

# ESET Endpoint Antivirus for macOS

## Používateľská príručka

[Pre zobrazenie tohto dokumentu v online verzii kliknite sem](#)

Copyright ©2023 ESET, spol. s r. o.

ESET Endpoint Antivirus for macOS bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke [www.eset.sk](http://www.eset.sk).

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukováná 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. 19.3.2023

1 ESET Endpoint Antivirus for macOS	1
1.1 Čo je nové vo verzii 6	1
1.2 Systémové požiadavky	2
2 Predstavenie ESET PROTECT	2
3 Predstavenie ESET PROTECT Cloud	4
4 Vzdialená inštalácia	4
4.1 Vytvorenie balíka na vzdialenú inštaláciu	6
5 Lokálna inštalácia	9
5.1 Typická inštalácia	10
5.2 Pokročilá inštalácia	11
5.3 Lokálne povolenie rozšírení systému	13
5.4 Lokálne povolenie úplného prístupu k disku	13
6 Aktivácia produktu	14
7 Odinštalovanie	15
8 Stručný prehľad	15
8.1 Klávesové skratky	16
8.2 Kontrola funkčnosti programu	16
8.3 Čo robiť, ak program nepracuje správne	17
9 Ochrana počítača	17
9.1 Antivírusová a antispyvérová ochrana	17
9.1 Všeobecné	18
9.1 Vylúčenia	18
9.1 Ochrana pri štarte počítača	19
9.1 Rezidentná ochrana súborového systému	19
9.1 Rozšírené nastavenia	19
9.1 Kedy je vhodné upraviť nastavenia rezidentnej ochrany	20
9.1 Overenie funkčnosti rezidentnej ochrany	20
9.1 Čo robiť, ak rezidentná ochrana nefunguje	20
9.1 Manuálna kontrola počítača	21
9.1 Typy kontroly	22
9.1 Smart kontrola	22
9.1 Prispôbená kontrola	22
9.1 Ciele kontroly	22
9.1 Profily kontroly	23
9.1 Nastavenie parametrov jadra ThreatSense	23
9.1 Objekty	24
9.1 Metódy	25
9.1 Liečenie	25
9.1 Vylúčenia	25
9.1 Obmedzenia	26
9.1 Ostatné	26
9.1 Našla sa infilácia	27
9.2 Webová a e-mailová ochrana	27
9.2 Ochrana prístupu na web	28
9.2 Porty	28
9.2 Zoznam URL adries	28
9.2 E-mailová ochrana	28
9.2 Kontrola protokolu POP3	29
9.2 Kontrola protokolu IMAP	30
9.3 Anti-Phishing	30

10 Správa zariadení .....	30
<b>10.1 Pravidlá</b> .....	31
11 Nástroje .....	33
<b>11.1 Protokoly</b> .....	33
11.1 Údržba protokolov .....	33
11.1 Filtrovanie protokolov .....	34
<b>11.2 Plánovač</b> .....	35
11.2 Vytváranie nových úloh .....	36
11.2 Vytvorenie úlohy definovanej používateľom .....	37
<b>11.3 ESET LiveGrid</b> .....	38
11.3 Podozrivé súbory .....	38
<b>11.4 Karanténa</b> .....	39
11.4 Uloženie súborov do karantény .....	39
11.4 Obnovenie súborov z karantény .....	39
11.4 Posielanie súboru z karantény .....	40
<b>11.5 Oprávnenia</b> .....	40
<b>11.6 Prezentačný režim</b> .....	40
<b>11.7 Spustené procesy</b> .....	41
12 Používateľské rozhranie .....	42
<b>12.1 Výstrahy a upozornenia</b> .....	42
12.1 Zobrazovanie upozornení .....	43
12.1 Stavby ochrany .....	43
<b>12.2 Kontextové menu</b> .....	43
13 Aktualizácia .....	43
<b>13.1 Nastavenie aktualizácií</b> .....	44
13.1 Rozšírené nastavenia .....	45
<b>13.2 Ako vytvoriť aktualizáciu úlohu</b> .....	46
<b>13.3 Aktualizácie systému</b> .....	46
<b>13.4 Import a export nastavení</b> .....	47
<b>13.5 Nastavenie proxy servera</b> .....	48
<b>13.6 Zdieľaná lokálna vyrovnávacia pamäť</b> .....	48
14 Licenčná dohoda s koncovým používateľom .....	49
15 Privacy Policy .....	55

# ESET Endpoint Antivirus for macOS

ESET Endpoint Antivirus for macOS 6 predstavuje nový prístup k integrovanej počítačovej bezpečnosti. Najnovšia verzia skenovacieho jadra ThreatSense® spája rýchlosť a presnosť pre maximálnu ochranu systému. Výsledkom je inteligentný systém, ktorý je neustále v pohotovosti pred útokmi a škodlivým softvérom ohrozujúcim váš počítač.

ESET Endpoint Antivirus for macOS 6 je komplexné bezpečnostné riešenie vytvorené dlhodobým úsilím skombinovať maximálnu ochranu a minimálne nároky na systém. Pokročilé technológie založené na umelej inteligencii sú schopné proaktívne eliminovať infiltrácie ako vírusy, červy, trójske kone, spyvér, advér, rootkity a iné internetové útoky bez negatívneho vplyvu na výkon či fungovanie systému.

Produkt je navrhnutý na ochranu pracovných staníc vo firmách či podnikoch. Môže byť použitý s nástrojom ESET PROTECT (predtým ESET Security Management Center), ktorý umožňuje jednoducho spravovať akýkoľvek počet pracovných staníc, hromadne na nich aplikovať politiky a pravidlá, sledovať zachytené infiltrácie a vzdialene ich nastavovať z iného počítača v sieti.

## Čo je nové vo verzii 6

Grafické používateľské rozhranie programu ESET Endpoint Antivirus for macOS bolo kompletne prepracované pre lepšiu čitateľnosť jednotlivých prvkov a viac intuitívne používanie. Verzia 6 prináša aj nasledujúce vylepšenia:

- Podpora ESET Enterprise Inspector – ESET Endpoint Antivirus for macOS môže byť od verzie 6.9 pripojený k ESET Enterprise Inspector (EEI). EEI predstavuje komplexný systém detekcie a reakcie na hrozby na koncových zariadeniach (Endpoint Detection and Response – EDR), ktorý zahŕňa funkcie, ako napr. detekcia incidentov, manažment a reakcia na incidenty, zozbieravanie údajov, detekcia indikátorov preukazujúcich narušenie zabezpečenia, detekcia anomálií, detekcia správania, detekcia porušenia pravidiel atď. Viac informácií o nástroji ESET Enterprise Inspector, jeho inštalácii a možnostiach nájdete v [Online pomocníkovi](#).
- **podpora 64-bitovej architektúry**
- **Ochrana prístupu na web** – kontroluje komunikáciu webových prehliadačov so vzdialenými servermi.
- **Emailová ochrana** – kontroluje e-mailovú komunikáciu prijímanú prostredníctvom protokolov POP3 a IMAP.
- **Antiphishingová ochrana** – chráni vás pred pokusmi o získanie vašich hesiel a iných citlivých informácií tým, že zamedzuje prístup na podvodné webové stránky, ktoré sa vydávajú za legitímne.
- **Správa zariadení** – umožňuje kontrolovať alebo blokovať zariadenia a prispôbovať filtre a oprávnenia používateľov pre prístup a prácu s externými zariadeniami. Táto funkcia je dostupná od produktovej verzie 6.1.
- **Prezentačný režim** – umožňuje mať spustený program ESET Endpoint Antivirus for macOS na pozadí bez zobrazovania notifikácií či vykonávania plánovaných úloh.
- **Zdieľaná lokálna vyrovnávacia pamäť** – zvyšuje rýchlosť kontroly vo virtuálnych prostrediach.

# Systémové požiadavky

Pre bezproblémový chod ESET Endpoint Antivirus for macOS je potrebné splniť nasledujúce požiadavky na hardvér a softvér:

	Systémové požiadavky:
Architektúra procesora	Intel 64-bit, Apple ARM 64-bitová architektúra
Operačný systém	macOS 10.12 a novšie verzie macOS Server 10.12 a novšie verzie
Pamäť	300 MB
Voľné miesto na disku	200 MB

Okrem procesorov Intel podporuje ESET Endpoint Antivirus for macOS od verzie 6.10.900.0 taktiež aj čip ARM od Apple (prostredníctvom emulátora Rosetta 2).

## Predstavenie ESET PROTECT

ESET PROTECT vám umožňuje spravovať v sieťovom prostredí z jedného miesta všetky produkty ESET nainštalované na pracovných staniciach, serveroch a mobilných zariadeniach.

Prostredníctvom ESET PROTECT Web Console môžete vzdialene nasadiť bezpečnostné riešenia ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na počítačoch. Prečítajte si tiež kapitoly [Prehľad architektúry a infraštruktúry ESET PROTECT](#), [Začíname s nástrojom ESET PROTECT Web Console](#) a [Podporované Desktop Provisioning prostredia](#).

ESET PROTECT pozostáva z nasledujúcich súčastí:

- [ESET PROTECT Server](#) – ESET PROTECT Server môže byť nainštalovaný na Windows aj Linux servery a môže mať tiež podobu virtuálneho zariadenia. Riadi komunikáciu s agentmi a zhromažďuje a uchováva dáta aplikácií v databáze.
- [ESET PROTECT Web Console](#) – ESET PROTECT Web Console je hlavným rozhraním, ktoré vám umožňuje spravovať klientske počítače vo vašej sieti. Poskytuje prehľad stavu klientskych zariadení v sieti a dá sa použiť na vzdialenú inštaláciu produktov spoločnosti ESET na nespravované počítače. Po inštalácii ESET PROTECT Servera máte prístup do Web Console prostredníctvom vášho webového prehliadača. Ak sa rozhodnete sprístupniť webový server na internete, budete môcť používať ESET PROTECT z akéhokoľvek miesta a zariadenia pripojeného na internet.
- [ESET Management Agent](#) – ESET Management Agent sprostredkúva komunikáciu medzi ESET PROTECT Serverom a klientskymi počítačmi. Agent musí byť nainštalovaný na každom klientskom počítači, ktorý má komunikovať s ESET PROTECT Serverom. Keďže sa agent nachádza na klientskom počítači a dokáže uchovávať viaceré bezpečnostné scenáre, používanie ESET Management Agentu výrazne skracuje čas reakcie na nové detekcie. Pomocou ESET PROTECT Web Console môžete [nasadiť ESET Management Agentu](#) na nespravované počítače, ktoré boli identifikované prostredníctvom Active Directory alebo nástrojom ESET [RD Sensor](#). V prípade potreby je možná aj [manuálna inštalácia ESET Management Agentu](#).

- [Rogue Detection Sensor](#) – ESET PROTECT Rogue Detection Sensor deteguje nespravované počítače, ktoré sa nachádzajú v sieti. Informácie o týchto počítačoch sú odosielané na ESET PROTECT Server. To umožňuje jednoducho pridať nové klientske počítače do vašej zabezpečenej siete. RD Sensor si pamätá počítače, ktoré už boli nájdené a nebude odosielať rovnaké informácie dvakrát.
- [Apache HTTP Proxy](#) – je to služba, ktorá môže byť použitá v kombinácii s nástrojom ESET PROTECT na:
  - Odistribúciu aktualizácií na klientske počítače a distribúciu inštalačných balíkov na ESET Management Agent, opresmerovanie komunikácie z ESET Management Agentov na ESET PROTECT Server.
- [Mobile Device Connector](#) – komponent, ktorý umožňuje správu mobilných zariadení pomocou nástroja ESET PROTECT. Umožňuje vám spravovať mobilné zariadenia (Android a iOS) a bezpečnostný produkt ESET Endpoint Security pre Android.
- [Virtuálne zariadenie ESET PROTECT](#) – ESET PROTECT VA je určené pre používateľov, ktorí chcú používať ESET PROTECT vo virtualizovanom prostredí.
- [ESET PROTECT Virtual Agent Host](#) – komponent programu ESET PROTECT, ktorý vytvára virtuálnych agentov, a umožňuje tak správu virtuálnych zariadení bez klasického agenta. Toto riešenie umožňuje automatizáciu, použitie dynamických skupín a správu úloh na rovnakej úrovni, ako tomu je pri klasických ESET Management Agentoch na fyzických počítačoch. Virtuálny agent zbiera informácie na virtuálnych počítačoch a odosiela ich na ESET PROTECT Server.
- [Mirror Tool](#) – tento nástroj sa používa na aktualizovanie programových modulov v offline prostredí. V prípade, že bezpečnostné produkty ESET na vašich klientských počítačoch nemajú pripojenie na internet, môžete použiť nástroj Mirror Tool, ktorý sťahuje aktualizčné súbory z aktualizčných serverov spoločnosti ESET a ukladá ich lokálne.
- [ESET Remote Deployment Tool](#) – tento nástroj slúži na nasadenie all-in-one inštalačných balíkov vytvorených pomocou nástroja <%PRODUCT%> Web Console. Ponúka tak pohodlný spôsob distribúcie ESET Management Agentu s bezpečnostným produktom ESET na klientske počítače v sieti.
- [ESET Business Account](#) – nový licenčný portál určený pre firemné produkty ESET vám umožňuje spravovať licencie. Bližšie informácie o aktivácii vášho produktu nájdete v kapitole [ESET Business Account](#), prípadne si môžete prečítať [používateľskú príručku](#) portálu ESET Business Account, kde nájdete podrobnejšie informácie o jeho používaní. Ak už máte prihlasovacie meno a heslo, ktoré vám boli vydané spoločnosťou ESET, môžete si ich skonvertovať na licenčný kľúč. Viac informácií nájdete v časti [Konvertovanie licenčných prihlasovacích údajov na licenčný kľúč](#).
- [ESET Enterprise Inspector \(EEI\)](#) – komplexný systém detekcie a reakcie na hrozby v koncových bodoch (Endpoint Detection and Response – EDR), ktorý zahŕňa funkcie, ako napr. detekcia incidentov, manažment a reakcia na incidenty, zozbieravanie údajov, detekcia indikátorov preukazujúcich narušenie zabezpečenia, detekcia anomálií, detekcia správania, detekcia porušenia pravidiel atď.

Pomocou nástroja ESET PROTECT Web Console môžete nasadiť bezpečnostné riešenia spoločnosti ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na vzdialených počítačoch.

**i** Viac informácií nájdete v [online používateľskej príručke pre ESET PROTECT](#).

# Predstavenie ESET PROTECT Cloud

ESET PROTECT CLOUD vám umožňuje spravovať v sieťovom prostredí produkty spoločnosti ESET nainštalované na pracovných staniciach a serveroch z jedného miesta bez potreby fyzického alebo virtuálneho servera, ktorý je však potrebný napríklad v prípade ESET PROTECT alebo ESET Security Management Center. Pomocou ESET PROTECT CLOUD Web Console môžete nainštalovať riešenia ESET, spravovať úlohy, vynucovať bezpečnostné politiky, monitorovať stav systému a rýchlo reagovať na problémy alebo hrozby na vzdialených počítačoch.

- [Podrobnejšie informácie nájdete v online používateľskej príručke pre ESET PROTECT CLOUD.](#)

## Vzdialená inštalácia

### Pred inštaláciou

^ [macOS 10.15 a staršie verzie](#)

Pred inštaláciou ESET Endpoint Antivirus for macOS na počítačoch s operačným systémom macOS 10.13 alebo novším povoľte rozšírenia jadra ESET. Na cieľových počítačoch s operačným systémom macOS 10.14 alebo novším povoľte aj úplný prístup k disku. Ak tieto možnosti povolíte až po dokončení inštalácie, používateľom sa dovedy budú zobrazovať upozornenia **Rozšírenie systému zablokované** a **Váš počítač je len čiastočne chránený**.

Pre vzdialené povolenie rozšírení jadra ESET a úplného prístupu k disku musí váš počítač byť zaregistrovaný na [MDM \(Mobile Device Management\) server](#), ako je napríklad Jamf.

### Povolenie systémových rozšírení ESET

Pre vzdialené povolenie rozšírení jadra na vašom zariadení:

OV prípade, že ako MDM používate Jamf, postupujte podľa krokov uvedených v [našom článku Databázy znalostí](#).

OV prípade, že používate odlišné MDM, [stiahnite .plist konfiguračný profil](#). Vygenerujte dve UUID pomocou ľubovoľného UUID generátora a použitím textového editora v stiahnutom konfiguračnom profile nahraďte reťazce **sem vložte UUID 1** a **sem vložte UUID 2** vami vygenerovanými UUID. Prostredníctvom MDM servera nasadte .plist súbor konfiguračného profilu. Aby si počítače prevzali konfiguráciu, musia byť zaregistrované na MDM server.

### Povolenie úplného prístupu k disku

Na počítačoch s macOS 10.14 sa v ESET Endpoint Antivirus for macOS po inštalácii zobrazí upozornenie **Váš počítač je len čiastočne chránený**. Pre zaistenie prístupu ku všetkým funkciám ESET Endpoint Antivirus for macOS a potlačenie zobrazovaného upozornenia je potrebné, aby ste povolili **Úplný prístup k disku** pre ESET Endpoint Antivirus for macOS ešte pred začatím inštalácie produktu. Pre vzdialené povolenie **Úplného prístupu k disku**:

OV prípade, že ako MDM používate Jamf, postupujte podľa krokov uvedených v [našom článku Databázy znalostí](#).

OV prípade, že používate inú službu MDM, [stiahnite .plist konfiguračný súbor](#). Vygenerujte dve UUID pomocou ľubovoľného UUID generátora a použitím textového editora v stiahnutom konfiguračnom profile



nahradte reťazce sem vložte UUID 1 a sem vložte UUID 2 vami vygenerovanými UUID.  
Prostredníctvom MDM servera nasadte .plist súbor konfiguračného profilu. Aby si počítače prevzali konfiguráciu, musia byť zaregistrované na MDM server.

## ^ macOS Big Sur (11)

Pred inštaláciou ESET Endpoint Antivirus for macOS na počítačoch s operačným systémom macOS Big Sur je potrebné najskôr povoliť systémové rozšírenia ESET a tiež úplný prístup k disku. Ak tieto možnosti povolíte až po dokončení inštalácie, používateľom sa dovedy budú zobrazovať upozornenia **Rozšírenie systému zablokované a Váš počítač je len čiastočne chránený**. Rozšírenie systému je možné povoliť vzdialene len pred spustením inštalácie ESET Endpoint Antivirus for macOS.

Pre vzdialené povolenie systémových rozšírení ESET a úplného prístupu k disku musí váš počítač byť zaregistrovaný na [MDM \(Mobile Device Management\) server](#), ako je napríklad Jamf.

### Povolenie systémových rozšírení ESET

Pre vzdialené povolenie systémových rozšírení na vašom zariadení:

OV prípade, že ako MDM používate Jamf, postupujte podľa krokov uvedených v [našom článku Databázy znalostí](#).

OV prípade, že používate odlišné MDM, [stiahnite .plist konfiguračný profil](#). Prostredníctvom MDM servera nasadte .plist súbor konfiguračného profilu. Aby si počítače prevzali konfiguráciu, musia byť zaregistrované na MDM server. Pri vytváraní vlastného konfiguračného profilu použite nižšie uvedené nastavenia:

Identifikátor tímu (TeamID)	P8DQRXPVLP
Identifikátor balíka (BundleID)	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

### Povolenie úplného prístupu k disku

Pre vzdialené povolenie **úplného prístupu k disku**:

OV prípade, že ako MDM používate Jamf, postupujte podľa krokov uvedených v [našom článku Databázy znalostí](#).

OV prípade, že používate inú službu MDM, [stiahnite .plist konfiguračný súbor](#). Prostredníctvom MDM servera nasadte .plist súbor konfiguračného profilu. Aby si počítače prevzali konfiguráciu, musia byť zaregistrované na MDM server. Pri vytváraní vlastného konfiguračného profilu použite nižšie uvedené nastavenia:

ESET Endpoint Antivirus	
Identifikátor	com.eset.eea.6
Typ identifikátora	bundleID
Požiadavka na kód	identifier "com.eset.eea.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
Aplikácia alebo služba	SystemPolicyAllFiles

Prístup	Allow
---------	-------

<b>ESET Endpoint Antivirus &amp; ESET Endpoint Security</b>	
Identifikátor	com.eset.devices
Typ identifikátora	bundleID
Požiadavka na kód	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRPVLP
Aplikácia alebo služba	SystemPolicyAllFiles
Prístup	Allow

<b>ESET Endpoint Antivirus &amp; ESET Endpoint Security</b>	
Identifikátor	com.eset.endpoint
Typ identifikátora	bundleID
Požiadavka na kód	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRPVLP
Aplikácia alebo služba	SystemPolicyAllFiles
Prístup	Allow

## Inštalácia

Pred spustením inštalácie si môžete vytvoriť balík na vzdialenú inštaláciu produktu ESET Endpoint Antivirus for macOS s prednastavenou konfiguráciou, ktorý môžete následne nasadiť prostredníctvom nástroja ESET PROTECT alebo preferovaného MDM.

