. Atidarykite „Windows“ komandinę eilutę (cmd) naudodamiesi funkcija **Paleisti administratoriaus teisėmis**.
3. Eikite į įrašymo vietą `xmlsigntool.exe`
4. Įvykdykite *.xml* formato konfigūracijos failo pasirašymo komandą: `xmlsigntool /version 1|2 <xml_file_path>`

`/version` Parametro reikšmė priklauso nuo jūsų ESET Internet Securityversijos. Ankstesnėms ESET Internet Security nei 11.1 versijoms naudokite `/version 1`. Dabartinei ESET Internet Security versijai naudokite `/version 2`.

5. Įveskite ir pakartokite Išplėstinių nustatymų slaptažodį, kai „XmlSignTool“ to paprašo. Jūsų *.xml* formato konfigūracijos failas dabar yra pasirašytas ir gali būti naudojamas importuoti į kitą ESET Internet Security egzempliorių naudojant ESET CMD suteikiant įgaliojimą slaptažodžiu.

Pasirašykite eksportuojamos konfigūracijos failo komandą:
`xmlsigntool /version 2 c:\config\settings.xml`



Jei pakeitėte savo Prieigos nustatymo slaptažodį ir norite importuoti konfigūraciją, kuri anksčiau buvo pasirašyta naudojant senąjį slaptažodį, turite dar kartą pasirašyti *.xml* formato konfigūracijos failą naudodami dabartinį slaptažodį. Tai leidžia naudoti ankstesnį konfigūracijos failą, prieš importavimą jo neeksportuojant į kitą įrenginį, kuriame veikia ESET Internet Security.

ESET CMD nerekomenduojama įjungti be įgaliojimo suteikimo, nes taip bus leidžiama importuoti bet kokią nepatvirtintą konfigūraciją. Meniu elemente Išplėstinis nustatymai > **Vartotojo sąsaja** > **Prieigos nustatymas** nustatykite slaptažodį, kuris neleistų vartotojams daryti nesankcionuotų pakeitimų.

Žurnalo failai

Registravimo konfigūraciją ESET Internet Security galite rasti Išplėstinis nustatymas > **Įrankiai** > **Žurnalo failai**. Žurnalų skyrius yra skirtas apibrėžti, kaip bus tvarkomi žurnalo įrašai. Programa automatiškai naikina senesnius žurnalo įrašus, kad būtų taupoma vieta diske. Galite žurnalo failams nurodyti šias parinktis:

Minimalus registravimo daugiažodiškumas – nurodo minimalų įvykių daugiažodiškumo lygį, kai jie registruojami:

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Klaidos** – įrašomos klaidos, pvz., „Klaida atsiunčiant failą“, ir kritinės klaidos.
- **Kritinės klaidos** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų, užkardą ir kt.).

Kai pasirinktas daugiažodiškumo lygis „Diagnostinis“, užregistruojami visi užblokuoti ryšiai.

Žurnalo įrašai, senesni nei lauke **Naikinti senesnius nei (dienų) įrašus** nurodytas dienų skaičius, bus automatiškai panaikinti.

Optimizuoti žurnalo failus automatiškai – pažymėjus žurnalo failai bus automatiškai defragmentuojami, jeigu procentinė reikšmė yra didesnė nei lauke **Jeigu nenaudojamų įrašų skaičius viršija (%)** nurodyta reikšme.

Jei norite pradėti žurnalo failų defragmentavimą, spustelėkite **Optimizuoti**. Atliekant šią procedūrą visi tušti žurnalo įrašai bus pašalinti ir tai pagerins žurnalų apdorojimo efektyvumą ir spartą. Šis pagerėjimas ypač akivaizdus, jeigu žurnaluose yra daug įrašų.

Parinktis **Įjungti teksto protokolą** suteikia galimybę žurnalus saugoti kitu failo formatu (atskirai nuo žurnalo failų):

- **Tikslinis aplankas** – aplankas, kuriame bus laikomi žurnalo failai (taikoma tik tekstui / CSV). Kiekvienas žurnalo skyrius turi savo failą su iš anksto apibrėžtu failo pavadinimu (pvz., jei žurnalams saugoti naudojate paprasto teksto failų formatą, virlog.txt skirtas žurnalo failų skyriui **Aptikimai**).
- **Tipas** – jei pasirinkote failų formatą **Tekstas**, žurnalai bus saugomi teksto faile, o duomenys bus atskiriami tabuliacijos ženklais. Taip pat taikoma kableliais atskiriamų duomenų **CSV** failo formatui. Jei pasirinksite **Įvykis**, žurnalai bus saugomi „Windows“ įvykių žurnale (jį galima peržiūrėti naudojant įvykių žiūryklę arba valdymo skydą), o ne faile.
- **Naikinti visus žurnalo failus** – ištrina visus saugomus žurnalus, šiuo metu pasirinktus išskleidžiamajame meniu **Tipas**. Sėkmingai panaikinus žurnalus bus parodytas pranešimas.

Kad būtų galima greičiau išspręsti problemas, ESET kartais jūsų gali paprašyti pateikti kompiuteryje saugomus žurnalus. ESET Log Collector priemonė leidžia paprastai surinkti reikiamą informaciją. Papildomos informacijos apie ESET Log Collector priemonę rasite ESET žinių bazės straipsnyje.

Žaidimų režimas

Žaidėjo režimas yra funkcija, skirta naudotojams, kuriems reikalingas nepertraukiamas jų programinės įrangos naudojimas, kai norima, kad netrukdytų pranešimo / perspėjimo langai ir nebūtų papildomai apkraunamas CPU. Žaidimų režimas taip pat gali būti naudojamas per pristatymus, kurie neturi būti pertraukiami antivirusinės programos veiksmų. Įjungus šią funkciją, visi iškylantieji langai išjungiami, o planuoklio veikla visiškai sustabdoma. Sistemos apsauga ir toliau veikia foniniu režimu, tačiau jai nereikia jokių vartotojo veiksmų.

Galite įjungti arba išjungti žaidėjo režimą pagrindiniame programos lange dalyje **Nustatymai** > **Kompiuterio apsauga** spustelėdami  arba  šalia **Žaidimų režimas**. Įjungus žaidimų režimą iškyla galima saugos rizika, todėl apsaugos būsenos piktograma užduočių juostoje įspėdama apie galimą pavojų pasidarys oranžinė. Be to, matysite šį įspėjimą pagrindiniame programos lange, kuriame **Žaidimų režimas aktyvus** švies oranžine spalva.

Dalyje **Išplėstiniai nustatymai** > Įrankiai > **Žaidimų režimas** suaktyvinkite **Įjungti žaidimų režimą automatiškai programoms veikiant viso ekrano režimu**, kad žaidimų režimas būtų paleidžiamas kaskart įjungus programą viso ekrano režimu ir būtų išjungtas ją uždarius.

Suaktyvinkite **Išjungti žaidimų režimą automatiškai po** ir nustatykite laiką, kuriam praėjus žaidimų režimas bus išjungtas automatiškai.

> Jei užkarda veikia interaktyviuoju režimu ir įjungtas žaidimų režimas, gali iškilti problemų jungiantis prie interneto. Tai gali sukelti nepatogumų, jeigu paleidžiate žaidimą, kuris jungiamas prie interneto. Paprastai jūsų būtų prašoma patvirtinti šį veiksmą (jeigu nebuvo nustatyta ryšio taisyklių arba išimčių), tačiau vartotojo veiksmai žaidimų režimu neleidžiami. Jei ryšį norite leisti, nustatykite ryšio taisyklę visoms programoms, kurios gali susidurti su šia problema, arba naudokite kitą užkardos Filtravimo režimą. Atminkite, kad įjungus žaidimų režimą ir apsilankius rizikingame tinklalapyje arba naudojantis programa, kuri gali kelti pavojų saugai, tinklalapis arba programa gali būti blokuojami neparodant jokio paaiškinimo arba įspėjimo, nes vartotojo veiksmai neleidžiami.

Diagnostika

Diagnostikos skiltyje pateikiamos ESET procesų programos strigčių atminties išklotinės (pvz., „ekrn“). Programos strigties atveju parengiama atminties išklotinė. Ji gali padėti programuotojams taisyti klaidas ir šalinti įvairias ESET Internet Security problemas.

Spustelėkite išskleidžiamąjį meniu, esantį šalia punkto **Atminties išklotinės tipas**, ir pasirinkite vieną iš trijų galimybių:

- Pasirinkite **Išjungti**, kad išjungtumėte šią savybę.
- **Miniatiūrinis** (numatytoji) – įrašo mažiausią naudingos informacijos rinkinį, kuris gali padėti identifikuoti, kodėl programa netikėtai sugedo. Šis atminties išklotinės failas gali būti naudojamas, kai yra riboti vietos ištekliai. O kadangi įtraukiamas tik ribotas informacijos kiekis, analizuojant šį failą gali būti neaptiktos klaidos, kurios nebuvo tiesiogiai susijusios su gija, vykdoma, kai iškilo problema.
- **Visas** – įrašo visą sistemos atminties turinį, kai programa nenumatytai sustoja. Visos atminties išklotinėje gali būti procesų, kurie buvo vykdomi, kai buvo renkama atminties išklotinė, duomenys.

Paskirties katalogas – katalogas, kuriame bus sukuriama atminties išklotinė įvykus gedimui.

Atidaryti diagnostikos aplanką – spustelėkite **Atidaryti**, kad atidarytumėte šį katalogą naujame *Windows explorer* lange.

Sukurti diagnostikos išklotinę – spustelėkite **Sukurti** ir sukurkite diagnostikos išklotinės failą **Paskirties kataloge**.

Išplėstinis prisijungimas

Įgalinti išplėstinį prisijungimą rinkodaros pranešimuose – įrašyti visus įvykius, susijusius su produkto rinkodaros pranešimais.

Įjungti išplėstinį apsaugos nuo brukalo modulio registravimą – įrašo visus įvykius, kurie įvyksta apsaugos nuo brukalo nuskaitymo metu. Tai padeda programų kūrėjams nustatyti ir pašalinti su ESET apsaugos nuo brukalo moduliu susijusias problemas.

Įjungti išplėstinį „Anti-theft“ modulio registravimą – įrašo visus įvykius, kurie įvyksta „Anti-theft“, kad būtų galima nustatyti ir išspręsti problemas.

Įgalinti naršyklės apsaugos išplėstinį registravimą – įrašomi visi įvykiai, kurie įvyksta naudojantis saugia bankininkyste ir naršymu.

Įjungti išplėstinį prisijungimą prie kompiuterio nuskaitymo programos – įrašykite visus įvykius, kurie įvyksta Kompiuterio nuskaitymo arba Failų sistemos apsaugos realiuoju laiku failų.

Įjungti išplėstinį įrenginio kontrolės registravimą – įrašykite visus įvykius, kurie įvyksta veikiant įrenginio kontrolei. Tai padeda programų kūrėjams nustatyti ir pašalinti su įrenginio kontrole susijusias problemas.

Įjungti išplėstinį „Direct Cloud“ registravimą – įrašykite visus įvykius, kurie įvyksta ESET LiveGrid®. Tai padeda programų kūrėjams nustatyti ir pašalinti su ESET LiveGrid® susijusias problemas.

Įjungti išplėstinį dokumentų apsaugos registravimą – įrašykite visus įvykius, kuriuos fiksuoja dokumento apsauga, kad būtų lengviau nustatyti ir išspręsti problemas.

Įgalinti išplėstinį prisijungimą prie el. pašto programų apsaugos – įrašykite visus įvykius, įvykusius el. pašto programų apsaugos priemonėje ir el. pašto programos papildinyje, kad būtų galima nustatyti ir išspręsti problemas.

Įgalinti išplėstinį prisijungimą prie branduolio – įrašyti visus įvykius, vykstančius ESET branduolyje (ekrn).

Įjungti išplėstinį licencijos registravimą – įrašo visus produkto ryšius su ESET aktyvinimo arba ESET License Manager serveriais.

Įgalinti atminties sekimą – įrašyti visus įvykius, kurie padeda kūrėjams aptikti atminties nutekėjimą.

Įjungti išplėstinį tinklo apsaugos registravimą – PCAP formatu įrašo visus tinklo duomenis, kurie pereina užkardą, kad programų kūrėjai galėtų nustatyti ir išspręsti problemas, susijusias su užkarda.

Įgalinti tinklo duomenų srauto skaitytuvo išplėstinį prisijungimą – įrašykite visus duomenis, perduodamus per tinklo duomenų srauto skaitytuvą, PCAP formatu, kad padėtumėte kūrėjams diagnozuoti ir spręsti su tinklo duomenų srauto skaitytuvu susijusias problemas.

Įgalinti išplėstinį prisijungimą prie operacinės sistemos – įrašyti papildomą informaciją apie operacinę sistemą,

pvz., vykdomus procesus, centrinio procesoriaus aktyvumą ir disko operacijas. Tai gali padėti kūrėjams nustatyti ir ištaisyti nesklandumus, susijusius su jūsų operacinėje sistemoje veikiančiu ESET produktu.

Įjungti išplėstinį tėvų kontrolės registravimą – įrašykite visus įvykius, kurie įvyksta veikiant tėvų kontrolei. Tai padeda programų kūrėjams nustatyti ir pašalinti su tėvų kontrole susijusias problemas.

Įgalinti išplėstinį prisijungimą siunčiant „push“ pranešimus – įrašyti visus įvykius, vykstančius siunčiant „push“ pranešimus.

Įgalinti išplėstinį prisijungimą prie Failų sistemos apsaugos realiuoju laiku – įrašyti visus įvykius, kurie įvyksta Failų sistemos apsaugos realiuoju laiku failų ir aplankų nuskaitymo metu.

Įjungti išplėstinį naujinimo modulio registravimą – įrašo visus įvykius, kurie įvyksta naujinimo proceso metu. Tai gali padėti programuotojams diagnozuoti ir išspręsti problemas, susijusias su naujinimo moduliu.

Žurnalo failai yra *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Techninė pagalba

Susisiekę su ESET techninė pagalba, kai naudojate ESET Internet Security, galite pateikti sistemos konfigūracijos duomenis. Išskleidžiamajame meniu **Pateikti sistemos konfigūracijos duomenis** pasirinkite **Visada pateikti**, kad duomenys būtų pateikiami automatiškai, arba pasirinkite **Klausti prieš pateikiant**, kad prieš pateikiant duomenis jūsų būtų klausiama.

Junglumas

Konkrečiuose tinkluose įgaliotasis serveris gali būti tarpinė grandis palaikyti ryšiui tarp jūsų kompiuterio ir interneto. Jei naudojate įgaliotąjį serverį, turite nustatyti šiuos parametrus. Priešingu atveju, ESET Internet Security ir jo moduliai negali būti atnaujinami automatiškai. Šiame ESET Internet Security, įgaliotojo serverio konfigūracija galima dviejuose skirtinguose Išplėstiniai nustatymai skyriuose.

Visuotinius įgaliotojo serverio nustatymus galima konfigūruoti pasirinkus Išplėstiniai nustatymai > **Jungiamumas** > **Įgaliotasis serveris**. Nurodžius įgaliotąjį serverį šiame lygmenyje, nustatomi visuotiniai įgaliotojo serverio parametrai visai programai ESET Internet Security. Čia nustatytus parametrus naudos visi moduliai, kuriems reikia jungtis prie interneto.

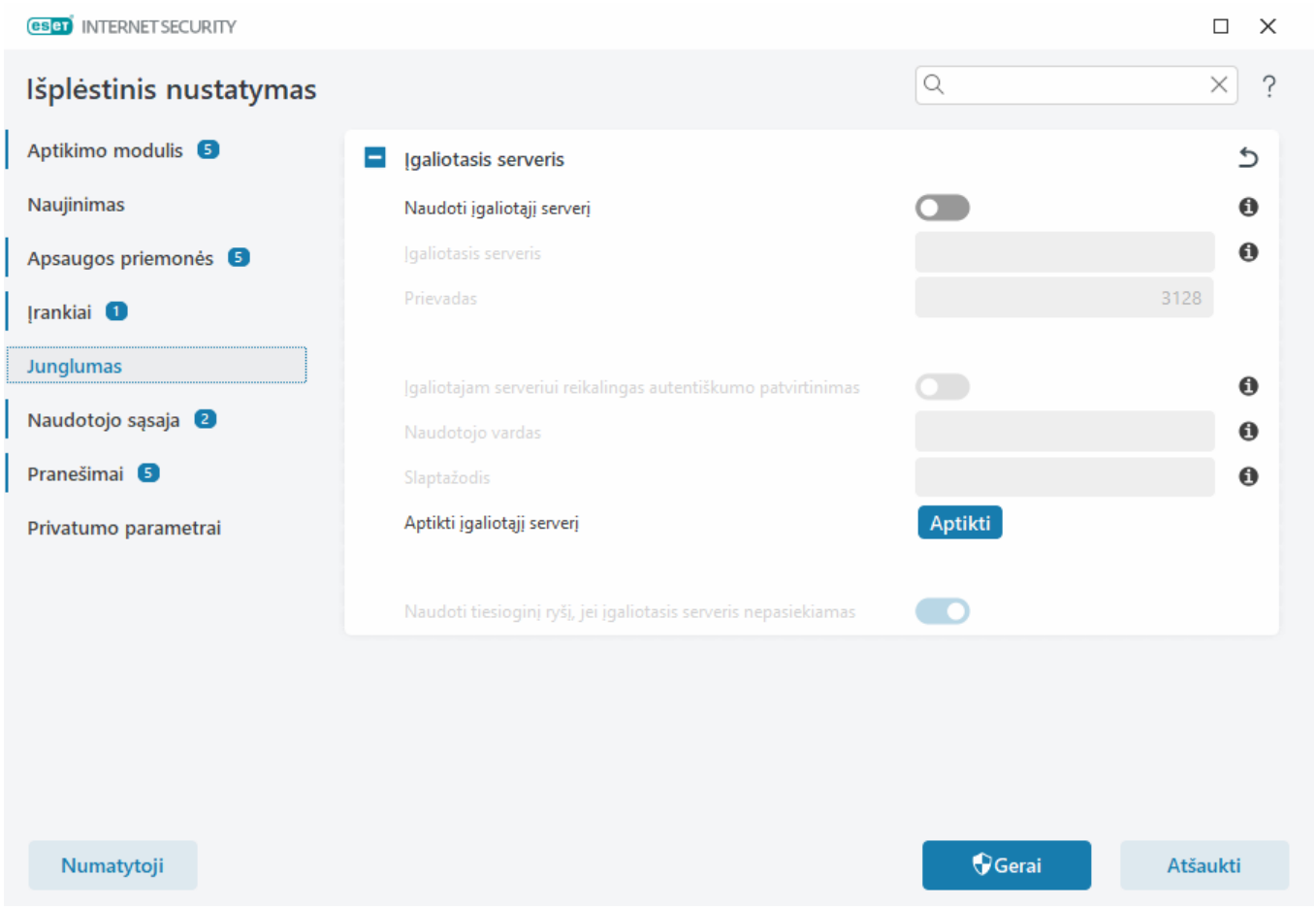
Norėdami nurodyti visuotinius įgaliotojo serverio nustatymus, įjunkite **Naudoti įgaliotąjį serverį** ir įveskite **įgaliotojo serverio** adresą kartu su įgaliotojo serverio **prievado** numeriu.

Jeigu ryšiui su įgaliotuoju serveriu reikalingas atpažinimas, pasirinkite **Įgaliotajam serveriui reikalingas atpažinimas** ir į atitinkamus laukus **Naudotojo vardas** bei **Slaptažodis** įveskite reikiamą informaciją. Spustelėkite **Aptikti įgaliotąjį serverį**, kad automatiškai aptiktumėte ir užpildytumėte įgaliotojo serverio nustatymus. ESET Internet Security nukopijuos parametrus, nurodytus interneto parinktyse Internet Explorer arba Google Chrome.

Įgaliotojo serverio parametruose vartotojo vardą ir slaptažodį turite įvesti rankiniu būdu.

Naudoti tiesioginį ryšį, jei įgaliotasis serveris nepasiekiamas – jei ESET Internet Security yra sukonfigūruotas, kad prisijungtų naudojant įgaliotąjį serverį, o šis serveris yra nepasiekiamas, ESET Internet Security nepaisys įgaliotojo serverio ir jungsis prie ESET serverių tiesiogiai.

Įgaliotojo serverio nustatymus galima konfigūruoti pasirinkus Išplėstinis nustatymas > **Naujinti** > **Profiliai** > **Naujinimai** > **Ryšio parinktys** pasirenkant išskleidžiamojo meniu **Įgaliotojo serverio režimas** punktą **Jungtis per įgaliotąjį serverį**. Ši konfigūracija taikoma tik naujinimams ir rekomenduojama nešiojamiesiems kompiuteriams, gaunantiems modulių naujinimus iš nuotolinių vietų. Daugiau informacijos ieškokite Išplėstinio naujinimo nustatymas.



Vartotojo sąsaja

Norėdami konfigūruoti programos grafinės naudotojo sąsajos (GUI) veikimą, atidarykite Išplėstinis nustatymas > **Naudotojo sąsaja**.

Programos išvaizdą ir efektus galite koreguoti Naudotojo sąsajos elementai išplėstinės sąrankos ekrane.

Jeigu norite užtikrinti maksimalią savo saugos programinės įrangos saugą, galite neleisti šalinti arba jokių neįgaliotų keitimų, apsaugodami parametrus slaptažodžiu, naudodami Prieigos nustatymo įrankį.

Norėdami konfigūruoti sistemos pranešimų, aptikimo įspėjimų ir programos būsenų veikimą, žr. skyrių Pranešimai.

Naudotojo sąsajos elementai

Galite koreguoti „ESET Internet Security“ darbinę aplinką (GUI) pagal savo poreikius dalyje Išplėstiniai nustatymai > **Naudotojo sąsaja** > **Naudotojo sąsajos elementai**.

Spalvų režimas – „ESET Internet Security“ išskleidžiamajame meniu pasirinkite GUI spalvų schemą:

- **Tas pats, kas sistemos spalva** – nustato „ESET Internet Security“ spalvų schemą pagal operacinės sistemos nustatymus.
- **Tamsus** – „ESET Internet Security“ turės tamsią spalvų schemą (tamsusis režimas).
- **Šviesus** – „ESET Internet Security“ turės standartinę, šviesią spalvų schemą.

