ESET LiveGuard Advanced

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

Copyright ©2024 ESET, spol. s r. o.

ESET LiveGuard Advanced bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukovaná žiadnym prostriedkom ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti ESET, spol. s r. o.

ESET, spol. s r. o. si vyhradzuje právo zmeny programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 31.1.2024

1 Úvod ... 1
2 Predstavenie produktu ... 2
2.1 Ako fungujú detekčné vrstvy ... 4
2.2 Požiadavky a podporované produkty ... 10
2.3 Používanie proxy s ESET LiveGuard Advanced ... 12
2.3 Apache HTTP Proxy ... 13
2.3 Konfigurácia proxy na systéme Linux ... 14
2.3 Konfigurácia proxy na systéme Windows ... 16
3 Ako si službu zakúpiť ... 19
4 Aktivácia ESET LiveGuard Advanced ... 20
4.1 Importovanie licencií do EBA ... 21
4.2 Synchronizácia EBA s ESET PROTECT On-Prem ... 22
4.3 Pridanie licencie do ESET MSP Administrator ... 25
4.4 Synchronizácia ESET MSP Administrator s ESET PROTECT On-Prem ... 30
4.5 Aktivácia na skupine počítačov ... 33
4.6 Aktivácia na vybraných počítačoch ... 38
4.7 Vzdialená inštalácia a aktivácia ... 40
5 Ako zapnúť a nakonfigurovať službu ESET LiveGuard Advanced ... 43
5.1 Konfigurácia bezpečnostného produktu ESET ... 43
5.2 Správa politík ... 46
6 Používanie ESET LiveGuard Advanced ... 49
6.1 ESET Mail Security ... 51
6.2 ESET Endpoint Security a ESET Server Security ... 55
6.3 ESET Cloud Office Security ... 59
6.4 Proaktívna ochrana ... 61
6.5 Zoznam odoslaných súborov ... 64
6.6 Vytvorenie reportu ... 68
6.7 Výsledok analýzy ... 72
6.7 Správa o aktivite súboru ... 74
6.8 Manuálne odoslanie súboru na analýzu ... 75
6.8 Odoslanie súboru prostredníctvom ESET PROTECT On-Prem ... 76
6.8 Odoslanie súboru prostredníctvom ESET Endpoint Security ... 77
6.8 Odoslanie súboru prostredníctvom ESET Server Security ... 78
6.8 Odoslanie súboru prostredníctvom ESET Mail Security ... 80
6.9 Vytvorenie vylúčenia ... 81
6.10 Použitie vylúčení pre zvýšenie výkonu ... 84
6.10 Kontrolný zoznam odoslaných súborov ... 84
6.10 Vylúčenie priečinkov ... 91
6.10 Vylúčenie procesu ... 95
6.10 Zistenie počtu odoslaných súborov ... 97
6.11 Oznámenia o detegovaných hrozbách ... 101
7 Najčastejšie otázky ... 103
8 Test fungovania služby ESET LiveGuard Advanced ... 106
9 Riešenie problémov ... 109
9.1 Diagnostika ... 116
9.2 Riešenie problémov s Apache HTTP Proxy ... 120
10 Zabezpečenie ESET LiveGuard Advanced ... 122
11 Zásady férového používania ... 126
12 Zásady ochrany osobných údajov ... 127

13 Podmienky používania 130
13.1 ESET Management Agent – Licenčná dohoda s koncovým používateľom 133
13.2 Dohoda o spracúvaní údajov 140
13.3 Štandardné zmluvné doložky 142

Úvod

Vitajte v používateľskej príručke pre ESET LiveGuard Advanced. Cieľom tohto dokumentu je priblížiť vám správu a používanie produktu ESET LiveGuard Advanced. Podrobne popísané je tu aj prepojenie medzi ESET LiveGuard Advanced a inými bezpečnostnými produktmi ESET určenými pre firemných zákazníkov.

Používame jednotný súbor symbolov na zvýraznenie tém, ktoré sú obzvlášť dôležité alebo inak významné. Táto príručka je rozdelená na niekoľko kapitol a podkapitol. Konkrétne informácie môžete vyhľadať pomocou vyhľadávacieho poľa v hornej časti.

Online pomocník je hlavným zdrojom pomocného obsahu. Pri pripojení na internet je zobrazovaná vždy najnovšia verzia Online pomocníka.

- Databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najrýchlejší nástroj na riešenie rozličných druhov problémov.

- ESET fórum poskytuje používateľom produktov spoločnosti ESET jednoduchý spôsob, ako získať pomoc a zároveň pomôcť iným. Môžete tam uverejniť akúkoľvek otázku alebo sa informovať o akomkoľvek probléme v súvislosti s produktmi spoločnosti ESET.

- V rámci Online pomocníka môžete odoslať svoje hodnotenie alebo poskytnúť spätnú väzbu na konkrétnu kapitolu. Kliknite na odkaz Zanechajte nám spätnú väzbu a následne môžete pridať hodnotenie či komentár.

V tejto používateľskej príručke môžete nájsť nasledujúce informačné polia:

Poznámky môžu poskytovať cenné informácie, ako napríklad špecifické funkcie alebo odkaz na súvisiacu kapitolu.

Takéto informácie si vyžadujú vašu pozornosť a neodporúča sa ich ignorovať. Zvyčajne ide o podstatné informácie, hoci nie sú mimoriadne závažné.

Upozornenia obsahujú mimoriadne dôležité informácie, pri ktorých by ste mali spozornieť. Upozornenia sú umiestnené tak, aby vás včas varovali a zároveň vám pomohli predísť chybám, ktoré by mohli mať negatívne následky. Prosím, dôkladne si prečítajte text ohraničený týmto označením, pretože sa týka vysoko citlivých systémových nastavení alebo upozorňuje na riziká.

Takto označený text poskytuje ukážkový príklad, ktorý priamo súvisí s informáciami v príslušnej kapitole. Príklady sa využívajú hlavne pri komplikovanejších kapitolách.

Použité štýly textu

Konvencia	Význam
Bold type	Pomenúva položky rozhrania, ako napr. polia a tlačidlá možností.
Code	Príklady kódov alebo príkazov.

Konvencia	Význam
Hyperlink	Poskytuje rýchly a jednoduchý prístup k súvisiacim prepojeným kapitolám alebo externým webovým lokalitám. Hypertextové prepojenia sú zvýraznené modrou farbou a môžu byť podčiarknuté.
%ProgramFiles%	Systémový adresár Windows, kde sú uložené programy systému Windows.

Predstavenie produktu

Popis služby

ESET LiveGuard Advanced je platená služba poskytovaná spoločnosťou ESET. Vytvára ďalšiu vrstvu ochrany, ktorá bola navrhnutá s cieľom chrániť pred úplne novými hrozbami.

Zmena názvu služby

23. marca 2022 došlo k zmene názvu služby ESET Dynamic Threat Defense na ESET LiveGuard Advanced. V rámci firemných produktov ESET službu nájdete aj pod názvom ESET LiveGuard. Oba názvy sa vzťahujú na rovnakú službu.

Dostupnosť služieb

ESET Status Portal poskytuje aktuálne informácie o dostupnosti služieb ESET. Poskytuje prehľad o službách spoločnosti ESET a reporty o stave služieb vrátane minulých incidentov. Ak máte ako používateľ akékoľvek problémy s používanou službou ESET a ESET Status Portal ich neuvádza, kontaktujte technickú podporu spoločnosti ESET.

Fungovanie

Podozrivé vzorky, ktoré ešte neboli potvrdené ako škodlivé a potenciálne by mohli prenášať malvér, sú automaticky odosielané do cloudu ESET na analýzu. Odoslané vzorky sú spúšťané v testovacom izolovanom priestore (tzv. sandboxe) a sú vyhodnocované prostredníctvom našich pokročilých detekčných techník. Škodlivé vzorky a podozrivé spamové e□maily sa posielajú do systému ESET LiveGrid®. Prílohy e□mailov sa spracúvajú samostatne a zasielajú sa do ESET LiveGuard Advanced. Správcovia alebo používatelia môžu nastaviť, aké súbory sa budú odosielať na analýzu, ako aj obdobie, počas ktorého sa budú súbory uchovávať v cloude ESET. Dokumenty a súbory PDF s aktívnym obsahom (makrá, javascript) sa na základe predvolených nastavení neodosielajú. Pozrite si podrobnosti o tom, ako fungujú detekčné vrstvy.

V konzole na vzdialenú správu v sekcii **Odoslané súbory** má správca k dispozícii stručnú správu o aktivite analyzovanej vzorky pre každý odoslaný súbor. Ak sa ukáže, že súbor je škodlivý, bude blokovaný ako podozrivý objekt u všetkých používateľov, ktorí sú zapojení do systému ESET LiveGrid®. V prípade, že je súbor vyhodnotený ako podozrivý, na základe nastavenia prahu citlivosti môže byť zablokovaný na všetkých zariadeniach v rámci danej organizácie.

Súbory môžu byť na analýzu odosielané manuálne alebo automatiky na základe nastavení v rámci politiky. Prostredníctvom ESET PROTECT Web Console môže používateľ odoslať súbory .exe nahlásené z klientskych zariadení.

Aký je rozdiel medzi ESET LiveGuard Advanced, ESET LiveGrid® a ESET Threat Intelligence?

Architektúra

Bezpečnostné produkty ESET a konzola na správu

Pri každom odoslaní vzorky na analýzu do služby ESET LiveGuard Advanced sa metadáta o tejto vzorke nahrajú do konzoly na správu (ak sa klient dokáže spojiť so serverom). Správca konzoly tak má k dispozícii zoznam všetkých vzoriek odoslaných do cloudu ESET.

Bezpečnostné produkty ESET a ESET LiveGuard Advanced

Ak aktivovaný a nakonfigurovaný bezpečnostný produkt ESET vyhodnotí, že vzorku je potrebné podrobiť analýze, odošle ju do ESET LiveGuard Advanced. Po vykonaní analýzy vzorky ESET LiveGuard Advanced odošle výsledok na všetky zariadenia v príslušnej spoločnosti (alebo u MSP zákazníka) a takisto všetkým spoločnostiam, ktoré niekedy v minulosti odoslali daný súbor. Bezpečnostný produkt následne vykoná akciu podľa nastavení v príslušnej politike. V produktoch ESET pre koncové zariadenia a servery si od verzie 7.2 môžete nastaviť akciu, ktorá sa vykoná s podozrivými súbormi sťahovanými prostredníctvom internetových prehliadačov alebo e□mailových klientov.

S cieľom znížiť riziko útoku sú všetky prenášané dáta podpísané spoločnosťou ESET. Pri použití HTTP pripojenia v internej sieti produkt skontroluje, či došlo k zmene pripojenia za proxy serverom na HTTPS. Ak proxy nie je správne nakonfigurované, HTTPS pripojenie bude použité aj v internej sieti.

Konzoly na správu produktov ESET a ESET LiveGuard Advanced

Služba ESET LiveGuard Advanced je dostupná v lokálnych aj cloudových konzolách na správu (ESET PROTECT On-Prem, ESET PROTECT). Keď ESET LiveGuard Advanced prijme vzorku z bezpečnostného produktu ESET, automaticky informuje konzolu na správu o stave analýzy. Po dokončení analýzy sa jej výsledok prenesie do konzoly na správu.

Mobilné klienty a ESET LiveGuard Advanced

Mobilný klient predstavuje akékoľvek klientske koncové zariadenie s nainštalovaným bezpečnostným produktom ESET, ktoré je mimo firemnej siete a nemá prístup k ESET PROTECT On-Prem (v angličtine sa takéto zariadenie označuje ako „Roaming Endpoint“). Najčastejšie ide o zariadenie, ktoré má zamestnanec doma alebo na služobnej ceste bez VPN. Mobilné klienty využívajú všetky výhody ESET LiveGuard Advanced, avšak neinformujú ESET PROTECT On-Prem o vzorkách odoslaných na analýzu. Keď sa však toto klientske zariadenie opäť pripojí do firemnej siete a nainštalovaný Agent sa pripojí k ESET PROTECT On-Prem Serveru, metadáta klientskeho zariadenia sa zosynchronizujú a dôjde k aktualizácii zoznamu odoslaných súborov. Ostatné klientske zariadenia vo vašej sieti dostanú informácie o výsledku analýzy novej hrozby, ktorá sa objavila u klienta pohybujúceho sa mimo siete, dokonca ešte pred jeho synchronizáciou s ESET PROTECT On-Prem.

ESET Cloud Office Security a ESET LiveGuard Advanced

ESET LiveGuard Advanced analyzuje odoslané súbory spustením podozrivého kódu v izolovanom prostredí s cieľom vyhodnotiť jeho správanie. ESET Cloud Office Security odosiela podozrivé e□mailové prílohy a súbory zo služby Microsoft Exchange Online, úložiska OneDrive, skupín Teams a lokalít SharePoint na analýzu do služby ESET LiveGuard Advanced. ESET Cloud Office Security nevyžaduje ani neodosiela údaje do konzoly na správu produktov ESET. Informácie o odoslaných súboroch a výsledkoch ich analýzy sú k dispozícii v riešení ESET Cloud Office Security.

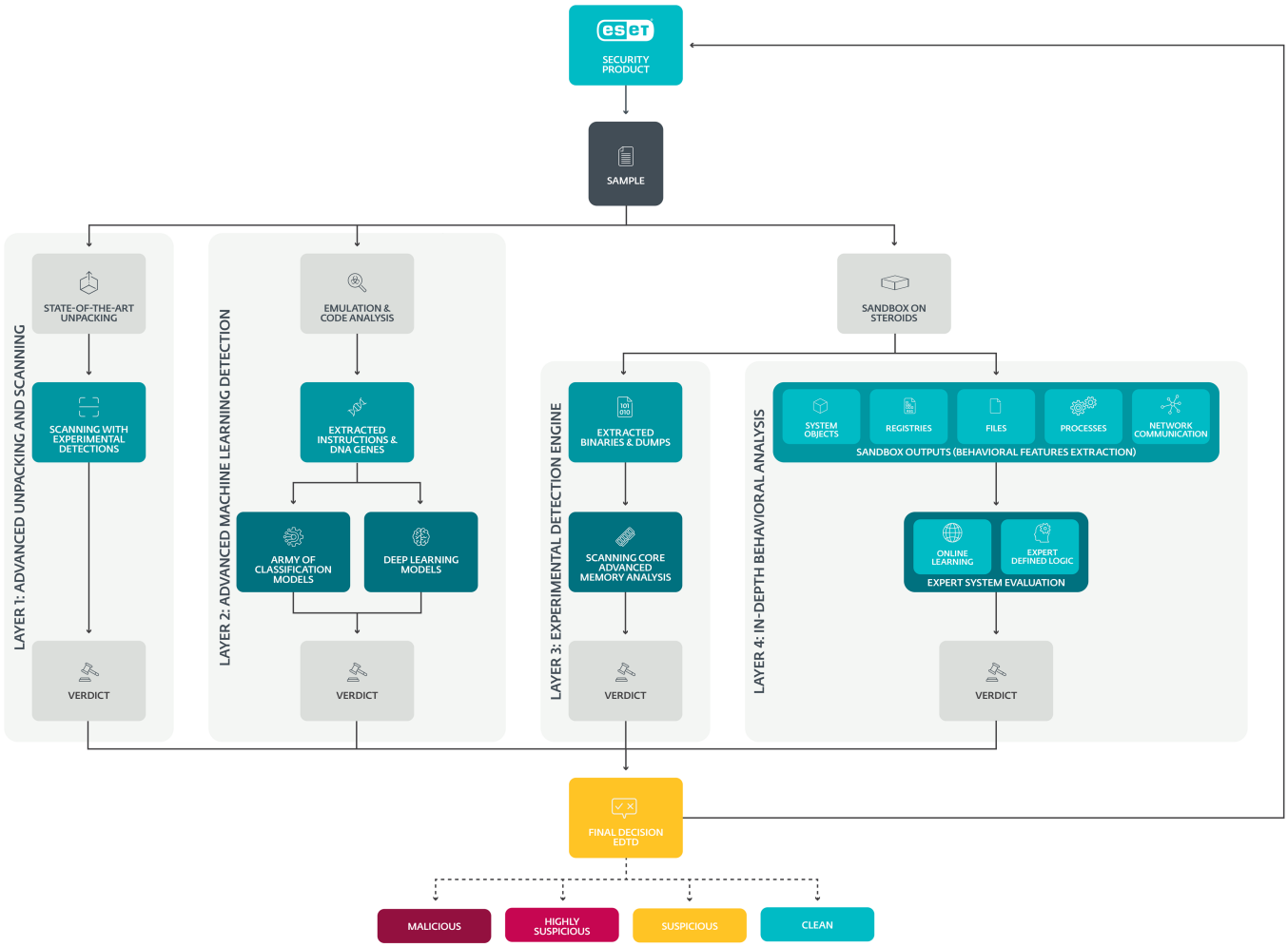
Globálna databáza

ESET LiveGuard Advanced využíva dve dátové centrá Azure (v USA a Európe) na ukladanie hash hodnôt súborov a výsledkov ich analýz. Dátové centrá poskytujú rýchlejšie výsledky pre už zanalyzované súbory. V sídle spoločnosti ESET, ktoré sa nachádza na Slovensku, sú uložené všetky odoslané súbory, kde následne dochádza k ich analýze. Údaje súvisiace s každým zákazníkom (alebo spoločnosťou) sú uchovávané osobitne v jednej globálnej databáze. ESET automaticky smeruje používateľa k najbližšiemu dátovému centru.

Dôrazne odporúčame používať Proxy na ukladanie odpovedí zo serverov ESET do vyrovnávacej pamäte. V sieťach s veľkým počtom klientskych zariadení (100 a viac) tak môžete výrazne znížiť množstvo prenášaných dát.
Môžete vylúčiť označené priečinky a procesy pre zníženie počtu odosielaných súborov a zlepšenie celkového výkonu.

Ako fungujú detekčné vrstvy

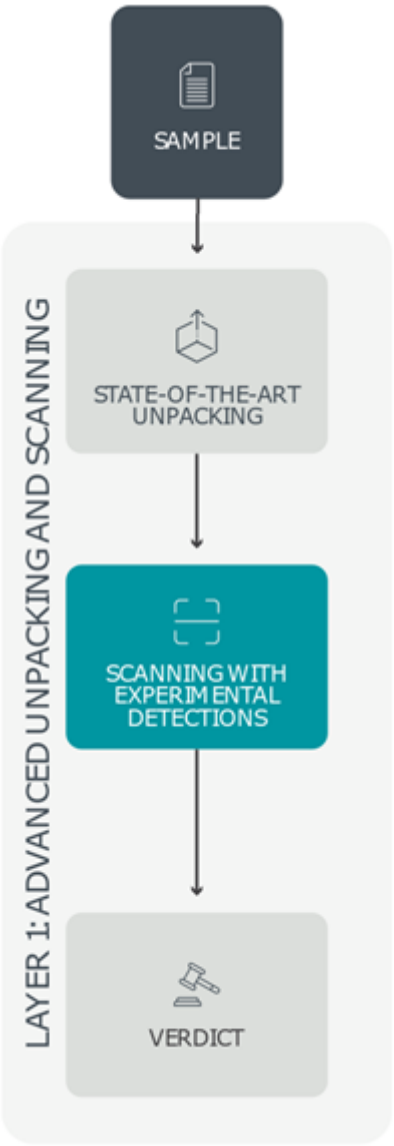
ESET LiveGuard Advanced využíva štyri samostatné detekčné vrstvy na zabezpečenie najvyššej možnej účinnosti detekcie. Každá vrstva analyzuje vzorku iným spôsobom a poskytuje vlastný výstup. Konečné hodnotenie je výsledkom všetkých zhromaždených informácií o vzorke. Prehľad celého procesu nájdete nižšie:



Kliknutím na obrázok ho zobrazíte v plnej veľkosti.

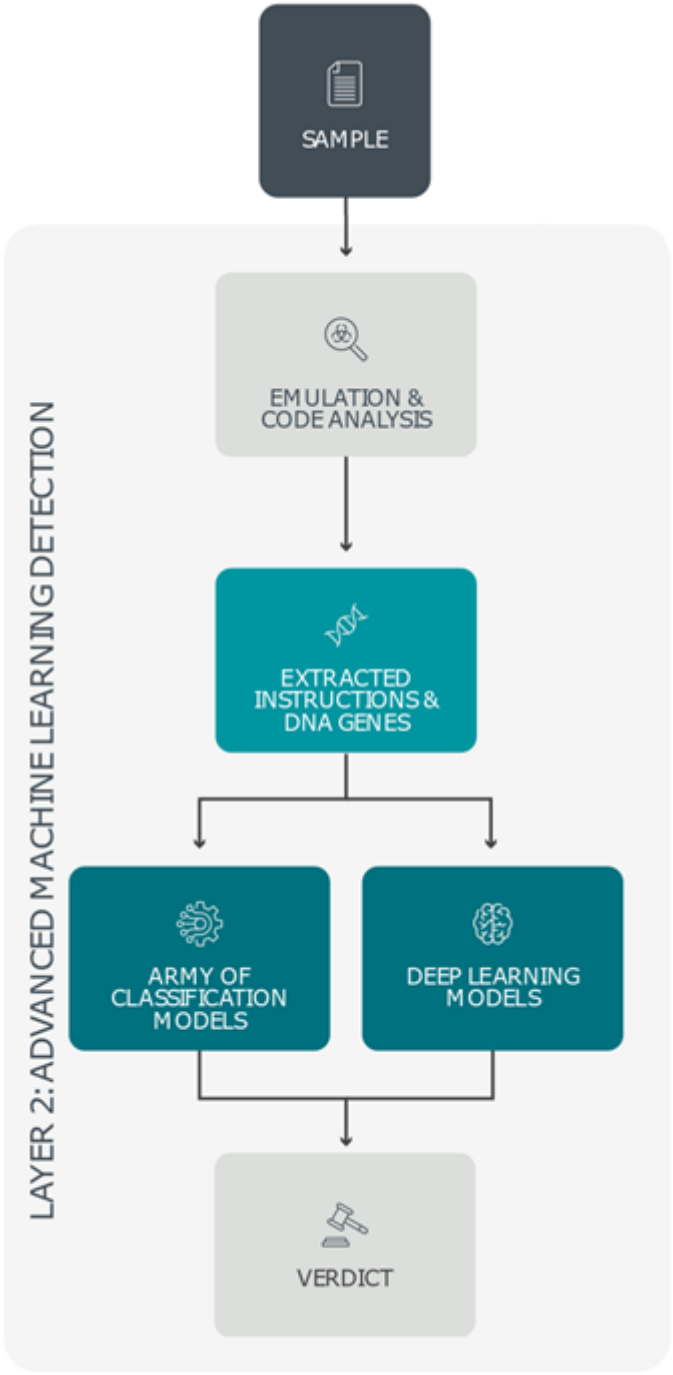
Vrstva č. 1: Pokročilá extrakcia a kontrola

Po vstupe do počiatočnej vrstvy produktu ESET LiveGuard Advanced, tzv. vrstvy pokročilej extrakcie a kontroly, sa statické vzorky porovnávajú s databázou hrozieb spoločnosti ESET, ktorá je doplnená aj o experimentálne a ešte nezverejnené detekcie. Rovnako sa porovnávajú aj s komplexným zoznamom neškodných, potenciálne nechcených (PUA) a potenciálne nebezpečných (PUsA) položiek. Malvér sa často snaží zabrániť detekcii tým, že svoje škodlivé jadro skrýva pod niekoľkými ochrannými vrstvami, preto je pre správnu analýzu potrebné ich odstrániť. ESET LiveGuard Advanced na to využíva práve detekčnú vrstvu pokročilej extrakcie a kontroly s použitím vysoko špecializovaných nástrojov založených na tzv. packeroch, ktoré výskumníci spoločnosti ESET našli v škodlivom kóde. Tieto špecializované nástroje na extrakciu odstraňujú ochrannú vrstvu malvéru, aby ESET LiveGuard Advanced mohol následne opätovne porovnať vzorku s databázou hrozieb doplnenou aj o dosiaľ nezverejnené detekcie. Vrstva pokročilej extrakcie a kontroly klasifikuje vzorku ako malvér, neškodnú, potenciálne nechcenú (PUA) alebo potenciálne nebezpečnú (PUsA) položku. Vzhľadom na bezpečnostné riziká a hardvérové nároky spojené s nástrojmi na extrakciu a ďalšími súvisiacimi postupmi je nevyhnutnosťou vysoko výkonné a bezpečné prostredie. Toto jedinečné prostredie zabezpečuje robustná a odolná cloudová infraštruktúra produktu ESET LiveGuard Advanced.



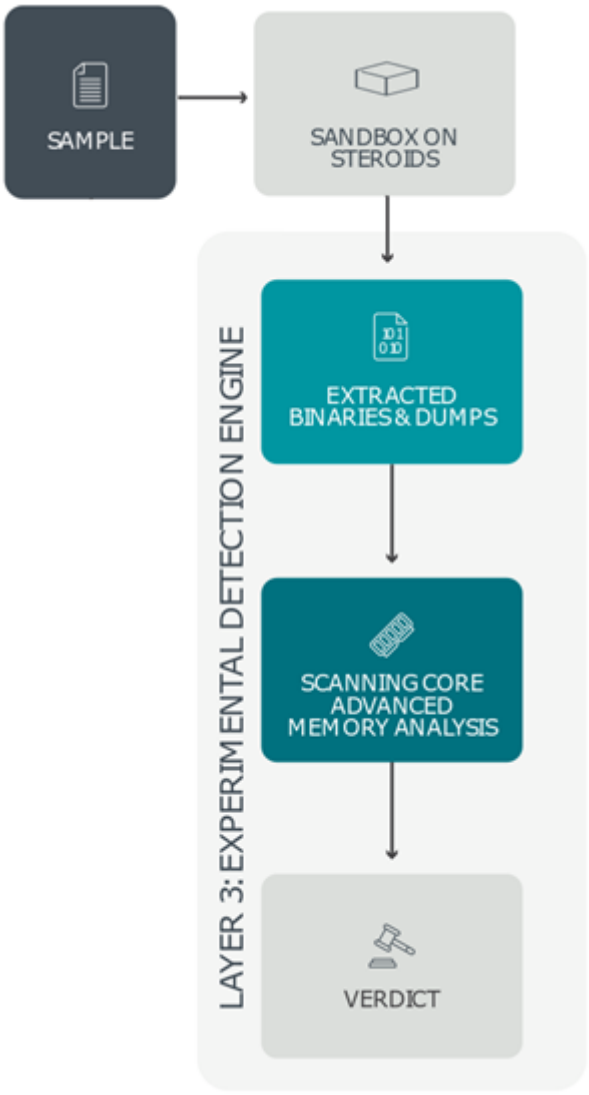
Vrstva č. 2: Detekcia pokročilého strojového učenia

Každá položka odoslaná do ESET LiveGuard Advanced je tiež podrobená statickej analýze prostredníctvom detekcie s využitím pokročilého strojového učenia, vďaka čomu možno získať základné vlastnosti vzorky. Keďže analýza skomprimovaného alebo zašifrovaného kódu bez ďalšieho spracovania by viedla len k pokusu o klasifikáciu dátového šumu bez relevantného výsledku, odoslaná položka sa súčasne podrobí ďalšej, dynamickejšej analýze, ktorá extrahuje jej inštrukcie a gény DNA. Opisom aktívnych vlastností a aktivít vzorky sa dajú odhaliť škodlivé charakteristiky maskujúcich sa objektov alebo objektov skrytých pod ochrannými vrstvami, a to aj bez spustenia vzorky. Informácie získané z predošlých krokov sa ďalej spracujú pomocou celého radu starostlivo vybraných klasifikačných modelov a algoritmov hĺbkového učenia. Nakoniec sa všetky tieto informácie spoja prostredníctvom neurónovej siete, ktorá klasifikuje vzorku buď ako škodlivú, veľmi podozrivú, podozrivú alebo neškodnú. Ak sa táto alebo iná vrstva ESET LiveGuard Advanced nepoužije, zobrazí sa správa „Analýza nie je potrebná“. Vzhľadom na zložitosť a hardvérové nároky týchto postupov je potrebná výrazne výkonnejšia infraštruktúra, než akú poskytuje koncové zariadenie používateľa. Na zvládnutie výpočtovo náročných úloh inžinieri spoločnosti ESET vyvinuli špičkovú a komplexnú sústavu systémov – ESET LiveGuard Advanced.



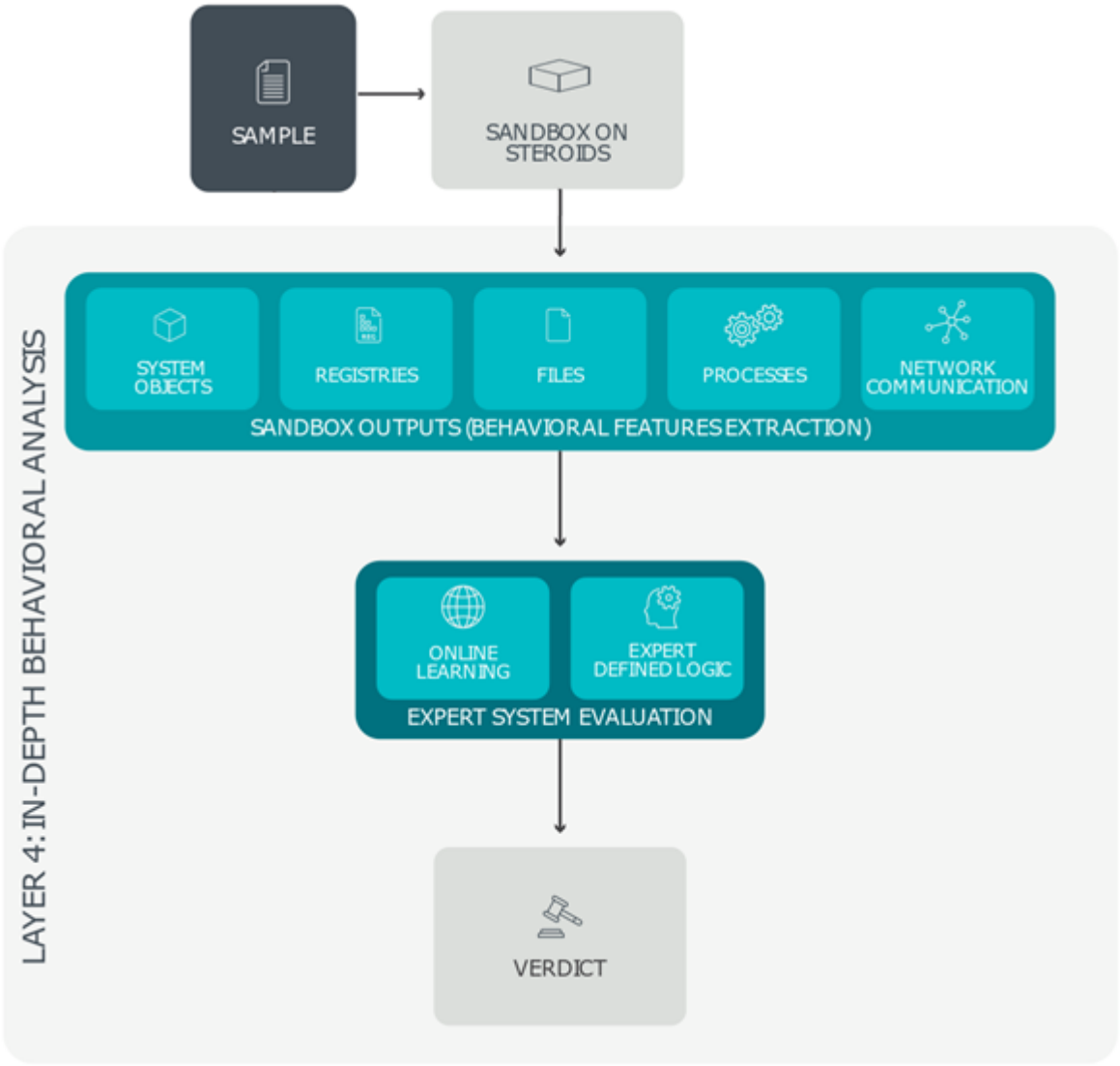
Vrstva č. 3: Experimentálne detekčné jadro

Na podrobnejší rozbor každej vzorky je potrebná hlbšia analýza jej aktivity, ktorá doplní predchádzajúce zistenia. Na zhromažďovanie tohto typu informácií o hrozbách slúži ďalšia detekčná vrstva ESET LiveGuard Advanced, konkrétne experimentálne detekčné jadro. Podozrivú položku vloží do sústavy presne nakonfigurovaných systémov, ktoré sú podobné skutočným používateľským zariadeniam s rôznymi operačnými systémami – ide o akýsi „sandbox na steroidoch“. Takéto vysoko kontrolované prostredia slúžia ako monitorovacie bunky vybavené skupinou detekčných algoritmov spoločnosti ESET, ktoré zaznamenávajú každú akciu. Experimentálne detekčné jadro vytvára na identifikáciu skrytého škodlivého správania aj veľké množstvo výpisov pamäte. Tie sú následne kontrolované a porovnávané s databázou hrozieb doplnenou o nezverejnené a experimentálne detekcie, ktorá zabezpečuje veľmi presné výsledky detekcie a extrémne nízky počet falošných poplachov. Informácie zozbierané prostredníctvom experimentálneho detekčného jadra sú tiež súčasťou komplexného zoznamu udalostí zachytených sandboxom. Zoznam sa následne vo finálnej detekčnej vrstve ESET LiveGuard Advanced použije na ďalšiu analýzu.



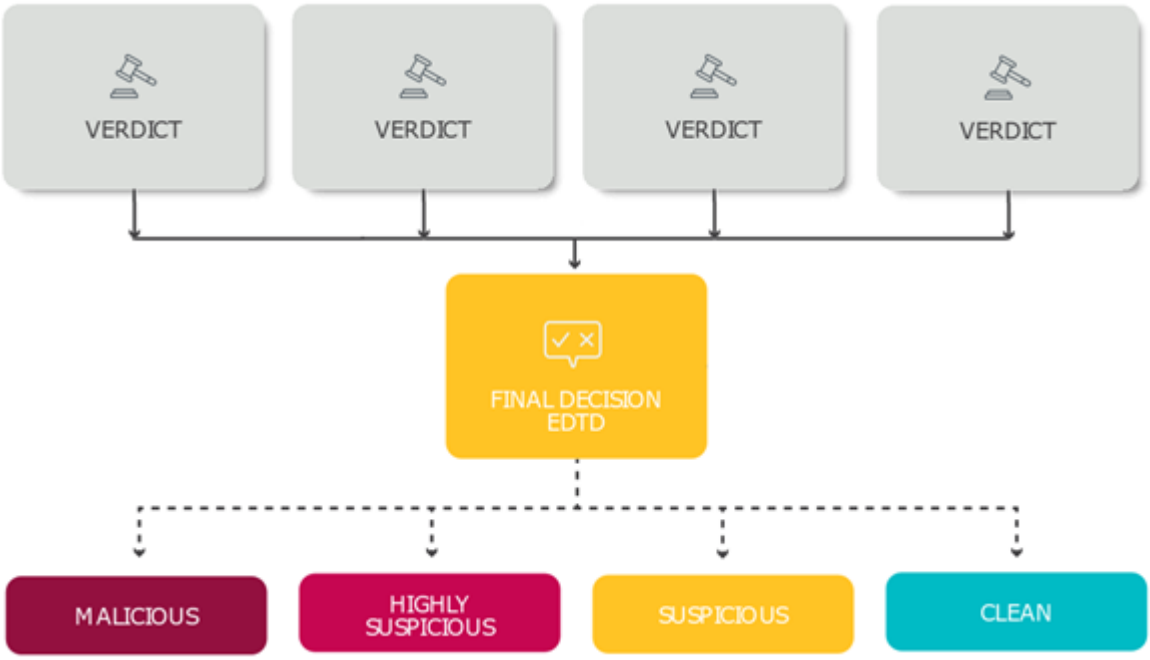
Vrstva č. 4: Hĺbková analýza aktivity

V poslednej detekčnej vrstve ESET LiveGuard Advanced, známej ako hĺbková analýza aktivity, sú všetky výstupy sandboxu – vrátane súborov vytvorených alebo odstránených z pevného disku, položiek pridaných alebo odstránených zo systémového registra Windows, všetkých pokusov o externú komunikáciu a spustených skriptov – podrobené dôkladnej analýze aktivity. V tejto fáze sa ESET LiveGuard Advanced zameriava na škodlivé a podozrivé akcie, ako sú pokusy o pripojenie na podozrivé webové lokality, používanie známych škodlivých objektov a používanie jedinečných reťazcov generovaných špecifickými rodinami malvéru. Hĺbková analýza aktivity tiež rozdeľuje výstupy zo sandboxu do logických blokov, ktoré sa potom porovnávajú s rozsiahlou a pravidelne kontrolovanou databázou predtým analyzovaných vzorcov a reťazcov akcií, aby sa identifikoval aj ten najmenší náznak škodlivého správania.



Konečný výsledok

ESET LiveGuard Advanced použije výsledky z jednotlivých detekčných vrstiev a na základe nich vyhodnotí stav vzorky. Výsledok je doručený bezpečnostnému produktu ESET na zariadení používateľa, odkiaľ bola vzorka odoslaná, ako aj všetkým zariadeniam v infraštruktúre daného zákazníka.



Požiadavky a podporované produkty

Požiadavky na používateľov lokálnych produktov

Pre správne fungovanie ESET LiveGuard Advanced musí vaše prostredie spĺňať nasledujúce požiadavky:

- aktívny účet ESET Business Account alebo ESET MSP Administrator synchronizovaný s konzolou na správu produktov ESET,
- podporovaná konzola na správu produktov ESET,
- nainštalované podporované bezpečnostné produkty ESET vo verzii 7.x alebo novšej,
- platná licencia na ESET LiveGuard Advanced,
- aktivované bezpečnostné produkty ESET s licenciou na ESET LiveGuard Advanced,
- zapnutá služba ESET LiveGuard Advanced v nastaveniach politík pre podporované bezpečnostné produkty ESET,
- sieťové požiadavky na otvorené porty, ktoré sú rovnaké ako pre ESET LiveGrid®.
- Ak používate Apache HTTP Proxy alebo ESET Bridge, sieťové požiadavky na otvorené porty sú rovnaké ako pre ESET LiveGrid®. Inak je port namiesto toho 443.
  - Prístup k online serverom ESET LiveGuard Advanced

Požiadavky na používateľov riešenia ESET Cloud Office Security

Ak chcete používať ESET LiveGuard Advanced v riešení ESET Cloud Office Security, potrebujete:

- aktívny účet ESET Business Account alebo ESET MSP Administrator prepojený s riešením ESET Cloud Office

Security,

- platnú licenciu na ESET LiveGuard Advanced.

ESET Cloud Office Security nezdieľa žiadne informácie o odoslaných súboroch s konzolami na správu produktov ESET.

Prístupové práva v rámci konzoly na správu

Zoznam odoslaných súborov a výsledky analýzy bude môcť vo Web Console vidieť iba používateľ s prístupovými právami k zariadeniu, ktoré vzorku na analýzu odoslalo. Z Web Console môžete manuálne odoslať na analýzu spustiteľný súbor nahlásený z ESET Inspect. Musíte mať pridelené povolenie na **použitie** pre počítač, ktorý danú detekciu nahlásil, a povolenie na **zápis** pre funkciu **Odoslať súbor do ESET LiveGuard** v rámci vašej domácej skupiny.

Mobilné klienty – ak ESET PROTECT Server nie je z klientskeho zariadenia dosiahnuteľný, no klient má prístup na servery cloudu ESET, informácie o súboroch odoslaných z tohto zariadenia budú v zozname viditeľné až po jeho opätovnom pripojení k Serveru.

Výkon

Na ukladanie výsledkov prichádzajúcich z ESET LiveGuard Advanced do vyrovnávacej pamäte môžete použiť ESET Bridge. Ukladanie do vyrovnávacej pamäte môže výrazne znížiť prenosové zaťaženie internetu v sieti.

V podnikovom prostredí (viac ako 1 000 spravovaných počítačov) odporúčame používať vyhradený ESET Bridge server. Ukladanie veľkého množstva súborov do vyrovnávacej pamäte by znížilo výkon servera. V prostrediach s vysokou dostupnosťou odporúčame nainštalovať každý komponent na osobitný počítač (ESET PROTECT Server, ESET Bridge, databázový server). Taktiež neodporúčame prevádzkovať na rovnakom počítači okrem ESET PROTECT On-Prem iné aplikácie náročné na prostriedky.

Ďalším spôsobom zvýšenia celkového výkonu je znížiť počet odosielaných súborov. Môžete vylúčiť súbory, priečinky alebo procesy a zabrániť tak odosielaniu súkromných súborov na analýzu, prípadne tým znížiť zaťaženie. Viac informácií nájdete v kapitole Použitie vylúčení pre zvýšenie výkonu.

Podporované licencie

ESET LiveGuard Advanced je možné aktivovať:

- ročnou, dvojročnou, trojročnou a predplatenou licenciou z účtu EBA,
- Predplatenými MSP licenciami z účtu ESET MSP Administrator.

Podporované produkty

Odosielanie súborov na analýzu do ESET LiveGuard Advanced je možné len z podporovaných produktov. Zoznam odoslaných súborov je dostupný len v podporovanej verzii konzoly na správu.

Bezpečnostné produkty

Produkt	Verzia
ESET Endpoint Antivirus pre Windows* ESET Endpoint Security for Windows	✓ verzia 7 a novšie
ESET Mail Security for Microsoft Exchange	✓ verzia 7 a novšie
ESET File Security pre Windows Server	✓ verzia 7.x
ESET Server Security for Windows Server (predtým ESET File Security pre Windows Server)	✓ verzia 8 a novšie
ESET Endpoint Antivirus for Linux	✓ verzia 8.1 a novšie
ESET Server Security for Linux	✓ verzia 8.1 a novšie
ESET Cloud Office Security	✓ (od decembra 2021)

* Služba ESET LiveGuard Advanced funguje rovnako pre ESET Endpoint Antivirus aj ESET Endpoint Security. V tejto používateľskej príručke sa z dôvodu zjednodušenia vždy odkazuje len na produkt ESET Endpoint Security. Inštrukciami pre ESET Endpoint Security uvedenými v tejto príručke by sa mali riadiť aj používatelia produktu ESET Endpoint Antivirus.

Konzoly na správu

Produkt a verzia	Podpora
ESET PROTECT On-Prem 8 a novšie verzie	✓
ESET Security Management Center 7.0 a 7.1	⛔ Podpora pre konzoly sa skončila.
ESET Security Management Center 7.2	⛔
ESET Remote Administrator 6.x a staršie verzie	⛔
ESET PROTECT	✓

Nepodporované operačné systémy
Služba ESET LiveGuard Advanced nie je podporovaná na klientskych pracovných staniciach s operačným systémom Windows XP a Microsoft Windows Server 2003. Tieto systémy nepodporujú protokol TLS 1.2, ktorý je nevyhnutný pre bezpečný transfer vzoriek.

Podporované proxy

ESET Bridge bolo vydané spolu s ESET PROTECT On-Prem 10.0 ako náhrada za Apache HTTP Proxy a je zahrnuté v All-in-one inštalátore konzoly na správu produktov. Môžete si ho tiež stiahnuť ako samostatný inštalátor z webovej stránky spoločnosti ESET. Apache HTTP Proxy bude stále funkčné, avšak odporúčame používať ESET Bridge.

Používanie proxy s ESET LiveGuard Advanced

ESET LiveGuard Advanced môže používať ESET Bridge na preposielanie komunikácie na servery spoločnosti ESET a ukladanie prenášaných dát do vyrovnávacej pamäte. Ukladanie dát do vyrovnávacej pamäte znižuje zaťaženie siete. Používať proxy je potrebné v prípade, ak klientsky počítač nemá priamy prístup na servery spoločnosti ESET. Ak používate ESET Bridge na preposielanie komunikácie medzi ESET PROTECT Serverom a ESET Management Agentmi, môžete použiť rovnaké proxy aj na ukladanie výsledkov prichádzajúcich z ESET LiveGuard Advanced do vyrovnávacej pamäte. ESET Bridge tiež podporuje proxy chaining.

> **Nastavenia proxy na klientskych počítačoch**
> Je potrebné nakonfigurovať proxy nastavenia (**Nastavenia** > **Nástroje** > **Proxy server**) v bezpečnostnom produkte ESET na klientskom počítači. Môžete to urobiť aj vzdialene prostredníctvom politiky.

Používatelia ESET PROTECT

Ak v jednej sieti (napríklad v jednej pobočke) máte aspoň 10 počítačov, mali by ste na ukladanie výsledkov detekcie do vyrovnávacej pamäte používať ESET Bridge. V prípade, že klientske počítače nezdieľajú internú sieť alebo VPN, proxy nepoužívajte. Viac informácií o ESET Bridge nájdete v dokumentácii k ESET PROTECT.

> **Používatelia Apache HTTP Proxy**
> Od verzie ESET PROTECT 4.0 a ESET PROTECT On-Prem 10.0 (vydané v novembri 2022) ESET Bridge nahrádza Apache HTTP Proxy. Služba Apache HTTP Proxy dosiahla úroveň obmedzenej podpory. Ak používate Apache HTTP Proxy, odporúčame vám prejsť na ESET Bridge.

Používatelia virtuálneho zariadenia ESET PROTECT

Zariadenie podporuje operačný systém CentOS 7, ktorý nie je podporovaný službou ESET Bridge. Používatelia virtuálneho zariadenia ESET PROTECT si môžu vybrať jedno z nasledujúcich riešení:

- Použiť ESET Bridge nainštalované na osobitnom počítači (pozrite si zoznam požiadaviek pre ESET Bridge).
- Použiť riešenie Apache HTTP Proxy, ktoré je súčasťou zariadenia.

Inštalácia ESET Bridge

ESET Bridge môžete nainštalovať niekoľkými spôsobmi. Odporúčame použiť najnovší All-in-one inštalátor pre ESET PROTECT.

Ukladanie výsledkov prichádzajúcich z ESET LiveGuard Advanced do vyrovnávacej pamäte

Služba ESET Bridge je správne nakonfigurovaná na ukladanie výsledkov do vyrovnávacej pamäte. Ukladanie výsledkov do vyrovnávacej pamäte sa začne po nakonfigurovaní ESET Bridge na používanie proxy riešenia na ukladanie do vyrovnávacej pamäte a po povolení ESET LiveGuard Advanced.

Apache HTTP Proxy

Odporúčanie

Služba Apache HTTP Proxy je funkčná, ale dosiahla úroveň obmedzenej podpory. Odporúčame vám používať ESET Bridge.

Konfiguračný súbor proxy

Na systémoch Linux a Windows majú konfiguračné súbory proxy odlišné umiestnenie – štandardné umiestnenie nájdete v tabuľke nižšie.

Operačný systém	Konfiguračné súbory
Windows	*C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
Linux (Debian distribúcia)	*/etc/apache2/mods-available/proxy.conf*
Virtuálne zariadenie (Linux)	*/etc/httpd/conf.d/proxy.conf*

Proxy chaining

Komunikáciu môžete smerovať aj na ďalšie podporované proxy. Na tento účel je potrebné do konfigurácie proxy pridať `ProxyRemote * AddressOfNextProxy`. Dané nastavenie musí byť použité pre všetky proxy, ktoré sa pripájajú na ďalšie proxy.

Nasleduje príklad, kde 10.1.1.2 je IP adresa ďalšieho (nadradeného) proxy:

```
ProxyRemote * http://10.1.1.2:3128
```

Na aplikovanie novej konfigurácie je potrebné reštartovať službu proxy.

Proxy tretích strán (nie Apache)

Proxy riešenia tretích strán nie sú podporované. Za určitých okolností síce ostatné proxy riešenia môžu fungovať, spoločnosť ESET však neposkytuje konfiguráciu ani podporu týkajúcu sa takýchto scenárov.

Riešenie problémov

Pre získanie podrobných protokolov z proxy zmeňte/pridajte parameter `LogLevel debug` do konfiguračného súboru a reštartujte príslušnú službu. Protokoly môžu byť užitočné pri hľadaní konkrétneho problému, prípadne môžu byť odoslané spoločnosti ESET pri poskytovaní pomoci.

Ak používate ESET LiveGuard Advanced v podnikovom prostredí (stovky a viac zariadení), odporúčame nasadiť HTTP Proxy na vyhradený samostatný server. Prevádzkovanie služby HTTP Proxy na intenzívne využívanom serveri (napr. popri ESET PROTECT Serveri alebo databáze) môže mať za následok problémy s ESET LiveGuard Advanced pripojením.
Môžete vylúčiť označené priečinky a procesy pre zníženie počtu odosielaných súborov a zlepšenie celkového výkonu.

Konfigurácia proxy na systéme Linux

Táto konfigurácia sa týka len Apache HTTP Proxy. Ak používate službu ESET Bridge, nakonfigurujte ju prostredníctvom ESET PROTECT Web Console.

Skontrolujte konfiguračný súbor proxy, či obsahuje nasledujúce riadky. Ak ich neobsahuje, pridajte ich.

1. Pre umožnenie ukladania do vyrovnávacej pamäte, pripojenia agenta, HTTPS pripojenia a zapisovania do protokolu pridajte do konfigurácie nasledujúce riadky:

```
CacheEnable disk http://
```

```
CacheDirLevels 4

CacheDirLength 2

CacheDefaultExpire 3600

CacheMaxFileSize 500000000

CacheMaxExpire 604800

CacheQuickHandler Off

CacheRoot /var/cache/httpd/proxy


AllowCONNECT 443 2222 53535


ProxyRequests On

ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900

SetEnv proxy-initial-not-pooled 1


ErrorLog "|/usr/sbin/rotatelogs -n 10 /var/log/httpd/error_log 1M"
```

Parametre `CacheRoot` a `ErrorLog` môžete v prípade potreby upraviť podľa svojho systému.

2. Pridajte nasledujúcu časť kódu za posledný riadok kódu uvedeného vyššie. Umožníte tým ukladanie komunikácie ESET LiveGuard Advanced do vyrovnávacej pamäte:

```
<VirtualHost *:3128>

 ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

        ServerName r.edtd.eset.com
```

```
        <If "%{REQUEST_METHOD} == 'CONNECT'">
           Require all denied
        </If>

        ProxyRequests Off
        CacheEnable disk /
        SSLProxyEngine On

        RequestHeader set Front-End-Https "On"
        ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
0 smax=10
        ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>
```

3. Uložte konfiguráciu a reštartujte službu proxy.

> **Zapnutie potrebných proxy režimov**
> Pri používaní vlastného Apache proxy na systéme Linux s ESET LiveGuard Advanced je potrebné zapnúť nasledujúce režimy: `headers ssl alias`.
> Napríklad, na Debian distribúciách použite tieto príkazy:
> 1.Pre načítanie modulu:
> `sudo a2enmod headers ssl alias`
>
> 2.Pre reštart služby:
> `service apache2 restart`

Konfigurácia proxy na systéme Windows

> Táto konfigurácia sa týka len Apache HTTP Proxy. Ak používate službu ESET Bridge, nakonfigurujte ju prostredníctvom ESET PROTECT Web Console.

Ak používate vlastné Apache HTTP Proxy na ukladanie súborov ESET LiveGuard Advanced do vyrovnávacej pamäte, je potrebné, aby ste si upravili svoj konfiguračný súbor *httpd.conf*. Tento súbor je zvyčajne umiestnený v Apache v priečinku *conf*.

Jednotlivé časti konfigurácie pridávajte v rovnakom poradí, v akom sú uvedené v tejto kapitole.

4. ESET LiveGuard Advanced vyžaduje, aby boli vo vašom proxy aktívne moduly SSL, headers a alias. Overte, či sú tieto moduly dostupné, a pridajte nasledujúce riadky do konfiguračného súboru pre načítanie potrebných

modulov:

```
LoadModule alias_module ..\modules\mod_alias.dll
LoadModule ssl_module ..\modules\mod_ssl.dll
LoadModule headers_module ..\modules\mod_headers.dll

<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

LoadModule proxy_module ..\modules\mod_proxy.dll
LoadModule proxy_http_module  ..\modules\mod_proxy_http.dll
LoadModule proxy_connect_module ..\modules\mod_proxy_connect.dll
LoadModule cache_module ..\modules\mod_cache.dll
LoadModule cache_disk_module ..\modules\mod_cache_disk.dll
```

5. Pre umožnenie ukladania do vyrovnávacej pamäte, pripojenia agenta, HTTPS pripojenia a zapisovania do protokolu pridajte do konfigurácie nasledujúce riadky:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off

AllowCONNECT 443 563 2222 8883

ProxyRequests On
```

```
ProxyVia On
SetEnv proxy-initial-not-pooled 1

ErrorLog "logs/error.log"
LogLevel warn
```

Parametre `ErrorLog` a `LogLevel` môžete v prípade potreby upraviť podľa svojho systému.

6. Pridajte nasledujúcu časť kódu za posledný riadok kódu uvedeného vyššie. Umožníte tým ukladanie dát ESET LiveGuard Advanced do vyrovnávacej pamäte:

```
AcceptFilter https none
AcceptFilter http none
EnableSendfile Off
EnableMMAP off

<VirtualHost *:3128>
 ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
        ServerName r.edtd.eset.com

        <If "%{REQUEST_METHOD} == 'CONNECT'">
           Require all denied
        </If>