- [Vytvorenie balíka na vzdialenú inštaláciu](#)

Program ESET Endpoint Antivirus for macOS môžete nainštalovať vzdialene použitím úlohy **Inštalácia softvéru** vytvorenej v konzole ESET na vzdialenú správu:

- [Klientska úloha na inštaláciu softvéru v ESET PROTECT](#)
- [Klientska úloha na inštaláciu softvéru v ESET Security Management Center](#)

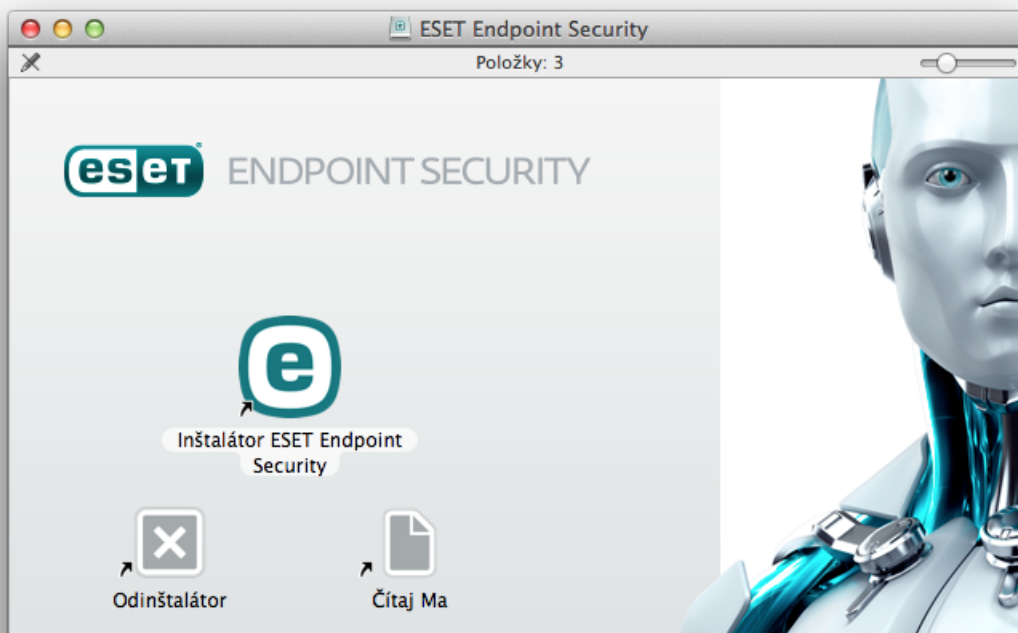
## Po inštalácii

Používateľom sa zobrazí nasledujúce upozornenie: **Aplikácia „ESET Endpoint Antivirus for macOS“ chce filtrovať obsah zo siete.** Keď sa používateľom zobrazí toto upozornenie, je potrebné kliknúť na tlačidlo **Povoliť**. V prípade zvolenia možnosti **Nepovoliť** nebude ochrana prístupu na web fungovať.

## Vytvorenie balíka na vzdialenú inštaláciu

## Vytvorenie inštalačného balíka na nasadenie prostredníctvom Apple Remote Desktop

1. Z webovej stránky spoločnosti ESET si stiahnite bežný inštalačný balík:  
[ESET Endpoint Antivirus for macOS](#)
2. Inštalátor produktu ESET Endpoint Antivirus for macOS spustíte dvojitém kliknutím na stiahnutý súbor.



1. Kliknite na **Inštalovať** ESET Endpoint Antivirus for macOS.
2. Po zobrazení výzvy kliknite na **Povoliť**, aby mohol inštalátor overiť, či je možné softvér nainštalovať.
3. Kliknite na tlačidlo **Pokračovať**. Pri vytváraní balíka na vzdialenú inštaláciu sa ESET Endpoint Antivirus for macOS na váš počítač nenainštaluje.
4. Skontrolujte, či spĺňate systémové požiadavky a kliknite na **Pokračovať**.
5. Prečítajte si licenčnú dohodu a ak súhlasíte s uvedenými podmienkami, kliknite na **Pokračovať** → **Súhlasím**.
6. V kroku **Režim inštalácie** vyberte možnosť **Vzdialená**.
7. Zvoľte programové súčasti, ktoré chcete nainštalovať. Predvolene sú vybrané všetky komponenty. Kliknite na tlačidlo **Pokračovať**.
8. V kroku **Proxy server** vyberte možnosť, ktorá zodpovedá vášmu internetovému pripojeniu. Ak si nie ste istý, použite predvolené systémové nastavenia. Následne kliknite na **Ďalej**. V prípade, že používate proxy server, v ďalšom kroku budete vyzvaný na zadanie adresy proxy servera, používateľského mena a hesla.
9. Vyberte, kto bude môcť meniť konfiguráciu programu. Iba oprávnení používatelia a skupiny môžu upravovať

nastavenia. Predvolene má toto oprávnenie skupina správcov. Pomocou možnosti **Zobraziť všetkých používateľov** alebo **Zobraziť všetky skupiny** si zobrazíte všetkých virtuálnych používateľov a skupiny, ako sú programy a procesy.

10. Na cieľovom počítači podľa vlastných preferencií môžete zapnúť ESET LiveGrid.

11. Rovnako môžete na cieľovom počítači zapnúť detekciu potenciálne nechcených aplikácií.

12. Vyberte režim firewallu:

**Automatický režim** – prednastavený režim. Je vhodný pre používateľov, ktorí potrebujú jednoduché a pohodlné používanie firewallu bez potreby vytvárania pravidiel. Povoľuje štandardnú odchádzajúcu komunikáciu z daného systému smerom do siete a blokuje všetky nevyžiadané spojenia prichádzajúce zo siete. Môžete tiež vytvárať vlastné používateľské pravidlá.

**Interaktívny režim** – umožňuje nastaviť si firewall na mieru podľa vašich požiadaviek. V prípade zistenia akejkoľvek komunikácie, na ktorú nie je možné aplikovať žiadne existujúce pravidlo, je používateľovi zobrazené informačné okno o zachytení neznámeho spojenia. Následne je možné túto komunikáciu povoliť alebo zamietnuť, pričom toto rozhodnutie môže byť uložené ako nové pravidlo firewallu. V prípade vytvorenia pravidla bude každá komunikácia tohto typu v budúcnosti povolená alebo zablokovaná podľa daného pravidla.

13. Uložte inštalačný súbor do svojho počítača. Ak ste už niekedy predtým v predvolenom umiestnení vytvárali inštalačný balík, vyberte iné umiestnenie cieľového priečinka alebo pred pokračovaním predošlé inštalačné súbory odstráňte. Týmto sa dokončí prvá fáza vzdialenej inštalácie. Lokálny inštalátor sa ukončí a následne v cieľovom priečinku vytvorí súbory na vzdialenú inštaláciu.

Súbory na vzdialenú inštaláciu zahŕňajú:

- *esets\_setup.dat* – údaje nastavení, ktoré ste zadali v sekcii Nastavenia v rámci inštalátora.
- *program\_components.dat* – informácie o vybraných programových súčiastiach. (Tento súbor je voliteľný a vytvorí sa iba v prípade, že sa rozhodnete nenainštalovať niektoré súčasti ESET Endpoint Antivirus for macOS.)
- *esets\_remote\_install.pkg* – balík na vzdialenú inštaláciu
- *esets\_remote\_uninstall.sh* – skript na vzdialené odinštalovanie

## Nainštalujte si Apple Remote Desktop

1. Spustíte aplikáciu Apple Remote Desktop a pripojte sa k cieľovému počítaču. Viac informácií nájdete v [dokumentácii pre Apple Remote Desktop](#).

2. Pomocou funkcie **Copy filer or folder** (Kopírovať súbor alebo priečinok) v aplikácii Apple Remote Desktop skopírujte nižšie uvedené súbory do priečinka */tmp* na cieľovom počítači:

Ak chcete nainštalovať všetky programové súčasti, skopírujte:

- *esets\_setup.dat*

Ak nechcete nainštalovať všetky programové súčasti, skopírujte:

- *esets\_setup.dat*

- *product\_components.dat*

3. Balík *esets\_remote\_install.pkg* nainštalujte na cieľový počítač použitím príkazu **Install packages**

(Nainštalovať balíky).

## Vzdialené odinštalovanie cez Apple Remote Desktop

1. Spustíte aplikáciu Apple Remote Desktop a pripojíte sa k cieľovému počítaču. Viac informácií nájdete v [dokumentácii pre Apple Remote Desktop](#).
2. Pomocou funkcie **Copy file or folder** (Kopírovať súbor alebo priečinok) v aplikácii Apple Remote Desktop skopírujte skript `esets_remote_uninstall.sh` do priečinka `/tmp` na cieľovom počítači.
3. V aplikácii Apple Remote Desktop spustíte na cieľovom počítači pomocou funkcie **Send a UNIX shell command** nasledujúci príkaz:

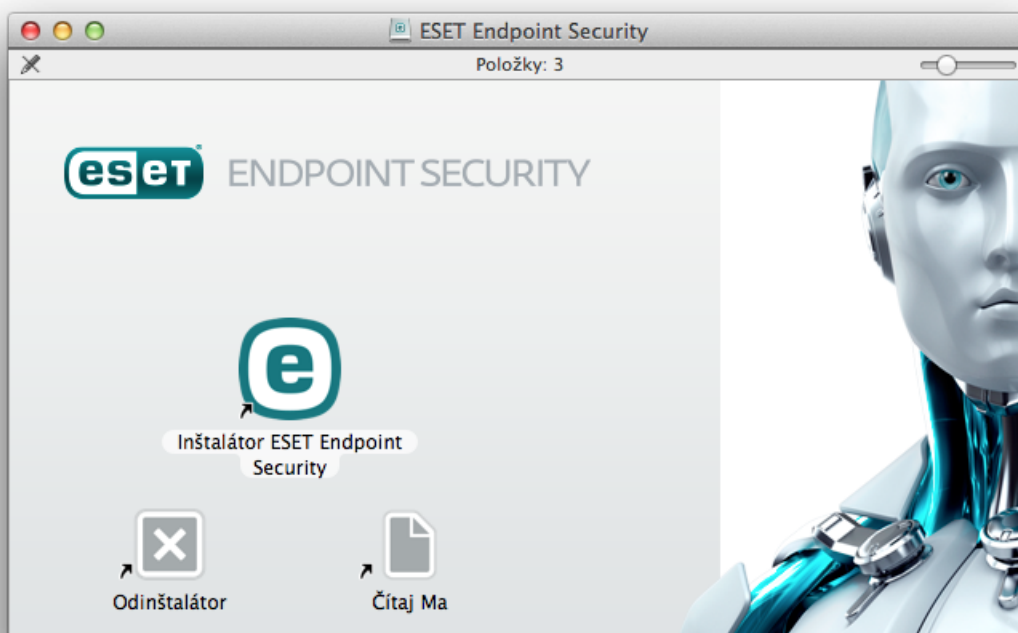
```
/tmp/esets_remote_uninstall.sh
```

Po dokončení procesu odinštalácie sa na cieľovom počítači zobrazí výstup konzoly Apple Remote Desktop.

## Inštalácia

Sprievodca inštaláciou vás prevedie základnými nastaveniami. Podrobný návod nájdete [v tomto článku Databázy znalostí spoločnosti ESET](#).

1. Inštalátor produktu ESET Endpoint Antivirus for macOS spustíte dvojitém kliknutím na stiahnutý súbor.



1. Pre spustenie inštalácie kliknite na tlačidlo **Inštalovať** ESET Endpoint Antivirus for macOS.

## Inštalácia z .pkg súboru

**!** Počas inštalácie a prvého spustenia produktu ESET pre macOS je potrebné, aby ste mali na svojom počítači internetové pripojenie pre overenie dôveryhodnosti systémových rozšírení ESET zo strany Apple.

2. Po zobrazení výzvy kliknite na **Povoliť**, aby mohol inštalátor overiť, či je možné softvér nainštalovať.
3. V prípade, že ste tak ešte neurobili, odstráňte zo systému iné bezpečnostné aplikácie, ako je antivírus, antispam alebo firewall. Ak v počítači žiadny takýto softvér nemáte, kliknite na **Pokračovať**.
4. Skontrolujte, či spĺňate systémové požiadavky a kliknite na **Pokračovať**.
5. Prečítajte si licenčnú dohodu a ak súhlasíte s uvedenými podmienkami, kliknite na **Pokračovať** → **Súhlasím**.
6. Vyberte typ inštalácie, ktorý vám vyhovuje.
  - [Typická inštalácia](#)
  - [Pokročilá inštalácia](#)
  - [Vzdialená inštalácia](#)

## Kontrola verzie

**i** Počas prvej fázy inštalácie inštalátor skontroluje, či nie je na internete dostupná novšia verzia produktu. Ak je k dispozícii novšia verzia, inštalátor vám ponúkne možnosť si túto verziu stiahnuť a následne pokračovať v inštaláčnom procese.

# Typická inštalácia

Typická inštalácia nainštaluje produkt s odporúčanými nastaveniami, ktoré sú vhodné pre väčšinu používateľov. Tieto nastavenia poskytujú maximálnu úroveň ochrany v kombinácii s nízkymi nárokmi na systémové prostriedky. Typická inštalácia je predvolenou voľbou a odporúčame ju použiť v prípade, že nemáte žiadne špecifické požiadavky ohľadom nastavení programu.

1. V okne **ESET LiveGrid** vyberte preferovanú možnosť a kliknite na **Pokračovať**. Ak sa neskôr rozhodnete, že chcete toto nastavenie zmeniť, prejdite do **Nastavení LiveGrid**. Viac informácií o technológii ESET LiveGrid nájdete v našom [slovníku pojmov](#).
2. V okne **Potenciálne nechcené aplikácie** vyberte preferovanú možnosť (prečítajte si [Čo je potenciálne nechcená aplikácia?](#)) a kliknite na **Pokračovať**. Ak sa neskôr rozhodnete, že chcete toto nastavenie zmeniť, použite **Rozšírené nastavenia**.
3. Kliknite na možnosť **Inštalovať**. Ak vás k tomu systém vyzve, zadajte svoje heslo do macOS a kliknite na **Inštalovať softvér**.

Po inštalácii produktu ESET Endpoint Antivirus for macOS:

## macOS Big Sur (11)

1. [Povoľte rozšírenia systému](#).

2. [Povoľte úplný prístup k disku.](#)

3. Povoľte programu ESET pridať nastavenia proxy. Zobrazí sa vám nasledujúce upozornenie: **Aplikácia „ESET Endpoint Antivirus for macOS“ chce filtrovať obsah zo siete.** Keď sa vám zobrazí toto upozornenie, kliknite na tlačidlo **Povoľiť**. Ak kliknete na **Nepovoľiť**, ochrana prístupu na web nebude fungovať.



### [macOS 10.15 a staršie verzie](#)

1. Na počítači so systémom macOS 10.13 alebo novším vám operačný systém zobrazí notifikáciu **Rozšírenie systému zablokované** a program ESET Endpoint Antivirus for macOS zobrazí upozornenie **Váš počítač nie je chránený**. Aby ste mohli využívať všetky funkcie programu ESET Endpoint Antivirus for macOS, je potrebné na vašom zariadení povoliť rozšírenia jadra. Pre povolenie rozšírení jadra prejdite na vašom zariadení do časti **Systémové nastavenia > Bezpečnosť a súkromie** a kliknite na možnosť **Povoľiť** pre povolenie systémového softvéru od výrobcu **ESET, spol. s r. o.** Podrobnejšie informácie nájdete [v tomto článku Databázy znalostí spoločnosti ESET](#).

2. Na počítači so systémom macOS 10.14 alebo novším vám program ESET Endpoint Antivirus for macOS zobrazí upozornenie na to, že váš počítač je chránený len čiastočne. Aby ste mohli využívať všetky funkcie programu ESET Endpoint Antivirus for macOS, je potrebné pre ESET Endpoint Antivirus for macOS povoliť **Úplný prístup k disku**. Prejdite na vašom zariadení do časti **Systémové nastavenia > Bezpečnosť a súkromie** a následne na kartu **Ochrana súkromia**, kde vyberte možnosť **Úplný prístup k disku**. Pre povolenie úprav kliknite na ikonu zámku. Následne kliknite na ikonu znamienka plus (+) a vyberte aplikáciu ESET Endpoint Antivirus for macOS. Systém vám zobrazí upozornenie o potrebe reštartu počítača. Kliknite na možnosť **Neskôr** a počítač ešte nereštartujte. V okne upozornenia programu ESET Endpoint Antivirus for macOS kliknite na možnosť **Začať znova** alebo reštartujte váš počítač. Podrobnejšie informácie nájdete [v tomto článku Databázy znalostí spoločnosti ESET](#).

Po nainštalovaní programu ESET Endpoint Antivirus for macOS vám odporúčame spustiť kontrolu počítača na prítomnosť malvéru. V hlavnom okne programu kliknite na možnosť **Kontrola počítača > Smart kontrola**. Viac informácií nájdete v kapitole [Manuálna kontrola počítača](#).

## Pokročilá inštalácia

Pokročilá inštalácia je určená pre skúsených používateľov, ktorí si chcú upraviť rozšírené nastavenia programu podľa svojich potrieb už počas procesu inštalácie.

### • Programové súčasti

ESET Endpoint Antivirus for macOS umožňuje inštalovať produkt bez niektorých vybraných programových súčastí (napr. bez Webovej a e-mailovej ochrany). Zrušte označenie vybranej položky v zozname, ak si neželáte, aby bola nainštalovaná ako súčasť produktu.

### • Proxy server

Ak používate proxy server, označte možnosť **Pri pripojení používam proxy server** a v nasledujúcom kroku môžete nastaviť jeho parametre. Do poľa **Adresa** zadajte IP adresu alebo URL adresu vášho proxy servera. Do poľa **Port** zadajte číslo portu, na ktorom proxy server prijíma spojenia (predvolene 3128). Ak proxy server vyžaduje pre prístup overenie, je potrebné správne vyplniť polia **Meno** a **Heslo** pre umožnenie pripojenia k proxy serveru. Ak nepoužívate proxy server, označte možnosť **Pri pripojení nepoužívam proxy server**. Ak si nie ste istý, či používate proxy server, označte možnosť **Chcem použiť systémové nastavenia (Odporúčané)**.

### • Oprávnenia



Máte možnosť nastaviť privilegovaných používateľov alebo skupiny používateľov, ktorí budú mať povolenie upravovať nastavenia programu. Zo zoznamu vľavo vyberte používateľov a potom ich pomocou tlačidla **Pridať** pridajte do zoznamu **Oprávnených používateľov** v pravej časti okna. Pre zobrazenie všetkých systémových používateľov zvolte možnosť **Zobraz všetkých používateľov**. Ak ponecháte zoznam oprávnených používateľov prázdny, všetci používatelia budú môcť vykonávať zmeny v programe.

- **ESET LiveGrid**

Viac informácií o technológii ESET LiveGrid nájdete v našom [slovníku pojmov](#).

- **Potenciálne nechcené aplikácie**

Viac informácií o potenciálne nechcených aplikáciách nájdete v [slovníku pojmov](#).

Po inštalácii produktu ESET Endpoint Antivirus for macOS:

## macOS Big Sur (11)

1. [Povoľte rozšírenia systému](#).
2. [Povoľte úplný prístup k disku](#).
3. Povoľte programu ESET pridať nastavenia proxy. Zobrazí sa vám nasledujúce upozornenie: **Aplikácia „ESET Endpoint Antivirus for macOS“ chce filtrovať obsah zo siete**. Keď sa vám zobrazí toto upozornenie, kliknite na tlačidlo **Povoliť**. Ak kliknete na **Nepovoliť**, ochrana prístupu na web nebude fungovať.



### [macOS 10.15 a staršie verzie](#)

1. Na počítači so systémom macOS 10.13 alebo novším vám operačný systém zobrazí notifikáciu **Rozšírenie systému zablokované** a program ESET Endpoint Antivirus for macOS zobrazí upozornenie **Váš počítač nie je chránený**. Aby ste mohli využívať všetky funkcie programu ESET Endpoint Antivirus for macOS, je potrebné na vašom zariadení povoliť rozšírenia jadra. Pre povolenie rozšírení jadra prejdite na vašom zariadení do časti **Systémové nastavenia > Bezpečnosť a súkromie** a kliknite na možnosť **Povoliť** pre povolenie systémového softvéru od výrobcu **ESET, spol. s r. o.** Podrobnejšie informácie nájdete [v tomto článku Databázy znalostí spoločnosti ESET](#).
2. Na počítači so systémom macOS 10.14 alebo novším vám program ESET Endpoint Antivirus for macOS zobrazí upozornenie na to, že váš počítač je chránený len čiastočne. Aby ste mohli využívať všetky funkcie programu ESET Endpoint Antivirus for macOS, je potrebné pre ESET Endpoint Antivirus for macOS povoliť **Úplný prístup k disku**. Prejdite na vašom zariadení do časti **Systémové nastavenia > Bezpečnosť a súkromie** a následne na kartu **Ochrana súkromia**, kde vyberte možnosť **Úplný prístup k disku**. Pre povolenie úprav kliknite na ikonu zámku. Následne kliknite na ikonu znamienka plus (+) a vyberte aplikáciu ESET Endpoint Antivirus for macOS. Systém vám zobrazí upozornenie o potrebe reštartu počítača. Kliknite na možnosť **Neskôr** a počítač ešte nereštartujte. V okne upozornenia programu ESET Endpoint Antivirus for macOS kliknite na možnosť **Začať znova** alebo reštartujte váš počítač. Podrobnejšie informácie nájdete [v tomto článku Databázy znalostí spoločnosti ESET](#).