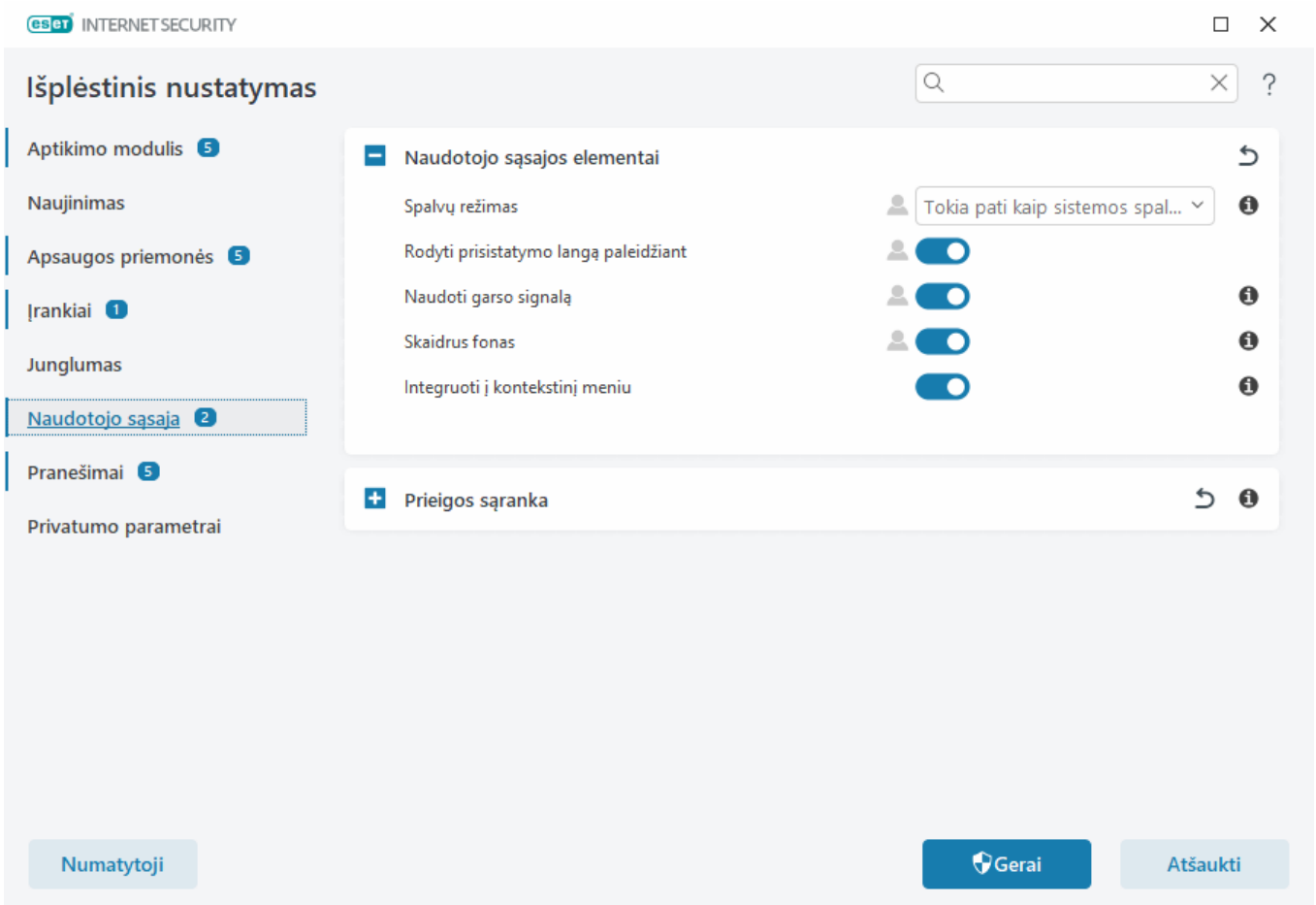
> Taip pat galite pasirinkti „ESET Internet Security“ GUI spalvų schemą viršutiniame dešiniajame pagrindinio programos lango kampe.

Rodyti paleidimo ekraną paleidžiant – „ESET Internet Security“ paleidimo metu rodomas paleidimo ekranas.

Naudoti garso signalą – leidžia garsą, kai nuskaitymo metu įvyksta kas nors svarbaus, pvz., kai aptinkama grėsmė arba baigiamas nuskaitymas.

Skaidrus fonas – įjungia skaidrų fono efektą pagrindiniame programos lange. Skaidrus fonas galimas tik naujausioms „Windows“ versijoms (RS4 ir naujesnėms versijoms).

Integruoti į kontekstinį meniu – integruoti ESET Internet Security valdymo elementus į kontekstinį meniu.



Prieigos nustatymas

ESET Internet Security parametrai yra itin svarbi jūsų saugos politikos dalis. Neįgalioti pakeitimai gali sukelti pavojų jūsų sistemos stabilumui ir saugai. Kad išvengtumėte neįgaliotų keitimų, nustatymų parametrus ir ESET

Internet Security šalinimą galite apsaugoti slaptažodžiu. Prieigos nustatymą galima konfigūruoti pasirinkus Išplėstinis nustatymas > **Naudotojo sąsajos** > **Prieigos nustatymai**.

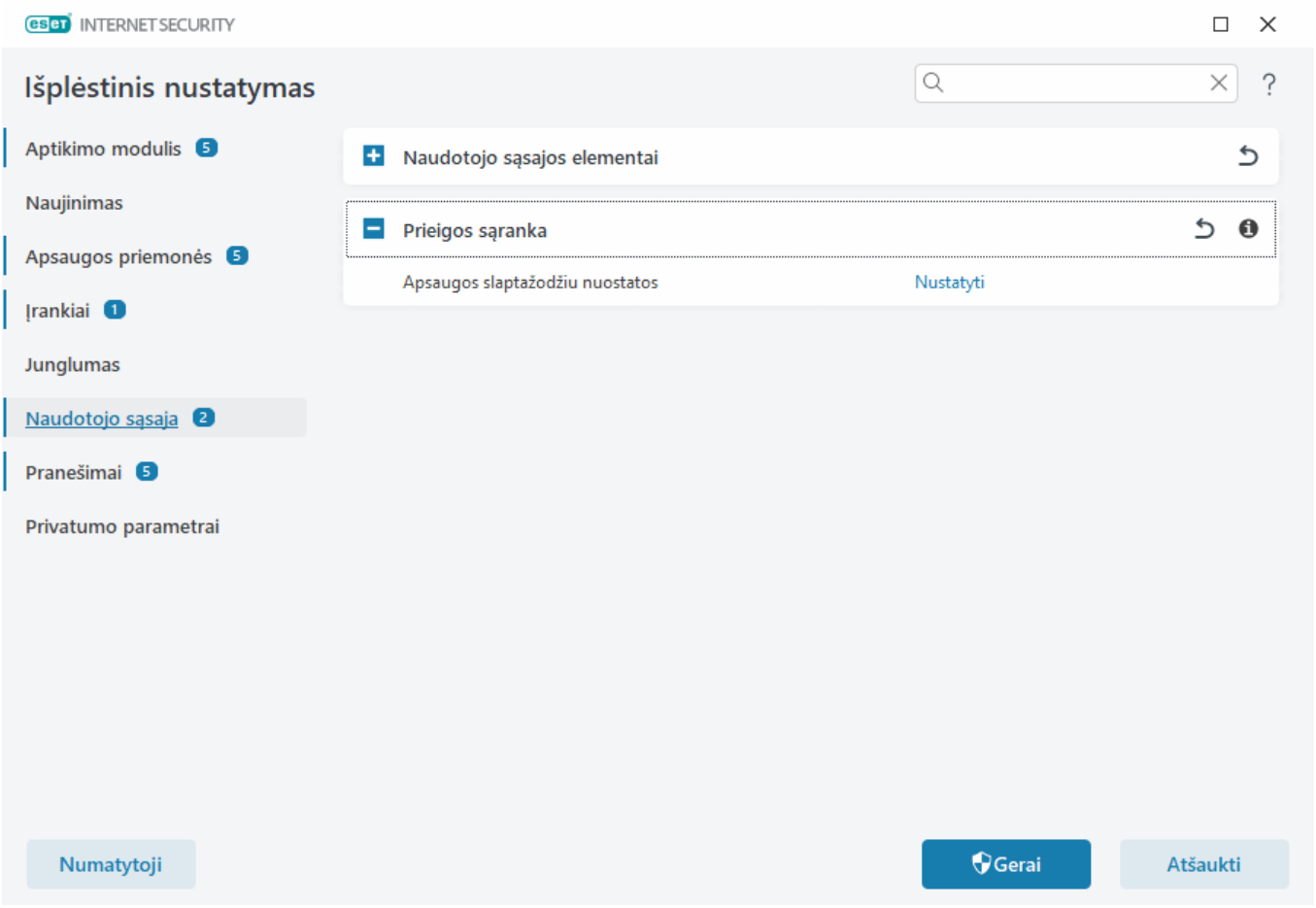
Jei norite nustatyti ar pakeisti slaptažodį, kad apsaugotumėte diegimo nustatymus ir ESET Internet Security šalinimą, spustelėkite **Nustatyti** prie **Apsaugos slaptažodžiu nuostatos**.

Norint pasiekti apsaugotą išplėstinį nustatymą, rodomas langas, skirtas įvesti slaptažodį. Jei pamiršote slaptažodį arba jo netekote, spustelėkite žemiau esančią parinktį **Atkurti slaptažodį** ir įveskite el. pašto adresą, kurį naudojote registruodami prenumeratą. ESET jums atsiųs el. laišką su patvirtinimo kodu ir instrukcija, kaip nustatyti iš naujo savo slaptažodį.

- Kaip atrakinti išplėstinį nustatymą

Norėdami pakeisti slaptažodį, spustelėkite **Keisti slaptažodį** šalia **Apsaugos slaptažodžiu nustatymai**.

Norėdami pašalinti slaptažodį, spustelėkite **Šalinti** šalia **Apsaugos slaptažodžiu nustatymai**.



Išplėstinio nustatymo slaptažodis

Norėdami apsaugoti „ESET Internet Security“ išplėstinę sąranką ir išvengti neteisėto modifikavimo, įveskite naują slaptažodį į laukus **Naujas slaptažodis** ir **Patvirtinti slaptažodį**. Spustelėkite **Gerai**.

Prireikus pakeisti esamą slaptažodį:

1. įveskite senąjį slaptažodį į lauką **Senas slaptažodis**.
2. Įveskite naująjį slaptažodį į laukus **Naujas slaptažodis** ir **Patvirtinti slaptažodį**.

3. Spustelėkite **Gerai**.

Šis slaptažodis bus reikalingas norint pasiekti išplėstinę sąranką.

Jei pamiršote slaptažodį, žiūrėkite Nustatymų slaptažodžio atrakinimas ESET HOME produktuose.

Norėdami atkurti prarastą ESET aktyvinimo raktą, prenumeratos galiojimo pabaigos datą arba kitą „ESET Internet Security“ prenumeratos informaciją, žr. Pamečiau aktyvinimo raktą.

Ekrano skaitytuvo palaikymas

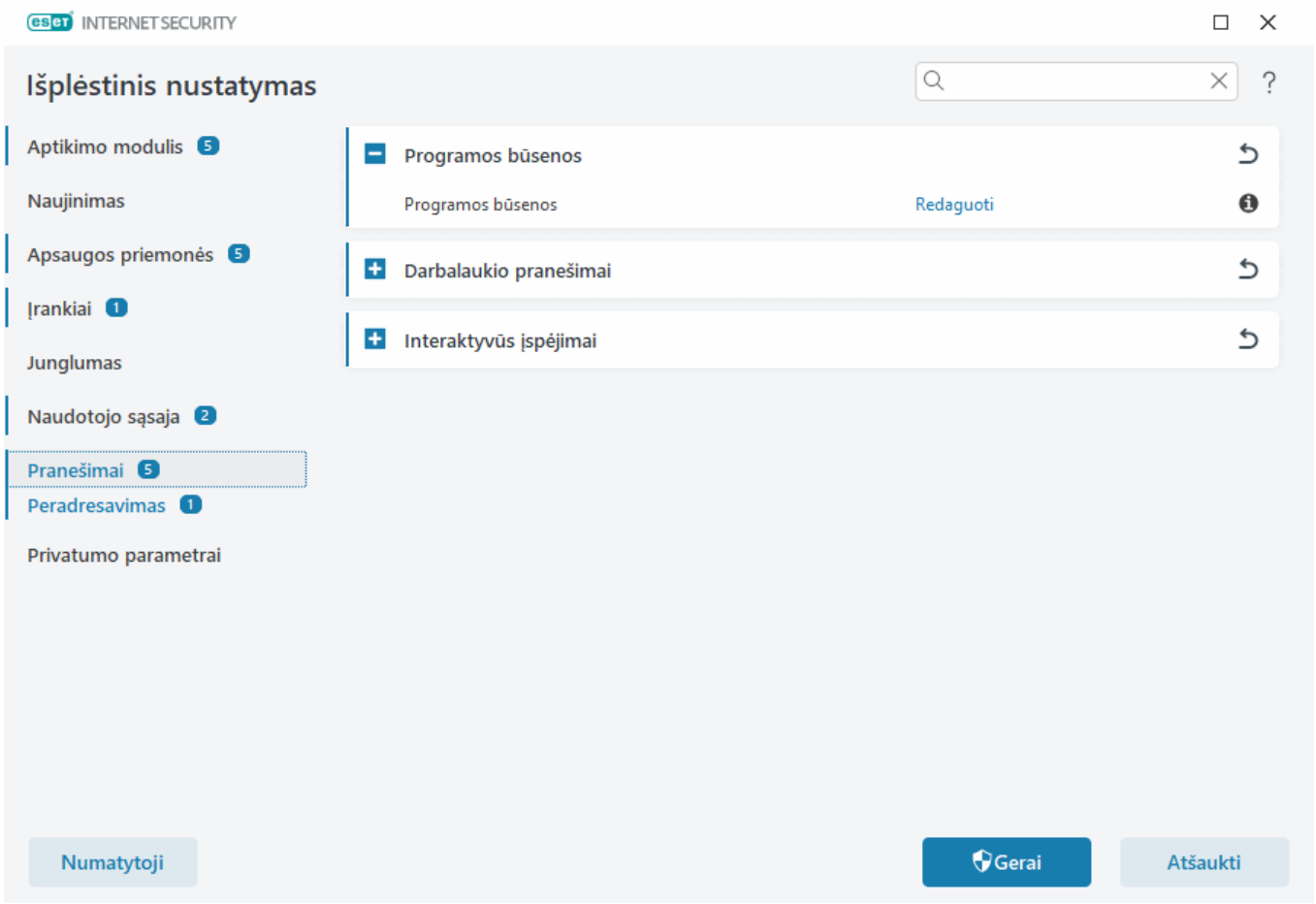
ESET Internet Security galima naudoti su ekrano skaityklėmis, kad silpnaregiai ESET naudotojai galėtų naršyti po produktą arba konfigūruoti nuostatas. Palaikomos šios ekrano skaityklės (JAWS, NVDA, Narrator).

Kad ekrano skaityklės programinė įranga galėtų pasiekti ESET Internet Security GUI tinkamai, vadovaukitės instrukcijomis Žinių bazės straipsnyje.

Pranešimai

Norėdami tvarkyti ESET Internet Security pranešimus, atidarykite Išplėstinis nustatymas > **Pranešimai**. Galite konfigūruoti šių tipų pranešimus:

- Programos būsenos – pranešimai, rodomi pagrindiniame programos lange > **Apžvalga**.
- Darbalaukio pranešimai – maži pranešimo langai šalia sistemos užduočių juostos.
- Interaktyvūs įspėjimai – įspėjimo langai ir pranešimų laukeliai, kuriuose reikalinga naudotojo sąveika.
- Peradresavimas (pranešimai el. paštu)– el. pašto pranešimai siunčiami nurodytu el. pašto adresu.



Programos būsenos

Programos būsenos – spustelėkite **Redaguoti**, kad pasirinktumėte, kurios programos būsenos bus rodomos pagrindinio programos lango > **Apžvalga** pagrindiniame puslapyje.

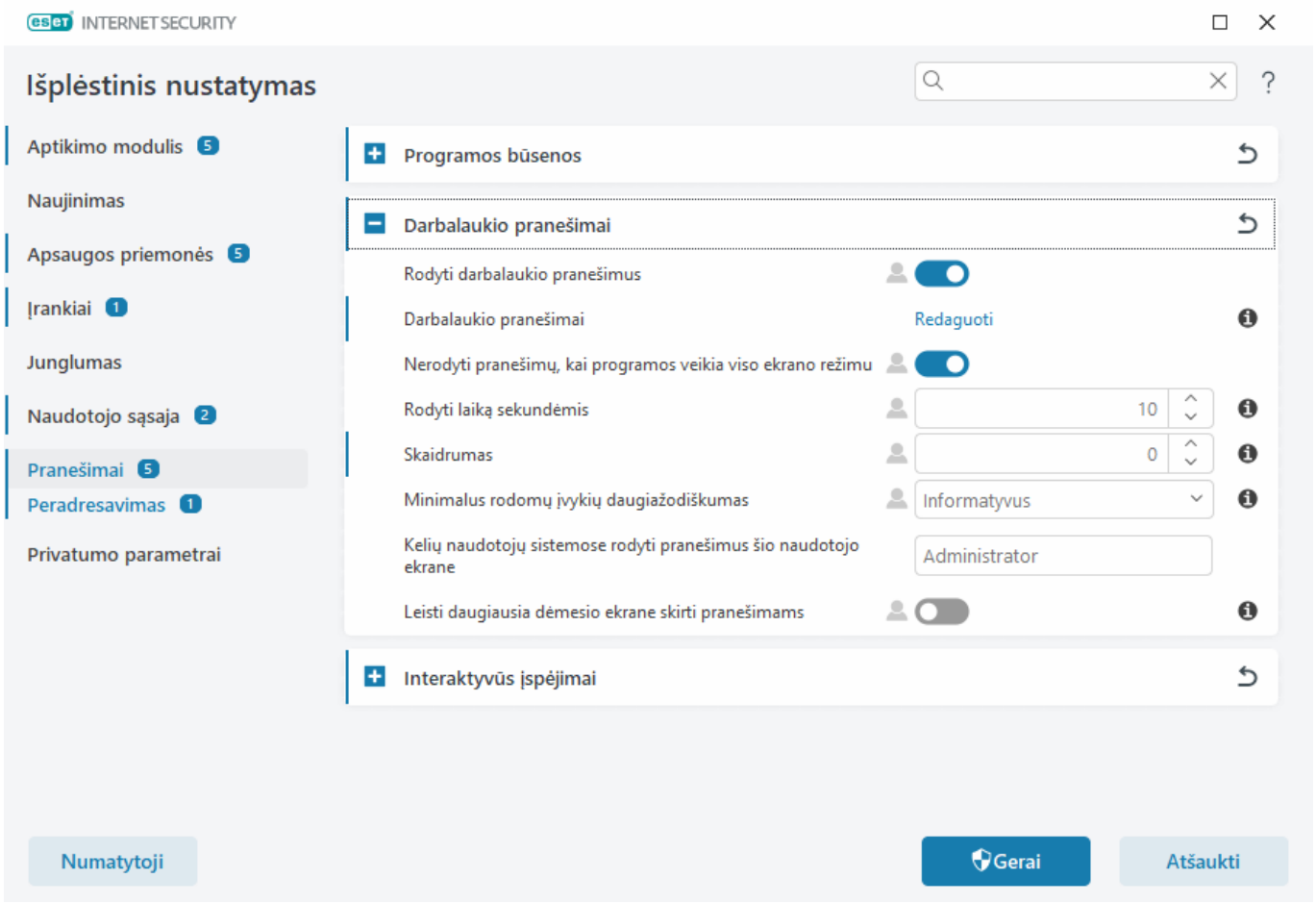
Dialogo langas – programos būsenos

Šiame dialogo lange galite pasirinkti, kurios programos būsenos bus rodomos. Pavyzdžiui, pristabdžius antivirusinę ir apsaugos nuo šnipinėjimo programą arba įjungus žaidėjo režimą.

Programos būsena bus rodoma ir tada, jei jūsų produktas nesuaktyvintas arba baigė galioti jūsų prenumerata.

Darbalaukio pranešimai

Darbalaukio pranešimai pateikiami nedideliame pranešimo lange šalia sistemos užduočių juostos. Pagal numatytuosius nustatymus jis rodomas 10 sekundžių, tada lėtai išnyksta. Pranešimais pranešama apie sėkmingus produktų atnaujinimus, naujus įrenginius, virusų nuskaitymo užduotis arba naują grėsmę.



Rodyti pranešimus darbalaukyje – rekomenduojame palikti šią parinktį, kad produktas galėtų informuoti jus apie naujus įvykius.

Darbalaukio pranešimai – spustelėkite **Redaguoti**, kad įjungtumėte arba išjungtumėte konkrečius Darbalaukio pranešimus.

Nerodyti pranešimų, kai programos veikia viso ekrano režimu – nerodyti visų neinteraktyvių pranešimų, kai programos veikia viso ekrano režimu.

Rodymo laikas sekundėmis – nustatoma pranešimo rodymo trukmė. Reikšmė turi būti nuo 3 iki 30 sekundžių.

Skaidrumas – nustatykite pranešimo skaidrumo procentą. Palaikomas intervalas yra nuo 0 (neskaidrus) iki 80 (labai skaidrus).

Minimalus rodomų įvykių daugiažodiškumas – nustatykite rodomą pradinį pranešimo svarbos lygį. Išplečiamajame meniu pasirinkite vieną iš šių parinkčių:

- **Diagnostika** – rodo informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.
- **Informacija** – rodo informacinius pranešimus, pvz., neįprastus tinklo įvykius, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – rodo įspėjamuosius pranešimus, klaidas ir kritines klaidas (pvz., „Atnaujinti nepavyko“).
- **Klaidos** – rodo klaidas (pvz., dokumentų apsauga nepradėta) ir kritines klaidas.

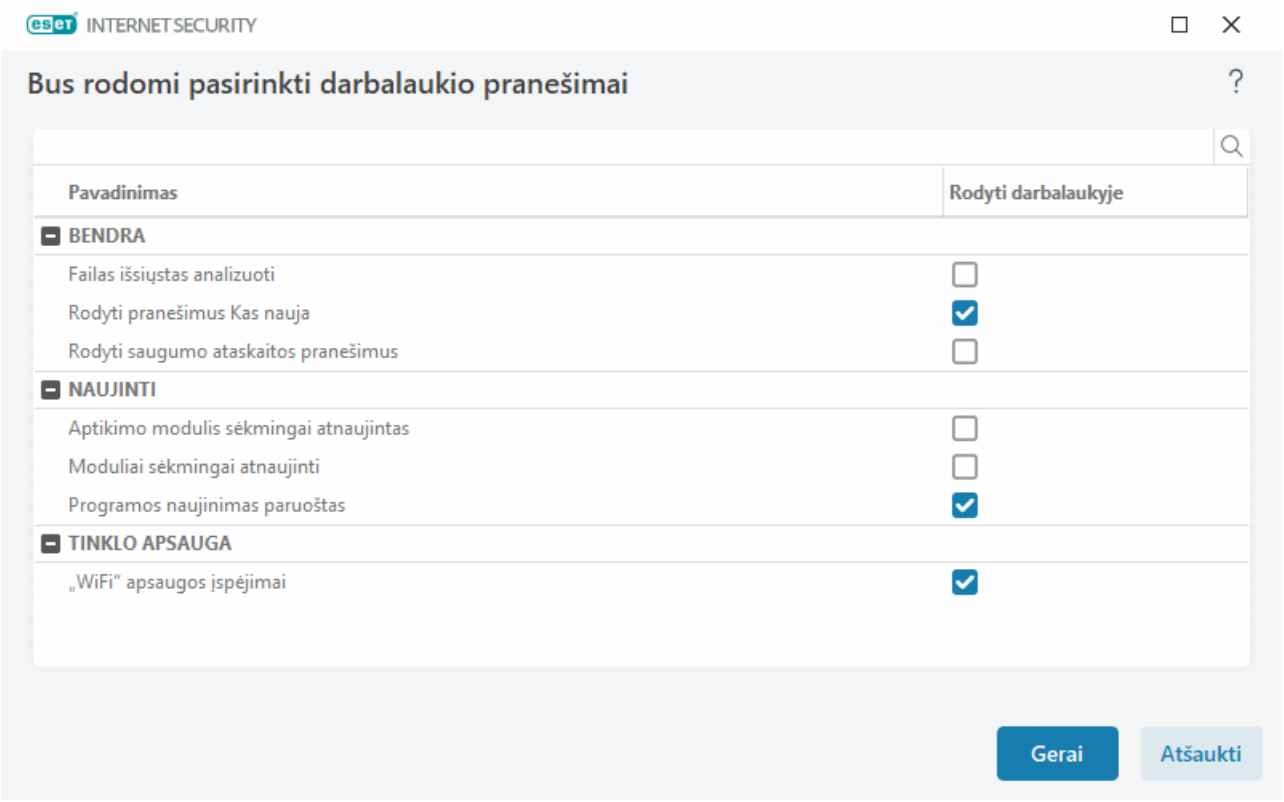
- **Kritiniai** – rodo tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų arba sistema užkrėsta ir t. t.).