        ProxyRequests Off
        CacheEnable disk /
        SSLProxyEngine On

        RequestHeader set Front-End-Https "On"
```

```
        ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
0 smax=10

        ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>
```

7. Uložte konfiguračný súbor a reštartujte službu proxy.

Zakúpenie služby

MSP používatelia

Licenciu ESET LiveGuard Advanced získate cez ESET MSP program.

> **ESET MSP Administrator vo verzii 1 nie je podporovaný.**
> Ak používate ESET MSP Administrator, uistite sa, že máte verziu 2 (portál dostupný na adrese msp.eset.com). Portál ESET MSP Administrator vo verzii 1 bol predtým dostupný na adrese ema.eset.com. Táto adresa je teraz presmerovaná na ESET MSP Administrator 2. Verzia 1 nepodporuje ESET LiveGuard Advanced.

Používatelia ESET Business Account

Zakúpte si licenciu od predajcu a pridajte ju do svojho účtu na portáli ESET Business Account. Váš ESET PROTECT On-Prem zosynchronizuje pridanú licenciu a je pripravený na používanie.

Používatelia ESET Cloud Office Security

Všetky licencie úrovne ESET Cloud Office Security obsahujú funkciu ESET LiveGuard Advanced. Vedľa ID licencie môžete vidieť označenie ESET LiveGuard. Ak máte samostatnú licenciu ESET Cloud Office Security, ESET ju automaticky zmigruje.

Vyskúšajte ESET LiveGuard Advanced zadarmo v ESET PROTECT

Používatelia ESET PROTECT si môžu pre produkt ESET LiveGuard Advanced vyžiadať bezplatnú 30-dňovú skúšobnú licenciu zo svojej cloudovej konzoly.

Kontaktujte nás

S otázkami týkajúcimi sa zakúpenia a licencovania produktu sa obráťte na obchodné oddelenie spoločnosti ESET. Technickú podporu spoločnosti ESET môžete kontaktovať e-mailom alebo telefonicky. Všetky kontakty nájdete na webovej stránke spoločnosti ESET.

Aktivácia ESET LiveGuard Advanced

Používatelia ESET Cloud Office Security

Funkcia ESET LiveGuard Advanced je súčasťou licencie ESET Cloud Office Security. ESET LiveGuard Advanced môžete povoliť vytvorením a priradením politík.

Používatelia ESET PROTECT On-Prem a ESET PROTECT

V závislosti od typu prostredia existuje viacero spôsobov, ako nasadiť ESET LiveGuard Advanced vo vašej sieti. Postupujte podľa nasledujúcich krokov:

I. Získajte licenciu pre ESET LiveGuard Advanced

- Používatelia ESET Business Account: Získajte licenciu pre ESET LiveGuard Advanced. Zakúpený licenčný kľúč vám bude zaslaný na vašu e-mailovú adresu.

- Používatelia ESET MSP Administrator: Svojmu zákazníkovi v účte ESET MSP Administrator priraďte licenciu na ESET LiveGuard Advanced.

II. Importujte licenciu

- Používatelia ESET Business Account: Zosynchronizujte ESET PROTECT On-Prem so svojím účtom EBA.

- Používatelia ESET MSP Administrator: Zosynchronizujte ESET PROTECT On-Prem so svojím účtom ESET MSP Administrator. (Používateľom ESET PROTECT sa cloudové licencie zosynchronizujú automaticky.)

ESET LiveGuard Advanced možno aktivovať len pomocou licencie z účtu EBA alebo ESET MSP Administrator.

III. Nainštalujte bezpečnostný produkt ESET

Vyberte zodpovedajúcu možnosť a postupujte podľa uvedených krokov:

Na svojich zariadeniach mám nainštalovaný a aktivovaný kompatibilný bezpečnostný produkt ESET

1. Spustite úlohu na aktiváciu so zvolenou licenciou pre ESET LiveGuard Advanced.
2. Vytvorte a priraďte politiky, v ktorých nastavíte zapnutie služby ESET LiveGuard Advanced.

Na svojich zariadeniach mám nainštalovaný len ESET Management Agent

Postupujte podľa pokynov uvedených v časti Vzdialená inštalácia a aktivácia.

Používam ESET PROTECT a na svojich zariadeniach nemám nainštalovaný žiadny produkt ESET

1.Pre inštaláciu agenta a bezpečnostného produktu na vaše koncové zariadenia postupujte podľa kapitoly Lokálne nasadenie.
2.Spustite úlohu na aktiváciu so zvolenou licenciou pre ESET LiveGuard Advanced.
3.Vytvorte a priraďte politiky, v ktorých nastavíte zapnutie služby ESET LiveGuard Advanced.

Používam ESET PROTECT On-Prem a na svojich zariadeniach nemám nainštalovaný žiadny produkt ESET

1.Pre inštaláciu agenta a bezpečnostných produktov na vaše koncové zariadenia postupujte podľa kapitoly Lokálne nasadenie.
2.Spustite úlohu na aktiváciu so zvolenou licenciou pre ESET LiveGuard Advanced.
3.Vytvorte a priraďte politiky, v ktorých nastavíte zapnutie služby ESET LiveGuard Advanced.

Importovanie licencií do EBA

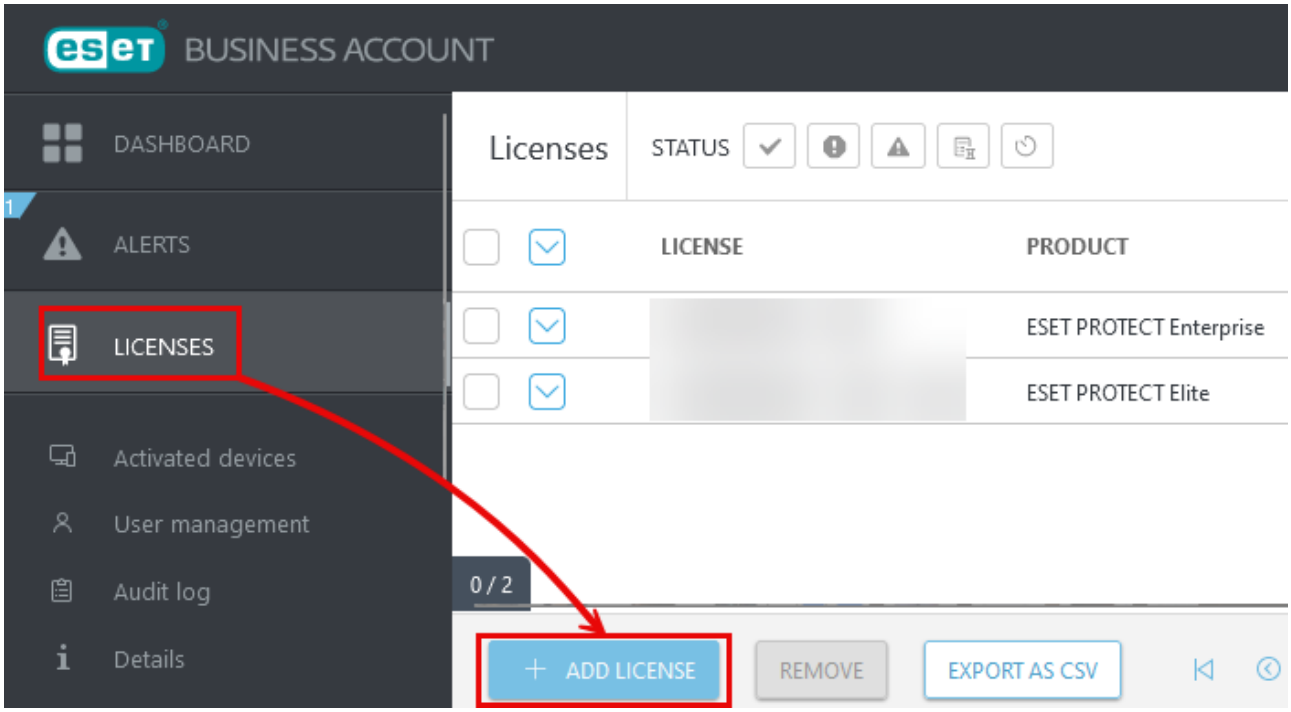
Požiadavky

- Používateľský účet EBA
- Licencia na ESET LiveGuard Advanced

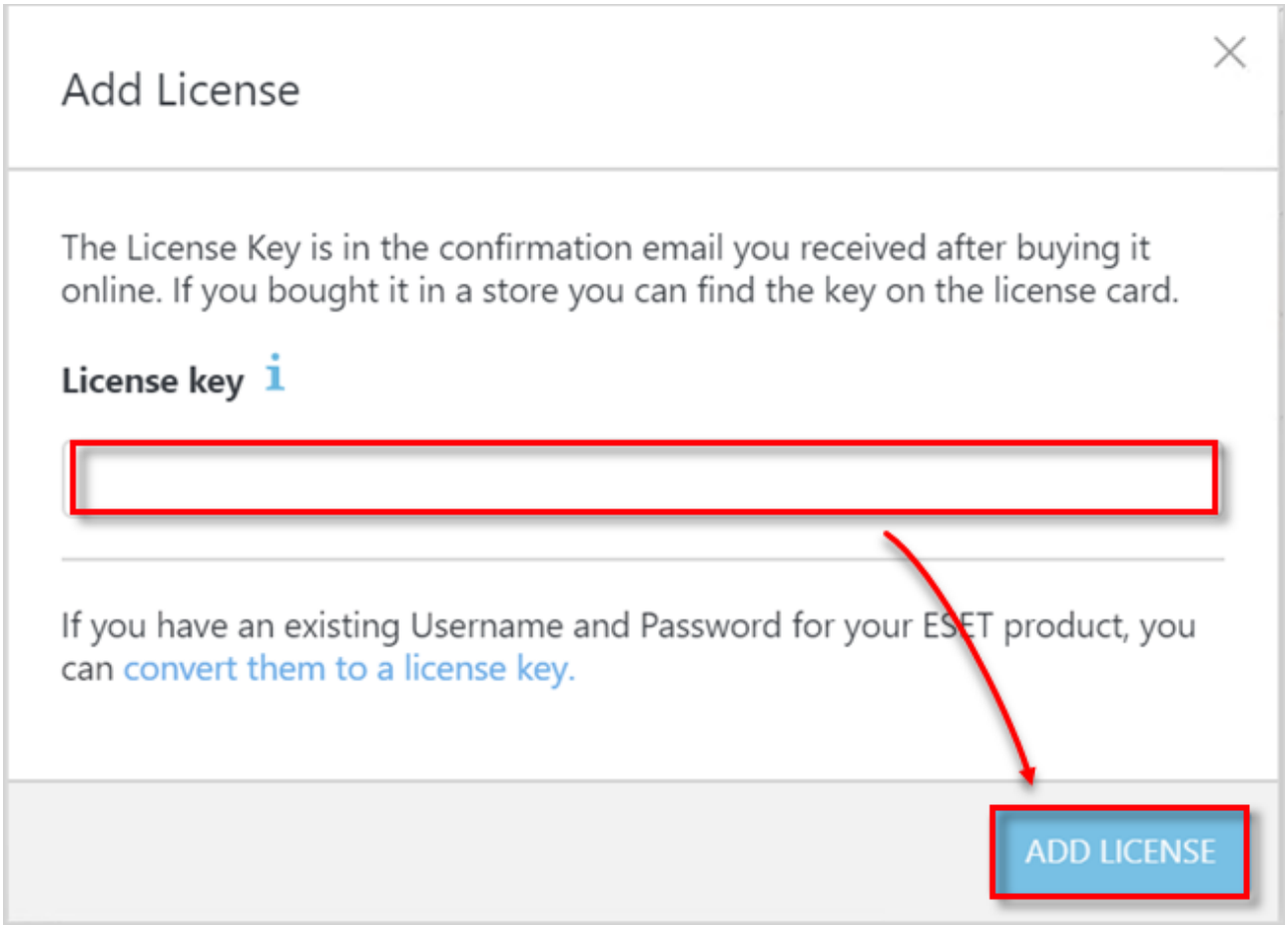
Importovanie

1.Prihláste sa do svojho účtu na portáli EBA.

2.Kliknite na **Licencie** > **Pridať licenciu** > **Licenčný kľúč**.



3.Zadajte svoj licenčný kľúč ESET LiveGuard Advanced a následne kliknite na **Pridať licenciu** pre naimportovanie licencie.



4.Odsúhlaste licenčnú dohodu s koncovým používateľom (EULA) v prípade, že s uvedenými podmienkami súhlasíte. Ak bol import úspešný, v zozname licencií sa zobrazí nová položka.

Licencia pre ESET LiveGuard Advanced môže byť súčasťou balíka obsahujúceho viacero produktov ESET alebo môže byť doplnená o licenčné jednotky umožňujúce využívať ESET LiveGuard Advanced s rôznymi produktmi ESET:

- ESET LiveGuard Advanced for ESET Endpoint Security
- ESET LiveGuard Advanced for ESET Server Security
- ESET LiveGuard Advanced for ESET Mail Security

Synchronizácia EBA s ESET PROTECT On-Prem

Požiadavky

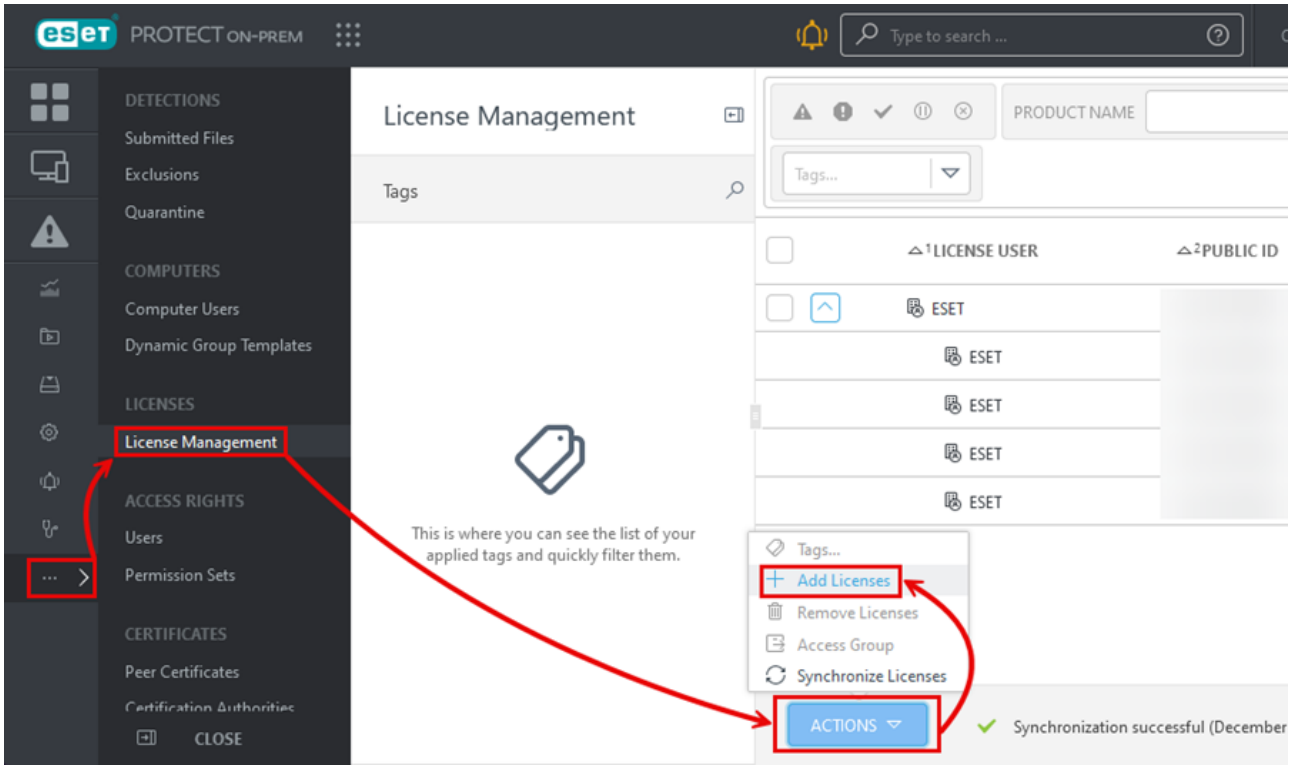
- Licenčný kľúč pre ESET LiveGuard Advanced importovaný do vášho účtu na portáli ESET Business Account (EBA)
- Nasadená konzola ESET PROTECT On-Prem
- Fungujúce spojenie medzi ESET PROTECT Serverom a portálom EBA

Ak už ste pridali svoj účet EBA do ESET PROTECT Web Console, v sekcii **Správa licencií** kliknite na možnosť **Synchronizovať**, čím manuálne vynútite aktualizáciu licenčných údajov vo Web Console. V tomto prípade nie je potrebné znovu zadávať prihlasovacie údaje do EBA.

Synchronizácia

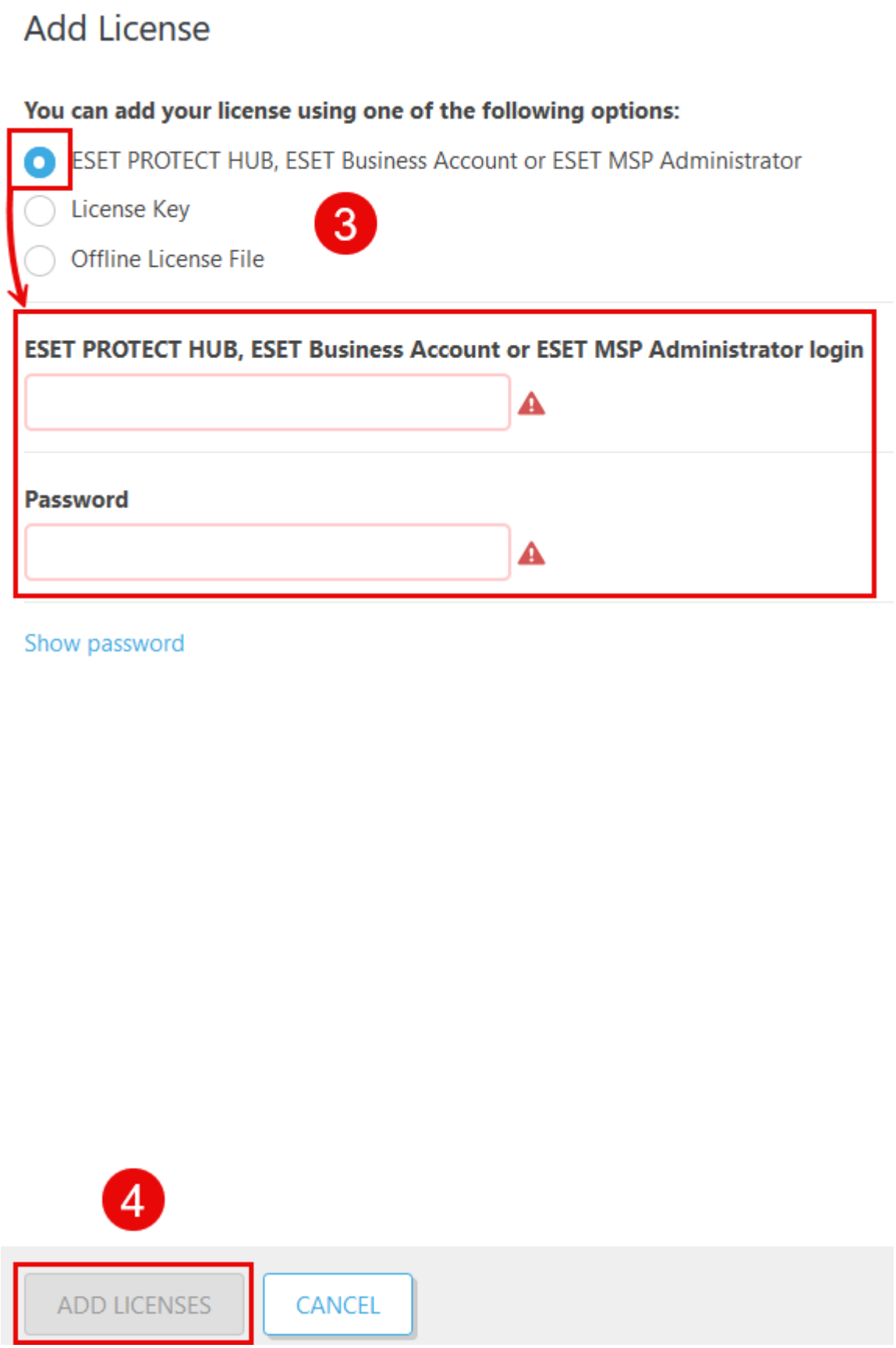
1.Prihláste sa do ESET PROTECT Web Console ako správca (účet Administrator) alebo pod iným používateľským účtom s dostatočnými prístupovými povoleniami.

2.Prejdite do sekcie **Viac** > **Správa licencií** > **Akcie** > **Pridať licenciu**.



3.Vyberte možnosť **Prihlasovacie údaje pre ESET Business Account alebo ESET MSP Administrator** a zadajte prístupové údaje k vášmu účtu na portáli EBA.

4.Kliknite na tlačidlo **Pridať licencie**, čím do ESET PROTECT On-Prem pridáte všetky licencie z vášho účtu.



Ak importujete licenčný kľúč pre ESET LiveGuard Advanced priamo do Web Console, zobrazí sa nasledujúce chybové hlásenie:
„Nepodarilo sa pridať licenciu pomocou licenčného kľúča: Licencia je vydaná pre produkt, ktorý nie je možné spravovať pomocou konzoly ESET PROTECT On-Prem. Zadajte inú licenciu, prosím.“
Licenciu pre ESET LiveGuard Advanced importujte vždy cez portál EBA alebo ESET MSP Administrator.

Pridanie licencie do ESET MSP Administrator

Portál ESET MSP Administrator poskytuje licenciu ESET LiveGuard Advanced, ktorá obsahuje licenčné jednotky pre:

- ESET LiveGuard Advanced pre Endpoint Security a Server Security
- ESET LiveGuard Advanced pre Mail Security

K dispozícii sú tiež úrovne licencií pre ESET PROTECT, ktoré obsahujú licenčné jednotky pre ESET LiveGuard Advanced:

- ESET PROTECT Complete
- ESET PROTECT Mail Plus
- ESET PROTECT Advanced

Overenie dostupnosti produktu ESET LiveGuard Advanced

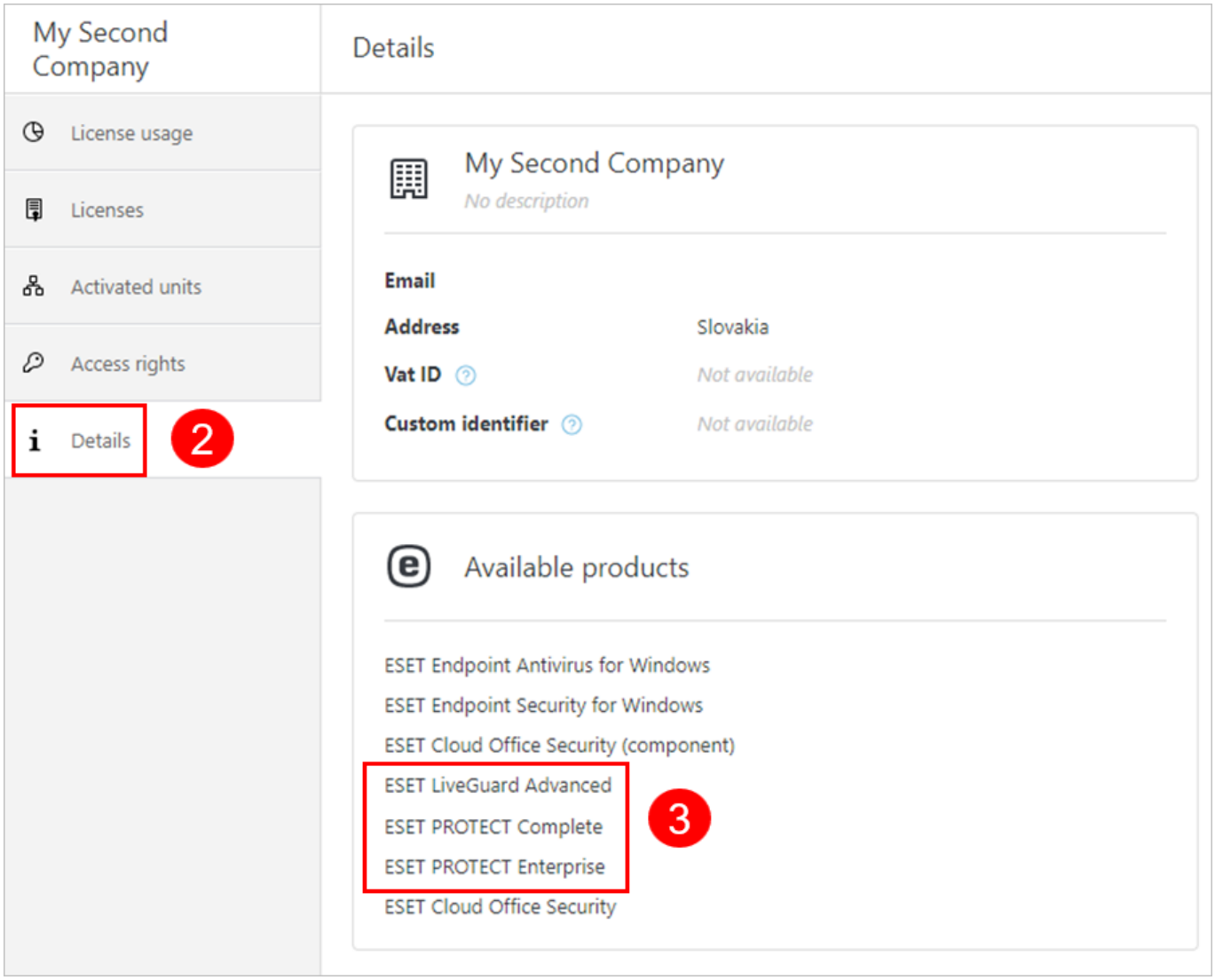
1. Prihláste sa do svojho účtu na portáli ESET MSP Administrator.

2. Kliknite na **Companies** (Spoločnosti), vyberte zákazníka a kliknite na **Details** (Podrobnosti).

3. V sekcii **Available products** (Dostupné produkty) nájdite **ESET LiveGuard Advanced** alebo úroveň zahŕňajúcu ESET LiveGuard Advanced.

Odsúhlasenie podmienok používania

Pred pridaním licencie je nutné na portáli ESET MSP Administrator odsúhlasiť Podmienky používania (pre ESET LiveGuard Advanced). Ak túto možnosť nemáte dostupnú, Podmienky používania musí odsúhlasiť nadradená spoločnosť, MSP manažér alebo používateľ s prideleným povolením na **Zápis** pre vašu spoločnosť.



Ak váš zákazník v sekcii **Available products** nemá dostupnú jednu z vhodných licenčných úrovní, musí ju do vášho účtu pridať distribútor (alebo MSP manažér).

Pridanie produktu ESET LiveGuard Advanced

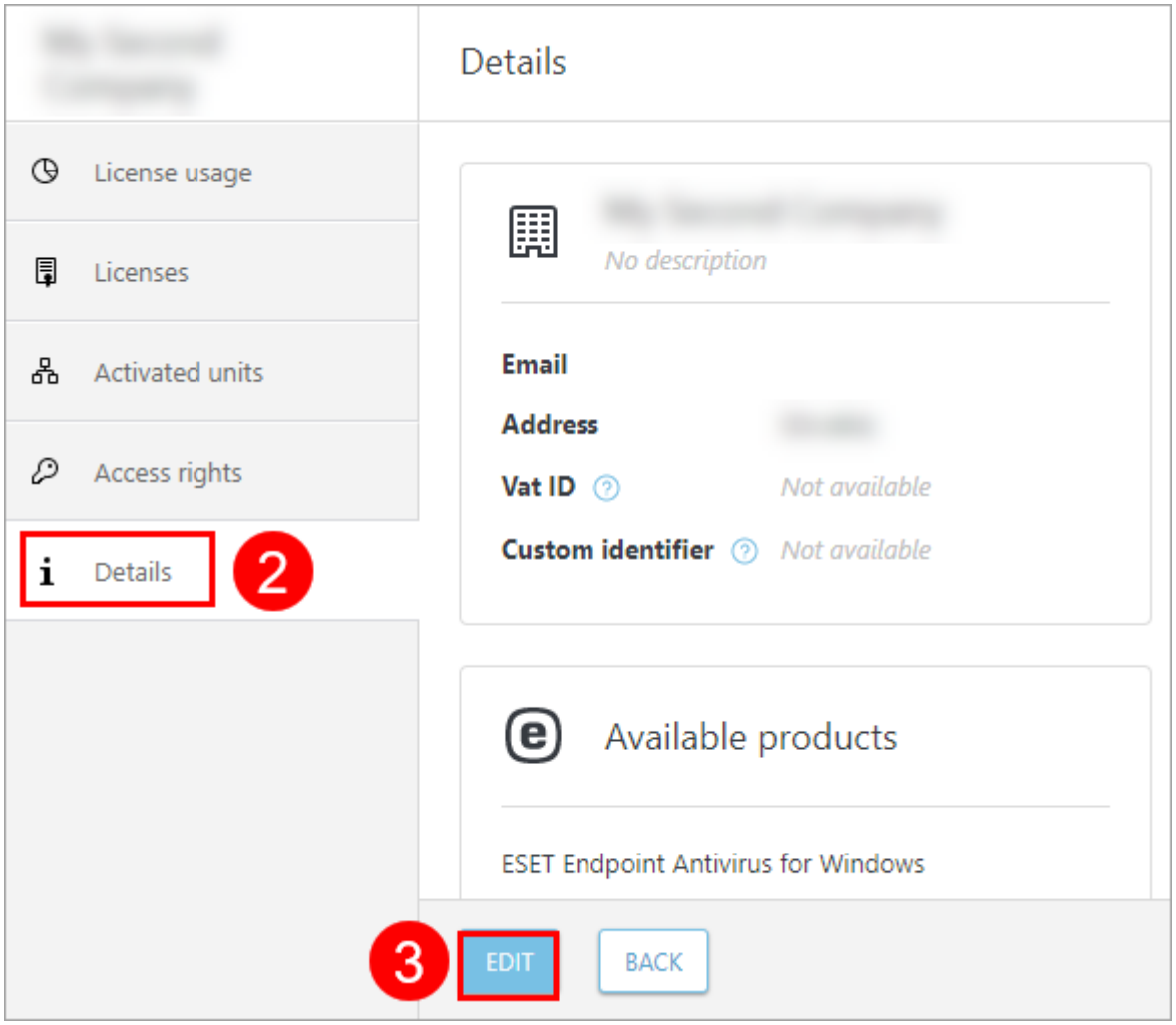
Ak v sekcii **Details** (Podrobnosti) vášho zákazníka nie je produkt ESET LiveGuard Advanced dostupný, požiadajte svojho distribútora alebo MSP manažéra, aby produkt pridal do vášho účtu ESET MSP Administrator.

Pre pridanie produktu do sekcie **Available products** z účtu distribútora postupujte podľa nasledujúcich krokov:

1. Prihláste sa do svojho účtu na portáli ESET MSP Administrator.

2. Kliknite na **Companies** (Spoločnosti), vyberte MSP zákazníka a kliknite na **Details** (Podrobnosti).

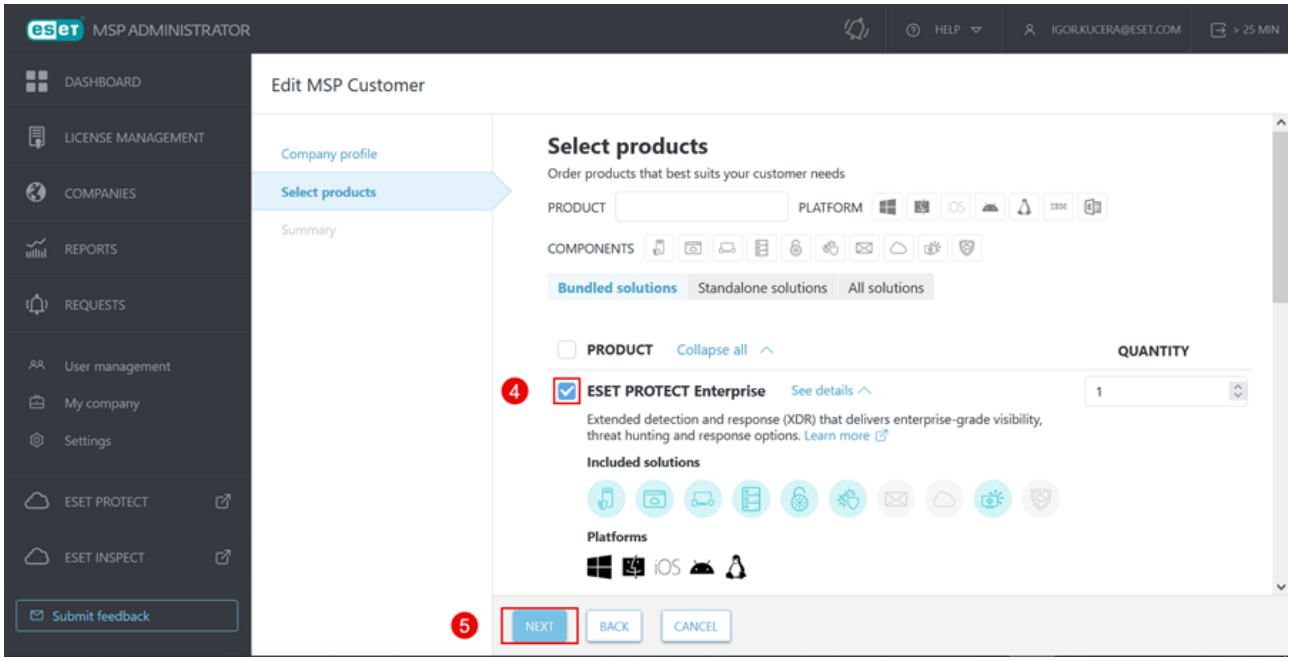
3. Kliknite na **Edit** (Upraviť).



4.Kliknite na **Next** (Ďalej) a na obrazovke Select Products (Vybrať produkty) zvoľte ESET LiveGuard Advanced alebo inú vhodnú licenciu.

5.Kliknite na **Ďalej**.

6.Zmeny skontrolujte v časti **Summary** (Súhrn) a kliknite na **Save** (Uložiť).



Pridanie licencie ESET LiveGuard Advanced vášmu MSP zákazníkovi

Ak má zákazník dostupnú licenciu ESET LiveGuard Advanced, môžete mu ju priradiť.

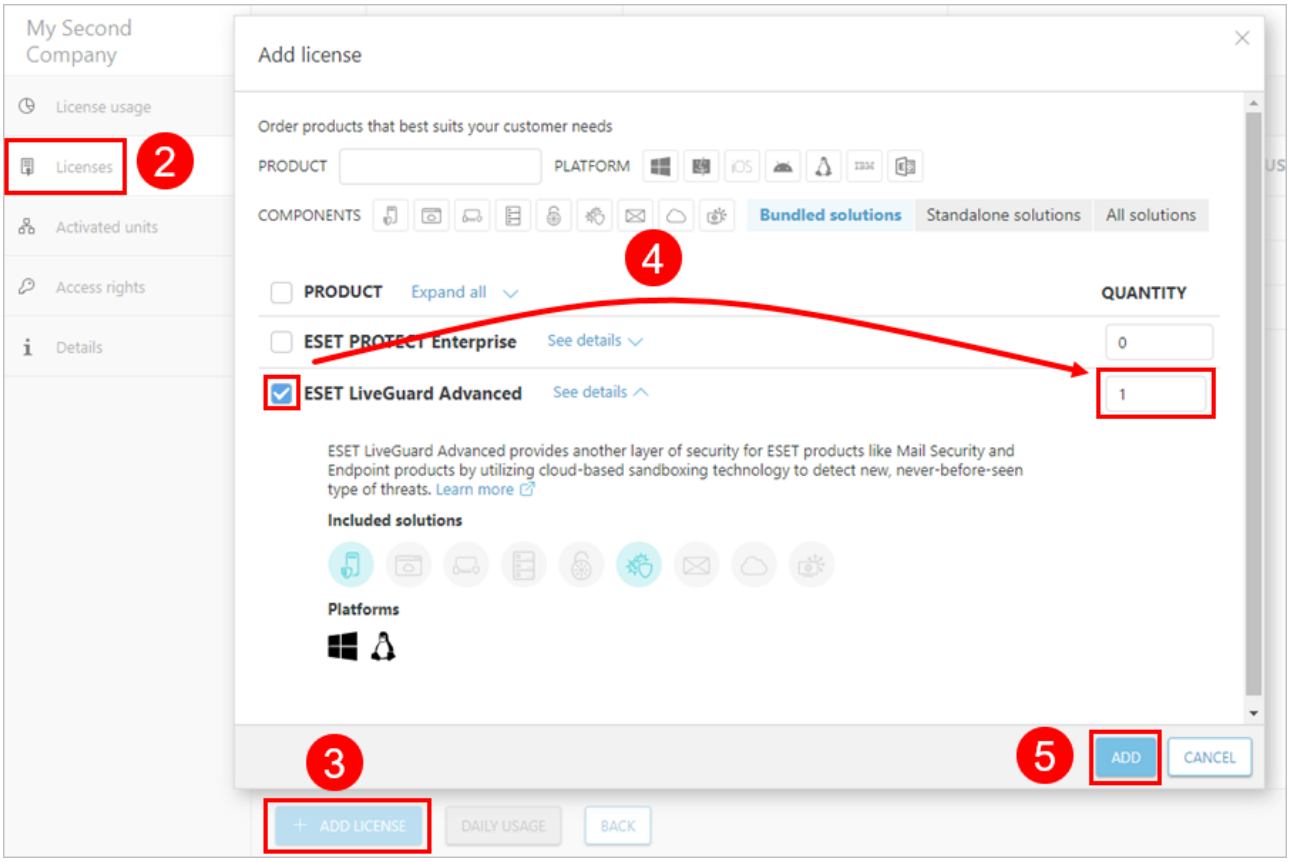
1.Prihláste sa do svojho účtu na portáli ESET MSP Administrator.

2.Kliknite na **Companies** (Spoločnosti), vyberte MSP zákazníka a kliknite na **Licenses** (Licencie).

3.Kliknite na **Add License** (Pridať licenciu), prípadne na **Request License** (Vyžiadať licenciu).

4.Označte začiarkavacie políčko vedľa položky **ESET LiveGuard Advanced** a v časti **Units** nastavte počet licenčných jednotiek.

5.Kliknite na **Add** (Pridať).



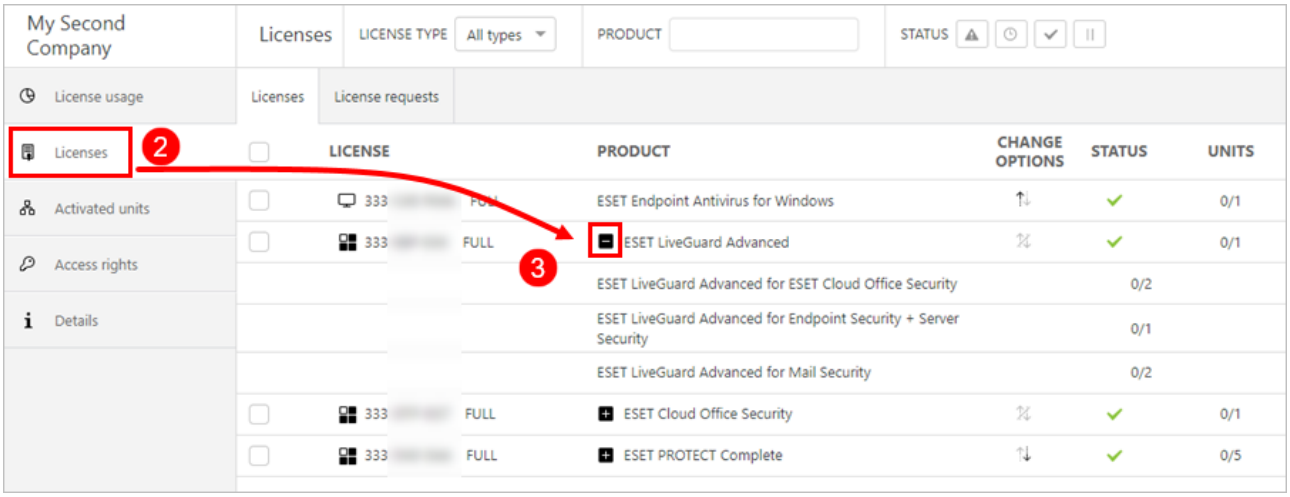
Zobrazenie informácií o licencii ESET LiveGuard Advanced

ESET LiveGuard Advanced sa predáva ako licenčná úroveň. Podrobnosti licencie si môžete zobraziť vo svojom účte ESET MSP Administrator.

1.Prihláste sa do svojho účtu na portáli ESET MSP Administrator.

2.Kliknite na **Companies** (Spoločnosti), vyberte MSP zákazníka a kliknite na **Licenses** (Licencie).

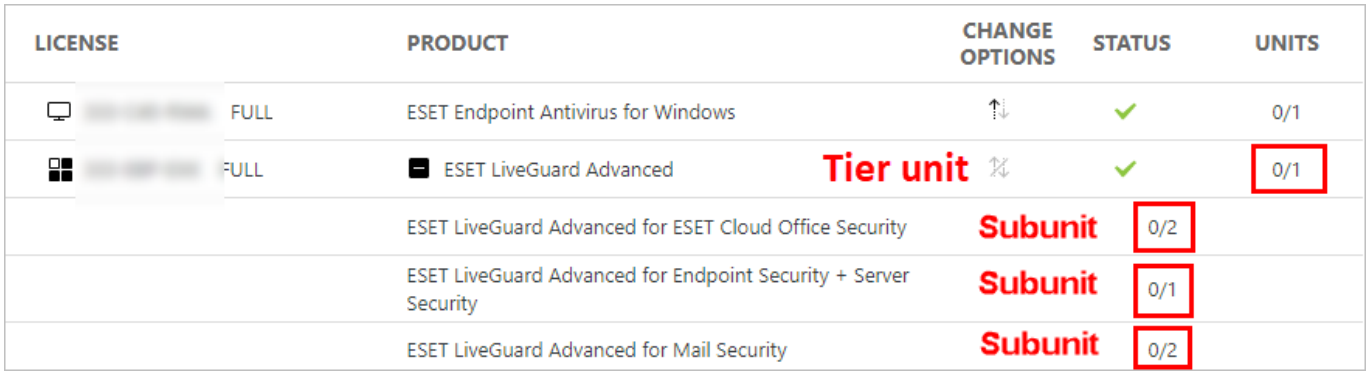
3.Pre rozbalenie licenčných informácií kliknite vedľa licencie ESET LiveGuard Advanced na ikonu ⊞.



Po pridaní licencie ESET LiveGuard Advanced spustite synchronizáciu s ESET PROTECT On-Prem.

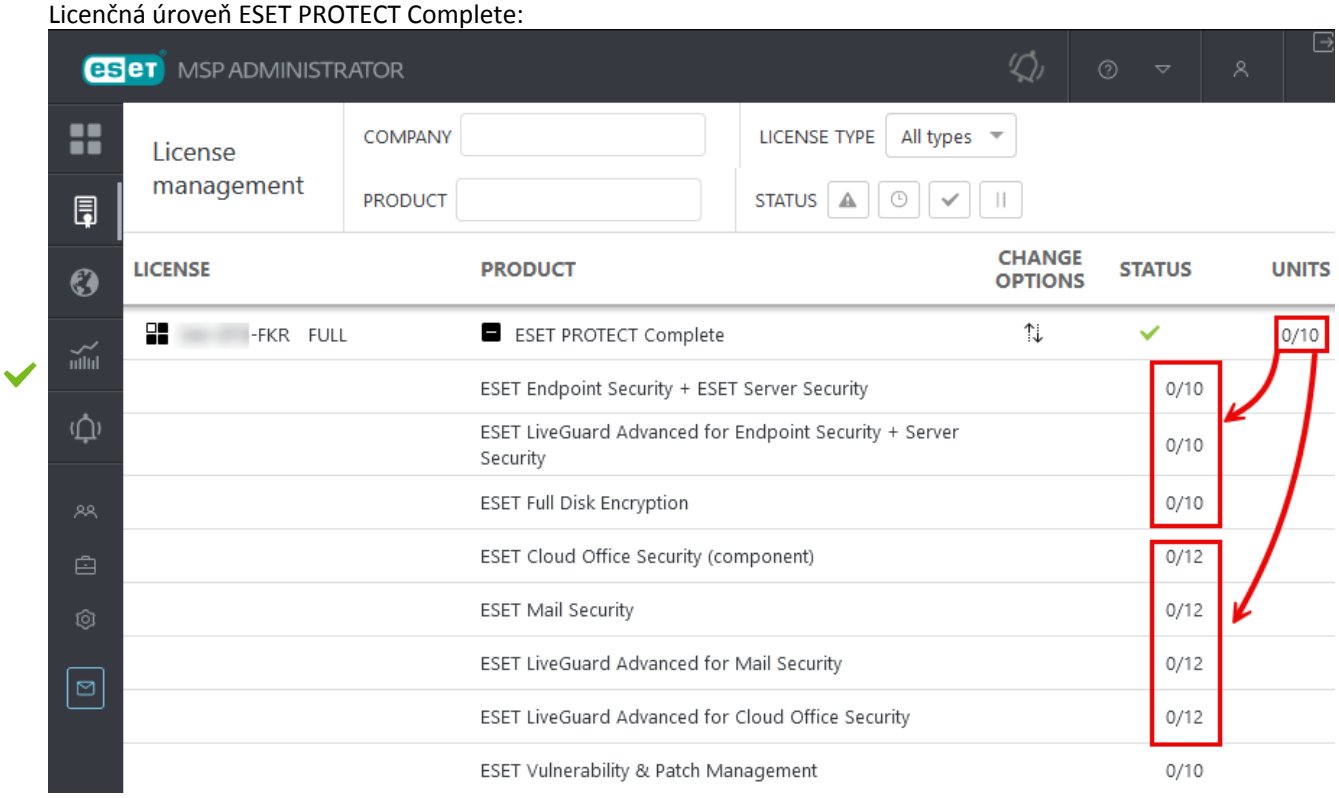
Jednotky a podjednotky

Počet jednotiek predstavuje počet objednaných a vyúčtovaných jednotiek licencie (úrovne licencií). Každá licenčná úroveň môže obsahovať rôzny pomer jednotiek a podjednotiek pre každý zahrnutý produkt.



Príklad distribúcie podjednotiek

Licenčná úroveň ESET PROTECT Complete:



Synchronizácia ESET MSP Administrator s ESET PROTECT On-Prem

Požiadavky

- Licencia na ESET LiveGuard Advanced vo vašom účte na portáli ESET MSP Administrator
- Nasadená konzola ESET PROTECT On-Prem

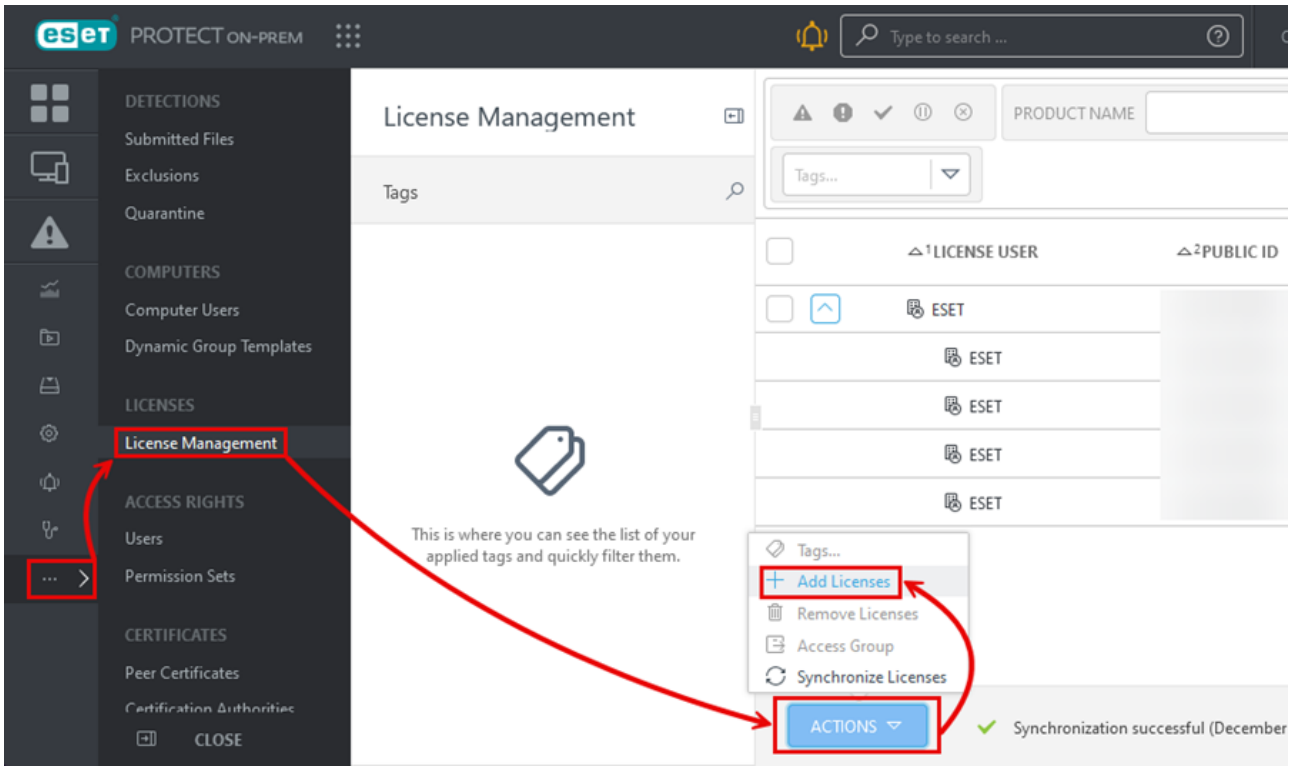
- Fungujúce spojenie medzi ESET PROTECT Serverom a portálom ESET MSP Administrator

Ak už ste pridali svoj účet EBA do ESET PROTECT Web Console, v sekcii **Správa licencií** kliknite na možnosť **Synchronizovať**, čím manuálne vynútite aktualizáciu licenčných údajov vo Web Console. V tomto prípade nie je potrebné znovu zadávať prihlasovacie údaje do ESET MSP Administrator.

Synchronizácia

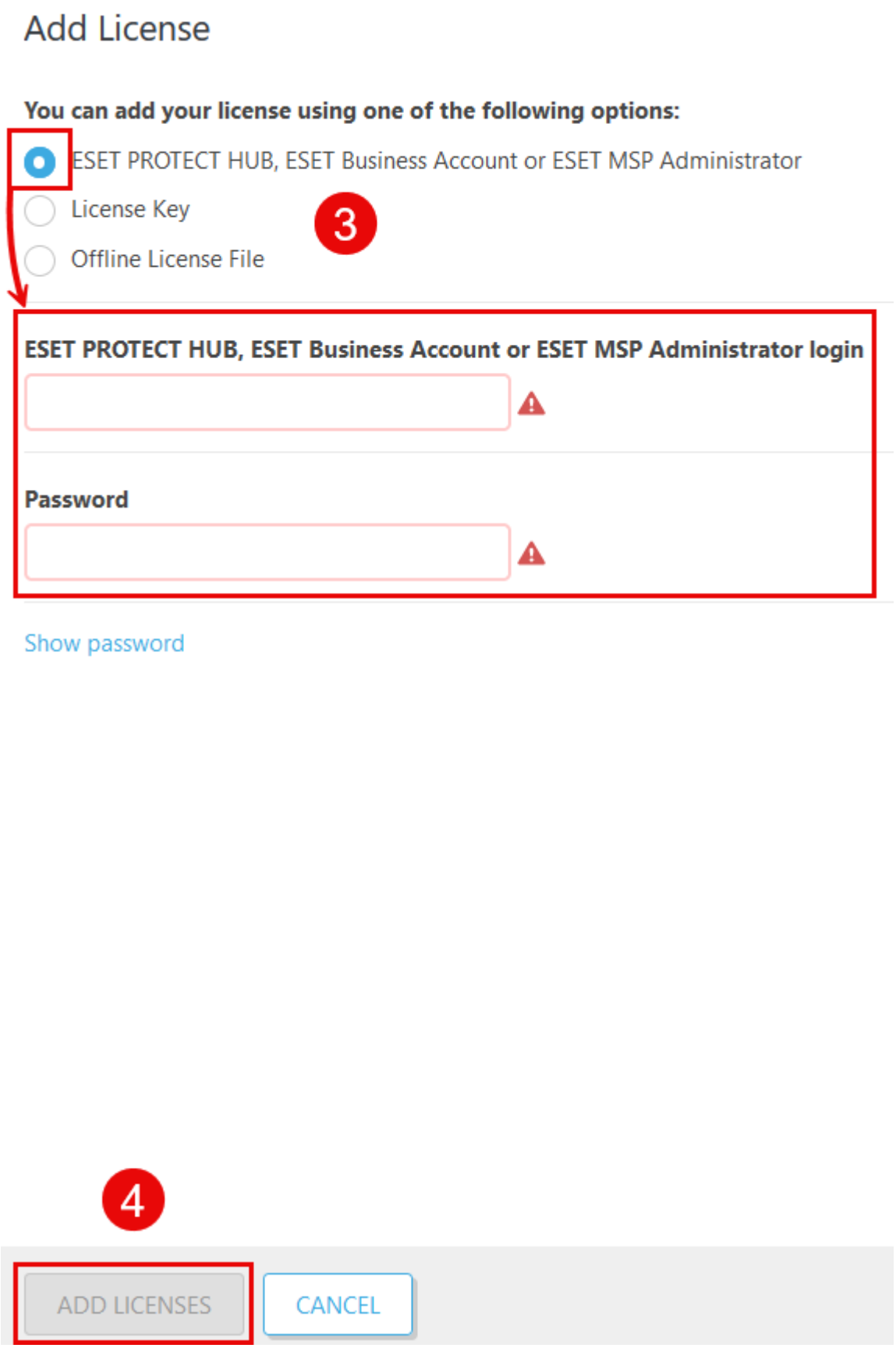
1.Prihláste sa do ESET PROTECT Web Console ako správca (účet Administrator) alebo pod iným používateľským účtom s dostatočnými prístupovými povoleniami.

2.Kliknite na **Viac** > **Správa licencií** > **Akcie** > **Pridať licenciu**.



3.Vyberte možnosť **Prihlasovacie údaje pre ESET Business Account alebo ESET MSP Administrator** a zadajte prístupové údaje k vášmu účtu na portáli ESET MSP Administrator.

4.Kliknite na tlačidlo **Pridať licencie**, čím do ESET PROTECT On-Prem pridáte všetky licencie z vášho účtu.



Ak importujete licenčný kľúč pre ESET LiveGuard Advanced priamo do Web Console, zobrazí sa nasledujúce chybové hlásenie:
„Nepodarilo sa pridať licenciu pomocou licenčného kľúča: Licencia je vydaná pre produkt, ktorý nie je možné spravovať pomocou konzoly ESET PROTECT On-Prem. Zadajte inú licenciu, prosím.“
Licenciu pre ESET LiveGuard Advanced importujte vždy cez portál EBA alebo ESET MSP Administrator.

Aktivácia na skupine počítačov

V prípade aktivácie na skupine počítačov cez konzolu ESET PROTECT On-Prem alebo ESET PROTECT použite zjednodušený proces aktivácie.

Požiadavky pre používateľov ESET PROTECT On-Prem

- Licencia pre ESET LiveGuard Advanced importovaná do ESET PROTECT On-Prem.
- Klientske počítače s verziou nástroja ESET Management Agent, ktorá nie je staršia ako verzia komponentu Server.
- Aktivovaný bezpečnostný produkt ESET podporujúci ESET LiveGuard Advanced.

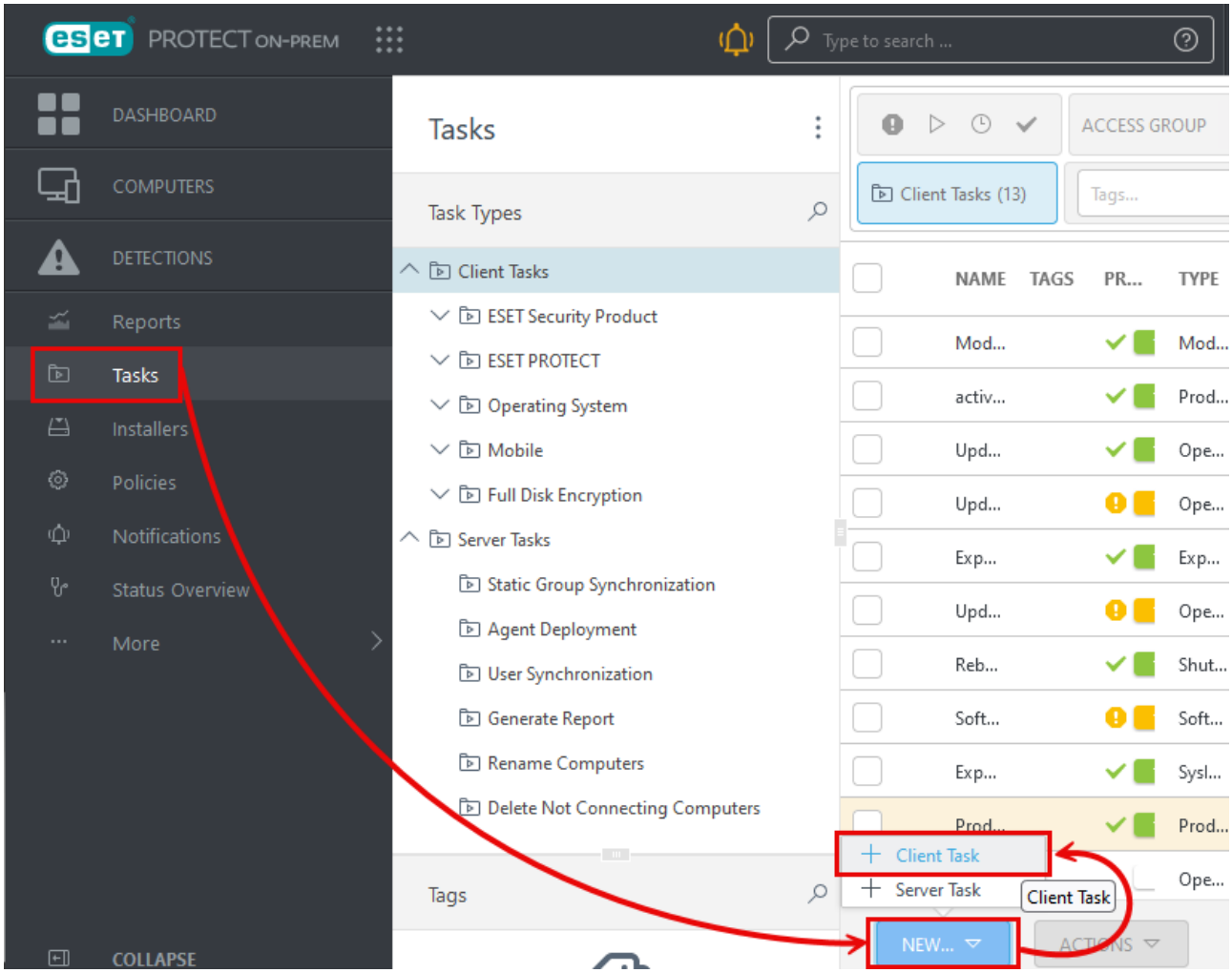
Požiadavky pre používateľov ESET PROTECT

- Licencia pre ESET LiveGuard Advanced importovaná do EBA.
- Na všetkých klientskych zariadeniach je najnovšia verzia ESET Management Agenta.
- Na klientskych zariadeniach musí byť nainštalovaný a aktivovaný bezpečnostný produkt ESET s podporou ESET LiveGuard Advanced).

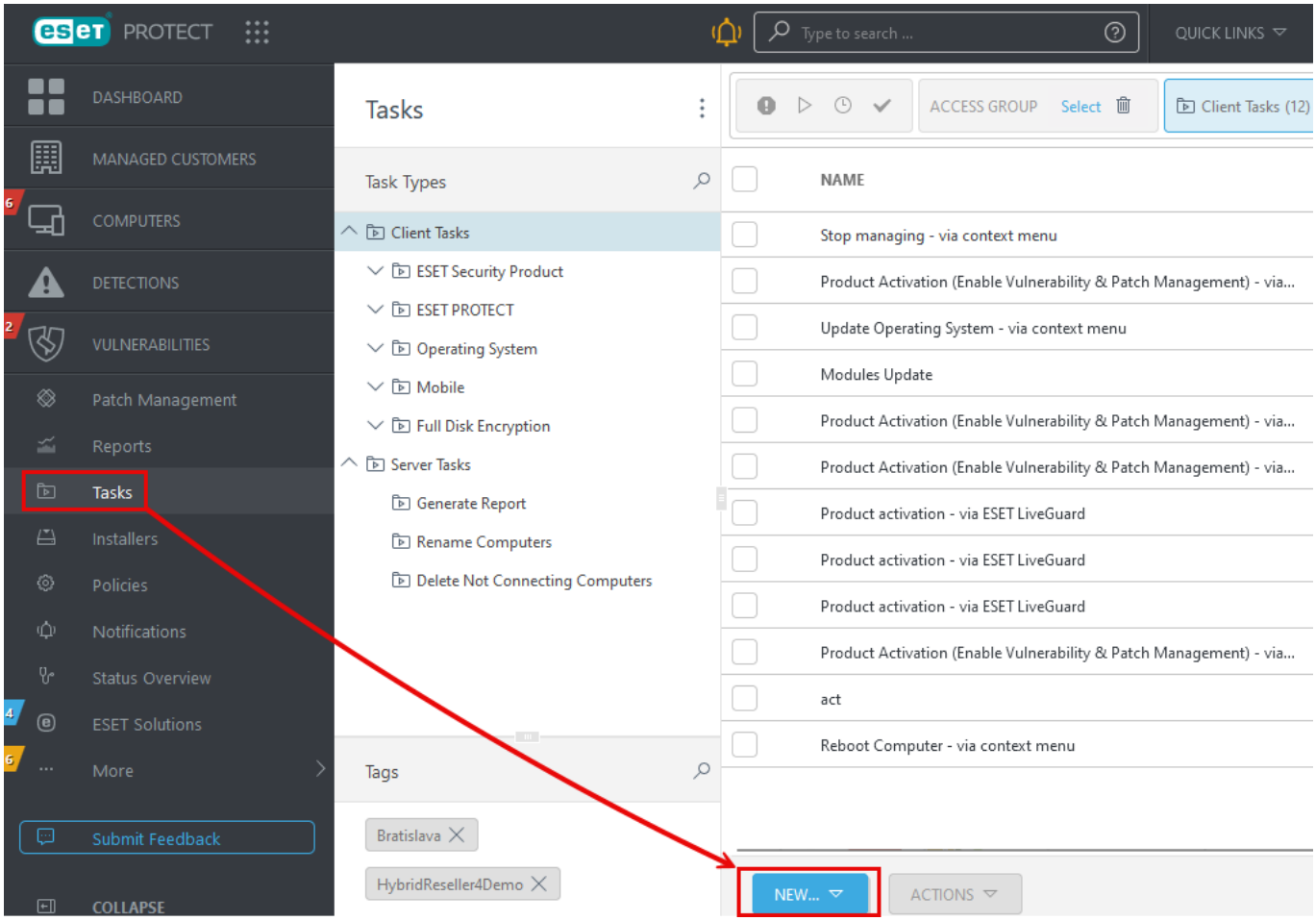
Úloha na aktiváciu produktu

1. Prihláste sa do Web Console.

2. Kliknite na **Úlohy** > **Nová** > **Klientska úloha**.

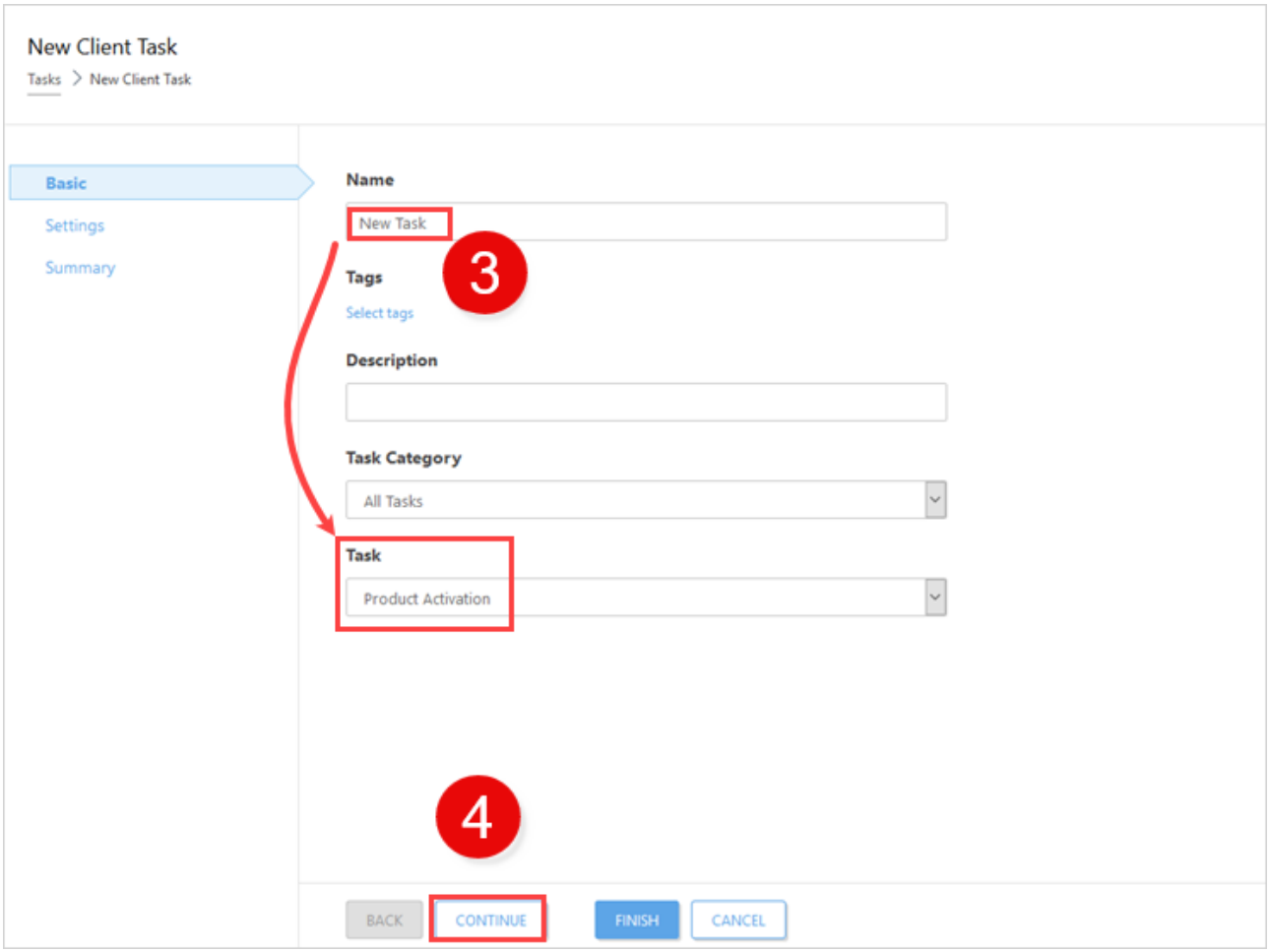


[Používam ESET PROTECT]



3.Zadajte pre vytváranú úlohu názov a ako typ **úlohy** vyberte **Aktiváciu produktu**.

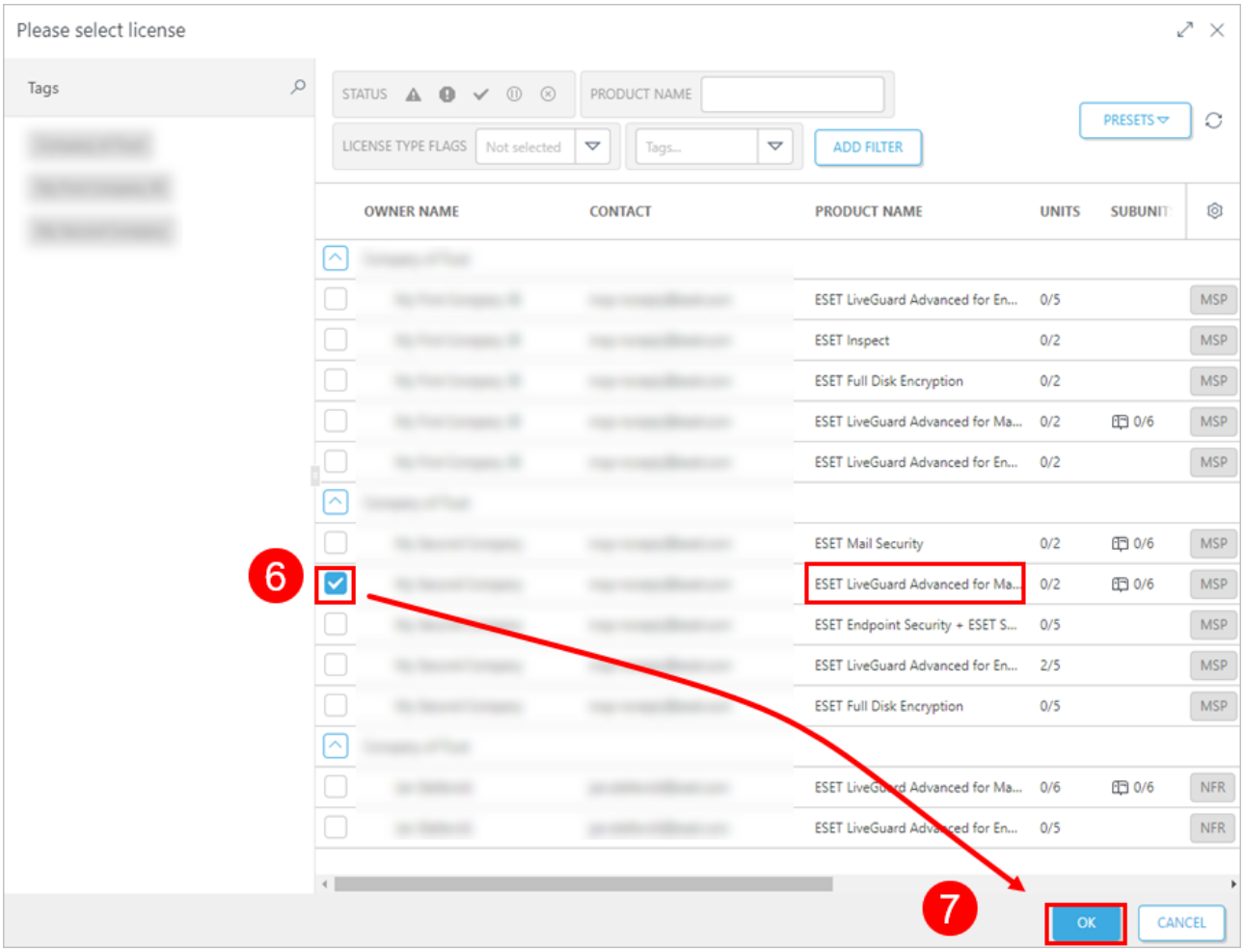
4.Kliknite na tlačidlo **Pokračovať**.



5.Kliknutím na výber licencie prejdite do zoznamu licencií a vyberte licenciu pre ESET LiveGuard Advanced.

6.ESET LiveGuard Advanced sa predáva vo forme licenčnej úrovne. Úroveň rozbaľte a vyberte produktovú licenciu, ktorú chcete použiť.

7.Kliknite na **OK**.



8.V časti **Súhrn** skontrolujte prehľad nastavení úlohy.

9.Ak je všetko v poriadku, kliknite na tlačidlo **Dokončiť**.

10. Po vytvorení úlohy je potrebné naplánovať jej spustenie. V okne s upozornením kliknite na tlačidlo **Vytvoriť spúšťač**.

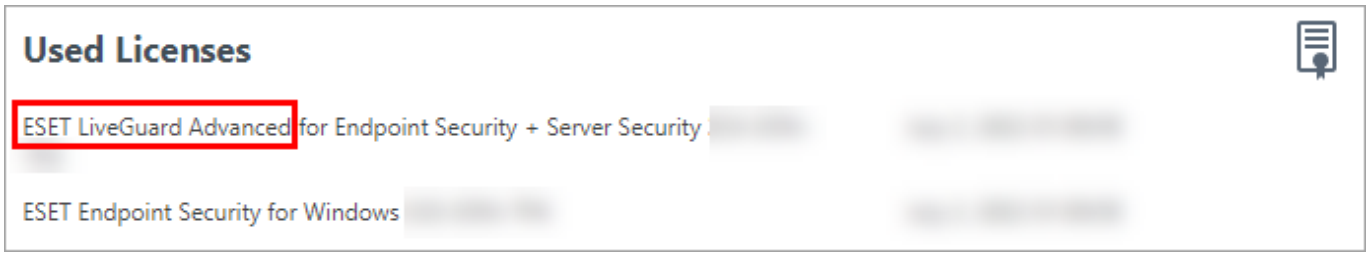
11. Vyplňte pole **Popis spúšťača** a kliknite na tlačidlo **Pokračovať**.