Po nainštalovaní programu ESET Endpoint Antivirus for macOS spustíte kontrolu počítača na prítomnosť malvéru. V hlavnom okne programu kliknite na možnosť **Kontrola počítača > Smart kontrola**. Viac informácií nájdete v kapitole [Manuálna kontrola počítača](#).



# Lokálne povolenie rozšírení systému

V systéme macOS 11 (Big Sur) boli rozšírenia jadra nahradené systémovými rozšíreniami. Pred načítaním nových systémových rozšírení tretích strán sa vyžaduje súhlas používateľa.

Po inštalácii ESET Endpoint Antivirus for macOS na počítači so systémom macOS Big Sur (11) alebo novším vám operačný systém zobrazí notifikáciu Rozšírenie systému zablokované a program ESET Endpoint Antivirus for macOS zobrazí upozornenie Váš počítač nie je chránený. Aby ste mohli využívať všetky funkcie programu ESET Endpoint Antivirus for macOS, je potrebné na vašom zariadení povoliť rozšírenia systému.

## Aktualizácia z predošlej verzie macOS na Big Sur.



Ak ste už nainštalovali ESET Endpoint Antivirus for macOS a chystáte sa aktualizovať systém na macOS Big Sur, bude potrebné po aktualizácii manuálne povoliť rozšírenia jadra ESET. Vyžaduje sa fyzický prístup ku klientskemu počítaču, keďže pri vzdialenom prístupe je tlačidlo Povoľiť vypnuté.

Pri inštalácii produktu ESET na macOS Big Sur alebo novšiu verziu systému musíte rozšírenia systému pre produkt ESET povoliť manuálne. Vyžaduje sa fyzický prístup ku klientskemu počítaču, keďže pri vzdialenom prístupe je táto možnosť vypnutá.

## Manuálne povolenie rozšírení systému

1. Kliknite na **Otvoriť systémové nastavenia** alebo **Otvoriť nastavenia bezpečnosti**.
2. Pre povolenie zmien v okne nastavení kliknite na ikonu zámku vľavo dole.
3. Použite funkciu Touch ID alebo kliknite na **Použiť heslo** a zadajte svoje používateľské meno a heslo a potom kliknite na možnosť **Odomknúť**.
4. Kliknite na tlačidlo **Detaily**.
5. Vyberte všetky tri možnosti ESET Endpoint Antivirus for macOS.**app**.
6. Kliknite na **OK**.

Podrobný návod nájdete v našom [článku Databázy znalostí](#). (Obsah nemusí byť dostupný vo všetkých jazykoch.)

## Lokálne povolenie úplného prístupu k disku

Na počítačoch s macOS 10.14 dostanete od ESET Endpoint Antivirus for macOS upozornenie **Váš počítač je len čiastočne chránený**. Pre prístup ku všetkým funkciám ESET Endpoint Antivirus for macOS je potrebné, aby ste povolili **Úplný prístup k disku** pre ESET Endpoint Antivirus for macOS.

1. V dialógovom okne upozornenia kliknite na možnosť **Otvoriť systémové nastavenia**.
2. Pre povolenie zmien v okne nastavení kliknite na ikonu zámku vľavo dole.
3. Použite funkciu Touch ID alebo kliknite na **Použiť heslo** a zadajte svoje používateľské meno a heslo a potom kliknite na možnosť **Odomknúť**.
4. Zo zoznamu vyberte ESET Endpoint Antivirus for macOS.**app**.

5. Zobrazí sa oznámenie o reštarte ESET Endpoint Antivirus for macOS. Kliknite na tlačidlo Neskôr.
6. Zo zoznamu vyberte možnosť **Rezidentná ochrana súborového systému** od spoločnosti ESET.


### Rezidentná ochrana súborového systému nie je v zozname

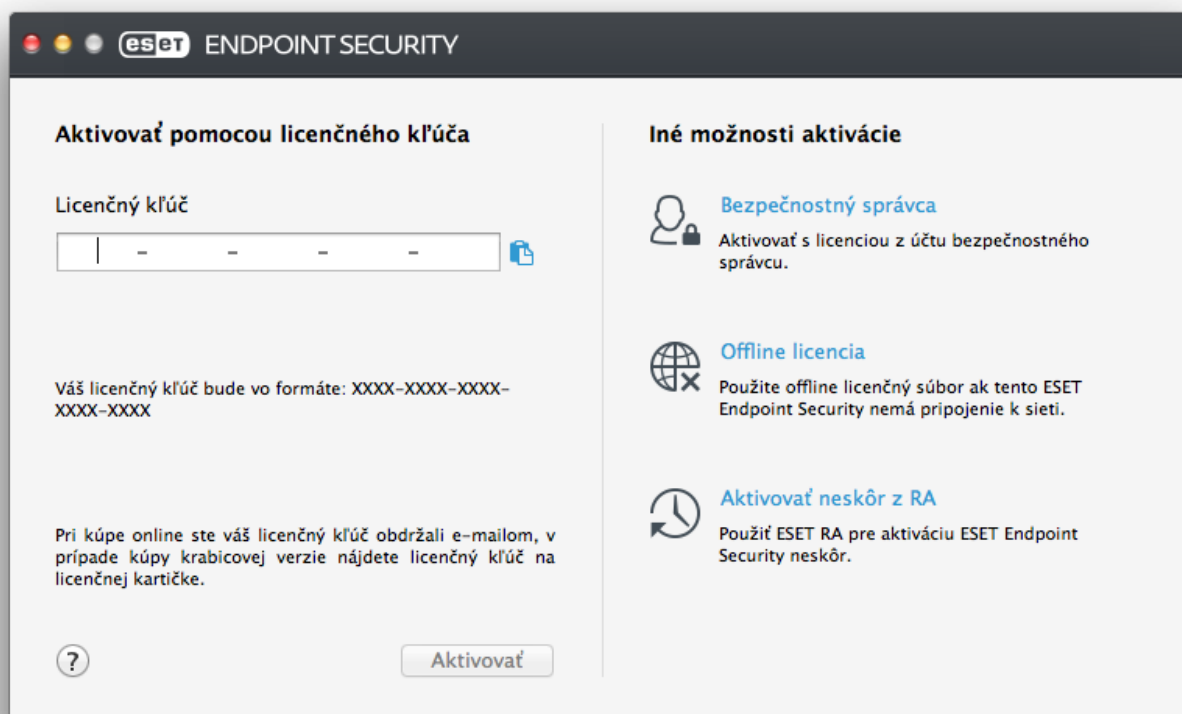
- ! Ak v zozname nie je uvedená možnosť **Rezidentná ochrana súborového systému**, musíte [povoliť systémové rozšírenia pre váš produkt ESET](#).

7. V dialógovom okne upozornenia produktu ESET Endpoint Antivirus for macOS kliknite na tlačidlo Spustiť znova alebo reštartujte počítač. Podrobnejšie informácie nájdete v našom [článku Databázy znalostí](#).

## Aktivácia produktu

Po ukončení inštalácie sa zobrazí dialógové okno s výzvou na aktiváciu produktu. Existuje niekoľko možností, ako aktivovať produkt. Dostupnosť nižšie uvedených metód aktivácie sa môže líšiť v závislosti od krajiny zákazníka, ako aj spôsobu distribúcie produktu (CD/DVD, webová stránka spoločnosti ESET a pod.).

Pre aktiváciu ESET Endpoint Antivirus for macOS priamo z programu kliknite na ikonu  zobrazenú na hornej lište systému macOS (v pravom hornom rohu obrazovky) a následne zvolte možnosť **Aktivácia produktu**. Váš produkt tiež môžete aktivovať z hlavného okna programu v sekcii **Pomocník > Správa licencií** alebo v sekcii **Stav ochrany > Aktivovať produkt**.



Môžete použiť nasledujúce metódy aktivácie produktu ESET Endpoint Antivirus for macOS:

- **Aktivovať pomocou licenčného kľúča** – jedinečný reťazec znakov vo formáte XXXX-XXXX-XXXX-XXXX-XXXX, ktorý sa používa na identifikáciu vlastníka licencie a aktiváciu licencie. Licenčný kľúč nájdete v e-mailovej správe, ktorú ste dostali od spoločnosti ESET po zakúpení produktu, alebo na licenčnej karte, ktorá bola súčasťou balenia produktu.
- **Bezpečnostný správca** – účet vytvorený na [portáli ESET License Administrator](#) s prihlasovacími údajmi (e-mailová adresa + heslo). Táto metóda vám umožní spravovať viacero licencií z jedného miesta.
- **Offline licencia** – automaticky vygenerovaný offline licenčný súbor s informáciami o vašej licencií. Offline licenčný súbor je generovaný pomocou portálu ESET License Administrator a používa sa, keď sa aplikácia nemôže pripojiť na licenčné servery v danej sieti.

Aktiváciu je možné vykonať aj neskôr, ak je váš počítač súčasťou spravovanej siete a správca siete plánuje produkt na vašom počítači aktivovať použitím nástroja ESET Remote Administrator.

### Tichá aktivácia

- i Prostredníctvom ESET Remote Administrator je možné klientske počítače aktivovať vzdialene v tzv. tichom režime (aktivácia prebieha na pozadí, bez oznámení) pomocou licencie sprístupnenej správcom.

ESET Endpoint Antivirus for macOS vo verzii 6.3.85.0 (a v novších verziách) vám umožňuje produkt aktivovať použitím Terminálu. Stačí použiť nasledujúci príkaz:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Nahradte v príkaze časť XXXX-XXXX-XXXX-XXXX-XXXX licenčným kľúčom, ktorý už bol použitý na aktivovanie programu ESET Endpoint Antivirus for macOS alebo bol zaregistrovaný na portáli [ESET License Administrator](#). Pri úspešnej aktivácii príkaz vráti stav „OK“ a pri zlyhaní aktivácie chybu.

## Odinštalovanie

ESET Endpoint Antivirus for macOS odinštalujete jednou z nasledujúcich možností:

- otvorte inštalačný súbor ESET Endpoint Antivirus for macOS (.dmg) a dvakrát kliknite na ikonu **Odinštalátor**,
- otvorte okno aplikácie **Finder**, kliknite na **Aplikácie** (alebo **Applications**), stlačte CTRL a kliknite na ikonu ESET Endpoint Antivirus for macOS. Z kontextového menu vyberte možnosť **Zobraziť obsah balíka** (alebo **Show Package Contents**). Otvorte adresár **Contents > Helpers** a dvakrát kliknite na ikonu **Uninstaller**.

### Odinštalovanie

- ! V priebehu odinštalovania bude nutné viackrát zadať heslo správcu, aby bolo možné ESET Endpoint Antivirus for macOS kompletne odstrániť.

## Stručný prehľad


Hlavné okno programu ESET Endpoint Antivirus for macOS je rozdelené na dve časti. Časť vpravo zobrazuje informácie, ktoré podliehajú voľbe vybranej v hlavnom menu vľavo.

Tu je zoznam možností, ktoré môžete nájsť v hlavnom menu:

- **Stav ochrany** – poskytuje informácie o stave ochrany vášho počítača a stave webovej a e-mailovej ochrany.
- **Kontrola počítača** – umožňuje nastaviť a spustiť [Manuálnu kontrolu počítača](#).
- **Aktualizácia** – zobrazí informácie týkajúce sa aktualizácií modulov.
- **Nastavenia** – vyberte si túto možnosť, ak chcete zmeniť nastavenia úrovne zabezpečenia vášho počítača.
- **Nástroje** – slúži na prístup k [Protokolom](#), [Plánovaču](#), [Karanténe](#) a [Spusteným procesom](#).
- **Pomocník** – poskytuje prístup k stránkam pomocníka, databáze znalostí spoločnosti ESET, webovému formuláru slúžiacemu na kontaktovanie Technickej podpory a zobrazuje informácie o produkte a licencií.

## Klávesové skratky

Pri práci s programom ESET Endpoint Antivirus for macOS môžete použiť nasledujúce klávesové skratky:

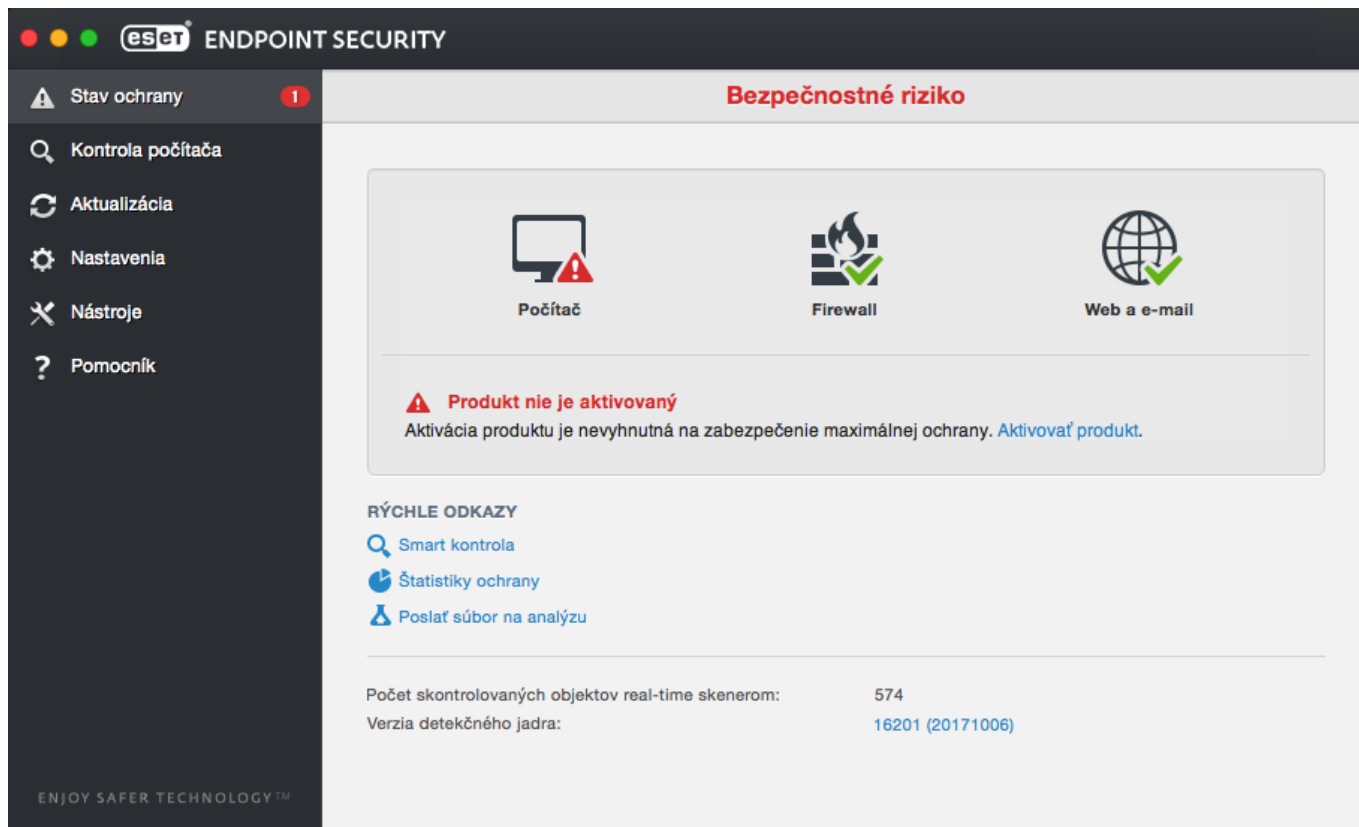
- *cmd+,* – zobrazí pokročilé nastavenia programu,
- *cmd+O* – zmení veľkosť hlavného okna programu ESET Endpoint Antivirus for macOS na predvolenú veľkosť a presunie ho do stredu obrazovky,
- *cmd+Q* – schová hlavné GUI okno ESET Endpoint Antivirus for macOS. Môžete ho znova otvoriť kliknutím na ikonu ESET Endpoint Antivirus for macOS  na hornej lište (Menu Bar) systému macOS,
- *cmd+W* – zavrie hlavné okno ESET Endpoint Antivirus for macOS.

Nasledujúce klávesové skratky fungujú iba v prípade, že povolíte možnosť **Používať štandardné menu** v sekcii **Nastavenia > Zobrazíť pokročilé nastavenia... > Rozhranie**:

- *cmd+alt+L* – otvorí sekciu **Protokoly**,
- *cmd+alt+S* – otvorí sekciu **Plánovač**,
- *cmd+alt+Q* – otvorí sekciu **Karanténa**.

## Kontrola funkčnosti programu

Pre zobrazenie stavu ochrany kliknite na položku **Stav ochrany** v hlavnom menu programu. V pravej časti okna sa zobrazí súhrn stavu fungovania jednotlivých modulov ESET Endpoint Antivirus for macOS.



## Čo robiť, ak program nepracuje správne

Ak zapnuté moduly fungujú správne, majú priradenú zelenú ikonu. Ak nie, zobrazí sa vedľa daného modulu červená ikona s výkričníkom alebo oranžová ikona oznámenia. Ďalšie informácie o module spolu s navrhovaným riešením problému sa zobrazia v hlavnom okne programu. Pre zmenu stavu jednotlivých modulov kliknite na modrý odkaz zobrazený pod správou s oznámením o stave modulu.

Ak sa vám nepodarí vyriešiť problém pomocou navrhovaných riešení, môžete vyhľadať riešenie v [Databáze znalostí spoločnosti ESET](#) alebo kontaktovať [Technickú podporu ESET](#). Pracovníci Technickej podpory rýchlo odpovedia na vaše otázky a pomôžu vám vyriešiť váš problém s ESET Endpoint Antivirus for macOS.

## Ochrana počítača

Parametre ochrany počítača môžete konfigurovať v sekcii **Nastavenia > Počítač**, kde je zobrazený stav modulov **Rezidentná ochrana súborového systému**. Pre vypnutie niektorého z modulov prepnete tlačidlo modulu do polohy **VYP (VYPNUTÁ)**. Toto ale môže znížiť úroveň ochrany vášho počítača. Podrobné nastavenia niektorého z modulov otvoríte kliknutím na tlačidlo **Nastavenia...**

## Antivírusová a antispyvérová ochrana

Antivírusová ochrana chráni systém pred útokmi a manipuláciou so súborami, ktoré predstavujú potenciálnu hrozbu. Ak bola zdetegovaná hrozba obsahujúca škodlivý kód, antivírusový modul ju dokáže odstrániť blokovaním a vyliečením, vymazaním alebo presunutím do karantény.

# Všeobecné

V časti **Všeobecné (Nastavenia > Zobrazíť pokročilé nastavenia... > Všeobecné)** môžete povoliť detekciu nasledujúcich typov aplikácií:



- **Potenciálne nechcené aplikácie** – aj keď tento softvér nemusí byť nevyhnutne škodlivý, môže negatívne ovplyvniť výkon vášho počítača. Takéto aplikácie sa zvyčajne inštalujú až po súhlase používateľa. Ak máte takéto aplikácie na vašom počítači, systém sa správa odlišne (v porovnaní s tým, ako pracoval pred nainštalovaním týchto aplikácií). Jednou z najvýraznejších zmien je zobrazovanie tzv. vyskakovacích (pop-up) okien, ale tiež spúšťanie a prevádzka skrytých procesov, zvýšené zaťaženie systémových zdrojov, zmeny vo výsledkoch vyhľadávania a komunikácia aplikácií so vzdialenými servermi.
- **Potenciálne nebezpečné aplikácie** – sem spadajú komerčné aplikácie a legítimný softvér, ako sú napr. nástroje pre vzdialený prístup. V prípade inštalácie bez súhlasu používateľa môžu byť tieto aplikácie útočnými zneužitými. Detekcia týchto aplikácií je na základe predvolených nastavení vypnutá.
- **Podozrivé aplikácie** – programy prevažne nakazené malvérom, ktoré sú komprimované pomocou packerov alebo protektorov (packerov, ktorých účelom je zabrániť reverznému inžinierstvu). Snahou týchto podozrivých aplikácií je, aby sa vyhli detekcii. Packer je spustiteľný samorozbalovací súbor, ktorý v sebe obsahuje niekoľko druhov malvéru v jednom balíku. Medzi najznámejšie packery patria napr. UPX, PE\_Compact, PKLite a ASPack. Ten istý malvér môže byť detegovaný rôzne, pretože môže byť komprimovaný vždy pomocou iného packera. Packery majú schopnosť mutácie vlastných „signatúr“, preto je takýto malvér ťažšie odhaliť a odstrániť.

[Vylúčenia z detekcie](#) nastavíte kliknutím na tlačidlo **Nastavenia...**

## Vylúčenia

V časti **Vylúčenia** máte možnosť vylúčiť z kontroly konkrétne súbory a priečinky, aplikácie a IP/IPv6 adresy.