Kelių naudotojų sistemose rodyti pranešimus šio naudotojo ekrane – leidžia pasirinktoms paskyroms gauti darbalaukio pranešimus. Pavyzdžiui, jei nenaudojate administratoriaus paskyros, įveskite visą paskyros pavadinimą ir bus rodomi nurodytos paskyros darbalaukio pranešimai. Darbalaukio pranešimus gali gauti tik viena naudotojo paskyra.

Leisti sutelkti dėmesį į pranešimus ekrane – leidžia sutelkti dėmesį į pranešimus ekraną ir juos pasiekti meniu **ALT + Tab**.

Darbalaukio pranešimų sąrašas

Norėdami pakoreguoti darbalaukio pranešimų matomumą (rodoma ekrano apatinėje dešinėje dalyje), atidarykite Išplėstinis nustatymas > **Pranešimai** > **Darbalaukio pranešimai**. Spustelėkite **Redaguoti** šalia **Darbalaukio pranešimai** ir pasirinkite atitinkamą žymės langelį **Rodyti**.



Bendra

Rodyti saugumo ataskaitos pranešimus – gaukite pranešimus, kai sugeneruojama nauja Saugumo ataskaita.

Rodyti pranešimus Kas nauja – pranešimai apie visas naujas ir patobulintas naujausios produkto versijos funkcijas.

Failas išsiųstas analizuoti – gaukite pranešimą kaskart, kai ESET Internet Security išsiunčia failą analizei.

Tinklo tikrinimo įrankis

Pranešti apie naujai aptiktus tinklo įrenginius – gaukite pranešimą, kai prie tinklo prijungiamas naujas įrenginys.

Tinklo apsauga

Tinklo profilis pakeistas – gaukite pranešimą, kai pakeičiamas tinklo profilis.

Wi-Fi apsaugos įspėjimai – gaukite pranešimą, kai bandote prisijungti prie Wi-Fi tinklo naudodami silpną slaptažodį arba jo neturėdami.

Naujinti

Ruošiamas programos naujinimas – gaukite pranešimą, kai bus paruoštas naujinys į naują ESET Internet Security versiją.

Aptikimo modulis sėkmingai atnaujintas – gaukite pranešimą, kai produktas atnaujina aptikimo modulius.

Moduliai sėkmingai atnaujinti – gaukite pranešimą, kai produktas atnaujina programos komponentus.

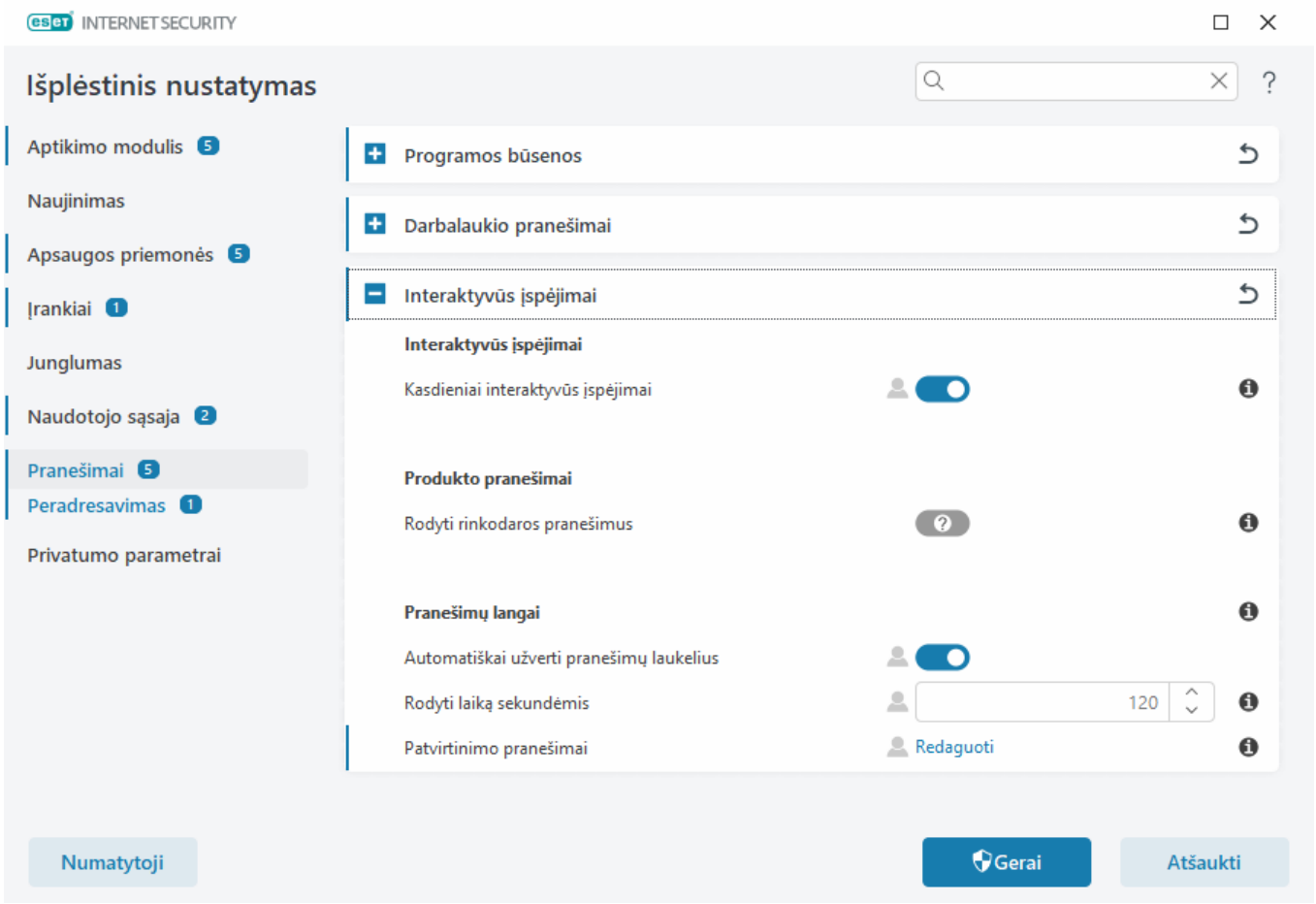
Norėdami nustatyti bendruosius nustatymus, skirtus darbalaukio pranešimams, pvz., kiek laiko bus rodomas pranešimas arba minimalus rodomų įvykių daugiažodiškumas, žr. Darbalaukio pranešimai dalyje Išplėstinis nustatymas > **Pranešimai**.

Interaktyvūs įspėjimai

Ieškote informacijos apie bendruosius perspėjimus ir pranešimus?

- Rasta grėsmė
- Adresas užblokuotas.
- Produktas nesuaktyvintas
- Keisti į produktą, kuriame pateikiama daugiau funkcijų
- Keisti į produktą, kuriame pateikiama mažiau funkcijų
- Prieinamas naujinimas
- Naujinimo informacija netinkama
- Pranešimo „Modulių naujinimas nepavyko“ trikčių šalinimas
- Modulių naujinimo klaidų sprendimas
- Užblokuota tinklo grėsmė
- Interneto svetainės sertifikatas atšauktas

Išplėstinės sąrankos > Pranešimai skyriuje **Interaktyvūs įspėjimai** galite konfigūruoti, kaip ESET Internet Security apdorojami pranešimų laukeliai ir interaktyvūs įspėjimai aptikimui, kai naudotojas (pvz., galima sukčiavimo apsimetant svetainė) turi priimti sprendimą.



Interaktyvūs įspėjimai

Išjungus parinktį **Rodyti interaktyvius perspėjimus**, bus slepiami visi perspėjimų ir naršyklės dialogų langai, ir tai tinka tik kai kurioms specifinėms situacijoms. Rekomenduojame palikti šią parinktį įjungtą.

Produkto pranešimai

Produkto pranešimai, teikiami tam, kad naudotojai gautų ESET naujienas bei kitą informaciją. Rinkodaros pranešimų siuntimui reikia vartotojo sutikimo. Todėl rinkodaros pranešimai pagal numatytuosius nustatymus vartotojui nesiunčiami (rodoma kaip klaustukas). Įjungdami šią parinktį, sutinkate gauti ESET rinkodaros pranešimus. Jei nesate suinteresuoti gauti ESET rinkodaros medžiagos, išjunkite parinktį **Rodyti rinkodaros pranešimus**.

Pranešimų langai

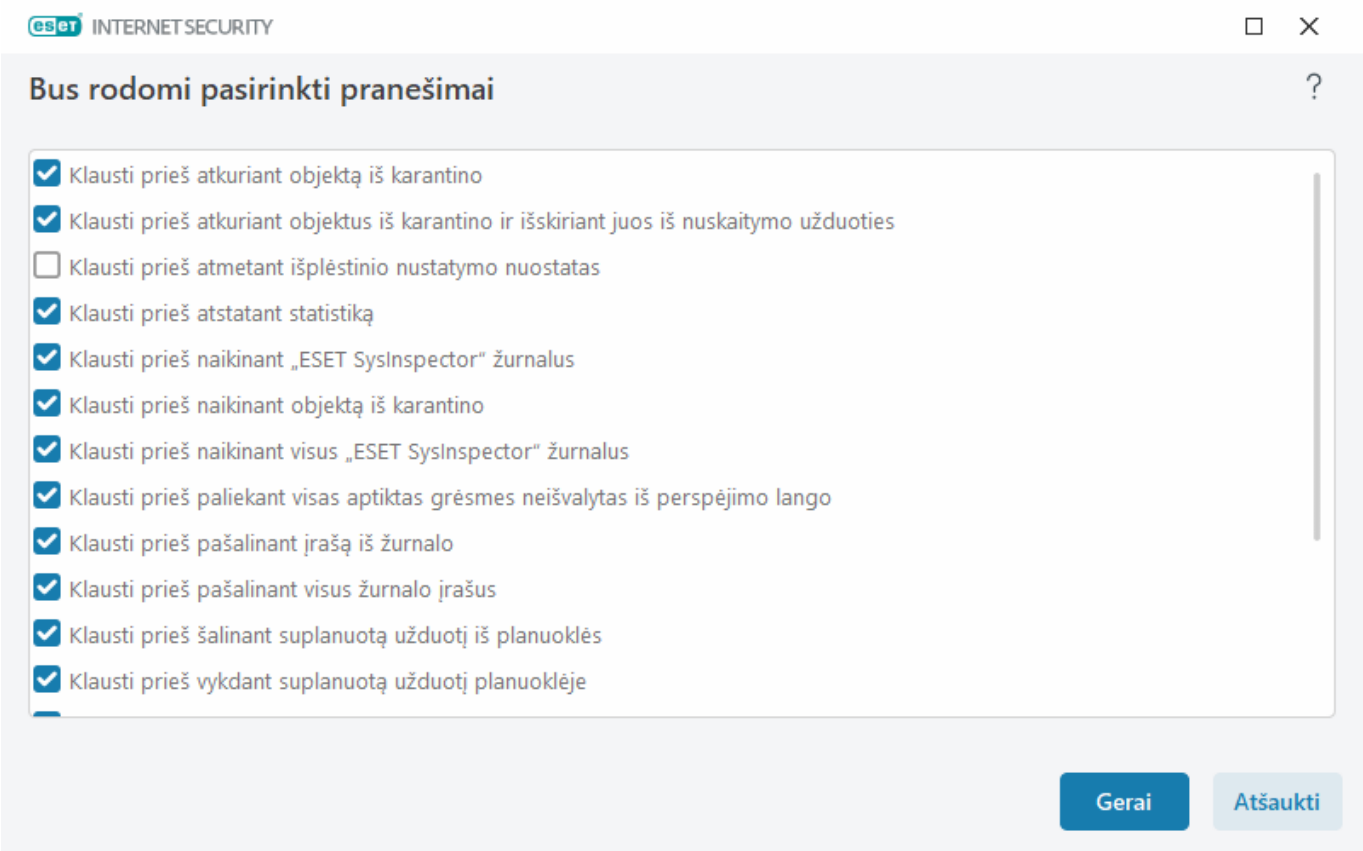
Norėdami po tam tikro laiko automatiškai uždaryti pranešimų langus, pasirinkite **Uždaryti pranešimų langus automatiškai**. Jeigu perspėjimo langai neuždaromi rankiniu būdu, jie bus automatiškai uždaryti pasibaigus nurodytam laikui.

Rodymo laikas sekundėmis – nustatoma įspėjimo rodymo trukmė. Reikšmė turi būti nuo 10 iki 999 sekundžių.

Patvirtinimo pranešimai – spustelėkite **Redaguoti**, kad būtų rodomas sąrašas su patvirtinimo pranešimais, kuriuos galima pasirinkti rodyti arba nerodyti.

Patvirtinimo pranešimai

Norėdami koreguoti patvirtinimo pranešimus, eikite į Išplėstinis nustatymas > **Pranešimai** > **Interaktyvūs įspėjimai** ir spustelėkite **Redaguoti** šalia **Patvirtinimo pranešimai**.



Šiame dialogo lange pateikiami patvirtinimo pranešimai, kuriuos ESET Internet Security rodys prieš atliekant bet kokį veiksmą. Pažymėkite laukelį šalia kiekvieno patvirtinimo pranešimo arba nuimkite žymas, kad juos įjungtumėte arba išjungtumėte.

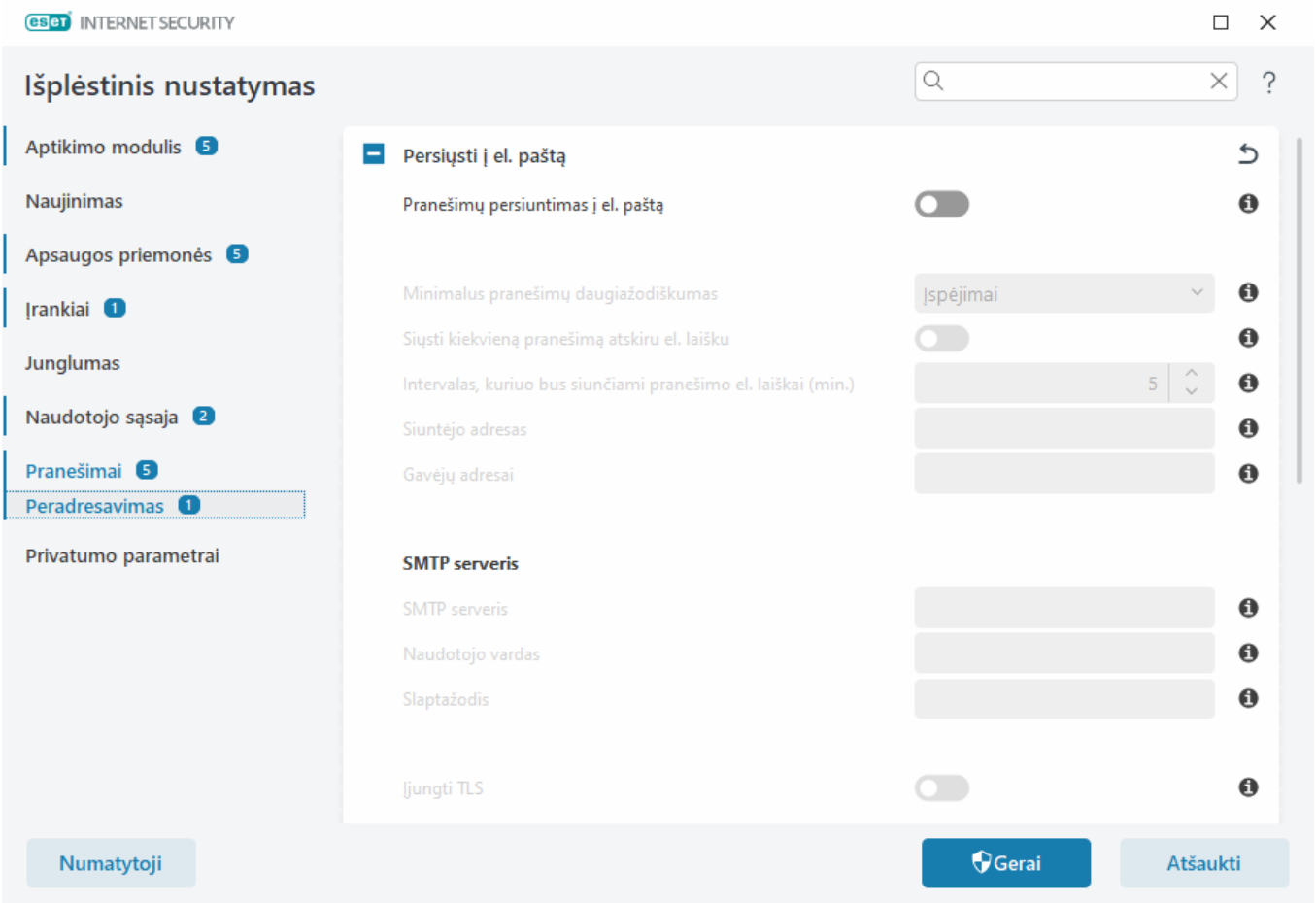
Sužinokite daugiau apie konkrečią funkciją, susijusią su patvirtinimo pranešimais:

- Klauskite prieš ištrindami ESET SysInspector žurnalus
- Klauskite prieš ištrindami visus ESET SysInspector žurnalus
- Klausti prieš naikinant objektą iš karantino
- Klausti prieš atmetant išplėstinio nustatymo nuostatas
- Klausti prieš paliekant visas aptiktas grėsmes neišvalytas iš perspėjimo lango
- Klausti prieš pašalinant įrašą iš žurnalo
- Klausti prieš šalinant suplanuotą užduotį iš planuoklės
- Klausti prieš pašalinant visus žurnalo įrašus
- Klausti prieš atstatant statistiką

- Klausti prieš atkuriant objektą iš karantino
- Klausti prieš atkuriant objektus iš karantino ir išskiriant juos iš nuskaitymo užduoties
- Klausti prieš vykdant suplanuotą užduotį planuoklėje
- Rodyti apsaugos nuo brukalo apdorojimo rezultatų pranešimus
- Rodyti apsaugos nuo brukalo apdorojimo rezultatų pranešimus el. pašto programose
- Rodyti el. pašto klientų „Outlook Express“ ir „Windows Mail“ produkto patvirtinimo dialogo langus
- Rodyti „Windows Live Mail“ produkto patvirtinimo dialogo langus
- Rodyti el. pašto kliento „Outlook“ produkto patvirtinimo dialogo langus

Peradresavimas

ESET Internet Security gali automatiškai siųsti pranešimų el. laiškus, jei įvyksta įvykis su pasirinktu daugiažodžio lygiu. Atidarykite Išplėstinis nustatymas > **Pranešimai** > **Persiuntimas** ir įgalinkite **Persiųsti pranešimus el. paštu**, kad suaktyvintumėte el. pašto pranešimus.



Išskleidžiamajame meniu **Minimalus pranešimų daugiažodiškumas** galite pasirinkti pradinį siunčiamų pranešimų griežtumo lygį.

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau

paminėtus įrašus.

- **Informacija** – įrašo informacinius pranešimus, pvz., neįprastus tinklo įvykius, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – įrašo kritines klaidas ir įspėjimo pranešimus (pavyzdžiui, „Atnaujinti nepavyko“).
- **Klaidos** – registruojamos klaidos (nepaleista dokumento apsauga) ir kritinės klaidos.
- **Kritinis** – registruoja tik kritines klaidas (pvz., klaida paleidžiant antivirusinę apsaugą arba aptikta grėsmė).

Siųsti kiekvieną pranešimą atskiru el. laišku – įjungus šią funkciją, gavėjas kiekvieną pranešimą gaus naujame el. laiške. Taip per trumpą laiką galima gauti daug el. laiškų.

Intervalas, kuriuo bus siunčiami pranešimai el. paštu (min.) – intervalas (minutėmis), po kurio nauji pranešimai bus siunčiami el. paštu. Jei šią reikšmę nustatysite kaip 0, pranešimai bus siunčiami iškart.

Siuntėjo adresas – nurodomas siuntėjo adresas, kuris bus rodomas pranešimų el. laiškų antraštėje.

Gavėjų adresai – nurodomi pranešimų el. laiškų antraštėje rodomi gavėjų adresai. Palaikomos kelios reikšmės. Kaip skyriklį naudokite kabliataškį.

SMTP serverį

SMTP serveris – SMTP serveris, naudojamas pranešimams siųsti (pavyzdžiui, smtp.provider.com:587, iš anksto nustatytas 25 prievadas).

ESET Internet Security nepalaiko SMTP serverių su TLS šifravimu.

Vartotojo vardas ir **slaptažodis** – jeigu SMTP serveriui reikalinga autentiškumo patvirtinimo procedūra, į šiuos laukus reikia įrašyti galiojantį vartotojo vardą ir slaptažodį, kad būtų galima prisijungti prie SMTP serverio.

Įjungti TLS – „Secure Alert“ ir pranešimai naudoja TLS šifravimą.

Testuoti SMTP jungtį – Gavėjo el. pašto adresu bus išsiųstas bandomasis el. laiškas. SMTP serverio, naudotojo vardo, slaptažodžio, siuntėjo adreso ir gavėjo adresų laukai turi būti užpildyti.

Pranešimo formatas

Ryšys tarp programos ir nuotolinio vartotojo arba sistemos administratoriaus yra palaikomas el. paštu arba LAN pranešimais (naudojant „Windows“ žinučių siuntimo paslaugą). **Naudoti numatytąjį pranešimo formatą** įspėjimo pranešimams ir perspėjimams bus optimalus daugeliu atvejų. Kai kuriomis aplinkybėmis gali prireikti pakeisti įvykių pranešimų formatą.

Įvykių pranešimų formatas – suformatuokite įvykių pranešimus, kurie rodomi nuotoliniuose kompiuteriuose.

Grėsmės įspėjimo pranešimų formatas – grėsmių perspėjimai ir pranešimai turi iš anksto apibrėžtą numatytąjį formatą. Rekomenduojame palikti iš anksto apibrėžtą formatą. Tačiau kai kuriomis aplinkybėmis (pvz., jeigu turite automatinę el. pašto apdorojimo sistemą) jums gali tekti pakeisti pranešimo formatą.

Simbolių rinkinys – el. laišką konvertuoja į ANSI simbolių šifravimą pagal „Windows“ regiono parametrus (pvz., windows-1250, Unicode (UTF-8), ACSII 7-bit arba Japonų (ISO-2022-JP)). Todėl "á" bus pakeista į "a", o nežinomas

simbolis į "?".