12. Kliknite na **Pridať počítače** alebo **Pridať skupiny** a vyberte zariadenia, na ktorých má byť produkt aktivovaný. Uistite sa, že na týchto vybraných klientskych zariadeniach sú nainštalované bezpečnostné produkty ESET kompatibilné s licenciou, ktorú ste zvolili v kroku 6. Kliknite na tlačidlo **OK** a následne na **Pokračovať**.

13. Môžete zvoliť **Typ spúšťača**. Odporúčame použiť predvolenú možnosť: **Čo najskôr**, ktorá zaistí okamžité spustenie úlohy. Ak zvolíte inú z možností, sprístupní sa sekcia **Rozšírené nastavenia – Obmedzovanie**.

14. Kliknite na tlačidlo **Dokončiť**, čím nastavíte naplánované spustenie úlohy na aktiváciu produktu.

Po úspešnej aktivácii produktu bude licencia zobrazená v podrobnostiach o zariadení. Vo Web Console prejdite do sekcie **Počítače**, zvoľte dané zariadenie a kliknite na **Zobraziť podrobnosti > Podrobnosti > Produkty a licencie**.



Aktivácia na vybraných počítačoch

Požiadavky pre používateľov ESET PROTECT On-Prem a ESET PROTECT

- V ESET PROTECT On-Premje naimportovaná licencia pre ESET LiveGuard Advanced alebo úroveň ochrany zahŕňajúca túto službu.
- Klientske počítače s verziou nástroja ESET Management Agent, ktorá je kompatibilná s verziou komponentu Server.
- Aktivovaný bezpečnostný produkt ESET podporujúci ESET LiveGuard Advanced.

Požiadavky pre používateľov ESET PROTECT

- V EBAje naimportovaná licencia pre ESET LiveGuard Advanced alebo úroveň ochrany zahŕňajúca túto službu.
- Na všetkých klientskych zariadeniach je najnovšia verzia ESET Management Agenta.
- Na klientskych zariadeniach musí byť nainštalovaný a aktivovaný bezpečnostný produkt ESET s podporou ESET LiveGuard Advanced).

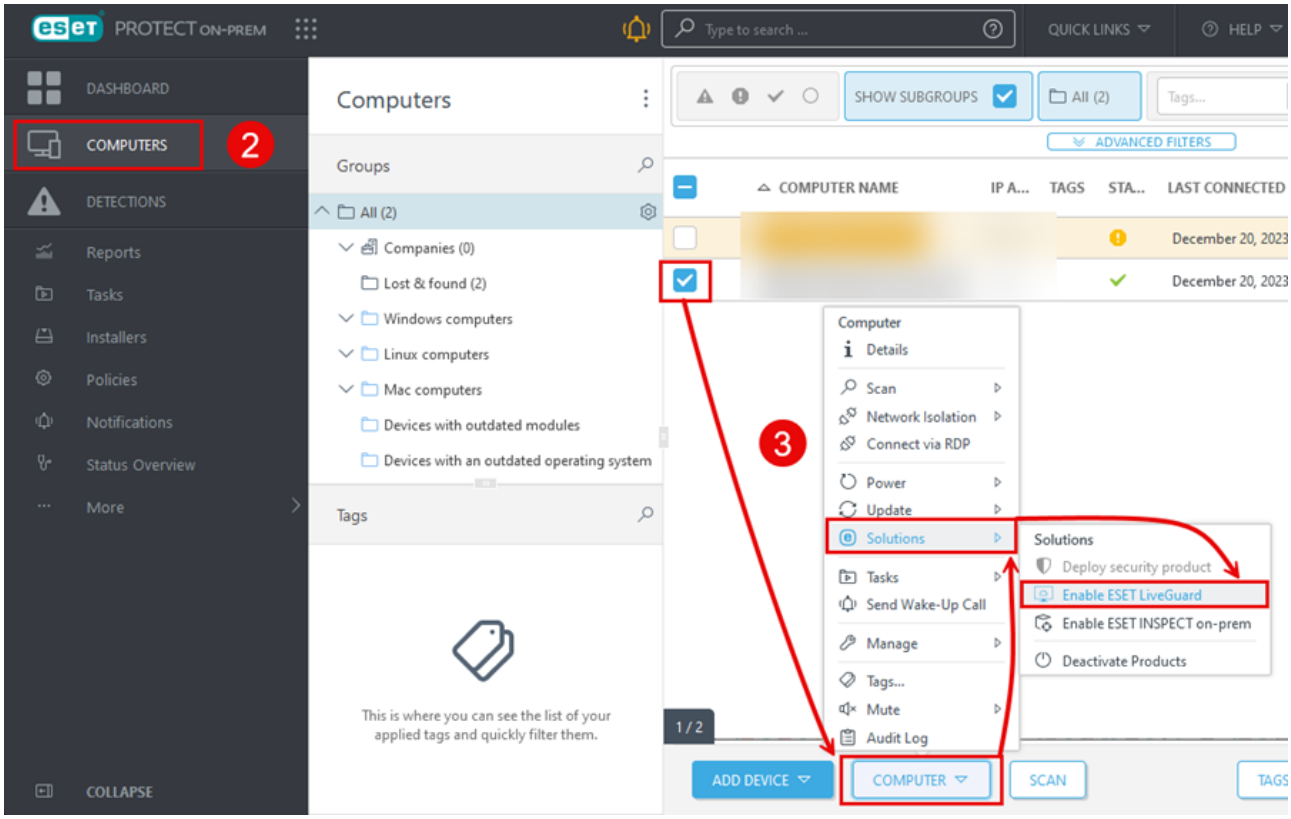
- Nikdy neimportujte licenciu pre ESET LiveGuard Advanced do konzoly na vzdialenú správu pomocou licenčného kľúča. Ak už ste tak urobili, takúto licenciu odstráňte a potom ju znova naimportujte prostredníctvom portálu EBA alebo ESET MSP Administrator.
- Pred použitím licencie ESET LiveGuard Advanced sa vždy uistite, že na vašom cieľovom počítači sa nachádza aktivovaný a podporovaný produkt.

Aktivácia a zapnutie ESET LiveGuard Advanced v ESET PROTECT On-Prem a ESET PROTECT

ESET PROTECT On-Prem a ESET PROTECT ponúkajú zjednodušenú aktiváciu.

1. Prihláste sa do Web Console.
2. V hlavnom menu prejdite do sekcie **Počítače**.

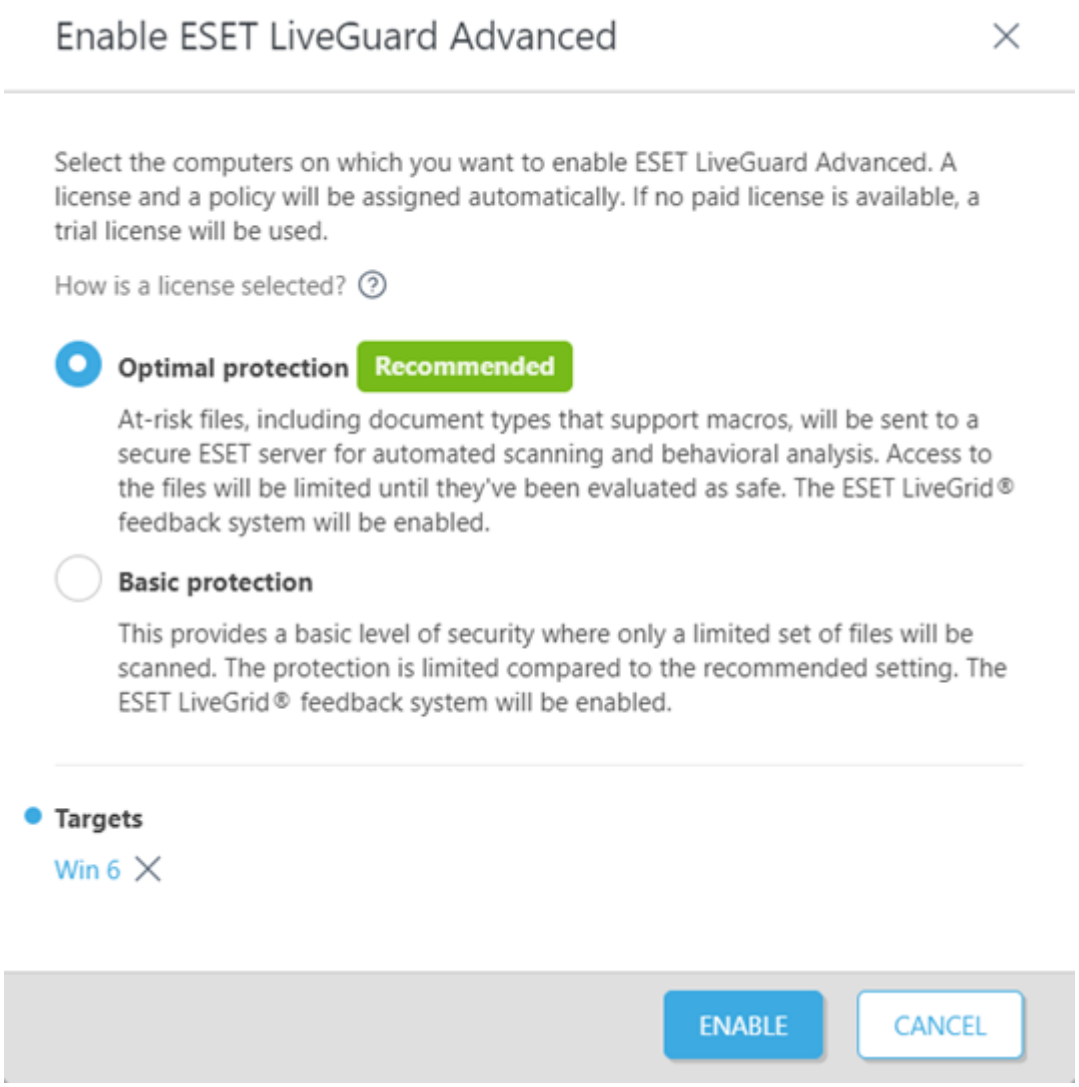
3.Označte začiarkavacie políčko pri počítačoch, ktoré chcete aktivovať, a kliknite na Akcie > Zapnúť ESET LiveGuard.



4.Vyberte si medzi **optimálnou ochranou** a **základnou ochranou**.

5.V sekcii Ciele skontrolujte počítač, na ktorom bude aktivovaný ESET LiveGuard Advanced.

6.Úlohu spustite kliknutím na **Zapnúť**.



Konzola na správu odošle na vybraný počítač aktivačnú úlohu a politiku. ESET LiveGuard Advanced sa zapne po ďalšom pripojení ESET Management Agenta, zvyčajne do niekoľkých minút.

Vzdialená inštalácia a aktivácia

Prostredníctvom inštalačnej úlohy v konzole ESET PROTECT On-Prem alebo ESET PROTECT je možné nainštalovať bezpečnostný produkt ESET, ako aj aktivovať a zapnúť ESET LiveGuard Advanced v rámci jednej akcie.

1.Prihláste sa do ESET PROTECT Web Console.

2.Kliknite na **Úlohy** > **Nová > Klientska úloha**.

3.Zadajte názov úlohy a z roletového menu **Úloha** vyberte možnosť **Inštalácia softvéru**.

4.Kliknite na tlačidlo **Pokračovať**.

5.Kliknite na možnosť **Vyberte balík** a vyberte príslušný produkt ESET.

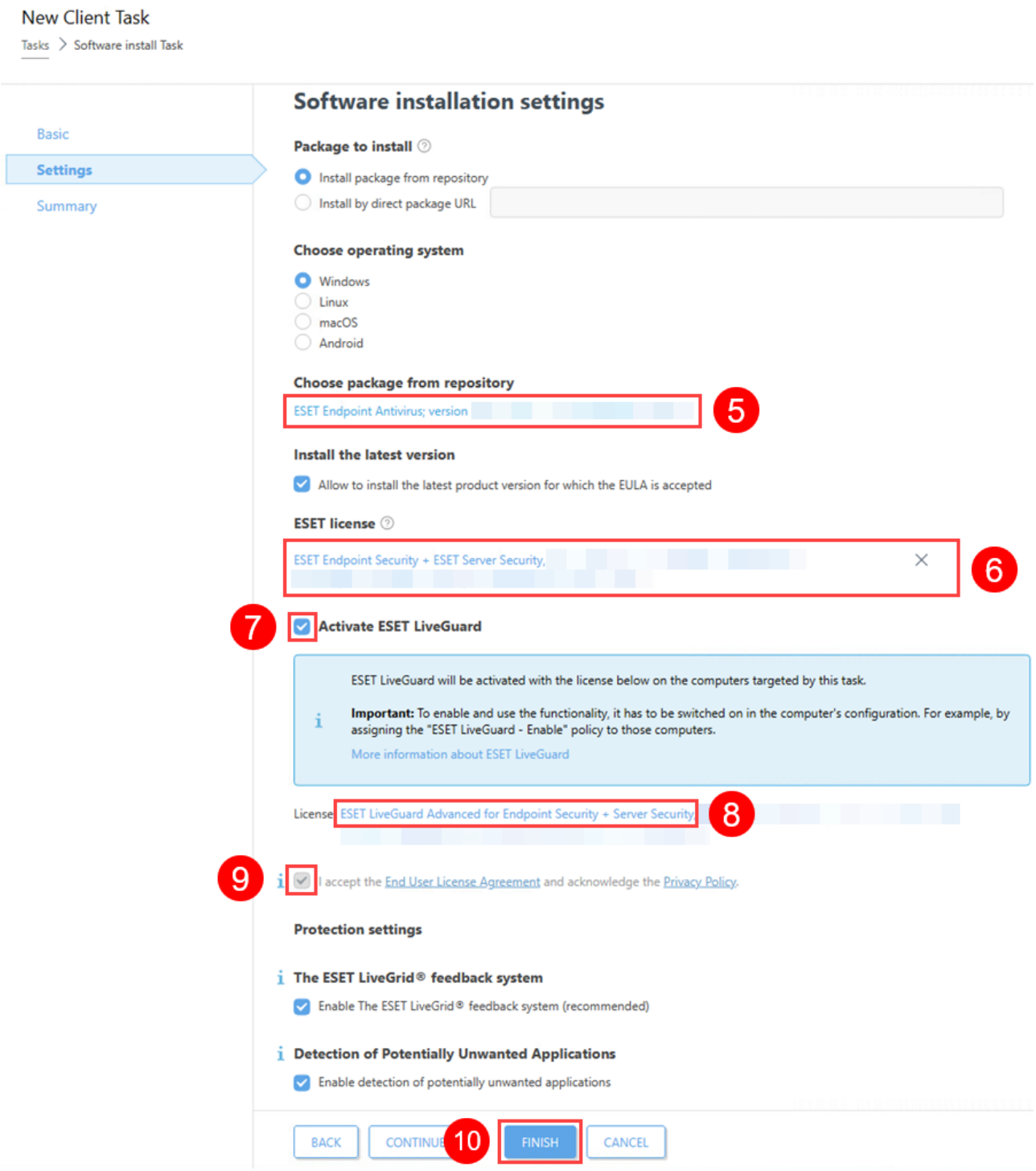
6.Vyberte licenciu ESET, ktorou sa produkt aktivuje.

7.Označte možnosť **Aktivovať ESET LiveGuard**.

8.Vyberte príslušnú licenciu pre ESET LiveGuard Advanced.

9.Označte možnosť **Súhlasím**, ak súhlasíte s Licenčnou dohodou s koncovým používateľom a Zásadami ochrany osobných údajov týkajúcich sa bezpečnostného produktu.

10. Kliknite na **Dokončiť**.



11. Kliknite na **Vytvoriť spúšťač**.

12. Zadajte názov spúšťača a kliknite na **Pokračovať**.

13. Kliknite na možnosť **Pridať ciele** a vyberte príslušné počítače alebo skupiny. Kliknite na **OK**.

14. Kliknite na tlačidlo **Dokončiť** pre okamžité spustenie inštalačnej úlohy.

Ako zapnúť a nakonfigurovať službu ESET LiveGuard Advanced

Požiadavky na aktiváciu

- Účet ESET Business Account alebo ESET MSP Administrator prepojený s podporovanou konzolou na správu
- Nainštalovaná alebo nasadená podporovaná konzola na správu
- Nainštalované kompatibilné bezpečnostné produkty ESET
- Platná licencia na ESET LiveGuard Advanced
- Aktivované bezpečnostné produkty ESET s licenciou na ESET LiveGuard Advanced
- Zapnutá služba ESET LiveGuard Advanced v nastaveniach politík pre kompatibilné bezpečnostné produkty ESET

Zapnutie služby ESET LiveGuard Advanced v bezpečnostnom produkte

- ESET Endpoint Security
- Ako fungujú politiky a ako vytvoriť novú politiku?

Zapnutie služby ESET LiveGuard Advanced v riešení ESET Cloud Office Security

Prečítajte si online pomocníka pre ESET Cloud Office Security alebo podrobné inštrukcie.

Konfigurácia bezpečnostného produktu ESET

Používatelia ESET Cloud Office Security

Ak chcete v riešení ESET Cloud Office Security využívať službu ESET LiveGuard Advanced, vytvorte novú alebo nakonfigurujte existujúcu politiku. Používatelia alebo skupiny priradené k tejto politike získajú dodatočnú ochranu. Viac informácií nájdete v kapitole Nastavenia ochrany pre ESET LiveGuard Advanced.

Nastavenie politiky ESET Cloud Office Security

1.Prihláste sa do služby ESET Cloud Office Security.

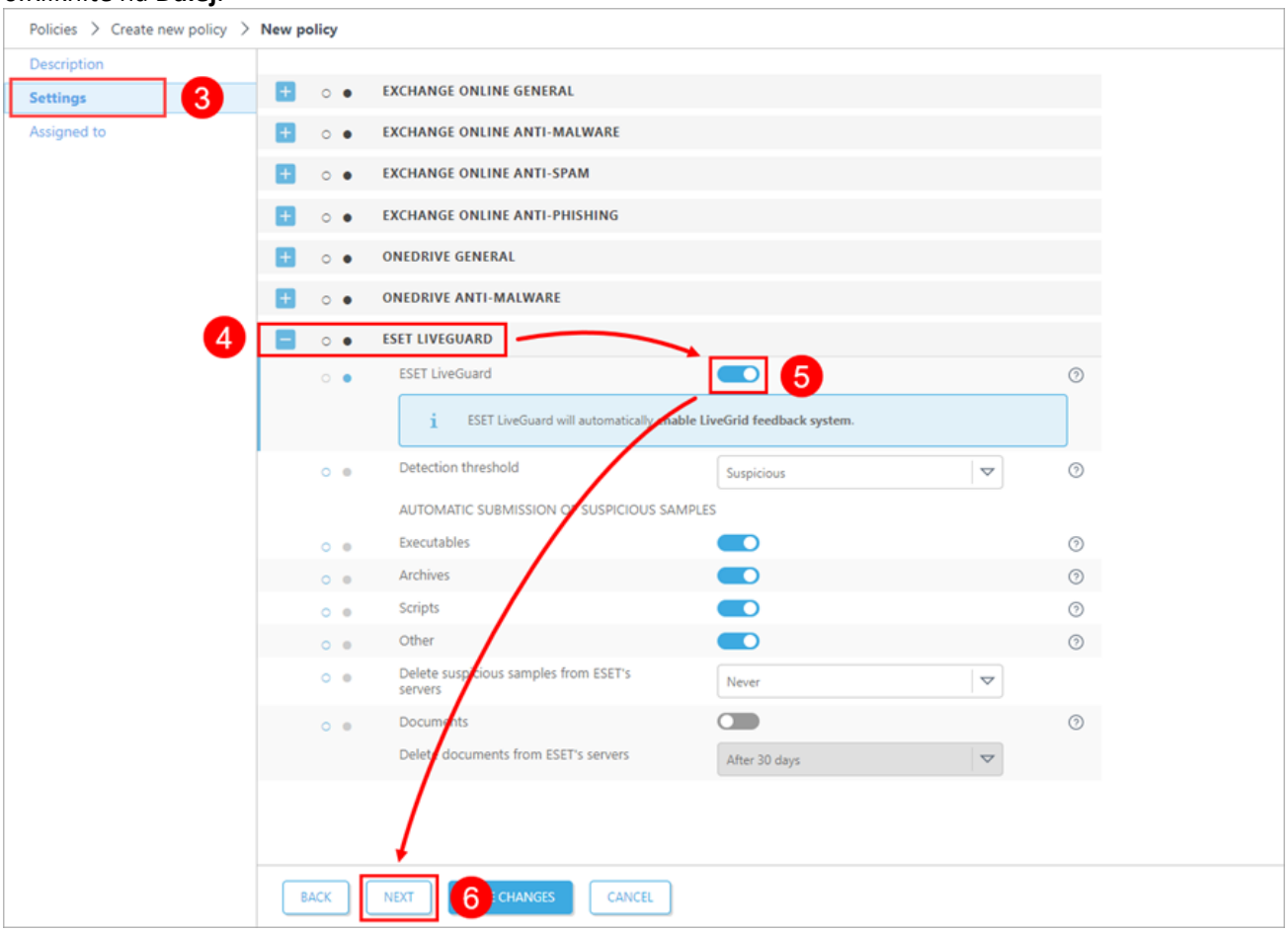
2.Kliknite na **Politiky**, vyberte politiku a kliknite na **Upraviť**.

3.Kliknite na **Nastavenia**.

4.Rozbaľte sekciu **ESET LiveGuard**.

5.Kliknite na prepínač vedľa **ESET LiveGuard**.

6.Kliknite na **Ďalej**.



Používatelia konzoly na správu produktov ESET

Pre zapnutie služby ESET LiveGuard Advanced na klientskom zariadení musíte mať splnené všetky požiadavky a následne vytvoriť politiku, prostredníctvom ktorej túto službu nastavíte.

V ESET PROTECT Web Console vytvorte novú politiku, prípadne si otvorte niektorú z existujúcich, a po vykonaní požadovaných zmien v rámci nastavení túto politiku priraďte k zariadeniam, na ktorých chcete službu ESET LiveGuard Advanced používať.

> Ak prostredníctvom politiky zapnete ESET LiveGuard Advanced na zariadení, na ktorom nie je táto služba aktivovaná príslušnou licenciou, dané nastavenie sa neaplikuje. Ostatné nastavenia zadefinované v politike aplikované budú.

Nastavenia ESET LiveGuard Advanced

1.Prihláste sa do Web Console na správu produktov ESET a vytvorte alebo upravte politiku.

2.V sekcii **Nastavenia** vyberte váš bezpečnostný produkt, ktorého nastavenia chcete konfigurovať, a prejdite do príslušnej časti:

Politika	Nastavenie
ESET Endpoint pre Windows	Detekčné jadro > Ochrana s podporou cloudu
ESET Mail Security pre Microsoft Exchange (V6+)	Počítač > Ochrana s podporou cloudu
ESET Server Security pre Microsoft Server (V6+)	Detekčné jadro > Ochrana s podporou cloudu
ESET Endpoint for Linux (V7+)	Detekčné jadro > Ochrana s podporou cloudu
ESET Server/File Security for Linux (V7+)	Detekčné jadro > Ochrana s podporou cloudu

3.Pre zapnutie služby ESET LiveGuard Advanced je potrebné povoliť všetky tri možnosti v sekcii **Ochrana s podporou cloudu**.



Počnúc verziou 10.1 produktu ESET Endpoint for Windows alebo novšou je odosielanie dokumentov predvolene povolené.

Sekcia: Ochrana s podporou cloudu	Popis
Zapnúť reputačný systém ESET LiveGrid® (odporúčané)	Využívanie informácií o reputácii súborov zo systému ESET LiveGrid®.
Zapnúť systém spätnej väzby ESET LiveGrid®	Odosielanie súborov do cloudu ESET.
Zapnúť ESET LiveGuard Advanced	Odosielanie súborov na analýzu do ESET LiveGuard Advanced.

4.Môžete nastaviť, ktoré súbory budú odosielané do cloudu ESET v prípade, že budú zachytené alebo vyhodnotené ako podozrivé.

Sekcia: Odosielanie vzoriek	Popis a odporúčanie
Manuálne odosielanie vzoriek	Umožňuje manuálne poslať vybrané súbory na analýzu (možnosť sa týka len produktov pre Windows)
Automatické odosielanie zachytených vzoriek	Vyberte, ktoré typy vzoriek sa budú po zachytení detekčným jadrom automaticky odosielať na analýzu do spoločnosti ESET.
Spustiteľné súbory, Archívy, Skripty, Iné	Vyberte, ktoré typy súborov sa budú automaticky odosielať na analýzu do cloudu ESET, ak ich nezachytí lokálne detekčné jadro. Odporúčame povoliť odosielanie všetkých typov súborov.
Potenciálne spamové e-maily	Odosielanie potenciálnych spamových e□mailov. (Týka sa iba produktov ESET Endpoint pre Windows.)
Odstrániť spustiteľné súbory, archívy, skripty, iné vzorky a potenciálne spamové e□maily zo serverov spoločnosti ESET	Akcia, ktorá sa vykoná po dokončení analýzy.
Dokumenty	Odosielanie dokumentov. Táto možnosť je predvolene povolená.

Sekcia: Odosielanie vzoriek	Popis a odporúčanie
Odstrániť dokumenty zo serverov spoločnosti ESET	Akcia, ktorá sa vykoná po dokončení analýzy.
Vylúčenia	Zoznam prípon súborov, ktoré budú vylúčené z odosielania. Prípony môžete pridávať vo formáte `*.ext?`, kde: `*` predstavuje názov súboru, `ext` predstavuje príponu súboru, `?` predstavuje jeden voliteľný znak. Táto možnosť je voliteľná.
Maximálna veľkosť vzoriek (MB)	Maximálna veľkosť odosielaného súboru.

5.Nastavte prah detekcie a akciu, ktorá sa má vykonať v prípade, že výsledok detekcie súboru bude pozitívny a prekročí nastavený prah detekcie.

Sekcia: ESET LiveGuard Advanced	Popis a odporúčanie
Prah detekcie	Status súboru na základe výsledku analýzy, ktorý spustí **Akciu po detekcii**.
Akcia po detekcii	Akcia, ktorú vykoná bezpečnostný produkt ESET v prípade, že výsledný status analyzovaného súboru je rovnaký alebo vyšší ako status zvolený v rámci **Prahu detekcie**.
Maximálna doba čakania na výsledok analýzy (v minútach)	Maximálna doba čakania na výsledok analýzy pred tým, ako bude e-mail doručený alebo sa sťahovaný súbor sprístupní.
Proaktívna ochrana	Nastavenie Proaktívnej ochrany. Môžete povoliť spúšťanie tých súborov, pre ktoré sa analýza ešte nedokončila.

6.Pre dokončenie politiky vyberte počítače alebo skupiny, ku ktorým chcete politiku priradiť. Nové nastavenia uvedené v politike sa aplikujú po ďalšej replikácii, t. j. pri najbližšom pripojení Agentov k Serveru (zvyčajne do pár minút).

Správa politík

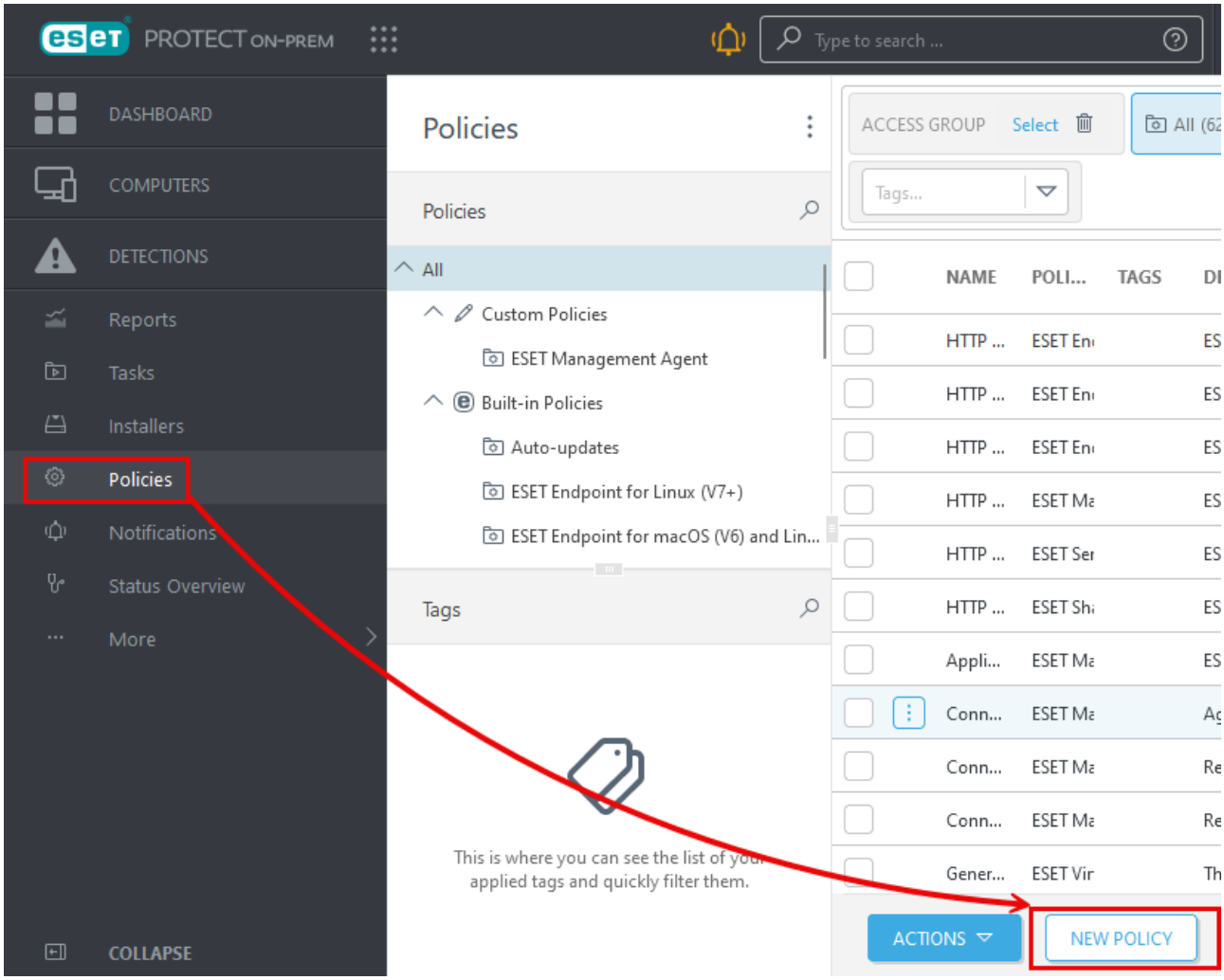
Politiky vám umožňujú z konzoly na správu vzdialene vynútiť uplatnenie požadovaných nastavení na klientske zariadenia. Každá politika sa viaže na konkrétny bezpečnostný produkt ESET a priraďuje sa k jednému klientskemu zariadeniu aj ku skupinám zariadení. V prípade, že je na zariadení aplikovaných viacero politík, politiky sa spoja a následne sa aplikuje výsledné nastavenie.

Pre fungujúce uplatňovanie politík musí byť na klientskych zariadeniach nainštalovaný ESET Management Agent, ktorý bude nakonfigurovaný tak, aby sa pripájal ku konzole na správu.

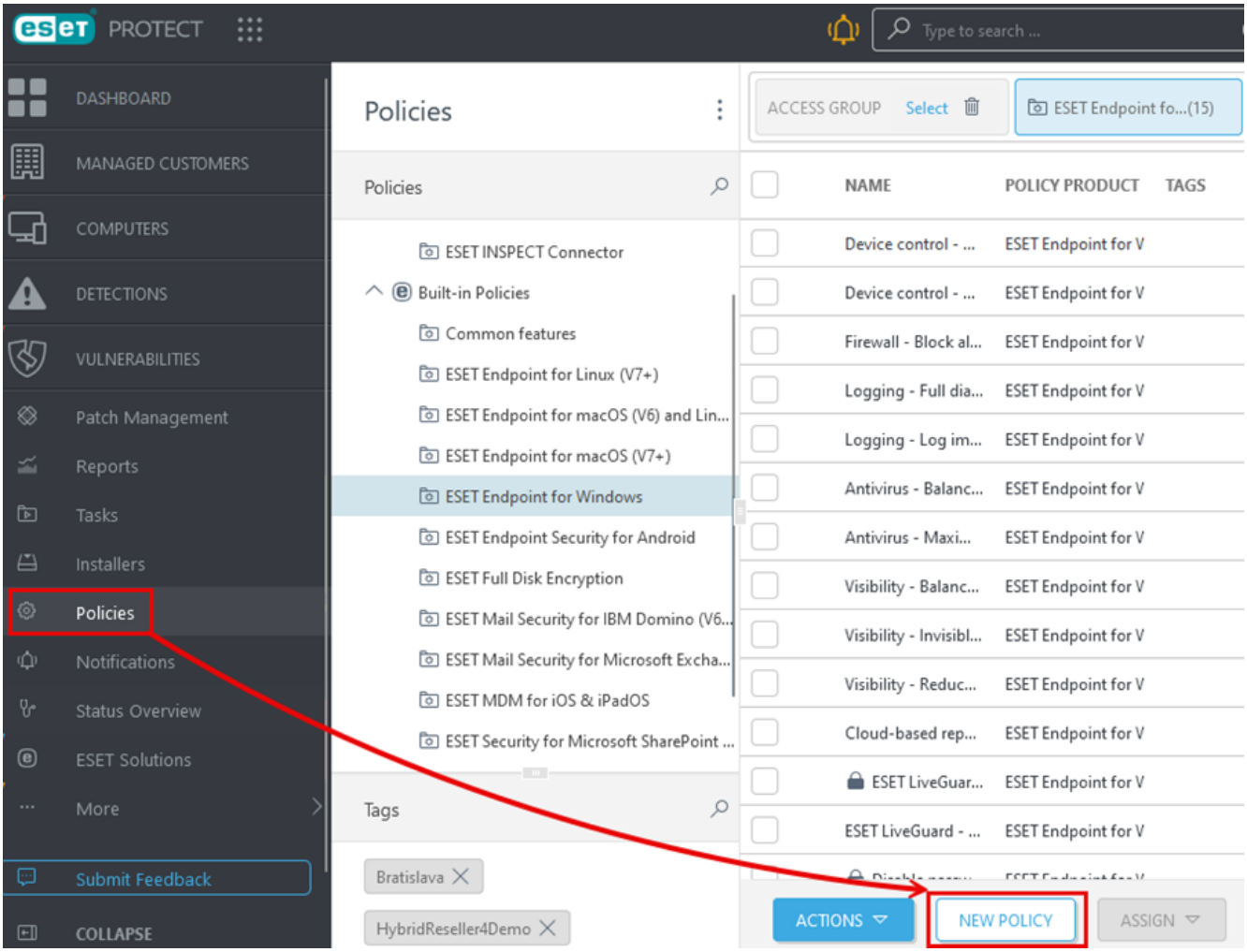
Vytvorenie novej politiky

1.Prihláste sa do Web Console.

2.Kliknite na **Politiky** > **Nová politika**.



[Používam ESET PROTECT]



3.Zadajte pre novovytváranú politiku názov a popis a kliknite na tlačidlo **Pokračovať**.

4.Zvoľte bezpečnostný produkt ESET, ktorého nastavenia má politika upravovať, a kliknite na tlačidlo **Pokračovať**.

5.Vyberte počítače alebo skupiny počítačov, ku ktorým chcete politiku priradiť, a kliknite na tlačidlo **Pokračovať**.

6.V časti **Súhrn** nájdete prehľad nastavení politiky. Pre aplikovanie politiky kliknite na tlačidlo **Dokončiť**.

Ako nakonfigurovať nastavenia v politike pre ESET LiveGuard Advanced?

Ako fungujú politiky?

V sprievodcovi vytvorením novej politiky vyberte produkt ESET, pre ktorý chcete vytvoriť politiku.

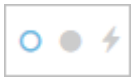
Každý riadok s nastavením obsahuje nasledujúce položky:

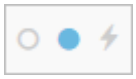
- Stav
- Názov

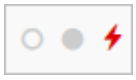
- Verzie podporujúce dané nastavenie (voliteľné)
- Hodnota nastavenia
- Pomocný popis (nie všetky nastavenia obsahujú pomocné popisy)



Stav nastavenia sa zobrazuje, ak je nastavenie v rámci danej politiky nakonfigurované alebo ak je vynútené bez ohľadu na nastavenie z iných politík. Pri nastavení môže byť uvedený jeden z nasledujúcich indikátorov stavu:

 – nastavenie je neaktívne a nebude politikou aplikované

 – nastavenie je aktívne a bude politikou aplikované

 – nastavenie je vynútené

V prípade, že sa na jedno zariadenie aplikuje viacero politík, alebo sú ich nastavenia zdedené, budú politiky zlúčené (na základe poradia). Viac informácií o politikách nájdete v dokumentácii pre ESET PROTECT On-Prem.

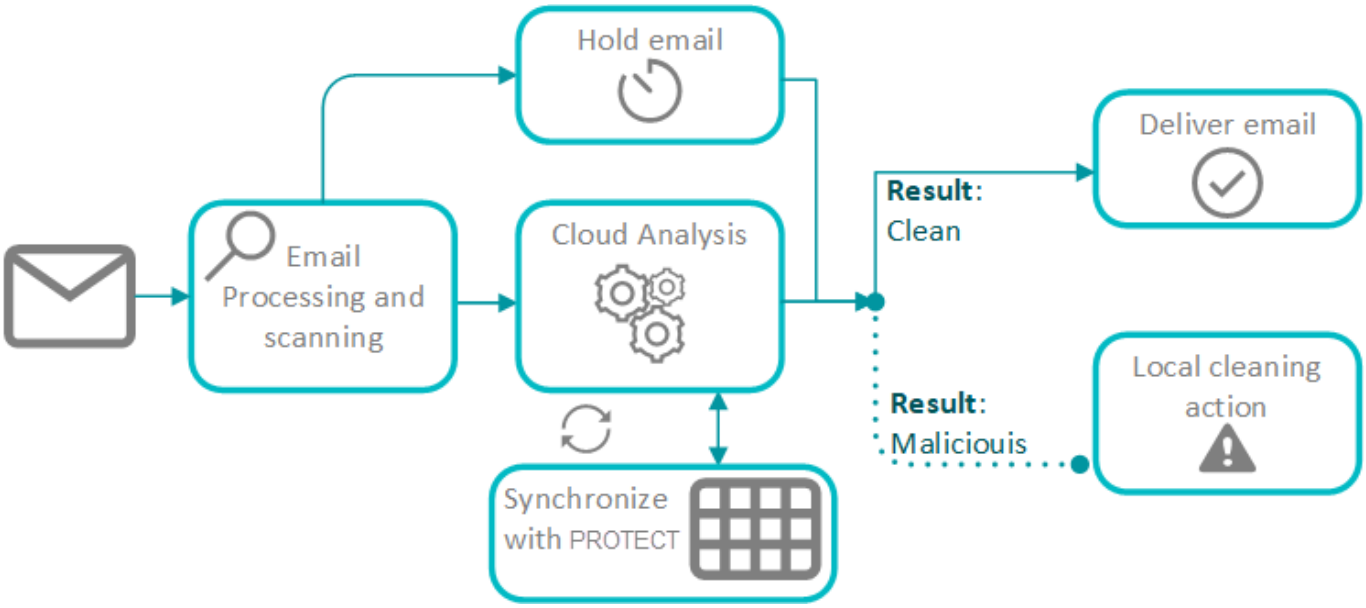
Používanie ESET LiveGuard Advanced

Fungovanie služby ESET LiveGuard Advanced pri produkte ESET Mail Security

Každý e-mail zachytený programom ESET Mail Security je skontrolovaný a doručený. V prípade, že program vyhodnotí e□mail ako podozrivý, jeho doručenie bude na prednastavené časové obdobie podržané a podozrivý e□mail sa zároveň zašle na analýzu využívajúcu niekoľko detekčných vrstiev.

ESET LiveGuard Advanced zanalyzuje súbory a výsledky doručí späť do vášho bezpečnostného produktu ESET. Na základe výsledkov analýzy a nastavení v politike pre dané klientske zariadenie vykoná produkt lokálne liečenie podozrivého objektu.

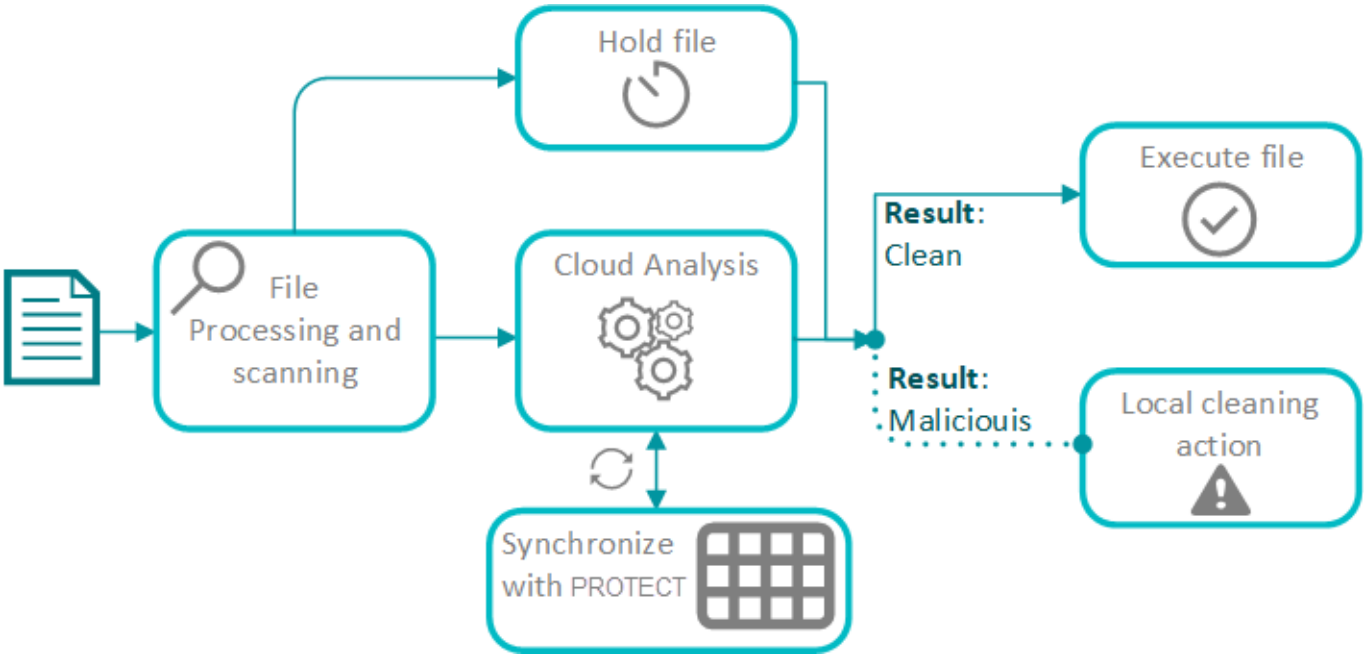
Nasledujúca schéma zobrazuje podrobný postup pri produkte ESET Mail Security:



Fungovanie služby ESET LiveGuard Advanced pri produkte ESET Endpoint Security/ESET Server Security

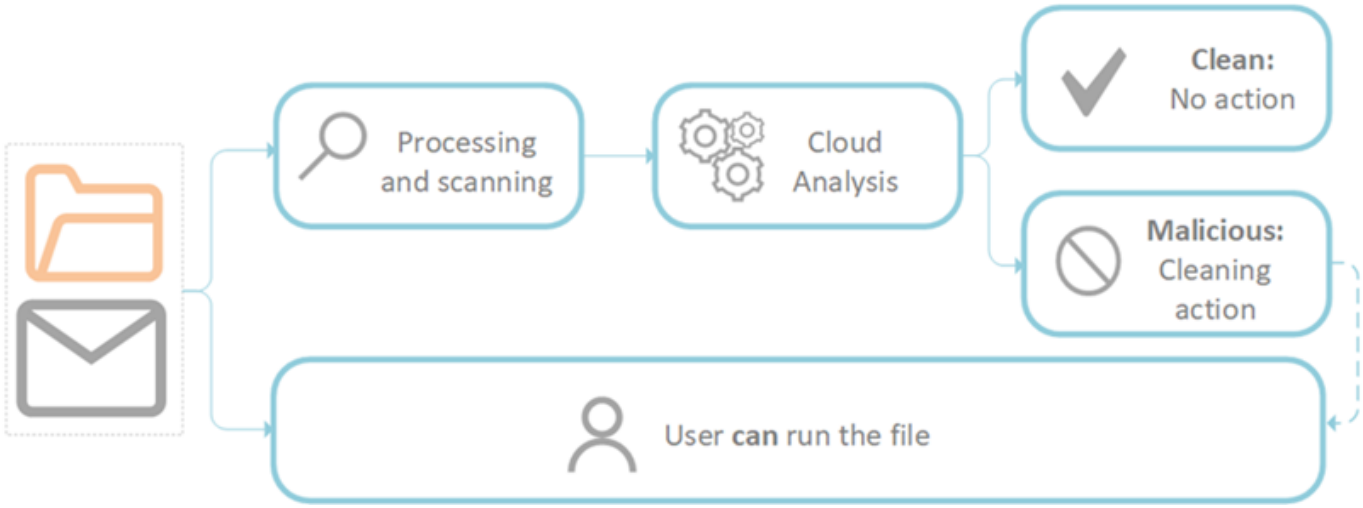
Nové alebo prichádzajúce súbory vybraných formátov zachytené pomocou ESET Endpoint Security/ESET Server Security sa skontrolujú a otvoria. V prípade, že program vyhodnotí súbor ako podozrivý, bude odoslaný na analýzu. Ide o súčasť proaktívnej ochrany. Môžete nastaviť časový úsek, počas ktorého nebude možné súbor spustiť a používateľ bude musieť počkať na výsledok analýzy. Výsledky analýzy sú uložené v cloudovej databáze (v cloude ESET). Na základe výsledkov analýzy a nastavení v politike pre dané klientske zariadenie vykoná bezpečnostný produkt ESET lokálne liečenie podozrivého objektu (proces je ukončený okamžite alebo bude zablokované jeho ďalšie spustenie).

Nasledujúca schéma zobrazuje podrobný postup pri produktoch ESET Endpoint Security/ESET Server Security:



Fungovanie služby ESET LiveGuard Advanced pri produkte ESET Cloud Office Security