Súbory a priečinky uvedené v zozname **Súborový systém** budú vylúčené zo všetkých druhov kontroly: kontrola pri štarte počítača, rezidentná kontrola a kontrola počítača.

- **Cesta** – úplná cesta k súborom alebo priečinkom, ktoré budú vylúčené z kontroly.
- **Hrozba** – ak je vedľa vylúčeného súboru zobrazený názov hrozby, znamená to, že súbor je vylúčený z kontroly len pre túto konkrétnu infiltráciu. Ak bude tento súbor neskôr napadnutý inou infiltráciou, dôjde k detekcii antivírusovým modulom.
-  – umožňuje vytvoriť nové vylúčenie. Zadať cestu k objektu, ktorý chcete vylúčiť z kontroly (môžete taktiež použiť zástupné znaky \* a ?), prípadne konkrétny súbor alebo priečinok vyberte zo stromovej štruktúry.
-  – umožňuje odstrániť vybrané vylúčenia.
- **Predvolené** – vrátenie zmien vylúčení do posledného uloženého stavu.


V záložke **Web a e-mail** môžete vylúčiť zo skenovania protokolov konkrétne **Aplikácie** alebo **IP/IPv6 adresy**.

# Ochrana pri štarte počítača

Tento druh ochrany automaticky kontroluje súbory spúšťané pri štarte systému. Na základe predvolených nastavení sa táto kontrola spúšťa pravidelne vo forme plánovanej úlohy po prihlásení používateľa alebo po úspešnej aktualizácii modulov. Nastavenie parametrov jadra ThreatSense pre modul Ochrany pri štarte počítača môžete meniť po kliknutí na tlačidlo **Nastavenia...** O nastavení parametrov jadra ThreatSense sa viac dočítate v [tejto kapitole](#).

## Rezidentná ochrana súborového systému

Rezidentná ochrana súborového systému kontroluje všetky typy médií, pričom táto kontrola býva spúšťaná viacerými podnetmi. Využíva metódy detekcie technológie ThreatSense (bližšie popísané v časti [Nastavenie parametrov skenovacieho jadra ThreatSense](#)) a môže sa líšiť pre novovytvorené a už existujúce súbory. Na novovytvorené súbory sa dá aplikovať hlbšia úroveň kontroly.

Štandardne sa každý súbor kontroluje pri udalostiach ako **Otvorenie súboru**, **Vytvorenie súboru** a **Spustenie súboru**. Odporúčame vám ponechať pôvodné nastavenia, ktoré zabezpečujú najvyššiu možnú úroveň rezidentnej ochrany pre váš počítač. Rezidentná ochrana sa spúšťa pri štarte systému a poskytuje nepretržitú kontrolu. V špeciálnych prípadoch (napr. v prípade konfliktu s iným rezidentným skenerom) je možné rezidentnú ochranu vypnúť kliknutím na ikonu ESET Endpoint Antivirus for macOS  nachádzajúcu sa na hornej lište (Menu Bar) systému macOS a aktivovaním voľby **Vypnúť rezidentnú ochranu súborového systému**. Rezidentnú ochranu môžete vypnúť v hlavnom okne programu (**Nastavenia** > **Počítač** a prepnete tlačidlo modulu do polohy **VYP**).

Z rezidentnej ochrany môžu byť vylúčené nasledujúce typy médií:

- **Lokálne disky** – systémové pevné disky
- **Vymeniteľné médiá** – CD, DVD, USB médiá, Bluetooth zariadenia a pod.
- **Sieťové disky** – všetky namapované jednotky

Odporúčame používať štandardné nastavenia a meniť výnimky z kontroly iba v špecifických prípadoch, ako napr. pri spomaľovaní prenosu dát medzi konkrétnymi médiami.

Ak chcete zmeniť rozšírené nastavenia rezidentnej ochrany, otvorte **Nastavenia** > **Zobraziť pokročilé nastavenia** ... (alebo stlačte *cmd+,*) > **Rezidentná ochrana** > **Nastavenia...** (tlačidlo vedľa možnosti **Rozšírené nastavenia**, ktoré sú bližšie popísané v kapitole [Rozšírené nastavenia](#)).

## Rozšírené nastavenia

V tomto okne môžete nastaviť typy objektov, ktoré bude technológia ThreatSense kontrolovať. Viac informácií o **Samorozbalovacích archívoch**, **Runtime archívoch** a **Pokročilej heuristike** nájdete v kapitole [Nastavenie parametrov skenovacieho jadra ThreatSense](#).

V sekcii **Predvolené nastavenie archívov** neodporúčame meniť pôvodné nastavenia, ak to nevyžaduje špecifická situácia, pretože vyššie hodnoty úrovne vnorenia môžu negatívne ovplyvniť výkon systému.

**Parametre ThreatSense pre spúšťané súbory** – štandardne sa **Pokročilá heuristika** vykonáva pri spúšťaní súborov. Pre zmiernenie dopadu na výkon systému odporúčame ponechať povolenú Smart optimalizáciu a ESET LiveGrid.

**Zvýšiť kompatibilitu sieťových zväzkov** – táto funkcionality zvýši výkon pri pristupovaní k súborom na sieti. Mala by byť povolená, ak máte spomalenia pri prístupe k sieťovým diskom. Funkcionality používa systémový súborový koordinátor na OS X 10.10 a vyššom. Majte na pamäti, že nie všetky aplikácie ho podporujú, napr. Microsoft Word 2011 ho nepodporuje, Word 2016 podporuje.

## Kedy je vhodné upraviť nastavenia rezidentnej ochrany

Rezidentná ochrana je kľúčový komponent pre udržanie bezpečnosti systému. K úprave parametrov rezidentnej ochrany prístupujte vždy s opatrnosťou. Odporúčame vám, aby ste upravovali tieto nastavenia len v špeciálnych prípadoch. Napríklad v situácii, keď nastane konflikt medzi produktom ESET a špecifickou aplikáciou alebo rezidentnou kontrolou antivírusového programu od iného výrobcu.

Po nainštalovaní ESET Endpoint Antivirus for macOS sú všetky nastavenia optimalizované na zabezpečenie najvyššej úrovne ochrany systému používateľa. Pre obnovenie pôvodných nastavení kliknite na tlačidlo **Štandardné** v ľavej spodnej časti okna **Rezidentná ochrana (Nastavenia > Zobrazíť pokročilé nastavenia ... > Rezidentná ochrana)**.

## Overenie funkčnosti rezidentnej ochrany

Na overenie funkčnosti rezidentnej ochrany použijete testovací súbor [eicar.com](http://eicar.com). Tento súbor je špeciálny neškodný objekt, ktorý detegujú všetky antivírusové programy. Súbor vytvorila organizácia EICAR (European Institute for Computer Antivirus Research) s cieľom testovať fungovanie antivírusových programov.

Stav rezidentnej ochrany je bez použitia ESET Security Management Center možné overiť pomocou **Terminálu** pripojením sa na danú pracovnú stanicu a vykonaním nasledujúceho príkazu:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Stav funkčnosti rezidentnej ochrany bude zobrazený ako `RTPStatus=Enabled` alebo `RTPStatus=Disabled`.

Výstup z príkazového riadka zahŕňa nasledujúce údaje:

- verzia programu ESET Endpoint Antivirus for macOS nainštalovaného na danom počítači,
- dátum a verzia detekčného jadra,
- cesta k aktualizáčnemu serveru.



### Používanie Terminálu

Používanie Terminálu je odporúčané iba pre skúsených používateľov.

## Čo robiť, ak rezidentná ochrana nefunguje

V tejto kapitole nájdete popis problémových situácií, ktoré pri používaní rezidentnej ochrany môžu vzniknúť, a tiež spôsoby, ako tieto problémy odstrániť.



## Rezidentná ochrana je vypnutá

Ak bola rezidentná ochrana vypnutá používateľom, je potrebné ju znovu zapnúť. Zapnete ju v sekcii **Nastavenia > Počítač** prepnutím tlačidla **Rezidentná ochrana súborového systému** do polohy **ZAPNUTÁ**. Iný spôsob, ako znovu zapnúť rezidentnú ochranu, je vojsť z okna rozšírených nastavení do **Rezidentná ochrana** a označiť možnosť **Zapnúť rezidentnú ochranu súborového systému**.

## Rezidentná ochrana nedeteguje a nelieči súbory s infiltráciami

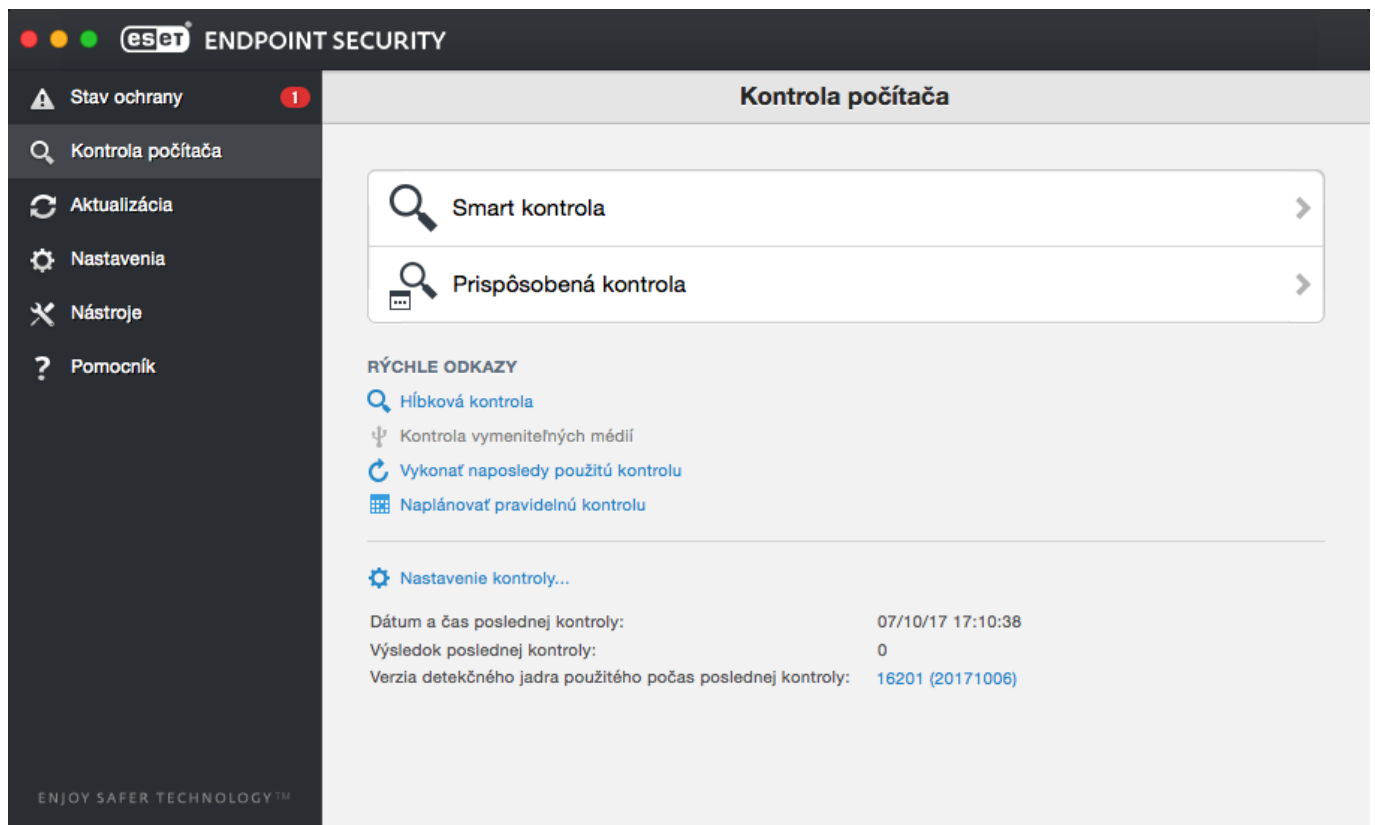
Uistite sa, že nemáte na počítači nainštalované žiadne iné antivírusové programy. Ak sú naraz zapnuté dve alebo viac rezidentných ochrán, môžu medzi nimi nastať konflikty. Odporúčame odinštalovať zo systému všetky antivírusové programy od iných výrobcov.

## Rezidentná ochrana sa nespustila


Ak sa rezidentná ochrana nespustí pri štarte systému, dôvodom môžu byť konflikty s ďalšími programami. V tomto prípade odporúčame obrátiť sa na špecialistov technickej podpory spoločnosti ESET.

## Manuálna kontrola počítača

Ak máte podozrenie, že je váš počítač napadnutý malvérom (pozorujete nezvyčajné správanie systému), spustíte **Smart kontrolu**, ktorá váš počítač skontroluje na prítomnosť vírusov a hrozieb. Pre zaistenie maximálnej úrovne ochrany je potrebné antivírusovú kontrolu počítača spúšťať pravidelne, nie len v prípade podozrenia na napadnutie malvérom. Pri pravidelných kontrolách môžu byť zachytené aj infiltrácie, ktoré neboli pri ukladaní na pevný disk detegované modulom rezidentnej ochrany. Uvedená situácia môže nastať v prípade, ak bola počas ukladania súboru vypnutá rezidentná ochrana, prípadne neboli aktualizované detekčné moduly.



Odporúčame vám spúšťať manuálnu kontrolu počítača najmenej raz za mesiac. Kontrola sa dá nastaviť ako jedna z plánovaných úloh v časti **Nástroje > Plánovač**.

Súbory a priečinky môžete skontrolovať aj ich presunutím (tzv. drag and drop) z pracovnej plochy alebo okna **Finder** do hlavného okna programu ESET Endpoint Antivirus for macOS, na ikonu v Docku , na ikonu na hornej lište (Menu Bar) alebo ikonu aplikácie v priečinku */Applications*.

## Typy kontroly

V programe sú dostupné dva typy kontroly počítača. **Smart kontrola** predstavuje rýchlu kontrolu počítača bez potreby nastavovania detailných parametrov. **Prispôsobená kontrola** umožňuje výber z preddefinovaných profilov kontroly a tiež nastavenie špecifických cieľov kontroly.

## Smart kontrola

Smart kontrola je rýchla kontrola počítača, ktorá lieči infikované súbory bez potreby zásahu používateľa. Hlavnou výhodou tohto typu kontroly je jej ľahká aplikácia bez potreby podrobného nastavovania parametrov kontroly. Smart kontrola prezrie všetky súbory a adresáre a automaticky vylieči alebo vymaže nájdené vírusy. Úroveň liečenia je automaticky nastavená na svoju pôvodnú hodnotu. Pre podrobnejšie informácie ohľadom typov liečenia si pozrite kapitolu [Liečenie](#).

## Prispôsobená kontrola

**Prispôsobená kontrola** je vhodným riešením, ak chcete špecifikovať parametre kontroly, ako sú ciele a metódy kontroly. Výhodou prispôsobenej kontroly je práve možnosť podrobne upraviť parametre kontroly podľa vlastných potrieb. Rôzne konfigurácie sa dajú ukladať ako profily definované používateľom, ktoré sú užitočné najmä vtedy, ak je potrebné periodicky opakovať kontrolu s tými istými parametrami.

Ak chcete určiť ciele kontroly, kliknite postupne na **Kontrola počítača > Prispôsobená kontrola** a v stromovej štruktúre označte požadované **Ciele kontroly**. Cieľ kontroly môžete bližšie špecifikovať aj zadaním cesty k adresáru alebo súboru/súborom, ktoré chcete zaradiť do kontroly. Ak chcete skontrolovať systém bez vykonania dostupných akcií liečenia, označte možnosť **Kontrolovať bez liečenia**. Celkovo si môžete vybrať z troch úrovní liečenia, a to kliknutím na **Nastavenia... > Liečenie**.

### Prispôsobená kontrola

Nastavovanie a spúšťanie prispôsobených kontrol odporúčame len pokročilým používateľom, ktorí už majú predchádzajúcu skúsenosť s používaním antivírusových programov.

## Ciele kontroly

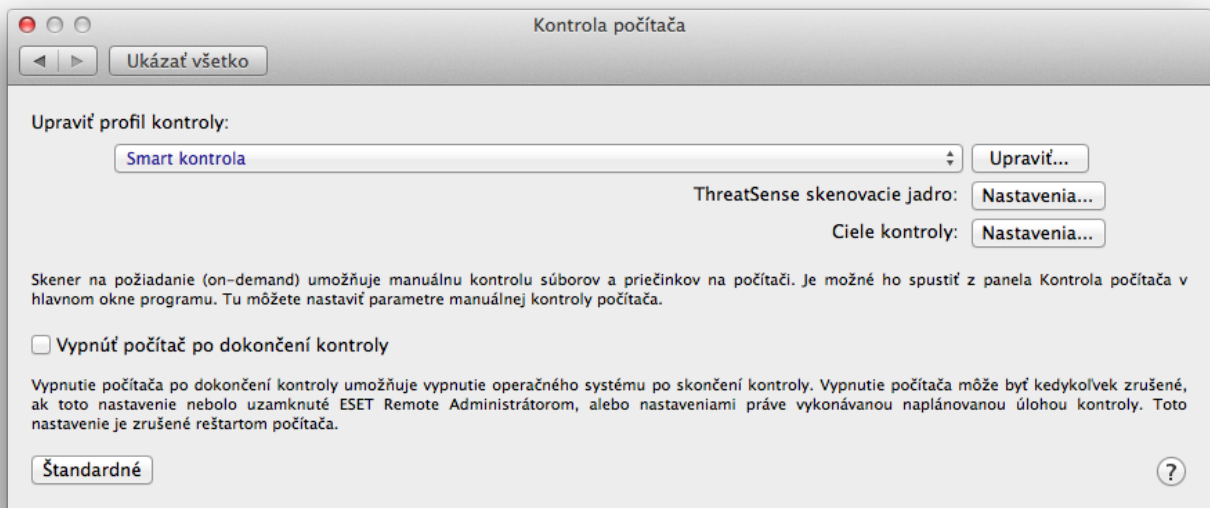
Stromová štruktúra cieľov kontroly slúži na výber súborov a adresárov, ktoré budú predmetom antivírusovej kontroly. Adresáre môžu byť označené tiež podľa nastavení profilu.

Cieľ kontroly môžete bližšie špecifikovať aj zadaním cesty k adresáru alebo súboru/súborom, ktoré chcete zaradiť do kontroly. Ciele kontroly si vyberte zo stromovej štruktúry, ktorá obsahuje všetky adresáre na počítači.

# Profily kontroly

Vami požadované nastavenia kontroly môžete uložiť pre použitie v budúcich kontrolách. Odporúčame vám, aby ste vždy vytvorili nový profil (s rôznymi cieľmi kontroly, metódami kontroly a ďalšími parametrami) pre každú pravidelne používanú kontrolu.

Pre vytvorenie nového profilu kliknite postupne na **Nastavenia > Zobrazíť pokročilé nastavenia...** (prípadne stlačte **cmd+,**) > **Kontrola počítača** a kliknite na **Upraviť** vedľa zoznamu aktuálnych profilov.



Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite kapitolu [Nastavenie parametrov skenovacieho jadra ThreatSense](#), ktorá obsahuje popis každého parametra kontroly.

## Príklad

Predpokladajme, že chcete vytvoriť svoj vlastný profil kontroly a čiastočne vám na tento účel vyhovuje konfigurácia Smart kontroly, ale nechcete aby boli kontrolované runtime archívy alebo potenciálne nebezpečné aplikácie a navyše chcete aplikovať metódu prísneho liečenia. V okne **Zoznam profilov kontroly počítača** napíšete názov pre váš profil, kliknete na **Pridať...** a potvrdíte stlačením **OK**. Potom upravíte parametre v nastaveniach **Skenovacieho jadra ThreatSense** a nastavíte **Ciele kontroly** tak, aby zodpovedali vašim potrebám.

Ak si želáte automaticky vypnúť počítač po vykonanej kontrole, označte možnosť **Vypnúť počítač po dokončení kontroly**.

## Nastavenie parametrov jadra ThreatSense

ThreatSense je názov technológie spoločnosti ESET, ktorú tvorí súbor komplexných metód detekcie hrozieb. Táto technológia je proaktívna, čo znamená, že poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. Využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické vzorky atď.), čo prispieva k výraznému zlepšeniu ochrany systému. Skenovacie jadro je schopné kontrolovať niekoľko dátových tokov súčasne, a tak maximalizovať svoj výkon a účinnosť detekcie. Technológia ThreatSense dokáže účinne odhaľovať aj rootkity.

Samotné nastavenia technológie ThreatSense umožňujú používateľovi špecifikovať viaceré parametre kontroly:

- typy súborov a prípony, ktoré sa majú kontrolovať,
- kombinácie rôznych metód detekcie,
- úrovne liečenia atď.