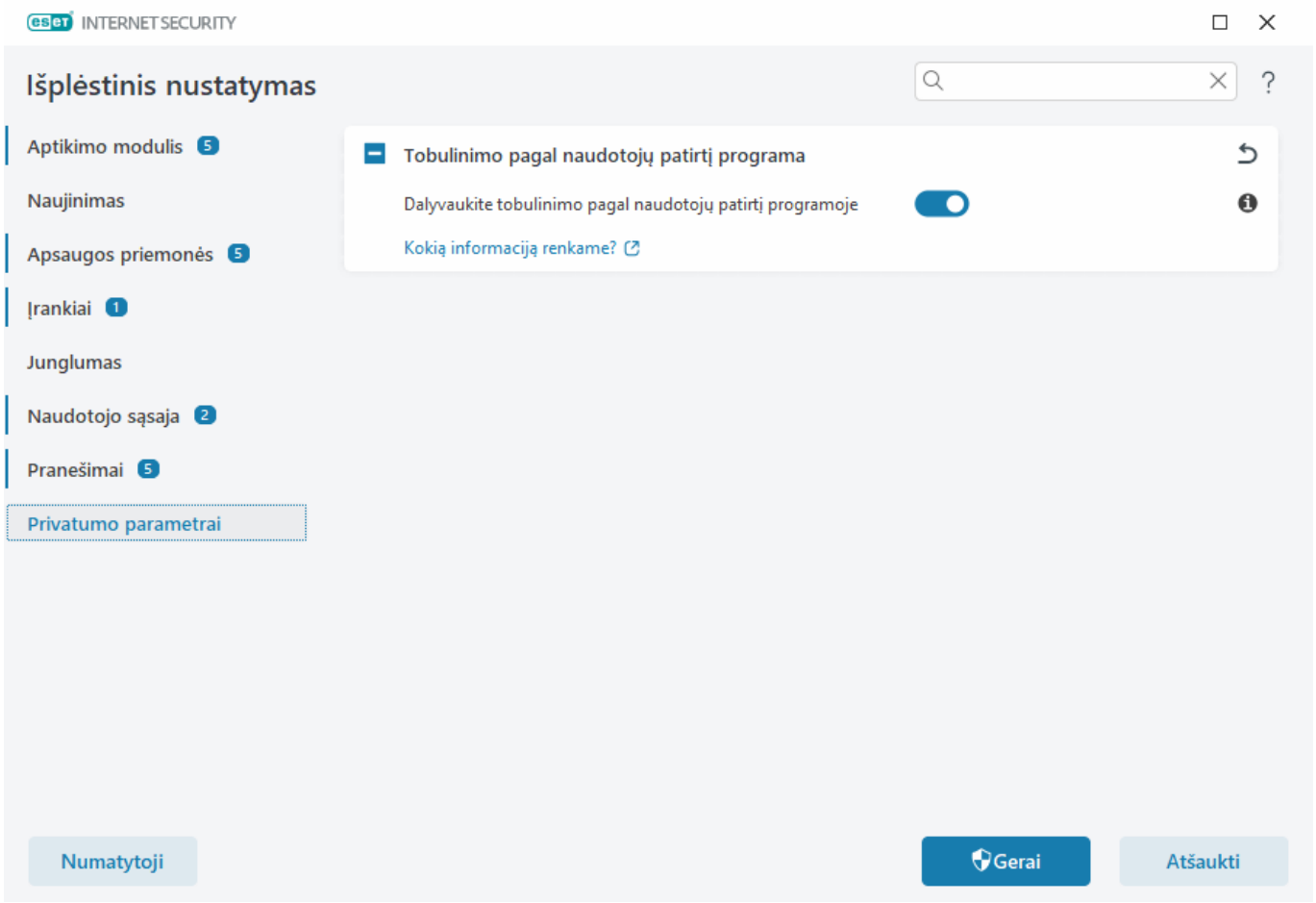
Naudoti spausdinamą šifravimą su kabutėmis – el. laiško šaltinis bus koduotas į „Quoted-printable“ (QP) formatą, kuris naudoja ASCII simbolius ir gali teisingai perduoti specialiuosius simbolius el. paštu 8 bitų formatu (áéíóú).

- **%TimeStamp%** – įvykio data ir laikas
- **%Scanner%** – susijęs modulis
- **%ComputerName%** – kompiuterio, iš kurio gautas įspėjimas, pavadinimas
- **%ProgramName%** – programa, sukūrusi įspėjimą
- **%InfectedObject%** – užkrėsto failo, pranešimo ir kt. pavadinimas
- **%VirusName%** – užkrato identifikavimas
- **%Action%** – veiksmas, kurio imtasi dėl įsiskverbimo
- **%ErrorDescription%** – nevirusinio įvykio aprašas

Raktažodžiai **%InfectedObject%** ir **%VirusName%** naudojami tik perspėjimų apie grėsmes pranešimuose, o **%ErrorDescription%** naudojamas tik įvykių pranešimuose.

Privatumo parametrai

Atidaryti Išplėstinis nustatymas > **Privatumo nustatymai**.



Tobulinimo pagal naudotojų patirtį programa

Įgalinkite perjungiklį šalia **Dalyvauti tobulinimo pagal naudotojų patirtį programoje**, kad prisijungtumėte prie tobulinimo pagal naudotojų patirtį programos. Prisijungę teikiate ESET anoniminę informaciją, susijusią su ESET produktų naudojimu. Surinkti duomenys padės mums pagerinti jūsų patirtį, jais niekada nebus dalijamasi su trečiosiomis šalimis. Kokią informaciją renkame?

Numatytųjų parametrų grąžinimas

Išplėstinėje sąrankoje spustelėkite Numatytieji, norėdami atkurti visų modulių visus programos nustatymus. Tai atstatys visų modulių programų parametrus į būseną, kuri būtų iš naujo įdiegus.

Taip pat žr. Parametrų importavimas ir eksportavimas.

Atkurti visus esamojo skyriaus parametrus

Spustelėkite lenktą rodyklę ⍰, norėdami grąžinti visus parametrus esamajame skyriuje ties ESET nustatytais numatytaisiais nustatymais.

Atminkite: spustelėjus **Atkurti numatytąsias**, bus prarasti visi padaryti pakeitimai.

Atkurti lentelių turinį – įjungus šią funkciją, bus prarastos visos rankiniu ar automatiniu būdu įtrauktos taisyklės, užduotys bei profiliai.

Taip pat žr. Parametrų importavimas ir eksportavimas.

Klaida išsaugant konfigūraciją

Šis klaidos pranešimas nurodo, kad parametrai nebuvo tinkamai įrašyti dėl klaidos.

Paprastai tai reiškia, kad programos parametrus bandęs keisti naudotojas:

- neturi pakankamai prieigos teisių arba neturi reikalingų operacinės sistemos privilegijų, reikalingų konfigūracijos failų ir sistemos registro keitimui.
  > Norint atlikti norimus pakeitimus, turi prisijungti sistemos administratorius.

- neseniai įjungė HIPS arba užkardos mokymosi režimą ir bandė pakeisti išplėstinius nustatymus.
  > Jei norite įrašyti konfigūraciją ir išvengti konfigūracijos konfliktų, uždarykite išplėstinius nustatymus neįrašę ir bandykite dar kartą atlikti norimus pakeitimus.

Kitas dažniausiai pasitaikantis atvejis gali būti, kad programa tinkamai nebeveikia, yra sugadinta, todėl turi būti įdiegta iš naujo.

Komandos eilutės skaitytuvas

ESET Internet Security antivirusinės programos modulis gali būti paleidžiamas komandos eilute – rankiniu būdu (komanda „ecls“) arba naudojant paketinį („bat“) failą.

ESET komandų eilutės skaitytuvo naudojimas:

```
ecls [OPTIONS..] FILES..
```

Šiuos parametrus ir jungiklius galima naudoti paleidžiant nuskaitymo programą pagal pareikalavimą iš komandos eilutės:

Parinktys

/base-dir=APLANKAS	įkelti modulius iš APLANKO
/quar-dir=APLANKAS	karantino APLANKAS
/exclude=KAUKĖ	nenuskaityti KAUKĘ atitinkančių failų
/subdir	nuskaityti poaplankius (numatyta)
/no-subdir	nenuskaityti poaplankių
/max-subdir-level=LYGIS	maksimalus nuskaitomų poaplankių lygis aplankuose
/symlink	sekti simbolinius saitus (numatyta)
/no-symlink	praleisti simbolinius saitus
/ads	nuskaityti ADS (numatyta)
/no-ads	nenuskaityti ADS
/log-file=FAILAS	registruoti išvestis į FAILĄ
/log-rewrite	perrašyti išvesties failą (numatyta – papildyti)
/log-console	registruoti išvestį pulte (numatyta)

/no-log-console	neregistruoti išvesties pulte
/log-all	registruoti ir švarius failus
/no-log-all	neregistruoti švarių failų (numatyta)
/aind	rodyti veiklos indikatorių
/auto	nuskaityti ir automatiškai valyti visus vietinius diskus

Nuskaitymo programos parinktys

/files	nuskaityti failus (numatyta)
/no-files	nenuskaityti failų
/memory	nuskaityti atmintį
/boots	nuskaityti paleidimo sektorius
/no-boots	nenuskaityti paleidimo sektorių (numatyta)
/arch	nuskaityti archyvus (numatyta)
/no-arch	nenuskaityti archyvų
/max-obj-size=DYDIS	nuskaityti tik failus, jei jie mažesni nei nurodytas DYDIS megabaitais (numatytoji reikšmė 0 = neribotas)
/max-arch-level=LYGIS	maksimalus nuskaitomas papildomas vidinių archyvų lygis (įdėtieji archyvai)
/scan-timeout=RIBA	nuskaityti archyvus ne ilgiau nei nurodyta RIBA sekundėmis
/max-arch-size=DYDIS	nuskaityti failus archyve, tik jeigu jie mažesni nei nurodytas DYDIS (numatyta, kad 0 = neribotas)
/max-sfx-size=DYDIS	nuskaityti tik išsiskleidžiančiajame archyve esančius failus, jeigu jie mažesni nei nurodytas DYDIS megabaitais (numatytoji reikšmė 0 = neribotas)
/mail	nuskaityti el. pašto failus (numatyta)
/no-mail	nenuskaityti el. pašto failų
/mailbox	nuskaityti pašto dėžutes (numatyta)
/no-mailbox	nenuskaityti pašto dėžučių
/sfx	nuskaityti išsiskleidžiančiuosius archyvus (numatyta)
/no-sfx	nenuskaityti išsiskleidžiančiųjų archyvų
/rtp	nuskaityti momentinio pakavimo programas (numatyta)
/no-rtp	nenuskaityti momentinio pakavimo programų
/unsafe	nuskaityti galimas nesaugias taikomąsias programas
/no-unsafe	nenuskaityti galimų nesaugių taikomųjų programų (numatyta)
/unwanted	nuskaityti galimas nepageidaujamas taikomąsias programas
/no-unwanted	nenuskaityti galimų nepageidaujamų taikomųjų programų (numatyta)
/suspicious	ieškoti įtartinų programų (numatytasis)
/no-suspicious	neieškoti įtartinų programų
/pattern	naudoti kodus (numatyta)
/no-pattern	nenaudoti kodų
/heur	įjungti euristiką (numatyta)
/no-heur	išjungti euristiką

/adv-heur	įjungti išplėstinę euristiką (numatyta)
/no-adv-heur	išjungti išplėstinę euristiką
/ext-exclude=PLĖTINIAI	neįtraukti dvitaškiu atskirtų failų PLĖTINIŲ
/clean-mode=REŽIMAS	naudoti valymo REŽIMĄ užkrėstiems objektams Galimos šios parinktys: • `nona` (numatytoji) – automatinis valymas nevykdomas. • `standard` – „ecls.exe“ pabandys automatiškai išvalyti arba panaikinti užkrėstus failus. • `Reiklus` – „ecls.exe“ pamėgins automatiškai išvalyti arba panaikinti užkrėstus failus be vartotojo įsikišimo (jūs nebūsite informuojami apie naikinamus failus). • `Griežtas` – „ecls.exe“ panaikins failus nebandydamas išvalyti jų, neatsižvelgiant į tai, kokie failai naikinami. • `Naikinti` – „ecls.exe“ panaikins failus nebandydamas jų išvalyti, tačiau svarbių failų (pvz., „Windows“ sisteminių failų) nepanaikins.
/quarantine	kopijuoti užkrėstus failus (jeigu išvalyti) į karantiną (papildo valant atliekamus veiksmus)
/no-quarantine	nekopijuoti užkrėstų failų į karantiną

Bendrosios parinktys

/help	rodyti žinyną ir baigti
/version	rodyti versijos informaciją ir baigti
/preserve-time	išsaugoti paskutinės prieigos laiko žymą

Išėjimo kodai

0	grėsmių nerasta
1	aptikta grėsmių ir jos išvalytos
10	kai kurių failų nepavyko nuskaityti (gali būti grėsmių)
50	rasta grėsmė
100	klaida

Didesni nei 100 išėjimo kodai reiškia, kad failas buvo nenuskaitytas, todėl gali būti užkrėstas.

DUK

Toliau pateikiami kai kurie dažniausiai užduodami klausimai ir problemos, su kuriomis susiduriama. Spustelėkite temos pavadinimą norėdami sužinoti, kaip spręsti problemą:

- Kaip naujinti ESET Internet Security
- ESET Internet Security aptiko grėsmę
- Kaip pašalinti virusą iš mano kompiuterio
- Kaip leisti ryšį tam tikroms taikomosioms programoms

- Kaip įjungti paskyros tėvų kontrolę
- Kaip sukurti naują užduotį planuoklėje
- Kaip planuoti nuskaitymo užduotį (kassavaitinę)
- Kaip atrakinti išplėstinį nustatymą
- Kaip išspręsti produkto išaktyvinimo problemą naudojant ESET HOME

Jeigu jūsų problemos nėra pirmiau pateikiamame sąraše, bandykite ieškoti ESET Internet Security internetiniame žinyne.

Jei negalite rasti savo problemos sprendimo ar atsakymo į klausimą ESET Internet Security internetiniame žinyne, apsilankykite reguliariai atnaujinamoje internetinėje ESET žinių bazėje. Nuorodos į populiariausius žinių bazės straipsnius pateikiami toliau:

- Kaip atnaujinti prenumeratą?
- Diegiant ESET gaminį įvyko aktyvinimo klaida. Ką tai reiškia?
- ESET „Windows“ namų produkto aktyvinimas naudojant aktyvinimo raktą
- Kaip pašalinti arba iš naujo įdiegti ESET namams skirtą produktą
- Gavau pranešimą, kad ESET diegimas pasibaigė pirma laiko
- Ką būtina padaryti atnaujinus prenumeratą? (Namų vartotojams)
- Ką daryti pakeitus el. pašto adresą?
- Kaip perkelti ESET produktą į naują kompiuterį arba įrenginį
- Kaip paleisti „Windows“ saugiuoju režimu arba saugiuoju režimu dirbant tinkle
- Neleisti blokuoti saugios interneto svetainės
- Leisti ESET GUI pasiekti ekrano skaitytuvų programinę įrangą

Prireikus galite susisiekti su techninės pagalbos tarnyba ir pateikti jai savo klausimus ar problemas.

Kaip naujinti ESET Internet Security

Naujinti ESET Internet Security galima rankiniu būdu arba automatiškai. Norėdami paleisti naujinimą, spustelėkite **Naujinti** pagrindiniame programos lange, tada spustelėkite **Ieškoti atnaujinimų**.

Pagal numatytuosius diegimo parametrus sukuriama automatinio naujinimo užduotis, kuri atliekama kas valandą. Jeigu jums reikia pakeisti intervalą, pereikite į **Įrankiai** > Planuoklė.

Kaip pašalinti virusą iš mano kompiuterio

Jei kompiuteryje pastebite užsikrėtimo kenkimo programa požymių, pvz., jis pradeda lėčiau veikti, dažnai užstringa, rekomenduojame atlikti šiuos veiksmus:

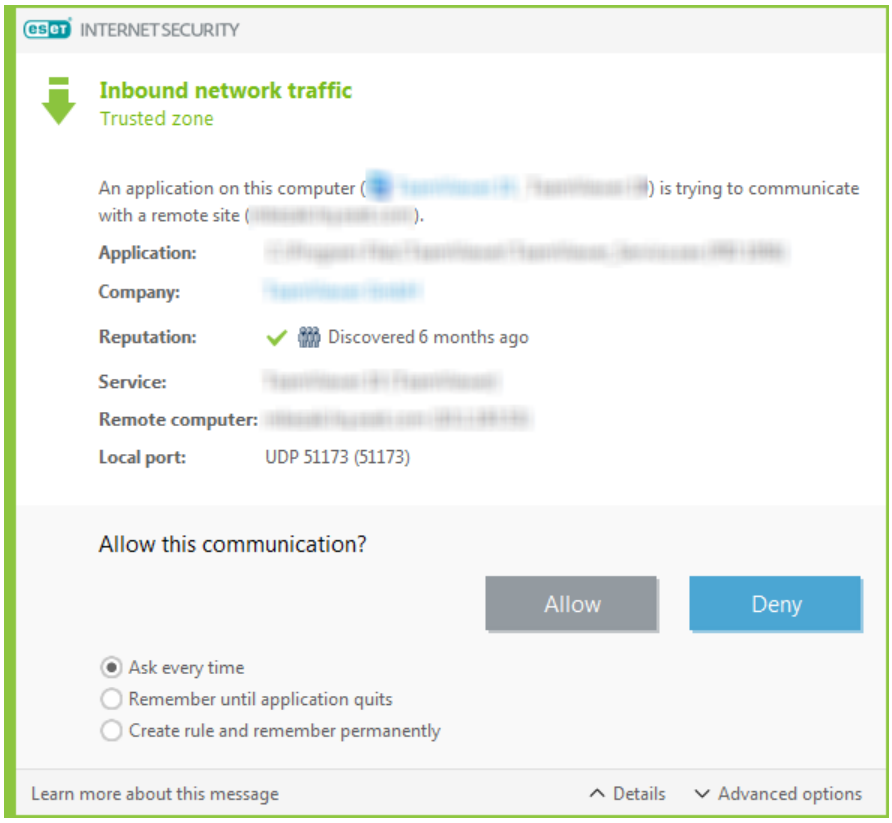
1. Pagrindiniame programos lange spustelėkite **Kompiuterio nuskaitymas**.
2. Spustelėkite **Nuskaityti jūsų kompiuterį**, kad prasidėtų jūsų sistemos nuskaitymas.
3. Kai nuskaitymas bus baigtas, peržiūrėkite žurnalą su nuskaitytų, užkrėstų ir išvalytų failų skaičiumi.
4. Jeigu norite nuskaityti tik pasirinktą disko dalį, spustelėkite **Pasirinktinis nuskaitymas** ir pasirinkite tikslus, kuriuos reikia nuskaityti ieškant virusų.

Dėl papildomos informacijos žr.:

- ESET žinių bazės straipsnį
- Karantinas

Kaip leisti ryšį tam tikroms taikomosioms programoms

Jeigu interaktyviuoju režimu aptinkamas naujas ryšys ir jeigu nėra atitinkamos taisyklės, jums bus pasiūlyta **leisti** arba **uždrausti** ryšį. Jeigu norite, kad ESET Internet Security atliktų tą patį veiksmą kiekvieną kartą, kai taikomoji programa bando užmegzti ryšį, pasirinkite žymės langelį **Kurti taisyklę ir įsiminti visam laikui**.



Galite sukurti naujas užkardos taisykles programoms prieš tai, kol jas aptiks „ESET Internet Security“, užkardos nustatymo skiltyje. Atidarykite pagrindinį programos langą > **Saranka** > **Tinklo apsauga** > spustelėkite šalia

parinkties **Užkarda** > **Konfigūruoti** > **Išplėstiniai** > **Taisyklės** > **Redaguoti**.

Spustelėkite mygtuką **Pridėti** ir skirtuke **Bendra** įveskite taisyklės pavadinimą, kryptį ir ryšio protokolą. Šiame lange galite nustatyti veiksmą, kuris bus atliktas pritaikius taisyklę.

Įveskite kelią į programos vykdomąjį failą ir vietinį ryšio prievadą skirtuke **Vietinis**. Eikite į skirtuką **Nuotolinis** ir įveskite nuotolinį adresą ir prievadą (jeigu naudojama). Naujai sukurta taisyklė bus taikoma, kai tik taikomoji programa bandys dar kartą užmegzti ryšį.

Kaip įjungti paskyros tėvų kontrolę

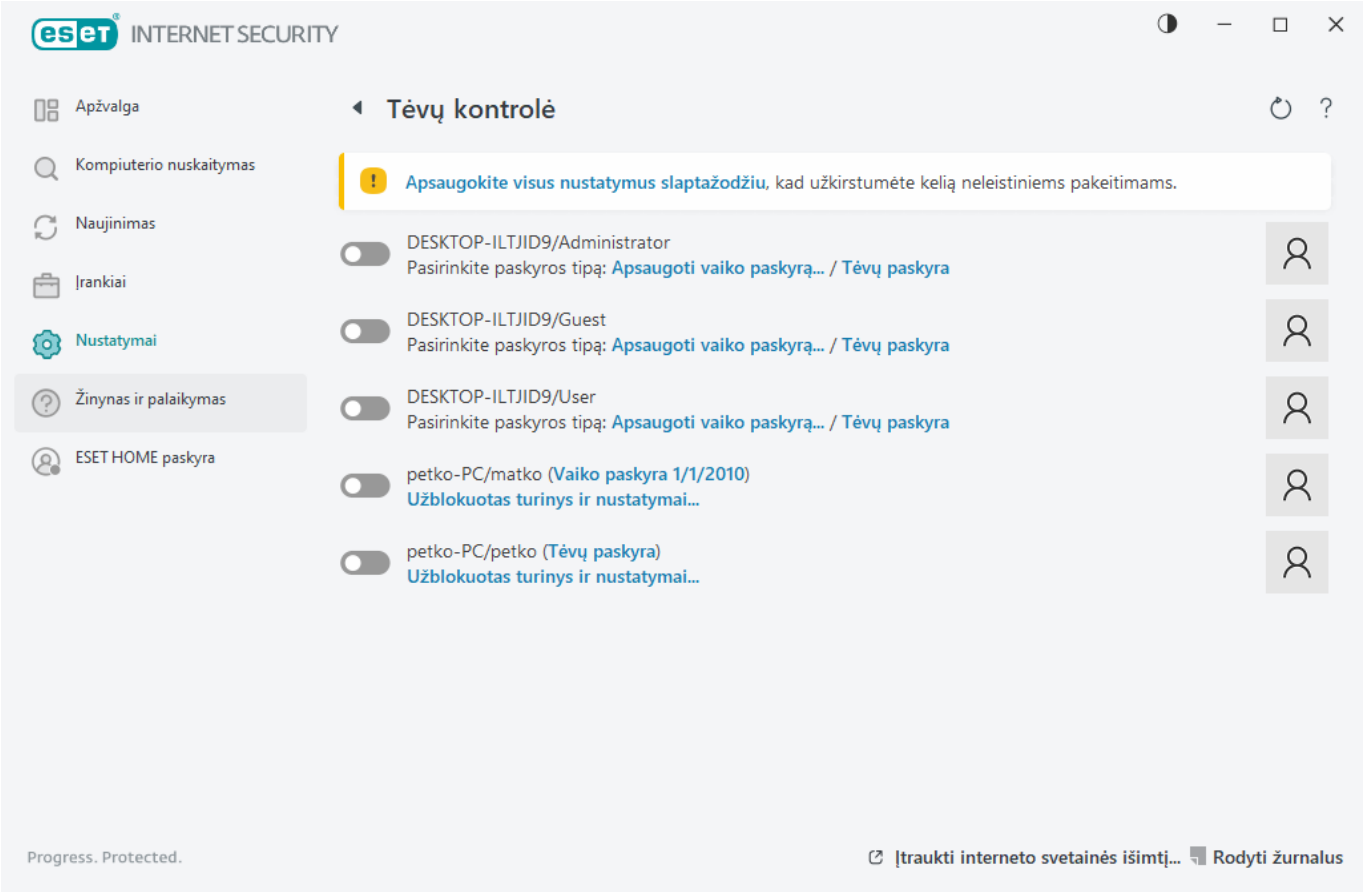
Norėdami aktyvinti konkrečios vartotojo paskyros tėvų kontrolę, atlikite žemiau pateiktus veiksmus:

1. Pagal numatytuosius nustatymus ESET Internet Security tėvų kontrolė yra išjungta. Yra du tėvų kontrolės aktyvinimo būdai:

   • Pagrindiniame programos lange spustelėkite perjungimo piktogramą, esančią **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė** ir pakeiskite tėvų kontrolės būseną į „Įjungta“.