Každý súbor zachytený bezpečnostným riešením ESET Cloud Office Security je skontrolovaný a otvorený. V prípade, že je súbor pri kontrole vyhodnotený ako podozrivý, odošle sa na analýzu. Výsledky analýzy sú uložené v cloudovej databáze (v cloude ESET). ESET Cloud Office Security na základe výsledkov analýzy a nastavených bezpečnostných politík pristúpi k liečeniu. Viac informácií o politikách ESET Cloud Office Security nájdete v kapitole Nastavenia ochrany pre ESET LiveGuard Advanced.

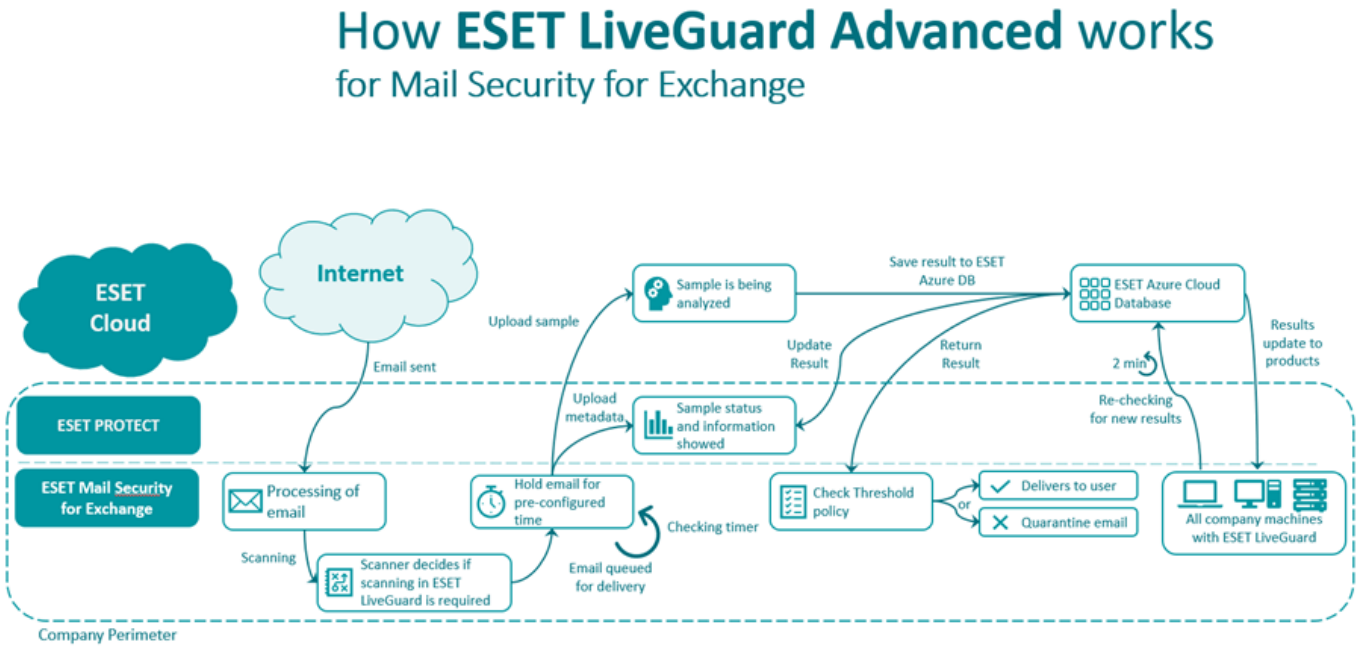


ESET Mail Security

Každý e-mail detegovaný programom ESET Mail Security s aktívnou službou ESET LiveGuard Advanced je spracovaný postupom popísaným v tejto kapitole. Prostredníctvom nastavení v rámci politiky môžete zadefinovať nasledujúce parametre:

- čas podržania e-mailu (len čo sa týka ochrany e□mailových schránok),
- úroveň zabezpečenia,
- akcia po detekcii (len čo sa týka ochrany hostiteľského servera).

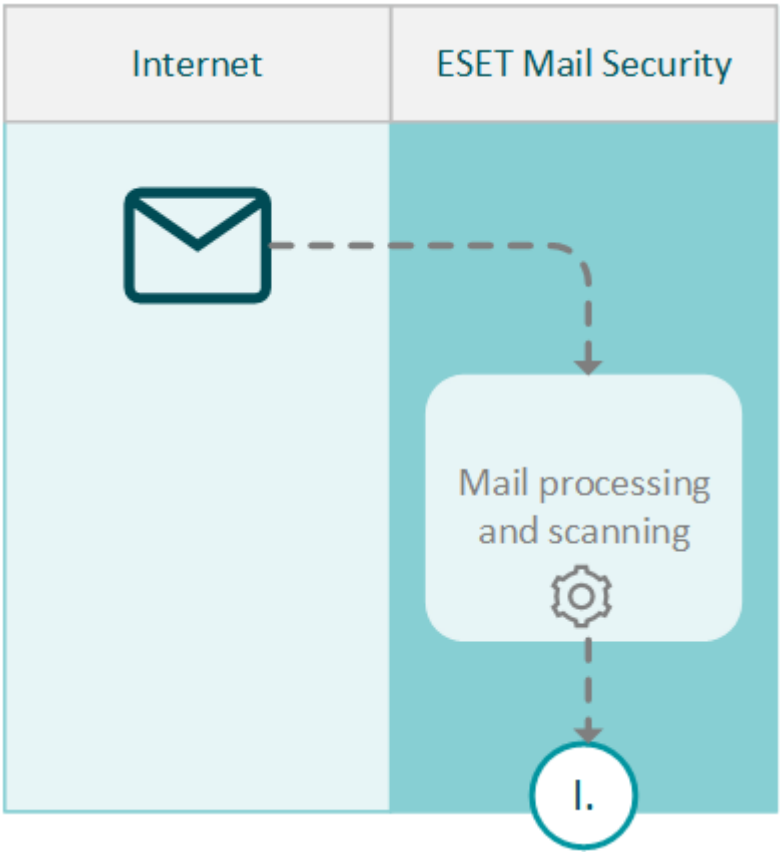
ESET Mail Security chráni hostiteľský server aj e-mailové schránky
Nižšie v tejto kapitole nájdete informácie o tom, ako ESET Mail Security s aktívnou službou ESET LiveGuard Advanced chráni e□mailové schránky. Čo sa týka ochrany hostiteľského zariadenia, zhoduje sa s ochranou popísanou pre ESET Server Security.



Analýza e-mailu pozostáva z nasledujúcich štyroch krokov:

1. Kontrola e-mailu

Pri stiahnutí e-mailu z internetu alebo iného nedôveryhodného zdroja Váš bezpečnostný produkt ESET tento e-mail spracuje a skontroluje.

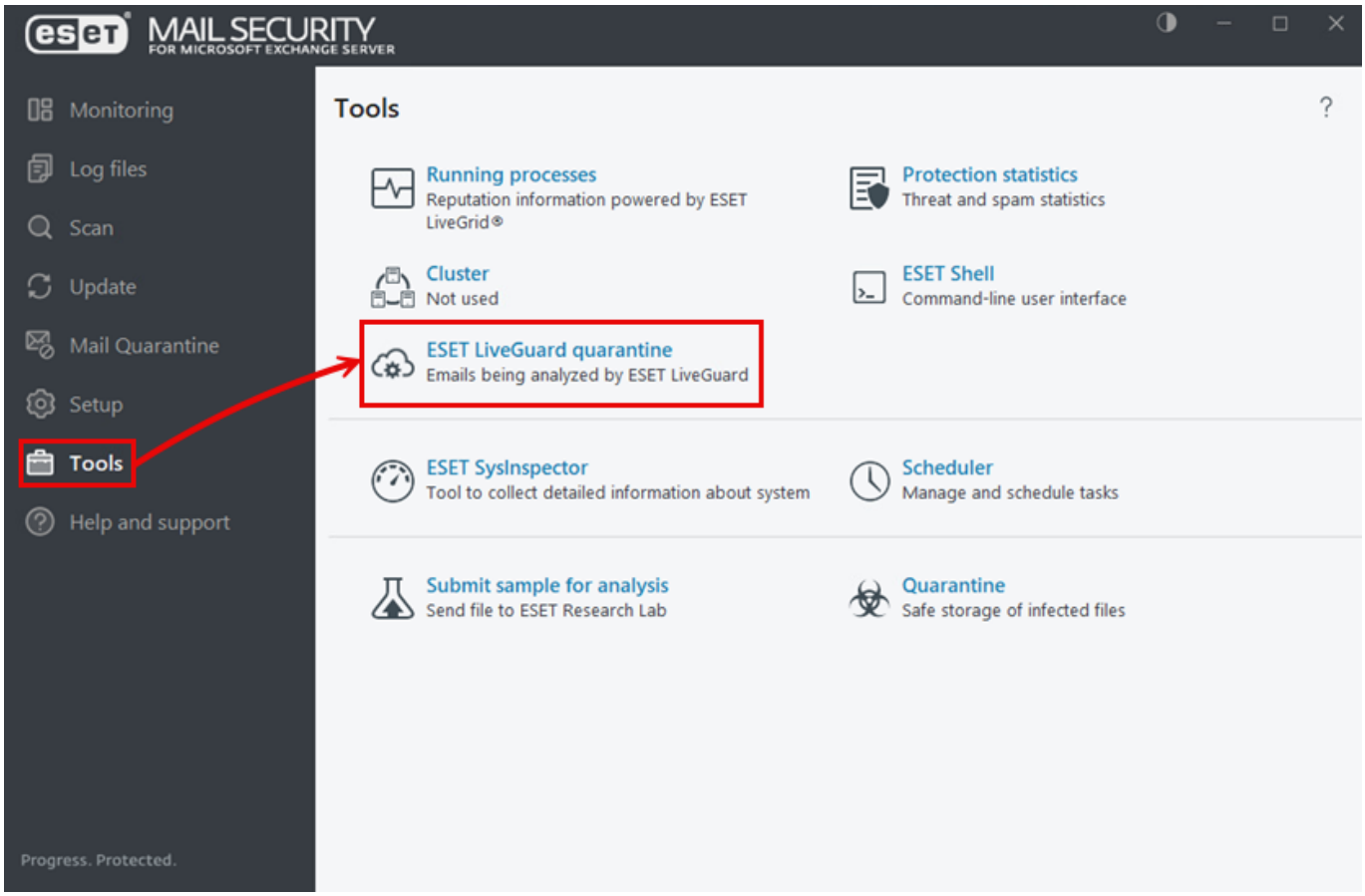


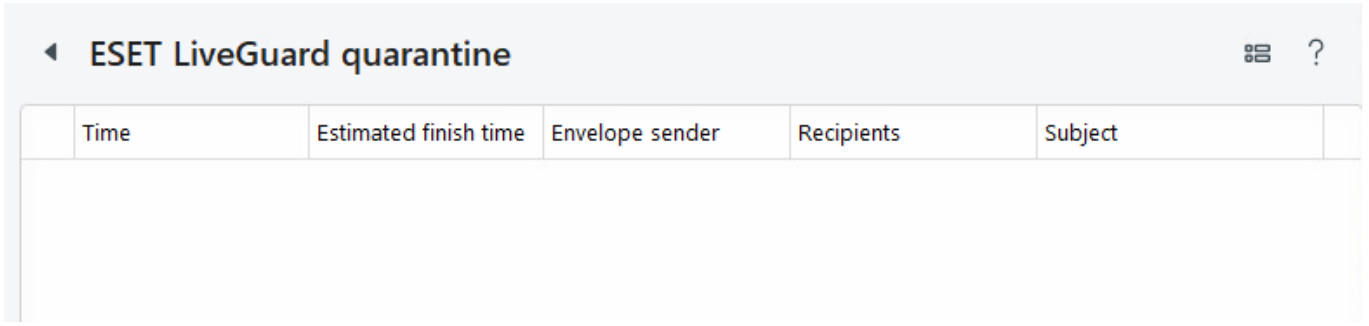
2. Analýza a doručenie e-mailu

V prípade, že bezpečnostný produkt vyhodnotí, že je potrebná analýza, e-mail bude na prednastavené časové obdobie podržaný. ESET LiveGuard Advanced medzitým zanalyzuje prílohu e-mailu. Ak výsledok analýzy

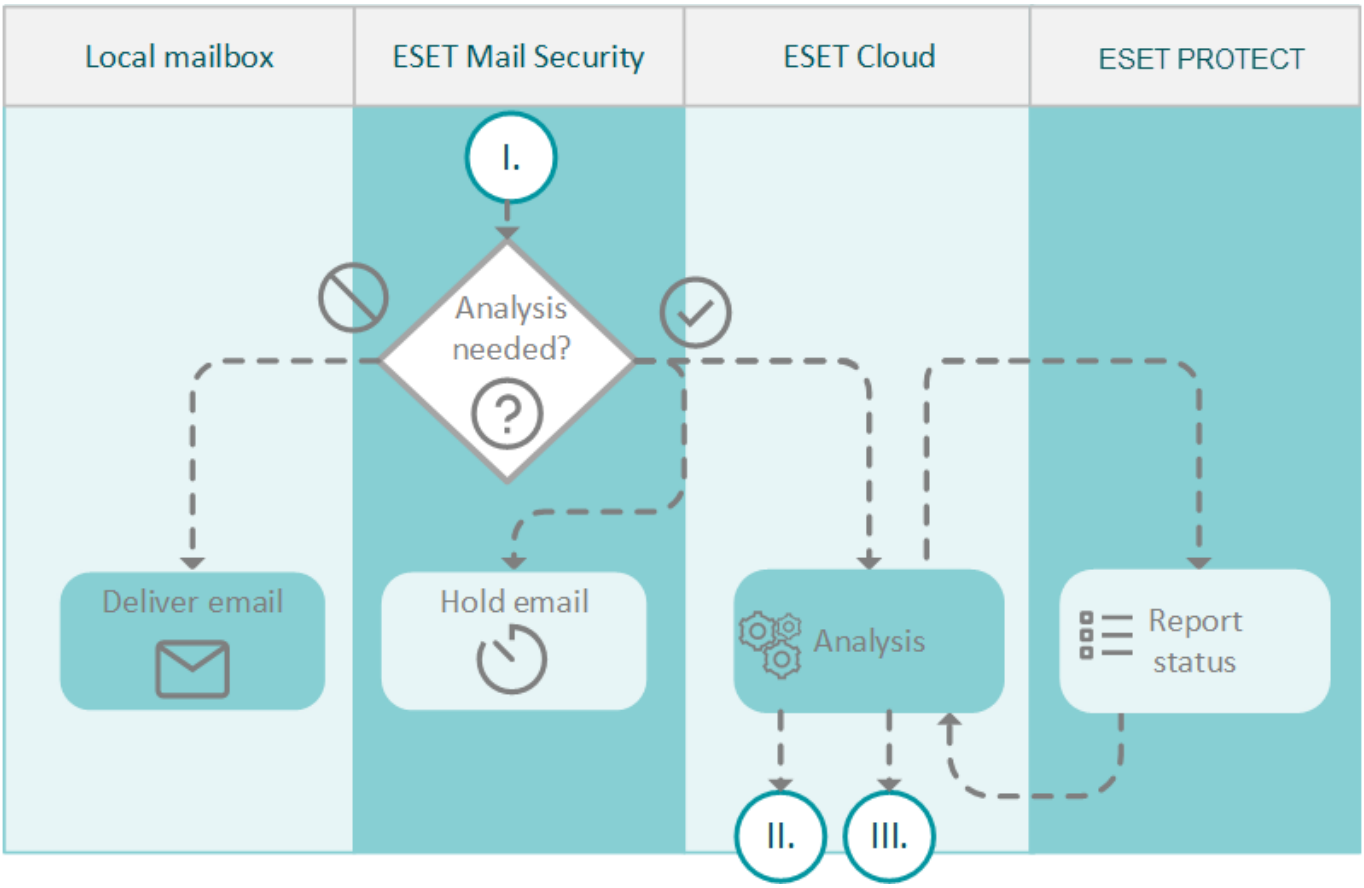
nepreukáže žiadnu hrozbu, e-mail bude okamžite doručený. Ak sa však zistí, že e-mail obsahuje nebezpečnú prílohu, bude vykonaná prednastavená akcia liečenia. Ak výsledok analýzy nestihne prísť ešte pred uplynutím prednastaveného času podržania e-mailu, bezpečnostný produkt e-mailovú správu doručí príjemcovi. V prípade, že výsledok analýzy preukazujúci hrozbu dorazí neskôr (do 2 minút), na všetkých počítačoch okamžite dôjde k zablokovaniu nebezpečnej prílohy e-mailu.

- Zoznam podržaných e-mailových správ nájdete v programe ESET Mail Security. Pre zobrazenie tohto zoznamu prejdite v hlavnom okne ESET Mail Security do sekcie **Nástroje** > **ESET LiveGuard Advanced**.



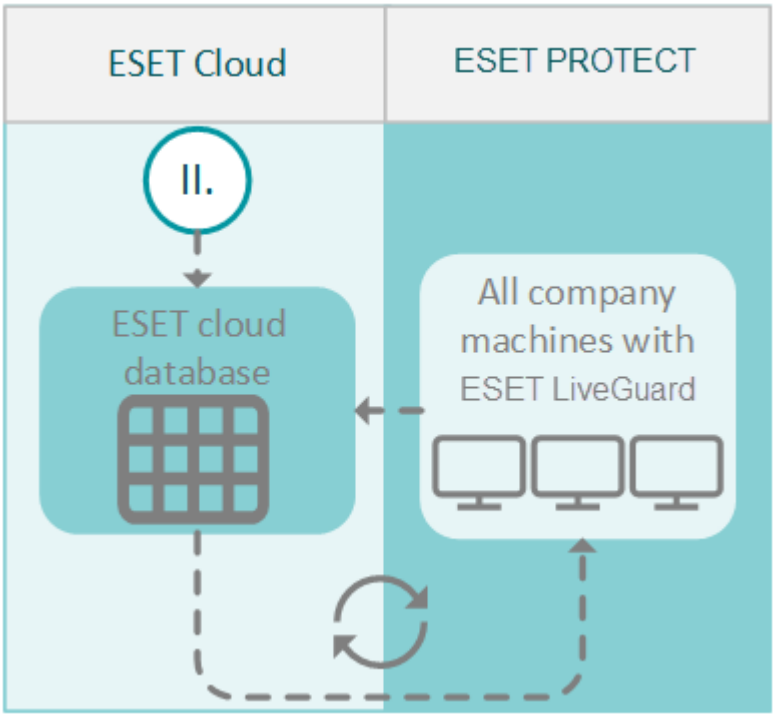


- Maximálny čas čakania na výsledok analýzy a podržania e-mailu nastavíte v politike pre produkt ESET Mail Security v sekcii Počítač > Ochrana s podporou cloudu > ESET LiveGuard > Maximálna doba čakania na výsledok analýzy.



3. Zdieľanie výsledku analýzy

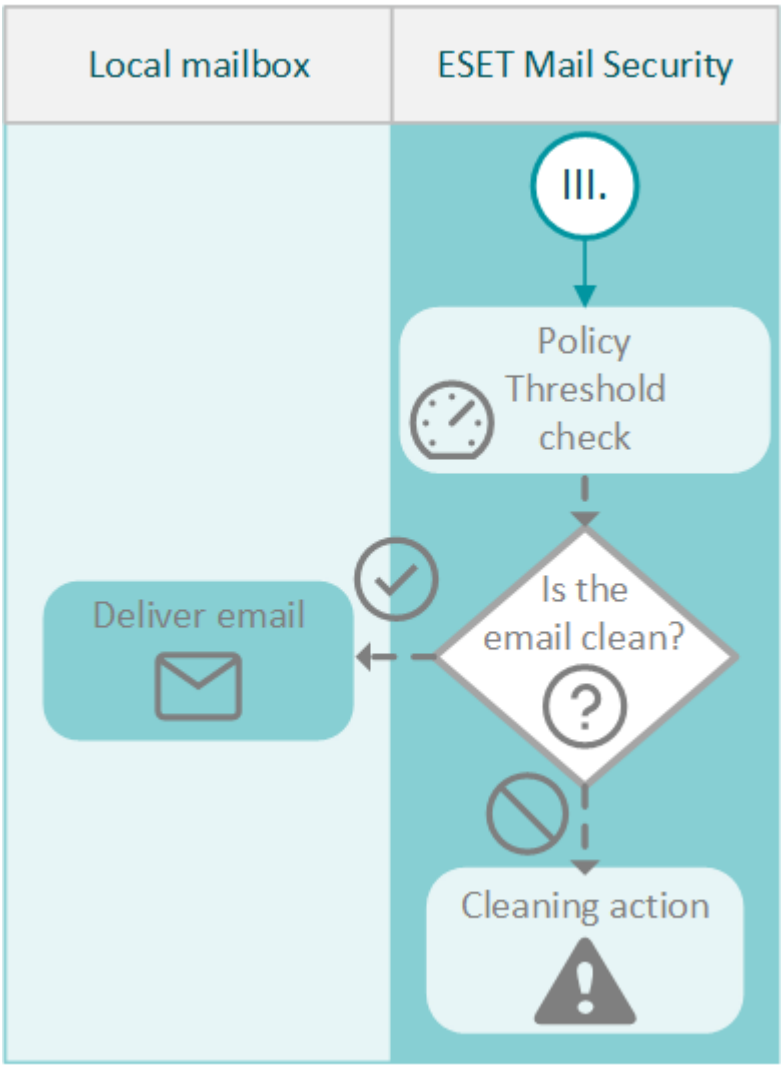
ESET LiveGuard Advanced používa štyri samostatné detekčné vrstvy a výsledok analýzy je uložený do databázy v cloude ESET. Obsah tejto databázy sa s ESET PROTECT On-Prem synchronizuje každú minútu. Všetky zariadenia s aktívnou službou ESET LiveGuard Advanced a bezpečnostným produktom ESET sú takisto synchronizované s cloudom ESET každé 2 minúty.



4. Vyhodnotenie nastavenej politiky a liečenie

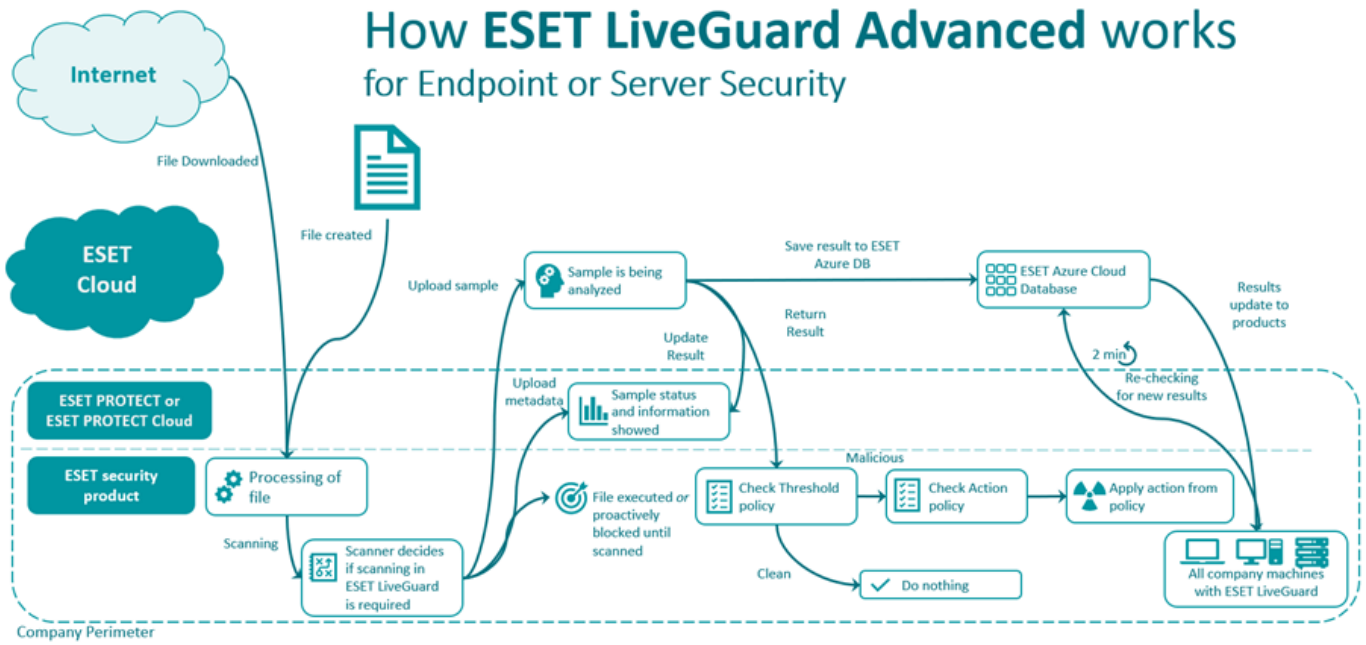
Výsledok analýzy je zaslaný aj bezpečnostnému produktu ESET, ktorý e-mail opätovne skontroluje. Ak e-mail neobsahuje žiadnu hrozbu, bude doručený (ak ešte neuplynul prednastavený čas podržania e-mailu).

Nastavenia pre detekciu a akcie súvisiace s liečením sa nachádzajú v sekcii **Server** v politike pre ESET Mail Security.



ESET Endpoint Security a ESET Server Security

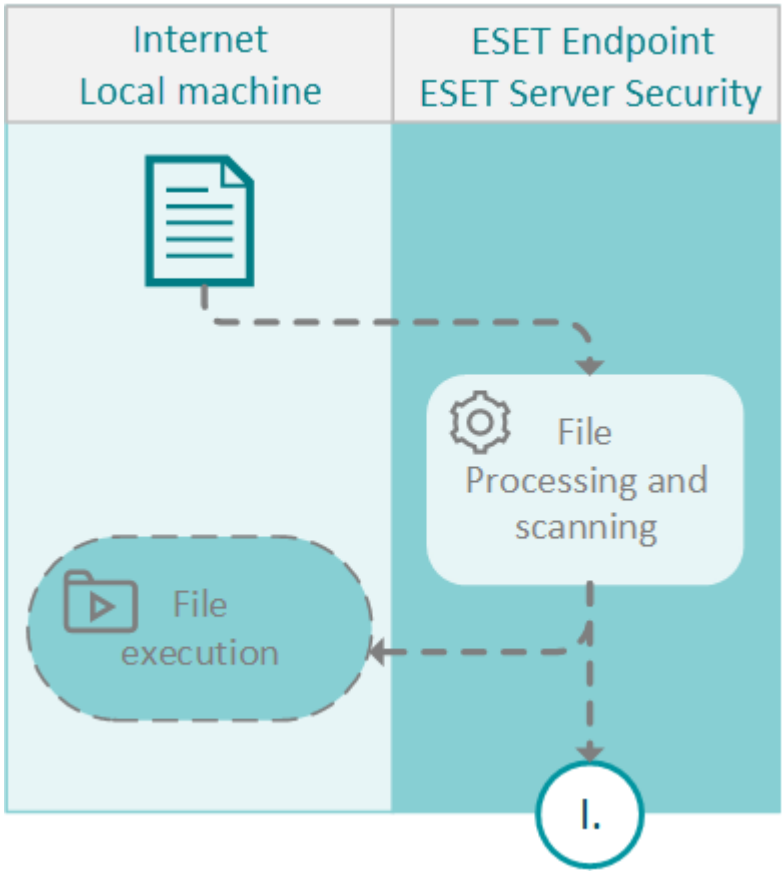
Každý súbor detegovaný programom ESET Endpoint Security alebo ESET Server Security s aktívnou službou ESET LiveGuard Advanced je spracovaný postupom popísaným v tejto kapitole. Prostredníctvom nastavení v rámci politiky pre skupinu alebo jednotlivé zariadenia môžete zadefinovať prah detekcie a akcie liečenia.



Analýza súboru pozostáva z nasledujúcich štyroch krokov:

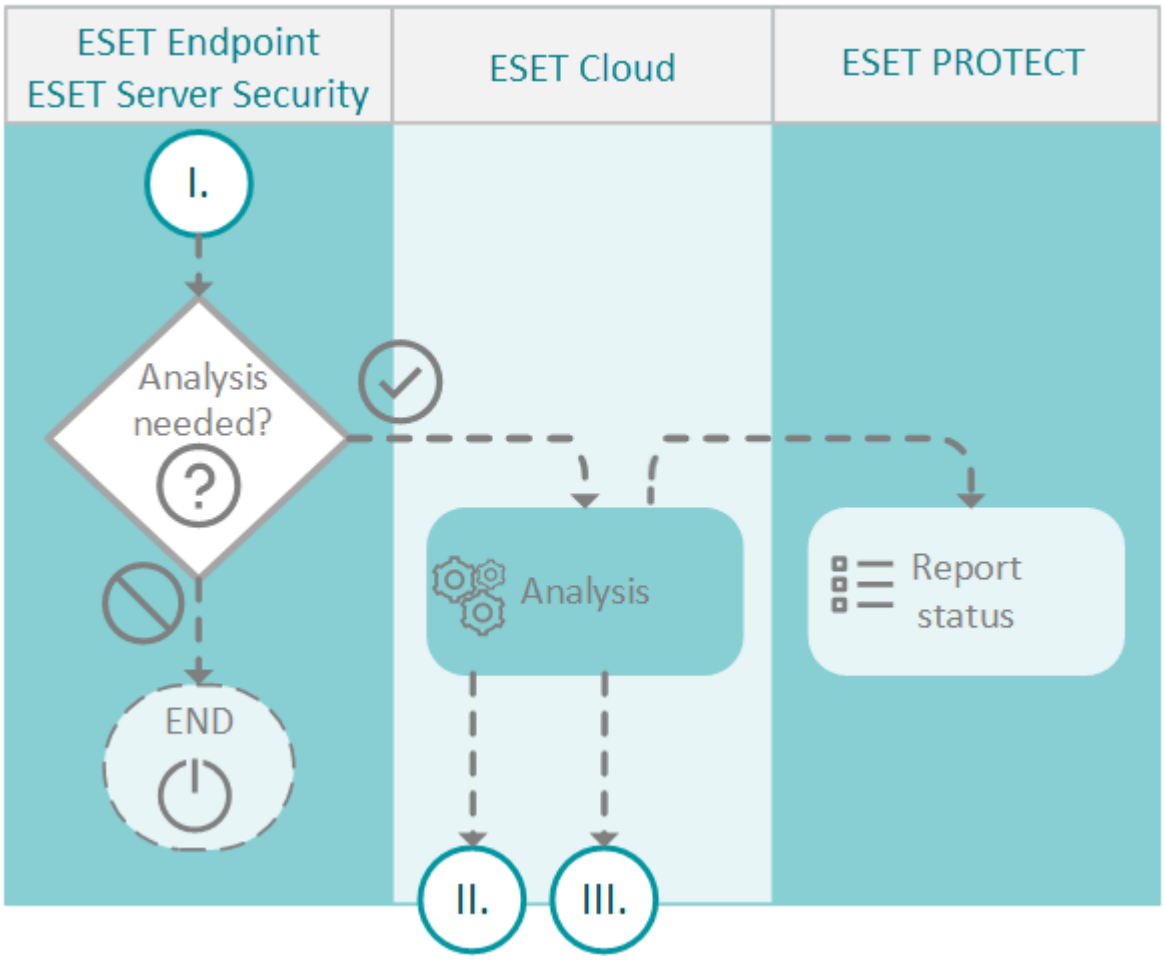
1. Kontrola súboru

V prípade stiahnutia súboru z internetu, skopírovania súboru na zariadenie alebo vytvorenia nového súboru, váš bezpečnostný produkt ESET tento súbor spracuje a skontroluje.



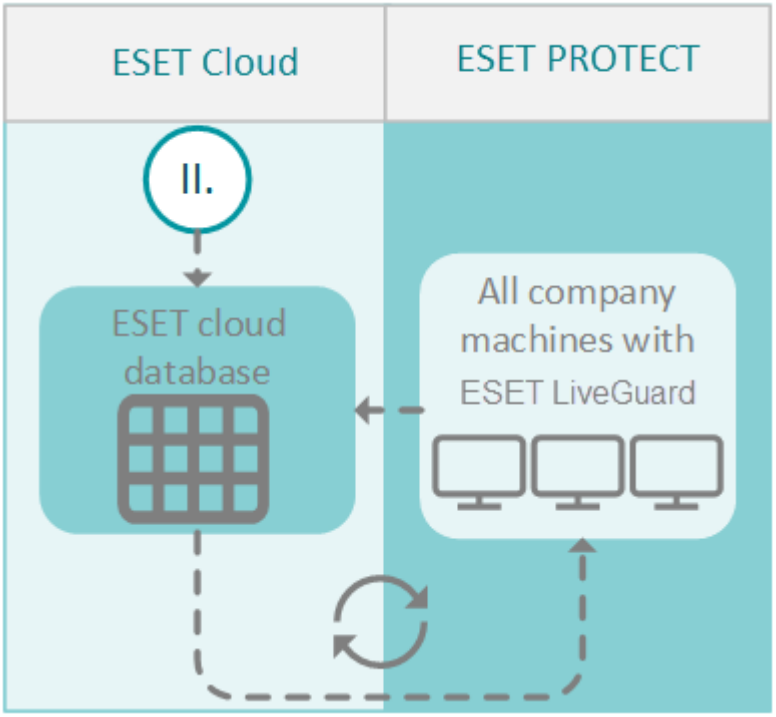
2. Analýza súboru

V prípade, že bezpečnostný produkt vyhodnotí, že je potrebná analýza, odošle súbor na analýzu. Štyri samostatné detekčné vrstvy súbor spracujú a poskytnú výsledok. Výsledky sú nahlasované do ESET PROTECT On-Prem. Ak analýza potrebná nie je, proces sa v tomto kroku skončí.



3. Zdieľanie výsledku analýzy

Výsledok analýzy je uložený do databázy v cloude ESET. Obsah tejto databázy sa s ESET PROTECT On-Prem synchronizuje každé dve minúty. Všetky zariadenia, na ktorých je aktívna služba ESET LiveGuard Advanced, dostávajú aktuálne informácie z cloudu ESET.

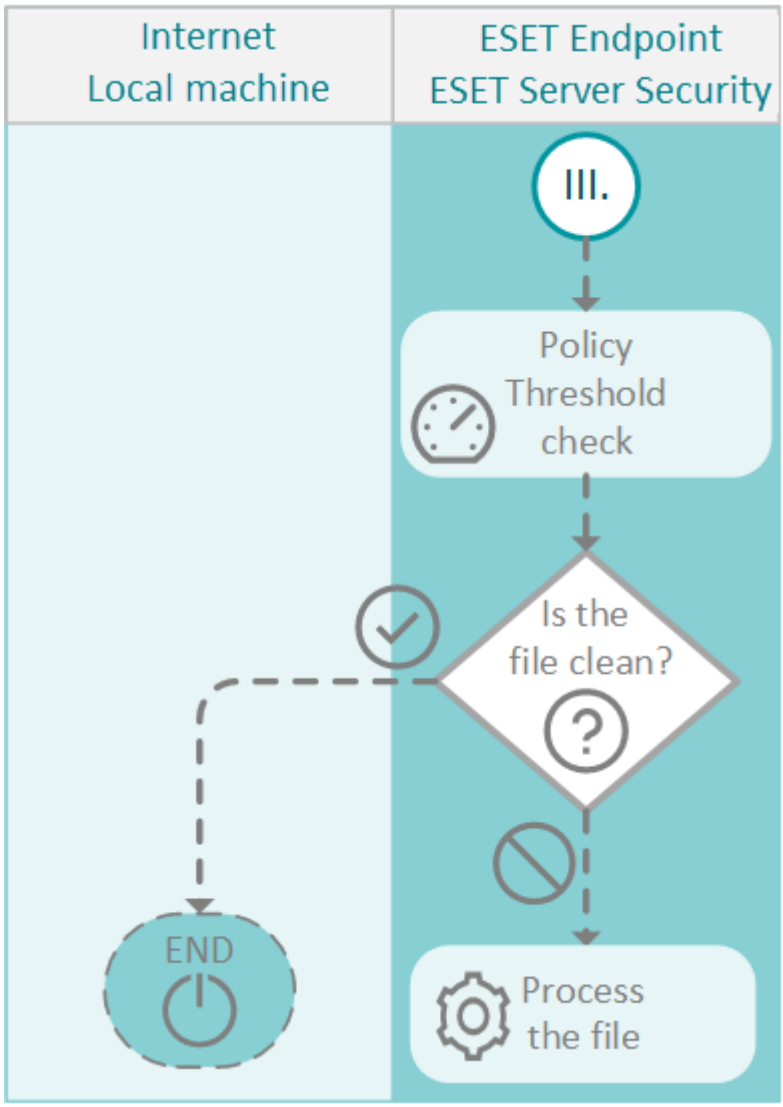


4. Vyhodnotenie lokálnej politiky

Výsledok analýzy je zaslaný aj bezpečnostnému produktu ESET, z ktorého bol súbor odoslaný. Bezpečnostný produkt ESET následne vykoná akciu nastavenú v politike (liečenie, odstránenie alebo žiadna akcia).

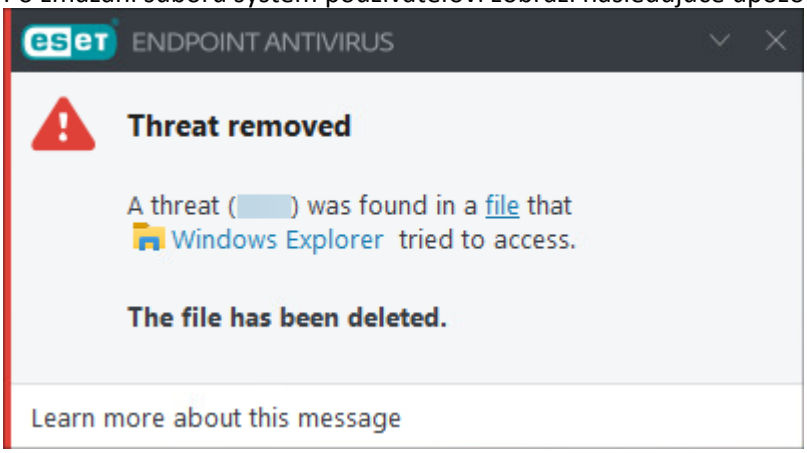
- Prah detekcie sa nastavuje v politike pre váš produkt ESET Endpoint Security/ESET Server Security v sekcii **Detekčné jadro** > **Ochrana s podporou cloudu** > **ESET LiveGuard Advanced** > **Prah detekcie**

- Akcia, ktorá má byť vykonaná so škodlivým objektom, sa nastavuje v politike pre váš produkt ESET Endpoint Security/ESET Server Security v sekcii **Detekčné jadro** > **Ochrana s podporou cloudu** > **ESET LiveGuard Advanced** > **Akcia po detekcii**



Príklad upozornenia

Ak ESET LiveGuard Advanced vyhodnotí súbor ako škodlivý, ESET Endpoint Security spustí akciu liečenia. Po zmazaní súboru systém používateľovi zobrazí nasledujúce upozornenie:



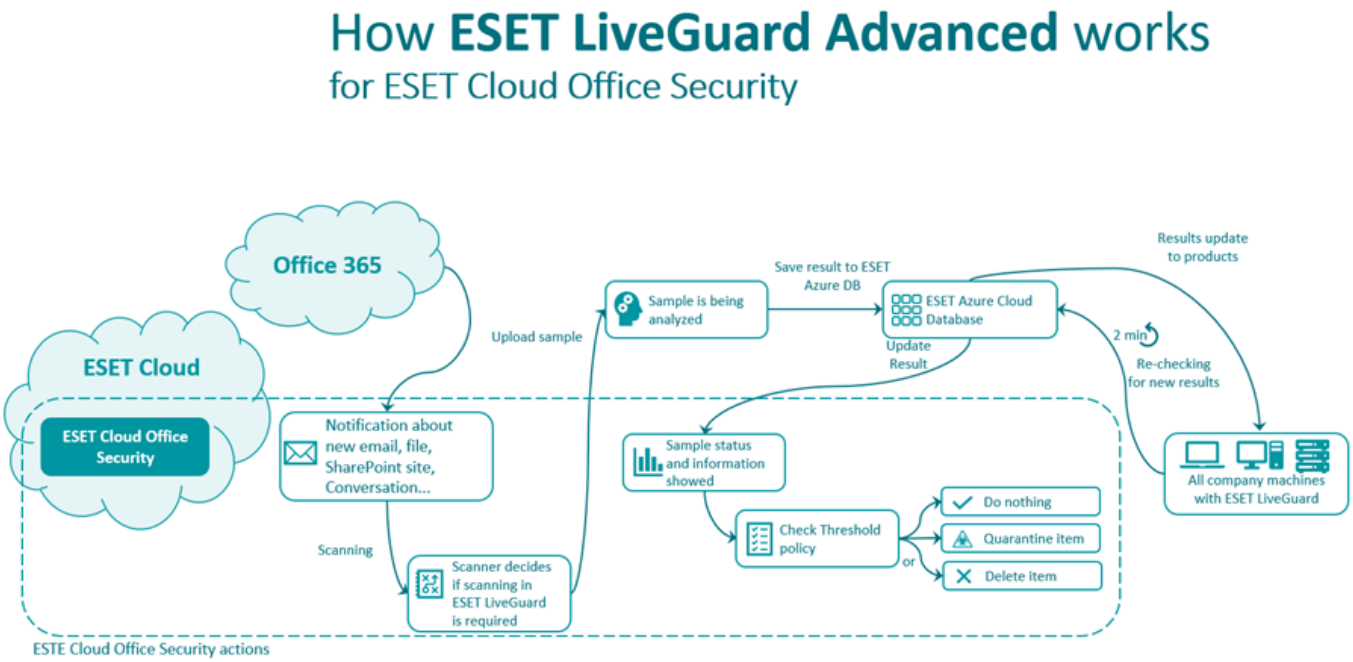
ESET Cloud Office Security

ESET Cloud Office Security využíva ESET LiveGuard Advanced na analýzu nových hrozieb. Nevyžaduje konzolu na správu produktov ESET (ESET PROTECT On-Prem/ESET PROTECT). Informácie, napríklad o všetkých odoslaných súboroch a výsledkoch ich analýzy, sú k dispozícii iba v riešení ESET Cloud Office Security.

• ESET Cloud Office Security neodosiela hlásenia do konzol na správu produktov ESET, a to ani v prípade, že je konzola pripojená k rovnakému licenčnému účtu.

• ESET Cloud Office Security zdieľa informácie o detekciách s koncovými zariadeniami pripojenými k rovnakému licenčnému účtu.

• ESET Cloud Office Security dokáže odosielať na analýzu podozrivé e-mailové prílohy a vzorky zdieľané cez Microsoft SharePoint, Teams a ďalšie programy balíka Office 365.



Analýza súboru z ESET Cloud Office Security pozostáva z nasledujúcich štyroch krokov:

1. Kontrola súboru

V cloudovom úložisku bol detegovaný nový súbor. Skener programu ESET tento súbor spracuje a skontroluje.

2. Analýza súboru

V prípade, že skener programu ESET vyhodnotí, že je potrebná analýza, odošle súbor na analýzu. Štyri samostatné detekčné vrstvy súbor spracujú a poskytnú výsledok, ktorý bude odoslaný do riešenia ESET Cloud Office Security. Ak analýza potrebná nie je, proces sa v tomto kroku skončí.

3. Zdieľanie výsledku analýzy

Výsledok analýzy je uložený do databázy v cloude ESET. O výsledkoch kontroly sú okamžite informované všetky zariadenia s aktívnou službou ESET LiveGuard Advanced, ktoré sú aktivované pomocou rovnakého licenčného účtu.

4. Rozhodnutie o akcii na základe politiky ESET Cloud Office Security

Výsledky analýzy sú zaslané späť do produktu ESET Cloud Office Security. Ten následne vykoná akciu nastavenú v politike (liečenie, odstránenie alebo žiadna akcia). Viac informácií nájdete v kapitole Nastavenia ochrany pre ESET LiveGuard Advanced.

Proaktívna ochrana

Proaktívna ochrana deteguje iba súbory z nasledujúcich zdrojov:

- súbory sťahované prostredníctvom podporovaného prehliadača,
- súbory sťahované z e□mailového klienta,
- súbory extrahované z nezašifrovaných aj zašifrovaných archívov prostredníctvom podporovaných nástrojov na prácu s archívmi,
- spúšťané a otvárané súbory umiestnené na vymeniteľných zariadeniach.

Ak je súbor podozrivý, proaktívna ochrana blokuje jeho spustenie do momentu, kým detekčné vrstvy nedokončia analýzu.

Podporované aplikácie a zariadenia

Táto funkcia je dostupná pre produkty nainštalované na zariadeniach s operačným systémom:

- Windows – všetky podporované produkty ESET Endpoint a produkt ESET Server Security vo verzii 7.2 a novších, produkt ESET Mail Security vo verzii 7.2 a novších.
- Linux - všetky podporované produkty.

Podporované aplikácie a zariadenia na systéme Windows

Webové prehliadače	E-mailové klienty	Nástroje pre prácu s archívmi	Vymeniteľné zariadenia
Internet Explorer	Microsoft Outlook	WinRAR	USB flash disk
Microsoft Edge	Mozilla Thunderbird	WinZIP	USB pevný disk
Chrome	Microsoft Mail	Vstavaný nástroj na extrakciu archívov vo Windows Prieskumníkovi	CD/DVD
Firefox		7zip	Disketa
Opera			Vstavaná čítačka pamäťových kariet
Prehliadač Brave			

Súbory kopírované pomocou Windows Prieskumníka z vylúčeného umiestnenia do chráneného umiestnenia sú blokované proaktívnou ochranou, pretože ESET LiveGuard Advanced rozpoznáva `explorer.exe` ako nástroj pre prácu s archívmi.

Podporované aplikácie a zariadenia na systéme Linux

Webové prehliadače	E-mailové klienty	Nástroje pre prácu s archívmi	Vymeniteľné zariadenia
Chrome	Mozilla Thunderbird	Nepodporované na systéme Linux	USB flash disk
Firefox	Evolution		USB pevný disk
Opera	Mailspring		CD/DVD

Webové prehliadače	E-mailové klienty	Nástroje pre prácu s archívmi	Vymeniteľné zariadenia
Brave Browser	KMail		Disketa
Vivaldi	Geary		Vstavaná čítačka pamäťových kariet
	Mutt		
	claws mail		
	Alpine		

Používatelia ESET Cloud Office Security

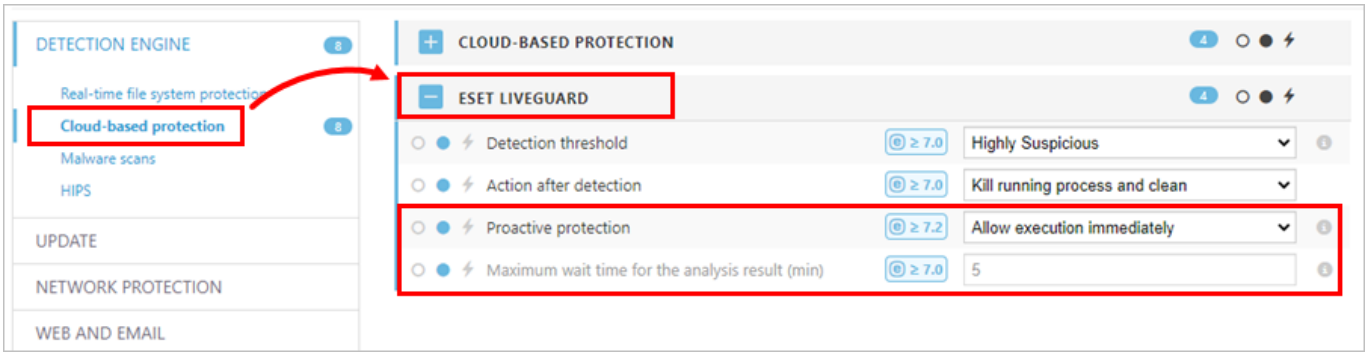
Proaktívna ochrana nie je v bezpečnostnom riešení ESET Cloud Office Security dostupná.

Konfigurácia ESET Endpoint Antivirus

Nastavenia proaktívnej ochrany môžete konfigurovať prostredníctvom politiky.

Vo Web Console prejdite do sekcie Politiky, vytvorte novú alebo upravte existujúcu politiku, vyberte cieľový produkt ESET a v konfigurácii kliknite na **Detekčné jadro** > **Ochrana s podporou cloudu** > **ESET LiveGuard Advanced** > **Proaktívna ochrana**.

- **Povoliť okamžité spustenie súboru** – používateľ môže spustiť daný súbor aj v prípade, že ešte prebieha jeho analýza. Po doručení výsledku analýzy produkt ESET vykoná zodpovedajúcu akciu.
- **Blokovať spustenie súboru do doručenia výsledku analýzy** – používateľ môže daný súbor spustiť až po dokončení jeho analýzy.

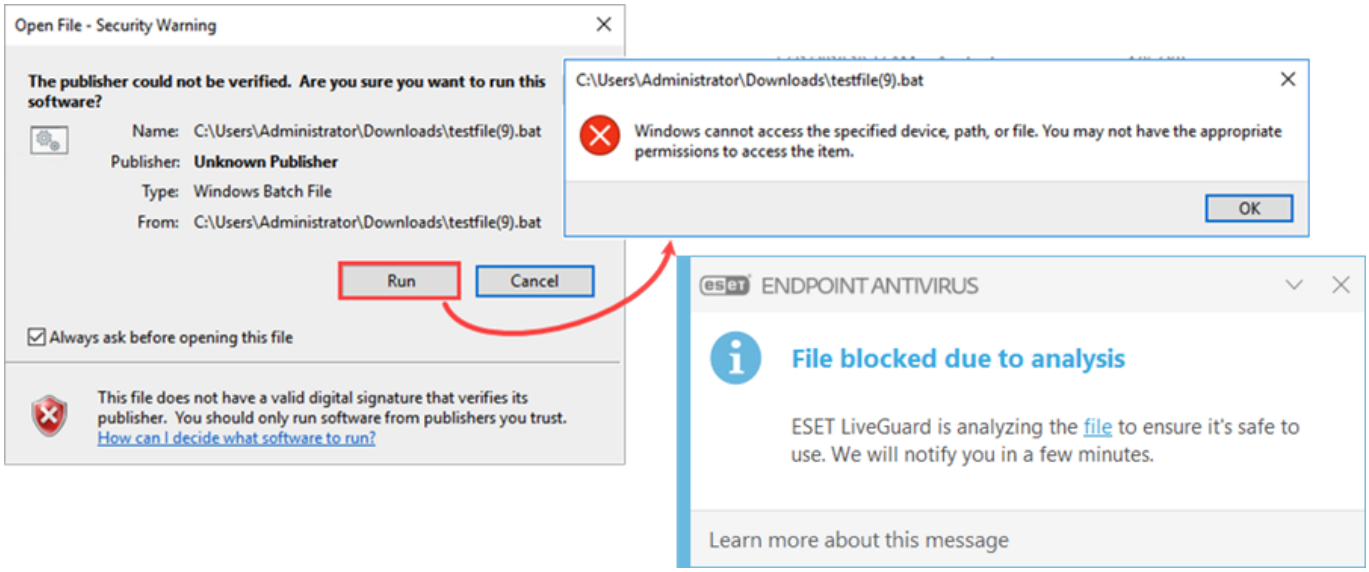


Používanie proaktívnej ochrany

Pri prvom spustení súboru, ktorý bol vyhodnotený ako podozrivý, môže váš operačný systém zobraziť výstražné upozornenie. Zároveň v takomto prípade produkt ESET zobrazí oznámenie, že sa začala analýza daného súboru. Ak sa však analýza dokončí ešte pred prvým spustením súboru, spomenuté oznámenie **Prebieha kontrola súboru** sa nezobrazí.

Používatelia systému Windows

V závislosti od zvolenej konfigurácie operačný systém Windows povolí alebo zablokuje spustenie súboru počas prebiehajúcej analýzy.

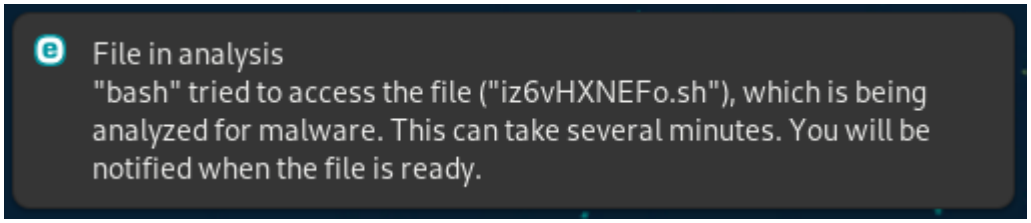


Používatelia systému Linux

ESET Server Security na systéme Linux nezobrazí žiadne upozornenie o prebiehajúcej analýze. Ak sa pokúsite spustiť súbor blokovaný proaktívnou ochranou:

- Operačný systém Linux zobrazí informáciu o zamietnutom prístupe.
- V termináli systém vráti správu `Operation not permitted`.

ESET Endpoint Security v prípade systému Linux s grafickým rozhraním zobrazí nasledujúce upozornenie:

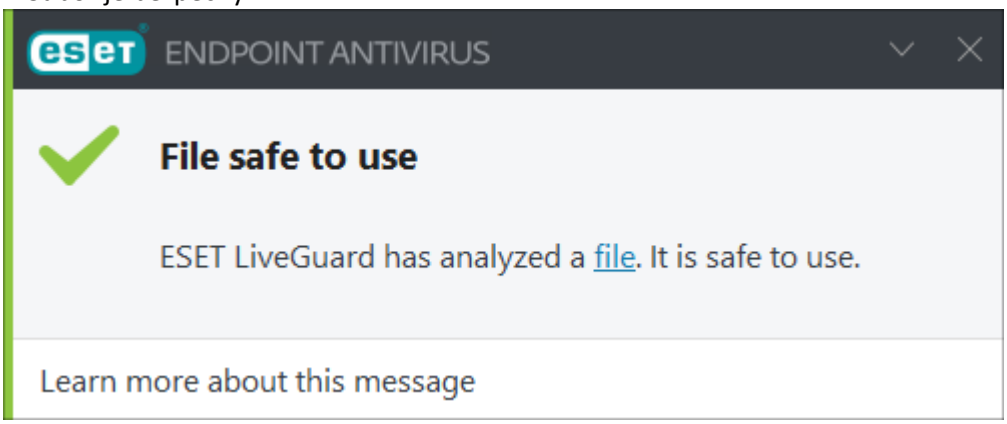


Výsledok analýzy

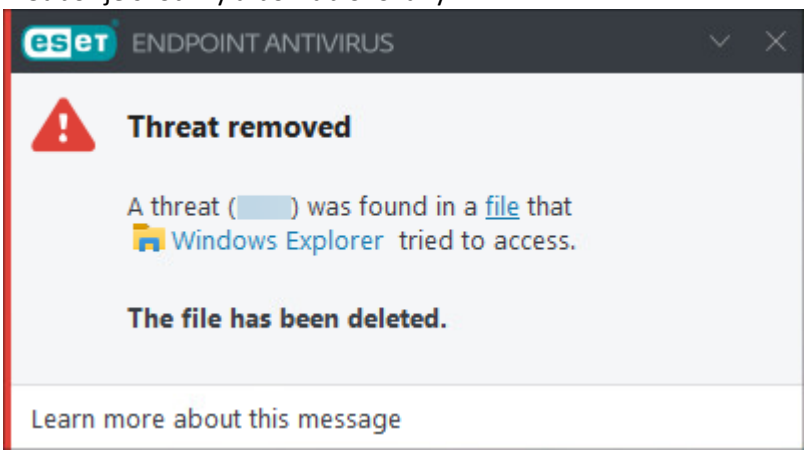
Doručenie výsledku pred uplynutím určeného času

V rámci konfigurácie môžete nastaviť maximálnu dobu čakania na výsledok analýzy. V prípade, že je výsledok analýzy doručený včas, môže sa zobraziť jedno z nižšie uvedených oznámení:

- Súbor je bezpečný:

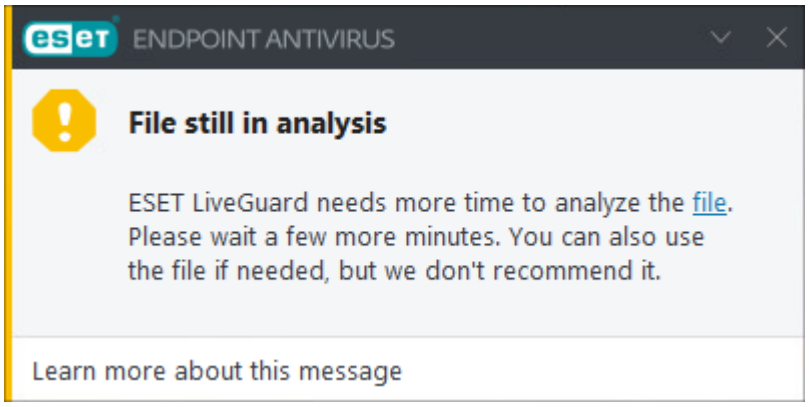


- Súbor je škodlivý a bol zablokovaný:



Doručenie výsledku po uplynutí určeného času

V prípade, že trvanie analýzy prekročí nastavenú maximálnu dobu čakania, súbor bude uvoľnený na používanie a zároveň sa používateľovi zobrazí informácia o prebiehajúcej analýze.



V prípade, že analýza preukáže, že súbor je škodlivý, produkt ESET zobrazí upozornenie a vykoná zodpovedajúcu akciu.

Zobrazenie zoznamu odoslaných súborov

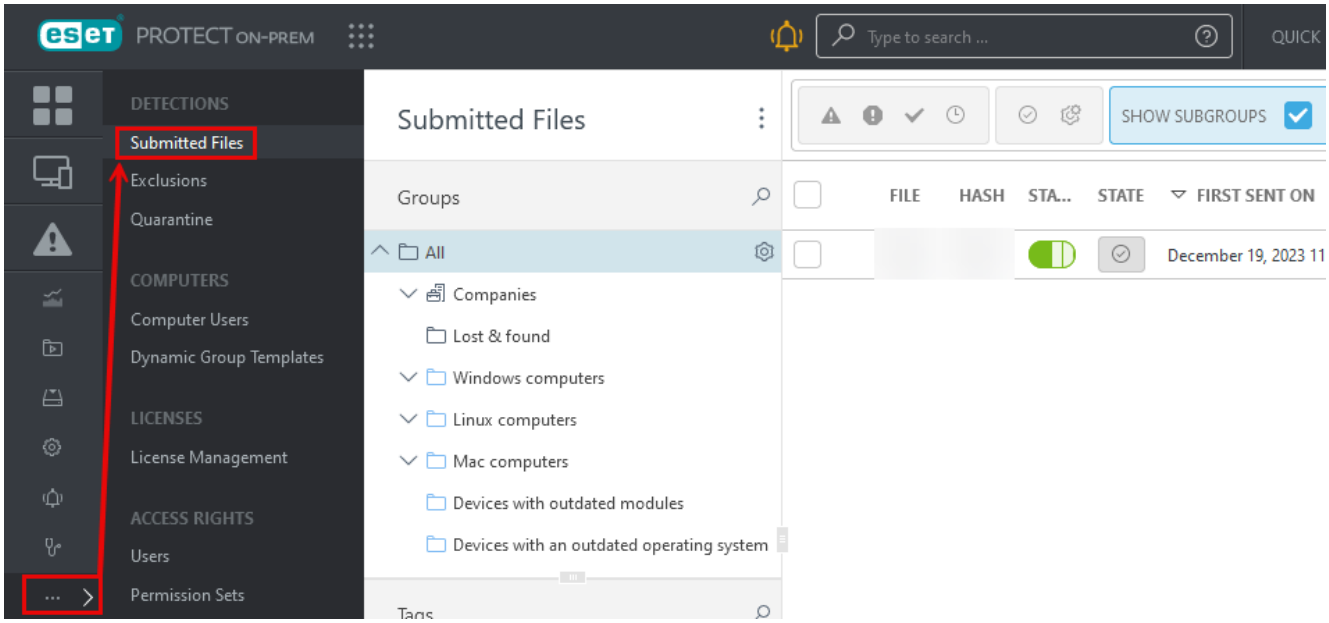
V sekcii **Odoslané súbory** nájdete zoznam súborov odoslaných na analýzu do spoločnosti ESET prostredníctvom ESET LiveGuard Advanced, ESET LiveGrid® alebo kontroly e-mailov. Správca Web Console má prístup k celému zoznamu všetkých odoslaných súborov. Táto funkcia je k dispozícii aj v prípade, že službu ESET LiveGuard Advanced zatiaľ nemáte aktivovanú. V tomto prípade uvidíte iba súbory odoslané prostredníctvom technológie ESET LiveGrid®.

> V sekcii **Odoslané súbory** sa používateľovi zobrazia len súbory odoslané zo zariadení, ku ktorým má daný používateľ pridelené prístupové povolenia aspoň na **čítanie**.

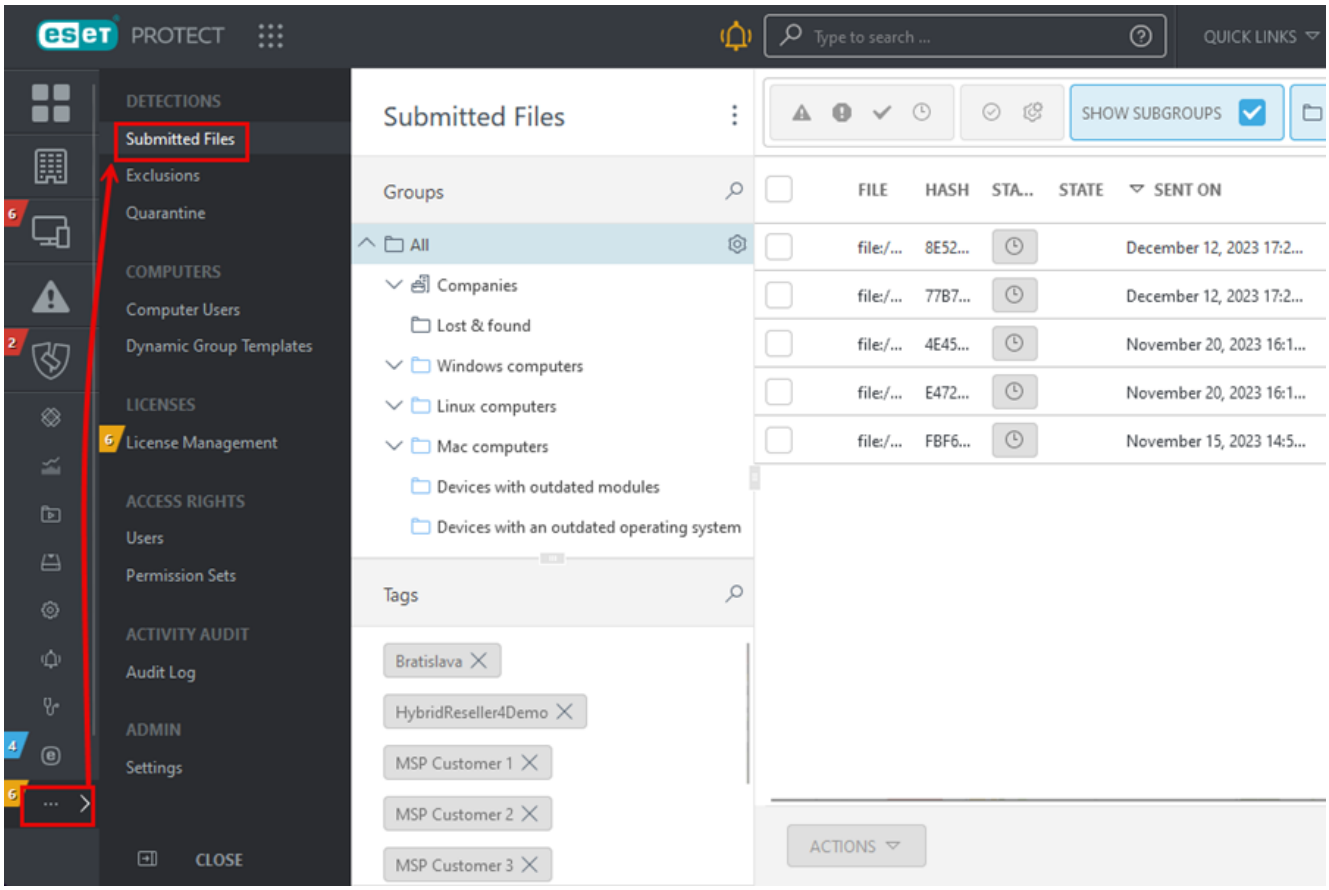
- **Prvýkrát odoslané** – tento stĺpec zobrazuje čas, kedy bol súbor prvýkrát odoslaný.
- **Naposledy spracované** – súbor môže byť odoslaný na analýzu viackrát, a to z viacerých počítačov a

spoločností. Tento stĺpec zobrazuje čas, kedy spoločnosť naposledy odoslala súbor.

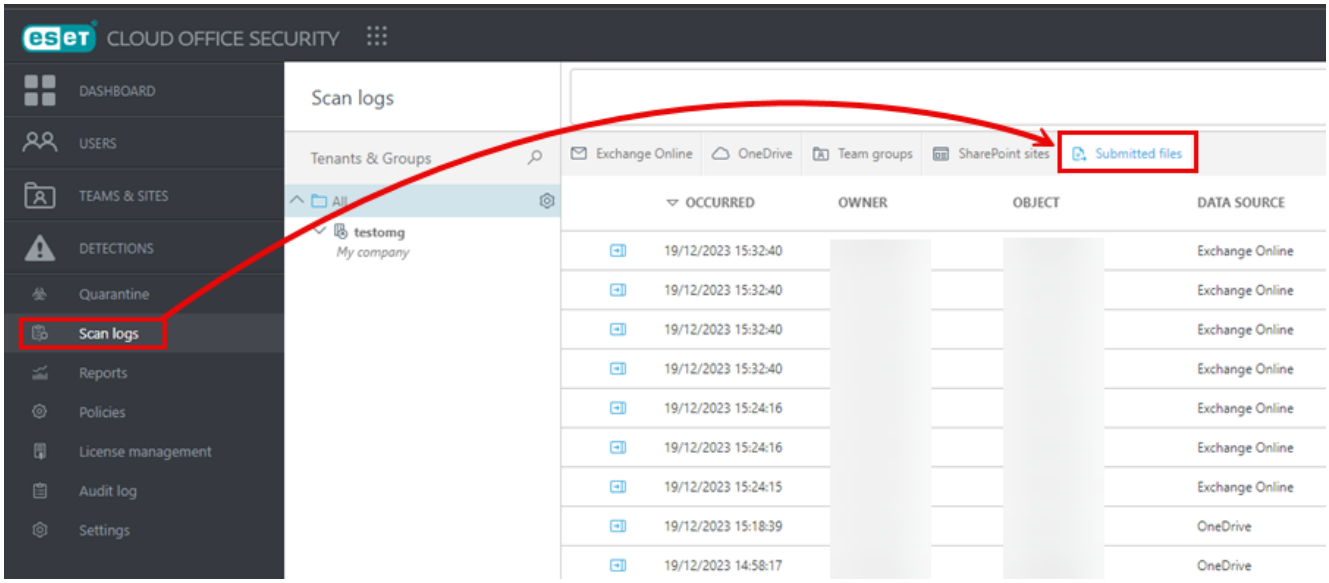
Používam ESET PROTECT On-Prem



Používam ESET PROTECT



Používam ESET Cloud Office Security

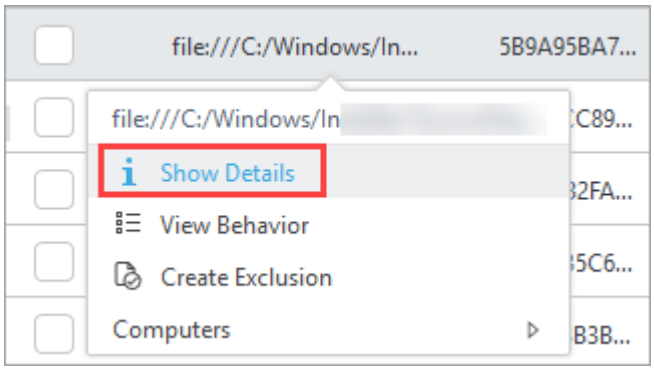


Podrobnosti o analyzovaných súboroch

Podrobnosti o analyzovaných súboroch nájdete vo Web Console v sekcii **Odoslané súbory**.

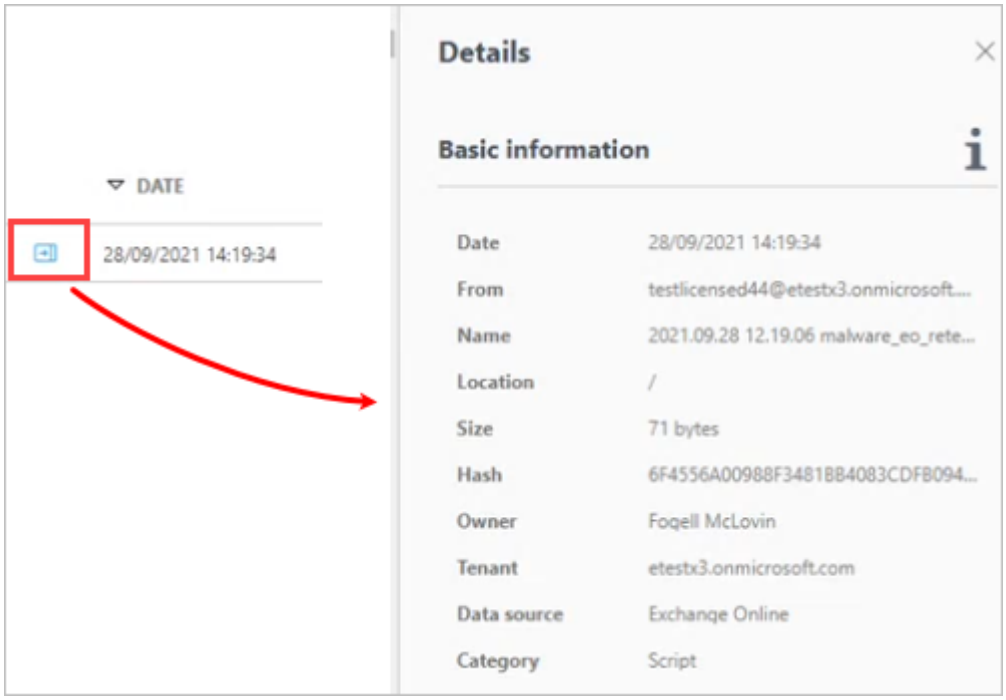
Používatelia konzoly na správu (ESET PROTECT On-Prem)

Vyberte súbor a kliknite na možnosť **Zobraziť podrobnosti**.



Používatelia ESET Cloud Office Security

Po kliknutí na modrú ikonu v riadku so súborom sa na obrazovke Odoslané súbory na bočnom paneli zobrazia podrobnosti o súbore.



Používatelia systému Linux

ESET Server Security pre Linux

Privilegovaní používatelia si môžu zoznam odoslaných súborov zobraziť v termináli pomocou príkazu:

```
/opt/eset/efs/bin/lslog -n
```

alebo

```
/opt/eset/efs/bin/lslog --sent-files
```

Viac informácií nájdete v dokumentácii k ESET Server Security.

Ak používate webové rozhranie:

1. Prihláste sa do webového rozhrania.

2. Kliknite na **Sent files** (Odoslané súbory).

ESET Endpoint Antivirus for Linux

Privilegovaní používatelia si môžu zoznam odoslaných súborov zobraziť v termináli pomocou príkazu:

```
/opt/eset/eea/sbin/lslog -n
```

alebo

```
/opt/eset/eea/sbin/lslog --sent-files
```

Vytvorenie reportu

Report s dátami týkajúcimi sa produktu ESET LiveGuard Advanced si môžete vygenerovať v konzole na vzdialenú správu. Využiť môžete prednastavené reporty, prípadne si vytvoriť vlastné.

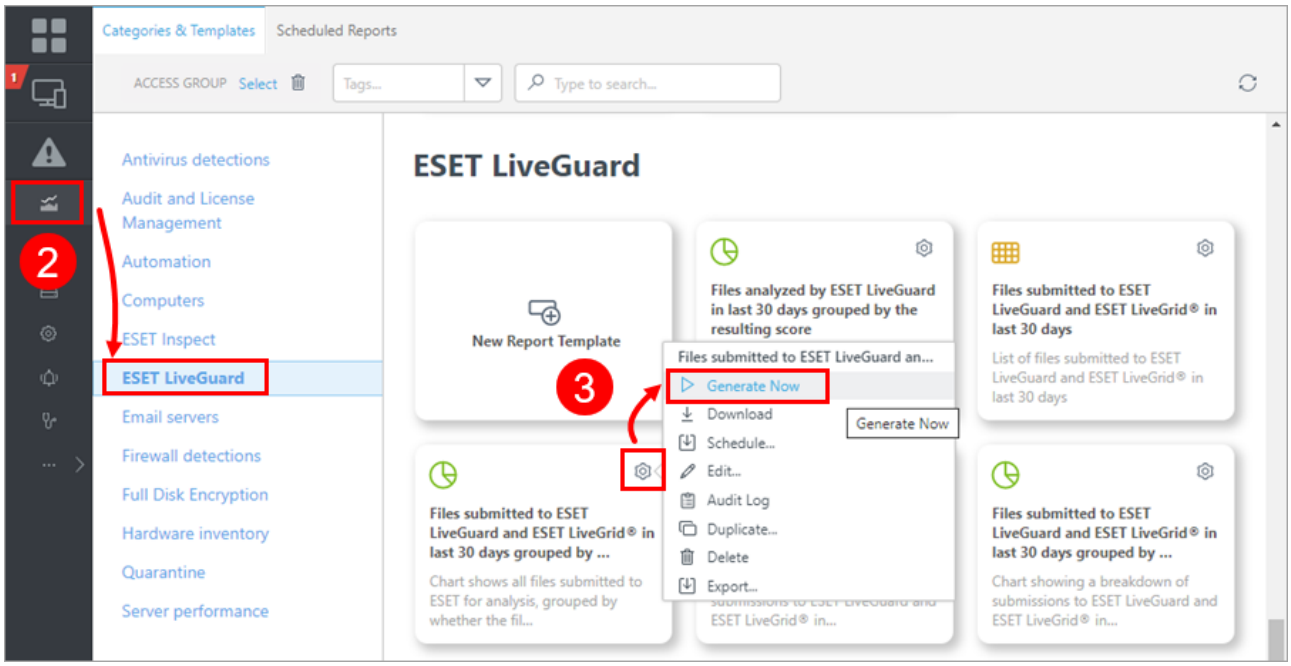
Nasledujúci postup sa týka ESET PROTECT On-Prem a ESET PROTECT.

Vstavané reporty

1.Prihláste sa do Web Console.

2.Kliknite na **Reporty** > **ESET LiveGuard**.

3.Vyberte si požadovaný report, kliknite na ikonu ozubeného kolesa a zvoľte možnosť **Generovať teraz**.

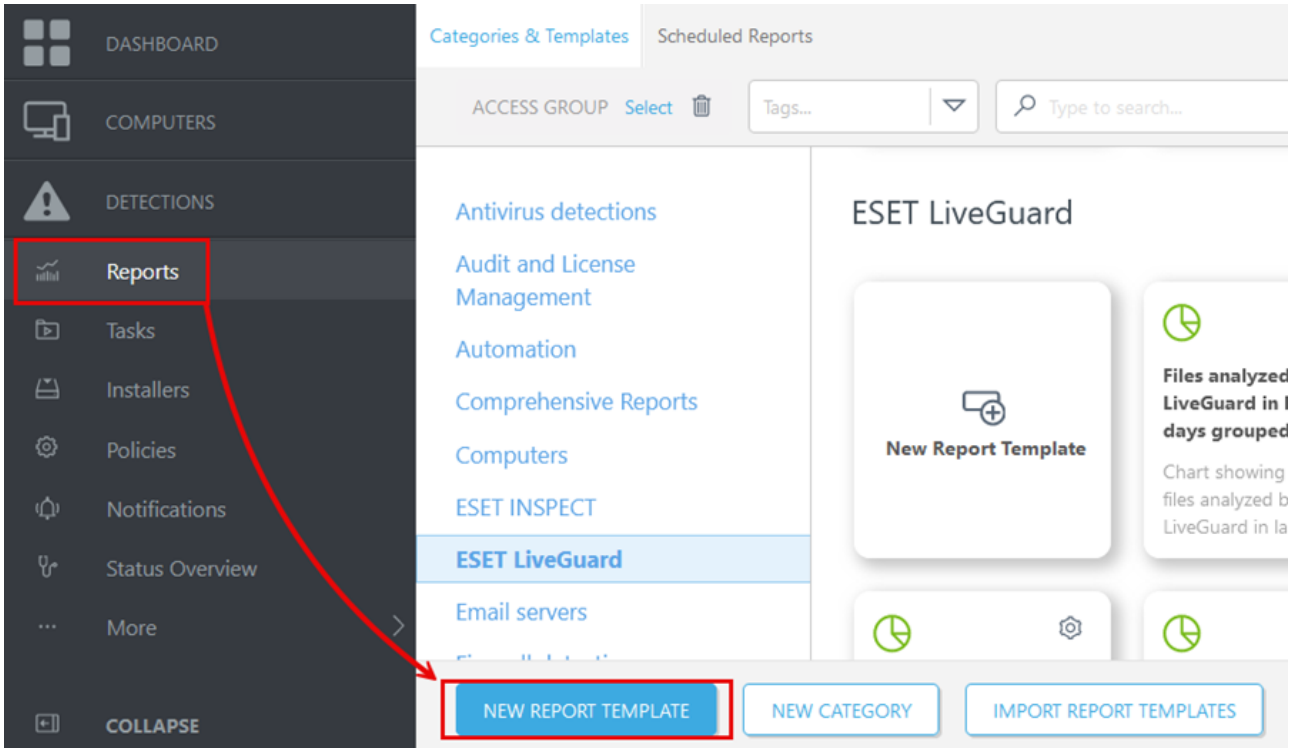


Vytvorenie vlastného reportu

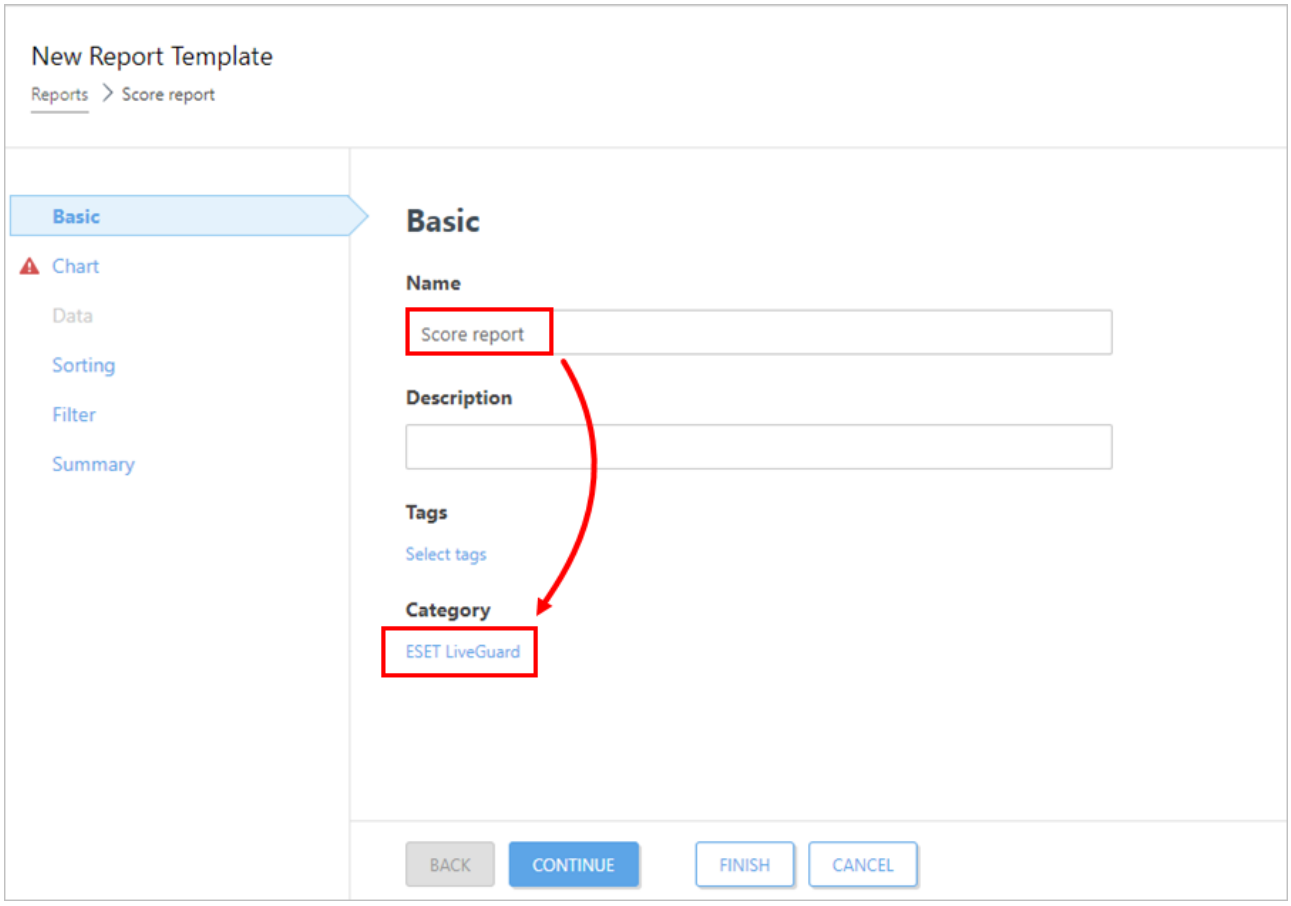
Ak chcete vytvoriť vlastný report, ktorý bude obsahovať skóre, cieľ a typ odosielaných súborov, postupujte nasledovne:

1.Prihláste sa do Web Console.

2.Kliknite na **Reporty** > **Nová šablóna reportu**.

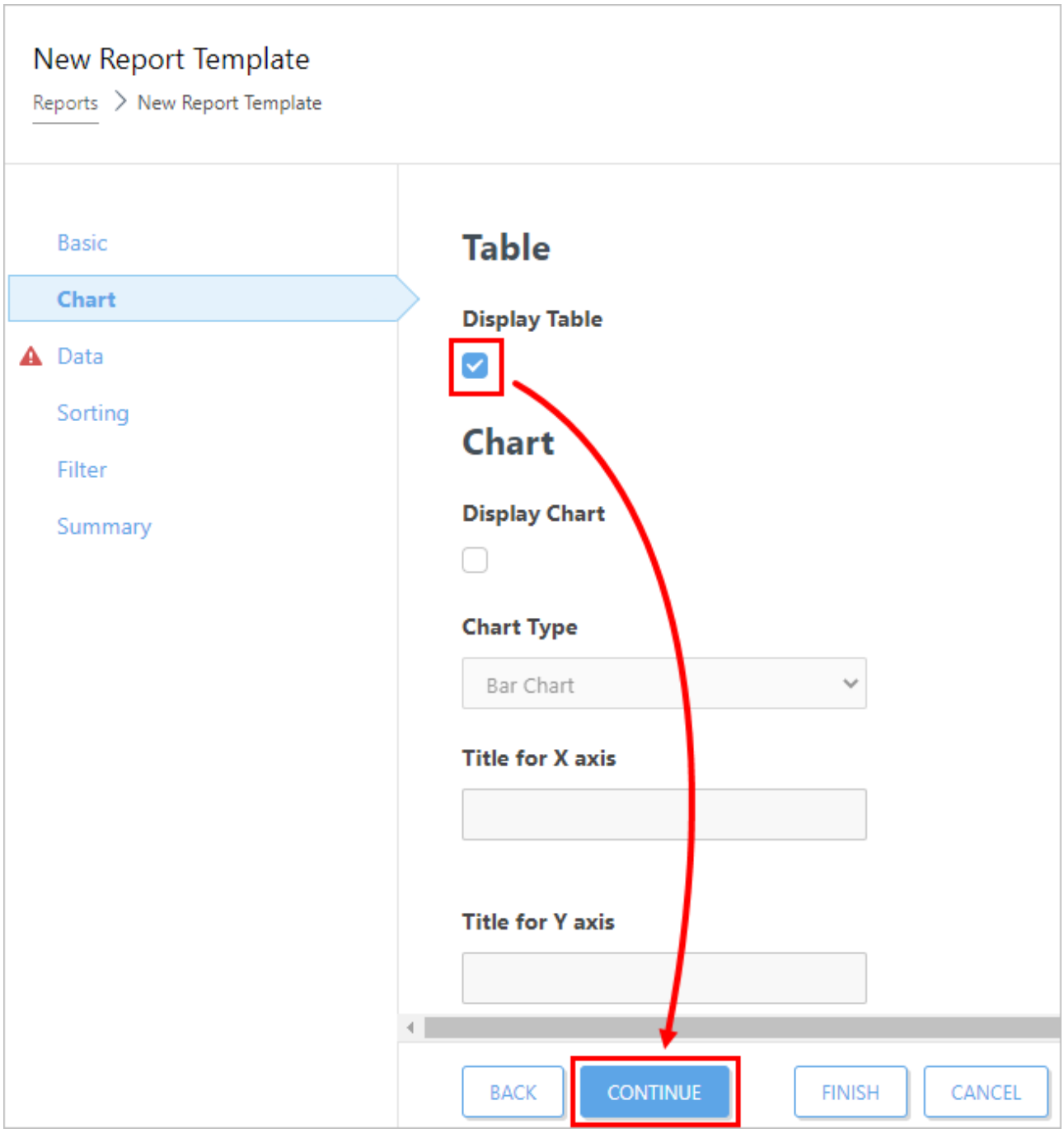


3.Zadajte pre novú šablónu **Názov** a ako **Kategóriu** vyberte **ESET LiveGuard**.

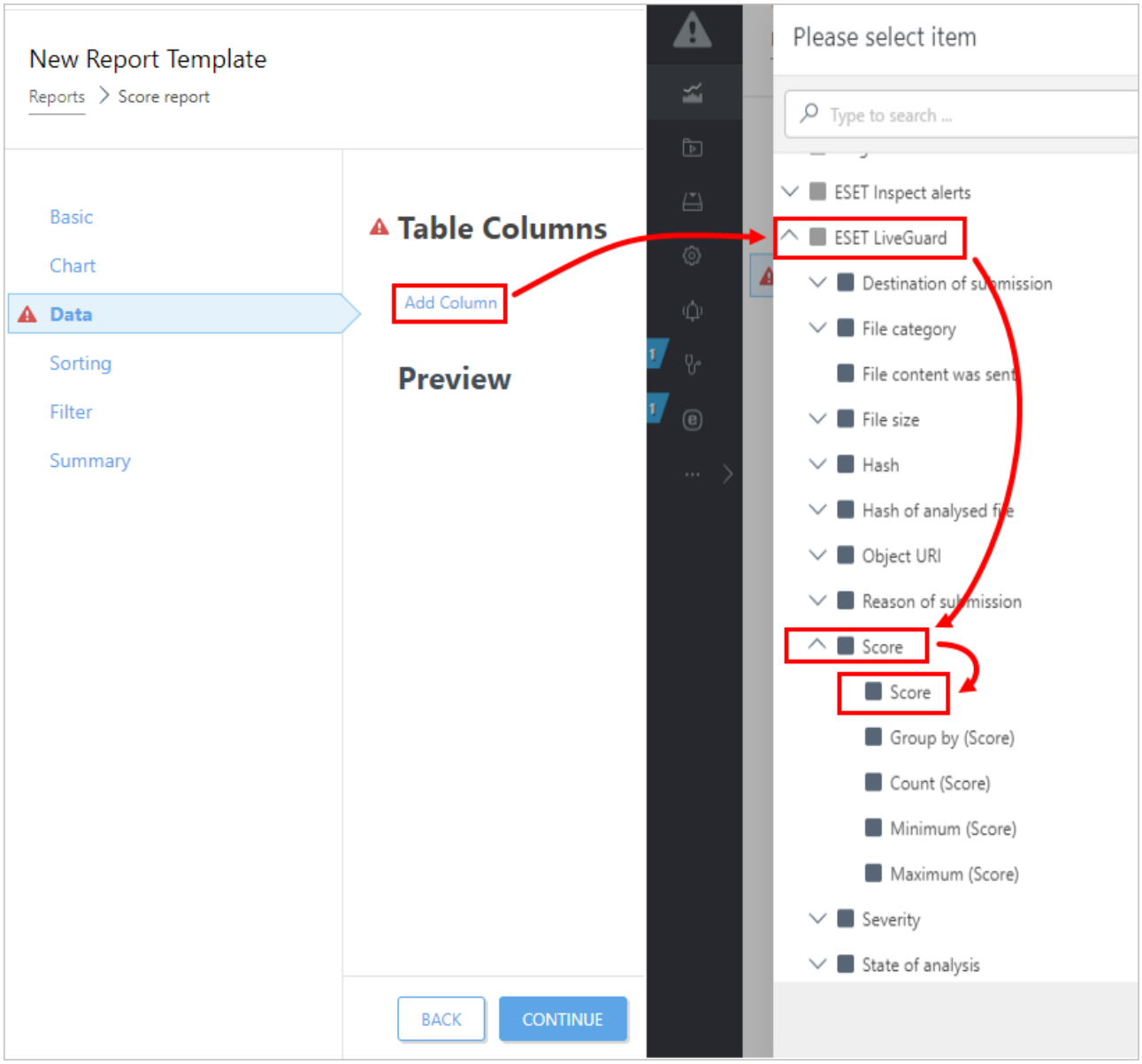


4.Kliknite na tlačidlo **Pokračovať**.

5.Označte možnosť **Zobraziť tabuľku** a kliknite na **Pokračovať**.



6.Kliknite na možnosť **Pridať stĺpec** a vyberte **ESET LiveGuard** > **Skóre** > **Skóre**. Pre potvrdenie kliknite na **OK**.

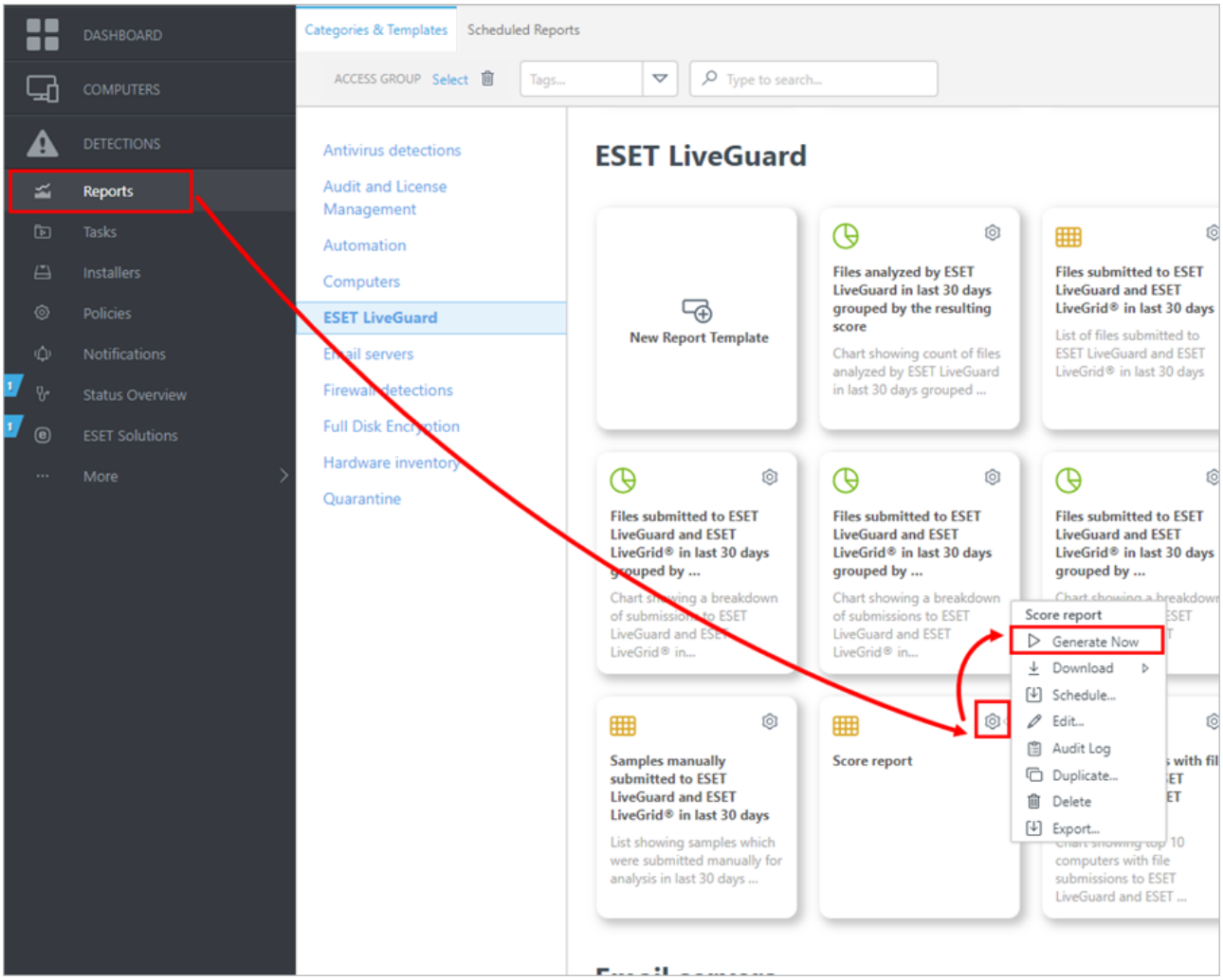


7.Kliknite na možnosť **Pridať stĺpec** a vyberte **ESET LiveGuard** > **Kategória súboru**. Pre potvrdenie kliknite na **OK**.

8.Kliknite na možnosť **Pridať stĺpec** a vyberte **ESET LiveGuard** > **Cieľ odoslania**. Pre potvrdenie kliknite na **OK**.

9.Kliknutím na **Dokončiť** uložte vytvorenú šablónu.

10. Ak chcete vytvoriť report, kliknite na **Reporty**, v rámci novovytvorenej šablóny kliknite na ikonu ozubeného kolesa a zvoľte možnosť **Generovať teraz**.



Výsledok analýzy

Po dokončení analýzy súboru odošle cloud ESET do konzoly na správu produktov ESET (alebo do riešenia ESET Cloud Office Security) informácie o výsledku analýzy a status súboru sa zmení z **Neznámeho** na jeden z nižšie uvedených. Informácie o súbore a krátky prehľad výsledkov analýzy nájdete v okne **Detaily súborov**.

Používatelia riešenia ESET Cloud Office Security nájdu zoznam odoslaných súborov a výsledky analýzy v protokoloch.



Parametre súboru	Popis
Počítač	Názov počítača, z ktorého bol súbor na analýzu odoslaný.

Parametre súboru	Popis
Používateľ	Používateľ počítača, ktorý súbor odoslal. V niektorých prípadoch môže ísť o systémového používateľa.
Dôvod	Dôvod odoslania (Automatický, Manuálny).
Odoslané do	Časť cloudu ESET, ktorá súbor prijala.
Hash	Hodnoty SHA-1 a SHA-256 hash odoslaného súboru.
Názov súboru	Názov súboru a úplná cesta k nemu v súborovom systéme počítača, z ktorého bol odoslaný.
Veľkosť	Veľkosť súboru.
Kategória	Kategória súboru (typ súboru). Kategórie súborov, ktoré môžu byť odosielané na analýzu, môžete nastaviť v konfigurácii.

Každá analyzovaná vzorka má dva kľúčové parametre: **Stav** a **Status**.

Parameter **Stav** vyjadruje, v ktorom bode procesu analýzy sa vzorka aktuálne nachádza.

Stav	Popis
Odoslané do LiveGrid(R)	Súbor bol odoslaný do cloudu ESET, no výsledok analýzy nebude k dispozícii.
Odoslané do ESET LiveGuard	Súbor bol odoslaný do cloudu ESET na analýzu prostredníctvom ESET LiveGuard Advanced.
Prebieha analýza	Vzorka sa analyzuje.
Dokončené	Súbor bol úspešne zanalyzovaný.
Prebieha opätovná analýza	K dispozícii je predchádzajúci výsledok analýzy, no súbor je opätovne podrobený analýze.

Parameter **Status** vyjadruje, či bola analýza vzorky vykonaná a s akým výsledkom.

Ikona	Status	Skóre	Popis
	Neznámy		Súbor zatiaľ nebol analyzovaný.
	Neškodný	1 – 74	Detekčné jadro nevyhodnotilo analyzovaný súbor ako škodlivý.
	Podozrivý **Veľmi podozrivý**	75 – 89 90 – 99	Detekčné jadro vyhodnotilo zachytenú aktivitu súboru ako podozrivú, avšak nie ako jednoznačne škodlivú.
	Škodlivý	100	Súbor je na základe zachytenej aktivity vyhodnotený ako škodlivý.

Odporúčania pre používateľov s podozrivou vzorkou

V prípade, že bol súbor vyhodnotený ako podozrivý alebo veľmi podozrivý, zvážte nasledujúce akcie:

- ak máte v rámci licencie prístup k správe o aktivite súboru, prezrite si informácie zistené pri analýze daného súboru,
- preverte pôvod súboru (odkiaľ sa k vám dostal) a položte si otázku, či je pre vás dôveryhodný,
- skontrolujte súbor prostredníctvom externého nástroja na testovanie súborov na prítomnosť vírusov, napríklad VirusTotal,
- ak usúdite, že vašej organizácii hrozí vysoké riziko útoku, nastavte prah detekcie na úroveň **Podozrivý**.

Správa o aktivite súboru

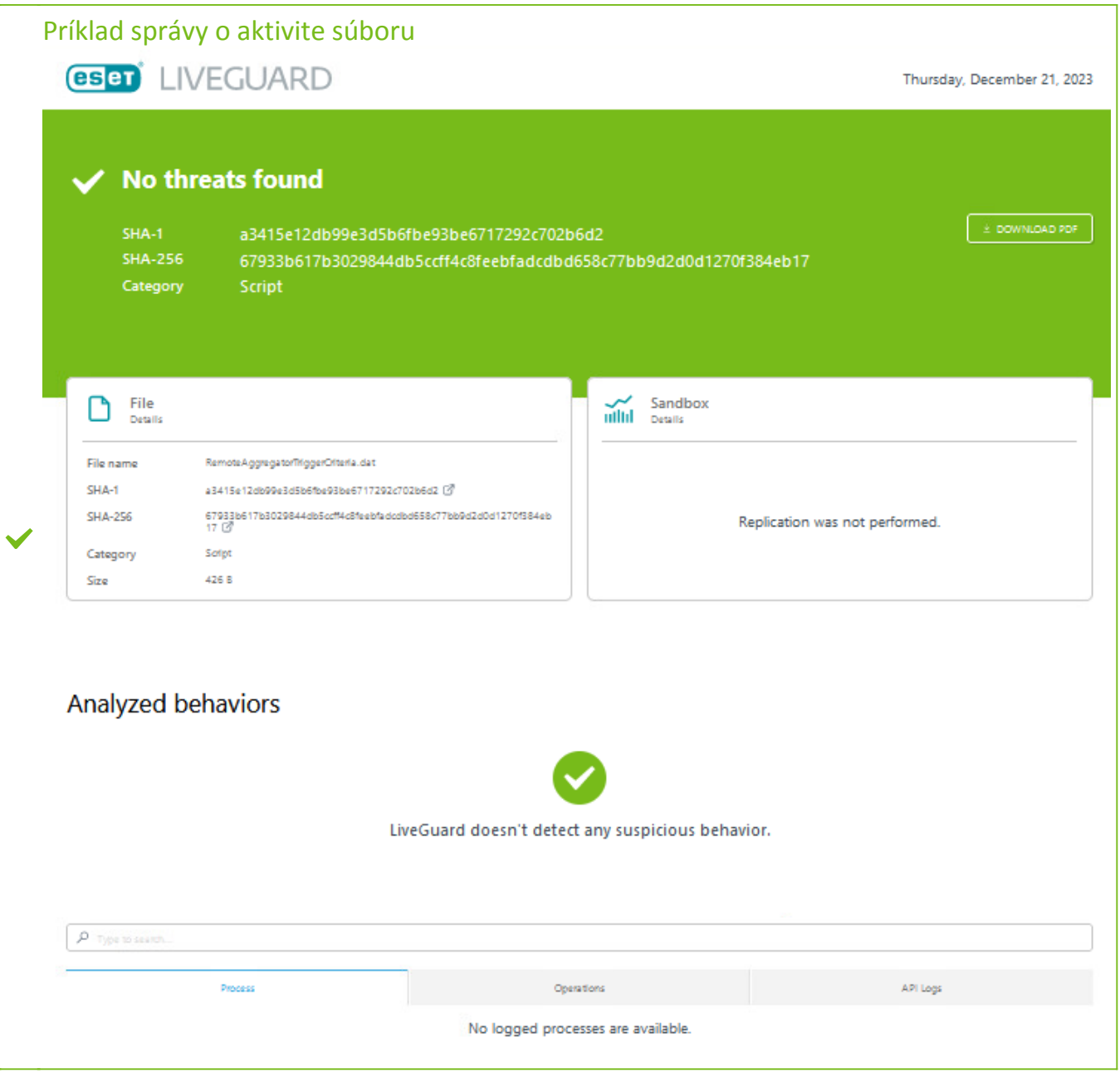
Vo Web Console prejdite do sekcie **Odoslané súbory**. Označte požadovaný súbor a kliknite na **Zobraziť podrobnosti** > **Zobraziť aktivitu** pre zobrazenie **Správy o aktivite súboru**. Táto správa obsahuje základné údaje o skontrolovanom súbore a jeho aktivitu zachytenú počas analýzy v sandboxe. Pri jednej analyzovanej vzorke môže byť zistených aj viacero druhov aktivít.

> Správu o aktivite súboru si môžete stiahnuť kliknutím na tlačidlo **Stiahnuť PDF**.

Správa sa skladá z týchto častí:

1. **Výsledok** – konečné hodnotenie súboru
2. Hodnota **SHA-1 hash** s odkazom na nástroj VirusTotal
3. Hodnota **SHA-256 hash**
4. **Detaily súborov** – výsledky z vrstvy kontroly
5. **Podrobnosti o sandboxe** – výsledky z vrstvy analýzy správania
6. **Analyzované aktivity** – zoznam odhalených aktivít a ich výsledky. Po analýze môžete na orientáciu v podrobnostiach použiť panel vyhľadávania.

Príklad správy o aktivite súboru



Manuálne odoslanie súboru na analýzu

Podozrivé súbory sú odosielané do cloudu ESET automaticky na základe nastavení v politike pre konkrétny bezpečnostný produkt ESET. Súbor však môže na analýzu zaslať manuálne aj sám používateľ bezpečnostného produktu ESET s aktívnou službou ESET LiveGuard Advanced. Použite odkaz pre váš produkt ESET pre zobrazenie inštrukcií, ako z daného programu odoslať súbor na analýzu.

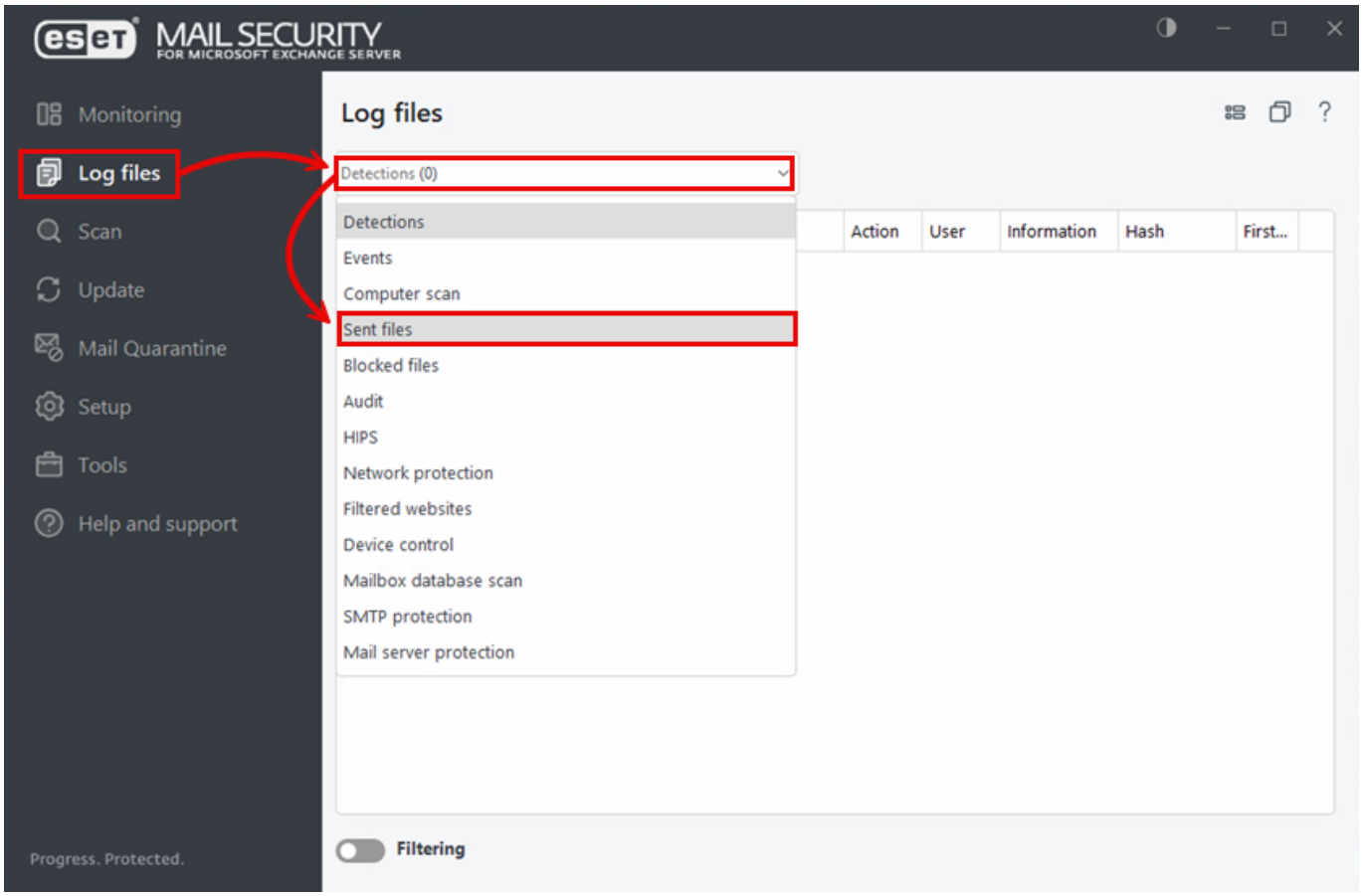
- Odoslanie z ESET PROTECT On-Prem
- Odoslanie z ESET Endpoint Security
- Odoslanie z ESET Server Security
- Odoslanie z ESET Mail Security

Lokálny zoznam odoslaných súborov

Vo vašom bezpečnostnom produkte ESET podporujúcom službu ESET LiveGuard Advanced si môžete zobraziť zoznam súborov odoslaných z daného klientskeho zariadenia na analýzu do spoločnosti ESET.

Pre zobrazenie zoznamu odoslaných súborov v programe **ESET Server Security** alebo **ESET Mail Security** prejdite v hlavnom okne do sekcie **Protokoly** a zo zobrazeného roletového menu vyberte možnosť **Odoslané súbory**.

Pre zobrazenie zoznamu odoslaných súborov v programe **ESET Endpoint Security** prejdite v hlavnom okne do sekcie **Nástroje** > **Protokoly** a zo zobrazeného roletového menu vyberte možnosť **Odoslané súbory**.



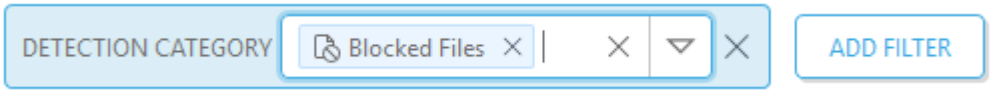
Odoslanie súboru prostredníctvom ESET PROTECT On-Prem

V ESET PROTECT On-Prem môžete na analýzu odoslať **Blokované súbory** nahlásené nástrojom ESET Inspect On-Prem. Riaďte sa nasledujúcimi krokmi pre odoslanie súborov na analýzu:

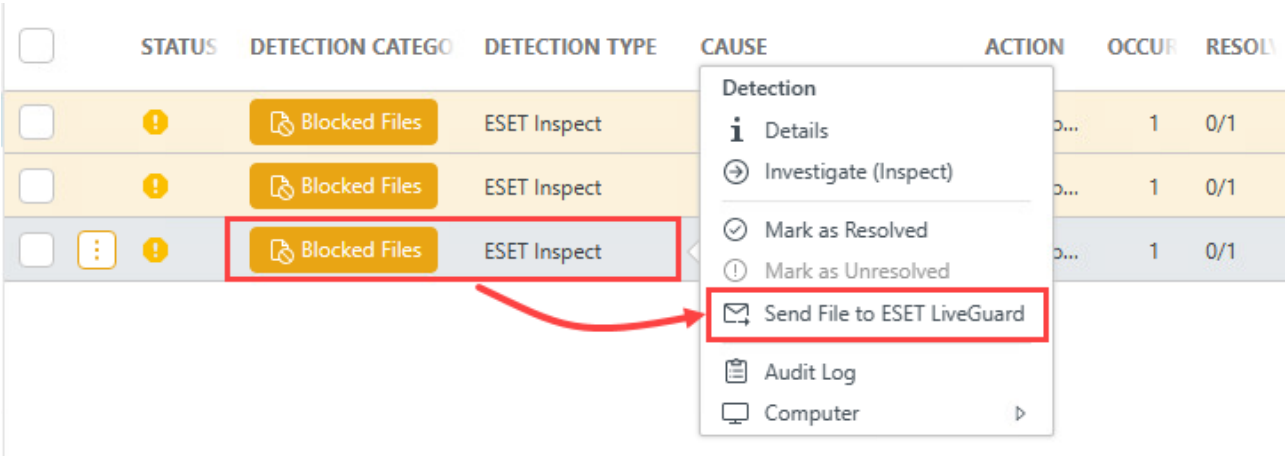
1. Prihláste sa do Web Console.

> Používateľ môže odosielať na analýzu len detekcie zachytené na počítačoch, ku ktorým má povolenia na prístup.

2. Kliknite na **Detekcie** a zvoľte zachytený objekt, ktorý chcete odoslať na analýzu. Odoslať je možné iba súbory zahrnuté v časti **Kategória detekcií**: **Blokované súbory**.



3.Vyberte súbor a kliknite na **Odoslať súbor do ESET LiveGuard** pre vytvorenie klientskej úlohy, na základe ktorej bude daný súbor odoslaný z klientskeho zariadenia do cloudu ESET.



- Vzorku na analýzu môžete odoslať aj zo zariadení, na ktorých nie je služba ESET LiveGuard Advanced aktívna.
- Výsledok analýzy pre takto zaslaný súbor nebude spätne doručený používateľovi, bude však zapracovaný a distribuovaný prostredníctvom systému ESET LiveGrid®.
- Manuálne odoslanie súboru na analýzu je k dispozícii len vtedy, keď je na danom zariadení povolený systém ESET LiveGrid®.

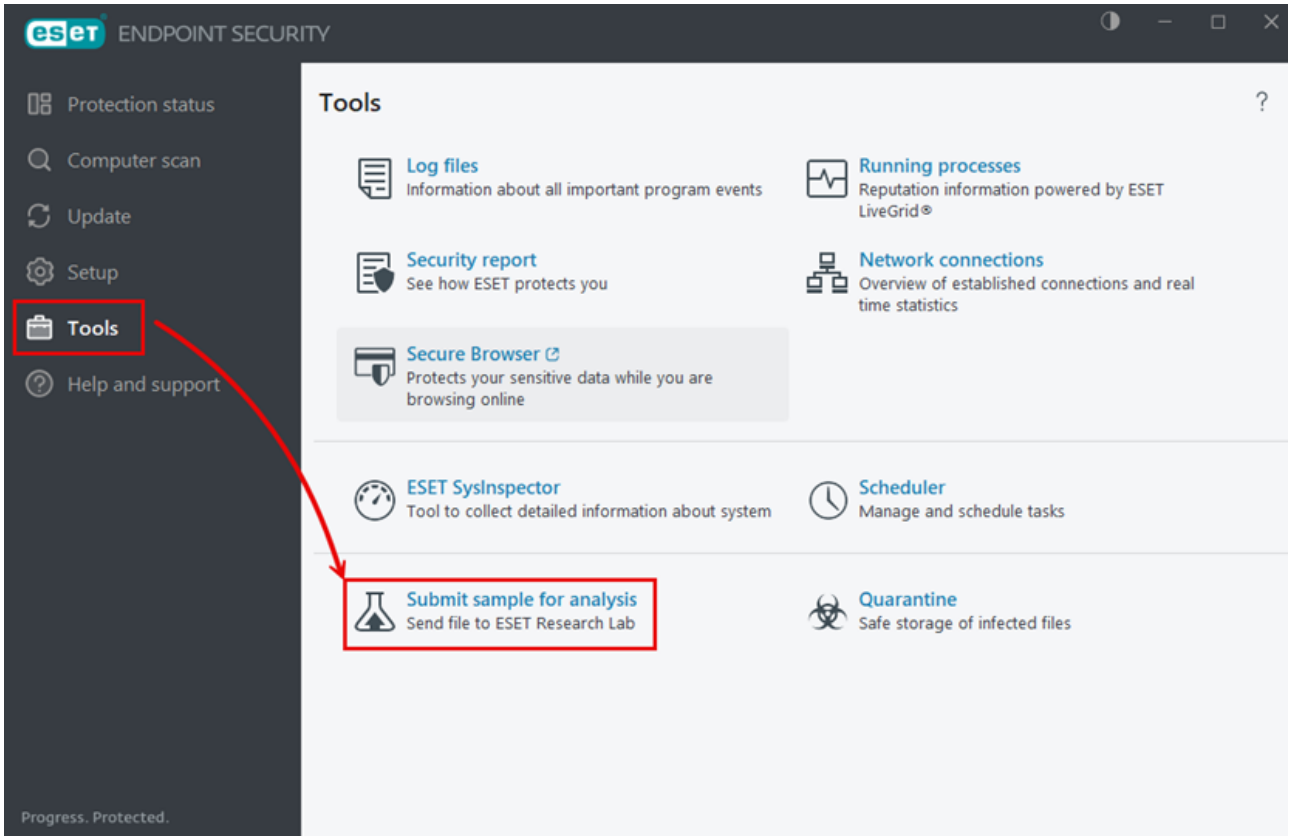
Odoslanie súboru prostredníctvom ESET Endpoint Security

Riaďte sa krokmi uvedenými nižšie pre odoslanie súboru na analýzu z produktu ESET Endpoint Security:

Používatelia systému Windows

1.Otvorte ESET Endpoint Security.

2.Kliknite na **Nástroje** > **Odoslanie vzorky na analýzu**.



3.Vyplňte povinné polia formulára **Vybrať vzorku na analýzu** a následne kliknite na tlačidlo **Ďalej**.

4.Voliteľne môžete pridať aj ďalšie informácie o zasielanom súbore. Nakoniec kliknite na tlačidlo **Odoslať**.

Používatelia systému Linux

Podozrivé súbory sa odosielajú automaticky. Na systéme Linux nemajú používatelia možnosť z produktu ESET Endpoint Security manuálne odoslať súbor na analýzu.

- Vzorku na analýzu môžete odoslať aj zo zariadení, na ktorých nie je služba ESET LiveGuard Advanced aktívna.
- Výsledok analýzy pre takto zaslaný súbor nebude spätne doručený používateľovi, bude však zapracovaný a distribuovaný prostredníctvom systému ESET LiveGrid®.
- Manuálne odoslanie súboru na analýzu je k dispozícii len vtedy, keď je na danom zariadení povolený systém ESET LiveGrid®.

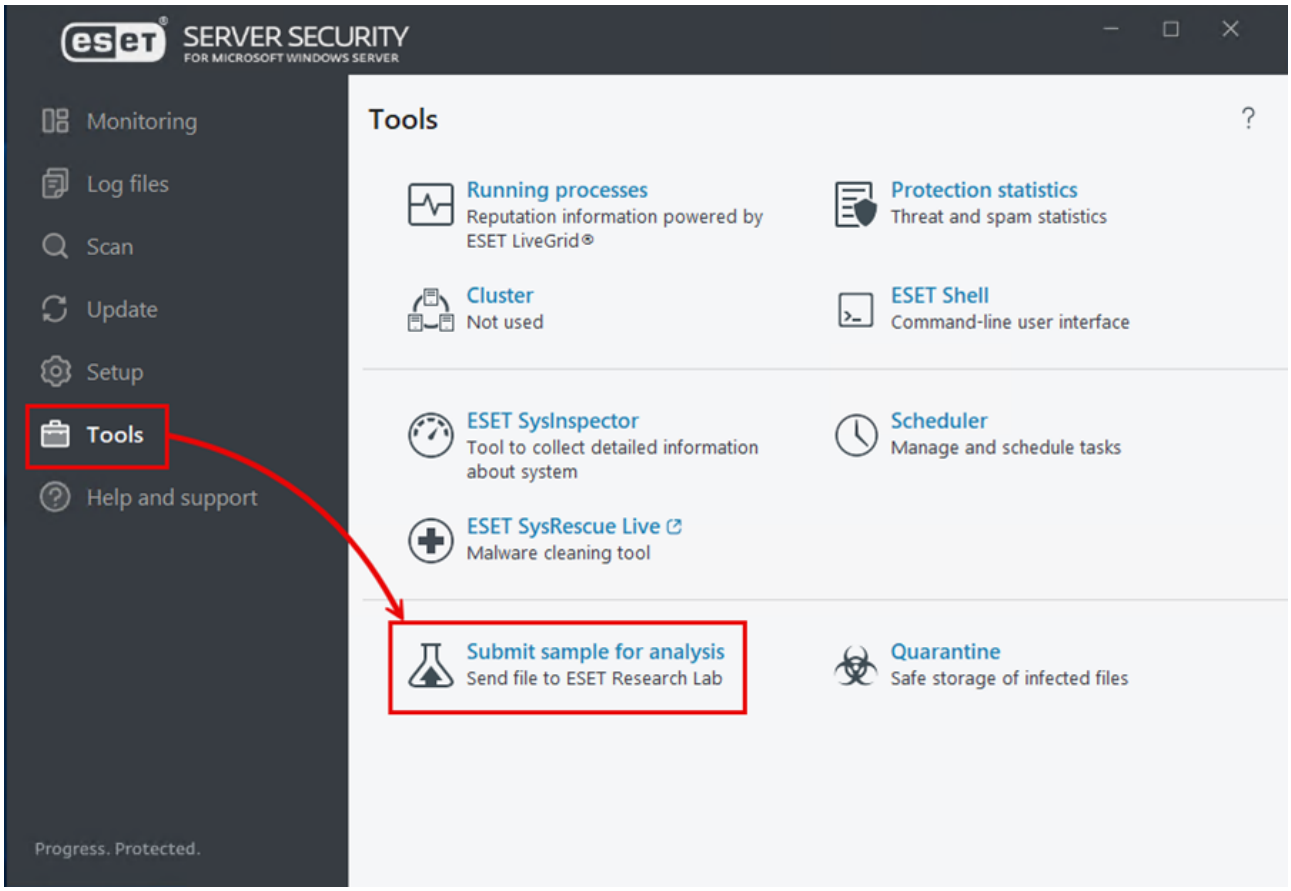
Odoslanie súboru prostredníctvom ESET Server Security

Riaďte sa krokmi uvedenými nižšie pre odoslanie súboru z produktu ESET Server Security na analýzu do ESET LiveGuard Advanced.

Používatelia systému Windows

1.Otvorte ESET Server Security.

2.Kliknite na **Nástroje** > **Odoslanie vzorky na analýzu**.



3.Vyplňte povinné polia formulára **Vybrať vzorku na analýzu** a následne kliknite na tlačidlo **Ďalej**.

4.Voliteľne môžete pridať aj ďalšie informácie o zasielanom súbore. Nakoniec kliknite na tlačidlo **Odoslať**.

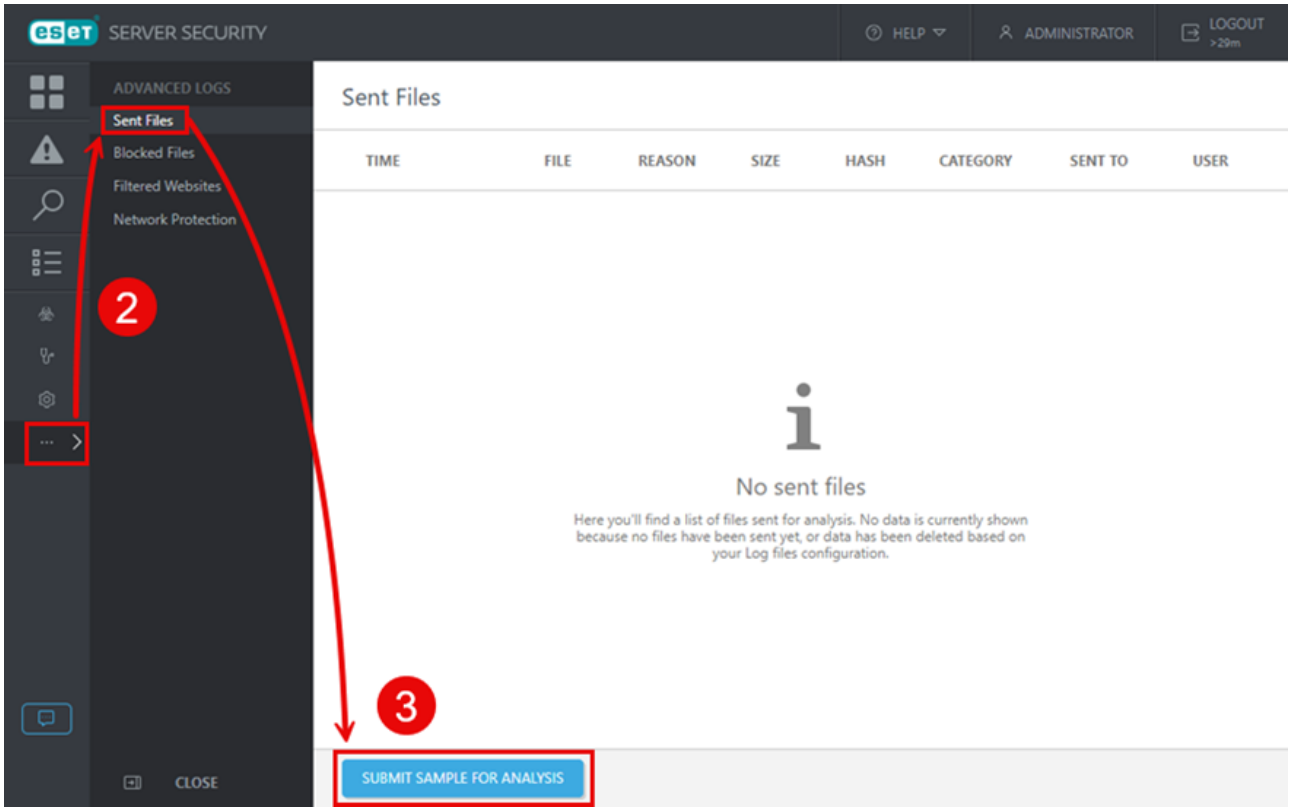
Používatelia systému Linux

Ak chcete odoslať vzorku na analýzu z webového rozhrania, postupujte nasledovne:

1.Prihláste sa do webového rozhrania.

2.Kliknite na **Sent files** (Odoslané súbory).

3.Kliknite na možnosť **Submit sample for analysis** pre odoslanie vzorky na analýzu.



4.Vyberte dôvod odoslania vzorky.

5.Zadajte URL adresu stránky alebo cestu k súboru.

6.Zadajte svoju e-mailovú adresu alebo zvoľte anonymné odoslanie cez možnosť **Submit anonymously**.

7.Kliknite na **Ďalej**.

8.Zadajte doplňujúce informácie.

9.Kliknite na **Send**.

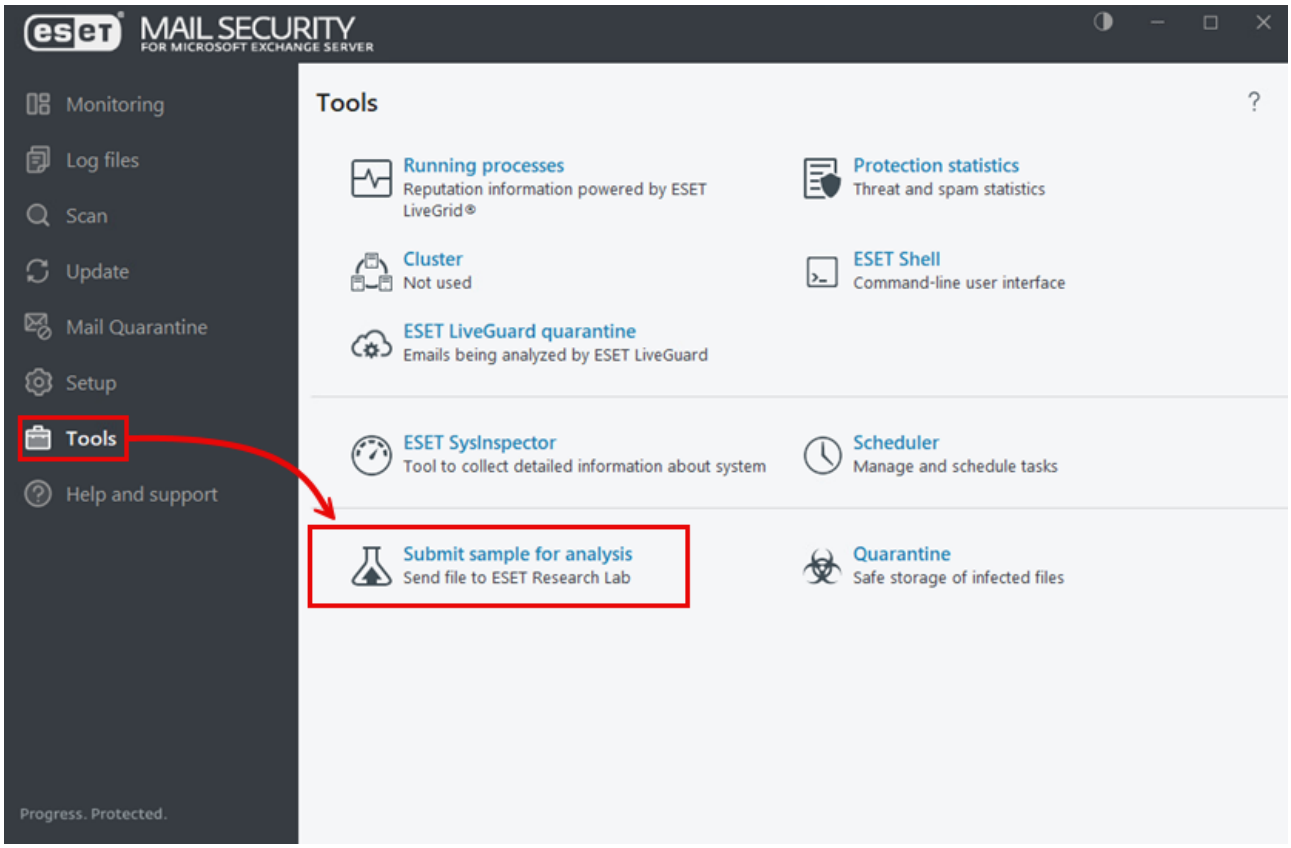
- Vzorku na analýzu môžete odoslať aj zo zariadení, na ktorých nie je služba ESET LiveGuard Advanced aktívna.
- Výsledok analýzy pre takto zaslaný súbor nebude spätne doručený používateľovi, bude však zapracovaný a distribuovaný prostredníctvom systému ESET LiveGrid®.
- Manuálne odoslanie súboru na analýzu je k dispozícii len vtedy, keď je na danom zariadení povolený systém ESET LiveGrid®.

Odoslanie súboru prostredníctvom ESET Mail Security

Riaďte sa krokmi uvedenými nižšie pre odoslanie súboru z produktu ESET Mail Security na analýzu do ESET LiveGuard Advanced:

1.Otvorte ESET Mail Security.

2.Prejdite do sekcie **Nástroje** > **Odoslanie vzorky na analýzu**.



3.Vyplňte povinné polia formulára **Vybrať vzorku na analýzu** a následne kliknite na tlačidlo **Ďalej**.

4.Voliteľne môžete pridať aj ďalšie informácie o zasielanom súbore. Nakoniec kliknite na tlačidlo **Odoslať**.

i
- Vzorku na analýzu môžete odoslať aj zo zariadení, na ktorých nie je služba ESET LiveGuard Advanced aktívna.
- Výsledok analýzy pre takto zaslaný súbor nebude spätne doručený používateľovi, bude však zapracovaný a distribuovaný prostredníctvom systému ESET LiveGrid®.
- Manuálne odoslanie súboru na analýzu je k dispozícii len vtedy, keď je na danom zariadení povolený systém ESET LiveGrid®.

Vytvorenie vylúčenia

V prípade, že je súbor zanalyzovaný a vyhodnotený ako škodlivý, bezpečnostný produkt ESET za normálnych okolností automaticky vykoná akciu zadefinovanú v nastaveniach v rámci politiky. Ak je na danom zariadení povolená karanténa, súbor bude presunutý do karantény (v hlavnom menu bezpečnostného produktu ju nájdete v sekcii **Nástroje** > **Karanténa**). Pre konkrétny súbor môžete v prípade potreby vytvoriť vylúčenie, napríklad ak ste si istý, že neobsahuje bezpečnostné hrozby alebo ho z nejakého dôvodu nechcete podrobiť kontrole a liečeniu. Vylúčenia, ktoré vytvoria mobilné klienty mimo dosahu servera, nebudú do Web Console pridané až do chvíle, kým sa agent na klientskom zariadení opäť nepripojí k serveru vzdialenej správy.

Vylúčenia môžu predstavovať riziko
Kým bude vytvorené vylúčenie aktívne, bezpečnostný produkt ESET nebude daný súbor kontrolovať. Pri vytváraní vylúčení preto buďte vždy opatrný.

Predpoklady pre vytvorenie vylúčenia:

- Súbor bol zaslaný na analýzu do ESET LiveGuard Advanced.
- Táto informácia bola zosynchronizovaná so serverom vzdialenej správy.

Vytvorenie výnimky, na základe ktorej bude súbor vylúčený z kontroly, pozostáva z nasledujúcich krokov:

1.Správca konzoly na správu pridá hash hodnotu súboru ako vylúčenie v rámci politiky.

2.Politika sa aplikuje na vybrané zariadenia. Vďaka tomu súbor nebude bezpečnostným programom ESET na týchto zariadeniach detegovaný a bude možné ho neobmedzene používať.

Môžete si vytvoriť samostatnú politiku pre vylúčenia. Politiku si však vytvorte ešte predtým, ako začnete pridávať vylúčenie.

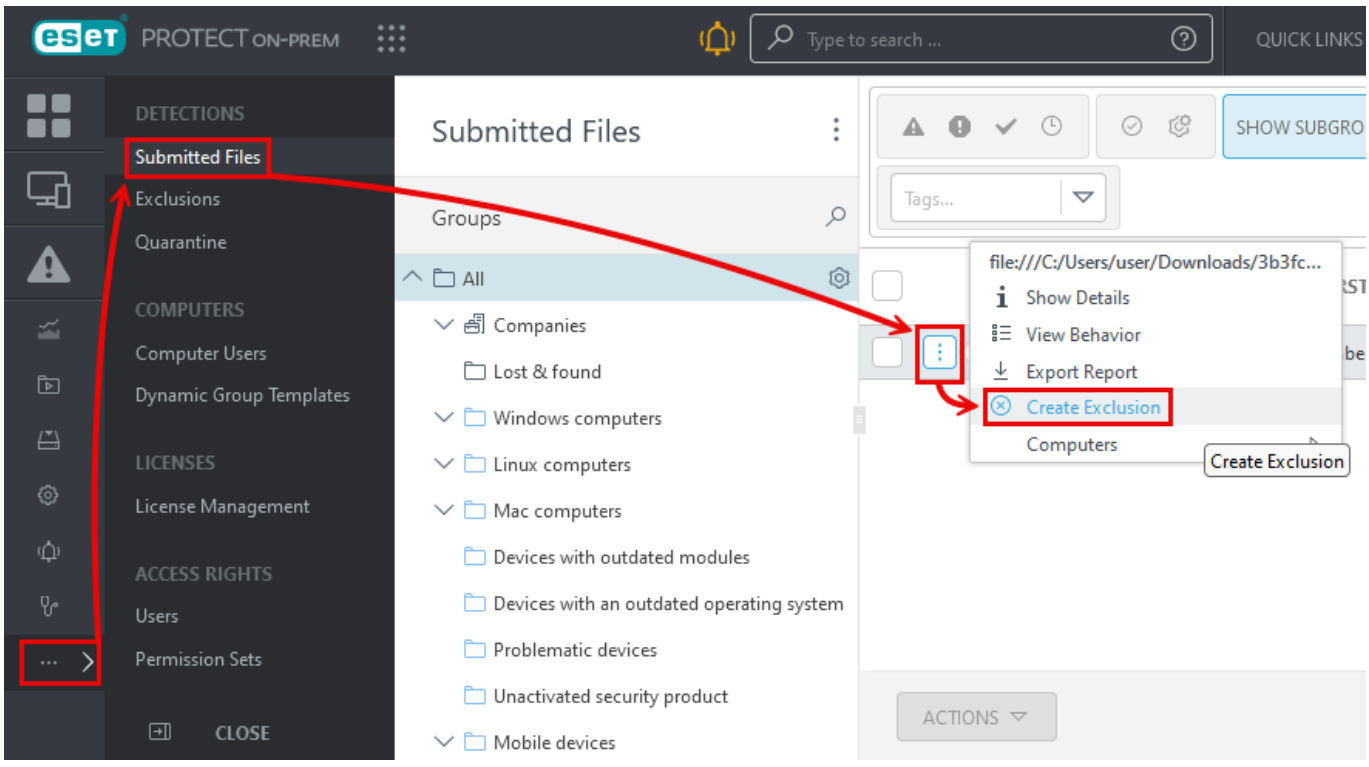
Vytvorenie politiky

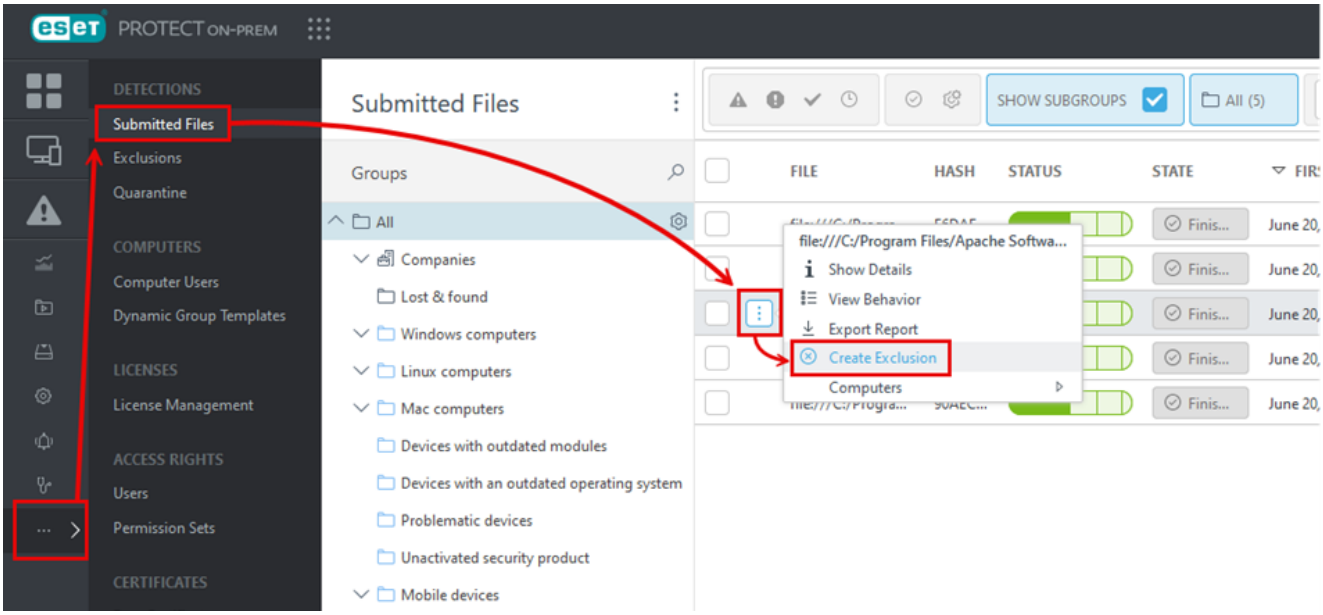
Vytvorenie vylúčenia

Ak chcete vytvoriť vylúčenie pre detegovaný súbor, ktorý je zobrazený v zozname **Odoslaných súborov** vo Web Console, postupujte nasledovne:

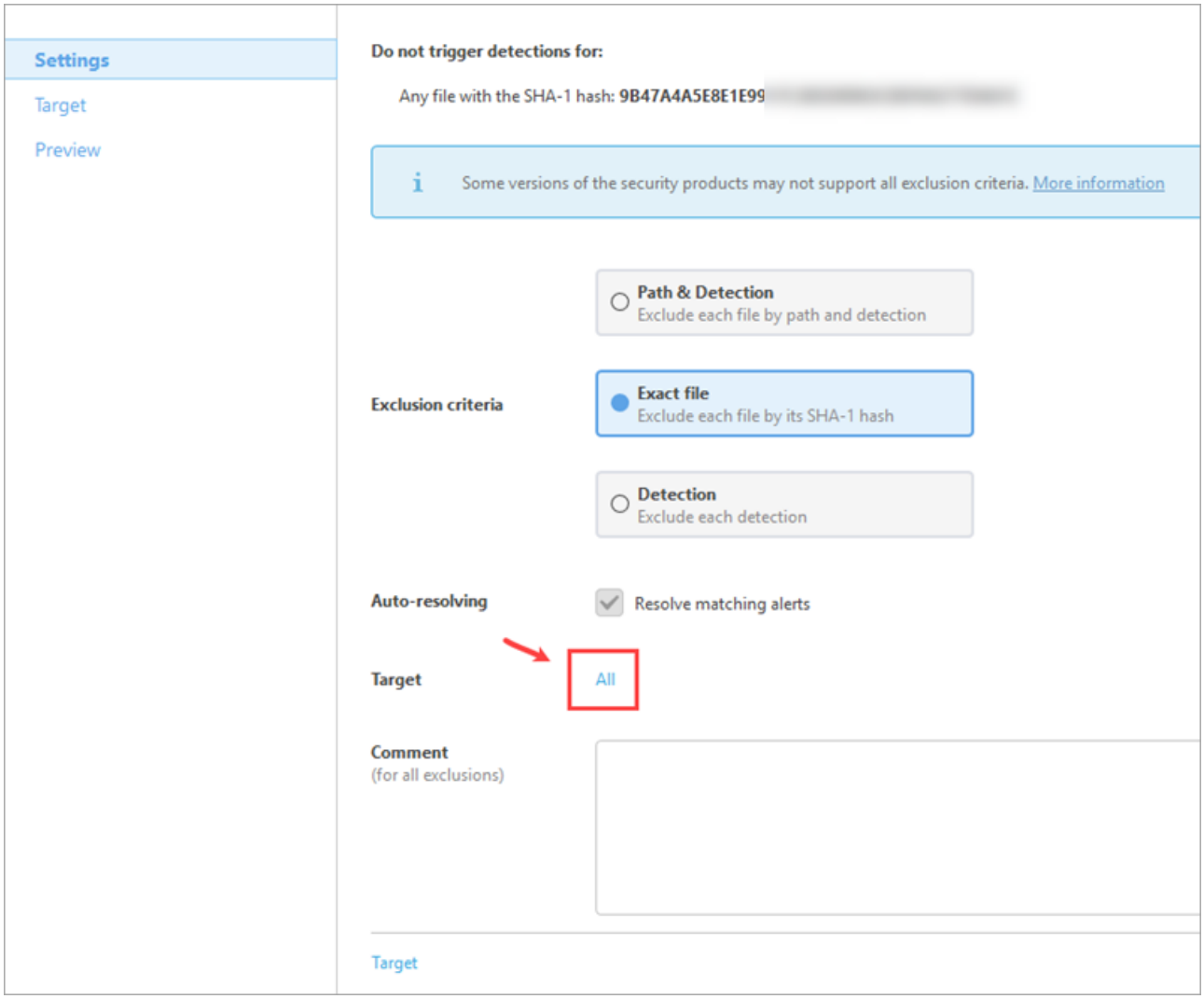
1.Prihláste sa do Web Console ako správca (účet Administrator) alebo ako iný používateľ s dostatočnými povoleniami pre prístup k počítaču, z ktorého bol daný súbor odoslaný.

2.Prejdite do sekcie **Odoslané súbory**, vyberte hash hodnotu súboru, ktorý chcete vylúčiť z kontroly, a následne zvoľte možnosť **Vytvoriť vylúčenie**.





3.V časti **Cieľ** vyberte cieľové zariadenie/a. Predvoleným cieľom je skupina **Všetko**. Vylúčenie sa aplikuje na všetky podporované produkty ESET na cieľovom zariadení.



4.Vylúčenie uložíte a aplikujete kliknutím na **Dokončiť**. Na koncových zariadeniach, ku ktorým je politika priradená, sa začne vytvorené vylúčenie prejavovať najneskôr po dvoch intervaloch replikácie (t. j. pripojeniach Agentov k Serveru). Zoznam všetkých vylúčení nájdete v sekcii **Vylúčenia**.

Použitie vylúčení pre zvýšenie výkonu

ESET LiveGuard Advanced dokáže vykonať automatickú analýzu – používateľ sa môže rozhodnúť vylúčiť súbory a umiestnenia z procesu odoslania napr. kvôli citlivým údajom, prípadne dôveryhodným súborom či umiestneniam. Vylúčením súborov alebo umiestnení môžete znížiť zaťaženie svojich sieťových komponentov. Veľké množstvo odosielaných súborov môže spomaliť sieťové komponenty (napr. proxy) a oneskoriť doručenie výsledkov analýzy. Postupujte podľa troch krokov nižšie pre zníženie celkového počtu odosielaných súborov a zlepšenie výkonu vášho systému.

Vždy buďte veľmi opatrný pri vytváraní vylúčenia v rámci ESET LiveGuard Advanced pre konkrétne umiestnenie. Vylúčenie môže mať za následok bezpečnostné riziko vo vašom systéme. Vždy zvážte možné následky vektory útoku.

I.Kontrola odosielaných súborov

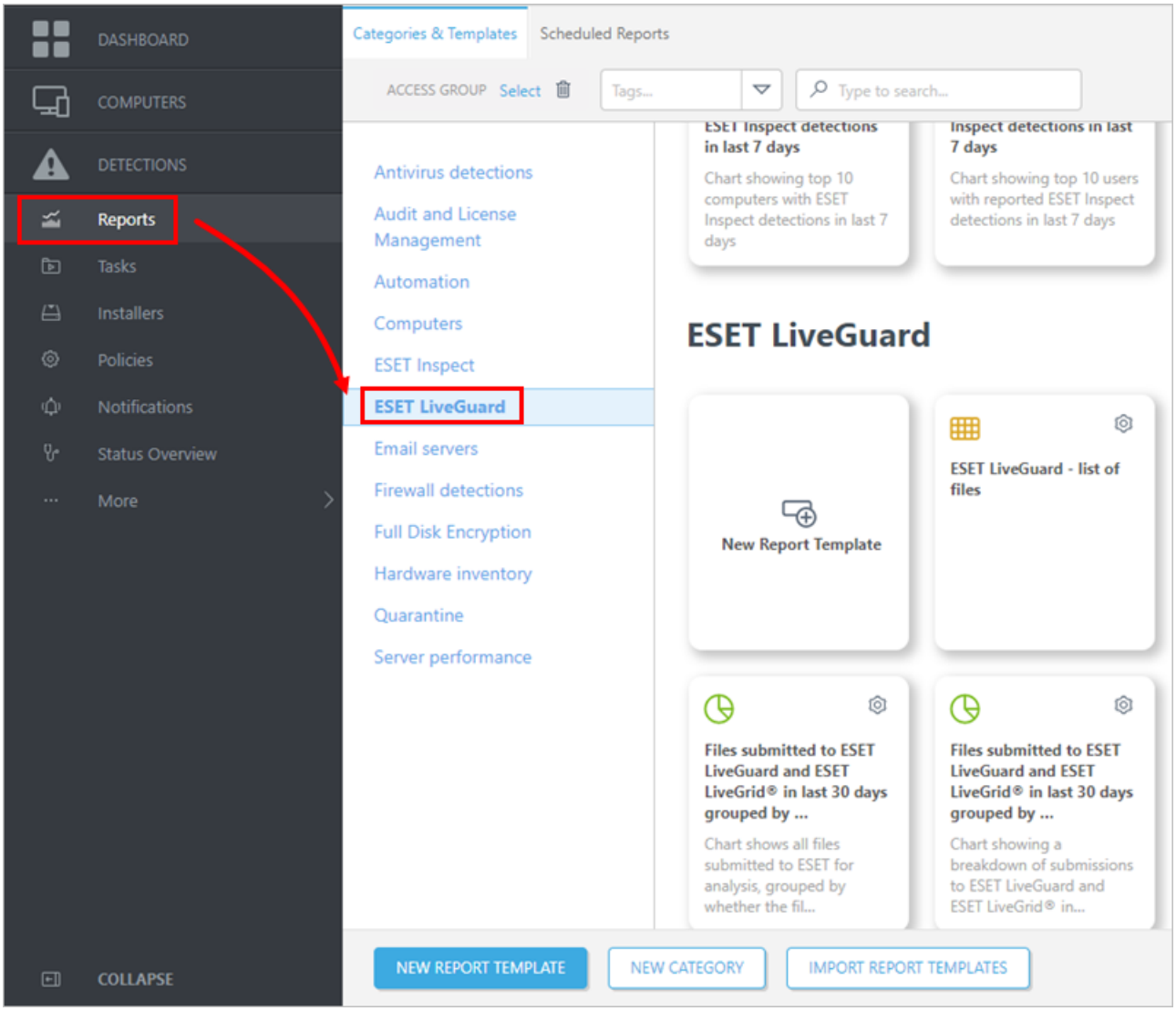
II.Vylúčenie priečinkov

III.Vylúčenie procesu

Kontrolný zoznam odoslaných súborov

Vytvorenie zoznamu počítačov, ktoré odosielajú najviac súborov

1.Kliknite na **Reporty** > **ESET LiveGuard**.



2.Nájdite šablónu reportu **Prvých 10 počítačov s najvyšším počtom odoslaných súborov do ESET LiveGuard a ESET LiveGrid za posledných 30 dní**.

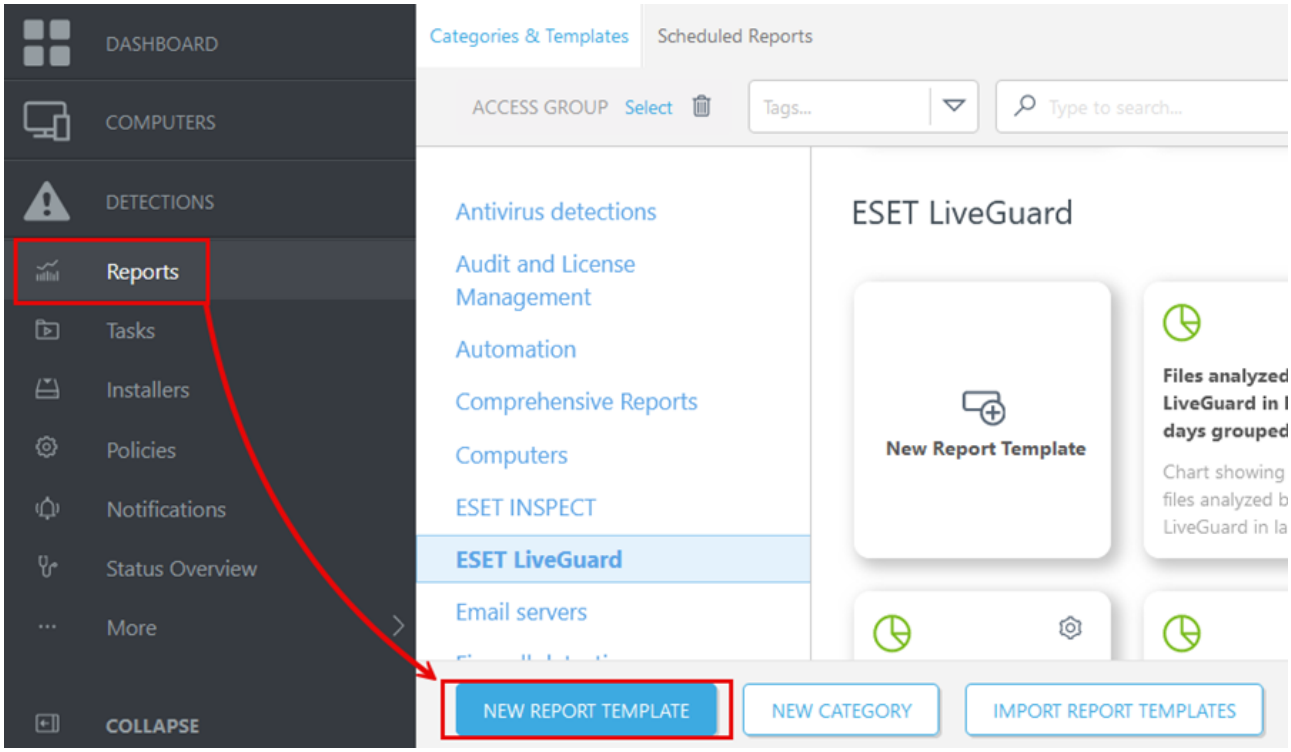
Môžete najskôr upraviť šablónu a zmeniť počet počítačov (10) alebo časový rámec (posledných 30 dní) na inú hodnotu. Je možné, že budete musieť vykonať dané zmeny, pokiaľ si to vyžaduje situácia vo vašej sieti.

3.Kliknite na **Generovať teraz** a uložte report (zoznam počítačov).

Vytvorenie zoznamu odoslaných súborov pre najčastejšie odosielajúce počítače

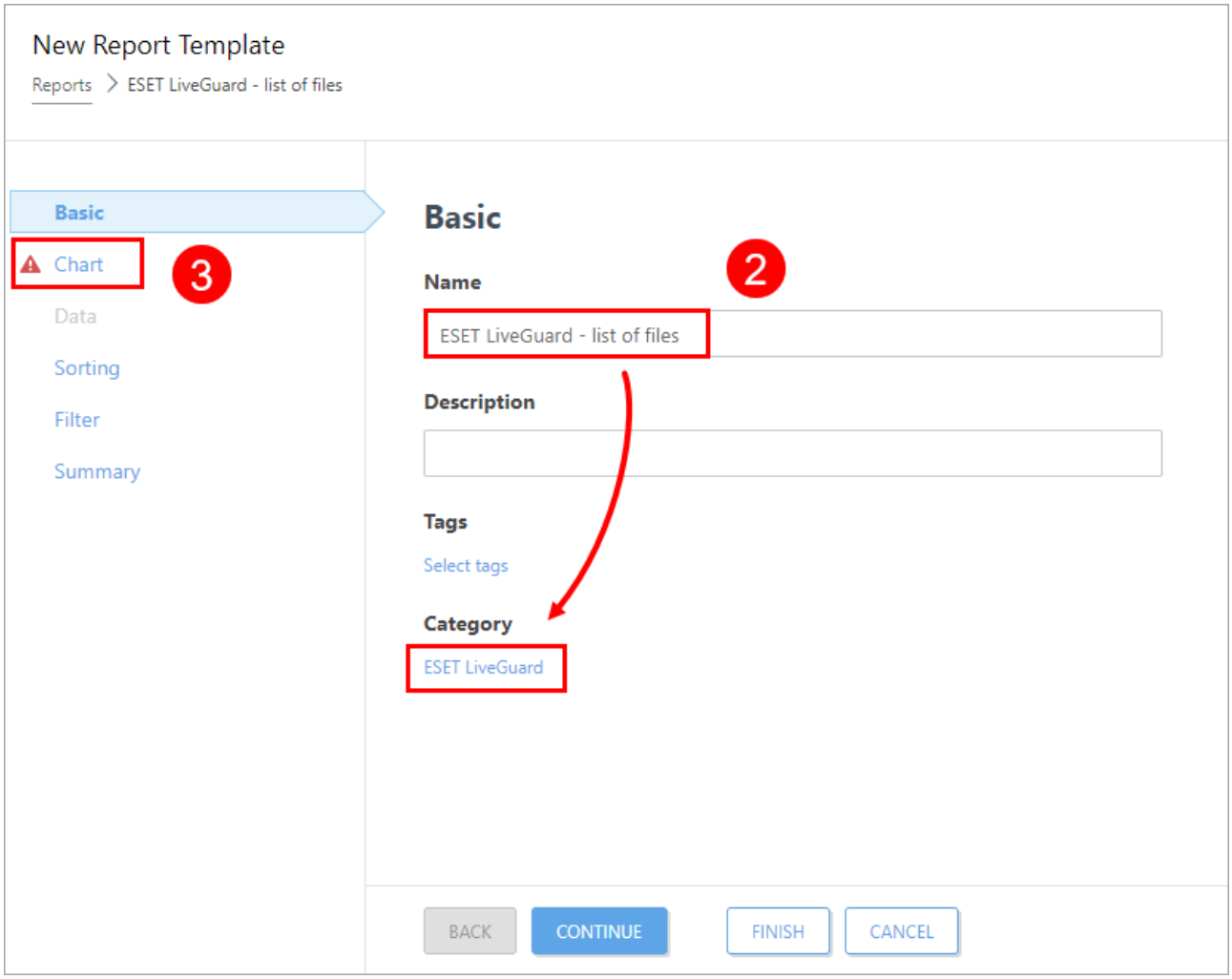
Na vykonanie nasledujúcich krokov potrebujete mať zoznam najčastejšie odosielajúcich počítačov z postupu vyššie.

1.Vo Web Console kliknite na **Reporty** > **Nová šablóna reportu**.

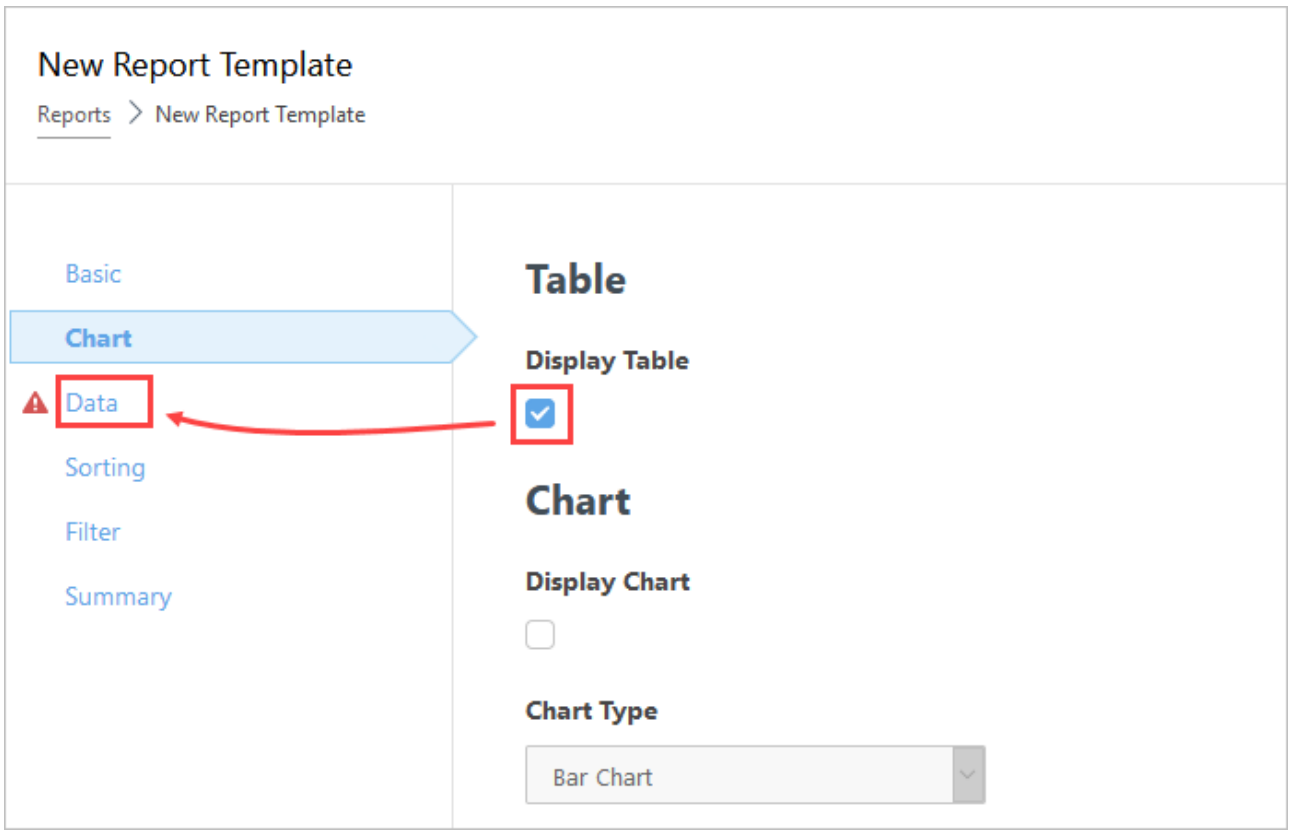


2.Zadajte **Názov** šablóny a vyberte vhodnú **Kategóriu**.

3.Pokračujte v sekcii **Graf**.

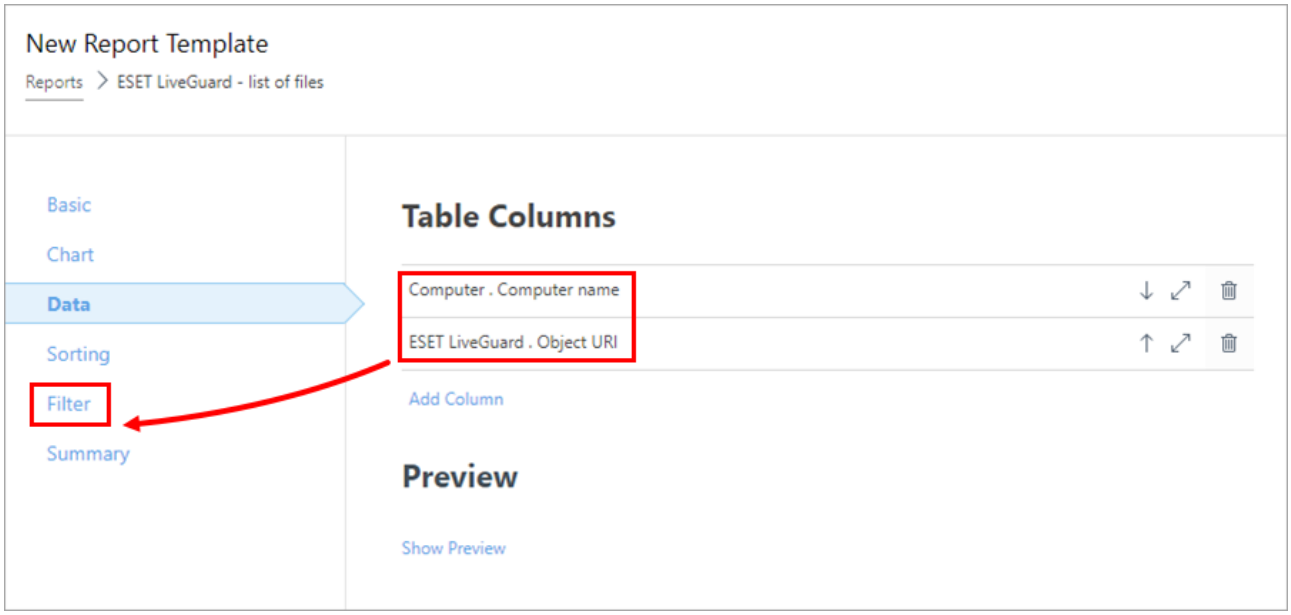


4.V sekcii **Graf** označte len možnosť **Zobraziť tabuľku** a pokračujte do sekcie **Dáta**.



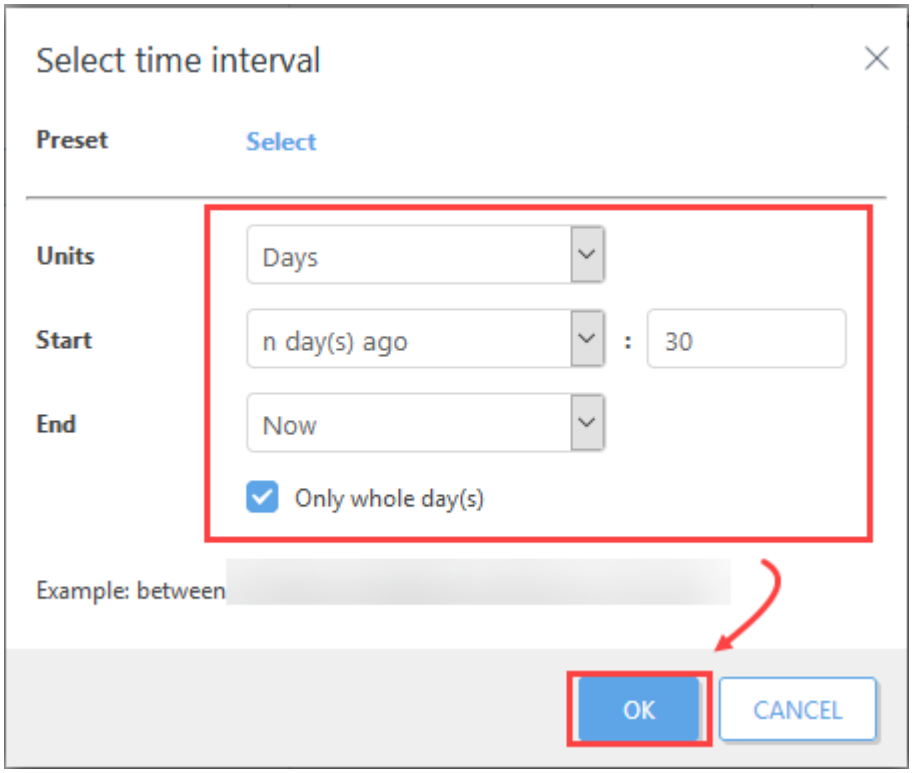
5.V sekcii **Dáta** kliknite na **Pridať stĺpec** a pridajte nasledujúce položky:
Počítač – Názov počítača
ESET LiveGuard – URI objektu

6.Kliknite na **Filter**.



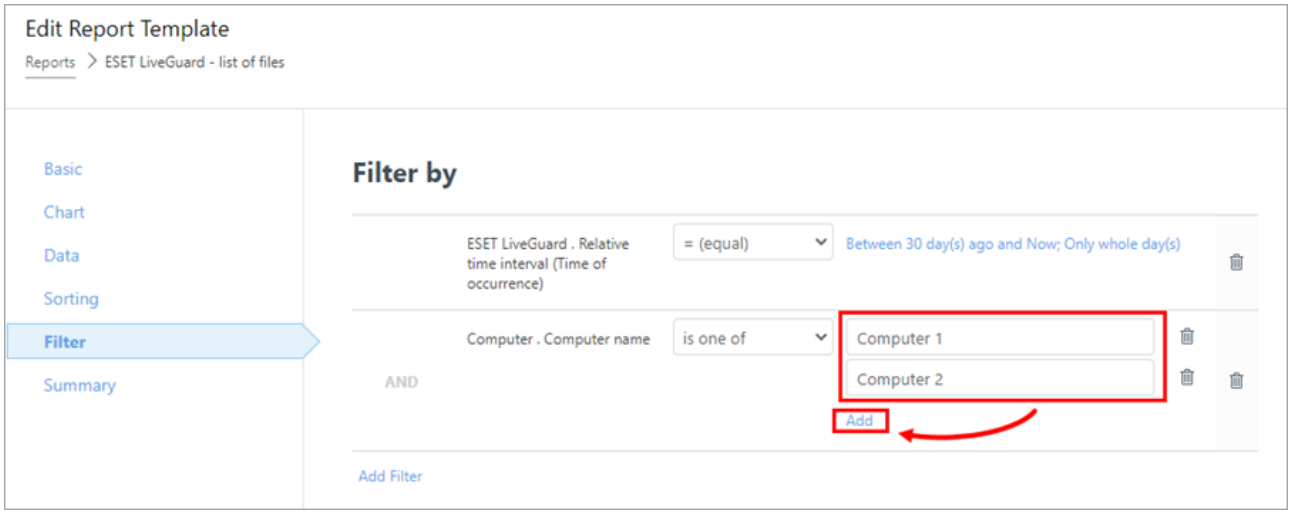
7.Kliknite na **Pridať stĺpec** a vyberte možnosť **ESET LiveGuard . Relatívny časový interval (Čas výskytu)**.

8.Nastavte interval na posledných 30 dní alebo na inú požadovanú hodnotu.



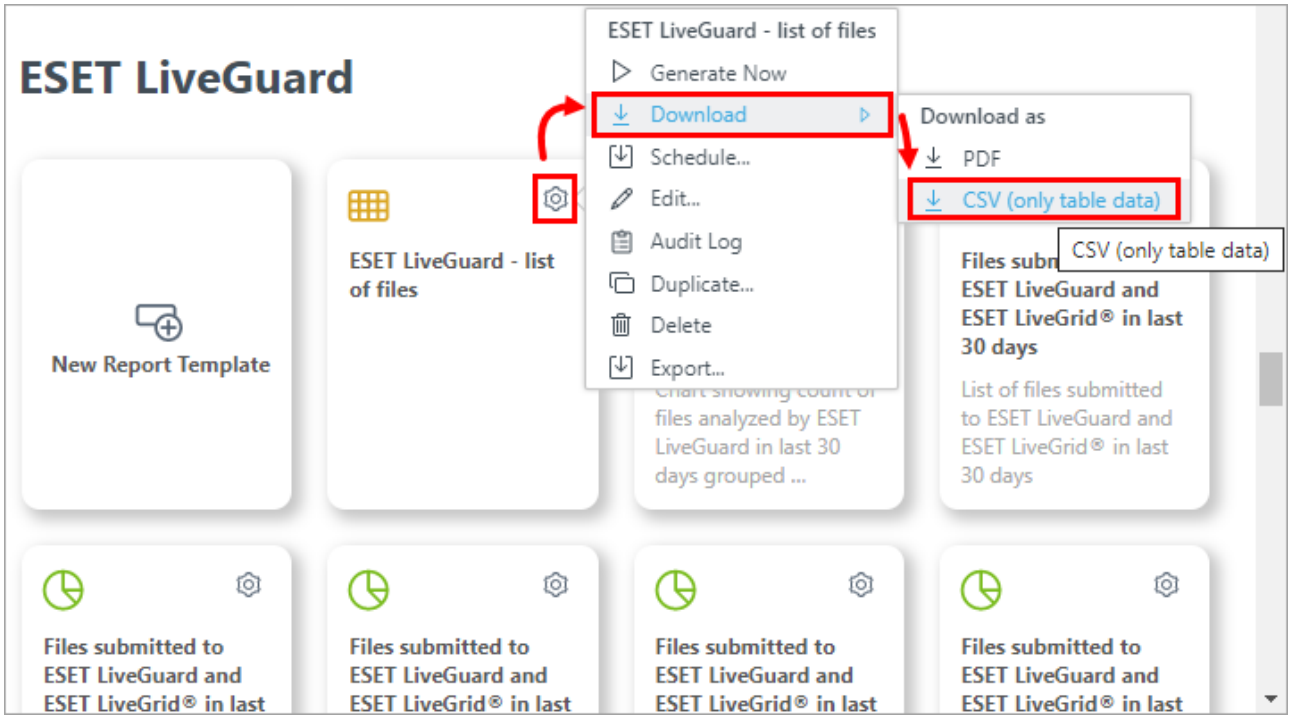
9.Znova kliknite na **Pridať stĺpec** a pridajte položku **Počítač . Názov počítača**.

10. Pridajte názvy všetkých najčastejšie odosielajúcich počítačov z predošlého postupu (10 najčastejšie odosielajúcich počítačov).



11. Kliknutím na **Dokončiť** uložte šablónu reportu.

12. Vyhľadajte novú šablónu reportu a vygenerujte súbor CSV.

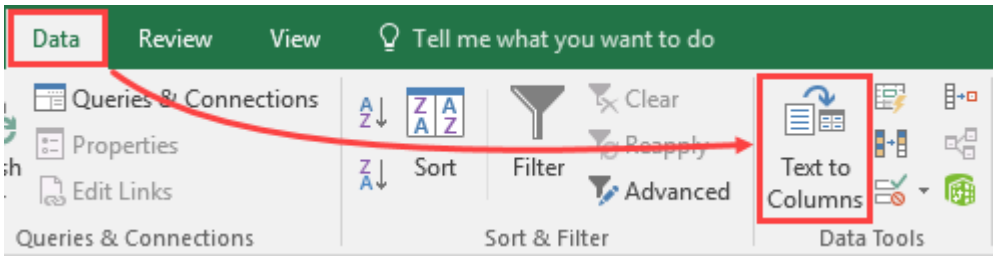


Analýza dát

Nasledujúci postup si vyžaduje softvér tretej strany (editor tabuľkových hárkov) a základné znalosti dátovej analýzy.

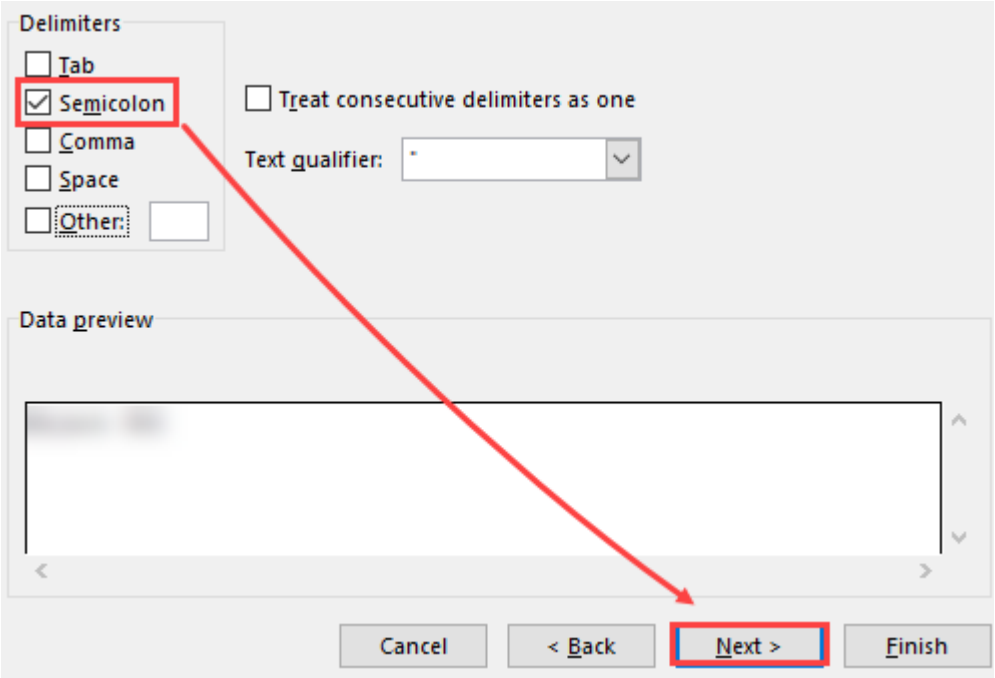
1.Otvorte vyexportovaný súbor CSV vo vhodnom editore (napr. Microsoft Excel).

2.Rozdeľte dáta do dvoch stĺpcov. V programe Microsoft Excel označte prvý stĺpec a prejdite do sekcie **Dáta** > **Text na stĺpce**.



3.Vyberte možnosť **Oddelené** > **Ďalej**.

4.Ako oddeľovač vyberte **Bodkočiarku** a kliknite na **Ďalej** > **Dokončiť**.



Analyzujte dáta.

Pokúste sa nájsť v odoslaných súboroch a ich umiestneniach určitý opakujúci sa vzor. Zvyčajne ide o priečinok, z ktorého je odoslaná väčšina súborov. Keď sa vám podarí nájsť vzor, podozrivý počítač alebo aplikáciu, je potrebné tento vzor preskúmať.
Hľadajte odpovede na tieto otázky:

- Ktorá aplikácia používa tento priečinok?
- Na čo sa tento počítač používa a v čom sa odlišuje od ostatných?
- Aký je pôvod týchto súborov?

Konečným cieľom skúmania je nájsť vzor pre vylúčenie.

Po jeho nájdení pokračujte kapitolou Vylúčenie priečinkov.

Vylúčenie priečinkov

Zvážte projektové priečinky

Používatelia, ktorí používajú vývojársky softvér (napr. Visual Studio), môžu vylúčiť priečinky, do ktorých kompilujú svoje projekty. Proces kompilácie vytvára množstvo nových súborov, ktoré môže ESET LiveGuard Advanced odoslať na analýzu. Nadmernému odosielaniu súborov do ESET LiveGuard Advanced je možné zabrániť. Napríklad môžete vylúčiť svoj projektový priečinok D:\Projects*

Proces vylúčenia priečinku

Umožňuje vylúčiť konkrétne súbory alebo priečinky z odosielania do ESET LiveGuard Advanced. Vylúčené súbory nebudú nikdy odosielané do laboratórií spoločnosti ESET na analýzu.

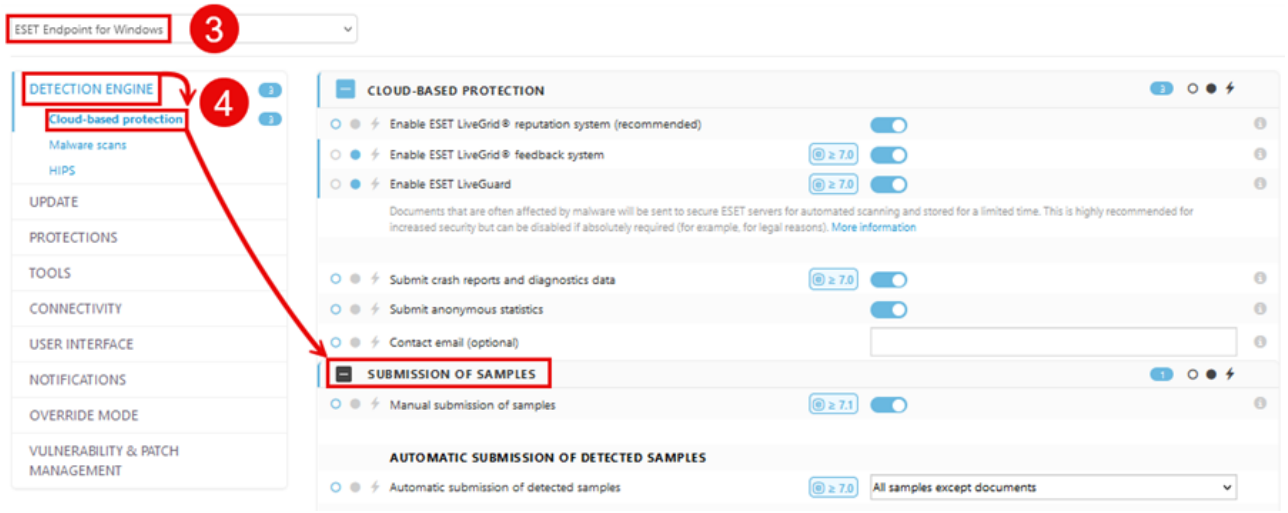
Pri vytváraní vylúčenia vždy dbajte na bezpečnosť. Zvážte, ktoré aplikácie môžu zapisovať do vylúčeného umiestnenia a zamyslite sa nad tým, ako by mohlo byť vylúčenie daného umiestnenia zneužité.

1.Prihláste sa do Web Console a kliknite na **Politiky** > **Nová politika**.

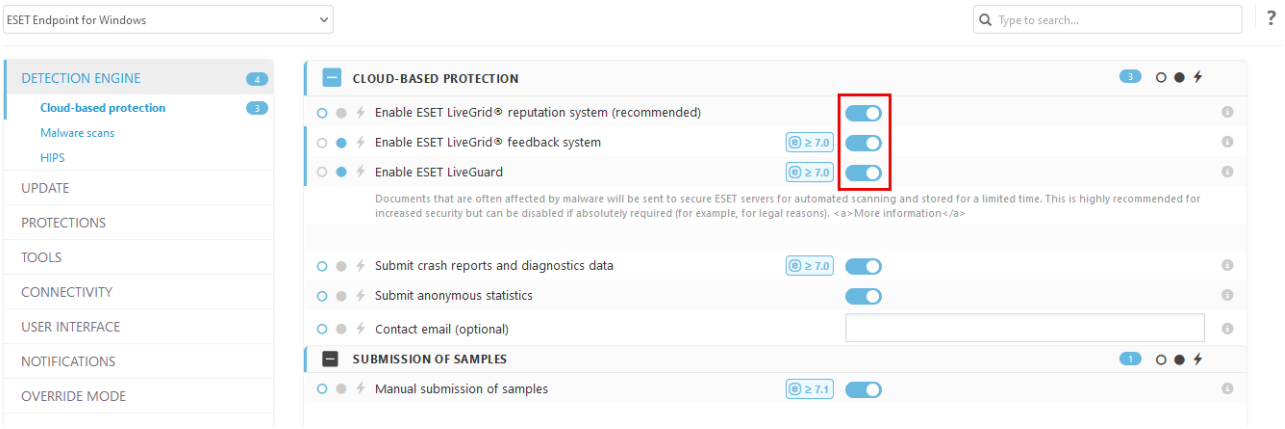
2.V sekcii **Základné** zadajte **Názov** politiky.

3.V sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows** (prípadne iný kompatibilný produkt).

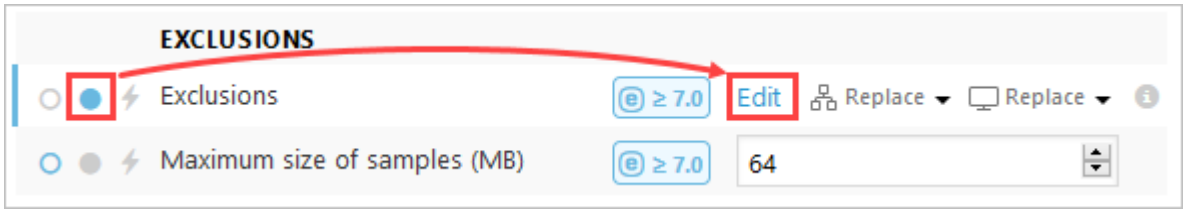
4.Kliknite na **Detekčné jadro** > **Ochrana s podporou cloudu**.



5.Zapnite **ESET LiveGrid a ESET LiveGuard Advanced** pomocou prepínačov.



6.V sekcii **Vylúčenia** povoľte **Vylúčenia** a kliknite na **Upraviť**.

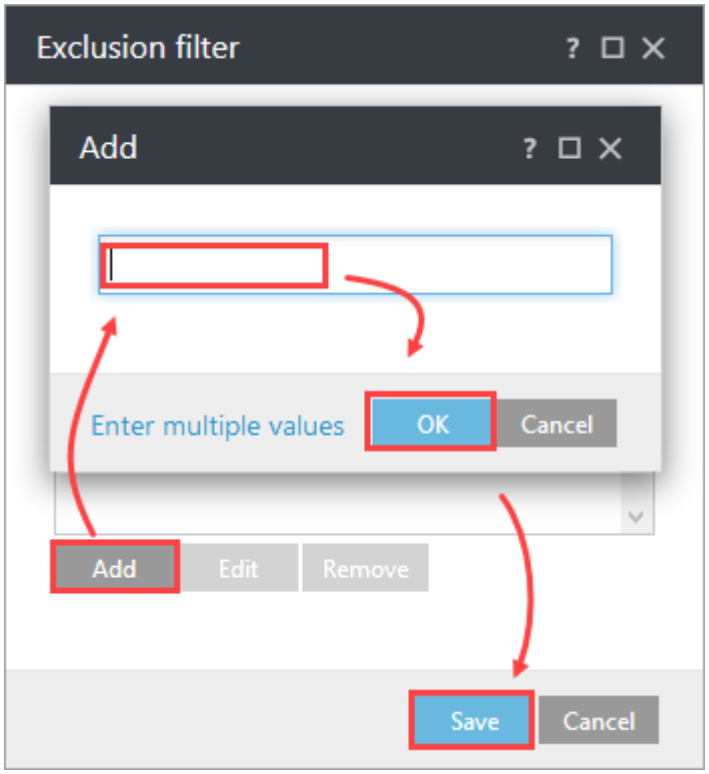


7.Kliknite na **Pridať** a zadajte vylúčenie. Pre potvrdenie kliknite na **OK** > **Uložiť**.

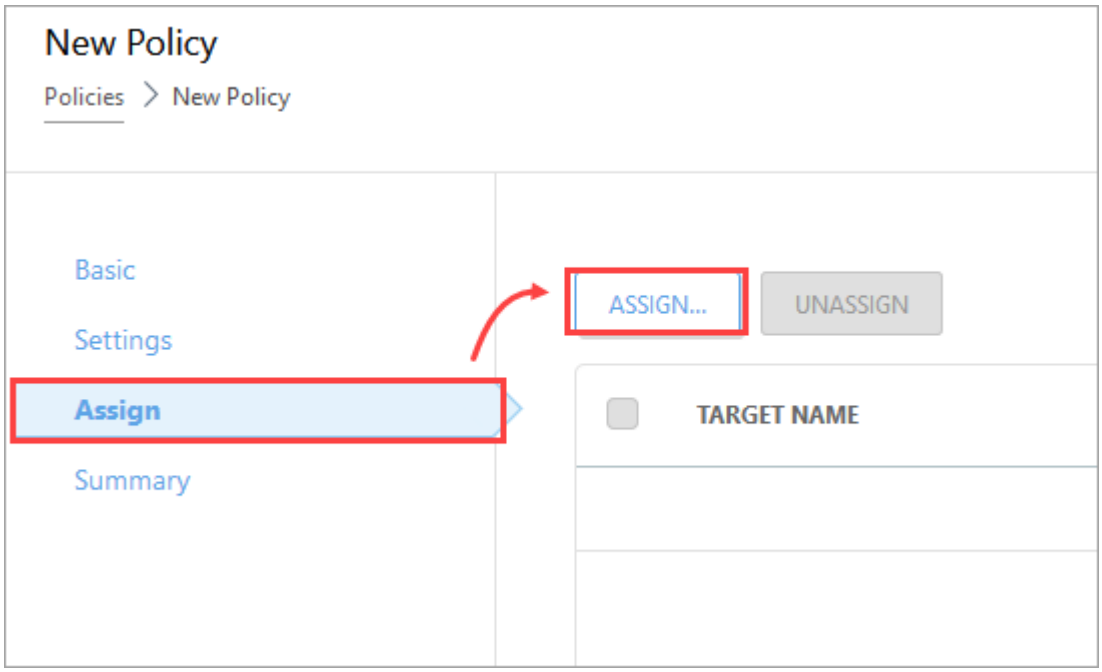
Príklady vylúčení:

```
C:\MyProjects\*
*\DEVtool\debug\*
```

- V rámci vylúčení môžete použiť zástupné znaky * a ?. (* – pre akýkoľvek reťazec znakov, ? – pre akýkoľvek jeden znak)
- Pri vylúčeniach sa nerozlišujú veľké a malé písmená.
- Vylúčenia neakceptujú systémové premenné ani regulárne výrazy.



8.Kliknite na **Priradiť** > **Priradiť** a vyberte počítače alebo skupiny, na ktoré sa bude politika uplatňovať.



9.Kliknite na **OK** > **Dokončiť** pre uloženie a aplikovanie politiky.

Proces výkonnostných vylúčení pri priečinkoch

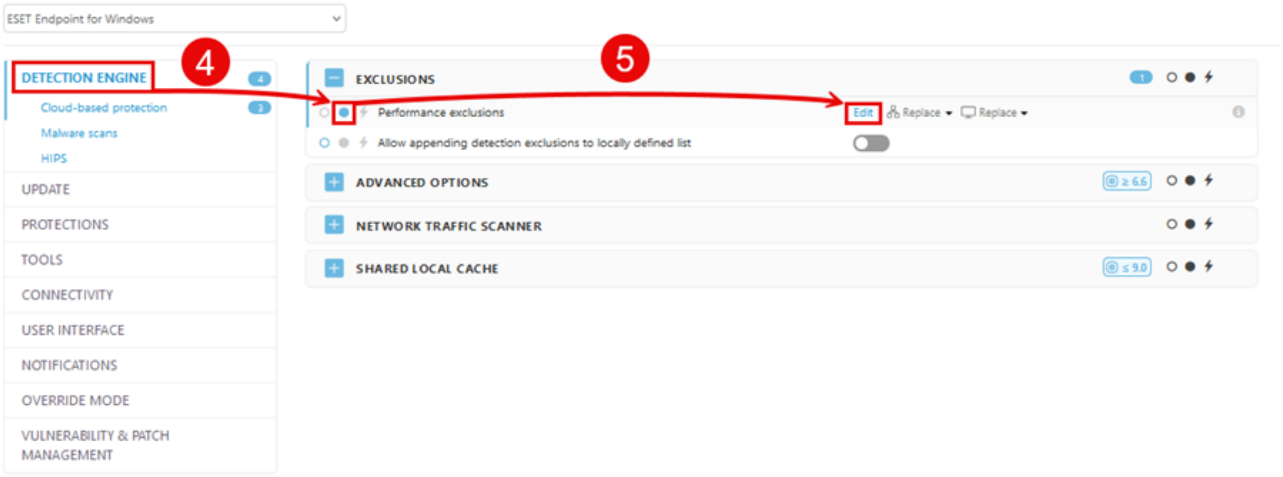
Konkrétne súbory alebo priečinky môžete pred kontrolou a odoslaním do ESET LiveGuard Advanced vylúčiť. Keď súbory presuniete mimo zadanú cestu alebo priečinok, odošlú sa do ESET LiveGuard Advanced.

1.Prihláste sa do Web Console a kliknite na **Politiky** > **Nová politika**.

2.V sekcii **Základné** zadajte **Názov** politiky.

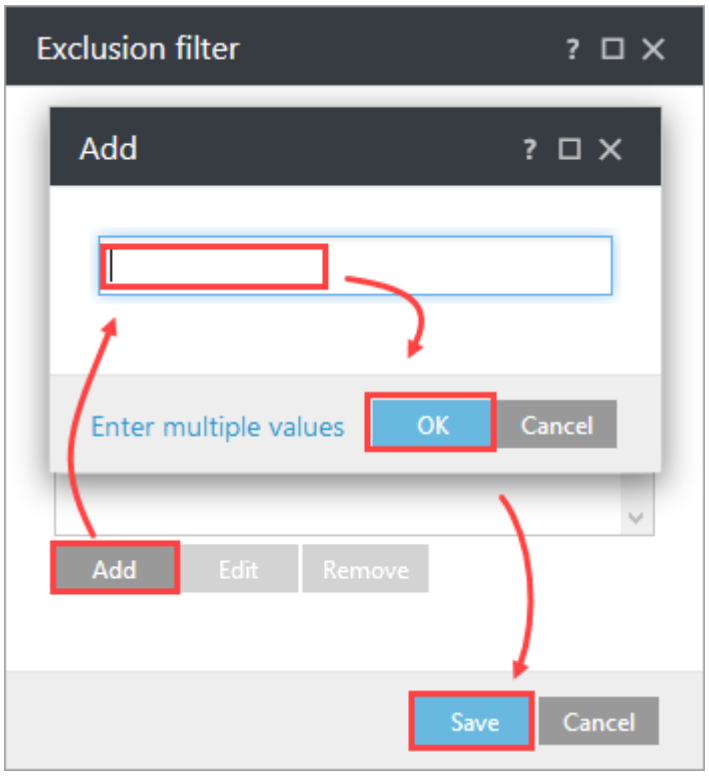
3.V sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows** (prípadne iný kompatibilný produkt).

4.Kliknite na **Detekčné jadro**.



5.V sekcii **Vylúčenia** povoľte **Výkonnostné vylúčenia** a kliknite na **Upraviť**.

6.Kliknite na **Pridať** a zadajte vylúčenie. Pre potvrdenie kliknite na **OK** > **Uložiť**.



7.Kliknite na **Priradiť** > **Priradiť** a vyberte počítače alebo skupiny, na ktoré sa bude politika uplatňovať.

8.Kliknite na **OK** > **Dokončiť** pre uloženie a aplikovanie politiky.

Môžete tiež preskúmať a vylúčiť procesy.

Vylúčenie procesu

Niekedy nie je možné určiť spoľahlivý vzor pre umiestnenia priečinkov a názvy súborov, môžete však namiesto toho vylúčiť názov procesu.

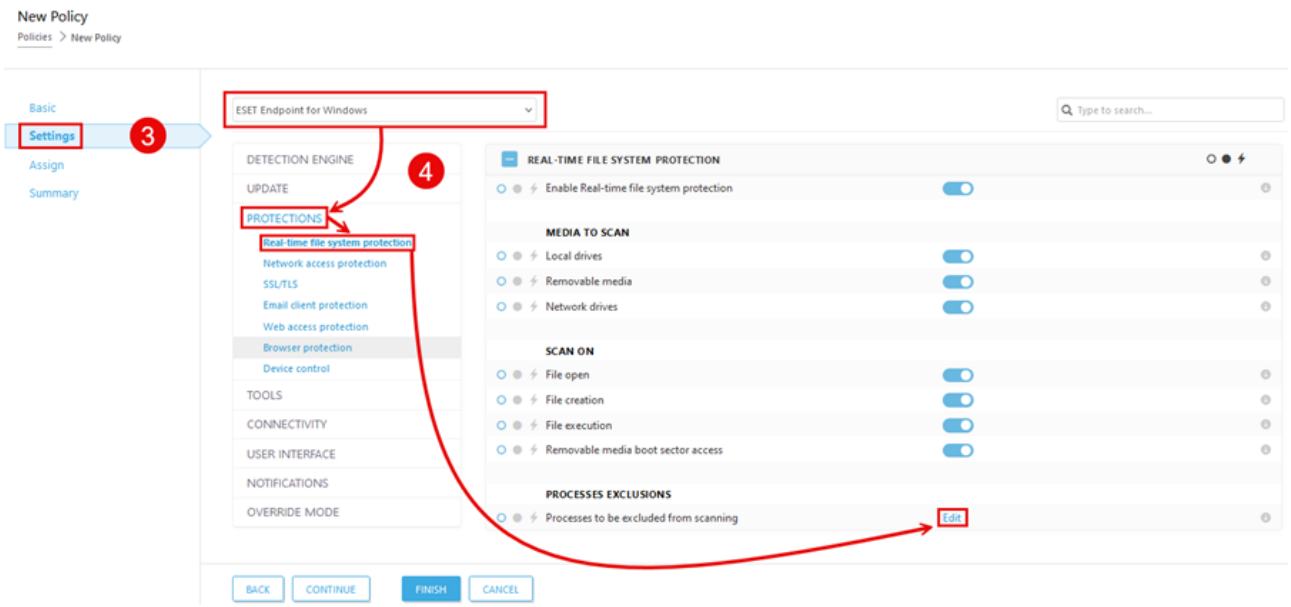
Pri vylúčení procesu nedochádza ku kontrole ani odosielaniu súborov, ktoré boli vytvorené alebo zmenené daným procesom.

1.Prihláste sa do Web Console a kliknite na **Politiky** > **Nová politika**.

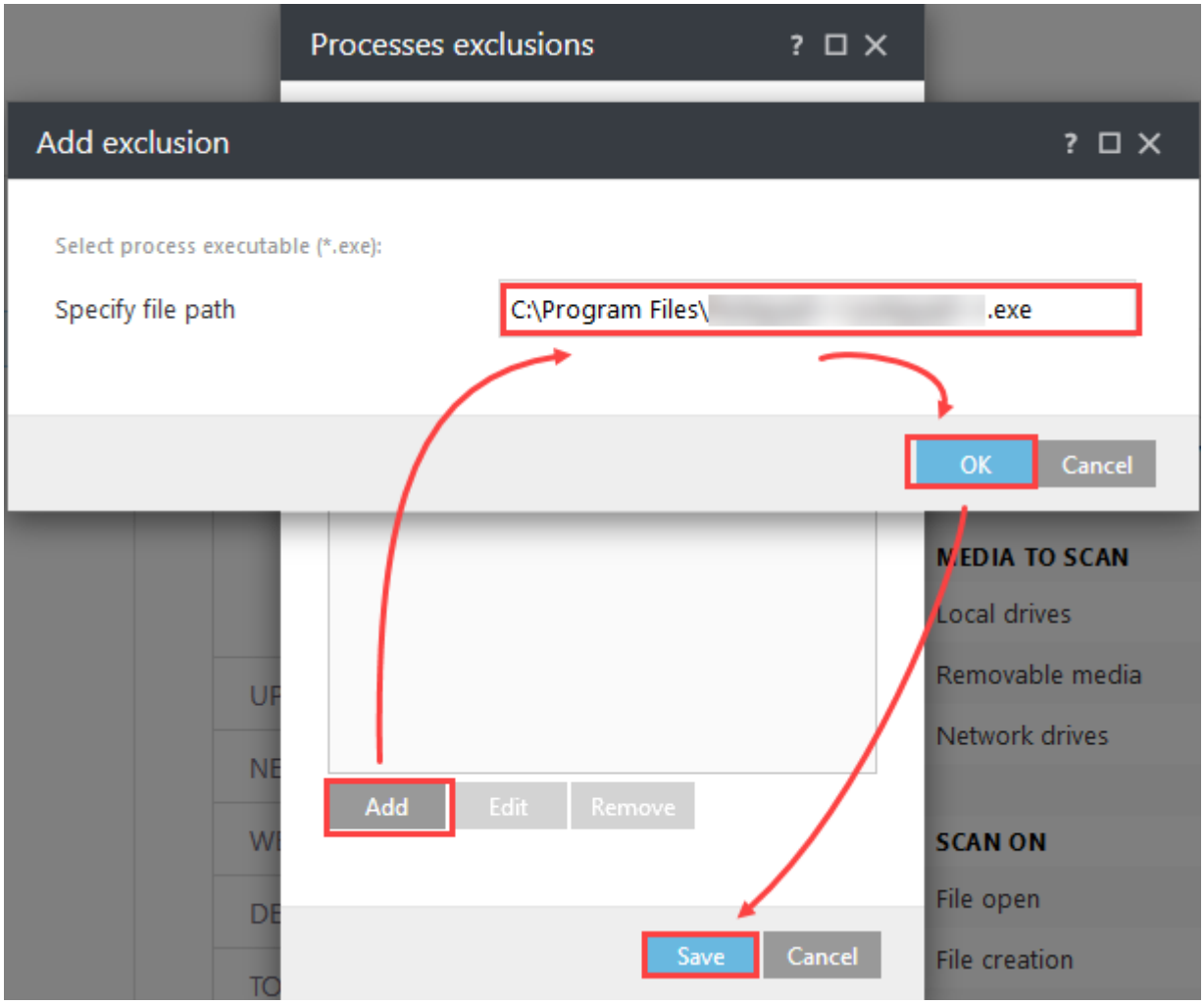
2.V sekcii **Základné** zadajte **Názov** politiky.

3.V sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows** (prípadne iný kompatibilný produkt).

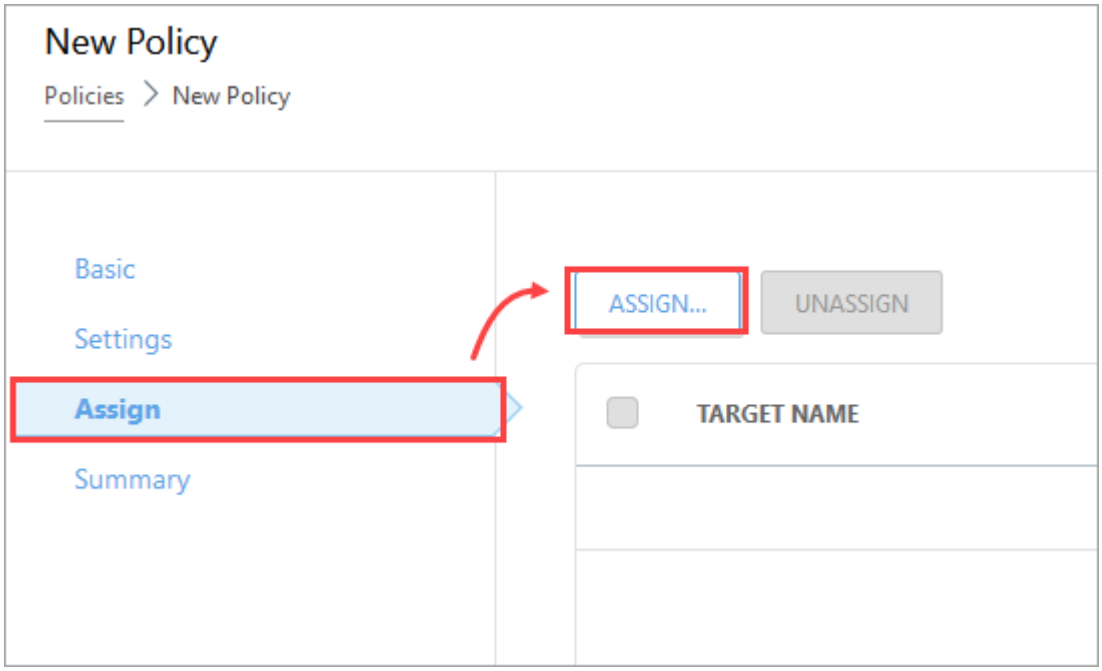
4.Kliknite na **Ochrana** > **Rezidentná ochrana súborového systému** > **Rezidentná ochrana súborového systému** > **Zoznam procesov vylúčených z kontroly** > **Upraviť**.



5.Kliknite na **Pridať**, zadajte názov procesu (úplná cesta k spustiteľnému súboru) a následne kliknite na **OK** > **Uložiť**.



6.Kliknite na **Priradiť** > **Priradiť** a vyberte počítače alebo skupiny, na ktoré sa bude politika uplatňovať.



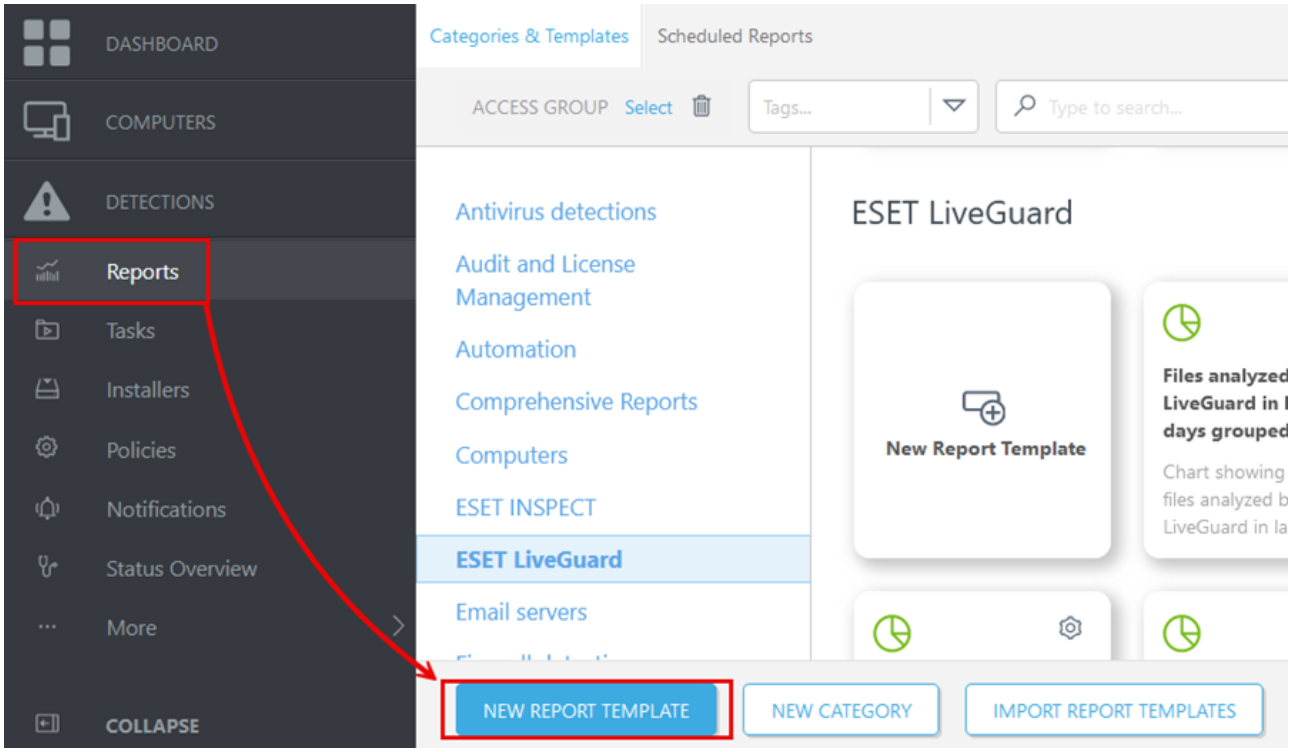
7.Kliknite na **OK** > **Dokončiť** pre uloženie a aplikovanie politiky.

Zistenie počtu odoslaných súborov

Ak chcete zistiť počet súborov odoslaných na servery ESET LiveGuard Advanced, využite možnosť vytvárania reportov v konzole na správu.

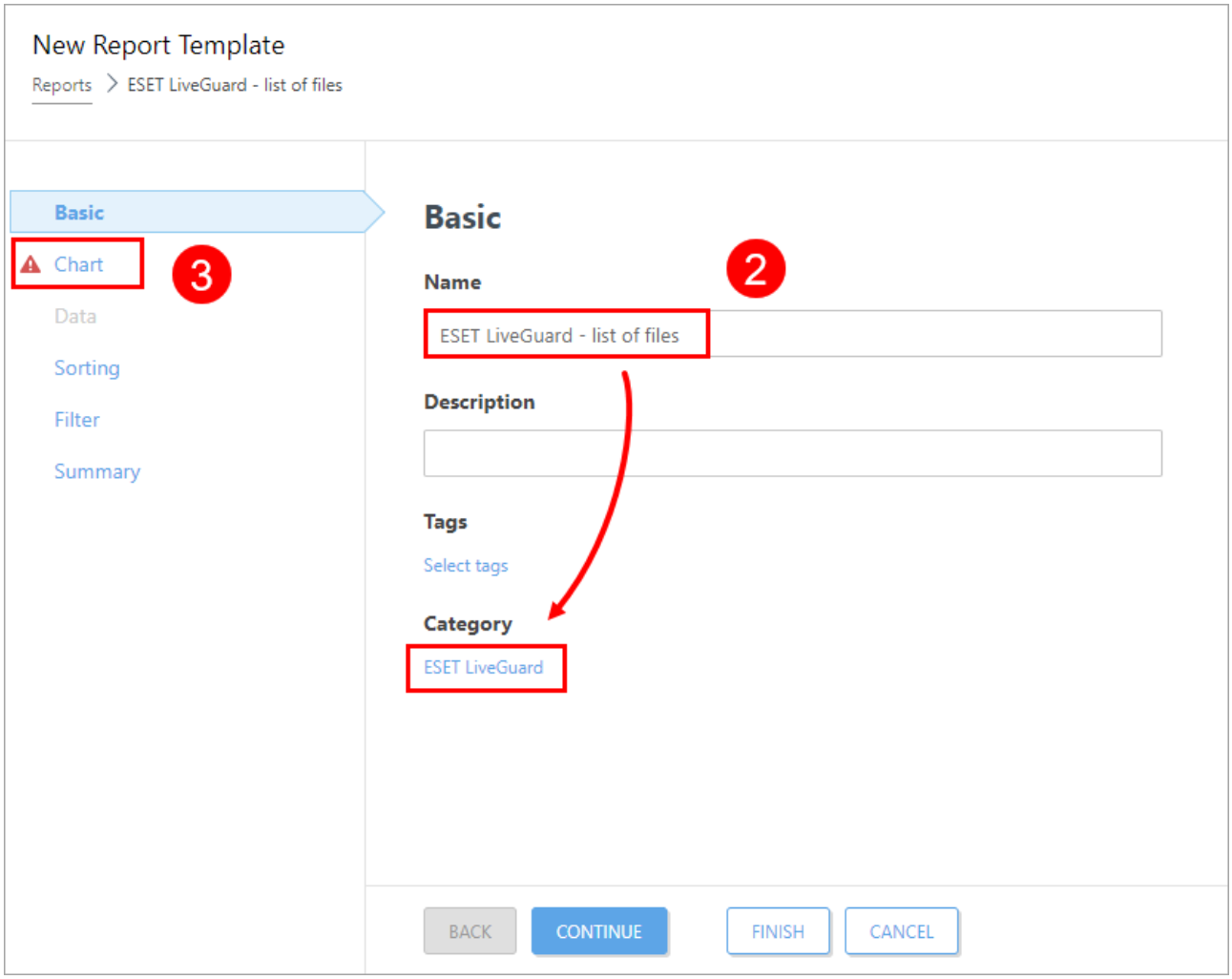
I. Vytvorenie zoznamu odoslaných súborov

1.Vo Web Console prejdite do sekcie **Reporty** > **Nová šablóna reportu**.

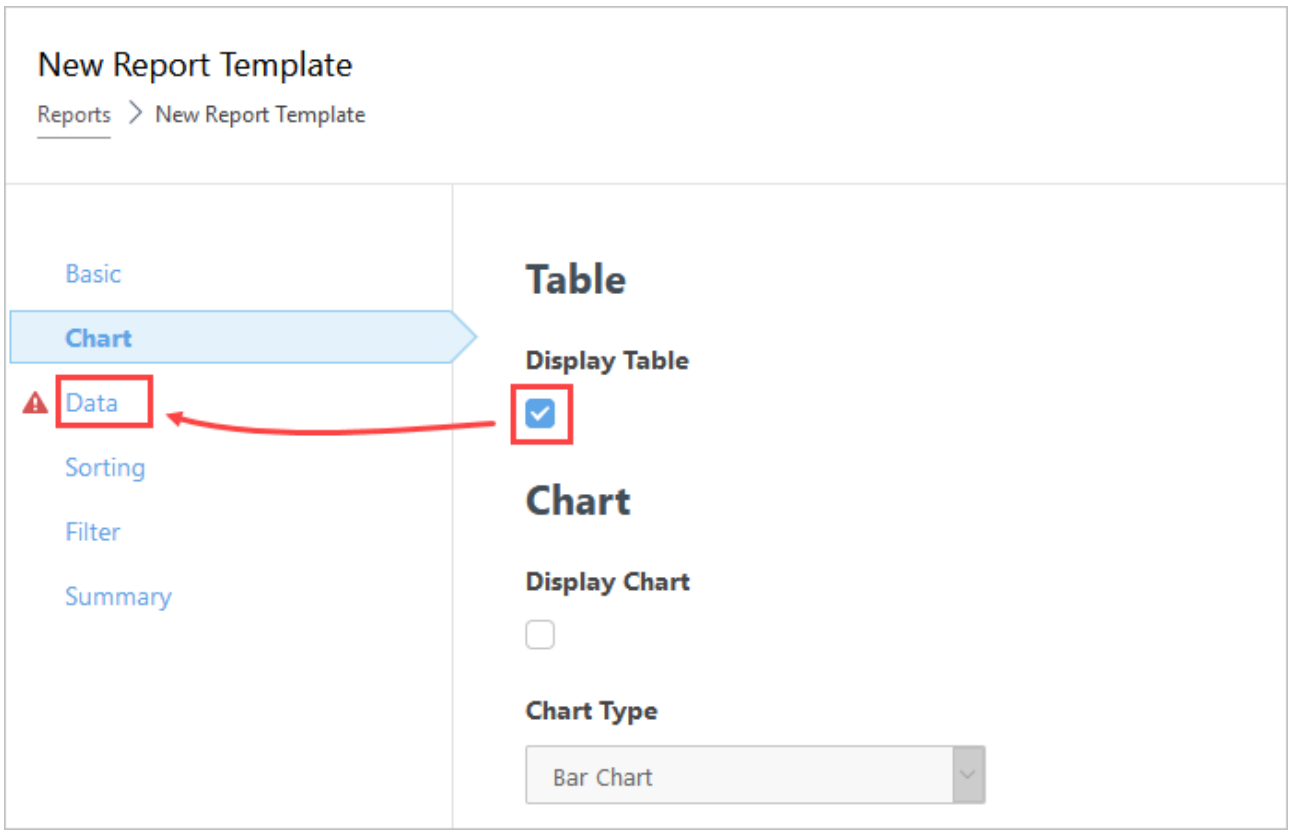


2.Zadajte **Názov** šablóny a vyberte vhodnú **Kategóriu**.

3.Pokračujte v sekcii **Graf**.



4.V sekcii **Graf** označte možnosť **Zobraziť tabuľku** a pokračujte do sekcie **Dáta**.

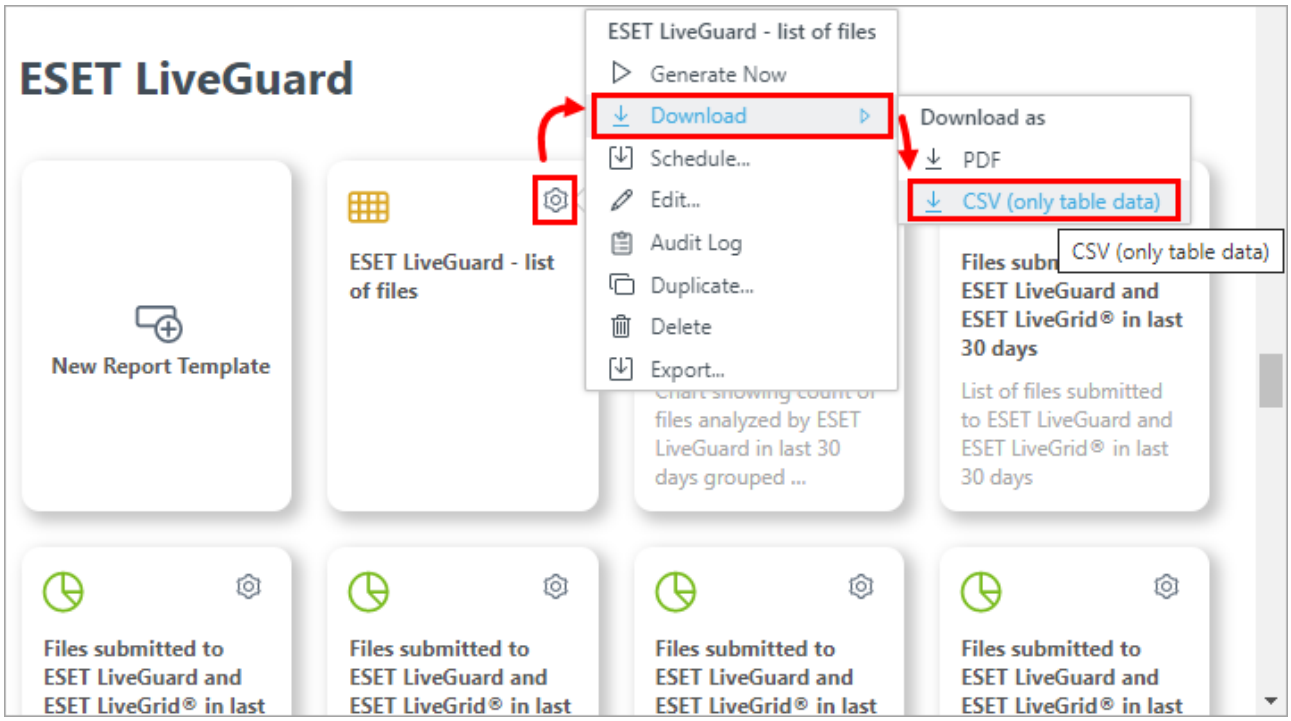


5.V sekcii **Dáta** kliknite na **Pridať stĺpec** a pridajte nasledujúce položky:
Počítač – Názov počítača
ESET LiveGuard – URI objektu
ESET LiveGuard – Čas výskytu
ESET LiveGuard – Obsah súboru bol odoslaný

6.Kliknutím na **Dokončiť** uložte šablónu reportu.

7.V sekcii **Reporty** prejdite do kategórie **ESET LiveGuard**.

8.Vyhľadajte novú šablónu reportu a vygenerujte súbor CSV.

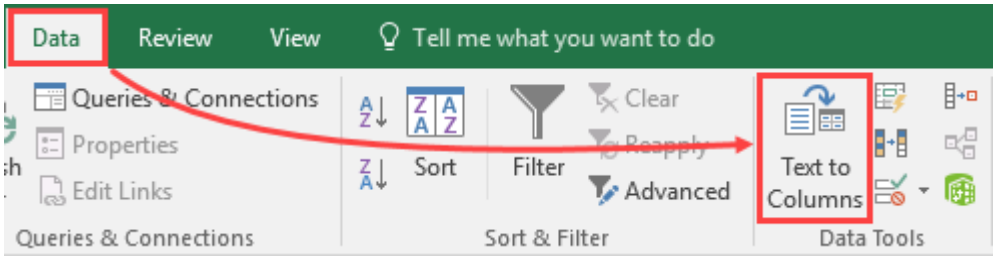


Analýza dát

Nasledujúci postup si vyžaduje softvér tretej strany (editor tabuľkových hárkov) a základné znalosti dátovej analýzy.

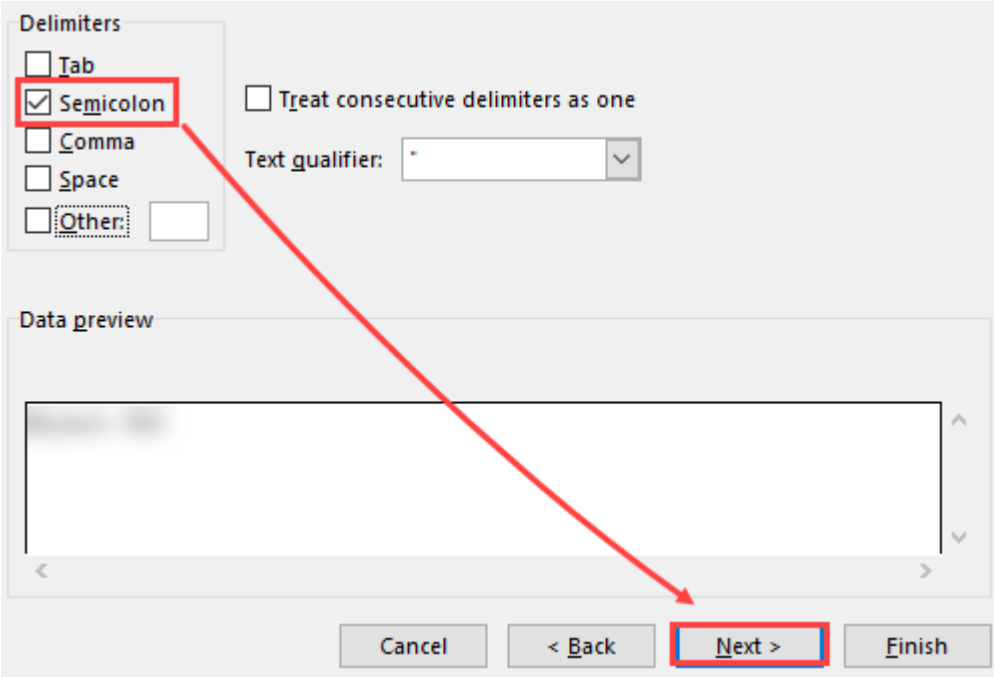
1.Otvorte vyexportovaný súbor CSV vo vhodnom editore (napr. Microsoft Excel).

2.Rozdeľte dáta do dvoch stĺpcov. V programe Microsoft Excel označte prvý stĺpec a prejdite do sekcie **Dáta** > **Text na stĺpce**.



3.Vyberte možnosť **Oddelené** > **Ďalej**.

4.Ako oddeľovač vyberte **Bodkočiarku** a kliknite na **Ďalej** > **Dokončiť**.



Analyzujte dáta.

Navrhované kroky analýzy

1.Odstráňte riadky, pri ktorých má atribút **Obsah súboru bol odoslaný** hodnotu **Nie**.

2.Zoraďte dáta zostupne podľa stĺpca **Čas výskytu**.

3.Vyberte požadované časové rozpätie, napríklad posledných 30 dní, a skopírujte si dáta do ďalšieho hárku.

4.Na ďalšom hárku zoraďte dáta podľa stĺpca **Názov počítača**.

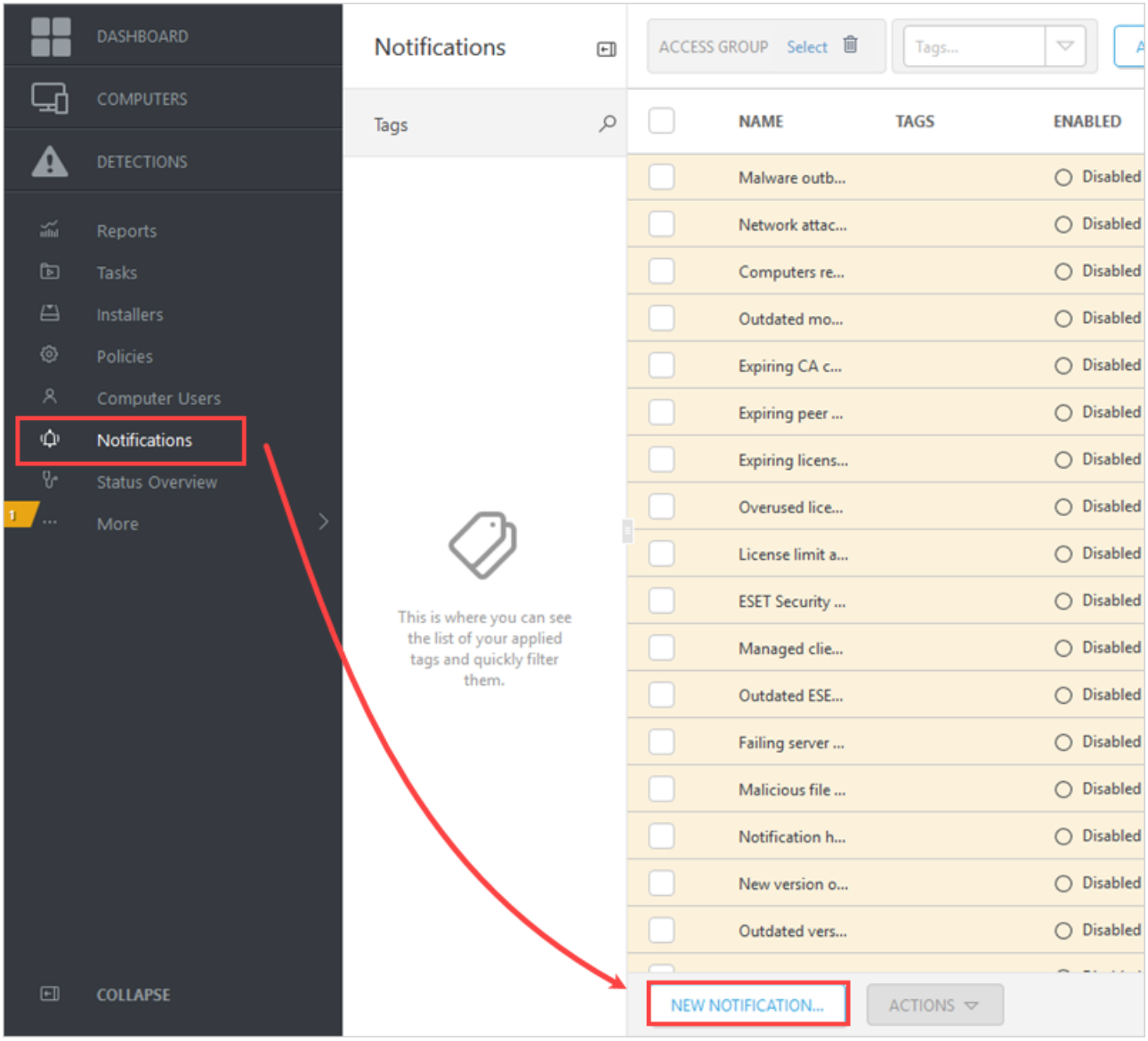
5.Spočítajte riadky (t. j. počet odoslaných súborov) pre jednotlivé počítače.

Oznámenia o detegovaných hrozbách

V konzole na vzdialenú správu môžete nastaviť, aby vám boli zasielané oznámenia o každom súbore, ktorý ESET LiveGuard Advanced označí ako hrozbu.

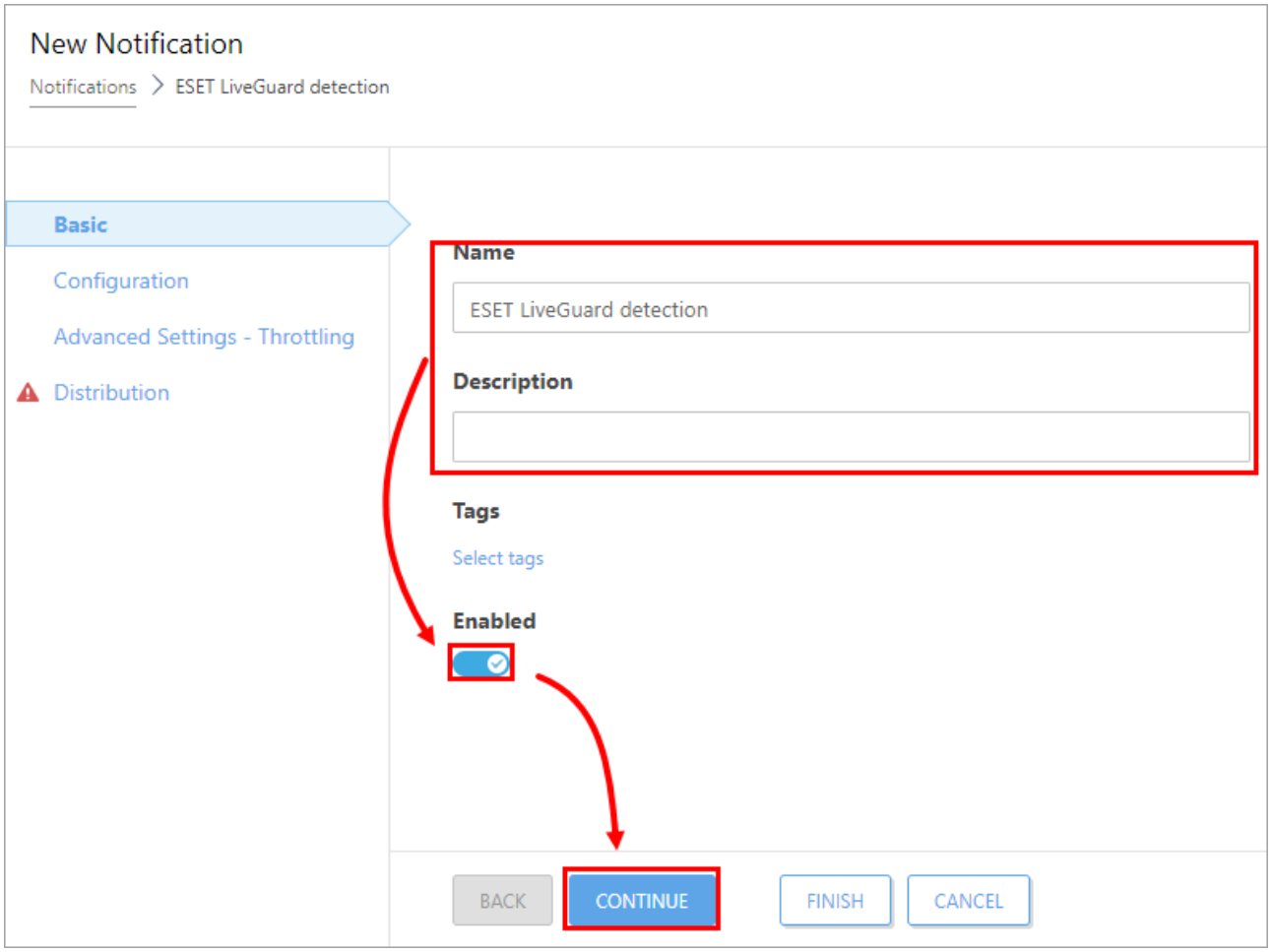
1. Prihláste sa do Web Console.

2. Kliknite na **Oznámenia** > **Nové oznámenie**.



3. Zadajte názov a voliteľne aj popis pre nové oznámenie.

4. Pre zapnutie oznámenia kliknite na prepínacie tlačidlo pod popisom a následne kliknite na **Pokračovať**.

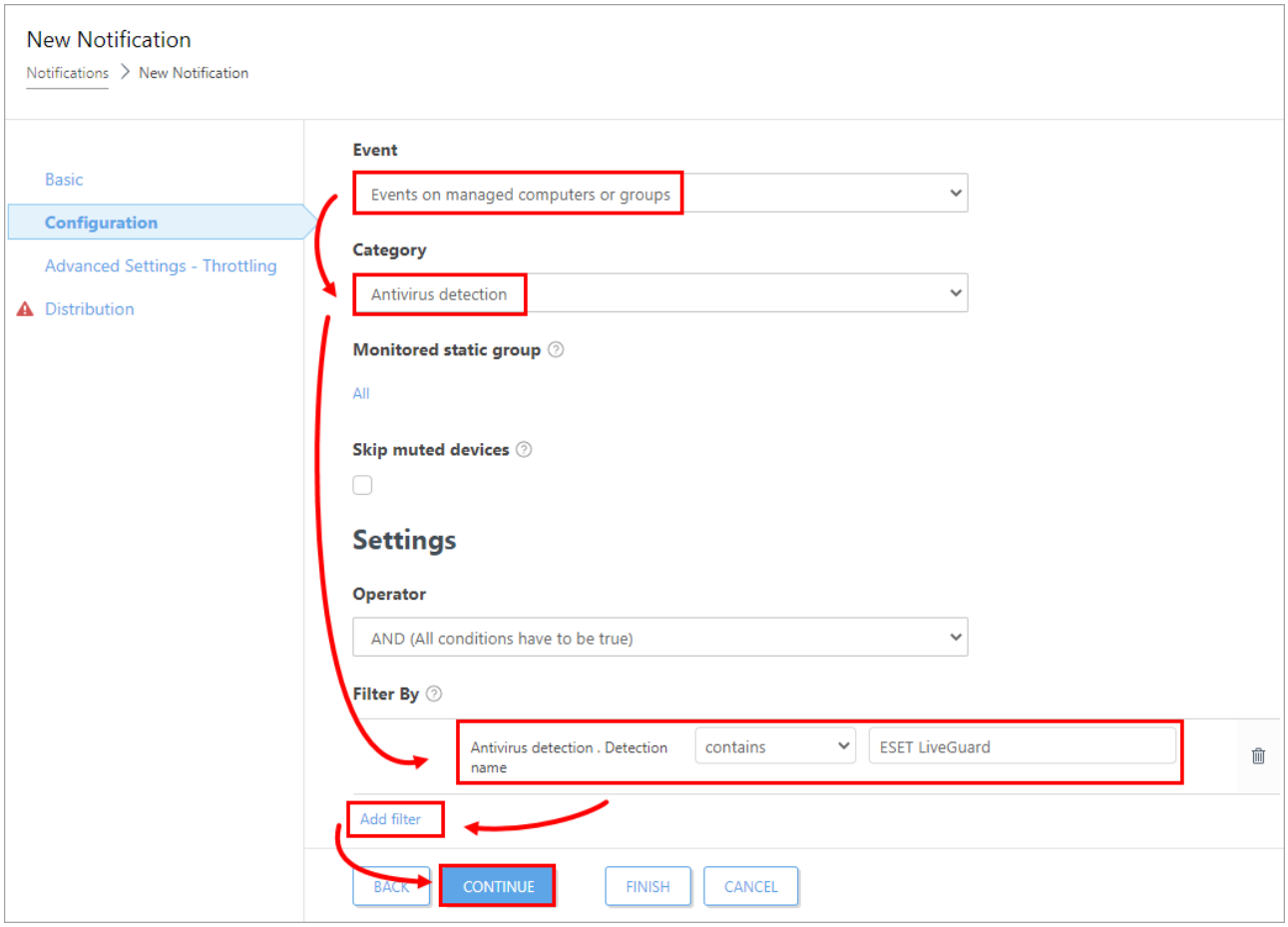


5.V sekcii **Konfigurácia** z roletového menu **Udalosti** vyberte možnosť **Udalosti na spravovaných počítačoch** a potom z roletového menu **Kategória** vyberte možnosť **Detekcia antivírusom**.

6.Môžete tiež zmeniť monitorovanú statickú skupinu. Pre potreby daného oznámenia budú sledované len počítače vo zvolenej skupine a jej podskupinách, ku ktorým má používateľ pridelené povolenia.

7.Ponechajte zvolený operátor **AND**, kliknite na možnosť **Pridať filter** a vyberte položku **Názov detekcie**.

8.Nastavte operátor filtra na **je jedným z**, do vedľajšieho textového poľa zadajte výraz *ESET LiveGuard* a nakoniec kliknite na tlačidlo **Pokračovať**.



9.V časti **Rozšírené nastavenia - Obmedzovanie** môžete nastaviť pokročilé možnosti načasovania pre zasielanie oznámení.

10. V časti Distribúcia si vyberte preferovaný distribučný kanál.

11. Nastavené oznámenie uložte.

> **Používatelia ESET File Security pre Windows**
> Do júna 2021 boli detekcie z ESET Server Security reportované ako: `Blokované EDTD`. Odvtedy došlo k zjednoteniu na `Dynamic Threat Defense` a neskoršiemu premenovaniu na `ESET LiveGuard`.

Najčastejšie otázky

Aké súbory sú odosielané do testovacieho izolovaného priestoru (tzv. sandboxu)?

V prípade manuálneho odosielania súboru na analýzu do ESET LiveGuard Advanced systém odošle zvolený súbor bez ohľadu na typ súboru. Pri automatickom odosielaní bezpečnostný produkt ESET odošle len tie súbory, ktoré ešte neboli kontrolované a ktoré podľa nastavení povolených typov súborov môžu byť odoslané. Typ súboru sa určuje na základe jeho obsahu, nie podľa jeho prípony, ktorú môže používateľ alebo malvér jednoducho zmeniť.

Produkty ESET Mail Security a ESET Endpoint Security využívajú pri spracovávaní súborov odlišný prístup. Rozličné

typy súborov sú spracovávané v každom z týchto produktov inak.

- ESET Mail Security – spracovávanie je synchrónne, systém čaká na výsledok analýzy.
- ESET Endpoint Security a ESET Server Security – spracovávanie je asynchrónne. Systém nečaká na výsledok analýzy.

To, či súbor je odoslaný alebo nie, závisí od jeho zdroja (web/mail/https).

Tabuľka akcií podľa typu súboru

Legenda

– Odoslať – Neodoslať

Typ súboru	Akcia (ESET Mail Security)	Akcia (ESET Endpoint Security, ESET Server Security)	Odosielať iba ak
Archívy (.zip, .rar, .7z, .bzip2 a ďalšie)			• Ak archív nie je šifrovaný • Ak je obsah archívu odoslaný na kontrolu (v tomto prípade je odoslaný celý archív) Týka sa iba produktu ESET Mail Security
Dokumenty (.docm, .xlsm, .pdf a ďalšie)			Ak je aktívny (obsahuje JavaScript alebo iné aktívne prvky)
Dokumenty vo formáte Rich Text Format (.rtf)			
Spustiteľné súbory (.exe, .dll, .sys, .elf, .so a ďalšie)			• Nasledujúce typy súborov sú odosielané len z Linuxových produktov: oSpustiteľný súbor na Linuxe (.elf) oLinuxové knižnice (.so)
Iné (.jar, .lnk, .reg, .msi, .swf a ďalšie)			
Skripty (.bat, .cmd, .js, .vbs, .ps, .py, .sh, .pl a ďalšie)			• Nasledujúce typy súborov sú odosielané len z Linuxových produktov: oPerl skripty (.pl) oPython skripty (.py) oShell skripty (.sh) ovšetky spustiteľné textové súbory (označené „x“)
Obrázky			
Ole2			Ak je aktívny (obsahuje JavaScript alebo iné aktívne prvky) – týka sa iba produktu ESET Mail Security
.hta			

Aká je maximálna veľkosť súboru, ktorý je možné odoslať?

Bezpečnostné produkty ESET môžu na analýzu odoslať súbor, ktorý má veľkosť maximálne 64 MB. Maximálnu veľkosť odosielaných súborov môžete nastaviť prostredníctvom politiky pre váš bezpečnostný produkt v sekcii s

nastaveniami služby ESET LiveGuard Advanced.

Čo znamenajú jednotlivé stavy analýzy a statusy analyzovaných súborov?

Podrobné informácie nájdete v tejto kapitole.

Ako predísť odstráneniu konkrétneho súboru bezpečnostným produktom ESET?

Môžete vytvoriť vylúčenie na základe hash hodnoty daného súboru. Po uplatnení tohto vylúčenia súbor obnovte. Súbor už viac nebude bezpečnostným produktom ESET kontrolovaný.

Ako sa ESET LiveGuard Advanced aktualizuje?

ESET LiveGuard Advanced sa v cloude ESET aktualizuje vzdialene. Nie je preto potrebné službu aktualizovať manuálne. Pre získanie nových funkcií aktualizujte svoje nainštalované bezpečnostné produkty ESET vždy, keď je k dispozícii nová verzia.

Čo sa stane s nastaveniami produktu po tom, čo uplynie platnosť licencie ESET LiveGuard Advanced?

Všetky nastavenia zostanú bez zmeny a Web Console zobrazí upozornenie na koniec platnosti licencie. Ak chcete vypnúť súvisiace nastavenia, aplikujte ďalšiu politiku.

Ako dlho trvá analýza vzorky?

Analýza vzorky, ktorú ESET LiveGuard Advanced nikdy predtým neanalyzoval, trvá zvyčajne do päť minút. Ak už vzorka bola analyzovaná, používateľ dostane výsledok v ďalšom cykle žiadosti, čo môže trvať maximálne dve minúty.

Môže počítač využívať výhody služby ESET LiveGuard Advanced bez odosielania súborov?

Pre počítač, pri ktorom sa vyžaduje vyššia úroveň zabezpečenia, môžete vytvoriť samostatnú politiku, na základe ktorej nebude povolené odosielanie žiadnych súborov z daného počítača. Ak je na takomto počítači aktivovaná služba ESET LiveGuard Advanced, nainštalovaný bezpečnostný produkt ESET bude môcť využívať výsledky analýzy súborov odosielaných z iných zariadení vo vašej spoločnosti. Súbory vyhodnotené ako škodlivé budú následne detegované systémom ESET LiveGrid®, čo prispeje k ochrane všetkých pripojených zariadení.

Ďalšie odpovede na časté otázky sa môžete dočítať v našom článku Databázy znalostí.

Zdieľa ESET LiveGuard Advanced výsledky analýzy so všetkými mojimi účtami alebo zákazníkmi?

- ESET LiveGuard Advanced okamžite zdieľa výsledky so všetkými počítačmi s nainštalovanými produktmi ESET aktivovanými z jedného účtu ESET Business Account, ktorý môže zahŕňať aj viacero licencií.

• Ak máte účet ESET MSP Administrator, ESET LiveGuard Advanced okamžite zdieľa výsledky iba v rámci jedného MSP zákazníka. Zákazníci jedného MSP svoje výsledky nezdieľajú.

Kedy sú výsledky detekcie zo služby ESET LiveGuard Advanced dostupné v systéme ESET LiveGrid®?

Najzávažnejšie detekcie sú dostupné niekoľko hodín po získaní výsledku, menej závažné detekcie neskôr.

Test fungovania služby ESET LiveGuard Advanced

Na otestovanie dostupnosti a funkčnosti služby ESET LiveGuard Advanced postupujte podľa nižšie uvedených krokov:

Používatelia s ESET PROTECT On-Prem

I. Požiadavky

Uistite sa, že služba ESET LiveGuard Advanced je aktivovaná, zapnutá a plne funkčná.

II. Príprava testovacieho súboru

1.Vytvorte si na počítači nový priečinok.

2.Tento priečinok pridajte medzi výkonnostné vylúčenia.

3.Do vylúčeného priečinka stiahnite testovací súbor:
testovací súbor pre Windows
testovací súbor pre Linux

4.Stiahnutý archív v priečinku rozbaľte. Archív je chránený nasledujúcim heslom: infected

5.Používatelia systému Windows: Ak chcete vytvoriť jedinečný súbor, otvorte príkazový riadok stlačením `Win+R` a zadajte `powershell`. Prejdite do vylúčeného priečinka s testovacím súborom. Spustite príkaz uvedený nižšie. Ten na koniec súboru pridá aktuálnu časovú pečiatku, vďaka čomu súbor získa nový hash:

```
Add-Content .\EdtdTestFile.exe $(date)
```

Používatelia systému Linux: Ak chcete vytvoriť jedinečný súbor, otvorte terminál, prejdite do priečinka s vylúčeným testovacím súborom a zadajte `date >> create_eicar.bin` (voliteľne môžete súbor premenovať). Tento príkaz pridá na koniec súboru aktuálnu časovú pečiatku, vďaka čomu súbor získa nový hash.

III. Test ESET LiveGuard Advanced

1.Skopírujte súbor pripravený v predošlej sekcii do priečinka, na ktorý nemáte vytvorené vylúčenie. Súbor bude okamžite odoslaný na analýzu do ESET LiveGuard Advanced, pretože ide o nový spustiteľný súbor.

2.Pomocou nasledujúcich krokov môžete overiť, či bol súbor skutočne odoslaný:
V bezpečnostnom produkte ESET: Kliknite na **Nástroje** > **Protokoly** > **Odoslané súbory**.
V ESET PROTECT Web Console: Kliknite na **Viac** > **Odoslané súbory**.

3.Po chvíli bude súbor odstránený z počítača a produkt zobrazí oznámenie o odstránení malvéru. Túto informáciu si môžete preveriť nasledujúcim spôsobom:
V bezpečnostnom produkte ESET: Kliknite na **Protokoly** > **Detekcie**.
V ESET PROTECT Web Console: Kliknite na **Viac** > **Odoslané súbory**.

4.Ak testovací súbor spustíte pred dokončením analýzy, zobrazí sa vám informácia o spustení testovacieho súboru ESET LiveGuard Advanced. Testovací súbor obsahuje Eicar (štandardný súbor na otestovanie malvérovej ochrany), ktorý bude okamžite odstránený. Po dokončení analýzy na testovacom súbore prebehne liečenie.

IV. Test viacerých súborov

Po detekcii testovacieho súboru sa jeho hash lokálne uloží. Ak sa pokúsite súbor skopírovať z vylúčeného priečinka, okamžite dôjde k detekcii. Môžete tiež vytvoriť jedinečný súbor, a to tak, že zopakujte krok II. 5., aby bol súbor opätovne odoslaný na analýzu. Potom postupujte podľa inštrukcií v sekcii III.

V. Test proaktívnej ochrany

1.Skontrolujte, či je proaktívna ochrana povolená. V bezpečnostnom produkte ESET prejdite do **Rozšírených nastavení** (alebo stlačte kláves F5) a kliknite na **Detekčné jadro** > **Ochrana s podporou cloudu** > **ESET LiveGuard Advanced** > **Proaktívna ochrana** = Blokovať spustenie súboru do doručenia výsledku analýzy.

2.Uistite sa, že je aktivované zobrazovanie príslušných oznámení. V bezpečnostnom produkte ESET stlačte kláves F5 alebo kliknite na **Rozšírené nastavenia** > **Oznámenia** > **Oznámenia na ploche** > **Oznámenia na ploche** > **Upraviť** a povoľte možnosti:
Súbor bol analyzovaný
Prebieha analýza súboru
Súbor nebol analyzovaný

3.Do umiestnenia, pre ktoré nemáte vytvorené vylúčenie, stiahnite druhý testovací súbor a spustite ho.
testovací súbor pre Windows
testovací súbor pre Linux

4.Zobrazí sa vám oznámenie o nepovolenej operácii. Počas trvania analýzy nie je možné súbor spustiť.

5.Keď sa po skončení analýzy potvrdí, že súbor je neškodný, budete ho môcť spustiť.

Používatelia ESET Cloud Office Security

I. Požiadavky

Zaistite, aby bola politika ESET LiveGuard Advanced v riešení ESET Cloud Office Security zapnutá.

II. Príprava testovacieho súboru

1.Do umiestnenia (alebo na zariadenie), ktoré nie je chránené politikou ESET LiveGuard Advanced, stiahnite testovací súbor.

2.Extrahujte stiahnutý súbor. Súbor je archív chránený heslom. Heslo je `infected`.

3.Ak chcete vytvoriť jedinečný súbor, otvorte príkazový riadok stlačením `Win+R` a zadajte `powershell`.

4.Prejdite do priečinka s testovacím súborom.

5.Spustite príkaz uvedený nižšie. Tento príkaz pridá na koniec súboru aktuálnu časovú pečiatku, vďaka čomu súbor získa nový hash:

```
Add-Content .\EdtdTestFile.exe $(date)
```

III. Test ESET LiveGuard Advanced

1.Súbor z kroku II použite jedným z nasledujúcich spôsobov:

Presuňte súbor do úložiska OneDrive.
Vytvorte koncept e□mailu (cez Microsoft Outlook) s testovacím súborom ako prílohou.
Uložte súbor do chráneného umiestnenia na Sharepoint.

2.Súbor bude okamžite odoslaný do služby ESET LiveGuard Advanced.

3.Ak si chcete overiť, či bol súbor odoslaný z riešenia ESET Cloud Office Security, kliknite na **Protokoly** > **Odoslané súbory**.

4.Po chvíli bude súbor odstránený. Výsledky analýzy nájdete v **Odoslaných súboroch**.

Najčastejšie otázky

Používa sa pri tomto teste skutočný malvér?

Nie, `EdtdTestFile.exe` slúži len ako tzv. dropper, ktorý nesie súbor Eicar (štandardný súbor na otestovanie malvérovej ochrany). Táto udalosť je detegovaná počas analýzy v cloudovom sandboxe služby ESET LiveGuard Advanced.

Ako sa o tom môžem uistiť?

Tu si môžete pozrieť zdrojový kód testovacích súborov:

- Spustiteľný súbor pre Windows

```
#include <fstream>

#include "tchar.h"

#include "windows.h"


int main()

{
```

```
    std::ofstream dropped;

    dropped.open(_T("eicar.com"));

    dropped << "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

    dropped.close();

    ::MessageBox(nullptr, _T("EDTD test file has been executed.\n2020.4.15 10:34"),
_T("EDTD test file"), MB_OK);

    return 0;

}
```

- Binárny súbor Linux

```
#include <fstream>

#include <iostream>

#include <stdio.h>


int main()

{

   std::ofstream dropped;

   dropped.open("eicar.com");

   dropped << "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

   dropped.close();

   std::cout << "EDTD test file has been executed." << std::endl;

   getchar();

   return 0;

}
```

Riešenie problémov

- Služba nefunguje.
- ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje.
- Kde nájdem protokoly?

- V ESET PROTECT Web Console nevidím odoslané súbory.
- Príznaky vyjadrujúce výsledok analýzy vzorky nie sú správne.
- Ako môžem zabrániť presunutiu detegovaného súboru do karantény?
- Čo robiť, ak licencii vyprší platnosť?
- Čo ak je pole Status v okne Odoslané súbory prázdne?
- ESET PROTECT On-Prem nesťahuje dáta z ESET LiveGuard Advanced
- V ESET PROTECT Web Console chýbajú výsledky pre odoslané súbory
- Čo ak sa mi zobrazuje stav „Odoslané do LiveGrid“ pre súbory odoslané do ESET LiveGuard Advanced
- Produkt odmieta moju licenciu pre ESET LiveGuard Advanced
- Zobrazuje sa mi niektoré z nasledujúcich chybových hlásení v sekcii Podrobnosti o počítači > Upozornenia
- Súbory odoslané do ESET LiveGuard Advanced sa nezobrazujú vo Web Console
- Zobrazila sa mi chyba: Vaša licencia neumožňuje prístup k správe o aktivite súboru
- Mám podozrivú vzorku, čo mám robiť?
- Aktivácia ESET LiveGuard Advanced nebola úspešná

Služba nefunguje

Uistite sa, že služba ESET LiveGuard Advanced je aktivovaná a nakonfigurovaná.

Overte tiež:

- Je licencia na ESET LiveGuard Advanced využívaná?
- Je politika pre ESET LiveGuard Advanced aplikovaná?

ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje.

Overte, či je medzi ESET Management Agentom a ESET PROTECT Serverom funkčné sieťové spojenie.

Prípadné problémy v komunikácii medzi serverom vzdialenej správy a ESET LiveGuard Advanced uvidíte priamo vo Web Console v sekcii **Riadiace panely** > **ESET PROTECT Server** > **Sieťové partnerské zariadenia ESET PROTECT On-Prem s problémami**.

Prekontrolujte tiež konfiguráciu **HTTP Proxy** v nastaveniach ESET PROTECT.

Zozbieranie protokolov

Viac informácií o protokoloch nájdete v online pomocníkovi pre ESET PROTECT On-Prem.

Vo Web Console nevidím odoslané súbory.

K tomuto zvykne dochádzať v prípade súborov odosielaných na analýzu z mobilných klientov mimo siete.

Príznaky vyjadrujúce výsledok analýzy vzorky nie sú správne.

V prípade, že príznaky súvisiace s aktivitou zachytenou pri analýze vzorky sa vám nezdajú byť správne:

- Nahláste túto situáciu technickej podpore spoločnosti ESET, prípadne vzorku pošlite na adresu samples@eset.com. Prečítajte si náš článok na tému odosielania vzoriek.
- Navštíviť ESET Bezpečnostné fórum a prediskutovať problém s ESET komunitou.

Ako môžem zabrániť presunutiu detegovaného súboru do karantény?

Ak ste si istý, že detegovaný súbor je bezpečný, môžete preň vytvoriť vylúčenie.

Čo robiť, ak licencii vyprší platnosť?

Aj keď licencii pre ESET LiveGuard Advanced vyprší platnosť, stále budete môcť posielať podozrivé súbory na analýzu. Nebudete však môcť dostať výsledky analýzy súboru ani správu o aktivite súboru.

Čo ak je pole Status v okne Odoslané súbory prázdne?

> **Používate ESET PROTECT?**
> Toto riešenie problémov je určené pre používateľov lokálnej konzoly na vzdialenú správu ESET PROTECT On-Prem.

1. Skontrolujte **Riadiaci panel** (vo svojej konzole na vzdialenú správu) podľa postupu v tejto časti: ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje.

2. Kliknite na položku **Reporty** > **Správa licencií a auditu** > **Protokol auditu** > **Vygenerovať a stiahnuť** > **PDF**. Tento stiahnutý protokol môžete priložiť k žiadosti o technickú podporu, prípadne si ho prezrieť sami.

Ak obsahuje chyby alebo problémy týkajúce sa ESET LiveGuard Advanced, získajte sledovacie protokoly (podľa pokynov uvedených nižšie) a kontaktujte oddelenie technickej podpory spoločnosti ESET. V opačnom prípade môžete reštartovať proces načítavania výsledkov analýzy na server vzdialenej správy.

Ako získať sledovacie protokoly:

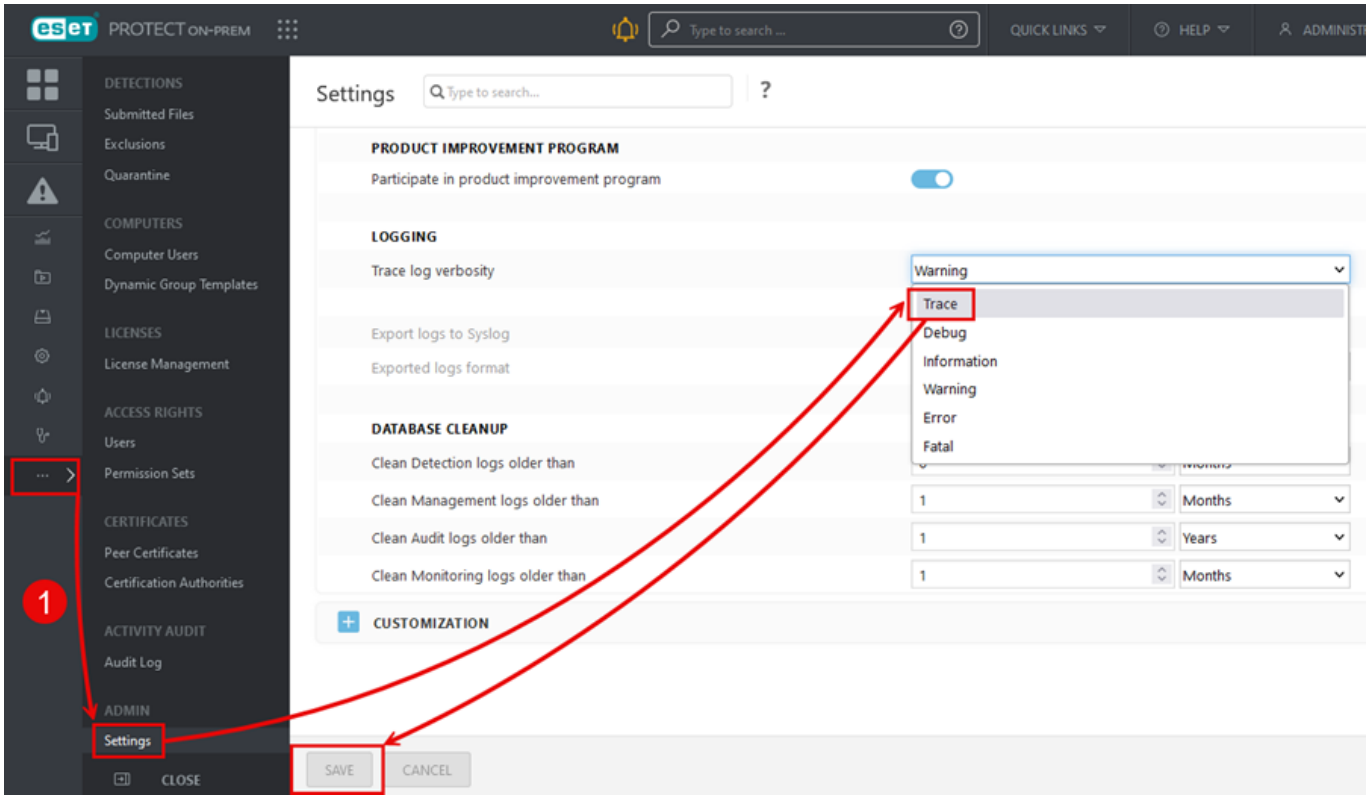
1.Vo Web Console povoľte zapisovanie do sledovacích protokolov kliknutím na **Viac…** > **Nastavenia** > **Pokročilé nastavenia** > **Zapisovanie do protokolov** > **Zaznamenávať protokoly od úrovne** > **Sledovanie**.

2.Reštartujte ESET PROTECT On-Prem službu alebo počítač a následne počkajte aspoň 15 – 20 minút.

3.Protokoly nájdete na ESET PROTECT Serveri:

I.Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

II.Linux: */var/log/eset/RemoteAdministrator/Server/*



Ako reštartovať sťahovanie výsledkov z ESET LiveGuard Advanced

Proces načítavania dát na ESET PROTECT Server môžete reštartovať. Reštart môže pomôcť v prípade, ak Server nesťahuje nové dáta z cloudu ESET alebo je sťahovanie príliš pomalé.

1.Vypnite službu ESET PROTECT Server.

2.Prihláste sa do ESET PROTECT databázy prostredníctvom SSMS (SQL Server Management Studio) alebo použitím MySQL klienta na systémoch Linux.

3.Upravte tabuľku tbl_key_value_pairs v databáze ESET PROTECT:

V prípade použitia SSMS (SQL Server Management Studio) otvorte tabuľku a odstráňte riadok obsahujúci reťazec `eset-dynamic-threat-detection-customers`

V prípade použitia MySQL otvorte databázu a spustite príkaz `delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';`

V prípade použitia virtuálneho zariadenia ESET PROTECT:

a)Prihláste sa do terminálu na virtuálnom počítači, na ktorom je spustené virtuálne zariadenie.

b)Prihláste sa do databázy: `mysql -u root -p era_db`

c)Zadajte heslo. Zvyčajne ide o to isté heslo, ktoré používate pre prihlásenie sa do Web Console do účtu

správcu (Admnistrator).

d)Spustite nasledujúci príkaz:

```
delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';
```

4.Zapnite ESET PROTECT Server a nasledujúcich 24 hodín ho nereštartujte ani nevypínajte.

V ESET PROTECT Web Console chýbajú výsledky pre odoslané súbory

Možné príčiny:

- ESET LiveGuard Advanced bol aktivovaný pomocou licenčného kľúča namiesto účtu EBA

Riešenie:

1.Odstráňte aktuálnu licenciu z ESET PROTECT On-Prem

2.Do účtu ESET Business Account pridajte licenciu vhodnú pre ELGA

3.Pomocou účtu EBA pridajte licenciu do ESET PROTECT On-Prem

4.Znovu aktivujte ESET LiveGuard Advanced pre klienta

5.Reštartujte službu ESET PROTECT Server.

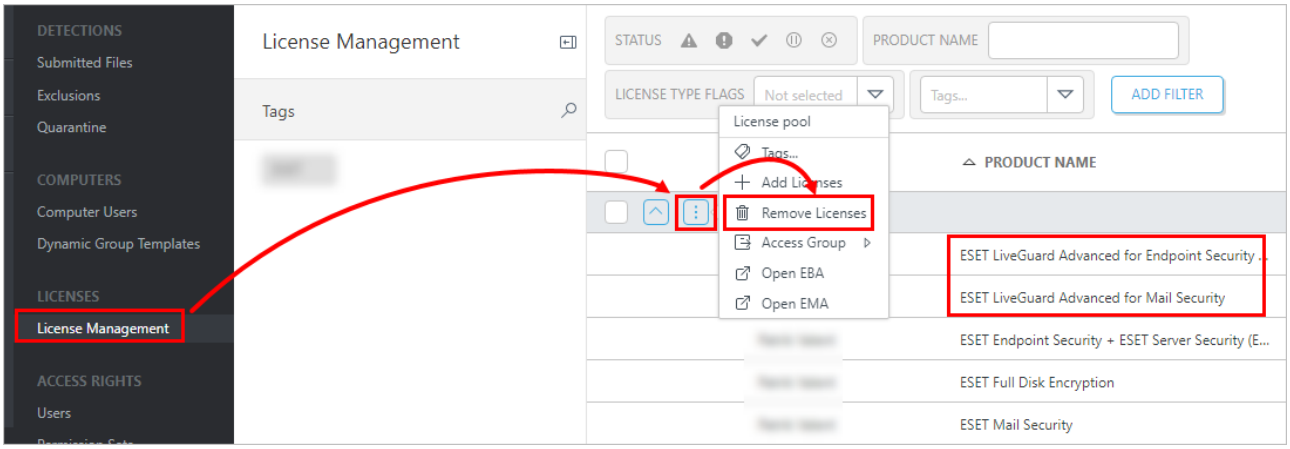
Čo ak sa mi zobrazuje stav „Odoslané do LiveGrid“ pre súbory odoslané do ESET LiveGuard Advanced

Možné príčiny:

- Súbor alebo spamový e mail, ktorý ste odoslali, bol už detegovaný.
- Problém môže byť v tom, že licencia pre ESET LiveGuard Advanced nebola importovaná prostredníctvom vášho účtu na portáli EBA, ale bola zadaná priamo do bezpečnostného produktu alebo do konzoly na vzdialenú správu.

Aby sa povolilo odosielanie súborov do ESET LiveGuard Advanced, postupujte nasledovne:

1.Odstráňte licenciu zo svojej **Správy licencií**.



2.Licenciu naimportujte do svojho účtu na portáli ESET Business Account (EBA).

3.Zosynchronizujte účet EBA so svojím serverom vzdialenej správy (ESET PROTECT On-Prem).

4.Niektoré moduly na klientskych počítačoch musia byť opätovne načítané. Máte na výber dve možnosti:

- Počkajte, kým v priebehu niekoľkých hodín dôjde k opätovnému načítaniu modulov.
- Pre okamžité načítanie môžete „reštartovať“ ESET LiveGuard Advanced na klientskych počítačoch. Stačí na počítače poslať politiku na deaktivovanie ESET LiveGuard Advanced. Po uplatnení tejto politiky pošlite na počítače ďalšiu politiku, tentokrát na aktivovanie služby.

Produkt odmieta moju licenciu pre ESET LiveGuard Advanced

- Po zadaní licenčného kľúča pre ESET LiveGuard Advanced do Web Console sa vám zobrazilo nasledujúce chybové hlásenie:
  - **Zlyhalo pridanie licencie pomocou licenčného kľúča: Licencia je vydaná pre produkt, ktorý nie je možné spravovať pomocou konzoly ESET PROTECT On-Prem. Zadajte inú licenciu, prosím.**
- Po zadaní licenčného kľúča pre ESET LiveGuard Advanced priamo do bezpečnostného produktu ESET sa vám zobrazilo nasledujúce chybové hlásenie:
  - **Aktivácia nebola úspešná. Licencia a produkt sa nezhodujú.**

Licencia musí byť pridaná výhradne cez váš účet na portáli ESET Business Account (EBA). Viac o importovaní licencie sa dozviete v tejto kapitole.

Zobrazuje sa mi niektoré z nasledujúcich chybových hlásení v sekcii Podrobnosti o počítači > Upozornenia

Problém	Podrobnosti problému	Príčina a riešenie
ESET LiveGuard Advanced nie je dostupný.	ESET LiveGuard Advanced nefunguje. Pripojenie k overovacím serverom zlyhalo.	Nie je možné získať prístup k licenčným serverom ESET. • Firewall (iné nastavenie) blokuje komunikáciu. • Služba je dočasne nedostupná. Skontrolujte nastavenia firewallu.

Problém	Podrobnosti problému	Príčina a riešenie
ESET LiveGuard Advanced nie je dostupný.	Uplynula platnosť licencie ESET LiveGuard Advanced.	Vaša licencia ESET LiveGuard Advanced bola funkčná, ale jej platnosť uplynula. Obnovte svoju licenciu alebo vypnite nastavenie ESET LiveGuard Advanced prostredníctvom politiky.
ESET LiveGuard Advanced nie je dostupný.	Servery ESET LiveGuard Advanced nie sú dostupné. Môže to byť spôsobené výpadkom alebo problémom so sieťovým pripojením.	Váš počítač sa nedokáže pripojiť k serverom ESET LiveGuard Advanced. Zvyčajne je to spôsobené zlyhaním služby proxy. Skúste reštartovať službu proxy. Ak problém pretrváva naďalej, môže to znamenať, že služba proxy je preťažená. Môžete: • rozdeliť zaťaženie spôsobené agentmi medzi viaceré proxy, • použiť výkonnejší hardvér na proxy zariadení, • použiť 64-bitovú verziu Apache HTTP Proxy (ak ste doteraz používali 32-bitovú verziu a váš systém má 64-bitovú architektúru), • dočasne pozastaviť službu proxy pre potvrdenie, že skutočne spôsobuje daný problém. • Ak používate Apache HTTP Proxy, môžete prejsť na ESET Bridge.
Web Console nezobrazuje žiadne výsledky.	Výsledky analýzy nie sú doručené na ESET PROTECT Server.	HTTP Proxy môže byť preťažená. Skúste presunúť HTTP Proxy na iný server, prípadne pridať ďalšie prostriedky. Po presunutí HTTP Proxy na novú adresu je potrebné aktualizovať politiku na koncových zariadeniach.
ESET LiveGuard Advanced nie je dostupný.	Chyba offline licencie ESET LiveGuard Advanced.	ESET LiveGuard Advanced nepodporuje aktiváciu offline licenciou. Skontrolujte si licenciu.
ESET LiveGuard Advanced nie je dostupný.	ESET LiveGuard Advanced nefunguje. Neznáma chyba overenia.	Overovacie servery ESET nie sú z klientskeho počítača dostupné. Overte, či máte prístup na *edf.eset.com*.

Súbory odoslané do ESET LiveGuard Advanced sa nezobrazujú vo Web Console

• Súbory sa neodosielajú na servery ESET LiveGuard Advanced, ak váš operačný systém (zvyčajne ide o starší systém Windows Server) nedôveruje certifikátu na *ts.eset.com*. Pre vyriešenie tohto problému importujte do svojho operačného systému koreňové certifikáty DigiCert Global Root G2 a Thawte TLS RSA CA G1.

• Vo Web Console sa môžu odoslané súbory zobraziť iba v prípade, že sa ESET Management Agent pripája (replikuje dáta) k ESET PROTECT Serveru. Informácie o súboroch odoslaných z mobilných klientov sa zobrazia až po pripojení Agenta k Serveru.

Ak používate ESET LiveGuard Advanced v podnikovom prostredí (stovky a viac zariadení), odporúčame nasadiť HTTP Proxy na vyhradený samostatný server. Prevádzkovanie služby HTTP Proxy na intenzívne využívanom serveri (napr. popri ESET PROTECT Serveri alebo databáze) môže mať za následok problémy s ESET LiveGuard Advanced pripojením.
Môžete vylúčiť označené priečinky a procesy pre zníženie počtu odosielaných súborov a zlepšenie celkového výkonu.

Zobrazila sa mi chyba: Vaša licencia neumožňuje prístup k správe o aktivite súboru

Ak používate na správu licencií portál EBA a váš celkový počet licenčných jednotiek v rámci licencií na ESET LiveGuard Advanced je nižší ako 100, nemáte možnosť zobraziť celú správu o aktivite súboru. Niektoré verzie konzoly na správu vôbec neposkytujú správu o aktivite súboru. Svoj počet licenčných jednotiek musíte navýšiť aspoň na 100, aby ste získali prístup k správe o aktivite súboru.

Mám podozrivú vzorku, čo mám robiť?

Prečítajte si kapitolu Odporúčania pre používateľov s podozrivou vzorkou.

Aktivácia ESET LiveGuard Advanced nebola úspešná

Ak ste pridali licenciu prostredníctvom licenčného kľúča a potom prešli na cloudovú úroveň ochrany, v konzole sa zobrazí licencia ESET LiveGuard Advanced, ale aktivácia zlyhá. V tomto prípade úroveň ochrany zo správy licencií v konzole odoberte a pridajte ju prostredníctvom účtu EBA.

Vykonanie diagnostiky

Ak ESET LiveGuard Advanced nefunguje:

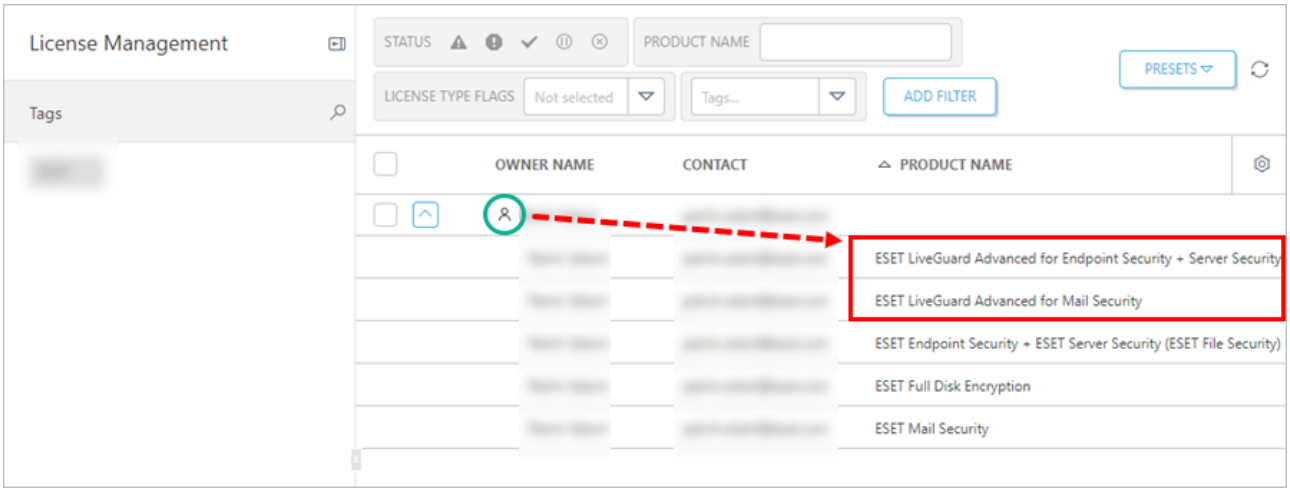
- uistite sa, že máte splnené všetky požiadavky,
- Vo Web Console vyhľadajte možnú príčinu podľa nasledujúcich inštrukcií.

Licencia na ESET LiveGuard Advanced

1. Prihláste sa do Web Console.

2. Kliknite na **Viac** > **Správa licencií**.

3. Skontrolujte, či je v zozname uvedená licencia pre ESET LiveGuard Advanced. Ak sa licencia v zozname nenachádza, pridajte ju prostredníctvom svojho účtu na portáli ESET Business Account alebo ESET MSP Administrator. Ak ste licenciu pridali prostredníctvom účtu ESET Business Account, uistite sa, že sa pri licencii zobrazuje ikona: Táto ikona indikuje, že licencia bola importovaná prostredníctvom účtu EBA.



Používatelia podporovaných produktov pre Linux si môžu svoju licenciu a ID licenčnej jednotky overiť lokálne pomocou terminálu.

- Overenie licencie v ESET Server Security pre Linux.
- Overenie licencie v ESET Endpoint Security pre Linux.

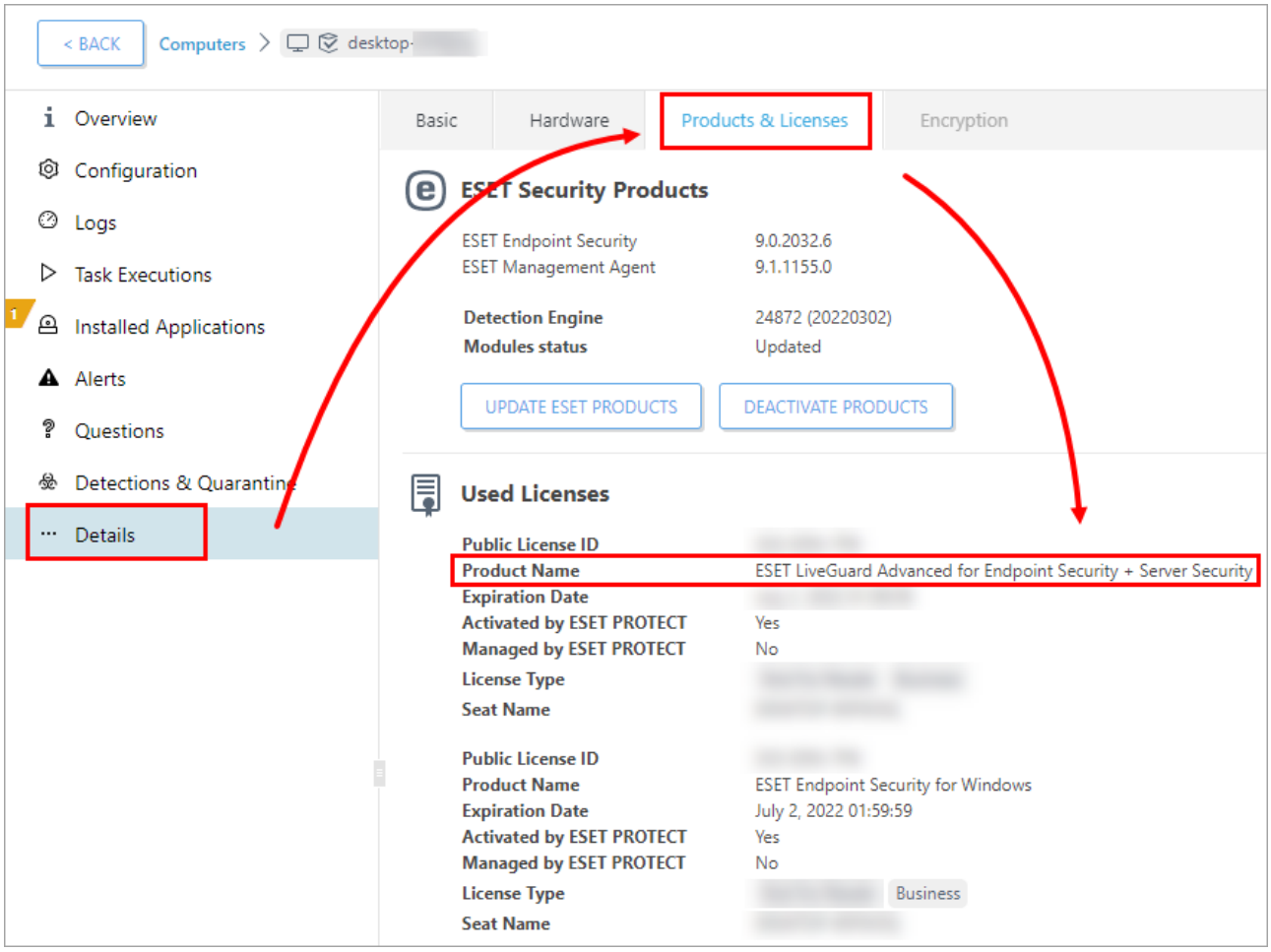
Aktivácia produktu

1.Prejdite do sekcie **Počítače**.

2.Kliknite na počítač > **Zobraziť podrobnosti**.

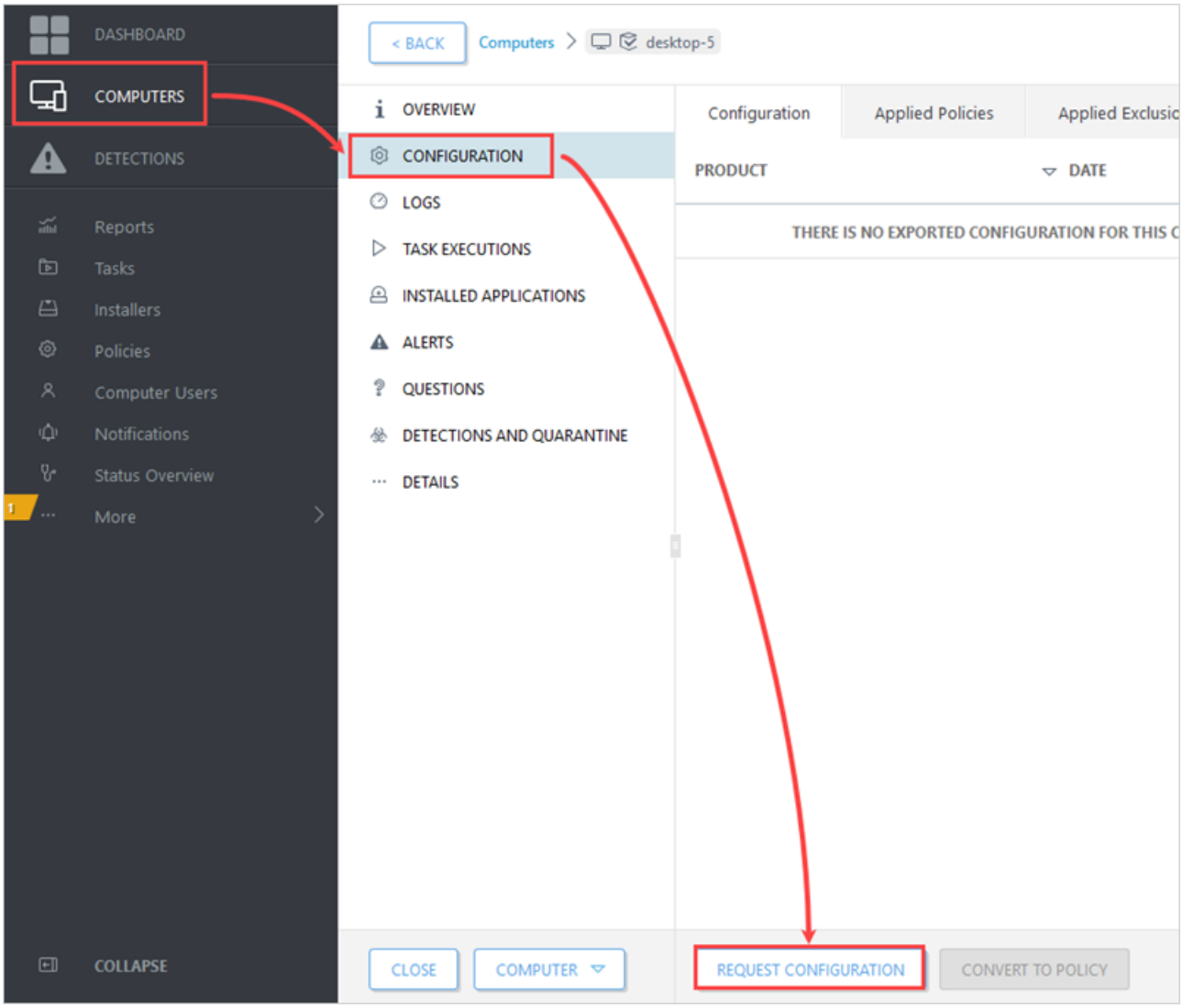
3.Prejdite do sekcie **Podrobnosti** a kliknite na záložku **Produkty a licencie**.

4.Skontrolujte, či je v zozname uvedená licencia ESET LiveGuard Advanced. Ak sa licencia v zozname nenachádza, produkt aktivujte.

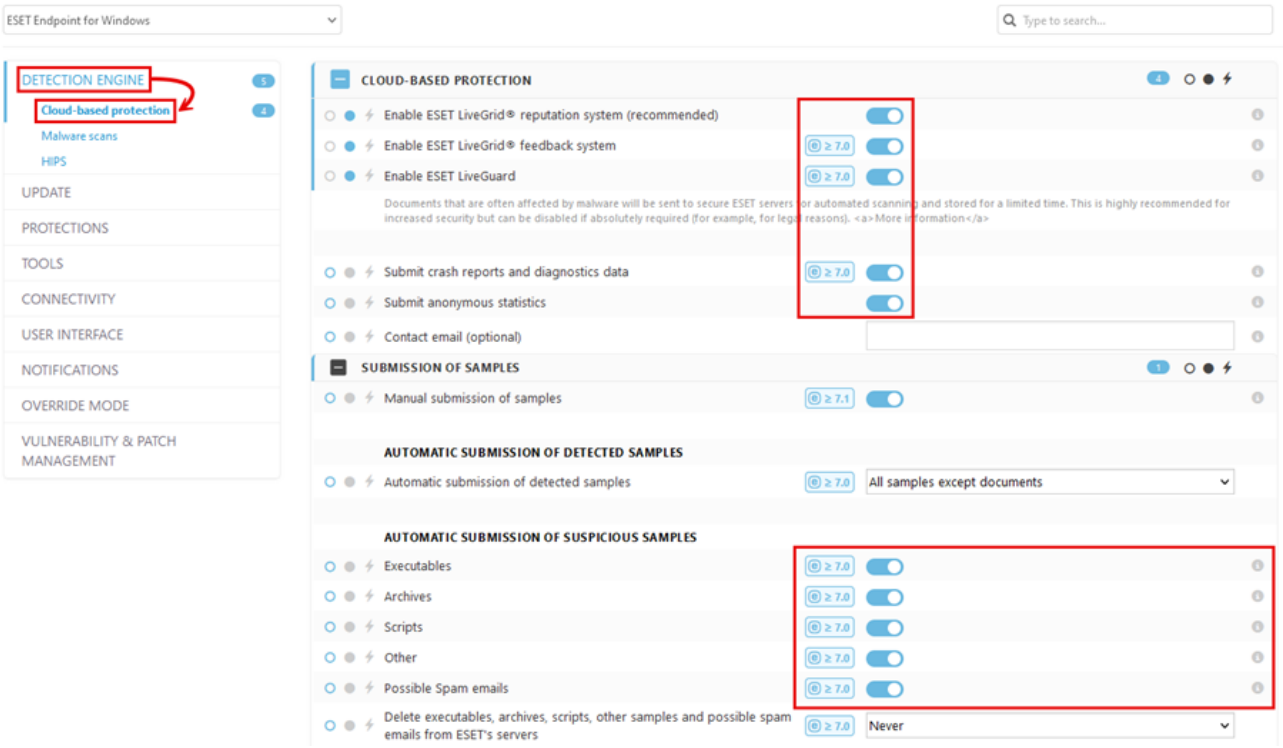


Konfigurácia produktu

1.Prejdite do sekcie **Počítače**, kliknite na počítač, zvoľte možnosť **Zobraziť podrobnosti**, kliknite na **Konfigurácia** a následne na možnosť **Požiadať o konfiguráciu**.



2.Po získaní konfigurácie (kliknite na ikonu pre obnovenie stránky) kliknite na **Bezpečnostný produkt** > **Otvoriť konfiguráciu**, v zobrazených nastaveniach bezpečnostného produktu prejdite do časti **Detekčné jadro** > **Ochrana s podporou cloudu** a skontrolujte, či je zapnutý systém ESET LiveGrid® aj služba ESET LiveGuard Advanced. Pri serverových produktoch prejdite do časti **Počítač** > **Ochrana s podporou cloudu**. V prípade potreby nakonfigurujte politiku, ktorá na danom počítači zapne službu ESET LiveGuard Advanced.



3.Ak sa po získaní vyžiadanej konfigurácie na karte **Konfigurácia** nezobrazí žiadny **Bezpečnostný produkt**, nainštalujte na cieľový počítač podporovaný bezpečnostný produkt ESET.

Riešenie problémov s Apache HTTP Proxy

> **ESET Bridge je odporúčané proxy riešenie pre produkty ESET**
> ESET distribuuje ESET Bridge s ESET PROTECT On-Prem 10.0 (a novšími verziami) ako proxy súčasť, ktorá nahrádza Apache HTTP Proxy. Pozrite si porovnanie ESET Bridge a Apache HTTP Proxy.

Ak na ukladanie komunikácie do vyrovnávacej pamäte používate Apache HTTP Proxy a ESET LiveGuard Advanced nefunguje, môžete zapnúť vytváranie diagnostických protokolov pre Apache HTTP Proxy. Tieto protokoly vám pomôžu zistiť príčinu problému. Protokoly môžete poskytnúť technickej podpore ESET na ďalšiu analýzu.

Proces vytvárania diagnostických protokolov je náročný na výkon. Je potrebné brať na vedomie potenciálnu stratu výkonu. Vytváranie diagnostických protokolov používajte len dočasne. Vytváranie protokolov ponechajte zapnuté iba na nevyhnutné časové obdobie.

Zapnutie vytvárania diagnostických protokolov pre Apache HTTP Proxy

1.Zastavte službu Apache HTTP Proxy pomocou nasledujúceho príkazu: sc stop ApacheHttpProxy

2.Zálohujte si konfiguračný súbor httpd.conf. Zvyčajne sa nachádza v umiestnení C:\Program Files\Apache HTTP Proxy\conf.

3.Upravte konfiguračný súbor podľa pokynov nižšie:

a)Odstráňte komentár (vymažte znak # nachádzajúci sa na začiatku):
`LoadModule log_config_module modules/mod_log_config.dll`

b)Pridajte riadok uvedený nižšie na začiatok sekcie `<IfModule log_config_module>`:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%{cache-
status}e\"" combined-cache
```

c)Označte nasledujúci riadok ako komentár (pridajte znak `#` na začiatok):
`CustomLog "logs/access.log" common`

d)Zmeňte riadok `CacheLockMaxAge 10` na `CacheLockMaxAge 15`

e)Zmeňte riadok `ProxyTimeOut 900` na `ProxyTimeOut 1200`

f)V sekcii `<VirtualHost *:3128>` pod riadok `ServerName r.edtd.eset.com` pridajte nasledujúce riadky:

```
<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>
```

g)Zmeňte riadok:

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
smax=10
```

na:

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 enablereuse=On keepalive=On
ttl=100 max=100 smax=10
```

h)Na koniec súboru pridajte nasledujúce riadky:

```
ErrorLog '|"C:/Program Files/Apache HTTP Proxy/bin/rotatelogs.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/error.log" 1M'

CustomLog '|"C:/Program Files/Apache HTTP Proxy/bin/rotatelogs.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/access.log" 100M' combined-cache
```

4.Uložte súbor httpd.conf a spustite službu Apache HTTP Proxy.
sc start ApacheHttpProxy

Ďalšie kroky

Vytváranie protokolov ponechajte zapnuté iba na nevyhnutné časové obdobie a po vypnutí tejto funkcie vytvorte kópiu protokolov. Protokoly sa nachádzajú v nasledujúcom umiestnení:

```
C:/Program Files/Apache HTTP Proxy/logs/error.log

C:/Program Files/Apache HTTP Proxy/logs/access.log
```

Vypnutie vytvárania diagnostických protokolov:

1.Zastavte službu Apache HTTP Proxy.

2.Obnovte konfiguračný súbor zo zálohy.

3.Spustite službu Apache HTTP Proxy.

Zabezpečenie ESET LiveGuard Advanced

Úvod

Účelom tohto dokumentu je zhrnúť bezpečnostné postupy a bezpečnostné kontroly uplatňované v rámci ESET LiveGuard Advanced. Bezpečnostné postupy a kontroly sú navrhnuté tak, aby chránili dôvernosť, integritu a dostupnosť informácií o zákazníkoch. Upozorňujeme, že bezpečnostné postupy a kontroly sa môžu meniť.

Rozsah

Tento dokument popisuje bezpečnostné postupy a bezpečnostné kontroly týkajúce sa infraštruktúry, organizácie, personálu a prevádzkových procesov spojených s ESET LiveGuard Advanced. Bezpečnostné postupy a kontroly zahŕňajú:

1. Politiky informačnej bezpečnosti
2. Organizácia informačnej bezpečnosti
3. Ľudské zdroje a bezpečnosť
4. Správa aktív
5. Kontrola prístupu
6. Kryptografia
7. Fyzické zabezpečenie a ochrana prostredia
8. Bezpečnosť operácií
9. Bezpečnosť sieťovej komunikácie
10. Akvizícia, vývoj a údržba systému
11. Dodávateľský vzťah
12. Správa incidentov v oblasti informačnej bezpečnosti
13. Aspekty informačnej bezpečnosti v rámci správy kontinuity prevádzky
14. Súlad s požiadavkami

Bezpečnostný koncept

Spoločnosť ESET, spol. s r. o., je držiteľom certifikátu ISO 27001:2013 s integrovaným systémom správy, ktorý pokrýva službu ESET LiveGuard Advanced.

Preto koncept informačnej bezpečnosti používa štandard ISO 27001 na implementáciu bezpečnostnej stratégie viacvrstvovej ochrany pri aplikovaní bezpečnostných kontrol na vrstve siete, operačných systémov, databáz, aplikácií, personálu a operačných procesov. Použité bezpečnostné postupy a bezpečnostné kontroly sa majú navzájom prekrývať a dopĺňať.

Bezpečnostné postupy a kontroly

1. Politiky informačnej bezpečnosti

Spoločnosť ESET uplatňuje politiky informačnej bezpečnosti, ktoré pokrývajú všetky aspekty štandardu ISO 27001 vrátane riadenia informačnej bezpečnosti a bezpečnostných kontrol a postupov. Politiky sa každoročne prehodnocujú a po výrazných zmenách aj aktualizujú, čo vedie k ich kontinuálnej vhodnosti, primeranosti a účinnosti.

Spoločnosť ESET vykonáva každoročnú revíziu týchto politík a interné bezpečnostné kontroly s cieľom zaistiť s nimi súlad. V prípade nedodržiavania politík informačnej bezpečnosti sú zamestnanci spoločnosti ESET vystavení

disciplinárnemu konaniu a dodávatelia zmluvným sankciám alebo až výpoveďou zmluvy.

2. Organizácia informačnej bezpečnosti

Organizácia informačnej bezpečnosti služby ESET LiveGuard Advanced pozostáva z viacerých tímov a jednotlivcov zaoberajúcich sa informačnou bezpečnosťou a oblasťou IT vrátane:

- výkonného manažmentu spoločnosti ESET,
- interných bezpečnostných tímov spoločnosti ESET,
- IT tímov zaoberajúcich sa firemnými aplikáciami,
- ostatných podporných tímov.

Záväzky a úlohy v oblasti informačnej bezpečnosti sa prideľujú v súlade so zavedenými politikami informačnej bezpečnosti. Interné procesy sú identifikované a posudzované z hľadiska rizík vyplývajúcich z neoprávnenej alebo neúmyselnej modifikácie či zneužitia aktív spoločnosti ESET. Pri rizikových alebo citlivých činnostiach v spojení s internými procesmi sa na zmiernenie rizika uplatňuje zásada rozdelenia povinností.

Právny tím spoločnosti ESET je zodpovedný za kontakt so štátnymi orgánmi vrátane slovenských regulačných orgánov v oblasti kybernetickej bezpečnosti a ochrany osobných údajov. Interný bezpečnostný tím spoločnosti ESET je zodpovedný za kontakt so záujmovými skupinami, ako napríklad ISACA. Tím výskumníkov spoločnosti ESET je zodpovedný za komunikáciu s ostatnými spoločnosťami zameranými na bezpečnosť a so širšou komunitou z oblasti kybernetickej bezpečnosti.

Informačná bezpečnosť sa pri riadení projektov zohľadňuje pomocou aplikovaného rámca riadenia projektov od koncepcie až po dokončenie projektu.

Práca na diaľku a práca z domu sú kryté politikou implementovanou na mobilných zariadeniach, ktorá zahŕňa používanie silnej kryptografickej ochrany údajov na mobilných zariadeniach počas prenosu cez nedôveryhodné siete. Bezpečnostné kontroly na mobilných zariadeniach sú navrhnuté tak, aby fungovali nezávisle od interných sietí a interných systémov spoločnosti ESET.

3. Ľudské zdroje a bezpečnosť

Spoločnosť ESET používa štandardné postupy v oblasti ľudských zdrojov vrátane politík určených na dodržiavanie informačnej bezpečnosti. Tieto postupy sa vzťahujú na celý životný cyklus zamestnanca a platia pre všetky tímy, ktoré majú prístup k prostrediu ESET LiveGuard Advanced.

4. Správa aktív

Infraštruktúra ESET LiveGuard Advanced je zahrnutá v inventároch aktív spoločnosti ESET s výhradným vlastníctvom a pravidlami uplatňovanými podľa typu a citlivosti aktív. Spoločnosť ESET má definovanú internú klasifikačnú schému. Všetky údaje a konfigurácie spojené s ESET LiveGuard Advanced sú klasifikované ako dôverné.

5. Kontrola prístupu

Politika kontroly prístupu spoločnosti ESET upravuje každý prístup v rámci ESET LiveGuard Advanced. Kontrola prístupu sa nastavuje na úrovni infraštruktúry, sieťových služieb, operačného systému, databázy a aplikácie. Správa úplného prístupu používateľov na úrovni aplikácie je autonómna.

Prístup k backendu je obmedzený výlučne na oprávnené osoby a roly. Na správu prístupu zamestnancov spoločnosti ESET k infraštruktúre a sieťam služby ESET LiveGuard Advanced sa používajú štandardné procesy ESET pre (de)registráciu používateľov, ich pridávanie alebo odoberanie, správu oprávnení a kontrolu prístupových práv

používateľov.

Na ochranu prístupu ku všetkým údajom týkajúcim sa služby ESET LiveGuard Advanced sa používa silné overovanie.

6. Kryptografia

Silná kryptografia (SSL) slúži na šifrovanie prenášaných údajov s cieľom ochrániť údaje v rámci služby ESET LiveGuard Advanced.

7. Fyzické zabezpečenie a ochrana prostredia

ESET LiveGuard Advanced je cloudová služba. Spoločnosť ESET používa súkromný cloud a cloudovú platformu Microsoft Azure. Fyzické umiestnenie dátového centra s údajmi zo súkromného cloudu je výlučne v Európskej únii (EÚ). Cloud na platforme Microsoft Azure nie je obmedzený len na územie EÚ, používa sa však iba na ukladanie jednosmerných hashov vytvorených z odoslaných súborov bez zahrnutia osobných údajov. Na ochranu používateľských dát počas prenosu slúži silná kryptografia.

8. Bezpečnosť operácií

Služba ESET LiveGuard Advanced je prevádzkovaná automatizovanými prostriedkami na základe prísnych prevádzkových postupov a konfiguračných šablón. Všetky zmeny vrátane zmien konfigurácie a nasadzovania nových balíkov sa pred nasadením do produkcie schvaľujú a testujú v špecializovanom testovacom prostredí. Vývojové, testovacie a produkčné prostredia sú navzájom oddelené. Údaje služby ESET LiveGuard Advanced sú dostupné len v produkčnom prostredí.

Prostredie služby ESET LiveGuard Advanced je sledované pomocou prevádzkového monitorovania s cieľom rýchlo identifikovať problémy a zabezpečiť dostatočnú kapacitu všetkých služieb na úrovni siete a hostiteľa.

Všetky konfiguračné údaje sú uložené v našich pravidelne zálohovaných úložiskách, aby bolo možné automaticky obnoviť konfiguráciu prostredia. Zálohované údaje služby ESET LiveGuard Advanced sa ukladajú lokálne aj externe.

Zálohy sú šifrované a pravidelne testované na obnoviteľnosť v rámci testovania kontinuity prevádzky.

Audit systémov sa vykonáva podľa interných noriem a usmernení. Záznamy a udalosti z infraštruktúry, operačného systému, databázy, aplikačných serverov a bezpečnostných kontrol sa zhromažďujú nepretržite. IT a interné bezpečnostné tímy následne tieto záznamy spracúvajú s cieľom identifikovať prevádzkové a bezpečnostné anomálie a incidenty týkajúce sa informačnej bezpečnosti.

Spoločnosť ESET sa riadi všeobecným technickým procesom správy zraniteľností na riešenie výskytu zraniteľností v infraštruktúre spoločnosti ESET vrátane ESET LiveGuard Advanced a ďalších produktov ESET. Tento proces zahŕňa proaktívnu kontrolu zraniteľností a opakované penetračné testovanie infraštruktúry, produktov a aplikácií.

Spoločnosť ESET má zavedené interné smernice pre bezpečnosť internej infraštruktúry, sietí, operačných systémov, databáz, aplikačných serverov a aplikácií. Ich dodržiavanie sa kontroluje prostredníctvom technického monitorovania súladu a nášho interného bezpečnostného auditu.

9. Bezpečnosť sieťovej komunikácie

Prostredie ESET LiveGuard Advanced je segmentované prostredníctvom natívnej cloudovej segmentácie, pričom prístup k sieti je obmedzený len na nevyhnutné služby v rámci sieťových segmentov. Dostupnosť sieťových služieb je zabezpečená pomocou natívnych cloudových kontrol, ako sú zóny dostupnosti, vyrovnávanie zaťaženia

a redundancia. Nasadia sa špeciálne komponenty na vyrovnávanie zaťaženia a overovanie sieťovej komunikácie medzi koncovými zariadeniami a inštanciou služby ESET LiveGuard Advanced. Sieťová komunikácia je nepretržite monitorovaná z hľadiska prevádzkových a bezpečnostných anomálií. Potenciálne útoky je možné vyriešiť pomocou natívnych cloudových kontrol alebo nasadených bezpečnostných riešení. Všetka sieťová komunikácia je šifrovaná prostredníctvom všeobecne dostupných techník vrátane protokolu IPsec a TLS.

10. Akvizícia, vývoj a údržba systému

Vývoj systémov služby ESET LiveGuard Advanced prebieha v súlade s politikou vývoja bezpečnostného softvéru spoločnosti ESET. Interné bezpečnostné tímy sú súčasťou projektu vývoja služby ESET LiveGuard Advanced od počiatočnej fázy a dohliadajú na všetky aspekty vývoja a údržby. Interný bezpečnostný tím stanovuje a kontroluje plnenie bezpečnostných požiadaviek v rôznych fázach vývoja softvéru. Bezpečnosť všetkých služieb, vrátane tých novo vyvinutých, sa od ich vydania nepretržite testuje.

11. Dodávateľský vzťah

Príslušný dodávateľský vzťah prebieha podľa platných smerníc spoločnosti ESET, ktoré upravujú celú správu vzťahov a zmluvné požiadavky z hľadiska informačnej bezpečnosti a ochrany osobných údajov. Kvalita a bezpečnosť služieb poskytovaných poskytovateľom kritických služieb sa pravidelne vyhodnocuje.

Spoločnosť ESET pre ESET LiveGuard Advanced využíva taktiež právo na prenosnosť údajov s cieľom vyhnúť sa závislosti od poskytovateľa.

12. Správa incidentov v oblasti informačnej bezpečnosti

Správa incidentov v oblasti informačnej bezpečnosti pre službu ESET LiveGuard Advanced je podobná riadeniu ostatných infraštruktúr ESET a opiera sa o definované postupy riešenia incidentov. Úlohy v rámci riešenia incidentov sú zadefinované a rozdelené medzi viaceré tímy z oblasti IT, bezpečnosti, právnych služieb, ľudských zdrojov, vzťahov s verejnosťou a výkonného manažmentu. Priradenie tímu na riešenie incidentu závisí od roztriedenia incidentov interným bezpečnostným tímom. Tento tím zabezpečí koordináciu ostatných tímov, ktoré incident riešia. Interný bezpečnostný tím je tiež zodpovedný za zhromažďovanie dôkazov k incidentu a získaných poznatkov. Vznik incidentu a jeho riešenie sa oznamuje dotknutým stranám. Právny tím spoločnosti ESET je v prípade potreby zodpovedný za nahlásenie incidentu regulačným orgánom v súlade so všeobecným nariadením o ochrane údajov (GDPR) a aktom EÚ o kybernetickej bezpečnosti transponujúcim smernicu o bezpečnosti sietí a informačných systémov (NIS).

13. Aspekty informačnej bezpečnosti v rámci správy kontinuity prevádzky

Kontinuita prevádzky služby ESET LiveGuard Advanced je zakódovaná v robustnej architektúre, ktorá maximalizuje dostupnosť poskytovaných služieb. V prípade úplného zlyhania všetkých redundantných uzlov pre súčasti ESET LiveGuard Advanced alebo službu ESET LiveGuard Advanced je možná kompletná obnova zo zálohovaných a konfiguračných údajov. Proces obnovy sa pravidelne testuje.

14. Súlad s požiadavkami

Dodržiavanie zmluvných požiadaviek a požiadaviek vychádzajúcich z právnych predpisov pre službu ESET LiveGuard Advanced sa pravidelne vyhodnocuje a kontroluje podobne ako iné infraštruktúry a procesy spoločnosti ESET, pričom sa tiež neustále prijímajú nevyhnutné kroky pre zabezpečenie súladu s požiadavkami. Spoločnosť ESET je registrovaná ako poskytovateľ digitálnych služieb v oblasti cloud computingu, kam spadajú viaceré služby spoločnosti ESET vrátane ESET LiveGuard Advanced. Upozorňujeme, že aktivity spoločnosti ESET zamerané na dodržiavanie požiadaviek nemusia nevyhnutne znamenať, že požiadavky zákazníkov v tejto oblasti sú kompletne splnené.

Zásady férového používania

Popis zásad férového používania

Zásady férového používania (politika FUP) stanovujú limit na počet súborov, ktoré môže zákazník poslať na analýzu. Limit na počet súborov sa vzťahuje na vybrané úrovne ochrany ESET LiveGuard Advanced. Viac informácií nájdete v tabuľke uvedenej nižšie.

Limit na počet súborov je: **50 súborov/zariadenie/mesiac**. Počet súborov sa počíta dokopy pre všetky zariadenia. To znamená, že jeden počítač môže na analýzu poslať viac vzoriek, ak ich iný počítač posiela menej.

Napríklad:

- Zákazník s 500 zariadeniami (licenčnými jednotkami) môže každý mesiac odoslať až 25 000 vzoriek.
- Zákazník s 10 000 zariadeniami (licenčnými jednotkami) môže každý mesiac odoslať až 500 000 vzoriek.

Vlastnosti úrovní ESET LiveGuard Advanced

Zoznam dostupných úrovní ESET LiveGuard Advanced a ich vlastnosti nájdete v tabuľke uvedenej nižšie.

Názov produktovej úrovne	Minimálny počet licenčných jednotiek	Dostupné pre ESET PROTECT On-Prem	Dostupné pre ESET PROTECT	Licencia umožňuje vytvorenie ESET PROTECT inštancie	Dostupné v ESET MSP Administrator 2	Limit na počet súborov
ESET LiveGuard Advanced	5	✓	✓	⛔	✓	Nie
ESET PROTECT Complete	5	✓	✓	✓	✓	Áno
ESET PROTECT Mail Plus		✓	✓	✓	✓	Áno
ESET PROTECT Advanced	5	✓	✓	✓	✓	Áno
ESET Dynamic Endpoint Protection	5	✓	⛔	⛔	⛔	Áno
ESET Dynamic Endpoint Protection - Antivirus Level	5	✓	⛔	⛔	⛔	Áno
ESET Targeted Attack Protection	250	✓	⛔	⛔	⛔	Áno

Ako získať licenciu bez limitu na počet súborov?

Pre viac informácií o úrovni ochrany bez limitu na počet odosielaných súborov sa obráťte na svojho lokálneho predajcu ESET.

Ako zistím počet odoslaných súborov?

V konzole na správu si vygenerujte report týkajúci sa počtu odoslaných súborov.

Ako vylúčim z odosielania určité súbory?

Ak prekračujete limit na počet odoslaných súborov, skontrolujte súbory, ktoré sa zo zariadení odosielajú. Následne zvážte vytvorenie vylúčení pre tie priečinky, z ktorých sa odosiela veľké množstvo súborov a ktoré zároveň viete s istotou označiť za bezpečné. Niektoré aplikácie alebo vývojárske nástroje môžu generovať nadmerné množstvo súborov, ktoré nepredstavujú hrozbu a nie je potrebné ich na analýzu posielať. Počet súborov odosielaných na analýzu môžete znížiť tak, že najskôr vyhodnotíte štatistiky odoslaných súborov a potom vytvoríte zodpovedajúce vylúčenia.

Zásady ochrany osobných údajov

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, ako prevádzkovateľ údajov (ďalej len „ESET“ alebo „my“) kladie veľký dôraz na ochranu osobných údajov. Chceme splniť požiadavku transparentnosti, ktorá je právne štandardizovaná vo všeobecnom nariadení EÚ o ochrane údajov (ďalej len „GDPR“). S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať nášho zákazníka (ďalej len „koncový používateľ“ alebo „vy“) ako dotknutú osobu o týchto témach ochrany osobných údajov:

- právny základ spracúvania osobných údajov;
- zdieľanie a dôvernosť údajov;
- bezpečnosť údajov;
- práva, ktoré máte ako dotknutá osoba;
- spracúvanie osobných údajov;
- Kontaktné informácie.

Spracúvanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho webového produktu sa poskytujú za podmienok používania (ďalej len „ToU“), niektoré z nich však môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o spracovaní údajov, ktoré súvisí s poskytovaním našich produktov a služieb. Poskytujeme rôzne služby opísané v podmienky a produktovej dokumentácii. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

- Vzorky, ako napríklad súbory preddefinované a vybraté koncovým používateľom, sa nahrajú do služby spoločnosti ESET na analýzu a výsledky sa vám odošlú späť. Metaúdaje sa zhromažďujú vo vašej lokálne nainštalovanej konzole na správu, ktorá musí byť uvedená ako podporovaná.

- Licenčné informácie, ako napríklad identifikácia licencie, a osobné údaje, ako napríklad meno, priezvisko, adresa a e-mailová adresa, sa vyžadujú na fakturačné účely, overenie pravosti licencie a poskytovanie našich služieb.

• Kontaktné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa vyžadujú na poskytnutie technickej alebo inej podpory spoločnosťou ESET. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a popis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia podpory vás môžeme požiadať o poskytnutie ďalších informácií.

Nemáme v úmysle zhromažďovať vaše údaje mimo tohto rozsahu, niekedy sa tomu však nedá zabrániť. Náhodne zhromaždené údaje môžu byť obsiahnuté v samotnom malvéri (zhromaždené bez vášho vedomia alebo súhlasu) alebo môžu byť súčasťou dokumentov a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

Zdieľanie a dôvernosť údajov

Vaše údaje nezdieľame s tretími stranami. Spoločnosť ESET však pôsobí globálne prostredníctvom pridružených spoločností alebo partnerov v rámci svojej siete predaja, služieb a podpory. Informácie o správe licencií, účtovaní a technickej podpore spracúvané spoločnosťou ESET sa môžu prenášať medzi pridruženými subjektmi alebo partnermi na účely plnenia dohody EULA, ako je napríklad poskytovanie služieb alebo podpory.

Spoločnosť ESET uprednostňuje spracúvanie údajov v krajinách Európskej únie (EÚ). V závislosti od vašej polohy (používanie našich produktov a/alebo služieb mimo EÚ) a/alebo vami vybratej služby však môže byť nevyhnutné preniesť vaše údaje do krajiny mimo EÚ. Využívame napríklad služby tretích strán spojené s cloudovou výpočtovou technikou. V týchto prípadoch si dôkladne vyberáme poskytovateľov služieb a dbáme na ochranu údajov na primeranej úrovni prostredníctvom zmluvných, ale tiež technických a organizačných opatrení. V prípade potreby sa spravidla dohodneme na štandardných zmluvných doložkách EÚ s doplnkovými zmluvnými pravidlami.

Pri niektorých krajinách mimo EÚ, ako je napríklad Spojené kráľovstvo a Švajčiarsko, už EÚ určila porovnateľnú úroveň ochrany údajov. Z dôvodu porovnateľnej úrovne ochrany údajov sa pri prenose údajov do týchto krajín nevyžaduje žiadne osobitné oprávnenie ani dohoda.

Využívame služby tretej strany súvisiace s technológiou cloud computing. Poskytuje ich spoločnosť Microsoft ako poskytovateľom cloudových služieb.

Práva dotknutej osoby

Práva každého koncového používateľa sú dôležité a chceme vás informovať, že všetci koncoví používatelia (z ktorejkoľvek krajiny EÚ aj mimo EÚ) majú práva uvedené nižšie zaručené spoločnosťou ESET. Ak chcete uplatniť svoje práva dotknutej osoby, môžete nás kontaktovať prostredníctvom formulára podpory alebo e-mailom na adrese dpo@eset.sk. Na účely identifikácie vás požiadame o tieto informácie: meno, e-mailovú adresu a (ak sú tieto informácie k dispozícii) licenčný kľúč alebo číslo zákazníka a pridruženú spoločnosť. Neodosielajte nám žiadne iné osobné údaje, napríklad dátum narodenia. Chceme zdôrazniť, že na účely spracovania vašej žiadosti, ako aj na účely identifikácie, budeme spracúvať vaše osobné údaje.

Právo na odvolanie súhlasu. Právo na odvolanie súhlasu sa uplatňuje v prípade spracúvania, ktoré je založené len na súhlase. Ak vaše osobné údaje spracúvame na základe vášho súhlasu, máte právo súhlas kedykoľvek odvolať aj bez uvedenia dôvodu. Odvolanie súhlasu je účinné len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred odvolaním.

Právo namietať. Právo namietať voči spracúvaniu sa uplatňuje v prípade spracúvania na základe oprávneného záujmu spoločnosti ESET alebo tretej strany. Ak vaše osobné údaje spracúvame na ochranu oprávneného záujmu, ako dotknutá osoba máte právo kedykoľvek namietať voči nami uvedenému oprávnenému záujmu a spracúvaniu vašich osobných údajov. Vaša námietka je účinná len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred námietkou. Ak vaše osobné údaje spracúvame na účely priameho marketingu, nie je potrebné

uvádzať dôvody námietky. Platí to aj pre profilovanie, pokiaľ je spojené s takýmto priamym marketingom. Vo všetkých ostatných prípadoch vás požiadame, aby ste nás stručne informovali o svojich sťažnostiach týkajúcich sa oprávneného záujmu spoločnosti ESET spracúvať vaše osobné údaje.

V niektorých prípadoch máme oprávnenie napriek vášmu odvolaniu súhlasu ďalej spracúvať vaše osobné údaje na inom právnom základe, napríklad na účely plnenia zmluvy.

Právo prístupu. Ako dotknutá osoba máte právo kedykoľvek bezplatne získať informácie o svojich údajoch, ktoré uchováva spoločnosť ESET.

Právo na opravu. Ak neúmyselne spracúvame vaše nesprávne osobné údaje, máte právo na ich opravu.

Právo na vymazanie a právo na obmedzenie spracúvania. Ako dotknutá osoba máte právo požiadať o vymazanie alebo obmedzenie spracúvania svojich osobných údajov. Ak napríklad vaše osobné údaje spracúvame s vaším súhlasom, odvoláte ho a neexistuje žiadny iný právny základ, ako je napríklad zmluva, vaše osobné údaje vymažeme okamžite. Vaše osobné údaje tiež budú vymazané, keď už nebudú potrebné na účely, ktoré sú pre ne uvedené, na konci nášho obdobia uchovávania.

Ak vaše osobné údaje používame výhradne na účely priameho marketingu a odvoláte súhlas alebo budete namietať voči existujúcemu oprávnenému záujmu spoločnosti ESET, spracúvanie vašich osobných údajov obmedzíme tak, že pridáme vaše kontaktné údaje do svojho interného blacklistu, aby nedošlo k nevyžiadanému kontaktu. V opačnom prípade sa vaše osobné údaje vymažú.

Upozorňujeme, že sa od nás môže žiadať, aby sme vaše údaje uchovávali až do uplynutia povinností a období uchovávania stanovených zákonodarcom alebo dozornými orgánmi. Povinnosti a obdobia uchovávania tiež môžu vyplývať z právnych predpisov Slovenskej republiky. Po ich uplynutí sa príslušné údaje vymažú zvyčajným spôsobom.

Právo na prenosnosť údajov. Ako dotknutej osobe vám radi poskytneme osobné údaje spracúvané spoločnosťou ESET vo formáte XLS.

Právo podať sťažnosť. Ako dotknutá osoba máte právo kedykoľvek podať sťažnosť dozornému orgánu. Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. Príslušným dozorným orgánom na ochranu údajov je Úrad na ochranu osobných údajov Slovenskej republiky so sídlom na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Veríme, že všetky informácie, ktoré spracúvame, sú cenné a potrebné z hľadiska nášho legitímneho záujmu, ktorým je poskytovanie služieb a produktov zákazníkom.

Kontaktné informácie

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk

Podmienky používania

S účinnosťou od 31. januára 2024.

Tieto podmienky používania (ďalej iba „podmienky“) predstavujú špeciálnu zmluvu medzi spoločnosťou ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanou v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532 (ďalej len „ESET“ alebo „poskytovateľ“) a vami, fyzickou alebo právnickou osobou (ďalej len „vy“ alebo „používateľ“ alebo formulácie vyjadrené v druhej osobe množného čísla), ktorá používa online službu ESET LiveGuard Advanced vlastnenú, riadenú a poskytovanú spoločnosťou ESET (ďalej iba „ESET LiveGuard Advanced“). Ak používate ESET LiveGuard Advanced v mene organizácie, potom s podmienkami súhlasíte v mene danej organizácie a zaručujete sa, že máte právomoc zaviazať ju týmito podmienkami. Označenie „používateľ“ a „vy“ alebo formulácie vyjadrené v druhej osobe množného čísla sa v takomto prípade budú vzťahovať na danú organizáciu. Pozorne si tieto podmienky prečítajte, vzťahujú sa aj na služby poskytované spoločnosťou ESET prostredníctvom služby ESET LiveGuard Advanced alebo vo vzťahu k nej. Špecifické podmienky používania jednotlivých služieb mimo týchto podmienok sú uvedené pri každej službe a ich prijatie je súčasťou procesu aktivácie služby.

Bezpečnosť a ochrana údajov

ESET LiveGuard Advanced poskytuje prístup k službám poskytovaným spoločnosťou ESET. Na zaregistrovanie a používanie služby ESET LiveGuard Advanced a na účely poskytovania a údržby služieb ESET LiveGuard Advanced sa vyžaduje plné meno používateľa, názov spoločnosti, krajina, platná e-mailová adresa, telefónne číslo, licenčné a štatistické údaje. Týmto súhlasíte so zhromažďovaním údajov a ich prenosom na servery poskytovateľa alebo jeho partnerov na účely zabezpečenia funkčnosti a overenia oprávnenia používať softvér a ochranu práv poskytovateľa. Po uzavretí dohody o týchto podmienkach získajú poskytovateľ alebo jeho partneri oprávnenie prenášať, spracovávať a uchovávať dôležité údaje, ktoré umožnia vašu identifikáciu, na účely poskytovania podpory a plnenia týchto podmienok. Máte oprávnenie používať ESET LiveGuard Advanced výhradne na účely určené v týchto podmienkach, individuálnych podmienkach poskytovania služby a dokumentácii.

Na poskytovanie služby ESET LiveGuard Advanced sa vyžaduje odosielanie súborov (ďalej iba „údaje“). Údaje poskytujete spoločnosti ESET výhradne na účely poskytovania služby ESET LiveGuard Advanced. Údaje sa budú spracovávať a ukladať v súlade s politikami a postupmi zabezpečenia spoločnosti ESET a tiež v súlade so zásadami ochrany osobných údajov.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov.

Zásady férového používania

Máte povinnosť dodržiavať technické obmedzenia uvedené v dokumentácii. Súhlasíte s tým, že účet a jeho funkcie budete používať výlučne spôsobom, ktorý neobmedzí možnosti iných používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým používateľom tak, aby umožnil využívanie týchto služieb čo najväčšiemu počtu používateľov. Obmedzenie rozsahu služieb môže tiež znamenať úplné ukončenie možnosti používať všetky funkcie účtu a odstránenie údajov a informácií.

Podrobné informácie o férovom používaní a politike FUP nájdete v zásadách férového používania.

Softvér

Spoločnosť ESET alebo jej jednotliví dodávatelia vlastnia alebo si môžu uplatňovať autorské práva k softvéru na webových lokalitách účtu (ďalej iba „softvér“). Softvér možno používať iba v súlade s licenčnou zmluvou koncového používateľa (ďalej iba „EULA“). EULA sa dodáva spolu so softvérom alebo je jeho súčasťou. Softvér dodávaný so zmluvou EULA nemožno nainštalovať bez toho, aby používateľ súhlasil so zmluvou EULA. Ďalšie informácie týkajúce sa licencovania, autorských práv, dokumentácie a ochranných známok sú uvedené v dokumente obsahujúcom právne informácie.

Obmedzenia

Účet nesmiete kopírovať, šíriť, oddeľovať jeho časti ani vytvárať od účtu odvodené diela. Pri používaní účtu máte povinnosť dodržiavať tieto obmedzenia:

(a) Účet nesmiete používať, upravovať, prekladať, reprodukovať ani prevádzať práva na používanie účtu alebo jeho častí inak, než je výslovne uvedené v týchto podmienkach.

(b) Účet nesmiete predať, sublicencovať, prenajať ani prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

(c) Účet nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu ani sa iným spôsobom pokúsiť získať zdrojový kód účtu s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

(d) Súhlasíte s tým, že budete účet používať iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom účet používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

Vyhlásenia

AKO POUŽÍVATEĽ TÝMTO UZNÁVATE, ŽE ÚČET, AKO AJ SLUŽBY, SÚ POSKYTOVANÉ „AKO STOJA A LEŽIA“, BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ ALEBO PRIDRUŽENÉ SPOLOČNOSTI ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ ŽIADNE VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY VRÁTANE, NIE VŠAK VÝHRADNE, ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE ÚČET ALEBO SLUŽBY NEPORUŠUJÚ ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. POSKYTOVATEĽ ANI ŽIADNA ĎALŠIA STRANA NEZARUČUJÚ, ŽE ÚČET ALEBO SLUŽBY BUDÚ VYHOVOVAŤ VAŠIM POŽIADAVKÁM ALEBO ŽE PREVÁDZKA ÚČTU ALEBO SLUŽIEB BUDE NEPRERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER A POUŽÍVANIE ÚČTU A SLUŽIEB NA DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV, KTORÉ S ÚČTOM DOSIAHNETE.

Tieto podmienky nezakladajú na strane poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne tu uvedených žiadne iné záväzky.

Obmedzenie zodpovednosti

V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO DODÁVATELIA V ŽIADNOM PRÍPADE ZODPOVEDAŤ ZA ŽIADNY UŠLÝ ZISK, PRÍJEM, PREDAJ ALEBO ZA ŽIADNU STRATU ÚDAJOV, ANI ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA PORANENIA OSÔB, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ ANI ZA ŽIADNE ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ,

ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ ÚČET, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ, JEHO DODÁVATELIA ALEBO PRIDRUŽENÉ SPOLOČNOSTI BOLI UPOZORNENÍ NA MOŽNOSŤ VZNIKU TAKÝCHTO ŠKÔD. KEĎŽE NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV, DODÁVATEĽOV ALEBO PRIDRUŽENÝCH SPOLOČNOSTÍ OBMEDZENÁ DO VÝŠKY SUMY, KTORÚ STE ZAPLATILI ZA PRÍSLUŠNÚ SLUŽBU ALEBO ÚČET.

Súlad s kontrolou obchodu

(a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej majú byť naplnené tieto Podmienky alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej majú byť naplnené tieto Podmienky alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje (právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

(b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia sekcie (a) tejto doložky Súlad s kontrolou obchodu týchto Podmienok; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z týchto Podmienok by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

(c) Žiadna časť týchto Podmienok nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

Rozhodujúce právo a jazyk

Tieto podmienky sa riadia zákonmi Slovenskej republiky a musia byť vykladané v súlade s nimi. Koncový používateľ a poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho práva a Dohovoru OSN o zmluvách pri

medzinárodnej kúpe tovarov sa nepoužijú. Ak ste spotrebiteľom s obvyklým pobytom v krajine EÚ, máte tiež k dispozícii ďalšiu ochranu, ktorú vám poskytujú povinné ustanovenia právnych predpisov platných v krajine vášho pobytu.

Výslovne súhlasíte s tým, že o akýchkoľvek nárokoch voči poskytovateľovi alebo spory s poskytovateľom týkajúce sa akýmkoľvek spôsobom používania softvéru, účtu alebo služieb alebo vyplývajúce z týchto podmienok alebo osobitných podmienok (ak sa uplatňujú) bude výhradne rozhodovať Okresný súd Bratislava I., Slovensko a tiež v spojení s akýmikoľvek takýmito nárokmi alebo spormi výslovne súhlasíte s vykonávaním osobnej jurisdikcie na Okresnom súde Bratislava I. Ak ste spotrebiteľom s obvyklým pobytom v krajine EÚ, môžete tiež uplatniť nárok na svoje práva spotrebiteľa, a to na mieste výhradnej jurisdikcie alebo v krajine EÚ, v ktorej žijete. Okrem toho môžete využiť platformu na riešenie sporov online, ku ktorej môžete získať prístup tu: https://ec.europa.eu/consumers/odr/. Žiadame vás však, aby ste pred uplatnením akéhokoľvek nároku úradnou cestou kontaktovali najskôr nás.

V prípade akýchkoľvek rozporov medzi jazykovými verziami týchto podmienok vždy platí verzia v angličtine dostupná tu.

Všeobecné ustanovenia

Spoločnosť ESET si vyhradzuje právo kedykoľvek zmeniť tieto podmienky a dokumentáciu alebo ich časť aktualizovaním príslušného dokumentu, aby odrážal zmeny zákona alebo účtu. O každej zmene týchto podmienok vás informujeme prostredníctvom účtu. Ak so zmenami podmienok nebudete súhlasiť, môžete svoj účet zrušiť. Ak po upozornení na zmeny účet nezrušíte, tak až do zrušenia účtu vás zaväzujú všetky podmienky používania, ich dodatky alebo zmeny. Mali by ste pravidelne navštevovať túto stránku a prejsť si aktuálne podmienky používania vzťahujúce sa na používanie účtu.

Oznámenia

Všetky oznámenia musia byť doručené na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Príloha č. 1

ESET Management Agent – Licenčná dohoda s koncovým používateľom

Príloha č. 2

Dohoda o spracúvaní údajov

Príloha č. 3

Štandardné zmluvné doložky

ESET Management Agent – Licenčná dohoda s koncovým používateľom

S účinnosťou od 19. októbra 2021.

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU**

VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532 („ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou („Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody a prijímate Zásady ochrany osobných údajov. Ak s niektorými podmienkami a požiadavkami tejto Dohody a/alebo Zásad ochrany osobných údajov nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru („Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto zmluvy a dodržiavate všetky jej zmluvné podmienky, poskytovateľ vám udeľuje nasledujúce práva („licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na

pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií.** Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent („MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač. Jednu licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má Koncový používateľ právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Home/Business Edition.** Verzia Softvéru Home Edition je určená výlučne na domáce a rodinné používanie v súkromných alebo nekomerčných prostrediach. Na použitie v komerčnom prostredí, ako aj na použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie.** Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér.** Softvér klasifikovaný ako OEM je obmedzený len na počítač, s ktorým bol získaný. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér.** Softvér označený ako „Nepredajný“, „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie.** Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zrušenia licencie musíte softvér a všetky záložné kópie okamžite odstrániť, zničiť alebo na svoje náklady vrátiť spoločnosti ESET alebo na miesto, kde ste softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4. **Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a príslušné zhromažďovanie údajov je nevyhnutné na fungovanie Softvéru a na aktualizáciu a inováciu Softvéru. Poskytovateľ môže vydávať aktualizácie alebo inovácie Softvéru („Update“), nie je však povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Pre poskytovanie aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

Na poskytovanie akýchkoľvek aktualizácií sa môžu vzťahovať Zásady Ukončenia životného cyklu („Zásady

Ukončenia životného cyklu“), ktoré sú k dispozícii na adrese https://go.eset.com/eol_business. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebudú sa poskytovať žiadne aktualizácie.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s

podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Dohody budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, tým nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Dohody.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Na vaše právo používať Softvér a ktorúkoľvek z jeho funkcií sa môžu vzťahovať Zásady Ukončenia životného cyklu. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, vaše právo používať Softvér zanikne. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY, ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY

VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ INŠTALÁCIOU, POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebude sa poskytovať žiadna technická podpora. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti Softvéru.** Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo). Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**.

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu

alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje.

(právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez toho, aby bolo dotknuté právo spoločnosti ESET oznámiť vám akékoľvek zmeny tejto Dohody, Zásad ochrany osobných údajov, Zásad Ukončenia životného cyklu a Dokumentácie v súlade s článkom 22 Dohody. Spoločnosť ESET vám môže posielať e-maily, oznámenia v aplikácii prostredníctvom Softvéru alebo uverejniť komunikáciu na svojej webovej lokalite. Súhlasíte s tým, že budete od spoločnosti ESET dostávať právnu komunikáciu v elektronickej forme vrátane akejkoľvek komunikácie o zmene podmienok, osobitných podmienok alebo zásad ochrany osobných údajov, akýchkoľvek návrhov/prijatí zmluvy alebo pozvánok, upozornení alebo inej právnej komunikácie. Takáto elektronická komunikácia sa bude považovať za prijatú v písomnej forme, pokiaľ príslušné právne predpisy osobitne nevyžadujú inú formu komunikácie.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky. Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. Táto Dohoda bola vyhotovená v angličtine. V prípade, že je z praktických dôvodov alebo na akýkoľvek iný účel vypracovaný akýkoľvek preklad Dohody, alebo v prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí verzia v angličtine.

Spoločnosť ESET si vyhradzuje právo kedykoľvek vykonať zmeny v Softvéri, ako aj kedykoľvek upraviť podmienky

tejto Dohody, jej prílohy, dodatky, Zásady ochrany osobných údajov, Zásady Ukončenia životného cyklu a dokumentáciu, prípadne ich ľubovoľnú časť tak, že aktualizuje príslušný dokument: (i) aby zohľadňoval zmeny v Softvéri alebo v tom, ako spoločnosť ESET vykonáva podnikateľskú činnosť, (ii) z právnych, regulačných alebo bezpečnostných dôvodov alebo (iii) na zabránenie zneužitiu alebo ublíženiu. O každej úprave Dohody vás informujeme prostredníctvom e-mailu, oznámenia v aplikácii alebo iným spôsobom elektronickej komunikácie. Ak s navrhovanými zmenami Dohody nebudete súhlasiť, môžete ju v súlade s článkom 10 ukončiť do 30 dní od prijatia oznámenia o zmene. Ak Dohodu v tejto časovej lehote neukončíte, navrhované zmeny sa budú považovať za prijaté a nadobudnú voči vám účinnosť k dátumu prijatia oznámenia o zmene.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

DODATOK K DOHODE

Komunikácia a správa údajov. Na komunikáciu a správu údajov sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

Softvér obsahuje funkciu, ktorá umožňuje prenos informácií medzi Počítačom a softvérom na vzdialenú správu. Informácie, ktoré sa prenášajú, obsahujú údaje správy, napríklad informácie o hardvéri a softvéri spravovaného počítača, a pokyny na správu od softvéru na vzdialenú správu. Iný obsah údajov prenášaných z Počítača závisí od nastavení softvéru nainštalovaného v Počítači. Obsah pokynov od softvéru na správu závisí od nastavení softvéru na vzdialenú správu.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Dohoda o spracúvaní údajov

V súlade s požiadavkami nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), poskytovateľ (ďalej len „sprostredkovateľ“) a vy (ďalej len „prevádzkovateľ“) vstupujete do zmluvného vzťahu týkajúceho sa spracúvania údajov s cieľom vymedziť podmienky pre spracúvanie osobných údajov a spôsob ich ochrany, ako aj stanoviť ďalšie práva a povinnosti obidvoch strán pri spracúvaní osobných údajov dotknutých osôb v mene prevádzkovateľa v priebehu vykonávania predmetu týchto podmienok ako hlavnej zmluvy.

1. **Spracúvanie osobných údajov.** Služby poskytované v súlade s týmito podmienkami zahŕňajú spracúvanie informácií týkajúcich sa identifikovanej alebo identifikovateľnej fyzickej osoby, ktoré sú uvedené v zásadách ochrany osobných údajov (ďalej len „osobné údaje“).

2. **Poverenie.** Prevádzkovateľ poveruje sprostredkovateľa spracúvaním osobných údajov, pričom

(i) „účel spracúvania“ znamená poskytovanie služieb v súlade s týmito podmienkami, sprostredkovateľ môže spracúvať osobné údaje v mene prevádzkovateľa len v súvislosti s poskytovaním služieb vyžiadaných prevádzkovateľom, všetky informácie zhromaždené na dodatočné účely sa spracúvajú mimo zmluvného vzťahu medzi prevádzkovateľom a sprostredkovateľom,

(ii) doba spracúvania znamená obdobie od začatia spolupráce podľa týchto podmienok do ukončenia služieb,

(iii) rozsah a kategórie osobných údajov. Tieto služby sú určené na spracúvanie iba všeobecných osobných údajov. Prevádzkovateľ však nesie výhradnú zodpovednosť za určenie rozsahu osobných údajov,

(iv) dotknutá osoba je fyzická osoba ako oprávnený používateľ zariadení prevádzkovateľa,

(v) spracovateľské činnosti predstavujú všetky operácie potrebné na spracúvanie,

(vi) „zdokumentované pokyny" znamenajú pokyny uvedené v týchto podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe. Prevádzkovateľ je zodpovedný za právnu prípustnosť spracúvania osobných údajov sprostredkovateľom s ohľadom na príslušné platné ustanovenia zákona o ochrane osobných údajov.

3. **Povinnosti sprostredkovateľa.** Sprostredkovateľ je povinný:

(i) spracúvať osobné údaje len na základe zdokumentovaných pokynov a na účely definované v podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe,

(ii) poučiť osoby oprávnené spracúvať osobné údaje (ďalej len „oprávnené osoby") o ich právach a povinnostiach podľa všeobecného nariadenia o ochrane údajov, o ich zodpovednosti v prípade porušenia a zabezpečiť, aby sa oprávnené osoby zaviazali zachovávať dôvernosť informácií a dodržiavali zdokumentované pokyny,

(iii) implementovať a dodržiavať opatrenia opísané v podmienkach, ich prílohách, zásadách ochrany osobných údajov a v dokumentácii k službe,

(iv) pomáhať prevádzkovateľovi reagovať na žiadosti dotknutých osôb súvisiace s ich právami. Sprostredkovateľ nesmie opraviť, odstrániť ani obmedziť spracúvanie osobných údajov bez pokynu prevádzkovateľa. Všetky žiadosti dotknutej osoby týkajúce sa osobných údajov spracúvaných v mene prevádzkovateľa sa bezodkladne prepošlú prevádzkovateľovi,

(v) pomáhať prevádzkovateľovi s oznámením porušenia ochrany osobných údajov dozornému orgánu a dotknutej osobe. Sprostredkovateľ oznámi prevádzkovateľovi každé porušenie spracúvania osobných údajov alebo bezpečnosti osobných údajov okamžite po jeho zistení. Sprostredkovateľ bude v primeranom rozsahu spolupracovať pri vyšetrovaní a náprave takéhoto porušenia a prijme primerané opatrenia, aby obmedzil ďalšie negatívne dôsledky.

(vi) podľa rozhodnutia prevádzkovateľa vymazať alebo vrátiť všetky osobné údaje prevádzkovateľovi po skončení doby spracúvania. Prevádzkovateľ sa zaväzuje informovať sprostredkovateľa o svojom rozhodnutí do desiatich (10) dní po skončení doby spracúvania. Toto ustanovenie nemá vplyv na právo sprostredkovateľa uchovávať osobné údaje v nevyhnutnom rozsahu na účely archivácie vo verejnom záujme, na účely vedeckého výskumu, na štatistické účely alebo na účely preukazovania, uplatňovania alebo ochrany právnych nárokov,

(vii) viesť aktuálny register všetkých kategórií spracovateľských činností, ktoré vykonal v mene prevádzkovateľa,

(viii) sprístupniť prevádzkovateľovi všetky informácie potrebné na preukázanie súladu v rámci podmienok, ich príloh, zásad ochrany osobných údajov a dokumentácie k službe. V prípade auditu alebo kontroly spracúvania osobných údajov zo strany prevádzkovateľa je prevádzkovateľ povinný písomne informovať sprostredkovateľa najmenej tridsať (30) dní pred plánovaným auditom alebo kontrolou.

4. **Zapojenie ďalšieho sprostredkovateľa.** Sprostredkovateľ je oprávnený zapojiť ďalšieho sprostredkovateľa na vykonávanie špecifických spracovateľských činností, ako je napríklad poskytovanie cloudového úložiska a infraštruktúry pre službu, v súlade s podmienkami, ich prílohami, zásadami ochrany osobných údajov a dokumentáciou k službe. V súčasnosti poskytuje cloudové úložisko a infraštruktúru spoločnosť Microsoft ako súčasť cloudovej služby Azure. Aj v tomto prípade zostane sprostredkovateľ jediným kontaktným miestom a stranou zodpovednou za zaistenie súladu s požiadavkami. Sprostredkovateľ sa týmto zaväzuje informovať Prevádzkovateľa o každom pridaní alebo nahradení iného sprostredkovateľa, čím mu umožní voči takejto zmene namietať.

5. **Územná pôsobnosť.** Sprostredkovateľ vynaloží maximálne úsilie s cieľom zabezpečiť, aby sa spracúvanie údajov uskutočňovalo v Európskom hospodárskom priestore alebo v krajine označenej Európskou komisiou za bezpečnú, a to na základe rozhodnutia Prevádzkovateľa. Štandardné zmluvné doložky sa uplatňujú v prípade prenosov údajov a spracúvania prebiehajúceho mimo Európskeho hospodárskeho priestoru alebo krajiny označenej Európskou komisiou za bezpečnú na žiadosť prevádzkovateľa.

6. **Bezpečnosť.** Sprostredkovateľ je držiteľom certifikátu ISO 27001:2013 a používa štandard ISO 27001 pre implementáciu bezpečnostnej stratégie viacvrstvovej ochrany pri aplikovaní bezpečnostných kontrol na vrstve siete, operačných systémov, databáz, aplikácií, personálu a operačných procesov. Dodržiavanie zmluvných požiadaviek a požiadaviek vychádzajúcich z právnych predpisov sa pravidelne vyhodnocuje a prehodnocuje podobne ako iné infraštruktúry a operácie sprostredkovateľa, pričom sa tiež neustále prijímajú nevyhnutné kroky na zabezpečenie súladu s požiadavkami. Sprostredkovateľ zaisťuje bezpečnosť údajov pomocou systému riadenia bezpečnosti informácií (ISMS) založenom na norme ISO 27001. Bezpečnostná dokumentácia obsahuje najmä dokumenty týkajúce sa politík pre bezpečnosť informácií, fyzickú bezpečnosť, zabezpečenie zariadení, správu incidentov, riešenie únikov údajov a bezpečnostných incidentov atď.

7. **Technické a organizačné opatrenia**. Sprostredkovateľ chráni osobné údaje pred náhodným a nezákonným poškodením a zničením, náhodnou stratou, zmenou, neoprávneným prístupom a zverejnením. Na tento účel sprostredkovateľ prijme primerané technické a organizačné opatrenia zodpovedajúce spôsobu spracúvania a riziku, ktoré spracúvanie predstavuje pre práva dotknutých osôb v súlade s požiadavkami všeobecného nariadenia o ochrane údajov. Detailný opis technických a organizačných opatrení je uvedený v bezpečnostnej politike.

8. **Kontaktné informácie sprostredkovateľa.** Všetky oznámenia, žiadosti, požiadavky a ďalšia komunikácia týkajúca sa ochrany osobných údajov sa adresujú spoločnosti ESET, spol. s.r.o., zodpovednej osobe: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Štandardné zmluvné doložky

ODDIEL I

Doložka 1 Účel a rozsah pôsobnosti

Účelom týchto štandardných zmluvných doložiek je zabezpečiť súlad s požiadavkami nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27.apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov) (1) pri prenose osobných údajov do tretej krajiny.

b) Zmluvné strany:

fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný orgán (ďalej len „subjekt“), ktoré uskutočňujú prenos osobných údajov, ako sa uvádza v prílohe I časti A (ďalej len „vývozca údajov“), a

subjekt v tretej krajine, ktorý prijíma osobné údaje od vývozcu údajov, a to priamo alebo nepriamo prostredníctvom iného subjektu, ktorý je tiež zmluvnou stranou týchto doložiek, ako sa uvádza v prílohe I časti A (ďalej len „dovozca údajov“),

sa dohodli na týchto štandardných zmluvných doložkách (ďalej len „doložky“).