Okno s nastaveniami skenovacieho jadra ThreatSense otvoríte kliknutím na **Nastavenia > Zobrazíť pokročilé nastavenia...** (alebo stlačením *cmd+*) a kliknutím na tlačidlo **Nastavenia...** vedľa popisu ThreatSense skenovacie jadro v rámci modulov **Ochrana pri štarte počítača**, **Rezidentná ochrana** a **Kontrola počítača**, ktoré všetky používajú technológiu ThreatSense (pozri nižšie). Odlišné bezpečnostné scenáre si vyžadujú rôzne nastavenia. Technológia ThreatSense je nastaviteľná zvlášť pre tieto moduly ochrany:

- **Ochrana pri štarte počítača** – kontrola súborov spúšťaných pri štarte počítača,
- **Rezidentná ochrana** – ochrana súborového systému v reálnom čase,
- **Kontrola počítača** – manuálna kontrola počítača,
- **Ochrana prístupu na web**,
- **E-mailová ochrana**.

Parametre ThreatSense sú špeciálne optimalizované pre každý modul a ich zmena môže značne ovplyvniť prácu systému. Príkladom môže byť zmena nastavení tak, aby bola vždy vykonaná kontrola runtime archívov, alebo zapnutie pokročilej heuristiky pre modul rezidentnej ochrany súborového systému. Takéto zmeny môžu spôsobiť celkové spomalenie systému. Preto odporúčame nemeniť predvolené nastavenia parametrov ThreatSense v rámci žiadneho z modulov ochrany s výnimkou modulu Kontroly počítača.

## Objekty

V sekcii **Objekty** máte možnosť nastaviť typy súborov, ktoré budú predmetom antivírusovej kontroly.

- **Symbolické odkazy** – (dostupné iba pre Kontrolu počítača) kontroluje špeciálne typy súborov, ktoré obsahujú reťazec textu definovaný operačným systémom ako cesta k inému súboru alebo priečinku,
- **E-mailové súbory** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje špeciálne súbory, v ktorých sa nachádza stiahnutá elektronická pošta,
- **E-mailové schránky** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje používateľské e-mailové schránky v systéme. Nesprávne použitie tejto voľby môže viesť ku konfliktu s vaším e-mailovým klientom. Ak sa chcete dozvedieť viac o výhodách a nevýhodách tejto možnosti, prečítajte si nasledujúci [článok](#) (dostupný iba v angličtine).
- **Archívy** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje súbory nachádzajúce sa v archívnych súboroch (RAR, ZIP, ARJ, TAR, atď.),

- **Samorozbaľovacie archívy** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje súbory v samorozbaľovacích archívoch,
- **Runtime archívy** – runtime archívy sa na rozdiel od klasických archívov dekomprimujú v pamäti počítača po spustení súboru. Ak je táto možnosť zvolená, kontrolované budú aj klasické statické packery (napr. UPX, ASPack, yoda, ASPack, FGS).

## Metódy

V časti **Metódy** môžete nastaviť, ktoré metódy sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú nasledujúce možnosti:


- **Heuristika** – heuristika používa algoritmus na analýzu (škodlivej) aktivity programov. Hlavnou výhodou heuristickej detekcie je jej schopnosť odhaliť aj tie najnovšie druhy škodlivého softvéru.
- **Pokročilá heuristika** – pokročilá heuristika používa jedinečný heuristický algoritmus vyvinutý spoločnosťou ESET, ktorý dokáže detegovať počítačové červy a trójske kone napísané v zložitých programovacích jazykoch. Schopnosť detekcie je tak vďaka pokročilej heuristike výrazne vyššia.

## Liečenie

Nastavenia pre liečenie určujú spôsob, akým kontrola vyčistí infikované súbory. Liečenie má tri úrovne:



- **Neliečiť** – infikované súbory sa automaticky nevyliečia. Program zobrazí okno s upozornením a možnosťou manuálneho výberu akcie.
- **Štandardné liečenie** – program sa pokúsi automaticky vyliečiť alebo vymazať infikovaný súbor. Ak nie je možné zvoliť správnu akciu automaticky, program ponúkne možnosť manuálneho výberu akcie. Používateľovi sa možnosť manuálneho výberu akcie zobrazí aj v tom prípade, že prednastavenú akciu nie je možné dokončiť.
- **Prísne liečenie** – program vylieči alebo vymaže všetky infikované súbory (vrátane archívov). Jedinou výnimkou sú systémové súbory. Ak takéto súbory nie je možné vyliečiť, program zobrazí okno s upozornením a výzvou na výber požadovanej akcie, ktorá sa má so súborom vykonať.

### Režim štandardného liečenia – infikované archívy

 Pri predvolenom režime štandardného liečenia je celý archív zmaný len v tom prípade, ak sú všetky súbory obsiahnuté v archíve infikované. Ak teda archív obsahuje aj legítimne súbory (nenapadnuté malvérom), nebude vymazaný. Ak je archív detegovaný v režime prísneho liečenia a obsahuje aspoň jeden súbor s infiltráciou, bude vymazaný celý archív bez ohľadu na to, či obsahuje aj bezpečné súbory.

## Vylúčenia

Prípona súboru je súčasťou jeho názvu, v ktorom je oddelená bodkou. Prípona označuje typ a obsah súboru. V tejto časti nastavení parametrov ThreatSense môžete nastaviť typy súborov, ktoré budú kontrolované.

Štandardne sa kontrolujú všetky súbory bez ohľadu na príponu. Do zoznamu súborov vylúčených z kontroly môže byť pridaná akákoľvek prípona. Pomocou tlačidiel  a  môžete povoliť alebo zakázať kontrolu požadovaných súborov podľa ich prípon.

Vylúčenie prípon je niekedy potrebné, ak prebiehajúca kontrola naruša činnosť špecifického programu, ktorý k daným typom súborov bude pristupovať. Napríklad môže byť niekedy vhodné vylúčiť prípony *log*, *cfg* a *tmp*. Správny formát pre definovanie prípon je:

*log*

*cfg*

*tmp*

## Obmedzenia

V sekcii **Obmedzenia** nastavíte maximálnu veľkosť kontrolovaných objektov a maximálnu hĺbku kontroly v archívoch (počet vnorených archívov do ktorého je vykonávaná kontrola).

- **Maximálna veľkosť:** určuje najväčšiu možnú veľkosť súborov, ktoré budú skontrolované. Modul antivírusu bude kontrolovať len objekty s menšou veľkosťou ako je definovaná hodnota. Neodporúčame meniť prednastavenú hodnotu, pretože väčšinou nie je na túto zmenu dôvod. Odporúčame aby túto hodnotu menili len pokročilí používatelia, ktorí majú dôvod na vylúčenie väčších objektov z kontroly.
- **Maximálny čas kontroly:** upravuje maximálny čas venovaný kontrole jedného objektu. Ak sem používateľ nastaví hodnotu, antivírusový modul prestane kontrolovať objekt po uplynutí nastavenej doby, bez ohľadu na to či bola kontrola objektu ukončená alebo nie.
- **Maximálna úroveň vnorenia:** upravuje maximálnu hĺbku vnorenia pri kontrole archívov. Ak nie ste skúsený používateľ, neodporúčame vám meniť prednastavenú hodnotu 10. Za bežných okolností nie je dôvod toto nastavenie meniť. Ak sa kontrola ukončí kvôli počtu úrovni vnorenia archívov, archív zostane neskontrolovaný.
- **Maximálna veľkosť súboru:** umožňuje nastaviť maximálnu reálnu veľkosť súborov v archívoch, ktoré budú skontrolované. Ak sa kontrola ukončí kvôli tomuto obmedzeniu, archív zostane neskontrolovaný.

## Ostatné

### Zapnúť Smart optimalizáciu

Pre kontrolu systému budú použité nastavenia zabezpečujúce najlepšiu optimalizáciu rýchlosti a úrovne kontroly, ktorá spočíva v inteligentnom použití rôznych skenovacích metód pre rôzne typy súborov v rámci jednotlivých ochranných modulov. Nastavenia Smart optimalizácie nie sú v produkte ESET Endpoint Antivirus for macOS zadefinované napevno. Vývojársky tím firmy ESET ich má možnosť podľa uváženia meniť prostredníctvom pravidelnej automatickej aktualizácie. Pokiaľ je Smart optimalizácia vypnutá, pri kontrole súborov sa aplikujú výlučne iba nastavenia zadefinované používateľom v nastaveniach jadra ThreatSense pre daný ochranný modul.

### Kontrolovať alternatívne dátové prúdy (platí iba pre manuálnu kontrolu počítača)

Alternatívne dátové prúdy (ADS) používané systémom NTFS sú bežným spôsobom neviditeľné asociácie k súborom a adresárom. Veľa vírusov ich preto využíva na svoje maskovanie pred prípadným odhalením.

# Našla sa infiltrácia

Infiltrácie sa do systému môžu dostať z najrôznejších prístupových bodov – internetových stránok, zdieľaných adresárov, e-mailov, vymeniteľných médií (USB, externé disky, CD, DVD atď.).

Ak má váš počítač príznaky infekcie škodlivým kódom, teda je pomalší, zamrzá a podobne, odporúčame nasledovné kroky:

1. Kliknite na **Kontrola počítača**.
2. Kliknite na **Smart kontrola** (pre viac informácií si pozrite kapitolu [Smart kontrola](#)).
3. Po ukončení kontroly skontrolujte počet kontrolovaných, infikovaných a vyliečených súborov v protokole.

Ak chcete skontrolovať len určitú časť vášho disku, kliknite na **Prispôsobená kontrola** a vyberte si ciele, ktoré budú skontrolované na prítomnosť malvéru.

Ako všeobecný príklad spôsobu, akým ESET Endpoint Antivirus for macOS rieši problém s infiltráciou, uveďme prípad, keď rezidentná ochrana súborového systému s nastavenou štandardnou úrovňou liečenia nájde vírus. Pokúsi sa o vyliečenie alebo vymazanie súboru. Ak modul rezidentnej ochrany nemá nastavenú akciu, ktorá sa má vykonať, požiada vás o výber z možností prostredníctvom okna s upozornením. Zvyčajne sú k dispozícii možnosti **Vyliečiť**, **Odstrániť** a **Žiadna akcia**. Poslednú možnosť neodporúčame. Výnimkou môže byť iba situácia, keď máte istotu, že súbor je neškodný a bol detegovaný omylom.

## Liečenie a mazanie

Použite liečenie, ak bol súbor napadnutý vírusom, ktorý k nemu pridal škodlivý kód. V tomto prípade sa najprv pokúste infikovaný súbor vyliečiť, aby sa tým obnovil do pôvodného stavu. Ak súbor pozostáva výhradne zo škodlivého kódu, bude vymazaný.

## Mazanie súborov v archívoch

V prednastavenom režime liečenia bude celý archív zmazaný len vtedy, ak obsahuje iba infikované a žiadne „čisté“ súbory. Inými slovami, archívy sa nevymazávajú, ak obsahujú aj neškodné (nenapadnuté) súbory. Zvýšená opatrnosť je však nutná, ak spustíte kontrolu s nastavením **Prísne liečenie** – v režime Prísne liečenie bude totiž archív vymazaný, ak obsahuje aspoň jeden súbor s infiltráciou, bez ohľadu na stav ostatných súborov v archíve.

# Web a e-mail

Nastavenia modulov webovej a e-mailovej ochrany nájdete v časti **Nastavenia > Web a mail**. Podrobné nastavenia pre každý z modulov zobrazíte kliknutím na tlačidlo **Nastavenia**.



### Výnimky kontroly

ESET Endpoint Antivirus for macOS nevykonáva kontrolu šifrovaných protokolov HTTPS, POP3S a IMAPS.

- **Ochrana prístupu na web** – monitoruje HTTP komunikáciu medzi webovými prehliadačmi a vzdialenými servermi.
- **Ochrana e-mailových klientov** – zabezpečuje kontrolu e-mailovej komunikácie prijímanej cez protokoly POP3 a IMAP.

- **Antiphishingová ochrana** – blokuje potenciálne phishingové útoky prichádzajúce z podozrivých webových stránok alebo domén.

## Ochrana prístupu na web

Ochrana prístupu na web monitoruje komunikáciu medzi internetovými prehliadačmi a vzdialenými servermi v súlade s pravidlami HTTP.

Filtrovanie webu môžete docieľiť definovaním [portov pre HTTP komunikáciu](#) a/alebo [URL adries](#).

## Porty

V záložke **Porty** môžete definovať porty používané protokolom HTTP. Štandardne sú preddefinované porty 80, 8080 a 3128.

## Zoznam URL adries

**Zoznam URL adries** dovoľuje definovať adresy, ktoré budú blokované, povolené alebo vylúčené z kontroly. Web stránky v zozname blokovaných adries nebudú dostupné. Web stránky v zozname vylúčených adries sú prístupné bez toho, aby boli kontrolované na prítomnosť škodlivého kódu.

Ak chcete povoliť prístup iba k URL adresám uvedeným v zozname **Povolené URL**, označte voľbu **Obmedziť prístup na URL adresy**.

Zoznam adries aktivujete voľbou **Povoliť**. Ak chcete vidieť notifikáciu o vstupe na URL adresu zo zoznamu, označte voľbu **Zapnúť notifikáciu**.

Vo všetkých zoznamoch môžete použiť špeciálne symboly \* (hviezdica) a ? (otáznik). Hviezdica nahrádza akýkoľvek reťazec znakov a otáznik nahrádza akýkoľvek symbol. Odporúčame zvýšenú opatrnosť pri zadávaní vylúčených URL adries. Tento zoznam by mal obsahovať iba overené a bezpečné adresy.

## E-mailová ochrana

E-mailová ochrana zabezpečuje kontrolu e-mailovej komunikácie prijímanej cez protokoly POP3 a IMAP. Pri kontrole prichádzajúcich e-mailových správ program ESET Endpoint Antivirus for macOS používa pokročilé metódy kontroly zahrnuté v skenovacom jadre ThreatSense. Kontrola komunikácie prijímanej cez protokoly POP3 a IMAP nie je závislá od typu vášho e-mailového klienta.

**ThreatSense skenovacie jadro: Nastavenia** – pokročilé nastavenia kontroly vám umožňujú nastaviť ciele kontroly, metódy detekcie atď. Kliknite na tlačidlo **Nastavenia...**, čím zobrazíte okno s podrobnými nastaveniami kontroly.

**Pridávať poznámku pod čiarou do e-mailových správ** – umožňuje do skontrolovaných e-mailových správ pridávať informáciu o výsledku kontroly. Na tieto poznámky sa nemožno úplne spoliehať, nakoľko nemusia byť doplnené do problematických HTML správ a taktiež môžu byť sfalšované vírusmi. K dispozícii sú nasledujúce možnosti:



- **Nepridávať do správ** – do správ nebudú pridávané žiadne poznámky s informáciou o výsledku kontroly,
- **Pridávať len do infikovaných správ** – program pridá poznámky iba do správ obsahujúcich škodlivý softvér,
- **Pridávať do všetkých kontrolovaných správ** – program ESET Endpoint Antivirus for macOS pridá poznámky do všetkých skontrolovaných správ.

**Pridávať poznámku do predmetu prijatých a čítaných infikovaných e-mailov** – označte túto možnosť, ak si želáte, aby program pridával do predmetu infikovaných správ upozornenie na vírus. Táto funkcia sa dá využiť pre jednoduché filtrovanie infikovaných správ. Poznámka v predmete správy tiež zvyšuje úroveň dôveryhodnosti pre príjemcu správy. V prípade nájdenia infiltrácie poznámka poskytne hodnotné informácie o hrozbe.

**Šablóna pridávaná do predmetu infikovaných e-mailov** – upravte túto šablónu, ak si želáte zmeniť formát predpony, ktorá bude pridaná na začiatok predmetu infikovaného e-mailu.

- %avstatus% – pridá stav e-mailu z hľadiska bezpečnosti (napríklad: infikovaný, čistý...)
- %virus% – pridá názov hrozby
- %product% – pridá názov vášho produktu ESET (v tomto prípade ESET Endpoint Antivirus for macOS)
- %product\_url% – pridá odkaz na webovú stránku spoločnosti ESET ([www.eset.com](http://www.eset.com))

V spodnej časti tohto okna môžete zapnúť/vypnúť kontrolu e-mailovej komunikácie prijímanej cez protokoly POP3 a IMAP. Viac sa dozviete v týchto kapitolách:

- [Kontrola protokolu POP3](#)
- [Kontrola protokolu IMAP](#)

## Kontrola protokolu POP3

POP3 je najrozšírenejší protokol slúžiaci na príjem e-mailovej komunikácie prostredníctvom e-mailového klienta. ESET Endpoint Antivirus for macOS zabezpečuje ochranu tohto protokolu nezávisle od používaného klienta.

Modul zabezpečujúci kontrolu sa zavádza pri štarte operačného systému a počas celej doby je zavedený v pamäti. Pre správne fungovanie stačí skontrolovať, či je modul zapnutý a kontrola POP3 protokolu je vykonávaná automaticky bez potreby konfigurácie e-mailového klienta. Štandardne je kontrolovaná komunikácia na porte 110 a v prípade potreby je možné pridať aj iný používaný port. Čísla portov sa oddeľujú čiarkou.

Ak je voľba **Zapnúť kontrolu protokolu POP3** označená, všetka komunikácia prúdiaca cez POP3 je monitorovaná pre škodlivý softvér.

# Kontrola protokolu IMAP

(IMAP) (Internet Message Access Protocol) je ďalší internetový protokol na prijímanie e-mailových správ. IMAP má v porovnaní s POP3 zopár výhod, ako napríklad možnosť viacerých klientov pripojiť sa na tú istú e-mailovú schránku a zachovať informácie stavu správy (napríklad, či správa bola alebo nebola prečítaná, odpovedaná alebo vymazaná). ESET Endpoint Antivirus for macOS zabezpečuje ochranu tohto protokolu nezávisle od používaného klienta.

Modul zabezpečujúci kontrolu sa zavádza pri štarte operačného systému a počas celej doby je zavedený v pamäti. Pre správne fungovanie stačí skontrolovať, či je modul zapnutý; kontrola IMAP protokolu je vykonávaná automaticky bez potreby konfigurácie e-mailového klienta. Štandardne je kontrolovaná komunikácia na porte 143 a v prípade potreby je možné pridať aj iný používaný port. Čísla portov sa oddeľujú čiarkou.

Ak je voľba **Zapnúť kontrolu protokolu IMAP** označená, všetka komunikácia prúdiaca cez IMAP je monitorovaná na prítomnosť škodlivého softvéru.

## Anti-Phishing

Pojmom phishing sa označuje kriminálna činnosť využívajúca techniky tzv. sociálneho inžinierstva (manipulácia používateľa s cieľom získať od neho dôverné informácie). Najčastejšie je cieľom získať citlivé údaje používateľa, napr. prístupové údaje k bankovým účtom, čísla kreditných kariet, PIN kódy, používateľské mená a heslá a podobne.

Odporúčame ponechať funkciu Anti-Phishing zapnutú (**Nastavenia > Zobrazíť pokročilé nastavenia... > Antiphishingová ochrana**). Blokované tak budú všetky potenciálne phishingové útoky prichádzajúce z podozrivých webových stránok alebo domén a o pokuse o útok vás bude program informovať zobrazením upozornenia.

## Správa zariadení

ESET Endpoint Antivirus for macOS umožňuje skenovať alebo blokovať zariadenia a prispôbovať filtre a oprávnenia používateľov pre prístup a prácu s externými pamäťovými zariadeniami. Toto je užitočný nástroj pre administrátorov, ktorí chcú zabrániť používaniu zariadení s nevhodným obsahom.

### Správa zariadení na systéme macOS 11 a novších



ESET Endpoint Antivirus for macOS nainštalovaný na macOS 11 a novších systémoch kontroluje iba pamäťové zariadenia (napr. USB kľúče, CD/DVD...).

Podporované externé zariadenia na systéme macOS 10.15 a starších:

- Diskové úložisko (HDD alebo USB výmenné médiá)
- CD/DVD
- USB tlačiareň
- Obrazové zariadenie
- Sériový port

- Sieť
- Prenosné zariadenie




Pri vložení zariadenia blokovaneho existujúcim pravidlom sa zobrazí upozornenie a prístup na zariadenie nebude povolený.

Protokol zapisuje všetky incidenty, ktoré spúšťajú funkcionality Správy zariadení. Záznamy protokolu môžete vidieť v hlavnom menu ESET Endpoint Antivirus for macOS v časti **Nástroje** > [Protokoly](#).

## Pravidlá

Nastavenia pre Správu zariadení môžete upravovať v časti **Nastavenia** > **Zobraziť pokročilé nastavenia...** > **Správa zariadení**.

Kliknutím na možnosť **Povolit správu zariadení** aktivujete túto funkciu v programe ESET Endpoint Antivirus for macOS. Po povolení Správy zariadení môžete upravovať pravidlá. Zaškrtnutím políčka vedľa názvu pravidla zapínate a vypínate dané pravidlo.

Pravidlá pridáte alebo odstránite tlačidlami  alebo . Pravidlá sú zoradené podľa priority, pričom pravidlá s najvyššou prioritou sú navrchu. Poradie zmeníte označením a potiahnutím (drag&drop) pravidla v zozname alebo kliknutím na  a výberom jednej z možností.

ESET Endpoint Antivirus for macOS automaticky deteguje všetky aktuálne vložené zariadenia a ich parametre (Typ zariadenia, Výrobca, Model, Sériové číslo). Namiesto vytvárania pravidiel manuálne môžete kliknúť na možnosť **Načítať**, zvoliť zariadenie a vytvoriť pravidlo kliknutím na **Pokračovať**.