   • Atidarykite Išplėstinis nustatymas > **Apsaugos priemonės** > **Prieigos prie saityno apsauga** > **Tėvų kontrolė** ir įjunkite perjungiklį šalia parinkties **Įgalinti tėvų kontrolę**.

2. Pagrindiniame programos lange spustelėkite **Nustatymai** > **Interneto apsauga** > **Tėvų kontrolė**. Nors prie funkcijos **Tėvų kontrolė** rodomas užrašas **Įjungta**, spustelėdami rodyklės simbolį ir kitame lange pasirinkdami **Apsaugoti vaiko paskyrą** arba **Tėvų paskyra** turite sukonfigūruoti tėvų kontrolę reikiamai paskyrai. Kitame lange pasirinkite gimimo datą, pagal kurią nustatomas prieigos lygis ir rekomenduojami pagal amžių tinkami tinklalapiai. Tada nurodytoje naudotojo paskyroje įjungiama tėvų kontrolė. Spustelėkite **Blokuojamas turinys ir nustatymai** po paskyros pavadinimu, kad galėtumėte tinkinti kategorijas, kurias norite leisti arba blokuoti skirtuke Kategorijos. Norėdami leisti arba blokuoti pasirinktinius tinklalapius, kurie neatitinka kategorijos, spustelėkite skirtuką Išimtys.



Kaip sukurti naują užduotį planuoklėje

Norėdami sukurti naują užduotį, skyriuje **Įrankiai** > **Planuoklė** spustelėkite **Pridėti užduotį** arba spustelėkite dešiniuoju pelės klavišu ir iš kontekstinio meniu pasirinkite **Pridėti**. Yra penki planinių užduočių tipai:

- **Vykdyti išorinę taikomąją programą** – leidžia planuoti išorinės taikomosios programos vykdymą.
- **Žurnalo priežiūra** – žurnalo failuose taip pat gali būti panaikintų įrašų likučių. Ši užduotis reguliariai optimizuoja įrašus žurnalo failuose, kad darbas būtų efektyvus.
- **Sistemos paleidimo failo patikra** – tikrina failus, kurie leidžiami vykdyti paleidžiant sistemą arba registruojantis.
- **Sukurti kompiuterio būsenos momentinę kopiją** – sukuria ESET SysInspector kompiuterio momentinę kopiją – surenka išsamią informaciją apie sistemos dalis (pvz., tvarkykles, programas) ir įvertina kiekvienos dalies rizikos lygį.
- **Kompiuterio nuskaitymas pareikalavus** – atlieka kompiuterio failų ir katalogų nuskaitymą.
- **Naujinti** – atnaujinant modulius suplanuojama naujinimo užduotis.

Kadangi **Naujinimas** yra viena iš dažniausiai naudojamų planinių užduočių, toliau paaiškinsime, kaip pridėti naują naujinimo užduotį:

Išskleidžiamajame meniu **Planuota užduotis** pasirinkite **Naujinimas**. Į lauką **Užduoties pavadinimas** įveskite užduoties pavadinimą ir spustelėkite **Toliau**. Pasirinkite užduoties vykdymo dažnumą. Galimos šios parinktys: **Vieną kartą**, **Pakartotinai**, **Kasdien**, **Kas savaitę** ir **Įvykus įvykiui**. Nurodykite **Praleisti užduotį, kai naudojama**

akumuliatoriaus energija, kad maksimaliai apribotumėte energijos sąnaudas, kai nešiojamasis kompiuteris veikia maitinamas akumuliatoriaus. Užduotis bus vykdoma laukuose **Užduoties vykdymas** nurodytą datą ir laiku. Po to apibrėžkite, kokį veiksmą vykdyti, jei užduoties negalima atlikti arba užbaigti suplanuotu laiku. Galimos šios parinktys:

- **Kitu suplanuotu laiku**
- **Kaip įmanoma greičiau**
- **Iškart, jei nuo paskutinio vykdymo praėjo daugiau laiko nei nurodyta reikšmė** (intervalą galima nustatyti naudojantis slinkimo laukeliu **Laikas nuo paskutinio vykdymo (valandomis)**)

Kitame žingsnyje parodomas suvestinės langas su informacija apie suplanuotąją užduotį. Atlikę pakeitimus spustelėkite **Baigti**.

Pasirodys dialogo langas, suteikiantis galimybę pasirinkti profilius, kurie bus naudojami suplanuotai užduočiai. Čia galima nustatyti pirminį ir alternatyvųjį profilį. Alternatyvusis profilis naudojamas tuo atveju, jei užduoties nepavyksta užbaigti naudojant pirminį profilį. Patvirtinkite paspausdami **Baigti**. Nauja suplanuota užduotis bus įtraukta į esamų suplanuotų užduočių sąrašą.

Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą

Norėdami planuoti reguliarią užduotį, atidarykite pagrindinį programos langą ir spustelėkite **Įrankiai** > **Planuoklė**. Žemiau rasite trumpus nurodymus, kaip suplanuoti užduotį, kuri nuskaitys jūsų vietinius diskų įrenginius kas savaitę. Jei reikia daugiau nurodymų, skaitykitežinių bazės straipsnį.

Norėdami suplanuoti nuskaitymo užduotį:

1. Spustelėkite **Pridėti** pagrindiniame planuoklės lange.
2. Įveskite užduoties pavadinimą ir išplečiamajame meniu **Užduoties tipas** pasirinkite **Kompiuterio nuskaitymas pareikalavus**.
3. Kaip užduoties dažnumą pasirinkite **Kas savaitę**.
4. Nustatykite dieną ir laiką, kada užduotis bus vykdoma.
5. Pasirinkite **Vykdyti užduotį, kai tik bus įmanoma**, kad užduotis būtų įvykdyta vėliau, jei dėl kokios nors priežasties suplanuota užduotis nepradedama vykdyti pagal planą (pvz., išjungtas kompiuteris).
6. Peržiūrėkite suplanuotos užduoties suvestinę ir spustelėkite **Baigti**.
7. Išskleidžiamajame meniu **Tikslai** pasirinkite **Vietiniai įrenginiai**.
8. Spustelėkite **Baigti**, kad priskirtumėte užduotį.

Kaip atrakinti slaptažodžiu apsaugotą išplėstinį

nustatymą

Norint pasiekti apsaugotą išplėstinį nustatymą, rodomas langas, skirtas įvesti slaptažodį. Jei pamiršote slaptažodį arba jo netekote, spustelėkite **Atkurti slaptažodį** ir įveskite el. pašto adresą, kurį naudojote registruodami prenumeratą. ESET jums atsiųs el. laišką su patvirtinimo kodu. Įveskite patvirtinimo kodą ir patvirtinkite naują slaptažodį. Patvirtinimo kodas galioja septynias dienas.

Slaptažodžio atkūrimas naudojant ESET HOME paskyrą – naudokite šią parinktį, jei aktyvinimui naudojama prenumerata susieta su jūsų ESET HOME paskyra. Įveskite el. pašto adresą, kurį naudojate prisijungdami prie ESET HOME paskyros.

Jei neprisimenate savo el. pašto adreso arba kyla sunkumų atkuriant slaptažodį, spustelėkite **Kreiptis į techninės pagalbos tarnybą**. Būsite nukreipti į ESET svetainę, kad susisiektumėte su mūsų techninės pagalbos tarnyba.

Generuoti kodą techninės pagalbos tarnybai. Ši funkcija sugeneruoja kodą, kuris pateikiamas techninės pagalbos tarnybai. Nukopijuokite techninės pagalbos tarnybos pateiktą kodą ir paspauskite **Aš turiu patvirtinimo kodą**. Įveskite patvirtinimo kodą ir patvirtinkite naują slaptažodį. Patvirtinimo kodas galioja septynias dienas.

Daugiau informacijos ieškokite Nustatymų slaptažodžio atrakinimas ESET „Windows“ namų produktuose.

Kaip išspręsti produkto išaktyvinimo problemą naudojant ESET HOME

Produktas nesuaktyvintas

Šis klaidos pranešimas rodomas, kai prenumeratos savininkas išaktyvina jūsų ESET Internet Security ESET HOME portale arba su jūsų ESET HOME paskyra bendrinama prenumerata nebebendrinama. Norėdami išspręsti šią problemą:

- Spustelėkite **Aktyvinti** ir naudokite vieną iš aktyvinimo būdų, kad aktyvintumėte ESET Internet Security.
- Susisiekite su prenumeratos savininku nurodydami, kad prenumeratos savininkas išaktyvino ESET Internet Security arba prenumerata su jumis nebebendrinama. Savininkas gali išspręsti problemą ESET HOME.

Produktas išjungtas, įrenginys atjungtas

Šis klaidos pranešimas rodomas pašalinus įrenginį iš ESET HOME valdymo portalo. Norėdami išspręsti šią problemą:

- Spustelėkite **Aktyvinti** ir naudokite vieną iš aktyvinimo būdų, kad aktyvintumėte ESET Internet Security.
- Kreipkitės į prenumeratos savininką nurodydami, kad jūsų „ESET Internet Security“ buvo išaktyvinta ir įrenginys buvo atjungtas nuo ESET HOME.
- Jei esate prenumeratos savininkas ir nežinote apie šiuos pakeitimus, peržiūrėkite ESET HOME veiklos srautą. Jei pastebėjote įtartiną veiklą, pakeiskite savo ESET HOME paskyros slaptažodį ir kreipkitės į ESET techninę pagalbą.

Produktas išjungtas, įrenginys atjungtas

Šis klaidos pranešimas rodomas pašalinus įrenginį iš ESET HOME valdymo portalo. Norėdami išspręsti šią problemą:

- Spustelėkite **Aktyvinti** ir naudokite vieną iš aktyvinimo būdų, kad aktyvintumėte ESET Internet Security.
- Kreipkitės į prenumeratos savininką nurodydami, kad jūsų „ESET Internet Security“ buvo išaktyvinta ir įrenginys buvo atjungtas nuo ESET HOME.
- Jei esate prenumeratos savininkas ir nežinote apie šiuos pakeitimus, peržiūrėkite ESET HOME veiklos srautą. Jei pastebėjote įtartiną veiklą, pakeiskite savo ESET HOME paskyros slaptažodį ir kreipkitės į ESET techninę pagalbą.

Produktas nesuaktyvintas

Šis klaidos pranešimas rodomas, kai prenumeratos savininkas išaktyvina jūsų ESET Internet Security ESET HOME portale arba su jūsų ESET HOME paskyra bendrinama prenumerata nebebendrinama. Norėdami išspręsti šią problemą:

- Spustelėkite **Aktyvinti** ir naudokite vieną iš aktyvinimo būdų, kad aktyvintumėte ESET Internet Security.
- Susisiekite su prenumeratos savininku nurodydami, kad prenumeratos savininkas išaktyvino ESET Internet Security arba prenumerata su jumis nebebendrinama. Savininkas gali išspręsti problemą ESET HOME.

0

Tobulinimo pagal naudotojų patirtį programa

Prisijungę prie tobulinimo pagal naudotojų patirtį programos pateikiate ESET anoniminę informaciją, susijusią su produktų naudojimu. Daugiau informacijos apie duomenų apdorojimą ieškokite mūsų privatumo politikoje.

Jūsų sutikimas

Dalyvavimas programoje yra savarankiškas ir jam būtinas jūsų sutikimas. Prisijungus dalyvavimas yra pasyvus, todėl jums nereikia imtis jokių tolimesnių veiksmų. Galite bet kada atsiimti sutikimą, pakeisdami produkto nustatymus. Taip uždrausite mums toliau apdoroti jūsų anoniminius duomenis.

Savo sutikimą galite atšaukti bet kuriuo metu pakeitę produkto nustatymus:

- Pakeiskite tobulinimo pagal naudotojų patirtį programos nustatymus ESET „Windows“ namų produktams

Kokio pobūdžio informaciją renkame?

Sąveikos su produktu duomenys

Šie duomenys leidžia sužinoti daugiau apie tai, kaip mūsų produktai naudojami. Pasinaudodami šiais duomenimis žinome, kokios funkcijos, pavyzdžiui, dažnai naudojamos, kokius nustatymus vartotojai modifikuoja arba kiek laiko

praleidžia naudodamiesi produktu.

Įrenginių duomenys

Šią informaciją renkame tam, kad žinotume, kur ir kokiuose įrenginiuose mūsų produktai naudojami. Paprastai renkame informaciją apie įrenginio modelį, šalį, versiją ir operacinės sistemos pavadinimą.

Klaidų diagnostikos duomenys

Taip pat renkame informaciją apie klaidas ir atvejus, kai įvyksta gedimai. Pavyzdžiui, kokia įvyko klaida ir kokie veiksmai lėmė jos atsiradimą.

Kodėl renkame šią informaciją?

Remdamiesi anonimine informacija galime tobulinti produktus, kuriais naudojatės jūs – mūsų vartotojai. Tokiu būdu produktuose galime pritaikyti naujausias technologijas, padaryti produktus kuo įmanoma lengviau naudojamus ir pasižyminčius kuo sklandesniu veikimu.

Kas valdo šią informaciją?

„ESET, spol. s r.o.“ yra vienintelis programos metu surinktų duomenų valdytojas. Ši informacija su trečiosiomis šalimis nebendrinama.

Galutinio vartotojo licencijos sutartis

Galioja nuo 2021 m. spalio 19 d.

SVARBU. prieš atsisiųsdami, diegdami, kopijuodami ar naudodami šį produktą, atidžiai perskaitykite produkto taikymo sąlygas. **ATSISIŲSDAMI, DIEGDAMI, KOPIJUODAMI AR NAUDODAMI ŠIĄ PROGRAMINĘ ĮRANGĄ JŪS IŠREIŠKIATE SAVO SUTIKIMĄ SU ŠIOMIS SĄLYGOMIS IR PRIPAŽĮSTATE PRIVATUMO POLITIKA.**

Galutinio vartotojo licencijos sutartį

Pagal šią Galutinio naudotojo licencijos sutartį (toliau – Sutartis), sudarytą tarp „ESET, spol. s r. o.“, kurios buveinė yra registruota adresu Einsteinova 24, 85101 Bratislava, Slovak Republic, ir kuri yra įtraukta į Bratislavos I apygardos teismo administruojamą Įmonių registrą (skyrius SRO, įrašo Nr. 3586/B), registracijos Nr. 31333532, (toliau – ESET arba Teikėjas) ir jūsų, fizinio ar juridinio asmens (toliau – Jūs ar Galutinis naudotojas), turite teisę naudotis Programine įranga, nurodyta Sutarties 1 straipsnyje. Sutarties 1 straipsnyje nurodyta Programinė įranga gali būti saugoma duomenų laikmenoje, siunčiama el. paštu, atsisiunčiama iš interneto, atsisiunčiama iš Teikėjo serverių ar įsigyjama iš kitų šaltinių, kaip tai apibrėžta toliau nurodytomis sąlygomis.

TAI GALUTINIO VARTOTOJO, O NE PARDAVIMO SUTARTIS. Programinės įrangos kopija ir fizinė laikmena iš įsigyto paketo, taip pat visos kitos kopijos, kurias Galutiniam vartotojui yra leista pasigaminti pagal Sutartį, toliau lieka pas Tiekėją.

Diegdami, kopijuodami ar naudodami Programinę įrangą spustelėję „Sutinku“, patvirtinsite, kad sutinkate su Sutarties sąlygomis ir Privatumo politika. Jei yra Sutarties ir (arba) Privatumo politikos sąlygų, su kuriomis Jūs nesutinkate, nedelsdami spustelėkite parinktį „Nesutinku“, atšaukite diegimą ar siuntimą arba Programinę įrangą, diegimo laikmeną, susijusius dokumentus ir pirkimo kvitą sunaikinkite arba grąžinkite ESET ar prekybos įmonei, iš kurios įsigijote Programinę įrangą.

JŪS SUTINKATE, KAD NAUDODAMI PROGRAMINĘ ĮRANGĄ PRIPAŽĮSTATE, KAD PERSKAITĖTE ŠIĄ SUTARTĮ, SU JA SUSIPAŽINOTE IR SUTINKATE VYKDYTI JOJE IŠDĖSTYTAS SĄLYGAS.

1. **Programinė įranga**. Šioje Sutartyje vartojama sąvoka „Programinė įranga“ reiškia: (i) pagal šią Sutartį tiekiama kompiuterio programa ir visi jos komponentai; (ii) visą diskų, CD-ROM, DVD diskų, el. laiškų ir kitų priedų turinį ar kitą laikmeną, su kuria gavote šią Sutartį, įskaitant Programinės įrangos objektinį kodą, gautą duomenų laikmenoje, el. paštu ar atsisiunčiant internetu; (iii) visą susijusią aiškinamąją rašytinę medžiagą ir visą kitą galimą dokumentaciją, susijusią su Programine įranga, bei visus Programinės įrangos aprašymus, techninius duomenis, Programinės įrangos ypatybių ar veikimo aprašymus, visus veikimo aplinkos, kurioje Programinė įranga yra naudojama, aprašymus, Programinės įrangos naudojimo ar diegimo instrukcijas arba visus Programinės įrangos naudojimo būdo aprašymus („Dokumentacija“); (iv) Programinės įrangos kopijas, galimų Programinės įrangos klaidų pataisas, Programinės įrangos priedus, Programinės įrangos plėtinius, modifikuotas Programinės įrangos versijas ir Programinės įrangos komponentų naujinius (jei tokių yra), kuriais naudotis jums teisę suteikia Teikėjas pagal šios Sutarties 3 straipsnį. Programinė įranga bus pateikiama išskirtinai tik vykdomo objektinio kodo forma.

2. **Diegimas, kompiuteris ir licencijos raktas**. Programinę įrangą, gautą duomenų laikmenoje, atsiųstą el. paštu, atsisiųstą internetu, atsisiųstą iš Teikėjo serverių ar gautą iš kito šaltinio, reikia įdiegti. Programinę įrangą turite įdiegti tinkamai sukonfigūruotame kompiuteryje, kuris atitinka dokumentacijoje nurodytus reikalavimus. Diegimo būdas aprašomas Dokumentacijoje. Kompiuteryje, kuriame ketinate diegti Programinę įrangą, negali būti įdiegta kompiuterių programų ar aparatinės įrangos, kuri galėtų neigiamai paveikti Programinę įrangą. Kompiuteris apima aparatinę įrangą, įskaitant (bet neapsiribojant) asmeninius kompiuterius, nešiojamuosius kompiuterius, kompiuterizuotas darbo vietas, delninius kompiuterius, išmaniuosius telefonus, delninukus ir kitus elektroninius įrenginius, kuriems programinė įranga kuriama, kuriuose ji diegiama arba naudojama. Licencijos raktas yra unikali simbolių, raidžių arba specialiųjų ženklų seka, suteikta Galutiniam naudotojui, kad šis galėtų teisėtai naudotis Programine įranga, jos konkrečia versija arba pratęsti Licencijos laikotarpį pagal Sutarties sąlygas.

3. **Licencija**. Jei sutikote su šios Sutarties sąlygomis ir laikotės visų čia nustatytų sąlygų, Teikėjas suteikia Jums šias teises („Licenciją“):

a) **Diegimas ir naudojimas.** Jums suteikiama neišskirtinė, neperduodama teisė įdiegti Programinę įrangą kompiuterio standžiajame diske ar kitoje nuolatinėje laikmenoje, skirtoje Programinės įrangos duomenims saugoti, jai diegti ir saugoti kompiuterinės sistemos atmintyje, ir Programinę įrangą realizuoti, saugoti bei atkurti.

b) **Susitarimas dėl licencijų skaičiaus.** Teisė naudoti Programinę įrangą yra susieta su Galutinių vartotojų skaičiumi. Vienas Galutinis vartotojas reiškia, kad: i) Programinė įranga yra įdiegta vienoje kompiuterinėje sistemoje arba ii) jei licencijos apimtis yra susieta su pašto dėžučių skaičiumi, tuomet vienas Galutinis vartotojas reiškia kompiuterio naudotoją, kuris gauna el. paštą per Pašto naudojimo programą („PNP“). Jei PNP priima el. laišką ir jį automatiškai paskirsto keliems naudotojams, Galutinių vartotojų skaičius bus nustatomas pagal faktinį naudotojų, kuriems el. laiškai yra paskirstomi, skaičių. Jei pašto serveris atlieka pašto apsaugos (vartų) funkciją, Galutinių vartotojų skaičius sutaps su pašto serverio naudotojų, kuriems teikiama pašto apsaugos funkcija, skaičiumi. Jei vienam naudotojui nukreipiamas nenurodytas el. pašto adresų skaičius ir jis juos priima (pvz., naudojant alternatyviuosius vardus), o programa automatiškai nepaskirsto el. laiškų didesniam naudotojų skaičiui, vienam kompiuteriui yra privaloma viena licencija. Draudžiama naudoti tą pačią Licenciją vienu metu daugiau nei viename kompiuteryje. Galutinis naudotojas turi teisę įvesti Programinės įrangos Licencijos raktą ir naudotis Programine įranga tiek, kiek Galutinis naudotojas turi teisę tai daryti, atsižvelgiant į apribojimus, atsirandančius dėl Teikėjo suteiktų licencijų skaičiaus. Licencijos raktas laikomas konfidencialiu ir Jūs negalite bendrinti licencijos su trečiosiomis šalimis arba leisti trečiosioms šalimis naudoti licencijos raktą, jei to neleidžia ši Sutartis arba Teikėjas. Jei Licencijos raktas pažeistas, nedelsdami informuokite Teikėją.

c) **„Home Edition“ / „Business Edition“ (namams / įmonėms skirta versija).** Programinės įrangos „Home Edition“ versija skirta naudoti tik privačioje ir (arba) nekomercinėje aplinkoje namų ar šeimos reikmėms. Programinės įrangos „Business Edition“ versiją privaloma įsigyti, jei Programinė įranga bus naudojama komercinėje aplinkoje,

pašto serveriuose, pašto perdavimo serveryje, pašto apsaugos serveryje ar interneto tinklų sietuve.

d) **Licencijos galiojimo laikas.** Teisė naudoti Programinę įrangą yra suteikiama ribotą laiką.

e) **OEM programinė įranga.** OĮG programinė įranga gali būti naudojama tik Kompiuteryje, su kuriuo ją įsigijote. Jos negalima perkelti į kitą kompiuterį.

f) **NESKIRTA PERPARDUOTI BANDOMOJI programinės įrangos versija.** Programinė įranga, KURI YRA NESKIRTA PERPARDUOTI ar BANDOMOJI, nėra apmokestinama ir turi būti naudojama tik Programinės įrangos funkcijoms pademonstruoti ar išbandyti.

g) **Licencijos nutraukimas.** Licencija automatiškai nutraukiama pasibaigus jos galiojimo laikui. Jei Jūs nesilaikysite Sutarties nuostatų, Tiekėjas turės teisę atsisakyti Sutarties ir pasinaudoti visomis teisėmis ar teisinėmis priemonėmis, kurios Tiekėjui prieinamos tokiais atvejais. Licencijos atšaukimo atveju privalote nedelsdami savo sąskaita Programinę įrangą ir visas jos atsargines kopijas ištrinti, sunaikinti arba grąžinti ESET arba prekybos įmonei, iš kurios Programinę įrangą įsigijote. Nutraukus licenciją, Tiekėjas taip pat turi teisę atšaukti galutinio vartotojo teisę naudotis Programinės įrangos funkcijomis, kurioms reikalingas prisijungimas prie Tiekėjo serverių ar trečiųjų šalių serverių.