Tieto doložky sa uplatňujú na prenos osobných údajov podľa prílohy I časti B.

Dodatok k týmto doložkám obsahujúci prílohy, na ktoré sa v týchto doložkách odkazuje, tvorí neoddeliteľnú súčasť týchto doložiek.

Doložka 2 Účinok a nemennosť doložiek

a) V týchto doložkách sa stanovujú primerané záruky vrátane vymáhateľných práv dotknutých osôb a účinných právnych prostriedkov nápravy podľa článku 46 ods.1 a článku 46 ods. 2 písm. c) nariadenia (EÚ) 2016/679, a pokiaľ ide o prenosy údajov od prevádzkovateľov sprostredkovateľom a/alebo od sprostredkovateľov sprostredkovateľom, štandardné zmluvné doložky podľa článku 28 ods. 7 nariadenia (EÚ) 2016/679, pokiaľ nie sú zmenené, okrem prípadu, keď sa vyberá vhodný modul/moduly, prípadne keď sa dopĺňajú alebo aktualizujú informácie v dodatku. To zmluvným stranám nebráni v tom, aby zahrnuli štandardné zmluvné doložky stanovené v týchto doložkách do širšej zmluvy a/alebo doplnili iné doložky či dodatočné záruky za predpokladu, že nie sú v priamom ani nepriamom rozpore s týmito doložkami ani neobmedzujú základné práva alebo slobody dotknutých osôb.

b) Týmito doložkami nie sú dotknuté povinnosti, ktoré sa vzťahujú na vývozcu údajov na základe nariadenia (EÚ) 2016/679.

Doložka 3 Oprávnenosť tretích strán

a) Dotknuté osoby sa môžu týchto doložiek dovolávať a vymáhať ich ako oprávnené tretie strany vo vzťahu k vývozcovi údajov a/alebo dovozcovi údajov s týmito výnimkami:

i) doložka 1, doložka 2, doložka 3, doložka 6, doložka 7;

ii) doložka 8 – modul č. 1: doložka 8 – modul č. 1: doložka 8.5 písm. e) a doložka 8.9 písm. b); modul č. 2: doložka 8.1 písm. b), doložka 8.9 písm. a), c), d) a e); modul č. 3: doložka 8.1 písm. a), c) a d), ako aj doložka 8.9 písm. a), c), d), e), f) a g); modul č. 4: doložka 8.1 písm. b) a doložka 8.3 písm. b);

iii) doložka 9 – modul č. 2: doložka 9 písm. a), c), d) a e); modul č. 3: doložka 9 písm. a), c), d) a e);

iv) doložka 12 – modul č. 1: doložka 12 písm. a) a d); moduly č. 2 a 3: doložka 12 písm. a), d) a f);

v) doložka 13;

vi) doložka 15.1 písm. c), d) a e);

vii) doložka 16 písm. e);

viii) doložka 18 – moduly č. 1, 2 a 3: doložka 18 písm. a) a b); modul č. 4: doložka 18.

b) Písmenom a) nie sú dotknuté práva dotknutých osôb podľa nariadenia (EÚ) 2016/679.

Doložka 4 Výklad

a) Ak sa v týchto doložkách používajú pojmy vymedzené v nariadení (EÚ) 2016/679, tieto pojmy majú rovnaký význam ako v uvedenom nariadení.

b) Tieto doložky sa vykladajú v zmysle ustanovení nariadenia (EÚ) 2016/679.

c) Tieto doložky sa nesmú vykladať spôsobom, ktorý je v rozpore správami a povinnosťami stanovenými v nariadení (EÚ) 2016/679.

Doložka 5 Hierarchia

V prípade rozporu medzi týmito doložkami a ustanoveniami súvisiacich dohôd medzi zmluvnými stranami, ktoré existovali v čase, keď sa dohodli tieto doložky, alebo ktoré sa uzavreli neskôr, majú prednosť tieto doložky.

Doložka 6 Opis prenosu

Informácie o prenose a najmä kategórie prenášaných osobných údajov a účel, na ktorý sa prenášajú, sú uvedené v prílohe I časti B.

Doložka 7 – nepovinná Doložka o pristúpení

a) Subjekt, ktorý nie je zmluvnou stranou týchto doložiek, môže so súhlasom zmluvných strán kedykoľvek pristúpiť k týmto doložkám ako vývozca alebo dovozca údajov vyplnením dodatku a podpísaním prílohy I časti A.

b) Po vyplnení dodatku a podpísaní prílohy I časti A sa pristupujúci subjekt stane zmluvnou stranou týchto doložiek a bude mať práva a povinnosti vývozcu alebo dovozcu údajov v súlade s označením v prílohe I časti A.

c) Pristupujúci subjekt nemá žiadne práva ani povinnosti vyplývajúce z týchto doložiek, pokiaľ ide o obdobie pred tým, ako sa stal zmluvnou stranou.

ODDIEL II – POVINNOSTI ZMLUVNÝCH STRÁN

Doložka 8 Záruky v oblasti ochrany údajov

Vývozca údajov vyhlasuje, že vynaložil primerané úsilie, na základe ktorého možno konštatovať, že dovozca údajov je vďaka prijatiu vhodných technických a organizačných opatrení schopný plniť svoje povinnosti podľa týchto doložiek.

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

8.1. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B. Osobné údaje môže spracúvať na iný účel len vtedy, ak:

i) získal predchádzajúci súhlas dotknutej osoby;

ii) je to nevyhnutné na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iii) je to nevyhnutné v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

8.2. Transparentnosť

a) S cieľom umožniť dotknutým osobám účinne uplatňovať práva podľa doložky 10 ich dovozca údajov priamo alebo prostredníctvom vývozcu údajov informuje:

i) o svojej totožnosti a kontaktných údajoch;

ii) o kategóriách spracúvaných osobných údajov;

iii) o práve získať kópiu týchto doložiek

iv) v prípade úmyslu uskutočniť následný prenos osobných údajov akejkoľvek tretej strane o príjemcovi alebo kategóriách príjemcov (podľa potreby s cieľom poskytnúť zmysluplné informácie), účele a dôvode tohto následného prenosu podľa doložky 8.7.

b) Písmeno a) sa neuplatňuje, ak po prvé dotknutá osoba už má informácie vrátane prípadu, keď takéto informácie už poskytol vývozca údajov, alebo ak sa po druhé poskytnutie informácií ukáže ako nemožné alebo by si vyžadovalo neprimerané úsilie dovozcu údajov. V druhom prípade dovozca údajov v čo najväčšej možnej miere sprístupní tieto informácie verejnosti.

c) Zmluvné strany sprístupnia dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane nimi vyplneného dodatku. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môžu zmluvné strany pred poskytnutím kópie dodatku odstrániť časť jeho textu, pričom však poskytnú zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií.

d) Písmenami a) až c) nie sú dotknuté povinnosti vývozcu údajov podľa článkov 13 a14 nariadenia (EÚ) 2016/679.

8.3. Správnosť a minimalizácia údajov

a) Každá zmluvná strana zabezpečí, aby osobné údaje boli správne a v prípade potreby aktualizované. Dovozca údajov prijme všetky primerané opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov spracúvania, bezodkladne vymazali alebo opravili.

b) Ak jedna zo zmluvných strán zistí, že osobné údaje, ktoré preniesla alebo získala, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje druhú zmluvnú stranu.

c) Dovozca údajov zabezpečí, aby osobné údaje boli primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely spracúvania.

8.4. Minimalizácia uchovávania

Dovozca údajov nesmie uchovávať osobné údaje dlhšie než je nevyhnutné na účely, na ktoré sa spracúvajú. Na účely splnenia si tejto povinnosti zavedie vhodné technické alebo organizačné opatrenia vrátane výmazu alebo anonymizácie (2) údajov a všetkých záloh v momente uplynutia obdobia uchovávania.

8.5. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti osobných údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknutú osobu, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania.

b) Zmluvné strany sa dohodli na technických a organizačných opatreniach uvedených v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

c) Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

d) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov.

e) V prípade porušenia ochrany osobných údajov, ktoré môže predstavovať riziko pre práva a slobody fyzických osôb, zašle o tom dovozca údajov bez zbytočného odkladu oznámenie vývozcovi údajov a príslušnému dozornému orgánu podľa doložky 13. Takéto oznámenie obsahuje i) opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch); ii) pravdepodobné následky porušenia; iii) prijaté alebo navrhované opatrenia s cieľom napraviť porušenie a iv) údaje kontaktného miesta, kde možno získať viac informácií. V rozsahu, v akom nie je možné, aby dovozca údajov poskytol všetky informácie súčasne, možno ich poskytnúť vo viacerých etapách bez ďalšieho zbytočného odkladu.

f) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, dovozca údajov bez zbytočného odkladu oznámi dotknutým osobám porušenie ochrany osobných údajov a povahu tohto porušenia, v prípade potreby v spolupráci s vývozcom údajov, spolu s informáciami uvedenými v písmene e) bodoch ii) až iv), okrem prípadov, ak dovozca údajov prijal opatrenia na výrazné zníženie rizika pre práva alebo slobody fyzických osôb, alebo ak by si oznámenie vyžadovalo neprimerané úsilie. Vtedy dovozca údajov namiesto toho uverejní oznámenie alebo prijme podobné opatrenie na informovanie verejnosti o porušení ochrany osobných údajov.

g) Dovozca údajov zdokumentuje všetky relevantné skutočnosti týkajúce sa porušenia ochrany osobných údajov vrátane jeho účinkov a všetkých prijatých opatrení na nápravu a vedie o nich záznamy.

8.6. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky prispôsobené osobitnej povahe údajov a súvisiacim rizikám. Môže to zahŕňať obmedzenie okruhu zamestnancov, ktorí majú prístup k osobným údajom, dodatočné bezpečnostné opatrenia (napríklad pseudonymizácia) a/alebo dodatočné obmedzenia v súvislosti s ďalším poskytnutím.

8.7. Následné prenosy

Dovozca údajov poskytne osobné údaje tretej strane nachádzajúcej sa mimo Európskej únie (3) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom. Inak môže dovozca údajov uskutočniť následný prenos len v týchto prípadoch:

i) uskutočňuje sa do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku 45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679 v súvislosti s predmetným spracúvaním;

iii) tretia strana uzavrie s dovozcom údajov dohodu o záväznom nástroji zabezpečujúcom rovnakú úroveň ochrany údajov ako podľa týchto doložiek a dovozca údajov poskytne kópiu týchto záruk vývozcovi údajov;

iv) je to nevyhnutné na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie;

v) je to potrebné v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby; alebo

vi) ak sa neuplatňuje žiadna z uvedených podmienok, dovozca údajov získal výslovný súhlas dotknutej osoby s následným prenosom v konkrétnej situácii po tom, ako ju informoval o jeho účele, totožnosti príjemcu a možných rizikách takéhoto prenosu pre ňu z dôvodu nedostatku primeraných záruk v oblasti ochrany údajov. V tomto prípade dovozca údajov informuje vývozcu údajov a na jeho žiadosť mu odovzdá kópiu informácií poskytnutých dotknutej osobe.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.8. Spracúvanie na základe poverenia dovozcu údajov

Dovozca údajov zabezpečí, aby akákoľvek osoba konajúca na základe jeho poverenia vrátane sprostredkovateľa spracúvala údaje výlučne podľa jeho pokynov.

8.9. Dokumentácia a splnenie povinností

a) Každá zmluvná strana musí byť schopná preukázať splnenie svojich povinností podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v rámci jeho zodpovednosti.

b) Dovozca údajov na požiadanie sprístupní túto dokumentáciu príslušnému dozornému orgánu.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

8.1. Pokyny

a) Dovozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov vývozcu údajov. Vývozca údajov môže udeľovať takéto pokyny počas celého trvania zmluvy.

b) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny dodržať.

8.2. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B, ak vývozca údajov neudelí iné pokyny.

8.3. Transparentnosť

Vývozca údajov sprístupní dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane dodatku, ktorý vyplnili zmluvné strany. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane opatrení uvedených v prílohe II a osobných údajov môže vývozca údajov pred poskytnutím kópie dodatku k týmto doložkám odstrániť časť jeho textu, pričom poskytne zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií. Touto doložkou nie sú dotknuté povinnosti vývozcu údajov podľa článkov 13 a 14 nariadenia (EÚ) 2016/679.

8.4. Správnosť

Ak dovozca údajov zistí, že osobné údaje, ktoré získal, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje vývozcu údajov. V takom prípade je dovozca údajov povinný spolupracovať s vývozcom údajov na účely výmazu alebo opravy údajov.

8.5. Obdobie spracúvania, výmaz alebo vrátenie údajov

Dovozca údajov je oprávnený spracúvať údaje len počas obdobia uvedeného v prílohe I časti B. Po ukončení poskytovania spracovateľských služieb dovozca údajov vymaže všetky osobné údaje spracúvané v mene vývozcu údajov a vývozcovi údajov túto skutočnosť potvrdí, alebo vývozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa vývozca údajov rozhodne. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a bude ich spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo. Tým nie je dotknutá doložka 14, najmä povinnosť dovozcu údajov podľa doložky 14 písm. e) zasielať počas trvania zmluvy vývozcovi údajov oznámenia v prípade, keď má dôvod domnievať sa, že sa naň vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami uvedenými v doložke 14 písm. a).

8.6. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu k týmto údajom (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti zmluvné strany náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknuté osoby, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania. V prípade pseudonymizácie zostávajú dodatočné informácie na priradenie osobných údajov ku konkrétnej dotknutej osobe, ak je to možné, pod výlučnou kontrolou vývozcu údajov. Pri plnení si povinností podľa tohto písmena je dovozca údajov povinný prijať prinajmenšom technické a organizačné opatrenia uvedené v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

b) Dovozca údajov poskytne prístup k osobným údajom svojim zamestnancom len v rozsahu, ktorý je nevyhnutne potrebný na plnenie, riadenie a monitorovanie zmluvy. Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

c) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia vrátane opatrení na zmiernenie jeho nepriaznivých účinkov. Dovozca údajov zašle vývozcovi údajov aj oznámenie o porušení bez zbytočného odkladu po tom, ako sa o tomto porušení dozvedel. Takéto oznámenie obsahuje údaje kontaktného miesta, kde možno získať viac informácií, opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch), pravdepodobné následky porušenia, ako aj prijaté alebo navrhované opatrenia s cieľom napraviť porušenie, v prípade potreby vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov. Pokiaľ nemožno poskytnúť všetky informácie súčasne, pôvodné oznámenie musí obsahovať informácie, ktoré boli v danom čase dostupné, pričom ďalšie informácie sa poskytnú bez zbytočného odkladu po tom, ako budú k dispozícii.

d) Dovozca údajov spolupracuje s vývozcom údajov a poskytuje mu pomoc pri plnení si povinností podľa nariadenia (EÚ) 2016/679, najmä pokiaľ ide o podávanie oznámení príslušnému dozornému orgánu a dotknutým osobám, ktoré sú ovplyvnené, pričom zohľadní povahu spracúvania a informácie, ktoré má k dispozícii dovozca údajov.

8.7. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo

filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky stanovené v prílohe I časti B.

8.8. Následné prenosy

Dovozca údajov poskytuje osobné údaje tretej strane len na základe zdokumentovaných pokynov vývozcu údajov. Údaje možno navyše poskytnúť tretej strane nachádzajúcej sa mimo Európskej únie (4) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom, alebo ak:

i) následný prenos sa uskutočňuje do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679 v súvislosti s predmetným spracúvaním;

iii) následný prenos je nevyhnutný na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iv) následný prenos je potrebný v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.9. Dokumentácia a splnenie povinností

a) Dovozca údajov sa bezodkladne a primerane zaoberá žiadosťami vývozcu údajov, ktoré sa týkajú spracúvania podľa týchto doložiek.

b) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v mene vývozcu údajov.

c) Dovozca údajov sprístupní vývozcovi údajov všetky informácie potrebné na preukázanie splnenia povinností stanovených v týchto doložkách a na žiadosť vývozcu údajov umožní audity spracovateľských činností, na ktoré sa vzťahujú tieto doložky, a poskytne pri nich potrebnú súčinnosť v primeraných intervaloch alebo ak existujú náznaky nesplnenia povinností. Pri rozhodovaní o preskúmaní alebo audite môže vývozca údajov zohľadniť relevantné certifikácie, ktorými disponuje dovozca údajov.

d) Vývozca údajov sa môže rozhodnúť, či vykoná audit sám alebo poverí nezávislého audítora. Audity môžu zahŕňať inšpekcie v priestoroch alebo fyzických zariadeniach dovozcu údajov a v prípade potreby sa vykonávajú po primeranom upovedomení.

e) Zmluvné strany sprístupnia príslušnému dozornému orgánu na požiadanie informácie uvedené v písmenách b) a c) vrátane výsledkov všetkých auditov.

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

8.1. Pokyny

a) Vývozca údajov informoval dovozcu údajov, že koná ako sprostredkovateľ podľa pokynov prevádzkovateľa, ktoré dá vývozca údajov pred spracúvaním k dispozícii dovozcovi údajov.

b) Dovozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov prevádzkovateľa, ktoré dovozcovi údajov oznámil vývozca údajov, a akýchkoľvek dodatočných zdokumentovaných pokynov vývozcu údajov. Takéto dodatočné pokyny nesmú byť v rozpore s pokynmi prevádzkovateľa. Prevádzkovateľ alebo vývozca údajov môže udeľovať ďalšie zdokumentované pokyny týkajúce sa spracúvania údajov počas celého trvania zmluvy.

c) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny dodržať. Ak dovozca údajov nie je schopný dodržať pokyny prevádzkovateľa, vývozca údajov bezodkladne zašle oznámenie prevádzkovateľovi.

d) Vývozca údajov vyhlasuje, že dovozcovi údajov uložil rovnaké povinnosti v oblasti ochrany údajov, ako sú stanovené v zmluve alebo inom právnom akte podľa práva Únie alebo členského štátu, ktoré boli uzatvorené medzi prevádzkovateľom a vývozcom údajov (5).

8.2. Obmedzenie účelu

Dovozca údajov je oprávnený spracúvať osobné údaje len na osobitné účely prenosu stanovené v prílohe I časti B, ak neexistujú iné pokyny prevádzkovateľa, ktoré vývozca údajov oznámil dovozcovi údajov, ani iné pokyny vývozcu údajov.

8.3. Transparentnosť

Vývozca údajov sprístupní dotknutej osobe na požiadanie a bezplatne kópiu týchto doložiek vrátane dodatku, ktorý vyplnili zmluvné strany. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže vývozca údajov pred poskytnutím kópie dodatku odstrániť časť jeho textu, pričom však poskytne zmysluplné zhrnutie, ak by dotknutá osoba inak nebola schopná pochopiť jeho obsah alebo uplatňovať svoje práva. Zmluvné strany na požiadanie oznámia dotknutej osobe dôvody odstránenia textu, pokiaľ možno bez toho, aby došlo k prezradeniu odstránených informácií.

8.4. Správnosť

Ak dovozca údajov zistí, že osobné údaje, ktoré získal, sú nesprávne alebo neaktuálne, bez zbytočného odkladu o tom informuje vývozcu údajov. V takom prípade je dovozca údajov povinný spolupracovať s vývozcom údajov na účely opravy alebo výmazu údajov.

8.5. Obdobie spracúvania, výmaz alebo vrátenie údajov

Dovozca údajov je oprávnený spracúvať údaje len počas obdobia uvedeného v prílohe I časti B. Po ukončení poskytovania spracovateľských služieb dovozca údajov vymaže všetky osobné údaje spracúvané v mene prevádzkovateľa a vývozcovi údajov túto skutočnosť potvrdí, alebo vývozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa vývozca údajov rozhodne. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a bude ich spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo. Tým nie je dotknutá doložka 14, najmä povinnosť dovozcu údajov podľa doložky 14 písm. e) zasielať počas trvania zmluvy vývozcovi údajov oznámenia v prípade, keď má dôvod domnievať sa, že sa naň vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami uvedenými v doložke 14 písm. a).

8.6. Bezpečnosť spracúvania

a) Dovozca údajov a počas prenosu aj vývozca údajov prijmú vhodné technické a organizačné opatrenia na zaistenie bezpečnosti údajov vrátane ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu k týmto údajom (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadnia najnovšie poznatky, náklady na vykonanie, povahu, rozsah, kontext a účely spracúvania, ako aj riziká pre dotknutú osobu, ktoré súvisia so spracúvaním. Zmluvné strany zvážia najmä použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania. V prípade pseudonymizácie zostávajú dodatočné informácie na priradenie osobných údajov ku konkrétnej dotknutej osobe, ak je to možné, pod výlučnou kontrolou vývozcu údajov alebo prevádzkovateľa. Pri plnení si povinností podľa tohto písmena je dovozca údajov povinný prijať prinajmenšom technické a organizačné opatrenia uvedené v prílohe II. Dovozca údajov je povinný vykonávať pravidelné kontroly s cieľom zabezpečiť, aby tieto opatrenia nepretržite poskytovali primeranú úroveň bezpečnosti.

b) Dovozca údajov poskytne prístup k údajom svojim zamestnancom len v rozsahu, ktorý je nevyhnutne potrebný na plnenie, riadenie a monitorovanie zmluvy. Zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

c) V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných dovozcom údajov podľa týchto doložiek prijme dovozca údajov primerané opatrenia na nápravu porušenia vrátane opatrení na zmiernenie jeho nepriaznivých účinkov. Dovozca údajov bez zbytočného odkladu zašle oznámenie vývozcovi údajov a v prípade potreby, ak je to možné, aj prevádzkovateľovi po tom, ako sa dozvedel o porušení. Takéto oznámenie obsahuje údaje kontaktného miesta, kde možno získať viac informácií, opis povahy porušenia (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a záznamov o osobných údajoch), pravdepodobné následky porušenia, ako aj prijaté alebo navrhované opatrenia s cieľom napraviť porušenie ochrany údajov vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov. Pokiaľ nemožno poskytnúť všetky informácie súčasne, pôvodné oznámenie musí obsahovať informácie, ktoré boli v danom čase dostupné, pričom ďalšie informácie sa poskytnú bez zbytočného odkladu po tom, ako budú k dispozícii.

d) Dovozca údajov spolupracuje s vývozcom údajov a poskytuje mu pomoc pri plnení si povinností podľa nariadenia (EÚ) 2016/679, najmä pokiaľ ide o podávanie oznámení prevádzkovateľovi tak, aby mohol tento prevádzkovateľ následne zaslať oznámenie príslušnému dozornému orgánu a dotknutým osobám, ktoré sú ovplyvnené, pričom zohľadní povahu spracúvania a informácie, ktoré má k dispozícii dovozca údajov.

8.7. Citlivé údaje

Ak prenos zahŕňa osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy (ďalej len „citlivé údaje“), uplatňuje dovozca údajov osobitné obmedzenia a/alebo dodatočné záruky stanovené v prílohe I časti B.

8.8. Následné prenosy

Dovozca údajov poskytuje osobné údaje tretej strane len na základe zdokumentovaných pokynov prevádzkovateľa, ktoré dovozcovi údajov oznámil vývozca údajov. Údaje možno navyše poskytnúť tretej strane nachádzajúcej sa mimo Európskej únie (6) (v rovnakej krajine ako dovozca údajov alebo v inej tretej krajine, ďalej len „následný prenos“) len vtedy, ak je táto tretia strana viazaná týmito doložkami alebo súhlasí s tým, že bude týmito doložkami viazaná, a to v súlade s príslušným modulom, alebo ak:

i) následný prenos sa uskutočňuje do krajiny, na ktorú sa vzťahuje rozhodnutie o primeranosti podľa článku45 nariadenia (EÚ) 2016/679, ktorého predmetom je následný prenos;

ii) tretia strana inak zabezpečuje primerané záruky podľa článkov 46 alebo 47 nariadenia (EÚ) 2016/679;

iii) následný prenos je nevyhnutný na účely preukazovania, uplatňovania alebo ochrany právnych nárokov v kontexte konkrétneho správneho alebo súdneho konania, prípadne konania v oblasti regulácie; alebo

iv) následný prenos je potrebný v záujme ochrany životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby.

Na účely akéhokoľvek následného prenosu sa vyžaduje, aby dovozca údajov dodržiaval všetky ostatné záruky podľa týchto doložiek, osobitne obmedzenie účelu.

8.9. Dokumentácia a splnenie povinností

a) Dovozca údajov sa bezodkladne a primerane zaoberá žiadosťami vývozcu údajov alebo prevádzkovateľa, ktoré sa týkajú spracúvania podľa týchto doložiek.

b) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek. Dovozca údajov uchováva najmä príslušnú dokumentáciu týkajúcu sa spracovateľských činností vykonávaných v mene prevádzkovateľa.

c) Dovozca údajov sprístupní vývozcovi údajov všetky informácie potrebné na preukázanie splnenia povinností stanovených v týchto doložkách, pričom vývozca údajov ich poskytne prevádzkovateľovi.

d) Dovozca údajov umožní vývozcovi údajov audity spracovateľských činností, na ktoré sa vzťahujú tieto doložky, a poskytne pri nich potrebnú súčinnosť v primeraných intervaloch alebo ak existujú náznaky nesplnenia povinností. To isté platí aj v prípade, keď vývozca údajov žiada o audit na základe pokynov prevádzkovateľa. Pri rozhodovaní o audite môže vývozca údajov zohľadniť relevantné certifikácie, ktorými disponuje dovozca údajov.

e) Ak sa audit vykonáva na základe pokynov prevádzkovateľa, vývozca údajov sprístupní výsledky prevádzkovateľovi.

f) Vývozca údajov sa môže rozhodnúť, či vykoná audit sám alebo poverí nezávislého audítora. Audity môžu zahŕňať inšpekcie v priestoroch alebo fyzických zariadeniach dovozcu údajov a v prípade potreby sa vykonávajú po primeranom upovedomení.

g) Zmluvné strany sprístupnia príslušnému dozornému orgánu na požiadanie informácie uvedené v písmenách b) a c) vrátane výsledkov všetkých auditov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

8.1. Pokyny

a) Vývozca údajov spracúva osobné údaje len na základe zdokumentovaných pokynov dovozcu údajov v postavení prevádzkovateľa.

b) Vývozca údajov bezodkladne informuje dovozcu údajov, ak nie je schopný dodržať predmetné pokyny, a to aj v prípade, že dané pokyny porušujú nariadenie (EÚ) 2016/679 alebo iné právne predpisy Únie alebo členského štátu o ochrane údajov.

c) Dovozca údajov sa zdrží akéhokoľvek konania, ktoré by vývozcovi údajov bránilo v plnení povinností podľa nariadenia (EÚ) 2016/679, a to aj v kontexte ďalšieho sprostredkovania alebo pokiaľ ide o spoluprácu s príslušnými dozornými orgánmi.

d) Po ukončení poskytovania spracovateľských služieb vývozca údajov vymaže všetky osobné údaje spracúvané v

mene dovozcu údajov a dovozcovi údajov túto skutočnosť potvrdí, alebo dovozcovi údajov vráti všetky osobné údaje spracúvané v jeho mene a vymaže existujúce kópie, a to podľa toho, pre ktorú z možností sa dovozca údajov rozhodne.

8.2. Bezpečnosť spracúvania

a) Zmluvné strany prijmú primerané technické a organizačné opatrenia na zaistenie bezpečnosti údajov, a to aj počas prenosu, ako aj ochrany pred porušením bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu alebo prístupu (ďalej len „porušenie ochrany osobných údajov“). Pri posudzovaní primeranej úrovne bezpečnosti náležite zohľadňujú najnovšie poznatky, náklady na vykonanie opatrení, povahu osobných údajov (7), povahu, rozsah, kontext a účel spracúvania a riziká spojené s spracúvaním pre dotknuté osoby, pričom najmä zvážia použitie šifrovania alebo pseudonymizácie, a to aj počas prenosu, ak možno vďaka nim splniť účel spracúvania.

b) Vývozca údajov pomáha dovozcovi údajov zabezpečiť primeranú bezpečnosť údajov v súlade s písmenom a). V prípade porušenia ochrany osobných údajov týkajúceho sa osobných údajov spracúvaných vývozcom údajov podľa týchto doložiek zašle vývozca údajov oznam dovozcovi údajov bez zbytočného odkladu po tom, ako sa o tejto skutočnosti dozvie, a dovozcovi údajov poskytne pomoc pri náprave porušenia.

c) Vývozca údajov zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje zaviazali, že zachovajú dôvernosť údajov, alebo aby sa na ne vzťahovala primeraná zákonná povinnosť zachovávať dôvernosť údajov.

8.3. Dokumentácia a splnenie povinností

a) Zmluvné strany musia byť schopné preukázať, že si splnili povinnosti podľa týchto doložiek.

b) Vývozca údajov sprístupní dovozcovi údajov všetky informácie potrebné na preukázanie, že si splnil povinnosti podľa týchto doložiek, umožní audity a poskytne pri nich potrebnú súčinnosť.

Doložka 9 Využívanie ďalších sprostredkovateľov

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

Dovozca údajov má všeobecné povolenie vývozcu údajov na zapojenie ďalších sprostredkovateľov z dohodnutého zoznamu. Dovozca údajov osobitne písomne informuje vývozcu údajov o všetkých zamýšľaných zmenách v tomto zozname, pokiaľ ide o pridanie alebo nahradenie ďalších sprostredkovateľov, a to najmenej [uveďte časové obdobie] vopred, čím poskytne vývozcovi údajov dostatočný čas na to, aby mohol proti takýmto zmenám vzniesť námietky pred zapojením ďalšieho sprostredkovateľa. Dovozca údajov poskytne vývozcovi údajov informácie, na základe ktorých môže uplatniť svoje právo namietať.

b) Ak dovozca údajov zapojí ďalšieho sprostredkovateľa do vykonávania konkrétnych spracovateľských činností (v mene vývozcu údajov), urobí to na základe písomnej zmluvy, v ktorej sa v podstate stanovujú rovnaké povinnosti v oblasti ochrany údajov ako sú tie, ktoré má dovozca údajov podľa týchto doložiek, a to aj pokiaľ ide o práva oprávnenej tretej strany v prípade dotknutých osôb. (8) Zmluvné strany vyhlasujú, že splnením povinností v zmysle tejto doložky si dovozca údajov zároveň splní aj povinnosti v zmysle doložky 8.8. Dovozca údajov zabezpečí, aby ďalší sprostredkovateľ dodržiaval povinnosti, ktoré sa podľa týchto doložiek vzťahujú na dovozcu údajov.

c) Dovozca údajov poskytne vývozcovi údajov na jeho žiadosť kópiu dohody s ďalším sprostredkovateľom, ako aj neskorších zmien tejto dohody. V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže dovozca údajov pred poskytnutím kópie tejto dohody odstrániť časti jej textu.

d) Dovozca údajov naďalej v plnom rozsahu zodpovedá vývozcovi údajov za plnenie povinností ďalšieho sprostredkovateľa podľa zmluvy, ktorú uzatvoril s dovozcom údajov. Dovozca údajov zašle vývozcovi údajov oznámenie o každom porušení povinností ďalšieho sprostredkovateľa v zmysle uvedenej zmluvy.

e) Dovozca údajov sa dohodne s ďalším sprostredkovateľom na doložke o oprávnenosti tretej strany, podľa ktorej má vývozca údajov v prípade, že dovozca údajov fakticky zanikol, prestal podľa práva existovať alebo sa stal insolventným, právo vypovedať zmluvu s ďalším sprostredkovateľom a ďalšiemu sprostredkovateľovi dať pokyn, aby osobné údaje vymazal alebo vrátil.

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Dovozca údajov má všeobecné povolenie prevádzkovateľa na zapojenie ďalších sprostredkovateľov z dohodnutého zoznamu. Dovozca údajov osobitne písomne informuje prevádzkovateľa o všetkých zamýšľaných zmenách v tomto zozname, pokiaľ ide o pridanie alebo nahradenie ďalších sprostredkovateľov, a to najmenej [uveďte časové obdobie] vopred, čím poskytne prevádzkovateľovi dostatočný čas na to, aby mohol proti takýmto zmenám vzniesť námietky pred zapojením ďalšieho sprostredkovateľa. Dovozca údajov poskytne prevádzkovateľovi informácie, na základe ktorých môže uplatniť svoje právo namietať. Dovozca údajov informuje vývozcu údajov o zapojení ďalšieho sprostredkovateľa.

b) Ak dovozca údajov zapojí ďalšieho sprostredkovateľa do vykonávania konkrétnych spracovateľských činností (v mene prevádzkovateľa), urobí to na základe písomnej zmluvy, v ktorej sa v podstate stanovujú rovnaké povinnosti v oblasti ochrany údajov ako sú tie, ktoré má dovozca údajov podľa týchto doložiek, a to aj pokiaľ ide o práva oprávnenej tretej strany v prípade dotknutých osôb. (9) Zmluvné strany vyhlasujú, že splnením povinností v zmysle tejto doložky si dovozca údajov zároveň splní aj povinnosti v zmysle doložky 8.8. Dovozca údajov zabezpečí, aby ďalší sprostredkovateľ dodržiaval povinnosti, ktoré sa podľa týchto doložiek vzťahujú na dovozcu údajov.

c) Dovozca údajov poskytne vývozcovi údajov na jeho žiadosť alebo na žiadosť prevádzkovateľa kópiu dohody s ďalším sprostredkovateľom, ako aj neskorších zmien tejto dohody V rozsahu potrebnom na ochranu obchodného tajomstva alebo iných dôverných informácií vrátane osobných údajov môže dovozca údajov pred poskytnutím kópie tejto dohody odstrániť časti jej textu.

d) Dovozca údajov naďalej v plnom rozsahu zodpovedá vývozcovi údajov za plnenie povinností ďalšieho sprostredkovateľa podľa zmluvy, ktorú uzatvoril s dovozcom údajov. Dovozca údajov zašle vývozcovi údajov oznámenie o každom porušení povinností ďalšieho sprostredkovateľa v zmysle uvedenej zmluvy.

e) Dovozca údajov sa dohodne s ďalším sprostredkovateľom na doložke o oprávnenosti tretej strany, podľa ktorej má vývozca údajov v prípade, že dovozca údajov fakticky zanikol, prestal podľa práva existovať alebo sa stal insolventným, právo vypovedať zmluvu s ďalším sprostredkovateľom a ďalšiemu sprostredkovateľovi dať pokyn, aby osobné údaje vymazal alebo vrátil.

Doložka 10 Práva dotknutých osôb

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

a) Dovozca údajov sa prípadne s pomocou vývozcu údajov zaoberá všetkými otázkami a žiadosťami, ktoré dostane od dotknutej osoby a ktoré sa týkajú spracúvania jej osobných údajov a uplatňovania jej práv podľa týchto doložiek, a to bez zbytočného odkladu a najneskôr do jedného mesiaca od prijatia predmetnej otázky alebo žiadosti. (10) Dovozca údajov prijme vhodné opatrenia na uľahčenie týchto otázok, žiadostí a uplatňovania práv dotknutej osoby. Všetky informácie poskytnuté dotknutej osobe musia byť v zrozumiteľnej a ľahko dostupnej forme, pričom musia byť formulované jasne a jednoducho.

b) Na žiadosť dotknutej osoby dovozca údajov predovšetkým bezplatne:

i) poskytne dotknutej osobe potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú; ak áno, kópiu údajov, ktoré sa jej týkajú, a informácie v prílohe I; ak osobné údaje boli alebo budú následne prenášané, poskytne informácie o príjemcoch alebo kategóriách príjemcov (podľa potreby s cieľom poskytnúť zmysluplné informácie), ktorým osobné údaje boli alebo budú následne prenášané, účel takýchto následných prenosov a ich dôvod podľa doložky 8.7; a poskytne informácie o práve podať sťažnosť dozornému orgánu v súlade s doložkou 12 písm. c) bodom i);

ii) opraví nesprávne alebo neúplné údaje týkajúce sa dotknutej osoby;

iii) vymaže osobné údaje týkajúce sa dotknutej osoby, ak sa takéto údaje spracúvajú alebo spracúvali v rozpore s doložkami, ktorých cieľom je zabezpečiť práva oprávnenej tretej strany, alebo ak dotknutá osoba odvolá súhlas, na ktorom je spracúvanie založené.

c) Ak dovozca údajov spracúva osobné údaje na účely priameho marketingu, spracúvanie na tieto účely ukončí, ak dotknutá osoba proti tomu namieta.

d) Dovozca údajov nie je oprávnený založiť rozhodnutie len na automatizovanom spracúvaní prenášaných osobných údajov (ďalej len „automatizované rozhodnutie“), ktoré by vyvolávalo právne účinky týkajúce sa dotknutej osoby alebo by ju podobne významne ovplyvňovalo, okrem prípadu, že by s tým dotknutá osoba výslovne súhlasila alebo dovozca údajov má na to oprávnenie podľa právnych predpisov krajiny určenia, pokiaľ sa v týchto právnych predpisoch stanovujú vhodné opatrenia na zaručenie práv a oprávnených záujmov dotknutej osoby. V takom prípade je dovozca údajov samostatne alebo v spolupráci s vývozcom údajov povinný:

i) informovať dotknutú osobu o zamýšľanom automatizovanom rozhodnutí a dôsledkoch, ako aj o súvisiacej logike, a

ii) zaviesť vhodné záruky, a to aspoň tak, že sa dotknutej osobe umožní napadnúť predmetné rozhodnutie, vyjadriť svoj názor a dosiahnuť preskúmanie človekom.

e) Ak sú žiadosti dotknutej osoby neprimerané najmä z dôvodu ich opakujúcej sa povahy, dovozca údajov môže buď vyúčtovať primeraný poplatok zohľadňujúci administratívne náklady v súvislosti s vybavením žiadosti, alebo žiadosť odmietnuť.

f) Dovozca údajov môže žiadosť dotknutej osoby zamietnuť, ak takéto zamietnutie povoľujú právne predpisy krajiny určenia, pričom je to nevyhnutné a primerané v demokratickej spoločnosti na ochranu jedného z cieľov uvedených v článku 23 ods. 1 nariadenia (EÚ) 2016/679.

g) Ak má dovozca údajov v úmysle zamietnuť žiadosť dotknutej osoby, informuje dotknutú osobu o dôvodoch zamietnutia a možnosti podať sťažnosť príslušnému dozornému orgánu a/alebo domáhať sa nápravy na súde.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

a) Dovozca údajov bezodkladne oznámi vývozcovi údajov každú žiadosť, ktorú dostal od dotknutej osoby. Na túto žiadosť nie je oprávnený sám reagovať, pokiaľ mu to vývozca údajov nepovolil.

b) Dovozca údajov pomáha vývozcovi údajov pri plnení povinnosti reagovať na žiadosti dotknutých osôb o výkon ich práv podľa nariadenia (EÚ) 2016/679. V tejto súvislosti zmluvné strany stanovia v prílohe II vhodné technické a organizačné opatrenia na poskytnutie pomoci, ako aj rozsah potrebnej pomoci, a to s ohľadom na povahu spracúvania.

c) Dovozca údajov dodržiava pri plnení svojich povinností podľa písmen a) a b) pokyny vývozcu údajov

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Dovozca údajov bezodkladne oznámi vývozcovi údajov a v prípade potreby aj prevádzkovateľovi každú žiadosť, ktorú dostal od dotknutej osoby, a to bez toho, aby na ňu reagoval, pokiaľ na to nebol poverený prevádzkovateľom.

b) Dovozca údajov v prípade potreby v spolupráci s vývozcom údajov pomáha prevádzkovateľovi pri plnení povinnosti reagovať na žiadosti dotknutých osôb o výkon ich práv podľa nariadenia (EÚ) 2016/679, prípadne nariadenia (EÚ) 2018/1725. V tejto súvislosti zmluvné strany stanovia v prílohe II vhodné technické a organizačné opatrenia na poskytnutie pomoci, ako aj rozsah potrebnej pomoci, a to s ohľadom na povahu spracúvania.

c) Dovozca údajov dodržiava pri plnení svojich povinností podľa písmen a) a b) pokyny prevádzkovateľa, ktoré mu oznámil vývozca údajov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Zmluvné strany si navzájom poskytujú pomoc pri reagovaní na otázky a žiadosti dotknutých osôb podľa miestneho práva uplatniteľného na dovozcu údajov alebo v prípade spracúvania údajov vývozcom údajov v EÚ podľa nariadenia (EÚ) 2016/679.

Doložka 11 Náprava

a) Dovozca údajov informuje dotknuté osoby v transparentnom a ľahko dostupnom formáte prostredníctvom individuálneho oznámenia alebo na svojom webovom sídle o kontaktnom mieste, ktoré je oprávnené vybavovať sťažnosti. Bezodkladne sa zaoberá všetkými sťažnosťami, ktoré dostane od dotknutej osoby.

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

b) V prípade sporu medzi dotknutou osobou a jednou zo zmluvných strán, ktorý sa týka dodržiavania ustanovení týchto doložiek, vynaloží táto zmluvná strana maximálne úsilie na rýchle vyriešenie sporu formou zmieru. Zmluvné strany sa navzájom informujú o takýchto sporoch a v prípade potreby spolupracujú na ich riešení.

c) Ak sa dotknutá osoba odvoláva na právo oprávnenej tretej strany podľa doložky 3, dovozca údajov akceptuje rozhodnutie dotknutej osoby:

i) podať sťažnosť dozornému orgánu v členskom štáte svojho obvyklého pobytu alebo miesta výkonu práce, alebo príslušnému dozornému orgánu podľa doložky 13;

ii) postúpiť spor príslušným súdom v zmysle doložky 18.

d) Zmluvné strany súhlasia s tým, aby dotknutú osobu zastupoval neziskový subjekt, organizácia alebo združenie za podmienok stanovených v článku 80 ods. 1 nariadenia (EÚ) 2016/679.

e) Dovozca údajov je povinný riadiť sa rozhodnutím, ktoré je záväzné podľa platných právnych predpisov EÚ alebo členského štátu.

f) Dovozca údajov vyjadruje súhlas s tým, že rozhodnutie dotknutej osoby nebude mať vplyv na jej hmotné a procesné práva domáhať sa nápravy v súlade s platnými právnymi predpismi.

Doložka 12 Zodpovednosť

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

a) Každá zmluvná strana je zodpovedná voči druhej zmluvnej strane za akúkoľvek ujmu, ktorú jej spôsobí v dôsledku porušenia týchto doložiek.

b) Každá zmluvná strana je zodpovedná voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú spôsobí dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy. Tým nie je dotknutá zodpovednosť vývozcu údajov podľa nariadenia (EÚ) 2016/679.

c) Ak je za ujmu spôsobenú dotknutej osobe v dôsledku porušenia týchto doložiek zodpovedná viac ako jedna zmluvná strana, tieto zmluvné strany zodpovedajú spoločne a nerozdielne, pričom dotknutá osoba je oprávnená podať žalobu na súd proti ktorejkoľvek z týchto zmluvných strán.

d) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť podľa písmena c) jedna zmluvná strana, je oprávnená žiadať od druhej zmluvnej strany vrátenie časti náhrady vyjadrujúcej jej zodpovednosť za ujmu.

e) Dovozca údajov sa nemôže odvolávať na konanie sprostredkovateľa alebo ďalšieho sprostredkovateľa s cieľom zbaviť sa svojej vlastnej zodpovednosti.

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Každá zmluvná strana je zodpovedná voči druhej zmluvnej strane za akúkoľvek ujmu, ktorú jej spôsobí v dôsledku porušenia týchto doložiek.

b) Dovozca údajov je zodpovedný voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú spôsobí on sám alebo ďalší sprostredkovateľ dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy.

c) Bez ohľadu na písmeno b) je vývozca údajov zodpovedný voči dotknutej osobe za akúkoľvek majetkovú alebo nemajetkovú ujmu, ktorú on sám alebo dovozca údajov (prípadne ďalší sprostredkovateľ) spôsobí dotknutej osobe porušením práv oprávnenej tretej strany podľa týchto doložiek, pričom dotknutá osoba má nárok na náhradu uvedenej ujmy. Tým nie je dotknutá zodpovednosť vývozcu údajov a v prípade, že vývozca údajov je sprostredkovateľom konajúcim v mene prevádzkovateľa, ani zodpovednosť prevádzkovateľa podľa nariadenia (EÚ) 2016/679, prípadne nariadenia (EÚ) 2018/1725.

d) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť za ujmu spôsobenú dovozcom údajov (alebo ďalším sprostredkovateľom) podľa písmena c) vývozca údajov, je oprávnený žiadať od dovozcu údajov vrátenie časti náhrady vyjadrujúcej jeho zodpovednosť za ujmu.

e) Ak je za ujmu spôsobenú dotknutej osobe v dôsledku porušenia týchto doložiek zodpovedná viac ako jedna zmluvná strana, tieto zmluvné strany zodpovedajú spoločne a nerozdielne, pričom dotknutá osoba je oprávnená podať žalobu na súd proti ktorejkoľvek z týchto zmluvných strán.

f) Zmluvné strany sa dohodli, že v prípade, keď nesie zodpovednosť jedna zmluvná strana podľa písmena e), je oprávnená žiadať od druhej zmluvnej strany vrátenie časti náhrady vyjadrujúcej jej zodpovednosť za ujmu.

g) Dovozca údajov sa nemôže odvolávať na konanie ďalšieho sprostredkovateľa s cieľom zbaviť sa svojej vlastnej zodpovednosti.

Doložka 13 Dohľad

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) [Ak je vývozca údajov usadený v členskom štáte EÚ:] Dozorný orgán zodpovedný za zabezpečenie toho, aby vývozca údajov dodržiaval ustanovenia nariadenia (EÚ) 2016/679 v oblasti prenosu údajov podľa prílohy I časti C, má postavenie príslušného dozorného orgánu.

[Ak vývozca údajov nie je usadený v členskom štáte EÚ, ale patrí do územnej pôsobnosti nariadenia (EÚ) 2016/679 v súlade s článkom 3 ods. 2, pričom určí zástupcu podľa článku 27 ods. 1 nariadenia (EÚ) 2016/679:] Dozorný orgán členského štátu, v ktorom je podľa prílohy I časti C usadený zástupca v zmysle článku 27 ods. 1 nariadenia (EÚ) 2016/679, má postavenie príslušného dozorného orgánu.

[Ak vývozca údajov nie je usadený v členskom štáte EÚ, ale patrí do územnej pôsobnosti nariadenia (EÚ) 2016/679 v súlade s článkom 3 ods. 2 bez toho, aby musel určiť zástupcu podľa článku 27 ods. 2 nariadenia (EÚ) 2016/679:] Dozorný orgán jedného z členských štátov, v ktorom sa nachádzajú dotknuté osoby, ktorých osobné údaje sa prenášajú v súlade s týmito doložkami v súvislosti s tovarom alebo službami, ktoré sa im ponúkajú, alebo ktorých správanie sa monitoruje, ako sa to uvádza v prílohe I časti C, má postavenie príslušného dozorného orgánu.

b) Dovozca údajov sa zaväzuje, že sa podriadi jurisdikcii príslušného dozorného orgánu a bude s ním spolupracovať v rámci akýchkoľvek konaní, ktorých cieľom je zabezpečiť dodržiavanie týchto doložiek. Dovozca údajov sa najmä zaväzuje reagovať na otázky, podriadiť sa auditom a konať v súlade s opatreniami prijatými dozorným orgánom vrátane nápravných a kompenzačných opatrení. Dozornému orgánu poskytne písomné potvrdenie, že boli prijaté potrebné opatrenia.

ODDIEL III – MIESTNE PRÁVNE PREDPISY A POVINNOSTI V PRÍPADE PRÍSTUPU ORGÁNOV VEREJNEJ MOCI

Doložka 14 Miestne právne predpisy a prax, ktoré majú vplyv na dodržiavanie doložiek

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi (ak sprostredkovateľ v EÚ kombinuje osobné údaje prijaté od prevádzkovateľa z tretej krajiny s osobnými údajmi, ktoré získal sprostredkovateľ v EÚ)

a) Zmluvné strany vyhlasujú, že nemajú žiadny dôvod považovať právne predpisy a prax v tretej krajine určenia, pokiaľ ide o spracúvanie osobných údajov dovozcom údajov vrátane akýchkoľvek požiadaviek na poskytovanie osobných údajov alebo opatrení, ktorými sa povoľuje prístup orgánov verejnej moci, za prekážku, ktorá by bránila dovozcovi údajov v plnení jeho povinností vyplývajúcich z týchto doložiek. Uvedené vychádza z výkladu, podľa

ktorého právne predpisy a prax, ktoré rešpektujú podstatu základných práv a slobôd a neprekračujú rámec toho, čo je nevyhnutné a primerané v demokratickej spoločnosti na zabezpečenie jedného z cieľov uvedených v článku 23 ods. 1 nariadenia (EÚ) 2016/679, nie sú v rozpore s týmito doložkami.

b) Zmluvné strany deklarujú, že v súvislosti s vyhlásením v písmene a) náležite zohľadnili najmä tieto prvky:

i) osobitné okolnosti prenosu vrátane dĺžky spracovateľského reťazca, počtu zapojených aktérov a použitých prenosových kanálov; zamýšľané následné prenosy; typ príjemcu; účel spracúvania; kategórie a formát prenášaných osobných údajov; odvetvie hospodárstva, v ktorom sa prevod uskutočňuje; miesto uchovávania prenášaných údajov;

ii) právne predpisy a prax tretej krajiny určenia – vrátane tých, podľa ktorých sa vyžaduje poskytovanie údajov orgánom verejnej moci alebo povoľuje prístup týchto orgánov, – ktoré sú relevantné vzhľadom na osobitné okolnosti prenosu, ako aj uplatniteľné obmedzenia a záruky (12);

iii) všetky príslušné zmluvné, technické alebo organizačné záruky zavedené na doplnenie záruk podľa týchto doložiek vrátane opatrení uplatňovaných počas prenosu a spracúvania osobných údajov v krajine určenia.

c) Dovozca údajov vyhlasuje, že pri vykonávaní posúdenia podľa písmena b) vynaložil maximálne úsilie na to, aby poskytol vývozcovi údajov relevantné informácie, a zaväzuje sa naďalej spolupracovať s vývozcom údajov tak, aby sa zabezpečilo dodržiavanie týchto doložiek.

d) Zmluvné strany sa zaväzujú zdokumentovať posúdenie podľa písmena b) a na požiadanie túto dokumentáciu sprístupniť príslušnému dozornému orgánu.

e) Dovozca údajov sa zaväzuje bezodkladne oznámiť vývozcovi údajov, či má po vyjadrení súhlasu s týmito doložkami počas trvania zmluvy dôvod domnievať sa, že sa na neho vzťahujú alebo začali vzťahovať právne predpisy alebo prax, ktoré nie sú v súlade s požiadavkami podľa písmena a), a to aj po zmene právnych predpisov tretej krajiny alebo prijatí opatrenia (ako je žiadosť o poskytnutie údajov) týkajúceho sa uplatnenia takýchto právnych predpisov v praxi, ktoré nie je v súlade s požiadavkami podľa písmena a). [V prípade modulu č. 3: Vývozca údajov postúpi oznámenie prevádzkovateľovi.] Vývozca údajov postúpi oznámenie prevádzkovateľovi.]

f) V nadväznosti na oznámenie podľa písmena e) alebo ak má vývozca údajov inak dôvod domnievať sa, že dovozca údajov už nemôže plniť svoje povinnosti podľa týchto doložiek, vývozca údajov bezodkladne určí vhodné opatrenia (napríklad technické alebo organizačné opatrenia na zaistenie bezpečnosti a dôvernosti), ktoré má prijať vývozca údajov a/alebo dovozca údajov na riešenie situácie [v prípade modulu č. 3: v prípade potreby po konzultácii s prevádzkovateľom]. Vývozca údajov preruší prenos údajov, ak sa domnieva, že nie je možné zabezpečiť primerané záruky pre takýto prenos, alebo ak mu dá na to pokyn [v prípade modulu č. 3: prevádzkovateľ alebo] príslušný dozorný orgán. V takom prípade je vývozca údajov oprávnený vypovedať zmluvu, pokiaľ ide o spracúvanie osobných údajov podľa týchto doložiek. Ak má zmluva viac ako dve zmluvné strany, vývozca údajov ju môže vypovedať len vo vzťahu k príslušnej zmluvnej strane, pokiaľ sa zmluvné strany nedohodli inak. V prípade vypovedania zmluvy podľa tejto doložky sa uplatní doložka 16 písm. d) a e).

Doložka 15 Povinnosti dovozcu údajov v prípade prístupu orgánov verejnej moci

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi(ak sprostredkovateľ v EÚ kombinuje osobné údaje prijaté od prevádzkovateľa z tretej krajiny s osobnými údajmi, ktoré získal sprostredkovateľ v EÚ)

15.1. Oznámenie

a) Dovozca údajov sa zaväzuje bezodkladne zaslať oznámenie vývozcovi údajov a prípadne dotknutej osobe (v prípade potreby s pomocou vývozcu údajov), ak:

i) dostane právne záväznú žiadosť od orgánu verejnej moci vrátane súdnych orgánov podľa právnych predpisov krajiny určenia o poskytnutie osobných údajov prenášaných podľa týchto doložiek; takéto oznámenie obsahuje informácie o požadovaných osobných údajoch, žiadajúcom orgáne, právnom základe žiadosti a poskytnutej odpovedi; alebo

ii) sa dozvie o akomkoľvek priamom prístupe orgánov verejnej moci k osobným údajom prenášaným podľa týchto doložiek v súlade s právnymi predpismi krajiny určenia; takéto oznámenie obsahuje všetky informácie, ktoré má dovozca k dispozícii.

[V prípade modulu č. 3: Vývozca údajov postúpi oznámenie prevádzkovateľovi.]

b) Ak sa dovozcovi údajov zakazuje podľa právnych predpisov krajiny určenia zaslať oznámenie vývozcovi údajov a/alebo dotknutej osobe, dovozca údajov sa zaväzuje vynaložiť maximálne úsilie na získanie výnimky zo zákazu s cieľom oznámiť čo najviac informácií a čo najskôr. Dovozca údajov sa zaväzuje zdokumentovať svoje maximálne úsilie tak, aby ho mohol na žiadosť vývozcu údajov preukázať.

c) Ak to právne predpisy krajiny určenia umožňujú, dovozca údajov sa zaväzuje, že počas trvania zmluvy bude vývozcovi údajov v pravidelných intervaloch poskytovať čo najviac relevantných informácií o prijatých žiadostiach (najmä počet žiadostí, druh požadovaných údajov, žiadajúci orgán, či boli žiadosti napadnuté a výsledok súvisiacich konaní atď.). [V prípade modulu č. 3: Vývozca údajov postúpi informáciu prevádzkovateľovi.]

d) Dovozca údajov sa zaväzuje, že informácie podľa písmen a) až c) uchová počas trvania zmluvy a na požiadanie ich sprístupní príslušnému dozornému orgánu.

e) Písmená a) až c) sa uplatňujú bez toho, aby bola dotknutá povinnosť dovozcu údajov podľa doložky 14 písm. e) a doložky 16, a to bezodkladne informovať vývozcu údajov, ak nie je schopný konať v súlade s týmito doložkami.

15.2. Preskúmanie zákonnosti a minimalizácia údajov

a) Dovozca údajov sa zaväzuje preskúmať zákonnosť žiadosti o poskytnutie údajov, najmä či je zachovaná právomoc žiadajúceho orgánu verejnej moci, a žiadosť napadnúť, ak po dôkladnom posúdení dospeje k záveru, že existujú opodstatnené dôvody domnievať sa, že žiadosť je nezákonná podľa právnych predpisov krajiny určenia, platných záväzkov podľa medzinárodného práva a zásad ústretovosti v medzinárodných vzťahoch. Dovozca údajov je za rovnakých podmienok povinný využívať možnosti odvolania. Pri napadnutí žiadosti dovozca údajov navrhne nariadenie predbežných opatrení s cieľom pozastaviť účinky žiadosti dovtedy, kým príslušný súdny orgán nerozhodne vo veci samej. Požadované osobné údaje poskytne až vtedy, keď je na to povinný podľa platných procesných pravidiel. Týmito požiadavkami nie sú dotknuté povinnosti dovozcu údajov podľa doložky 14 písm. e).

b) Dovozca údajov sa zaväzuje zdokumentovať príslušné právne posúdenie, ako aj akékoľvek napadnutie žiadosti o poskytnutie údajov, a v rozsahu povolenom právnymi predpismi krajiny určenia sprístupní dokumentáciu vývozcovi údajov Na požiadanie sprístupní túto dokumentáciu aj príslušnému dozornému orgánu. [V prípade modulu č. 3: Vývozca údajov sprístupní posúdenie prevádzkovateľovi.]

c) Dovozca údajov sa zaväzuje, že v rámci odpovede na žiadosť o poskytnutie údajov poskytne minimálne dovolené množstvo informácií, a to na základe primeraného výkladu žiadosti.

ODDIEL IV – ZÁVEREČNÉ USTANOVENIA

Doložka 16 Nedodržanie doložiek a ukončenie platnosti

a) Dovozca údajov bezodkladne informuje vývozcu údajov, ak nie je schopný tieto pokyny z akéhokoľvek dôvodu dodržať.

b) V prípade, že dovozca údajov porušuje tieto doložky alebo nie je schopný plniť si povinnosti podľa týchto doložiek, vývozca údajov pozastaví prenos osobných údajov dovozcovi údajov, kým sa opäť nedosiahne súlad alebo nedôjde k ukončeniu platnosti zmluvy. Doložka 14 písm. f) tým nie je dotknutá.

c) Vývozca údajov je oprávnený vypovedať zmluvu v rozsahu, v akom sa týka spracúvania osobných údajov podľa týchto doložiek, ak:

i) vývozca údajov prerušil prenos osobných údajov dovozcovi údajov podľa písmena b) a dodržiavanie týchto doložiek sa neobnoví v primeranej lehote a v každom prípade do jedného mesiaca od prerušenia;

ii) dovozca údajov závažným alebo trvalým spôsobom porušuje tieto doložky; alebo

iii) dovozca údajov porušuje záväzné rozhodnutie príslušného súdu alebo dozorného orgánu, pokiaľ ide o jeho povinnosti podľa týchto doložiek.

V týchto prípadoch informuje o tomto porušení príslušný dozorný orgán [v prípade modulu č. 3: a prevádzkovateľa]. Ak má zmluva viac ako dve zmluvné strany, vývozca údajov ju môže vypovedať len vo vzťahu k príslušnej zmluvnej strane, pokiaľ sa zmluvné strany nedohodli inak.

d) [V prípade modulov č. 1, 2 a 3: Osobné údaje, ktoré boli prenesené pred vypovedaním zmluvy podľa písmena c), sa bezodkladne vrátia vývozcovi údajov alebo v celom rozsahu vymažú, a to podľa toho, pre ktorú z možností sa vývozca údajov rozhodne. To isté platí v prípade kópií údajov.] [V prípade modulu č. 4: Osobné údaje získané vývozcom údajov v EÚ, ktoré boli prenesené pred vypovedaním zmluvy podľa písmena c), sa bezodkladne v celom rozsahu vymažú, vrátane ich kópií.] Dovozca údajov vydá vývozcovi údajov potvrdenie o tom, že údaje boli vymazané. Dovozca údajov zabezpečuje dodržiavanie týchto doložiek dovtedy, kým nedôjde k vymazaniu alebo vráteniu údajov. Pokiaľ ide o miestne právne predpisy uplatniteľné na dovozcu údajov, ktorými sa zakazuje vrátenie alebo vymazanie prenesených osobných údajov, dovozca údajov vyhlasuje, že bude naďalej zabezpečovať súlad s týmito doložkami a údaje bude spracúvať len v takom rozsahu a tak dlho, ako to vyžaduje uvedené miestne právo.

e) Ktorákoľvek zo zmluvných strán môže odvolať svoj súhlas s tým, že bude viazaná týmito doložkami, ak i) Európska komisia prijme rozhodnutie podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 týkajúce sa prenosu osobných údajov, na ktoré sa vzťahujú tieto doložky, alebo ii) nariadenie (EÚ) 2016/679 sa stane súčasťou právneho rámca krajiny, do ktorej sa osobné údaje prenášajú. Tým nie sú dotknuté ostatné povinnosti vzťahujúce sa na predmetné spracúvanie podľa nariadenia (EÚ) 2016/679.

Doložka 17 Rozhodné právo

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

Tieto doložky sa riadia právom členského štátu Európskej únie, ak toto právo priznáva účinok právam oprávnenej

tretej strany. Zmluvné strany sa dohodli, že toto bude právny poriadok ako je to definované v Podmienkach.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Tieto doložky sa riadia právom krajiny, ktoré priznáva účinok právam oprávnenej tretej strany. Zmluvné strany sa dohodli, že toto bude právny poriadok ako je to definované v Podmienkach.

Doložka 18 Voľba súdu a právomoci

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

a) Na rozhodovanie sporov vyplývajúcich z týchto doložiek sú príslušné súdy členského štátu EÚ.

b) Zmluvné strany sa dohodli, že týmito súdmi sú súdy ako je definované v Podmienkach.

c) Dotknutá osoba môže podať návrh na začatie konania proti vývozcovi údajov a/alebo dovozcovi údajov aj na súdoch členského štátu, v ktorom má obvyklý pobyt.

d) Zmluvné strany sa dohodli, že sa podriadia právomoci týchto súdov.

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Na rozhodovanie sporov vyplývajúcich z týchto doložiek sú príslušné súdy ako je definované v Podmienkach.

DODATOK

VYSVETLIVKA: Musí byť možné jasne rozlišovať informácie uplatniteľné na jednotlivé prenosy alebo kategórie prenosov a v tomto ohľade identifikovať úlohy jednotlivých zmluvných strán v postavení vývozcov údajov a/alebo dovozcov údajov. V tomto ohľade nie je nevyhnutné, aby došlo k vyplneniu a podpisu osobitných dodatkov pre každý prevod/kategóriu prevodov a/alebo zmluvný vzťah, ak túto transparentnosť možno dosiahnuť prostredníctvom jedného dodatku. Ak je však potrebné zabezpečiť dostatočnú jasnosť, mali by sa použiť samostatné dodatky.

PRÍLOHA I

A. ZOZNAM ZMLUVNÝCH STRÁN

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Vývozca údajov: [Totožnosť a kontaktné údaje vývozcu údajov a prípadne jeho zodpovednej osoby a/alebo zástupcu v Európskej únii]

1. Prevádzkovateľ v zmysle Dohody o spracúvaní údajov

2. Sprostredkovateľ v zmysle Dohody o spracúvaní údajov

(na základe toku údajov)

Dovozca údajov: [Totožnosť a kontaktné údaje dovozcu údajov vrátane akejkoľvek kontaktnej osoby zodpovednej za ochranu údajov]

1. Prevádzkovateľ v zmysle Dohody o spracúvaní údajov

2. Sprostredkovateľ v zmysle Dohody o spracúvaní údajov

(na základe toku údajov)

B. OPIS PRENOSU

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

MODUL č. 4: Prenos od sprostredkovateľa k prevádzkovateľovi

Kategórie dotknutých osôb, ktorých osobné údaje sa prenášajú: Ako je definované v Dohode o spracúvaní údajov.

Kategórie prenášaných osobných údajov: Ako je definované v Dohode o spracúvaní údajov a Zásadách ochrany osobných údajov.

Prenášané citlivé údaje (v relevantných prípadoch) a uplatňované obmedzenia alebo záruky, ktoré v plnej miere zohľadňujú povahu údajov a súvisiace riziká, ako napríklad prísne obmedzenie účelu, obmedzenia prístupu (vrátane prístupu len pre personál, ktorý absolvoval špecializovanú odbornú prípravu), vedenie záznamov o prístupe k údajom, obmedzenia následných prenosov alebo dodatočné bezpečnostné opatrenia: Ako je definované v Dohode o spracúvaní údajov a Zásadách ochrany osobných údajov.

Frekvencia prenosu (napríklad či sa údaje prenášajú jednorazovo alebo sústavne): Sústavný prenos.

Povaha spracúvania: Automatizovaná.

Účel prenosu a ďalšieho spracúvania údajov: Poskytovanie služby v zmysle Podmienok, ich príloh, Zásad ochrany osobných údajov a dokumentácie k službe.

Obdobie uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jeho určenie: Ako je definované v Dohode o spracúvaní údajov.

V prípade prevodov sprostredkovateľom alebo ďalším sprostredkovateľom uveďte aj predmet, povahu a trvanie spracúvania: Ako je definované v Dohode o spracúvaní údajov.

C. PRÍSLUŠNÝ DOZORNÝ ORGÁN

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

Uveďte príslušný dozorný orgán v súlade s doložkou 13: Ako je definované v Zásadách ochrany osobných údajov

PRÍLOHA II TECHNICKÉ A ORGANIZAČNÉ OPATRENIA VRÁTANE TECHNICKÝCH A ORGANIZAČNÝCH OPATRENÍ NA ZAISTENIE BEZPEČNOSTI ÚDAJOV

MODUL č. 1: Prenos od prevádzkovateľa k prevádzkovateľovi

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

VYSVETLIVKA: Technické a organizačné opatrenia treba opísať konkrétne, nie všeobecne. Pozri aj všeobecnú poznámku na prvej strane dodatku, najmä pokiaľ ide o potrebu jasne uviesť, ktoré opatrenia sa vzťahujú na konkrétny prevod/súbor presunov.

Opis technických a organizačných opatrení prijatých dovozcom údajov (vrátane všetkých príslušných certifikácií) s cieľom zabezpečiť primeranú úroveň bezpečnosti, pričom sa zohľadní povaha, rozsah, kontext a účel spracúvania, ako aj riziká pre práva a slobody fyzických osôb: Ako je definované v bezpečnostnej politike

V prípade prenosov sprostredkovateľom alebo ďalším sprostredkovateľom opíšte aj osobitné technické a organizačné opatrenia, ktoré má prijať sprostredkovateľ alebo ďalší sprostredkovateľ, aby mohol poskytnúť pomoc prevádzkovateľovi, a v prípade prenosov od sprostredkovateľa k ďalšiemu sprostredkovateľovi vývozcovi údajov

PRÍLOHA III ZOZNAM ĎALŠÍCH SPROSTREDKOVATEĽOV

MODUL č. 2: Prenos od prevádzkovateľa k sprostredkovateľovi

MODUL č. 3: Prenos od sprostredkovateľa k sprostredkovateľovi

VYSVETLIVKA: Túto prílohu je potrebné vyplniť v prípade modulov č. 2 a 3, pokiaľ ide o osobitné povolenie pre ďalších sprostredkovateľov [doložka 9 písm. a) možnosť 1].

Prevádzkovateľ povolil využitie týchto ďalších sprostredkovateľov: Ako je definované v Dohode o spracúvaní údajov

Odkazy:

(1) Ak je vývozca údajov sprostredkovateľom, na ktorého sa vzťahuje nariadenie (EÚ) 2016/679 a ktorý koná v mene inštitúcie alebo orgánu Únie ako prevádzkovateľ, tak uplatňovaním týchto doložiek sa pri zapojení iného sprostredkovateľa (ďalšie sprostredkovanie), na ktorého sa nevzťahuje nariadenie (EÚ) 2016/679, zabezpečuje aj súlad s článkom 29 ods. 4 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39), pokiaľ sú tieto doložky a povinnosti v oblasti ochrany údajov, ktoré sú stanovené v zmluve alebo inom právnom akte uzavretom medzi prevádzkovateľom a sprostredkovateľom podľa článku 29 ods. 3 nariadenia (EÚ) 2018/1725, vo vzájomnom súlade. Platí to najmä v prípade, keď sa prevádzkovateľ a sprostredkovateľ odvolávajú na štandardné zmluvné doložky uvedené v rozhodnutí 2021/915.

(2) Je teda nevyhnutné, aby boli údaje anonymizované tak, aby nikto nemohol jednotlivca identifikovať, ako sa to

uvádza v odôvodnení 26 nariadenia (EÚ) 2016/679, pričom tento postup musí byť nezvratný.

(3) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(4) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(5) Pozri článok 28 ods. 4 nariadenia (EÚ) 2016/679 a v prípade, že prevádzkovateľom je inštitúcia alebo orgán EÚ, článok 29 ods. 4 nariadenia (EÚ) 2018/1725.

(6) Dohodou o Európskom hospodárskom priestore (ďalej len „Dohoda o EHP“) sa vnútorný trh Európskej únie rozširuje o tri štáty EHP – Island, Lichtenštajnsko a Nórsko. Na právne predpisy Únie v oblasti ochrany osobných údajov vrátane nariadenia (EÚ) 2016/679 sa vzťahuje Dohoda o EHP a tieto predpisy boli začlenené do prílohy XI k tejto dohode. Preto akékoľvek poskytnutie údajov zo strany dovozcu údajov tretej strane nachádzajúcej sa v EHP sa na účely týchto doložiek nepovažuje za následný prenos.

(7) Vrátane toho, či prenos a ďalšie spracúvanie zahŕňajú osobné údaje odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, genetické alebo biometrické údaje na účely jedinečnej identifikácie fyzickej osoby, údaje týkajúce sa zdravia alebo sexuálneho života či sexuálnej orientácie osoby, alebo údaje týkajúce sa odsúdenia za trestné činy.

(8) Túto požiadavku môže ďalší sprostredkovateľ, ktorý pristupuje k týmto doložkám v súlade s príslušným modulom, splniť podľa doložky 7.

(9) Túto požiadavku môže ďalší sprostredkovateľ, ktorý pristupuje k týmto doložkám v súlade s príslušným modulom, splniť podľa doložky 7.

(10) Túto lehotu možno predĺžiť najviac o dva mesiace, a to v nevyhnutnom rozsahu a s ohľadom na zložitosť a počet žiadostí. Dovozca údajov náležite a bezodkladne informuje dotknutú osobu o každom takomto predĺžení.

(11) Dovozca údajov môže ponúknuť nezávislé riešenie sporov na rozhodcovskom orgáne len vtedy, ak je usadený v krajine, ktorá ratifikovala Newyorský dohovor o výkone rozhodcovských rozhodnutí.

(12) Pokiaľ ide o vplyv týchto právnych predpisov a praxe na dodržiavanie týchto doložiek, v rámci celkového posúdenia možno zohľadniť rôzne prvky. Medzi tieto prvky možno zahrnúť relevantné a zdokumentované praktické skúsenosti s predchádzajúcimi prípadmi žiadostí orgánov verejnej moci o poskytnutie údajov alebo neexistenciu takýchto žiadostí, ktoré sa vzťahujú na dostatočne reprezentatívny časový rámec. Ide najmä o interné záznamy alebo inú dokumentáciu, ktoré boli vypracúvané priebežne v súlade s náležitou starostlivosťou a certifikované na úrovni vyššieho manažmentu, ak možno tieto informácie zákonne poskytovať tretím stranám. Pokiaľ možno na základe týchto praktických skúseností dospieť k záveru, že dovozcovi údajov nič nebráni v dodržiavaní týchto doložiek, treba uviesť aj ďalšie relevantné objektívne prvky, pričom zmluvným stranám prináleží dôkladne posúdiť, či tieto prvky ako celok majú dostatočnú váhu na podporu tohto záveru, pokiaľ ide o ich spoľahlivosť a reprezentatívnosť. Zmluvné strany musia predovšetkým prihliadnuť na to, či sú ich praktické skúsenosti potvrdené, a teda nie v rozpore s verejnými alebo inak dostupnými a spoľahlivými informáciami o existencii alebo neexistencii žiadostí v rámci toho istého odvetvia a/alebo uplatňovaním právnych predpisov v praxi, ako je napríklad judikatúra a správy nezávislých orgánov dohľadu.