Konkrétne zariadenia môžu byť povolené alebo blokované vzhľadom na používateľa, skupinu používateľov alebo iné parametre, ktoré zadefinujete v konfigurácii pravidla. Zoznam pravidiel pozostáva z niekoľkých parametrov, ako sú názov, typ zariadenia, závažnosť vytvorených protokolov a akcia, ktorá sa má vykonať po pripojení zariadenia k počítaču.

### Názov

Do poľa **Názov** zadajte popis pravidla pre jeho lepšiu identifikáciu. Možnosť **Pravidlo zapnuté** slúži na aktivovanie alebo deaktivovanie konkrétneho pravidla, čo je užitočné v prípade, že si neželáte pravidlo odstrániť natrvalo.

### Typ zariadenia

Z roletového menu vyberte typ externého zariadenia. Informácia o type zariadenia je prevzatá od operačného systému. Úložné zariadenia zahŕňajú externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty. Keďže tieto zariadenia poskytujú informácie len o svojej činnosti, nie o používateľoch, môžu byť blokovanie len globálne pre všetkých používateľov.

## Akcia

Prístup k zariadeniam bez úložiska môže byť povolený alebo blokovaný. Na druhej strane v rámci prístupových práv k úložným zariadeniam môžete vybrať jednu z nasledujúcich možností:

**Čítanie/Zápis** – bude povolený úplný prístup k zariadeniu.

**Iba na čítanie** – povolený bude prístup k zariadeniu len na čítanie, nie na zápis.

**Blokovať** – prístup k zariadeniu bude blokovaný.

## Typ kritéria

Zvoľte **Zariadenie** alebo **Skupinu zariadení**. Nasledujúce parametre môžu byť použité na vyladenie pravidla tak, aby bolo platné pre vybrané zariadenie.

**Výrobca** – filtrovanie podľa názvu výrobcu alebo ID.

**Model** – názov daného zariadenia.

**Sériové číslo** – externé zariadenia zvyčajne majú svoje vlastné sériové číslo. V prípade CD/DVD ide o sériové číslo daného média, nie CD mechaniky.

### Žiadne zadefinované parametre

- i** Ak vyššie spomenuté parametre nie sú zadefinované, pravidlo nebude tieto polia brať do úvahy. Parametre vo všetkých poliach okna nerozlišujú malé a veľké písmená a nepodporujú zástupné znaky (\*, ?).

### TIP

- i** Pre získanie informácií o konkrétnom zariadení najprv vytvorte pravidlo pre povolenie daného typu zariadení a zariadenie pripojte k počítaču. Po pripojení zariadenia k počítaču jeho parametre zistíte v [Protokole správy zariadení](#).

## Závažnosť zapisovania do protokolu

**Vždy** – zapisuje všetky udalosti.

**Diagnostické** – zaznamenáva do protokolu informácie dôležité pre ladenie programu.

**Informácie** – zaznamenáva informatívne správy.

**Upozornenie** – zaznamenáva kritické chyby a varovné správy.

**Žiadne** – nebude vytvorený žiadny protokol.

## Zoznam používateľov

Pravidlo môže byť obmedzené len na určitých používateľov alebo skupiny používateľov ich pridaním do Zoznamu používateľov:

**Upraviť...** – otvorí **Editor identity**, v ktorom môžete pridať používateľov alebo skupiny používateľov. Pre zadefinovanie zoznamu používateľov jednoducho zvolte používateľov zo zoznamu **Používatelia** na ľavej strane a kliknite na tlačidlo **Pridať**. Pre odstránenie používateľa kliknite na jeho meno v zozname **Vybraní používatelia** a kliknite na **Odobrať**. Pre zobrazenie všetkých systémových používateľov zvolte možnosť **Zobraz všetkých používateľov**. Ak necháte zoznam používateľov prázdny, pravidlo bude platné pre všetkých používateľov.

### Obmedzenie pre pravidlá zohľadňujúce zoznamy používateľov

- ! Nie všetky typy zariadení sa dajú filtrovať podľa pravidiel zohľadňujúcich zoznamy používateľov (napríklad zobrazovacie zariadenia neposkytujú informácie o používateľoch, ale len o akciách).

## Nástroje

Menu **Nástroje** obsahuje moduly, ktoré zjednodušujú spravovanie programu a ponúkajú dodatočné možnosti pre pokročilých používateľov.

## Protokoly

Protokoly obsahujú informácie o dôležitých udalostiach v programe a poskytujú prehľad všetkých odhalených hrozieb. Protokoly sú užitočným zdrojom informácií pri hľadaní chýb a odhaľovaní prienikov do vášho systému. Zapisovanie do protokolov prebieha aktívne na pozadí bez akejkoľvek interakcie zo strany používateľa. Informácie sú zaznamenávané na základe nastavenej úrovne podrobnosti zápisu do protokolov. Textové správy a protokoly je možné prezerať či archivovať priamo z prostredia ESET Endpoint Antivirus for macOS.

Protokoly sú dostupné z hlavného menu ESET Endpoint Antivirus for macOS kliknutím na **Nástroje > Protokoly**. Zvoľte požadovaný typ protokolov z roletového menu Protokoly v hornej časti okna. Dostupné sú nasledujúce protokoly:

1. **Zachytené hrozby** – informácie o udalostiach v programe, ktoré sa týkajú detekcie infiltrácií.
2. **Udalosti** – všetky dôležité akcie vykonané programom ESET Endpoint Antivirus for macOS sú zaznamenané v protokoloch udalostí.
3. **Kontrola počítača** – výsledky všetkých ukončených kontrol sú zobrazené v tomto okne. Dvojitým kliknutím na akýkoľvek záznam v protokole zobrazíte podrobnosti príslušnej kontroly.
4. **Správa zariadení** – záznamy o vymeniteľných médiách alebo zariadeniach, ktoré boli pripojené k počítaču. Do protokolu sú zaznamenávané len zariadenia s vytvoreným pravidlom. Ak sa na pripojené zariadenie nevzťahuje žiadne pravidlo, záznam v protokole sa pre zariadenie nevytvorí. Môžete tu tiež vidieť podrobnosti o zariadeniach, ako napríklad typ zariadenia, sériové číslo, názov výrobcu a veľkosť pamäte média (ak je dostupná).
5. **Filtrované stránky** – v tomto zozname nájdete webové stránky, ktoré boli zablokované [Ochranou prístupu na web](#). V týchto protokoloch môžete vidieť čas, URL, stav, IP adresu, používateľa a aplikáciu, ktorá nadviazala spojenie s konkrétnou webovou stránkou.

Pre skopírovanie obsahu protokolu do schránky kliknite pravým tlačidlom myši na konkrétny protokol a potom na možnosť **Kopírovať**.

## Údržba protokolov

Nastavenia protokolov ESET Endpoint Antivirus for macOS sú dostupné z hlavného okna programu. Kliknite na **Nastavenia > Zobrazíť pokročilé nastavenia... > Nástroje > Protokoly**. Môžete nastaviť tieto parametre:

- **Automaticky mazať staré záznamy protokolov** – záznamy v protokoloch staršie ako zadany počet dní budú

automaticky vymazané.

- **Automaticky optimalizovať protokoly** – umožní automatickú defragmentáciu protokolov, ak je prekročené zadané percento nevyužitých záznamov.

Všetky dôležité informácie zobrazené v grafickom rozhraní, správy o nájdených hrozbách a udalostiach môžu byť uložené v čitateľnom textovom formáte ako obyčajný text alebo CSV súbor (s hodnotami oddelenými čiarkou). Ak chcete, aby boli tieto súbory k dispozícii pre spracovanie pomocou nástrojov tretích strán, označte možnosť

**Povoliť záznamy do textových súborov.**

Pre nastavenie cieľového priečinka, do ktorého sa majú protokoly ukladať, kliknite na tlačidlo **Nastavenia...** vedľa popisu **Rozšírené nastavenia**.

V závislosti od výberu možností v časti **Textové súbory protokolov: Upraviť** môžete ukladať protokoly s nasledujúcimi informáciami:

- Udalosti ako *Neplatné používateľské meno a heslo*, *Moduly nie je možné aktualizovať* a pod. sú uložené do súboru *eventslog.txt*.
- Hrozby zachytené modulmi *Ochrana pri štarte počítača*, *Rezidentná ochrana* alebo *Kontrola počítača* sa ukladajú do súboru s názvom *threatslog.txt*.
- Výsledky dokončených kontrol sa ukladajú vo formáte *scanlog.NUMBER.txt*.
- Zariadenia zablokované modulom *Správa zariadení* sú uvedené v súbore *devctllog.txt*.

Pre nastavenie filtrov v časti **Štandardné záznamy kontroly počítača** kliknite na tlačidlo **Upraviť...** a označte/zrušte označenie jednotlivých typov protokolov podľa vášho uváženia. Viac informácií o typoch a filtrovaní protokolov sa dočítate v kapitole [Filtrovanie protokolov](#).

## Filtrovanie protokolov

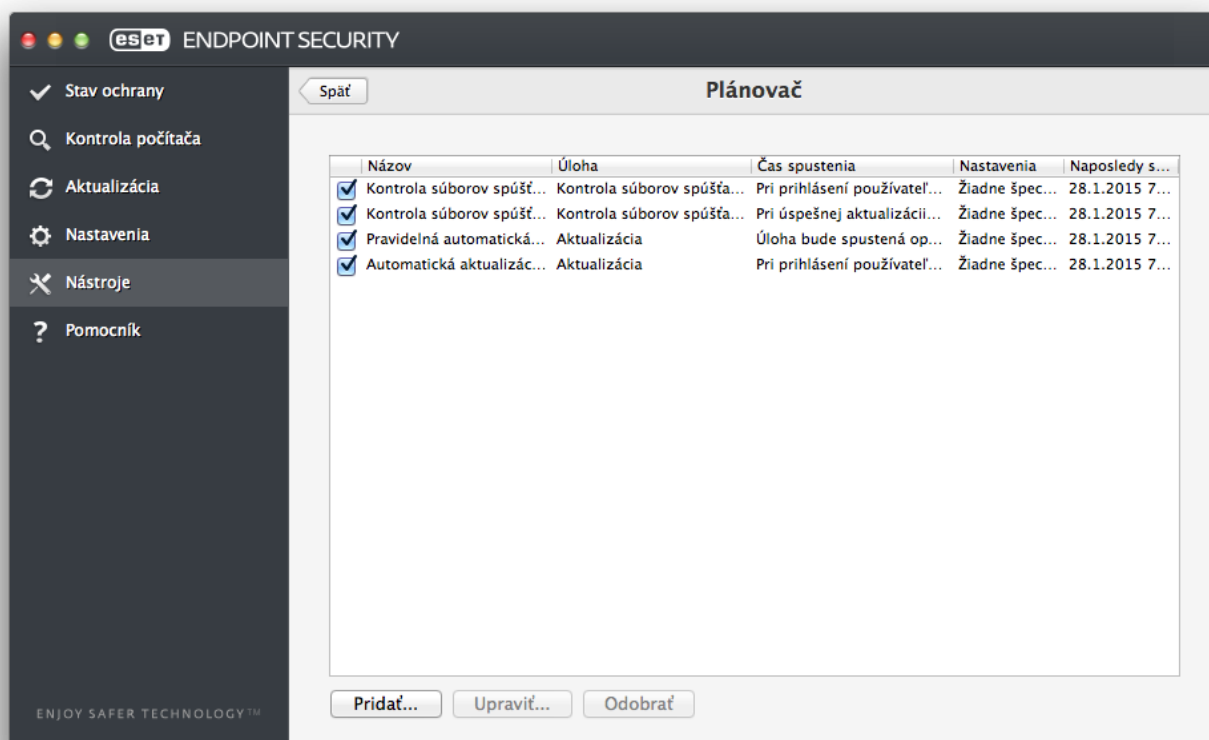
Protokoly uchovávajú informácie o dôležitých systémových udalostiach. Funkcia filtrovania protokolov vám umožňuje zobraziť záznamy týkajúce sa špecifickej udalosti.

Najpoužívanejšie typy protokolov sú uvedené nižšie:

- **Kritické upozornenia** - Kritické systémové chyby (napr. ak sa nespustí Antivírusová ochrana)
- **Chyby** - Chybové hlásenia ako napr. *"Chyba pri sťahovaní súboru"* a kritické chyby
- **Varovania** - Varovné hlásenia
- **Informačné záznamy** - Informatívne správy obsahujúce úspešné aktualizácie, varovania atď.
- **Diagnostické záznamy** - Informácie potrebné pre doladenie programu ako aj protokoly popísané vyššie

# Plánovač

**Plánovač** nájdete v hlavnom menu programu ESET Endpoint Antivirus for macOS v sekcii **Nástroje**. **Plánovač** obsahuje zoznam všetkých naplánovaných úloh a ich nastavení, ako napríklad dátum a čas vykonania kontroly či použitý profil kontroly.



Plánovač spravuje a spúšťa naplánované úlohy s prednastavenými parametrami a vlastnosťami. Parametre úlohy obsahujú informácie ako dátum a čas, ako aj profil, ktorý sa použije počas vykonania úlohy.

Štandardne sa v Plánovači zobrazujú nasledujúce úlohy:

- Údržba protokolov (po zapnutí možnosti **Zobrazovať systémové úlohy** v nastaveniach plánovača)
- Kontrola súborov spúšťaných pri štarte počítača po prihlásení používateľa
- Kontrola súborov spúšťaných pri štarte počítača po úspešnej aktualizácii detekčných modulov
- Pravidelná automatická aktualizácia
- Automatická aktualizácia po prihlásení používateľa

Pre zmenu konfigurácie existujúcej naplánovanej úlohy (predvolenej aj vytvorenej používateľom) stlačte CTRL a kliknite na úlohu, ktorú chcete zmeniť, a zvolte **Upraviť**, prípadne vyberte úlohu a kliknite na tlačidlo **Upraviť...**

# Vytváranie nových úloh

Pre vytvorenie novej úlohy v Plánovači kliknite na tlačidlo **Pridanie plánovanej úlohy** alebo stlačte kláves CTRL, kliknite na prázdne miesto v zozname a zvolte možnosť **Pridať** z kontextového menu. Dostupné sú 4 typy plánovaných úloh:

- Spustenie aplikácie
- Aktualizácia
- Manuálna kontrola počítača
- Kontrola súborov spúšťaných pri štarte počítača

## Plánované úlohy definované používateľom

**i** Na základe predvoleného nastavenia sú aplikácie spúšťané špeciálnym ESET používateľom, ktorý má obmedzené práva. Pre zmenu používateľa zadajte na začiatok príkazu meno želaného používateľa nasledované dvojbodkou (:). Pomocou tejto možnosti môžete spustiť aplikáciu aj pod používateľom **root**.

## Príklad: Spustenie úlohy ako používateľ

V tomto príklade si ukážeme, ako prostredníctvom plánovanej úlohy spustiť pod používateľom **UserOne** v konkrétnom čase aplikáciu Kalkulačka:

1. V **Plánovači** vyberte možnosť **Pridanie plánovanej úlohy**.
2. Zadajte názov úlohy. Ako typ **Plánovanej úlohy** vyberte možnosť **Spustenie aplikácie**. V okne **Vykonanie úlohy** vyberte možnosť **Raz** pre jednorazové spustenie úlohy. Pokračujte kliknutím na tlačidlo **Ďalej**.
- ✓ 3. Kliknite na tlačidlo **Prechádzať** a vyberte aplikáciu Kalkulačka.
4. Na začiatok cesty k aplikácii zadajte **UserOne**:  
(UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') a pokračujte kliknutím na tlačidlo **Ďalej**.
5. Vyberte čas, keď sa má úloha spustiť, a následne kliknite na tlačidlo **Ďalej**.
6. Nastavte, čo sa má stať, ak sa úlohu nepodarí v stanovenom čase spustiť. Potom kliknite na **Ďalej**.
7. Kliknite na tlačidlo **Dokončiť**.
8. Plánovač programu ESET spustí v nastavený čas aplikáciu Kalkulačka.

## Obmedzenia týkajúce sa mena používateľa

**!** Medzery alebo biele znaky nesmú byť použité pred menom používateľa a ani sa v ňom nemôžu vyskytovať. Namiesto toho použite prázdny znak.

## Vykonávanie kontroly ako vlastník adresára

Kontrolu adresárov môžete spustiť ako používateľ, ktorý je vlastníkom daného adresára:

**i** `root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME" '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done`

Ako aktuálne prihlásený používateľ môžete kontrolovať /tmp priečinok:

`root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp`



### Príklad: Úloha na aktualizáciu produktu

V tomto príklade si ukážeme, ako vytvoriť aktualizáciu úlohu, ktorá sa bude spúšťať v konkrétny čas.

1. Z roletového menu **Plánovaná úloha** zvolíte **Aktualizácia**.

2. Zadáte názov do poľa **Názov úlohy**.

3. Frekvenciu opakovania úlohy nastavíte zvolením hodnoty v roletovom menu **Vykonanie úlohy**. Na

✓ základe zvolenej frekvencie budete môcť špecifikovať rozličné parametre aktualizácie. Ak ste si v rámci frekvencie opakovania úlohy zvolili možnosť **Definované používateľom**, budete vyzvaný zadať dátum a čas vo formáte cron (pre viac informácií prejdite na kapitolu [Vytvorenie úlohy definovanej používateľom](#)).

4. V nasledujúcom kroku nastavte, aká akcia sa má vykonať v prípade, že nebude možné spustiť alebo dokončiť úlohu v naplánovanom čase.

5. Kliknite na tlačidlo **Dokončiť**. Nová plánovaná úloha bude pridaná do zoznamu aktuálnych plánovaných úloh.

Už na základe predvolených nastavení obsahuje program ESET Endpoint Antivirus for macOS dôležité plánované úlohy, ktoré sú nakonfigurované tak, aby zaisťovali správne fungovanie. Tieto úlohy by nemali byť menené a štandardne sú skryté. Ak si chcete tieto úlohy prezrieť, z hlavného okna programu kliknite na **Nastavenia** > **Zobraziť pokročilé nastavenia...** > **Plánovač** a zvolíte možnosť **Zobrazovať systémové úlohy**.

## Vytvorenie úlohy definovanej používateľom

Ak z roletového menu **Vykonanie úlohy** chcete vybrať možnosť **Definované používateľom**, je potrebné mať zadefinovaných niekoľko špeciálnych parametrov.

Dátum a čas používateľom definovanej úlohy musí byť zadaný v cron formáte s pridaným údajom o roku (reťazec pozostávajúci zo 6 polí oddelených medzerou):

minúta(0-59) hodina(0-23) deň v mesiaci(1-31) mesiac(1-12) rok(1970-2099) deň v týždni(0-7) (Nedeľa = 0 alebo 7)

### ✓ Príklad:

30 6 22 3 2012 4

Špeciálne znaky podporované v cron výrazoch:

- hviezdička (\*) – nahrádza všetky možné hodnoty v danom poli; napr. hviezdička v treťom poli (deň v mesiaci) znamená každý deň
- spojovník (-) – definuje rozsah; napríklad. 3-9
- čiarka (,) – oddeľuje položky v zozname; napr. 1, 3, 7, 8
- lomka (/) – definuje postupnosť v rozsahu; napr. 3-28/5 v treťom poli (deň v mesiaci) znamená 3. deň v mesiaci a následne každých 5 dní.

Názvy dní ((Monday-Sunday)) a názvy mesiacov ((January-December)) nie sú podporované.



### Plánované úlohy definované používateľom

Ak definujete deň v mesiaci a zároveň deň v týždni, príkaz sa vykoná len vtedy, ak sa budú zhodovať.

# ESET LiveGrid

ESET LiveGrid je pokročilý systém včasného varovania, ktorý umožňuje spoločnosti ESET okamžite reagovať na najnovšie hrozby. Obojsmerný systém včasného varovania LiveGrid má jediný účel – poskytnúť našim zákazníkom najvyššiu možnú ochranu pred novovzniknutými hrozbami. Najlepší spôsob, ako zabezpečiť, aby sme sa dozvedeli o nových hrozbách okamžite po ich objavení, je zozbierať aktuálne informácie o hrozbách od používateľov bezpečnostných produktov ESET. Tieto informácie sú následne analyzované v našich vírusových laboratóriách a spracovávané do aktualizácií detekčných modulov. K dispozícii sú dve možnosti nastavenia:

1. Môžete sa rozhodnúť neaktivovať ESET LiveGrid. Neprídete tým o žiadnu funkcionality programu, avšak pri povolenom systéme ESET LiveGrid dokáže program ESET Endpoint Antivirus for macOS v niektorých prípadoch na nové hrozby reagovať skôr, ako dôjde k aktualizácii detekčných modulov.

2. Môžete sa rozhodnúť ESET LiveGrid aktivovať, čo vám umožní odosielať anonymné informácie o nových hrozbách a o tom, kde sa škodlivý kód nachádza. Podozrivú vzorku je možné poslať na podrobnú analýzu do spoločnosti ESET. Skúmanie týchto vzoriek nám pomôže aktualizovať detekčné moduly a zlepšovať schopnosť našich produktov detegovať hrozby.

ESET LiveGrid zozbiera z vášho počítača len tie informácie, ktoré sa priamo týkajú novej infiltrácie. Môže ísť o vzorku alebo kópiu súboru, v ktorom sa infiltrácia objavila, názov adresára, kde sa súbor nachádzal, názov súboru, dátum a čas detekcie, spôsob, akým sa infiltrácia dostala do vášho počítača a informáciu o operačnom systéme vášho počítača.

Žiadna z týchto informácií V ŽIADNOM PRÍPADE nebude použitá na iný účel, ako je čo najrýchlejšia reakcia na novoobjavenú hrozbu.

Nastavenia systému LiveGrid sú dostupné z hlavného menu programu v časti **Nastavenia > Zobrazíť pokročilé nastavenia... > Live Grid**. Označte možnosť **Zapnúť reputačný systém ESET LiveGrid (odporúčané)**, čím aktivujete systém ESET LiveGrid, a následne kliknite na tlačidlo **Nastavenia...** vedľa popisu **Rozšírené nastavenia**.

## Podozrivé súbory

Na základe predvolených nastavení ESET Endpoint Antivirus for macOS odosiela podozrivé vzorky do vírusového laboratória spoločnosti ESET, kde sú podrobené podrobnej analýze. Ak si neželáte odosielať tieto podozrivé súbory automaticky, zrušte označenie možnosti **Posielať podozrivé súbory** v časti **Nastavenia > Zobrazíť pokročilé nastavenia... > Live Grid > Nastavenia...**

Ak nájdete podozrivý súbor, máte možnosť ho okamžite poslať na analýzu do našich laboratórií. Kliknite v hlavnom menu programu na **Nástroje > Poslať súbor na analýzu**. Ak sa ukáže, že skutočne ide o hrozbu, jej detekcia bude pridaná do najbližšej aktualizácie detekčného jadra.

**Posielanie anonymných štatistických informácií** – systém včasného varovania ESET LiveGrid zbiera anonymné informácie z vášho počítača priamo súvisiace s novými hrozbami. Tieto informácie obsahujú názov infiltrácie, dátum a čas detekcie, verziu bezpečnostného produktu ESET, typ operačného systému a nastavenie umiestnenia. Tieto štatistické informácie sa na servery spoločnosti ESET odosielať raz, prípadne dvakrát za deň.

### Príklad: Zaslané štatistické informácie

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
✓ # osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

**Vylúčenie z posielania** – táto možnosť vám umožňuje vylúčiť niektoré typy súborov zo zasielania do laboratórií ESET. Napríklad môže byť užitočné vylúčiť súbory, ktoré by mohli obsahovať dôverné či citlivé informácie, ako sú dokumenty alebo tabuľky. Najbežnejšie typy takýchto súborov sú už vylúčené na základe predvolených nastavení programu (.doc, .rtf a podobne). Do zoznamu vylúčených súborov sa dajú pridávať aj ďalšie typy súborov.

**Kontaktný e-mail (nepovinný údaj)** – váš kontaktný e-mail bude použitý v prípade, že by boli potrebné doplnkové informácie na vykonanie analýzy podozrivej vzorky. Spoločnosť ESET vás bude prostredníctvom e-mailu kontaktovať len vtedy, keď bude potrebné získať ďalšie informácie.

## Karanténa

Hlavná úloha karantény je bezpečne uchovať infikované súbory. Súbory by mali byť uložené do karantény, ak nemôžu byť vyliečené alebo ak nie je bezpečné alebo odporúčané ich zmazať, prípadne ak ich ESET Endpoint Antivirus for macOS falošne označil ako infikované.

Do karantény môžu byť súbory pridané aj samotným používateľom. Je vhodné tak urobiť napríklad v prípade, že súbor nie je detegovaný antivírusovou kontrolou, ale má podozrivé správanie. Súbory z karantény môžu byť zaslané na analýzu do vírusového laboratória spoločnosti ESET.

Súbory uložené v priečinku karantény je možné zobrazíť v tabuľke, ktorá obsahuje dátum a čas, kedy bol súbor uložený do karantény, cestu k pôvodnému miestu súboru, jeho veľkosť, dôvod (napr. pridaný používateľom) a počet hrozieb (ak archív obsahuje viacero infiltrácií). Priečinok karantény so súbormi uloženými do karantény (*/Library/Application Support/Eset/esets/cache/quarantine*) ostáva v systéme aj po odinštalácii ESET Endpoint Antivirus for macOS. Súbory v karanténe sú uložené v bezpečnej kryptovanej forme a môžu byť obnovené po opätovnej inštalácii ESET Endpoint Antivirus for macOS.

## Uloženie súborov do karantény

ESET Endpoint Antivirus for macOS automaticky ukladá zmazané súbory do karantény (ak ste túto možnosť neodmietli v okne s upozornením). Z okna Karanténa môžete kliknutím na tlačidlo Uložiť do karantény manuálne pridať akýkoľvek súbor do karantény. Kedykoľvek tiež môžete po stlačení klávesu Ctrl a kliknutí na súbor z kontextového menu vybrať možnosť Služby > ESET Endpoint Antivirus for macOS - Presunúť súbory do karantény, čím daný súbor odošlete do karantény.

## Obnovenie súborov z karantény

Súbory uložené do karantény je možné obnoviť na ich pôvodné miesto. Pre tento účel označte požadovaný súbor v karanténe a kliknite na tlačidlo **Obnoviť**. Obnovenie je tiež možné z kontextového menu – súčasne stlačte kláves

CTRL a kliknite na požadovaný súbor v okne Karantény a následne zvolte možnosť **Obnoviť**. Môžete tiež použiť možnosť **Obnoviť do...**, ktorá vám umožňuje obnoviť súbor na iné miesto než to pôvodné, z ktorého bol presunutý do karantény.

## Posielanie súboru z karantény

Ak ste do karantény uložili podozrivý súbor, ktorý nebol detegovaný programom, prípadne ak bol súbor nesprávne vyhodnotený ako infikovaný (napríklad heuristickou analýzou kódu) a následne uložený do karantény, zašlite prosím takýto súbor do Vírusového laboratória ESET. Na odoslanie súboru stlačte CTRL, kliknite na príslušný súbor a zvolte možnosť **Poslať súbor na analýzu** z kontextového menu.

## Oprávnenia

Nastavenia ESET Endpoint Antivirus for macOS môžu byť veľmi dôležité pre bezpečnosť vašej firmy. Neoprávnené zmeny môžu ohroziť stabilitu a ochranu vášho systému. Preto si môžete zvoliť, ktorý používateľ bude mať práva na zmeny nastavení programu.

Ak chcete nastaviť oprávnených používateľov, prejdite do sekcie **Nastavenia > Zobrazíť pokročilé nastavenia... > Používateľ > Oprávnenia**.

Pre zabezpečenie maximálnej ochrany vášho systému je dôležité správne nakonfigurovanie programu. Neoprávnené zmeny môžu viesť ku strate dôležitých informácií. Pre nastavenie zoznamu oprávnených používateľov jednoducho zvolte používateľov zo zoznamu **Používatelia** na ľavej strane a kliknite na tlačidlo **Pridať**. Pre odstránenie používateľa kliknite na jeho meno v zozname **Oprávnení používateľa** a kliknite na **Odobrať**. Pre zobrazenie všetkých systémových používateľov zvolte možnosť **Zobraz všetky používateľov**.

**i** **Prázdny zoznam oprávnených používateľov**  
Ak ponecháte zoznam oprávnených používateľov prázdny, všetci používatelia budú mať oprávnenie vykonávať zmeny v nastaveniach programu.

## Prezentačný režim

**Prezentačný režim** je funkcia určená pre používateľov, ktorí potrebujú neprerušovane používať svoj softvér, neželajú si byť vyrušovaní notifikáciami a dialógovými oknami a požadujú minimálne zaťaženie procesora antivírusovým programom. Prezentačný režim možno použiť aj pri prezentáciách, keď nechcete byť vyrušovaný činnosťou či notifikáciami antivírusu. Po zapnutí prezentačného režimu bude zobrazovanie všetkých notifikácií programu zakázané a naplánované úlohy nebudú spúšťané. Samotná ochrana systému naďalej prebieha na pozadí, ale nevyžaduje žiadne zásahy používateľa.

Pre manuálne zapnutie prezentačného režimu kliknite na **Nastavenia > Zobrazíť pokročilé nastavenia... > Prezentačný režim > Povolíť prezentačný režim**.

Ak si želáte, aby sa prezentačný režim automaticky zapol vždy pri spustení aplikácie v režime na celú obrazovku, označte možnosť **Automaticky povoliť v režime celej obrazovky**. Prezentačný režim sa automaticky zapne vždy, keď spustíte aplikáciu na celú obrazovku a po jej skončení sa opäť automaticky vypne. Táto možnosť je užitočná pre okamžité spustenie prezentačného režimu pri začatí prezentácie.

Môžete tiež označiť možnosť **Automaticky vypnúť prezentačný režim po určenom čase** a zadať požadované

časové obdobie (v minútach), po uplynutí ktorého sa Prezentačný režim automaticky vypne.

Zapnutie prezentačného režimu môže predstavovať potenciálne bezpečnostné riziko, a preto sa ikona stavu ochrany v ESET Endpoint Antivirus for macOS zmení na oranžovú a zobrazí sa upozornenie.

## Spustené procesy

Zoznam **spustených procesov** zobrazuje spustené programy a procesy na vašom počítači a zabezpečuje pohotovú a neustálu informovanosť spoločnosti ESET o nových infiltráciách. Prostredníctvom technológie ESET LiveGrid poskytuje ESET Endpoint Antivirus for macOS detailnejšie informácie o spustených procesoch.



- **Proces** – názov aplikácie alebo procesu, ktorý aktuálne beží na vašom počítači. Tiež môžete použiť tzv. Activity monitor (nájdete ho v časti */Applications/Utilities*) pre zobrazenie všetkých procesov spustených na tomto počítači.
- **Úroveň rizika** – vo väčšine prípadov priradí ESET Endpoint Antivirus for macOS stupeň rizika pomocou technológie LiveGrid na základe heuristických pravidiel a kontroly každého subjektu pre prítomnosť škodlivého kódu. Potom na základe týchto výsledkov prideli procesom úroveň rizika. Aplikácie označené zelenou farbou sú bezpečné a budú vyňaté z kontroly. Toto urýchľuje rýchlosť Kontroly počítača alebo Rezidentnej ochrany súborového systému. Aj v prípade, že je aplikácia označená oranžovou farbou, nemusí to znamenať, že obsahuje škodlivý kód. Obvykle je to nová aplikácia. Ak si nie je používateľ istý, či je to naozaj tak, má možnosť poslať súbor na analýzu do vírusového laboratória spoločnosti ESET. Ak sa potvrdí, že ide o aplikáciu obsahujúcu škodlivý kód, jej detekcia bude zahrnutá do ďalšej aktualizácie.
- **Počet používateľov** – počet používateľov, ktorí používajú danú aplikáciu. Táto informácia je získavaná technológiou ESET LiveGrid.
- **Čas objavenia** – doba, odkedy bol proces objavený technológiou ESET LiveGrid.
- **ID aplikačného zväzku** – názov výrobcu alebo proces aplikácie.

Po kliknutí na jednotlivé aplikácie sa v spodnej časti okna zobrazia nasledovné informácie:

- **Súbor** – umiestnenie aplikácie na vašom počítači,
- **Veľkosť súboru** – fyzická veľkosť súboru na disku,
- **Popis súboru** – charakteristika súboru, vychádzajúca z jeho popisu od operačného systému,
- **ID aplikačného zväzku** – názov výrobcu alebo proces aplikácie,
- **Verzia súboru** – informácia od vydavateľa aplikácie,
- **Názov produktu** – názov aplikácie, obvykle obchodné meno.

# Používateľské rozhranie

Nastavenia používateľského rozhrania vám umožňujú prispôbiť pracovné prostredie vašim potrebám. Tieto možnosti sú dostupné v časti **Nastavenia > Zobrazíť pokročilé nastavenia...** (prípadne stlačte `cmd+,`) > **Rozhranie**.

- Pre zobrazenie úvodného obrázku ESET Endpoint Antivirus for macOS pri štarte systému zvolte možnosť **Zobrazovať úvodný obrázok pri štarte**.
- Možnosť **Zobrazovať aplikáciu v Docku** umožňuje zobrazenie ikonky ESET Endpoint Antivirus for macOS  v macOS docku a prepínanie medzi ESET Endpoint Antivirus for macOS a inými spustenými aplikáciami stlačením `cmd+tab`. Zmena sa prejaví po reštarte programu ESET Endpoint Antivirus for macOS (obvykle po reštarte počítača).
- Možnosť **Používať štandardné menu** vám umožňuje používať niektoré klávesové skratky (pozri [Klávesové skratky](#)) a zobrazovať štandardné položky menu (Používateľské rozhranie, Nastavenia a Nástroje) na hornej lište (Menu bar) systému macOS.
- Pre zobrazovanie popisov (tzv. tooltips) k tlačidlám a voľbám programu ESET Endpoint Antivirus for macOS zapnite možnosť **Zobrazovať popisy tlačidiel**.
- Možnosť **Zobrazovať skryté súbory** vám umožňuje vidieť skryté súbory v nastaveniach **Cieľov kontroly v Kontrole počítača**.
- Na základe predvolených nastavení sa ikona programu ESET Endpoint Antivirus for macOS  zobrazuje v pravej časti hornej lišty (Menu Bar Extras) systému macOS. Ak si želáte zobrazovanie ikony vypnúť, zrušte označenie možnosti **Zobrazíť ikonku v doplnkoch panela s ponukami**. Zmena sa prejaví po reštarte programu ESET Endpoint Antivirus for macOS (obvykle po reštarte počítača).

## Výstrahy a upozornenia

Sekcia **Výstrahy a upozornenia** vám umožňuje nastaviť, ako sa budú správať výstražné upozornenia a systémové oznámenia a aké stavy ochrany sa budú zobrazovať v ESET Endpoint Antivirus for macOS.

Vypnutie možnosti **Zobrazovať výstražné upozornenia** vypne všetky výstražné upozornenia a je vhodné len pre špecifické situácie. Pre väčšinu používateľov je odporúčané nechať túto možnosť zapnutú (štandardné nastavenie). Pokročilé nastavenia sú opísané [v tejto kapitole](#).

Zvolením možnosti **Zobrazovať upozornenia na pracovnej ploche** zapnete výstražné okná, ktoré nevyžadujú zásah používateľa, na pracovnej ploche (štandardne v pravom hornom rohu obrazovky). Zadaním hodnoty **Upozornenia zatvárať automaticky po X sekundách** môžete nastaviť čas zobrazenia každej notifikácie (predvolene 5 sekúnd).

Od verzie ESET Endpoint Antivirus for macOS 6.2 môžete zabrániť zobrazovaniu niektorých **Stavov ochrany** v hlavnom okne programu (okno **Stav ochrany**). Viac sa dozviete v kapitole [Stavy ochrany](#).

## Zobrazovanie upozornení

ESET Endpoint Antivirus for macOS zobrazuje výstražné upozornenia, ktoré vás informujú o nových verziách programu, aktualizáciách operačného systému, vypnutí určitých programových komponentov, mazaní záznamov a podobne. V každom takomto okne môžete potlačiť jednotlivé notifikácie zvolením možnosti **Tento dialóg už nezobrazovať**.

**Zoznam hlásení (Nastavenia > Zobrazíť pokročilé nastavenia... > Výstrahy a upozornenia > Zobrazovať výstražné upozornenia: Nastavenia...)** zobrazuje zoznam všetkých výstražných dialógov, ktoré spúšťa ESET Endpoint Antivirus for macOS. Pre povolenie alebo vypnutie jednotlivých notifikácií použite zaškrŕavacie políčka pri **Názve hlásenia**. Navyše je možné definovať **Podmienky zobrazenia**, ktoré určujú podmienky vykonania danej akcie.

## Stavy ochrany

Aktuálny stav ochrany ESET Endpoint Antivirus for macOS môžete meniť aktivovaním a deaktivovaním stavov v časti **Nastavenia > Zobrazíť pokročilé nastavenia... > Výstrahy a upozornenia > Zobrazíť na obrazovke Stav ochrany: Nastavenia....** Stav rôznych funkcií programu bude zobrazený alebo schovaný z hlavnej obrazovky ESET Endpoint Antivirus for macOS (okno **Stav ochrany**).

Stav ochrany môžete schovať pre nasledujúce funkcie a moduly:

- Anti-Phishing
- Ochrana prístupu na web
- Ochrana e-mailových klientov
- Prezentačný režim
- Aktualizácia operačného systému
- Vypršanie licencie
- Vyžaduje sa reštart počítača

## Kontextové menu

Integrácia funkcií ESET Endpoint Antivirus for macOS do kontextového menu systému môže byť povolená v časti **Nastavenia > Zobrazíť pokročilé nastavenia... > Kontextové menu** zvolením možnosti **Pridať do kontextového menu**. Zmeny sa prejavia po odhlásení sa alebo reštartovaní počítača. Možnosti kontextového menu budú dostupné v okne **Finder** po stlačení tlačidla CTRL a kliknutí na ľubovoľný súbor alebo priečinok.

## Aktualizácia

Pravidelné aktualizácie programu ESET Endpoint Antivirus for macOS sú kľúčom k udržaniu čo najvyššej úrovne bezpečnosti. Modul aktualizácií zabezpečuje, aby bol program vždy aktuálny a obsahoval tú najnovšiu verziu detekčného jadra.

V sekcii **Aktualizácia** v hlavnom okne programu je zobrazený aktuálny stav aktualizácie, vrátane informácie o dátume a čase poslednej úspešnej aktualizácie, prípadne aj o dostupnosti novej aktualizácie. Proces aktualizácie môžete spustiť manuálne kliknutím na tlačidlo **Aktualizovať moduly**.

Za normálnych okolností (keď pravidelné sťahovanie aktualizácií prebieha úspešne) sa v okne **Aktualizácia** zobrazuje správa *Aktualizácia nie je potrebná – nainštalované moduly sú aktuálne*. Ak moduly nie je možné aktualizovať, odporúčame vám skontrolovať [nastavenia aktualizácie](#) – najčastejšou príčinou neúspešného sťahovania aktualizácií sú nesprávne zadané [licenčné údaje](#), prípadne nesprávne nastavené [pripojenie](#).

V okne **Aktualizácia** taktiež nájdete číslo verzie detekčného jadra. Po kliknutí na toto numerické označenie budete presmerovaný na webovú stránku spoločnosti ESET s informáciami o nových vzorkách v rámci danej aktualizácie detekčného jadra.

## Nastavenie aktualizácií

V sekcii Aktualizácia môžete konfigurovať aktualizčné servery, z ktorých si program bude sťahovať aktualizácie modulov. Ak server vyžaduje autentifikáciu, máte možnosť zadať príslušné meno a heslo. Roletové menu **Server aktualizácie** je predvolene nastavené na možnosť **Automatický výber servera**. Tým je zabezpečené, že aktualizácie sa automaticky sťahujú z aktualizčných serverov spoločnosti ESET s minimálnym zaťažením siete.

The screenshot shows the 'Aktualizácia' (Updates) window in a Mac OS style. At the top, there are window controls and a title bar. Below the title bar, there are navigation arrows and a button 'Ukázať všetko'. The main content area has two tabs: 'Primárny' (Primary) and 'Sekundárny' (Secondary). Under the 'Primárny' tab, there is a section 'Server aktualizácie' (Update server) with a dropdown menu set to 'Automatický výber servera' and an 'Upraviť...' button. Below this are input fields for 'Meno:' (Name) and 'Heslo:' (Password). Further down is a 'Režim proxy:' (Proxy mode) dropdown set to 'Použiť globálne nastavenie proxy servera' (Use global proxy server settings), with a descriptive text below it. Below the proxy mode is a 'Proxy server' section with an input field for the proxy address, a port field set to '3128', and a 'Detegovať' (Detect) button. Below these are input fields for 'Meno:' and 'Heslo:', and a checkbox 'Ukázať heslo' (Show password). At the bottom of the proxy section is a checkbox 'Použite priame pripojenie, ak nie je k dispozícii HTTP proxy' (Use direct connection if HTTP proxy is not available). Below the proxy section are two buttons: 'Rozšírené nastavenia: Nastavenia...' (Advanced settings: Settings...) and 'Vyčistiť aktualizáciu vyrovnávacu pamäť: Vyčistiť' (Clear update cache: Clear). At the very bottom, there is a 'Štandardné' (Standard) button and a help icon.



Zoznam dostupných aktualizčných serverov nájdete v roletovom menu **Server aktualizácie**. Pre pridanie nového aktualizčného servera kliknite na tlačidlo **Upraviť...**, zadajte adresu nového servera do poľa **Aktualizačný server** a kliknite na **Pridať**.

ESET Endpoint Antivirus for macOS umožňuje nastaviť alternatívny alebo záložný (tzv. failover) server pre aktualizácie. **Primárny** server môže byť váš mirror server a ako **Sekundárny server** môžete použiť štandardný aktualizčný server spoločnosti ESET. Sekundárny server sa musí líšiť od primárneho, inak nebude použitý. Ak nešpecifikujete Sekundárny server, Meno a Heslo, funkcionality záložného aktualizčného servera nebude fungovať. Môžete tiež zvoliť možnosť Automatický výber servera a zadať vaše používateľské meno a heslo, aby program ESET Endpoint Antivirus for macOS automaticky vybral a použil ten najvhodnejší aktualizčný server.

**Režim proxy** vám umožňuje aktualizovať detekčné moduly použitím proxy servera (napr. cez lokálny HTTP proxy server). Tento server sa môže ale nemusí zhodovať s globálnym proxy serverom, ktorý sa používa pre všetky programové funkcie a komponenty vyžadujúce pripojenie. Nastavenia globálneho proxy servera by mali byť definované už počas inštalácie programu alebo v [nastaveniach proxy servera](#).

Sťahovanie aktualizácií výhradne z proxy servera nastavíte nasledovne:

1. Z roletového menu vyberte možnosť **Spojenie pomocou proxy servera**.
2. Kliknite na **Detegovať**, aby program ESET Endpoint Antivirus for macOS sám vyplnil IP adresu a číslo portu (predvolene **3128**).
3. Ak sa pre prístup k proxy serveru vyžaduje autentifikácia, zadajte platné prístupové údaje do polí **Meno** a **Heslo**.

ESET Endpoint Antivirus for macOS preberá nastavenia proxy zo Systémových nastavení macOS. Konfigurácia proxy servera je v macOS dostupná po kliknutí na  > **Systémové nastavenia** > **Sieť** > **Rozšírené** > **Proxy**.

Ak povolíte možnosť **Použiť priame pripojenie, ak nie je k dispozícii HTTP proxy**, ESET Endpoint Antivirus for macOS sa automaticky pokúsi nadviazať spojenie s aktualizčnými servermi bez použitia proxy. Táto možnosť je vhodná pre mobilných používateľov s laptopmi MacBook.

Ak má program problémy pri sťahovaní aktualizácií detekčných modulov, skúste vyčistiť aktualizčnú vyrovnávaciu pamäť (cache) a vymazať dočasné aktualizčné súbory stlačením tlačidla **Vyčistiť**.

## Rozšírené nastavenia

Ak si neželáte zobrazovať upozornenie po každej úspešnej aktualizácii, ktorá v programe prebehne, označte možnosť **Nezobrazovať oznámenie o úspešnej aktualizácii**.

Možnosť **Predbežné aktualizácie** umožňuje sťahovanie aktualizácií modulov vo finálnej fáze testovania ešte pred ich vydaním. Výhodou povolenia predbežných aktualizácií je možnosť prístupu k najnovším opravám, ktoré môžu pomôcť pri riešení problémov s produktom. Možnosť Oneskorené aktualizácie umožňuje sťahovať aktualizácie niekoľko hodín po tom, čo boli vydané. Výhodou je sťahovanie overených aktualizácií otestovaných v reálnom prostredí, ktoré nespôsobujú problémy a sú stabilné.

ESET Endpoint Antivirus for macOS zálohuje programové a detekčné moduly pre prípad obnovenia staršej verzie

(tzv. **rollback**). Aby sa automaticky vytvárali snímky (tzv. snapshoty) modulov, ponechajte možnosť **Povoliť zálohovanie modulov** označenú. Ak máte podozrenie, že nová verzia detekčného jadra alebo programových modulov môže byť nestabilná alebo poškodená, môžete prejsť späť na predchádzajúcu verziu a na určený časový interval pravidelné aktualizácie pozastaviť. V tejto sekcii tiež môžete povoliť pravidelné aktualizácie, ktoré ste predtým odložili na neurčito. Ak sa rozhodnete vykonať obnovu predchádzajúcej verzie modulov zo zálohy, použite roletové menu **Nastaviť dobu pozastavenia aktualizácie modulov** pre nastavenie časového obdobia, počas ktorého budú pravidelné aktualizácie pozastavené. Ak si želáte pravidelné aktualizácie odložiť na neurčito, až pokým ich neskôr manuálne nepovolíte, vyberte možnosť **Do zrušenia**. Časové obdobie, počas ktorého budú aktualizácie pozastavené, nastavujte obozretne, keďže odkladanie aktualizácií na dlhší čas môže predstavovať potenciálne bezpečnostné riziko.

**Automaticky nastaviť maximálny vek detekčného jadra** – umožňuje vám nastaviť maximálne časové obdobie (v dňoch), po uplynutí ktorého bude detekčné jadro považované za neaktuálne a používateľovi sa zobrazí upozornenie. Prednastavená hodnota je 7 dní.

## Ako vytvoriť aktualizáciu úlohu

Aktualizáciu je možné kedykoľvek manuálne spustiť kliknutím na možnosť **Aktualizovať moduly** v časti **Aktualizácia** v hlavnom okne programu.

Aktualizácie sa dajú spúšťať aj ako plánované úlohy. Tie možno nastaviť po kliknutí na **Nástroje > Plánovač**. V programe ESET Endpoint Antivirus for macOS sú predvolene aktivované nasledujúce aktualizčné úlohy:

- **Pravidelná automatická aktualizácia**
- **Automatická aktualizácia po prihlásení používateľa**

Každú z vyššie uvedených aktualizčných úloh môžete upraviť tak, aby zodpovedala vašim potrebám. Okrem predvolených aktualizčných úloh môžete vytvoriť nové plánované úlohy s vlastným nastavením. Pre bližší popis vytvárania a nastavenia aktualizčných úloh si pozrite kapitolu [Plánovač](#).

## Aktualizácie systému

Možnosť aktualizovať operačný systém macOS je dôležitým prvkom ochrany používateľov pred škodlivým softvérom. Pre udržanie maximálnej úrovne bezpečnosti odporúčame nainštalovať tieto aktualizácie ihneď po ich zverejnení. ESET Endpoint Antivirus for macOS vás bude notifikovať o chýbajúcich aktualizáciách na základe úrovne zobrazovania, ktorú si nastavíte. Dostupnosť notifikácií si môžete upraviť v sekcii **Nastavenia > Zobrazíť pokročilé nastavenia...** (prípadne stlačte cmd+,) > **Výstrahy a upozornenia > Nastavenia.... Použite voľbu Podmienky zobrazenia**, ktorá sa nachádza v riadku **Aktualizácie operačného systému**.

- **Zobrazíť všetky aktualizácie** – upozornenie sa zobrazí v prípade každej chýbajúcej aktualizácie.
- **Iba odporúčané aktualizácie** - budete informovaný iba o odporúčaných aktualizáciách.

Ak nechcete byť informovaný o chýbajúcich aktualizáciách systému, zrušte označenie možnosti **Aktualizácie operačného systému**.

Okno informujúce o dostupnosti aktualizácií vám poskytuje prehľad o aktualizáciách pre operačný systém macOS a aplikácie aktualizované cez "natívny" nástroj macOS - Software updates. Aktualizácie môžete spustiť priamo z okna upozornení alebo z programu ESET Endpoint Antivirus for macOS > sekcia **Domov** > **Inštalovať chýbajúcu aktualizáciu**.

Okno upozornení obsahuje názov aplikácie, verziu, veľkosť, vlastnosti (flags) a ďalšie informácie o dostupných aktualizáciách. Stĺpec **Flags** (alebo **Vlastnosti**) obsahuje:

- **[odporúčané]** - výrobca operačného systému odporúča nainštalovať takúto aktualizáciu pre zvýšenie bezpečnosti a stability systému
- **[reštart]** - reštart počítača je v tomto prípade vyžadovaný
- **[vypnúť]** - počítač musíte vypnúť a zapnúť

Okno s upozornením zobrazuje aktualizácie získané pomocou nástroja príkazového riadka 'softwareupdate'. Aktualizácie získané týmto nástrojom sa môžu líšiť od aktualizácií zobrazených aplikáciou „Aktualizácia softvéru“. Ak si želáte nainštalovať všetky dostupné aktualizácie zobrazené v okne „Chýbajúce aktualizácie systému“ a taktiež tie, ktoré nie sú zobrazené aplikáciou „Aktualizácia softvéru“, musíte použiť nástroj príkazového riadka „softwareupdate“. Viac sa o nástroji „softwareupdate“ dozviete v príslušnej používateľskej príručke, ktorá je dostupná po zadaní príkazu `man softwareupdate` do okna **Terminálu**. Táto možnosť je určená iba pre skúsených používateľov.

## Import a export nastavení

Možnosť importovať a exportovať nastavenia ESET Endpoint Antivirus for macOS sa nachádza pod položkou **Nastavenia** v hlavnom menu.

Import aj Export používajú súbor na ukladanie konfigurácie. Tieto možnosti sú užitočné pri ukladaní aktuálnej konfigurácie programu ESET Endpoint Antivirus for macOS pre neskoršie použitie. Export nastavení je užitočný pri nastavovaní vlastnej preferovanej konfigurácie ESET Endpoint Antivirus for macOS na viacerých systémoch. Stačí, ak prenesiete konfiguráciu z vyexportovaného súboru, čím sa prenesú preferované nastavenia na cieľový systém.



Pre import kliknite na **Import nastavení** a zadajte do poľa **Názov súboru** cestu ku konfiguračnému súboru alebo kliknite na tlačidlo **Prehľadávať...** a vyhľadajte požadovaný súbor. Pre export vyberte možnosť **Export nastavení** a zadajte Názov súboru. Vo vyhľadávači vyberte umiestnenie, na ktoré sa súbor s nastaveniami uloží.

## Nastavenie proxy servera

Nastavenia proxy servera môžete upravovať v sekcii **Nastavenia > Zmeniť pokročilé nastavenia... > Proxy server**. Nastavenia proxy servera vykonané na tejto úrovni platia ako globálne nastavenia proxy servera pre celý ESET Endpoint Antivirus for macOS. Tu nastavené parametre sa použijú vo všetkých moduloch, ktoré potrebujú pripojenie na Internet. ESET Endpoint Antivirus for macOS podporuje nasledujúce spôsoby overenia: Basic Access a NTLM (NT LAN Manager).

Ak chcete upraviť nastavenia proxy servera na tejto úrovni, označte možnosť **Používať proxy server** a potom zadajte IP adresu alebo URL proxy servera do poľa **Proxy server**. Do poľa Port zadajte číslo portu, na ktorom proxy server prijíma spojenie (predvolene 3128). Môžete tiež kliknúť na **Detegovať**, aby program obe polia predvyplnil.

Ak sa pre komunikáciu s proxy serverom vyžaduje aj autorizácia, zadajte platné **Meno** a **Heslo** do príslušných polí.

## Zdieľaná lokálna vyrovnávacia pamäť

Ak si želáte povoliť používanie tejto funkcie, prejdite do sekcie **Nastavenia > Zobraziť pokročilé nastavenia... > Zdieľaná lokálna vyrovnávacia pamäť** a aktivujte možnosť **Používanie vyrovnávacej pamäte**. Táto funkcia zvyšuje výkon vo virtualizovaných prostrediach tým, že predchádza duplicitnej kontrole na sieti. Každý súbor bude skontrolovaný len raz a uložený v zdieľanej vyrovnávacej pamäti (cache). Ak je táto funkcia aktívna, informácie o kontrolách súborov a priečinkov vo vašej sieti budú uložené do lokálnej vyrovnávacej pamäte. Pri novej kontrole bude ESET Endpoint Antivirus for macOS hľadať kontrolované súbory vo vyrovnávacej pamäti. Ak nájde zhodné súbory, vynechá ich z kontroly.

Nastavenia zdieľanej lokálnej vyrovnávacej pamäte obsahujú:

- **Server** – názov alebo IP adresa počítača, na ktorom sa nachádza vyrovnávacia pamäť.

- **Port** – číslo portu použitého pre komunikáciu (predvolene 3537).
- **Heslo** – voliteľne môžete nastaviť heslo.

### Podrobné inštrukcie

**i** Podrobné inštrukcie, ako nainštalovať a nakonfigurovať ESET Zdieľanú lokálnu vyrovnávaciu pamäť nájdete v [Používateľskej príručke](#). (Príručka je dostupná iba v angličtine.)

## Licenčná dohoda s koncovým používateľom

**DÔLEŽITÉ:** Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIU, STIAHNUŤ, 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 (ďalej len „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 (ďalej len „ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou (ďalej len „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. Ak s niektorými podmienkami a požiadavkami tejto Dohody nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalčné 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 USTANOVENIAMÍ.

**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 (ďalej len „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, číslíc 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 Dohody a dodržiavate všetky jej zmluvné podmienky, Poskytovateľ vám udeľuje nasledujúce práva (ďalej len „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 (ďalej len „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 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) Business Edition.** Pre 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.** OEM Softvér sa viaže na počítač, s ktorým ste ho získali. 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 zániku Licencie musíte Softvér a všetky jeho záložné kópie okamžite zničiť alebo na vlastné 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 zhromažďovanie údajov je nevyhnutné na tieto funkcie Softvéru:

a) **Aktualizácia Softvéru.** Poskytovateľ môže z času na čas vydať aktualizáciu Softvéru („Update“), avšak nie je 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. Na účely poskytovania 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.

b) **Preposielanie infiltrácií a informácií Poskytovateľovi.** Softvér obsahuje funkcie, ktoré zhromažďujú vzorky počítačových vírusov a iných škodlivých počítačových programov, ako aj podozrivých, problémových, potenciálne nechcených alebo potenciálne nebezpečných objektov, ako sú napríklad súbory, URL adresy, IP pakety a ethernetové rámce (ďalej len „Infiltrácie“), a potom ich odosiela Poskytovateľovi vrátane, nie však výhradne, informácií o procese inštalácie, počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, a/alebo informácií o prevádzke a fungovaní Softvéru a informácie o zariadeniach v lokálnych sieťach, ako sú typ, dodávateľ, model a/alebo názov zariadenia (ďalej len „Informácie“.) Informácie a Infiltrácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov) o Koncovom používateľovi alebo iných používateľoch počítača, v ktorom je Softvér nainštalovaný, a súboroch postihnutých Infiltráciami spolu so súvisiacimi metaúdajmi.

Informácie a Infiltrácie sa môžu zhromažďovať prostredníctvom nasledujúcich funkcií Softvéru:

i. Súčasťou funkcie LiveGrid Reputation System je zhromažďovanie a odosielanie jednosmerných hodnôt hash súvisiacich s infiltráciami Poskytovateľovi. Táto funkcia sa zapína v štandardných nastaveniach Softvéru.

ii. Súčasťou funkcie LiveGrid Feedback System je zhromažďovanie a odosielanie Infiltrácií spolu so súvisiacimi metaúdajmi a Informáciami Poskytovateľovi. Túto funkciu môže aktivovať Koncový používateľ počas inštalácie Softvéru.

Poskytovateľ použije získané Informácie a Infiltrácie iba na účely analýzy a preskúmania Infiltrácií, vylepšenia Softvéru a overenia pravosti Licencie, pričom vykoná primerané opatrenia na zachovanie zabezpečenia získaných Infiltrácií a Informácií. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Infiltrácie a Informácie v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Tieto funkcie môžete kedykoľvek deaktivovať.

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. Týmto súhlasíte s prijímaním oznámení a správ vrátane, okrem iného, marketingových informácií.

**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, reprodukovat', alebo prevádzkať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

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

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzkať 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 zahrňajúce 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 Zmluvy budete spätne analyzovať, dekompilovať, prevádzkať 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, čím nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Zmluvy.

**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 kópií 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 predáť, 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. 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 AKÝKOĽVEK 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, VZNIKNUTE POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOLKO 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. 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 používateľ (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 licencií 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 licencií (meno používateľa a heslo). Informácie o Licencií 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 (ďalej iba 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 vládny, 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 (ďalej iba Zákony na kontrolu vývozu); 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 vládny, 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 (ďalej iba Sankčné zákony).

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.

**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 akýchkoľvek 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. V prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí anglická verzia. Zmeny tejto Dohody sú možné iba v písomnej forme, pričom za Poskytovateľa musí takúto zmenu podpísať štatutárny zástupca alebo osoba k tomuto úkonu výslovne splnomocnená.

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.

EULA ID: BUS-STANDARD-20-01

## Privacy Policy

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, chce byť ako kontrolór údajov (ďalej len „ESET“ alebo „my“ alebo formulácie vyjadrené v prvej osobe množného čísla) pri spracovaní osobných údajov a ochrane osobných údajov svojich zákazníkov transparentná. S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať našich zákazníkov (ďalej len „koncový používateľ“ alebo „vy“ alebo formulácie vyjadrené v druhej osobe množného čísla) o nasledujúcich témach:

- Spracovávanie osobných údajov,
- Dôvernoscť údajov,
- práva dotknutej osoby.

## Spracovávanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho produktu sa poskytujú za podmienok Licenčnej zmluvy koncového používateľa (ďalej len "EULA"), niektoré z nich však môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o zhromažďovaní údajov, ktoré súvisí s poskytovaním našich služieb. Poskytujeme rôzne služby, ktoré sú opísané v zmluve EULA, ako aj v produktovej dokumentácii. Patria k nim napríklad služby aktualizácie/inovácie, ESET LiveGrid®, ochrana pred zneužitím údajov, podpora atď. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

- Informácie o aktualizáciách a ďalšie štatistické informácie týkajúce sa procesu inštalácie a počítača vrátane

informácií o platforme, na ktorej je produkt nainštalovaný, a informácií o operáciách a funkčnosti našich produktov, napríklad informácie o operačnom systéme, hardvéri, identifikátoroch inštalácie, identifikácii licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu.

- Jednosmerné haše súvisiace s infiltráciami, ktoré sú zhromažďované v rámci reputačného systému ESET LiveGrid® a ktorými sa zlepšuje účinnosť našich antimalvérových riešení na základe porovnávania naskenovaných súborov s databázou položiek zaradených na whitelist a blacklist v cloude.
- Prijaté podozrivé vzorky a metadáta zhromažďované v rámci systému spätnej väzby ESET LiveGrid®, ktoré umožňujú spoločnosti ESET okamžite reagovať na potreby svojich koncových používateľov, ako aj na najnovšie hrozby. Spoliehame sa na to, že nám zašlete

Oinfiltrácie, ako napríklad vzorky potenciálnych vírusov a iných škodlivých a podozrivých programov; problematické, potenciálne neželané alebo potenciálne nebezpečné objekty, ako napríklad spustiteľné súbory, e-mailové správy, ktoré ste nahlásili ako spam alebo ktoré takto označil váš produkt;

Oinformácie o zariadeniach v lokálnej sieti, ako napríklad typ, dodávateľ, model a/alebo názov zariadenia;

Oinformácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;

Osúbory výpisov pri zlyhaní a informácie, ktoré obsahujú.

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 názvov súborov či URL adries a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

- 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.

## Dôvernosť údajov

ESET je spoločnosť s celosvetovou pôsobnosťou prostredníctvom pridružených subjektov alebo partnerov, ktorí sú súčasťou našej distribučnej, servisnej či podpornej siete. Informácie spracúvané spoločnosťou ESET sa môžu na účely výkonu zmluvy EULA, napríklad na poskytovanie služieb či podpory alebo fakturácie, prenášať medzi jednotlivými pridruženými subjektmi alebo partnermi. V závislosti od vašej polohy a služby, ktorú si vyberiete, sa od nás môže žiadať prenos vašich údajov do krajiny, v ktorej neplatí príslušné rozhodnutie Európskej komisie. Aj v takom prípade podlieha každý prenos informácií úprave vychádzajúcej z právnych predpisov o ochrane údajov a uskutočňuje sa iba v prípade potreby. Bez výnimky musia byť zavedené štandardné zmluvné doložky, záväzné vnútropodnikové pravidlá alebo iné vhodné záruky.

Čo najviac sa snažíme zabrániť tomu, aby sa pri poskytovaní služieb podľa zmluvy EULA údaje uchovávali dlhšie, než je naozaj potrebné. Obdobie uchovávania môže prekračovať platnosť vašej licencie, aby ste mali čas na jej jednoduché a pohodlné obnovenie. Minimalizované a pseudonymizované štatistické a iné údaje zo systému ESET LiveGrid® sa môžu ďalej spracúvať na štatistické účely.

Spoločnosť ESET realizuje vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti, ktorá zodpovedá potenciálnym rizikám. Čo najlepšie sa snažíme zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania údajov. V prípade úniku údajov, ktorý má za následok ohrozenie vašich práv a slobôd, sme však pripravení informovať dozorný orgán, ako aj dotknuté osoby. Ako dotknutá osoba máte právo podať sťažnosť dozornému orgánu.

## Práva dotknutej osoby

Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. V súlade s podmienkami určenými príslušnými zákonmi na ochranu údajov máte ako dotknutá osoba tieto práva:

- právo požiadať spoločnosť ESET o prístup k svojim osobným údajom;
- právo na opravu svojich osobných údajov, ak sú nepresné (máte tiež právo doplniť neúplné osobné údaje);
- právo požiadať o vymazanie svojich osobných údajov;
- právo požiadať o zákaz spracovania svojich osobných údajov;
- právo namietat' voči spracovaniu
- právo podať sťažnosť, ako aj
- právo na prenosnosť údajov.

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