4. **Funkcijos, kurios renka duomenis ir kurioms reikalingas interneto ryšys.** Kad tinkamai veiktų, programinei įrangai reikalingas interneto ryšys ir ji turi reguliariai užmegzti ryšį su Teikėjo serveriais arba trečiųjų šalių serveriais ir taikomu duomenų rinkimu, kaip tai numatoma Privatumo politikoje. Interneto ryšys ir atitinkamas duomenų rinkimas būtinas toliau nurodomoms programinės įrangos funkcijoms.

a) **Programinės įrangos naujinimai.** Tiekėjas turi teisę kartais išleisti Programinės įrangos naujinimus (toliau – Naujinimai), tačiau jų teikti neprivalo. Ši funkcija įjungiama standartiniuose Programinės įrangos nustatymuose, todėl, jei Galutinis naudotojas automatinio Naujinimų diegimo funkcijos neišjungė, Naujinimai yra įdiegiami automatiškai. Teikiant Naujinimus reikalingas Licencijų autentiškumo patvirtinimas, įskaitant informaciją apie Kompiuterį ir (arba) platformą, kurioje įdiegta Programinė įranga, kaip nurodyta Privatumo politikoje.

Bet kokių Naujinimų teikimui gali būti taikoma gyvavimo ciklo pabaigos politika (toliau – EOL politika), kurią galima rasti https://go.eset.com/eol_home. Jokie Naujinimai nebus teikiami po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje.

b) **Įsiskverbčių ir informacijos peradresavimas Teikėjui.** Programinėje įrangoje įdiegta funkcijų, kurios renka kompiuterinių virusų, kitų kompiuterinių kenkimo programų bei įtartinų, probleminių, galimų nepageidaujamų ar galimų nesaugių objektų (failų, URL, IP paketų ir eterneto kadrų) pavyzdžius („Įsiskverbtimis“) ir siunčia juos Teikėjui kartu su (neapsiribojant vien tik tuo) informacija apie diegimo procesą, kompiuterį ir (arba) platformą, kurioje Programinė įranga įdiegta, ir informacija apie Programinės įrangos operacijas bei funkcijas („Informacija“). Informacijoje ir Įsiskverbtyse gali būti duomenų (įskaitant atsitiktinai ar netyčia gautus asmeninius duomenis) apie Galutinį naudotoją ar kitus kompiuterio, kuriame įdiegta Programinė įranga, naudotojus, taip pat – failų, kuriuos paveikia Įsiskverbtys su susijusiais metaduomenimis.

Informaciją ir Įsiskverbtis gali rinkti šios Programinės įrangos funkcijos:

i. „LiveGrid“ reputacijos sistemos funkcija renka ir Teikėjui siunčia vienpusius informacijos rinkinius, susijusius su Įsiskverbtimis. Ši funkcija įjungiama Programinės įrangos standartinėse nuostatose.

ii. „LiveGrid“ grįžtamojo ryšio sistemos funkcija apima Infiltravimų su susijusiais metaduomenimis ir Informacijos rinkimą ir siuntimą Teikėjui. Galutinis vartotojas šią funkciją gali įjungti programinės įrangos diegimo metu.

Teikėjas gautą informaciją ir infiltravimus gali naudoti tik analizei ir atliekant infiltravimų tyrimus, tobulinant programinę įrangą ir licencijų autentiškumo patvirtinimą ir privalo imtis atitinkamų priemonių, kad būtų

užtikrintas gautų infiltravimų ir informacijos saugumas. Suaktyvinus šią programinės įrangos funkciją, Teikėjas gali rinkti ir apdoroti infiltravimus ir informaciją taip, kaip tai nurodoma Privatumo politikoje ir vadovaujantis galiojančiais įstatymais. Šias funkcijas galima išjungti bet kuriuo metu.

Įgyvendinant šią Sutartį, būtina rinkti, apdoroti ir saugoti duomenis, kurie įgalina Teikėją identifikuoti jus vadovaujantis Privatumo politika. Jūs sutinkate, kad Teikėjas, norėdamas patikrinti, ar Jūs naudojate Programinę įrangą pagal Sutarties sąlygas, naudotų savo priemones. Jūs pateikiate sutikimą, kad ryšio tarp Programinės įrangos ir Teikėjo kompiuterių sistemų ar jo verslo partnerių kompiuterių sistemų metu būtų vykdomas duomenų perdavimas, kurio tikslas yra užtikrinti Programinės įrangos funkcionalumą ir leidimą ją naudoti bei Teikėjo teisių apsaugą.

Sudarius Sutartį Teikėjas ar bet kuris jo verslo partneris, kaip Teikėjo platinimo ir palaikymo tinklo dalis, sąskaitų pateikimo tikslu, vykdydamas šią Sutartį ir perduodamas pranešimus į jūsų kompiuterį, turi teisę perduoti, apdoroti ir saugoti pagrindinius Jus identifikuojančius duomenis.

Duomenys apie privatumą, asmeninių duomenų apsaugą ir jūsų teises pateikiami Privatumo politikoje, kurią rasite Teikėjo svetainėje ir galėsite pasiekti diegimo proceso metu. Taip pat galite ją rasti Programinės įrangos žinyno skyriuje.

5. **Galutinio vartotojo teisių įgyvendinimas**. Galutinio vartotojo teises galite įgyvendinti asmeniškai arba per savo darbuotojus. Jūs turite teisę Programinę įrangą naudoti tik tam, kad apsaugotumėte savo veiklą ir apsaugotumėte kompiuterines sistemas, kurioms Licencija yra taikoma.

6. **Teisių apribojimai.** Neturite teisės kopijuoti, platinti, išimti Programinės įrangos sudedamąsias dalis ar gaminti iš jos išvestinius produktus. Naudodami Programinę įrangą privalote laikytis šių apribojimų.

a) Nuolatinėje atminties laikmenoje galite pasigaminti vieną Programinės įrangos kopiją kaip archyvinę atsarginę kopiją su sąlyga, kad jūsų archyvinė atsarginė kopija nebus įdiegta ir naudojama kitame kompiuteryje. Visos kitos Jūsų pagamintos Programinės įrangos kopijos bus laikomos Sutarties pažeidimu.

b) Draudžiama naudoti, keisti, versti ar atgaminti Programinę įrangą, perleisti teises naudoti Programinę įrangą ar Programinės įrangos kopijas kokiu nors Sutartyje nenurodytu būdu.

c) Draudžiama parduoti, sublicencijuoti, nuomoti ar nuomotis, skolintis Programinę įrangą arba naudoti Programinę įrangą norint teikti komercines paslaugas.

d) Draudžiama keisti duomenis, perdaryti ar išardyti Programinę įrangą ar kitais būdais bandyti nustatyti pradinį Programinės įrangos kodą, išskyrus atvejus, kai šį apribojimą aiškiai draudžia įstatymas.

e) Sutinkate Programinę įrangą naudoti tik tokiu būdu, kuris neprieštarauja įstatymams, galiojantiems jurisdikcijoje, kurioje naudojate Programinę įrangą, įskaitant galiojančius apribojimus dėl autorių teisių ir kitas intelektinės nuosavybės teises, bet tuo nepasiribojant.

f) Sutinkate, kad Programine įranga ir jos funkcijomis naudositės tik taip, kad neribotumėte kitų galutinių vartotojų prieigos prie šių paslaugų. Tiekėjas pasilieka teisę apriboti atskiriems galutiniams vartotojams teikiamų paslaugų apimtį, kad paslaugomis galėtų naudotis kuo didesnis galutinių vartotojų skaičius. Apribojus paslaugų apimtį taip pat visiškai panaikinama galimybė naudotis bet kuriomis Programinės įrangos ir Duomenų trynimo funkcijomis bei su kuria nors iš Programinės įrangos funkcijų susijusia informacija, kuri saugoma Tiekėjo ar trečiųjų šalių serveriuose.

g) Jūs sutinkate neatlikti jokių veiksmų naudodamiesi licencijos raktu, kurie prieštarautų šios Sutarties sąlygoms arba suteiktų Licencijos raktą asmeniui, kuris neturi teisės naudotis programine įranga, pvz., naudotos arba nenaudotos Licencijos rakto perdavimas bet kokia forma, taip pat neteisėtas atkūrimas, dubliuotų arba

sugeneruotų licencijos raktų platinimas, arba programinės įrangos naudojimas pritaikius ne iš Teikėjo gautą licencijos raktą.

7. **Autorių teisės**. Programinė įranga ir visos teisės be apribojimų, įskaitant nuosavybės teises ir intelektinės nuosavybės teises, priklauso ESET ir (arba) jos licencijų išdavėjams. Jas gina tarptautinių susitarimų nuostatos ir visi kiti šalies, kurioje Programinė įranga yra naudojama, galiojantys nacionaliniai įstatymai. Programinės įrangos struktūra, organizacija ir kodas yra vertingos prekybos paslaptys ir konfidenciali ESET ir (arba) jos licencijos išdavėjų informacija. Draudžiama daryti Programinės įrangos kopijas, išskyrus 6 straipsnio a dalyje numatytus atvejus. Visoms kopijoms, kurias Jūs galite pasidaryti remdamasis šia Sutartimi, galioja tos pačios autorių teisės ir kiti nuosavybės reikalavimai, nurodyti ant Programinės įrangos. Jei Jūs pažeisdami Sutartį pakeisite duomenis, perdarysite ar išardysite Programinę įrangą ar kitais būdais pabandysite nustatyti pradinį Programinės įrangos kodą, sutinkate tokiu būdu gautą informaciją automatiškai ir neatšaukiamai perduoti vien tik Tiekėjo nuosavybėn nuo to momento, kai tokia informacija atsiranda, nepaisant Tiekėjo teisių, susijusių su Sutarties pažeidimu.

8. **Teisių išlaikymas**. Teikėjas išlaiko visas teises į Programinę įrangą, išskyrus pagal Sutarties sąlygas Jums kaip Programinės įrangos Galutiniam vartotojui aiškiai suteiktas teises.

9. **Versijos keliomis kalbomis, sudvejintos laikmenos su programine įranga, keli kopijų egzemplioriai**. Tuo atveju, kai Programinė įranga palaiko kelias platformas ar kalbas arba jei Jūs gavote kelis Programinės įrangos kopijos egzempliorius, kompiuterinių sistemų, kuriose turite teisę naudoti Programinę įrangą ir Jūsų įsigytas versijas, skaičius priklauso nuo įsigytų Licencijų skaičiaus. Draudžiama Jūsų nenaudojamas Programinės įrangos versijas ar kopijas parduoti, nuomoti, sublicencijuoti, skolinti ar perduoti.

10. **Sutarties įsigaliojimas ir nutraukimas.** Sutartis įsigalioja nuo tos dienos, kai sutinkate su Sutarties sąlygomis. Sutartį bet kada galite nutraukti visam laikui savo sąskaita pašalindami, sunaikindami ar grąžindami Programinę įrangą, visas atsargines kopijas ir susijusią medžiagą, pateiktą Tiekėjo ar jo verslo partnerių. Jūsų teisei naudotis Programine įranga ir bet kuria jos funkcija gali būti taikoma EOL politika. Jūsų teisė naudotis Programine įranga pasibaigs po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje. Nepriklausomai nuo Sutarties nutraukimo būdo, 7, 8, 11, 13, 19 ir 21 straipsnių nuostatos toliau galioja neribotą laiką.

11. **GALUTINIO VARTOTOJO PAREIŠKIMAI**. BŪDAMAS GALUTINIU VARTOTOJU JŪS PATVIRTINATE, KAD PROGRAMINĖ ĮRANGA YRA „PATEIKTA TOKIA, KOKIA YRA“, BE JOKIOS GARANTIJOS, TIKSLIAI APIBRĖŽTOS ARBA NUMANOMOS, PAGAL GALIOJANČIUS ĮSTATYMUS. NEI TIEKĖJAS, JO LICENCIJOS IŠDAVĖJAI AR ANTRINĖS BENDROVĖS, NEI AUTORIŲ TEISIŲ SAVININKAI NEPATEIKIA JOKIŲ PASTABŲ AR NESUTEIKIA GARANTIJŲ, TIKSLIAI APIBRĖŽTŲ ARBA NUMANOMŲ, ĮSKAITANT GARANTIJAS DĖL PERKAMUMO AR TINKAMUMO TAM TIKRAM TIKSLUI ARBA, KAD PROGRAMINĖ ĮRANGA NEPAŽEIS JOKIŲ TREČIŲJŲ ASMENŲ PATENTŲ, AUTORIŲ TEISIŲ, PREKIŲ ŽENKLŲ AR KITŲ TEISIŲ, BET TUO NEAPSIRIBOJANT. NEI TIEKĖJAS, NEI JOKIA KITA ŠALIS NESUTEIKIA GARANTIJOS, KAD PROGRAMINĖS ĮRANGOS FUNKCIJOS ATITIKS VARTOTOJO REIKALAVIMUS ARBA, KAD PROGRAMINĖ ĮRANGA VEIKS NEPERTRAUKIAMAI, AR BE JOKIŲ KLAIDŲ. PASIRINKDAMI PROGRAMINĘ ĮRANGĄ PRISIIMATE VISĄ ATSAKOMYBĘ IR RIZIKĄ, TAIP PAT ATSAKOMYBĘ DĖL PROGRAMINĖS ĮRANGOS ĮDIEGIMO, NAUDOJIMO IR REZULTATŲ, PASIEKTŲ NAUDOJANT PROGRAMINĘ ĮRANGĄ.

12. **Kitų įsipareigojimų nėra**. Sutartis nenumato kitų Teikėjo ir jo licencijų išdavėjų įsipareigojimų, išskyrus šiame dokumente konkrečiai numatytus įsipareigojimus.

13. **ATSAKOMYBĖS APRIBOJIMAS**. ATSIŽVELGDAMAS Į GALIOJANČIUS ĮSTATYMUS, GAMINTOJAS, JO DARBUOTOJAI AR LICENCIJŲ IŠDAVĖJAI JOKIU ATVEJU NĖRA ATSAKINGI DĖL PRARASTO PELNO, PAJAMŲ, PARDAVIMO, DUOMENŲ AR PIRKIMO KAINŲ, TURTO NUOSTOLIŲ, ASMENINIŲ SUSIŽEIDIMŲ, VERSLO TRUKDŽIŲ, VERSLO INFORMACIJOS NUTEKĖJIMO AR DĖL JOKIŲ SPECIALIŲ, TIESIOGINIŲ, NETIESIOGINIŲ, ATSITIKTINIŲ, EKONOMINIŲ, DRAUDIMO, TEISMO PRITEISTŲ, YPATINGŲ NUOSTOLIŲ, KAIP NORS KILUSIŲ AR KYLANČIŲ DĖL SUTARTIES, CIVILINĖS TEISĖS PAŽEIDIMŲ, NEAPDAIRUMO AR KITŲ ATSAKOMYBĖS ATVEJŲ, KYLANČIŲ DĖL

PROGRAMINĖS ĮRANGOS ĮDIEGIMO, NAUDOJIMO AR NEGALĖJIMO NAUDOTIS JA, NET JEI GAMINTOJUI YRA ŽINOMA GALIMYBĖ PATIRTI TOKIĄ ŽALĄ. KADANGI KAI KURIOSE ŠALYSE IR JURISDIKCIJOSE DRAUDŽIAMA IŠSKIRTI TAM TIKRĄ ATSAKOMYBĘ, TAČIAU LEIDŽIAMAS ATSAKOMYBĖS APRIBOJIMAS, TEIKĖJO, JO DARBUOTOJŲ, LICENCIJŲ IŠDAVĖJŲ AR ANTRINIŲ ĮMONIŲ ATSAKOMYBĖ APSIRIBOJA MOKESČIO UŽ LICENCIJĄ SUMA.

14. Šios Sutarties nuostatos neapriboja bet kuriai šaliai, veikiančiai kaip vartotojui, įstatymais suteiktų teisių, jei jos prieštarauja čia pateiktoms.

15. **Techninė pagalba**. ESET ar ESET įgaliotosios trečiosios šalys techninę pagalbą teikia savo nuožiūra, nesuteikdamos jokių garantijų ar pareiškimų. Jokie techninė pagalba nebus teikiama po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje. Prieš suteikiant techninę pagalbą Galutinis vartotojas privalo pasigaminti turimų duomenų, programinės įrangos ir programų atsargines kopijas. ESET ir (arba) ESET įgaliotosios šalys neprisiima atsakomybės už žalą ar prarastus duomenis, turtą, programinę įrangą ar aparatinę įrangą, ar dėl techninės pagalbos prarastą pelną. ESET ir (arba) ESET įgaliotosios šalys pasilieka teisę nuspręsti, ar problemos pašalinimui gali būti teikiama techninė pagalba. ESET pasilieka teisę savo nuožiūra atsisakyti suteikti techninę pagalbą, laikinai ją sustabdyti ar nutraukti. Vadovaujantis Privatumo politika, licencijos informacija, informacija ir kiti duomenys gali būti reikalingi teikiant techninio palaikymo pagalbą.

16. **Licencijos perdavimas**. Programinę įrangą galima perkelti iš vienos kompiuterinės sistemos į kitą, jei tai neprieštarauja Sutarties sąlygoms. Jei tai neprieštarauja Sutarties sąlygoms, tik gavęs Tiekėjo sutikimą Galutinis naudotojas turės teisę visam laikui perduoti Licenciją ir visas iš šios Sutarties kylančias teises kitam Galutiniam naudotojui, su sąlyga, kad (i) pradinis Galutinis naudotojas nepasiliko Programinės įrangos kopijų; (ii) teisių perdavimas vykdomas tiesiogiai, t. y. pradinis Galutinis naudotojas jas perduoda naujajam Galutiniam naudotojui; (iii) naujasis Galutinis naudotojas prisiims visas teises ir įsipareigojimus, pagal Sutartį priklausančius pradiniam Galutiniam naudotojui; (iv) pradinis Galutinis naudotojas pateiks naujajam Galutiniam naudotojui dokumentus, leidžiančius įsitikinti 17 straipsnyje nurodytos Programinės įrangos autentiškumu.

17. **Programinės įrangos autentiškumo patikrinimas.** Galutinis vartotojas teisę naudotis Programine įranga gali įrodyti vienu iš toliau pateikiamų būdų: (i) pateikdamas Teikėjo ar Teikėjo paskirtos trečiosios šalies išduotą licencijos pažymėjimą; (ii) pateikdamas rašytinę licencijos sutartį, jei tokia sutartis buvo sudaryta; (iii) pateikdamas Teikėjo siųstą el. laišką, kuriame yra licencijavimo informacijos (naudotojo vardas ir slaptažodis). Pgal Privatumo politiką Licencijos informacija ir Galutinio vartotojo identifikavimo duomenys gali būti reikalingi patvirtinant Programinės įrangos autentiškumą.

18. **Licencijos išdavimas valstybės įstaigoms ir JAV vyriausybei**. Programinė įranga teikiama valstybės įstaigoms, įskaitant Jungtinių Amerikos Valstijų vyriausybę, taikant licencijavimo teises ir apribojimus, aprašytus šioje Sutartyje.

19. **Prekybos kontrolės reikalavimų laikymasis**.

a) Tiesiogiai ar netiesiogiai neeksportuosite, nereeksportuosite, neperleisite ar kitaip nesuteiksite programinės įrangos jokiam asmeniui, nenaudosite jos jokiais būdais ir nedalyvausite jokiuose veiksmuose, dėl kurių ESET arba jos kontroliuojančiosios bendrovės, jos patronuojamosios įmonės ir bet kurios jos kontroliuojančiosios bendrovės patronuojamosios įmonės, taip pat jos kontroliuojančiųjų bendrovių kontroliuojami subjektai (filialai) gali pažeisti prekybos kontrolės įstatymus arba patirti dėl jų neigiamų pasekmių, įskaitant:

i. bet kokius įstatymus, kuriais kontroliuojami, ribojami arba nustatomi licencijų išdavimo reikalavimai prekių, programinės įrangos, technologijų ar paslaugų eksportui, reeksportui ar perdavimui, kuriuos išduoda arba priima bet kuri Jungtinių Amerikos Valstijų, Singapūro, Jungtinės Karalystės, Europos Sąjungos ar bet kurios jos valstybės narės vyriausybė, valstija ar reguliavimo institucija ar bet kuri šalis, kurioje turi būti vykdomi įsipareigojimai pagal Susitarimą arba kurioje ESET ar bet kuris jos filialas yra įregistruoti arba veikia, ir

ii. bet kokią ekonominę, finansinę, prekybos ar kitą sankciją, apribojimą, embargą, importo ar eksporto draudimą, draudimą pervesti lėšas ar turtą arba teikti paslaugas, taip pat lygiavertę priemonę, kurią nustato bet kuri Jungtinių Amerikos Valstijų, Singapūro, Jungtinės Karalystės, Europos Sąjungos ar bet kurios jos valstybės narės vyriausybė, valstija ar reguliavimo institucija ar bet kuri šalis, kurioje turi būti vykdomi įsipareigojimai pagal Susitarimą arba kurioje ESET ar bet kuris jos filialas yra įregistruoti arba veikia.

(i ir ii punktuose nurodyti teisės aktai kartu vadinami Prekybos kontrolės įstatymais).

b) ESET turi teisę nedelsdama sustabdyti savo įsipareigojimus pagal šias sąlygas arba nutraukti sąlygų galiojimą, jei:

i. ESET nustato, kad, jos pagrįsta nuomone, naudotojas pažeidė arba gali pažeisti Susitarimo 19 straipsnio a dalį, arba

ii. galutiniam naudotojui ir (arba) programinei įrangai taikomi prekybos kontrolės įstatymai, todėl ESET nustato, kad, jos pagrįsta nuomone, dėl nuolatinių įsipareigojimų pagal Susitarimą vykdymo ESET arba jos filialai gali pažeisti prekybos kontrolės įstatymus arba patirti dėl jų neigiamų pasekmių.

c) Susitarime nėra numatyta ir jo nuostatos neturėtų būti aiškinamos ar vertinamos taip, kad kuri nors šalis būtų skatinama ar verčiama imtis veiksmų arba nuo jų susilaikyti (arba sutikti imtis veiksmų arba nuo jų susilaikyti) tokiu būdu, kuris prieštarauja galiojantiems prekybos kontrolės įstatymams, už kurį yra baudžiama arba kuris yra draudžiamas.

20. **Pranešimai**. Visi pranešimai turi būti siunčiami, o Programinė įranga ir Dokumentai grąžinami adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, nepažeidžiant ESET teisės pranešti jums apie bet kokius šios Sutarties, Privatumo politikos, EOL politikos ir Dokumentų pakeitimus pagal Sutarties 22 straipsnį. ESET gali siųsti jums el. laiškus ir pranešimus programoje per jūsų Programinę įrangą arba paskelbti pranešimą mūsų svetainėje. Jūs sutinkate elektroninėmis priemonėmis gauti ESET teisinius pranešimus, įskaitant bet kokius pranešimus apie Sąlygų, Specialiųjų sąlygų ar Privatumo politikos pakeitimus, bet kokį sutarties pasiūlymą / priėmimą ar kvietimus tvarkyti, pranešimus ar kitus teisinius pranešimus. Toks bendravimas elektroninėmis priemonėmis laikomas raštišku, išskyrus atvejus, kai pagal galiojančius įstatymus konkrečiai reikalaujama kitokios bendravimo formos.

21. **Taikomi teisės aktai**. Ši sutartis sudaryta pagal Slovakijos Respublikos įstatymus. Galutinis vartotojas ir Tiekėjas sutinka, kad jai netaikomi teisių konflikto principai ir Jungtinių Tautų konvencija dėl tarptautinio prekių pirkimo-pardavimo sutarčių. Jus sutinkate, kad visi ginčai ar pretenzijos, kylantys iš šios Sutarties ir susiję su Tiekėju, ar visi ginčai ar pretenzijos, susijusios su Programinės įrangos naudojimu, yra sprendžiami Bratislavos I apygardos teisme, ir Jūs aiškiai sutinkate su šio teismo jurisdikcija.

22. **Bendrosios nuostatos**. Jei kuri nors Sutarties nuostata pasirodys negaliojanti ir negalinti būti ieškinio pagrindas, ji nepaveiks bendro kitų Sutarties nuostatų teisėtumo, o Sutartis galios toliau ir bus vykdoma remiantis Sutartyje numatytomis sąlygomis. Ši Sutartis sudaryta anglų kalba. Jei patogumo ar kitais tikslais buvo parengtas šios Sutarties vertimas ir jei Sutarties kalbos versijos skiriasi, pirmenybė teikiama versijai anglų kalba.

ESET pasilieka teisę keisti Programinę įrangą, taip pat bet kuriuo metu peržiūrėti šią Sutartį, jos Priedus, Priedėlius, Privatumo politiką, EOL politiką ir Dokumentus arba jų dalį, atnaujindama atitinkamą dokumentą, i) kad būtų atsižvelgta į Programinės įrangos pakeitimus arba į tai, kaip ESET vykdo veiklą, ii) dėl teisinių, reguliavimo ar saugumo priežasčių arba iii) siekiant užkirsti kelią piktnaudžiavimui ar žalai. Apie bet kokią Sutarties peržiūrą jums bus pranešta el. paštu, pranešimu programoje ar kitomis elektroninėmis priemonėmis. Jei nesutinkate su siūlomais Sutarties pakeitimais, per 30 dienų nuo pranešimo apie pakeitimus gavimo galite ją nutraukti pagal 10 straipsnį. Jei per šį laikotarpį Sutarties nenutrauksite, siūlomi pakeitimai bus laikomi priimtais ir įsigalios jums nuo tos dienos, kai gausite pranešimą apie pakeitimą.

Tai yra visa Teikėjo ir Jūsų sudaryta Sutartis dėl Programinės įrangos; ji panaikina visus su Programine įranga susijusius ankstesnius teiginius, pokalbius, įsipareigojimus, pranešimus ar reklaminius teiginius.

SUTARTIES PRIEDAS

Prie tinklo prijungtų įrenginių saugos vertinimas. Prie tinklo prijungtų įrenginių saugos vertinimui taikomos papildomos nuostatos:

Programinėje įrangoje įdiegta funkcija, skirta Galutinio vartotojo vietos tinklo ir vietos tinklo įrenginių saugai patikrinti. Tam reikia vietos tinklo pavadinimo ir su licencijos informacija susijusios informacijos apie vietos tinklo įrenginius, pavyzdžiui, apie vietos tinklo įrenginių buvimą, tipą, pavadinimą, IP adresą ir MAC adresą. Informacija taip pat apima maršrutizatoriaus įrenginių belaidžio tinklo saugos tipą ir belaidžio tinklo šifravimo tipą. Ši funkcija taip pat pateikia informaciją apie saugos programinės įrangos sprendimo vietos tinklo įrenginiams apsaugoti prieinamumą.

Apsauga nuo netinkamo duomenų naudojimo. Apsaugai nuo netinkamo duomenų naudojimo taikomos papildomos nuostatos:

Programinėje įrangoje yra funkcija, apsauganti nuo svarbių duomenų praradimo arba netinkamo naudojimo, jei Kompiuteris būtų pavogtas. Pagal numatytuosius programinės įrangos parametrus ši funkcija yra išjungta. Kad ją aktyvintumėte, turite susikurti ESET HOME paskyrą, per kurią ši funkcija aktyvina duomenų rinkimą kompiuterio vagystės atveju. Jei pasirinksite aktyvinti šią programinės įrangos funkciją, duomenys apie pavogtą kompiuterį bus renkami ir siunčiami Teikėjui; šie duomenys gali apimti kompiuterio tinklo vietą, duomenis apie kompiuterio ekrane rodomą turinį, duomenis apie kompiuterio konfigūraciją ir (arba) prie kompiuterio prijungtos kameros įrašytus duomenis (toliau – Duomenys). Galutinis naudotojas privalo turėti įgaliojimus naudoti šios funkcijos ir ESET HOME paskyros surinktus duomenis, kai tai reikalinga norint ištaisyti nepalankią situaciją, susiklosčiusią dėl kompiuterio vagystės. Atsižvelgdamas į šios funkcijos paskirtį, Teikėjas apdoroja Duomenis vadovaudamasis Privatumo politika ir atitinkamais galiojančiais teisės aktais. Teikėjas turi suteikti Galutiniam vartotojui prieigą prie Duomenų reikiamam laikotarpiui, kad būtų įgyvendintas tikslas, dėl kurio ir buvo renkami šie duomenys. Šis laikotarpis negali būti ilgesnis nei Privatumo politikoje nurodytas saugojimo laikotarpis. Duomenų apsauga nuo netinkamo naudojimo taikoma tik tuose Kompiuteriuose ir paskyrose, prie kurių Galutinis vartotojas turi teisėtą prieigą. Apie bet kokį neteisėto naudojimo atvejį bus pranešta reikiamoms institucijoms. Teikėjas privalo laikytis atitinkamų įstatymų ir padėti teisėsaugos institucijoms netinkamo naudojimo atvejais. Žinote ir pripažįstate, kad esate atsakingi už slaptažodžio, kuris naudojamas ESET HOME paskyrai pasiekti, apsaugą, ir sutinkate savo slaptažodžio neatskleisti jokioms trečiosioms šalims. Galutinis naudotojas yra atsakingas už bet kokią veiklą naudojantis Apsaugos nuo netinkamo duomenų naudojimo funkcija ir ESET HOME paskyra, neatsižvelgiant į tai, ar buvo suteiktas leidimas. Jei ESET HOME Paskyrai kilo pavojus, nedelsdami praneškite Teikėjui. Papildomos nuostatos dėl Apsaugos nuo neteisingo duomenų naudojimo bus taikomos išskirtinai „ESET Internet Security“ ir „ESET Smart Security Premium“ galutiniams naudotojams.

ESET Secure Data. „ESET Secure Data“ taikomos papildomos nuostatos:

1. Apibrėžtys. Šiose papildomose nuostatose dėl „ESET Secure Data“ pateikiamos toliau nurodytų žodžių reikšmių apibrėžtys:

a) „Informacija“ bet kokia informacija arba duomenys, kurie užšifruojami arba iššifruojami naudojantis programine įranga;

b) „Produktai“ yra „ESET Secure Data“ programinė įranga ir dokumentacija;

c) „ESET Secure Data“ yra programinė įranga, kuri naudojama užšifruojant ir iššifruojant elektroninius duomenis;

Visos nuorodos į daugiskaitą reiškia ir vienaskaitą, o visos nuorodos į vyrišką giminę reiškia ir moterišką bei

bevardę giminę ir atvirkščiai. Žodžiai, kurių apibrėžtys nepateikiamos, naudojami vadovaujantis Sutartyje pateikiamomis apibrėžtimis.

2. Papildoma galutinio vartotojo deklaracija. Jūs pritariate ir sutinkate:

a) jūs esate atsakingas už informacijos apsaugą ir atsarginių kopijų kūrimą;

b) jūs turite sukurti visos informacijos ir duomenų (įskaitant neribotai visą kritinę informaciją ir duomenis) atsargines kopijas savo kompiuteryje prieš diegdami „ESET Secure Data“;

c) turite saugiai laikyti visų slaptažodžių arba kitos informacijos, skirtos programinės įrangos ESET Secure Data sąrankai bei naudojimui, įrašus, be to, turite sukurti visų šifravimo raktų, licencijų kodų, raktinių failų bei kitų sugeneruotų duomenų atsargines kopijas atskiroje laikmenoje;

d) jūs esate atsakingas už produktų naudojimą. Teikėjas nėra atsakingas už bet kokius praradimus, pretenzijas ar pažeidimus, atsiradusius dėl neįgalioto ar klaidingo informacijos ar duomenų užšifravimo arba iššifravimo (įskaitant neribotą informaciją), nesvarbu, kur ir kaip ši informacija ar duomenys laikomi;

e) nors teikėjas ėmėsi visų pagrįstų veiksmų, kad būtų užtikrintas „ESET Secure Data“ vientisumas ir sauga, produktai (arba bet kuris iš jų) neturi būti naudojami jokiose srityse, kurios yra priklausomos nuo saugos patikimumo lygio arba kurios yra potencialiai pavojingos, įskaitant be apribojimų branduolinę įrangą, orlaivių navigaciją, valdymo arba ryšio sistemas, ginklų ir gynybos sistemas bei gyvybės palaikymo ar gyvybės stebėjimo sistemas;

f) jūsų pareiga yra įsitikinti, kad numatytas produktų saugumo ir šifravimo lygis atitiktų jūsų reikalavimus;

g) jūs esate atsakingas, kad produktai (arba bet kuris iš jų) įskaitant be ribojimų būtų naudojami laikantis visų taikytinų Slovakijos Respublikos arba kitų šalių, sričių ar valstijų, kuriose produktas naudojamas, įstatymų ir taisyklių. Turite užtikrinti, kad prieš bet kokį produktų naudojimą, būtų įsitikinta, jog tai neprieštarauja jokiems valstybinių institucijų (Slovakijos Respublikos ar kitų šalių) embargo reikalavimams;

h) jūs sutinkate, kad „ESET Secure Data“ gali kartais susisiekti su Teikėjo serveriais, kad patikrintų licencijos informaciją, galimas pataisas, pakeitimų paketus ir kitus naujinimus, kurie gali pagerinti, tvarkyti, keisti arba patobulinti „ESET Secure Data“ programinės įrangos veikimą ir siųsti bendrą sistemos informaciją, susijusią su programinės įrangos veikimu vadovaujantis Privatumo politika.

i) Teikėjas nėra atsakingas už bet kokius praradimus, pažeidimus, išlaidas ar pretenzijas, atsiradusias dėl praradimo, vagystės, netinkamo naudojimo, gedimo, pažeidimo arba dėl slaptažodžių, sąrankos informacijos, šifravimo raktų, licencijos aktyvinimo kodų ir kitų sugeneruotų arba išsaugotų duomenų sugadinimo naudojant programinę įrangą.

Papildomos nuostatos dėl „ESET Secure Data“ taikomos tik „ESET Smart Security Premium“ galutiniams naudotojams.

Password Manager Programinė įranga. „Password Manager“ programinei įrangai taikomos papildomos nuostatos:

1. Papildoma galutinio vartotojo deklaracija. Jūs sutinkate ir patvirtinate, kad negalėsite:

a) naudoti „Password Manager“ programinės įrangos kritinėse situacijose, kur gali kilti pavojus žmonių gyvybei ar turtui. Jūs suprantate, kad „Password Manager“ programinė įranga nėra skirta tokiems tikslams ir jos triktis gali sukelti mirtį, kūno sužalojimus arba didelius nuostolius turtui ar aplinkai, už kuriuos teikėjas nėra atsakingas.

„PASSWORD MANAGER“ PROGRAMINĖ ĮRANGA NĖRA SUKURTA, SKIRTA ARBA LICENCIJUOTA NAUDOTI

PAVOJINGOJE APLINKOJE, KURIAI REIKALINGAS PATIKIMAS VALDYMAS, ĮSKAITANT, BET NEAPSIRIBOJANT, ATOMINIŲ ĮRENGINIŲ, ORLAIVIŲ NAVIGACIJOS ARBA RYŠIO SISTEMŲ, AVIACIJOS VALDYMO IR GYVYBĖS PALAIKYMO ARBA GINKLŲ SISTEMŲ KŪRIMĄ, KONSTRAVIMĄ, PRIEŽIŪRĄ AR NAUDOJIMĄ. TEIKĖJAS AIŠKIAI ATSISAKO VISŲ IŠREIKŠTŲ ARBA NUMANOMŲ TINKAMUMO ŠIEMS TIKSLAMS GARANTIJŲ.

b) naudoti „Password Manager“ programinę įrangą taip, kad būtų pažeidžiama ši sutartis arba Slovakijos Respublikos ar jūsų jurisdikcijos įstatymai. „Password Manager“ programinės įrangos negalima naudoti vykdant arba skatinant bet kokią neteisėtą veiklą, įskaitant kenksmingo turinio duomenų persiuntimą arba duomenų, kurie gali būti naudojami neteisėtai veiklai ar kurie kokiu nors būdu pažeidžia įstatymus ar trečiųjų šalių teises (įskaitant visas intelektinės nuosavybės teises), įskaitant, bet neapsiribojant, bet kokius bandymus gauti prieigą prie paskyrų saugykloje (šiose „Password Manager“ programinės įrangos sąlygose „Saugykla“ vadinama duomenų saugojimo vieta, kurią tvarko teikėjas arba trečioji šalis (ne teikėjas ir naudotojas), skirta naudotojo duomenims sinchronizuoti ir jų atsarginėms kopijoms saugoti) arba kitų „Password Manager“ programinės įrangos arba saugyklos naudotojų paskyrų ir duomenų. Jeigu pažeisite bet kurią šių nuostatų, teikėjas turi teisę iškart nutraukti šią sutartį ir peradresuoti jums visų būtinų atkuriamųjų veiksmų išlaidas, o taip pat imtis reikiamų veiksmų, kad neleistų jums toliau naudotis „Password Manager“ programine įranga, be galimybės atgauti įmoką.

2. ATSAKOMYBĖS APRIBOJIMAS. „PASSWORD MANAGER“ PROGRAMINĖ ĮRANGA PATEIKIAMA TOKIA, „KOKIA YRA“. NESUTEIKIAMA JOKIO POBŪDŽIO IŠREIKŠTŲ AR NUMANOMŲ GARANTIJŲ. PROGRAMINĘ ĮRANGĄ NAUDOJATE SAVA RIZIKA. GAMINTOJAS NĖRA ATSAKINGAS UŽ DUOMENŲ PRARADIMĄ, SUGADINIMĄ, PASLAUGŲ PRIEINAMUMO RIBOJIMĄ, ĮSKAITANT VISUS DUOMENIS, „PASSWORD MANAGER“ PROGRAMINĖS ĮRANGOS IŠSIŲSTUS Į IŠORINĘ ATMINTĮ DUOMENIMS SINCHRONIZUOTI IR ATSARGINĖMS KOPIJOMS KURTI. DUOMENŲ ŠIFRAVIMAS NAUDOJANT „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ NEĮPAREIGOJA TEIKĖJO PRISIIMTI BET KOKIĄ ATSAKOMYBĘ DĖL DUOMENŲ SAUGOS. JŪS AIŠKIAI SUTINKATE, KAD DUOMENYS, GAUNAMI, NAUDOJAMI, ŠIFRUOJAMI, IŠSAUGOMI, SINCHRONIZUOJAMI ARBA SIUNČIAMI NAUDOJANT „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ, GALI BŪTI SAUGOMI IR TREČIŲJŲ ŠALIŲ SERVERIUOSE (TAIKOMA TIK NAUDOJANT „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ, KAI LEIDŽIAMOS SINCHRONIZAVIMO IR ATSARGINIO KOPIJAVIMO PASLAUGOS). JEIGU TEIKĖJAS SAVO NUOŽIŪRA PASIRENKA TOKIĄ TREČIŲJŲ ŠALIŲ SAUGYKLA, SVETAINĘ, ŽINIATINKLIO PORTALĄ, SERVERĮ ARBA PASLAUGĄ, TEIKĖJAS NĖRA ATSAKINGAS UŽ TOKIOS TREČIŲJŲ ŠALIŲ PASLAUGOS KOKYBĘ, SAUGĄ ARBA PASIEKIAMUMĄ IR JOKIA APIMTIMI TEIKĖJAS JUMS NĖRA ATSAKINGAS UŽ BET KOKĮ TREČIŲJŲ ŠALIŲ SUTARTIES AR TEISINIŲ ĮSIPAREIGOJIMŲ NESILAIKYMĄ IR UŽ ŽALĄ, PELNO PRARADIMĄ, FINANSINĘ IR NEFINANSINĘ ŽALĄ ARBA BET KOKIĄ KITĄ ŽALĄ NAUDOJANT ŠIĄ PROGRAMINĘ ĮRANGĄ. TEIKĖJAS NĖRA ATSAKINGA UŽ BET KOKIŲ GAUNAMŲ, NAUDOJAMŲ, ŠIFRUOJAMŲ, SAUGOMŲ, SINCHRONIZUOJAMŲ ARBA SIUNČIAMŲ DUOMENŲ TURINĮ, KAI NAUDOJATE „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ ARBA LAIKOTE SAUGYKLOJE. JŪS ESATE INFORMUOTI, KAD TEIKĖJAS NETURI PRIEIGOS PRIE SAUGOMŲ DUOMENŲ TURINIO IR NEGALI STEBĖTI JŲ ARBA PAŠALINTI TEISIŠKAI KENKSMINGO TURINIO.

Teikėjui priklauso visos „Password Manager“ programinės įrangos patobulinimų, naujinimų ir taisymų („patobulinimai“) teisės, net tuo atveju, jeigu šie patobulinimai buvo padaryti remiantis jūsų bet kokia forma pateiktais atsiliepimais, idėjomis ar pasiūlymais. Jūs neturėsite teisės į jokias kompensacijas, įskaitant bet kokias autoriaus teises, susijusias su šiais patobulinimais.

TEIKĖJO ĮMONĖS IR LICENCIJŲ TURĖTOJAI NEBUS JUMS ATSAKINGI UŽ BET KOKIO TIPO PRETENZIJAS IR ATSAKOMYBES, KYLANČIAS DĖL JŪSŲ AR TREČIŲJŲ ŠALIŲ BET KOKIO „PASSWORD MANAGER“ PROGRAMINĖS ĮRANGOS NAUDOJIMO AR KAIP NORS SU JUO SUSIJUSIOS, DĖL BET KOKIO BROKERIO ĮMONĖS AR ATSTOVO NAUDOJIMO AR NENAUDOJIMO, ARBA BET KOKIOS SAUGOS PARDAVIMO AR PIRKIMO, NESVARBU, AR ŠIOS PRETENZIJOS IR ATSAKOMYBĖS PAREMTOS KOKIOMIS NORS JURIDINĖMIS AR TEISINĖMIS TEORIJOMIS.

TEIKĖJO ĮMONĖS IR LICENCIJŲ TURĖTOJAI NĖRA JUMS ATSAKINGI UŽ JOKIUS TIESIOGINIUS, ATSITIKTINIUS, SPECIALIUS, NETIESIOGINIUS ARBA IŠPLAUKIANČIUS NUOSTOLIUS, ATSIRADUSIUS DĖL BET KOKIOS TREČIOSIOS ŠALIES PROGRAMINĖS ĮRANGOS, DĖL BET KOKIŲ PER „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ PASIEKIAMŲ DUOMENŲ NAUDOJIMO AR NEGALĖJIMO NAUDOTI, ARBA NEGALĖJIMO PASIEKTI DUOMENŲ PER

„PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ, NESVARBU, AR ŠIOS PRETENZIJOS IR ATSAKOMYBĖS PAREMTOS KOKIOMIS NORS JURIDINĖMIS AR TEISINĖMIS TEORIJOMIS. ŠIAME PUNKTE IŠSKIRTI NUOSTOLIAI BE RIBOJIMŲ YRA VERSLO PELNO PRARADIMAS, ŽMONIŲ SUŽALOJIMAS AR TURTO SUGADINIMAS, VERSLO NUTRŪKIMAS, DARBINĖS ARBA ASMENINĖS INFORMACIJOS PRARADIMAS. KAI KURIOS JURISDIKCIJOS NELEIDŽIA RIBOTI ATSITIKTINIŲ ARBA IŠPLAUKIANČIŲ NUOSTOLIŲ, TADA ŠIS RIBOJIMAS JUMS NETAIKOMAS. TOKIU ATVEJU TEIKĖJO ATSAKOMYBĖS APIMTIS BUS MAŽIAUSIA, LEIDŽIAMA PAGAL TAIKYTINĄ TEISĘ.

PER „PASSWORD MANAGER“ PROGRAMINĘ ĮRANGĄ PATEIKIAMA INFORMACIJA, ĮSKAITANT AKCIJŲ KAINAS, ANALIZĘ, RINKOS INFORMACIJĄ, NAUJIENAS IR FINANSINIUS DUOMENIS, GALI BŪTI PAVĖLUOTA, NETIKSLI ARBA SU KLAIDOMIS AR PRALEIDIMAIS, IR TEIKĖJO ĮMONĖS BEI LICENCIJŲ TURĖTOJAI NĖRA DĖL TO ATSAKINGI. TEIKĖJAS GALI KEISTI ARBA NUTRAUKTI BET KOKIAS „PASSWORD MANAGER“ PROGRAMINĖS ĮRANGOS SAVYBES AR FUNKCIJAS ARBA VISŲ AR BET KURIŲ FUNKCIJŲ AR TECHNOLOGIJŲ NAUDOJIMĄ „PASSWORD MANAGER“ PROGRAMINĖJE ĮRANGOJE BET KURIUO METU IŠ ANKSTO JŪSŲ NEPERSPĖJĘS.

JEIGU ŠIAME STRAIPSNYJE PATEIKTOS NUOSTATOS DĖL KOKIŲ NORS PRIEŽASČIŲ ANULIUOJAMOS ARBA TEIKĖJAS LAIKOMAS ATSAKINGU UŽ PRARADIMUS, PAŽEIDIMUS IR T. T. PAGAL TAIKYTINUS ĮSTATYMUS, ŠALYS SUTINKA, KAD TEIKĖJO ATSAKOMYBĖ JUMS RIBOJASI VISA JŪSŲ UŽ LICENCIJAS SUMOKĖTA SUMA.

JŪS SUTINKATE APSAUGOTI, GINTI IR LAIKYTI NEATSAKINGAIS TEIKĖJĄ IR JO DARBUOTOJUS, DUKTERINES ĮMONES, FILIALUS, PERPARDAVINĖTOJUS IR KITUS PARTNERIUS NUO BET KOKIŲ IR VISŲ TREČIŲJŲ ŠALIŲ (ĮSKAITANT ĮRENGINIŲ SAVININKUS ARBA ŠALIS, KURIŲ TEISES PAŽEIDĖ DUOMENYS, NAUDOJAMI „PASSWORD MANAGER“ PROGRAMINĖJE ĮRANGOJE ARBA SAUGYKLOJE) PRETENZIJŲ, ATSAKOMYBIŲ, PAŽEIDIMŲ, PRARADIMŲ, KAINŲ, IŠLAIDŲ, MOKESČIŲ, KURIUOS ŠIOS ŠALYS GALI PATIRTI DĖL JŪSŲ NAUDOJIMOSI „PASSWORD MANAGER“ PROGRAMINE ĮRANGA.

3. Duomenys „Password Manager“ programinėje įrangoje. Jeigu kitaip ir aiškiai nepasirinkote kitaip, visi jūsų įvesti duomenys, kurie yra saugomi „Password Manager“ programinės įrangos duomenų bazėje, yra laikomi užšifruotu formatu jūsų kompiuteryje, arba kitame, jūsų nurodytame saugojimo įrenginyje. Jūs suprantate, kad panaikinus arba sugadinus bet kurią „Password Manager“ programinės įrangos duomenų bazę ar kitus failus, visi ten laikomi duomenys bus negrąžinamai prarasti, ir jūs suprantate bei prisiimate šią riziką. Tas faktas, kad jūsų asmeniniai duomenys yra laikomi užšifruotu formatu kompiuteryje, nereiškia, kad informacija negali būti pavogta arba netinkamai panaudota tų, kas sužinos pagrindinį slaptažodį arba gaus prieigą prie kliento nustatyto aktyvinimo įrenginio duomenų bazei atidaryti. Jūsų pareiga užtikrinti visų prieigos būdų saugą.

4. Asmeninių duomenų persiuntimas teikėjui arba į saugyklą. Jeigu jūs tai pasirinkote, kad būtų užtikrintas savalaikis duomenų sinchronizavimas bei atsarginis kopijavimas, „Password Manager“ programinė įranga perduoda arba siunčia asmeninius duomenis iš „Password Manager“ programinės įrangos duomenų bazės – t. y. slaptažodžius, prisijungimo informaciją, paskyras ir tapatybes – internetu į saugyklą. Duomenys išskirtinai siunčiami užšifruota forma. Kai naudojate „Password Manager“ programinę įrangą interneto formoms su slaptažodžiais, prisijungimais ar kitais duomenimis užpildyti, ši informacija gali būti siunčiama internetu į jūsų nurodytą svetainę. Šio duomenų persiuntimo „Password Manager“ programinė įranga neinicijuoja, todėl teikėjas negali būti atsakingas už tokių veiksmų, atliekamų su įvairių teikėjų palaikomomis svetainėmis, saugą. Visos transakcijos internetu, susijusios ar nesusijusios su „Password Manager“ programine įranga, yra atliekamos jūsų nuožiūra bei rizika ir tik jūs būsite atsakingas už visus jūsų kompiuterio sistemos pažeidimus ar duomenų praradimą dėl bet kokios tokios medžiagos ar paslaugos atsisiuntimo ir (arba) naudojimo. Kad būtų sumažinta vertingų duomenų praradimo rizika, teikėjas rekomenduoja klientams periodiškai kurti duomenų bazės ir kitų svarbių failų atsargines kopijas išoriniuose diskų įrenginiuose. Teikėjas negali suteikti jums jokios pagalbos atkuriant prarastus ar pažeistus duomenis. Jeigu teikėjas teikia vartotojui duomenų bazės failų atsarginio kopijavimo paslaugas, sugadinus arba panaikinus šiuos failus vartotojų kompiuteriuose, šiai atsarginio kopijavimo paslaugai nesuteikiama jokia garantija ir neužtraukia teikėjui jokios atsakomybės.

Naudodami „Password Manager“ programinę įrangą jūs sutinkate, kad programinė įranga gali kartais susisiekti su teikėjo serveriais, kad patikrintų licencijos informaciją, galimas pataisas, pakeitimų paketus ir kitus naujinimus,

kurie gali pagerinti, tvarkyti, keisti arba patobulinti „Password Manager“ programinės įrangos veikimą. Programinė įranga gali siųsti bendrą sistemos informaciją, susijusią su „Password Manager“ programinės įrangos veikimu.

5. Pašalinimo informacija ir instrukcijos. Prieš pašalinant „Password Manager“ programinę įrangą, visą informaciją, kurią gavote iš duomenų bazės, reikia eksportuoti.

Papildomos nuostatos dėl „Password Manager“ programinės įrangos taikomos tik „ESET Smart Security Premium“ galutiniams naudotojams.

ESET LiveGuard. „ESET LiveGuard“ taikomos papildomos nuostatos:

Programinėje įrangoje yra galutinio naudotojo pateiktų failų papildomos analizės funkcija. Teikėjas naudoja tik Galutinio naudotojo pateiktus failus ir analizės rezultatus laikydamasis Privatumo politikos ir atitinkamų teisės aktų.

Papildomos nuostatos dėl „ESET LiveGuard“ taikomos tik „ESET Smart Security Premium“ galutiniams naudotojams.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Privatumo politika

Asmens duomenų apsauga ypač svarbi ESET, spol. s r. o., kurios registruota buveinė yra Einsteinova 24, 851 01 Bratislava, Slovak Republic, užregistruota prekybos registre, kurį administruoja Bratislavos I apylinkės teismo, Sro skyrius, įrašo Nr., 3586/B, įmonės registracijos numeris 31333532 kaip duomenų valdytojas (toliau – ESET arba „mes“). Norime laikytis skaidrumo reikalavimo, teisiškai standartizuoto pagal ES bendrąjį duomenų apsaugos reglamentą (BDAR). Šią privatumo politiką skelbiame tam, kad pasiektume šį tikslą ir informuotume savo klientą (toliau – „galutinis naudotojas“ arba „jūs“), kaip duomenų subjektą, toliau nurodytomis su asmens duomenų apsauga susijusiomis temomis:

- Asmens duomenų tvarkymo teisinis pagrindas,
- Duomenų bendrinimas ir konfidencialumas,
- Duomenų saugumas,
- Jūsų, kaip duomenų subjekto, teisės,
- Jūsų asmens duomenų tvarkymas
- Kontaktinė informacija.

Asmens duomenų tvarkymo teisinis pagrindas

Tvarkome duomenis remdamiesi tik keletu teisinių pagrindų, laikydamiesi su asmens duomenų apsauga susijusios teisės aktų sistemos. Asmens duomenų tvarkymas ESET iš esmės yra būtinas Galutinio vartotojo licencijos sutartį (GNLS) su galutiniam naudotoju (BDAR 6 straipsnio 1 dalies b punktas), kuris taikomas ESET produktams ar paslaugoms teikti, nebent aiškiai nurodyta kitaip, pvz.:

- Teisėto intereso teisinis pagrindas (BDAR 6 straipsnio 1 dalies f punktas), leidžiantis tvarkyti duomenis, susijusius su tuo, kaip mūsų klientai naudojasi mūsų Paslaugomis, ir jų pasitenkinimu, kad suteiktume savo

naudotojams geriausią apsaugą, palaikymą ir patirtį, kurią galime pasiūlyti. Teisėtu interesu pagal taikytinus teisės aktus pripažįstama net rinkodara, todėl tuo remdamiesi palaikome ryšius su savo klientais rinkodaros srityje.

- Sutikimas (BDAR 6 straipsnio 1 dalies a punktas), kurio mes galime jūsų prašyti konkrečiais atvejais, kai manome, kad šis teisinis pagrindas yra tinkamiausias, arba jei to reikalaujama pagal teisę.

- Teisinio įsipareigojimo (BDAR 6 straipsnio 1 dalies c punktas), kuriuo nustatomi reikalavimai dėl elektroninių ryšių, sąskaitų faktūrų išrašymo ir atsiskaitymo, vykdymas.

Duomenų bendrinimas ir konfidencialumas

Nebendriname jūsų duomenų su trečiosiomis šalimis. Tačiau ESET yra įmonė, veikianti visame pasaulyje per asocijuotąsias įmones ar susijusius partnerius, kurie priklauso mūsų prekybos, paslaugų ir palaikymo tinklo. ESET tvarkoma licencijavimo, sąskaitų faktūrų išrašymo ir techninės pagalbos informacija gali būti perduodama susijusiems subjektams ar partneriams arba perduodama jų, kad būtų galima vykdyti GNLS, pavyzdžiui, teikti paslaugas arba palaikymą.

ESET pageidauja tvarkyti duomenis Europos Sąjungoje (ES). Tačiau, atsižvelgiant į jūsų buvimo vietą (naudojimąsi mūsų produktais ir (arba) paslaugomis už ES ribų) ir (arba) jūsų pasirinkta paslauga, gali prireikti perkelti jūsų duomenis į šalį, nepriklausančią ES. Pavyzdžiui, debesijos kompiuterijos srityje naudojamės trečiųjų šalių paslaugomis. Tokiais atvejais kruopščiai atrenkame savo paslaugų teikėjus ir užtikriname tinkamą duomenų apsaugos lygį taikydami sutartines, technines ir organizacines priemones. Paprastai susitariame dėl ES standartinių sutarčių sąlygų, jei reikia, su papildomomis sutarčių taisyklėmis.

Kai kurioms ES nepriklausančioms šalims, pavyzdžiui, Jungtinei Karalystei ir Šveicarijai, ES jau nustatė panašų duomenų apsaugos lygį. Dėl palyginamo duomenų apsaugos lygio duomenų perdavimui į šias šalis nereikia jokio specialaus leidimo ar susitarimo.

Duomenų saugumas

ESET įgyvendina tinkamas technines ir organizacines priemones, užtikrinančias galimą riziką atitinkantį saugumo lygį. Mes darome viską, kad užtikrintume nuolatinį tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą. Tačiau jei duomenų saugumo pažeidimas kelia pavojų jūsų teisėms ir laisvėms, esame pasirengę pranešti atitinkamai priežiūros institucijai ir paveiktiems galutiniams naudotojams bei duomenų subjektams.

Duomenų subjekto teisės

Kiekvieno galutinio naudotojo teisės yra svarbios ir norėtume jus informuoti, kad visi galutiniai naudotojai (iš bet kurios ES ar bet kurios ES nepriklausančios šalies) turi toliau nurodytas ESET garantuojamas teises. Norėdami pasinaudoti savo duomenų subjekto teisėmis, galite susisiekti su mumis užpildę pagalbos formą arba el. paštu dpo@eset.sk. Identifikavimo tikslais prašome jūsų pateikti šią informaciją: Vardą ir pavardę, el. pašto adresas ir, jei yra, licencijos raktą arba kliento numerį ir įmonės priklausomybę. Prašome nesiųsti mums jokių kitų asmens duomenų, pvz., gimimo datos. Norėtume atkreipti dėmesį į tai, jog tam, kad galėtume tvarkyti jūsų prašymą, taip pat identifikavimo tikslais tvarkysime jūsų asmens duomenis.

Teisę atšaukti sutikimą. Teisė atšaukti sutikimą taikoma tuo atveju, kai duomenų tvarkymas grindžiamas tik sutikimu. Jei jūsų asmens duomenis tvarkome remdamiesi jūsų sutikimu, turite teisę bet kuriuo metu atšaukti sutikimą nenurodydami priežasčių. Jūsų sutikimo atšaukimas galioja tik ateityje ir neturi įtakos iki atšaukimo tvarkomų duomenų teisėtumui.

Teisę nesutikti. Teisė nesutikti su duomenų tvarkymu taikoma tuo atveju, kai duomenų tvarkymas grindžiamas teisėtu ESET arba trečiosios šalies interesu. Jei jūsų asmens duomenis tvarkome, kad apsaugotume teisėtą interesą, jūs, kaip duomenų subjektas, turite teisę bet kuriuo metu nesutikti su mūsų įvardytu teisėtu interesu ir jūsų asmens duomenų tvarkymu. Jūsų prieštaravimas galioja tik ateityje ir neturi įtakos iki prieštaravimo tvarkomų duomenų teisėtumui. Jei jūsų asmens duomenis tvarkome tiesioginės rinkodaros tikslais, nebūtina nurodyti prieštaravimo priežasčių. Tai taip pat taikoma profiliavimui tiek, kiek jis susijęs su tokia tiesiogine rinkodara. Visais kitais atvejais prašome trumpai informuoti mus apie savo skundus dėl teisėto ESET intereso tvarkyti jūsų asmens duomenis.

Atkreipkite dėmesį, kad kai kuriais atvejais, nepaisant jūsų sutikimo atšaukimo, turime teisę toliau tvarkyti jūsų asmens duomenis remdamiesi kitu teisiniu pagrindu, pvz., sutarties vykdymo tikslais.

Prieigos teisę. Kaip duomenų subjektas, turite teisę bet kuriuo metu nemokamai gauti informaciją apie ESET saugomus jūsų duomenis.

Teisę ištaisyti. Jei netyčia tvarkome neteisingus jūsų asmens duomenis, turite teisę juos ištaisyti.

Teisę ištrinti ir teisę apriboti tvarkymą. Kaip duomenų subjektas, turite teisę prašyti pašalinti asmens duomenis arba apriboti jų tvarkymą. Jei jūsų asmens duomenis tvarkome, pavyzdžiui, jums sutikus, jūs atšaukiate savo sutikimą ir nėra jokio kito teisinio pagrindo, pavyzdžiui, sutarties, mes nedelsdami pašaliname jūsų asmens duomenis. Jūsų asmens duomenys taip pat bus pašalinti, kai tik pasibaigus saugojimo laikotarpiui jie nebebus reikalingi nurodytiems tikslams.

Jei jūsų asmens duomenis naudosime tik tiesioginės rinkodaros tikslais ir jūs atšaukėte savo sutikimą arba išreiškėte prieštaravimą pagrindiniam teisėtam ESET interesui, apribosime jūsų asmens duomenų tvarkymą tiek, kiek įtrauksime jūsų kontaktinius duomenis į savo vidaus juodąjį sąrašą, kad išvengtume nepageidaujamo kontakto. Priešingu atveju jūsų asmens duomenys bus pašalinti.

Atkreipkite dėmesį, kad iš mūsų gali būti pareikalauta saugoti jūsų duomenis iki saugojimo įsipareigojimų ir įstatymų leidėjo ar priežiūros institucijų nustatytų terminų pabaigos. Saugojimo įsipareigojimai ir laikotarpiai taip pat gali atsirasti dėl Slovakijos teisės aktų. Po to atitinkami duomenys bus reguliariai pašalinami.

Teisę į duomenų perkeliamumą. Džiaugiamės galėdami jums, kaip duomenų subjektui, pateikti ESET tvarkomus asmens duomenis xls formatu.

Teisę pateikti skundą. Kaip duomenų subjektas, turite teisę pateikti skundą priežiūros institucijai. ESET taikomi Slovakijos įstatymai, ir, kadangi priklausome Europos Sąjungai, esame saistomi jos duomenų apsaugos teisės aktų. Atitinkama duomenų priežiūros institucija yra Slovakijos Respublikos asmens duomenų apsaugos tarnyba, įsikūrusi Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Jūsų asmens duomenų tvarkymas

ESET paslaugos, įdiegtos mūsų produkte, yra teikiamos pagal EULAsąlygas, tačiau kai kurioms iš jų gali reikėti ypatingo dėmesio. Norėtume suteikti jums daugiau informacijos apie duomenų rinkimą, susijusį su mūsų teikiamomis paslaugomis. Teikiame įvairias paslaugas, aprašytas GNLS ir produkto dokumentuose. Kad visos jos veiktų, turime rinkti arba turėti prieigą prie šios informacijos:

Licencijavimo ir sąskaitų faktūrų išrašymo duomenys. Vardą ir pavardę, el. pašto adresą, licencijos raktą ir (jei taikoma) adresą, įmonės priklausomybės ir mokėjimo duomenis renka ir tvarko ESET, kad palengvintų licencijos aktyvinimą, licencijos rakto pristatymą, priminimus apie galiojimo pabaigą, palaikymo užklausas, licencijos tikrumo patikrinimą, mūsų paslaugų ir kitų pranešimų, įskaitant rinkodaros pranešimus, teikimą pagal galiojančius teisės aktus arba jūsų sutikimą. ESET teisiškai privalo saugoti sąskaitų faktūrų išrašymo informaciją 10 metų, tačiau

licencijavimo informacija bus anonimizuota ne vėliau kaip per 12 mėnesių nuo licencijos galiojimo pabaigos.

Atnaujinimas ir kita statistika. Tvarkoma informacija apima informaciją apie diegimo procesą ir jūsų kompiuterį, įskaitant platformą, kurioje įdiegtas mūsų produktas, ir informaciją apie mūsų produktų operacijas ir funkcionalumą, pvz., operacinę sistemą, aparatinės įrangos informaciją, diegimo ID, licencijos ID, IP adresą, MAC adresą, produkto konfigūracijos nustatymus, kurie tvarkomi teikiant atnaujinimo ir naujovinimo paslaugas ir techninės priežiūros tikslais, saugumą ir mūsų vidinės infrastruktūros tobulinimą.

Ši informacija yra atskirta nuo identifikavimo informacijos, reikalingos licencijavimo ir sąskaitų faktūrų išrašymo tikslais, nes nereikalaujama galutinio naudotojo identifikavimo. Saugojimo laikotarpis yra iki 4 metų.

Reputacijos sistema **ESET LiveGrid®.** Vienakryptės maišos, susijusios su įsiskverbimu, tvarkomos ESET LiveGrid® reputacijos sistemos tikslais, o tai pagerina mūsų apsaugos nuo kenkėjiškų programų sprendimų efektyvumą, lyginant nuskaitytus failus su į baltąjį sąrašą įtrauktų ir į juodąjį sąrašą įtrauktų elementų duomenų baze debesyje. Šio proceso metu galutinio naudotojo tapatybė nenustatoma.

Atgalinio ryšio sistema **ESET LiveGrid®.** Įtartini pavyzdžiai ir metaduomenys iš nevaldomo aplinkos yra reputacija grindžiamos sistemos „ESET LiveGrid®“ dalis, kuri suteikia ESET galimybę nedelsiant reaguoti į mūsų galutinių naudotojų poreikius ir į naujausias grėsmes. Mums būtini jūsų

- Įsiskverbimai, pvz., galimų virusų ir kitų kenkėjiškų programų pavyzdžiai bei kiti įtartini, problemiški, galimai nepageidaujami ir galimai nesaugūs objektai, pvz., vykdomieji failai, el. laiškai, kuriuos jūs arba mūsų produktas laiko brukalu;

- Informacija, susijusi su interneto naudojimu, pvz., IP adresas ir geografinė informacija, IP paketai, URL ir interneto kadrai;

- Strigčių atminties failai ir jų informacija.

Mes nenorime rinkti jokių kitų jūsų duomenų, tačiau kartais to išvengti neįmanoma. Atsitiktinai surinkti duomenys gali būti įtraukti į pačią kenkėjišką programinę įrangą (surinktą be jūsų žinios arba pritarimo) arba į jos failo pavadinimą arba URL, todėl mes nesiekiame, kad jie būtų mūsų sistemose arba tvarkyti jų šioje privatumo politikoje nurodytu tikslu.

Visa informacija, gauta ir tvarkoma naudojant atgalinio ryšio sistemą „ESET LiveGrid®“, turi būti naudojama nenustačius galutinio naudotojo tapatybės.

Prie tinklo prijungtų įrenginių saugos vertinimas. Norėdami pateikti saugumo vertinimo funkciją, apdorojame vietinio tinklo pavadinimą ir informaciją apie vietinio tinklo įrenginius, pvz., vietinio tinklo įrenginio buvimą, rūšį, pavadinimą, IP adresą ir MAC adresą, susijusius su licencijos informacija. Informacija taip pat apima maršrutizatoriaus įrenginių belaidžio tinklo saugos tipą ir belaidžio tinklo šifravimo tipą. Licencijos informacija, pagal kurią galima nustatyti galutinio naudotojo tapatybę, bus anonimizuota ne vėliau kaip per 12 mėnesių nuo licencijos galiojimo pabaigos.

Techninė pagalba. Palaikymo paslaugoms teikti gali reikėti jūsų palaikymo užklausose esančios kontaktinės ir licencijavimo informacijos ir duomenų. Remdamiesi jūsų pasirinktu susisiekimo su mumis kanalu, galime rinkti jūsų el. pašto adresą, telefono numerį, licencijos informaciją, produkto informaciją ir jūsų palaikymo atvejo aprašymą. Kad būtų lengviau teikti palaikymo paslaugą, galite būti paprašyti pateikti kitą informaciją. Techninės pagalbos tikslais tvarkomi duomenys saugomi 4 metus.

Apsauga nuo netinkamo duomenų naudojimo. Jei ESET HOME paskyra sukuriama adresu https://home.eset.com ir galutinis naudotojas aktyvina funkciją dėl kompiuterio vagystės, bus renkama ir tvarkoma ši informacija: vietos duomenys, ekrano kopijos, duomenys apie kompiuterio konfigūraciją ir kompiuterio kameros įrašyti duomenys.

Surinkti duomenys saugomi mūsų serveriuose arba mūsų paslaugų teikėjų serveriuose ir jų saugojimo laikotarpis yra 3 mėnesiai.

Password Manager Jei pasirinksite aktyvinti funkciją „Password Manager“, duomenys, susiję su jūsų prisijungimo duomenimis, bus saugomi užšifruota forma tik jūsų kompiuteryje ar kitame nurodytame įrenginyje. Jei aktyvinate sinchronizavimo paslaugą, užšifruoti duomenys saugomi mūsų serveriuose arba mūsų paslaugų teikėjų serveriuose, kad būtų užtikrintas paslaugos teikimas. Nei ESET, nei paslaugų teikėjas neturi prieigos prie užšifruotų duomenų. Tik jūs turite raktą duomenims iššifruoti. Išaktyvinus funkciją, duomenys bus pašalinti.

ESET LiveGuard. Jei pasirinksite aktyvinti funkciją ESET LiveGuard, reikės pateikti pavyzdžių, pvz., galutinio naudotojo iš anksto nustatytus ir pasirinktus failus. Nuotolinei analizei parinkti pavyzdžiai bus nusiųsti į ESET tarnybą, o analizės rezultatas bus nusiųstas atgal į jūsų kompiuterį. Visi įtartini pavyzdžiai tvarkomi atgalinio ryšio sistemos ESET LiveGrid® surinktos informacijos būdu.

Tobulinimo pagal naudotojų patirtį programa. Jei pasirinkote aktyvinti Tobulinimo pagal naudotojų patirtį programa , anoniminė telemetrijos informacija, susijusi su mūsų produktų naudojimu, bus renkama ir naudojama atsižvelgiant į jūsų sutikimą.

Atkreipkite dėmesį, kad jei mūsų produktais ir paslaugomis besinaudojantis asmuo nėra galutinis naudotojas, įsigijęs produktą ar paslaugą ir su mumis sudaręs galutinio naudotojo licencijos sutartį (pvz., galutinio naudotojo darbuotojas, šeimos narys ar asmuo, kitaip galutinio naudotojo įgaliotas naudotis produktu ar paslauga pagal GNLS, duomenys tvarkomi atsižvelgiant į teisėtą ESET interesą, kaip apibrėžta BDAR 6 straipsnio 1 dalies f punkte, kad galutinio naudotojo įgaliotas naudotojas galėtų naudotis mūsų pagal teikiamais produktais ir paslaugomis pagal GNLS.

Kontaktinė informacija

Jei norėtumėte pasinaudoti savo, kaip duomenų subjekto, teise arba jei turite klausimų ar problemų, atsiųskite mums pranešimą šiuo adresu:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk