ENDPOINT SECURITY

pre macOS

Používateľská príručka

(určená pre verziu 6.0 a vyššiu)

Pre stiahnutie najnovšej verzie tohto dokumentu kliknite sem

Technická podpora: http://support.eset.sk

REV. 24. 4. 2017

Obsah

1. ESET Endpoint Security....4
1.1 Čo je nové vo verzii 6....4
1.2 Systémové požiadavky....4
2. Dokumentácia pre používateľov pripojených cez ESET Remote Administrator....4
2.1 ESET Remote Administrator Server....5
2.2 Web Console....5
2.3 Proxy....5
2.4 Agent....5
2.5 RD Sensor....6
3. Inštalácia....6
3.1 Typická inštalácia....6
3.2 Pokročilá inštalácia....7
3.3 Vzdialená inštalácia....7
3.3.1 Vytvorenie balíčka pre vzdialenú inštaláciu....7
3.3.2 Inštalácia na cieľovú stanicu....8
3.3.3 Vzdialená odinštalácia....8
3.3.4 Aktualizácia staníc....8
4. Aktivácia produktu....8
5. Odinštalácia....9
6. Stručný prehľad....9
6.1 Klávesové skratky....9
6.2 Kontrola funkčnosti programu....10
6.3 Čo robiť ak program nepracuje správne....10
7. Ochrana počítača....10
7.1 Antivirus a antispyware....10
7.1.1 Všeobecné....10
7.1.1.1 Vylúčenia....10
7.1.2 Ochrana pri štarte počítača....11
7.1.3 Rezidentná ochrana súborového systému....11
7.1.3.1 Rozšírené nastavenia....11
7.1.3.2 Kedy je vhodné upraviť nastavenia rezidentnej ochrany....11
7.1.3.3 Overenie rezidentnej ochrany....11
7.1.3.4 Čo robiť ak rezidentná ochrana nefunguje....12
7.1.4 Kontrola počítača....12
7.1.4.1 Typy kontroly....12
7.1.4.1.1 Smart kontrola....12
7.1.4.1.2 Prispôsobená kontrola....13
7.1.4.2 Ciele kontroly....13
7.1.4.3 Profily kontroly....13
7.1.5 Nastavenie skenovacieho jadra ThreatSense....13
7.1.5.1 Objekty....14
7.1.5.2 Metódy....14
7.1.5.3 Liečenie....14
7.1.5.4 Vylúčenia....14
7.1.5.5 Obmedzenia....15
7.1.5.6 Ostatné....15
7.1.6 Našla sa infiltrácia....15
7.2 Web a e-mail....16
7.2.1 Ochrana prístupu na web....16
7.2.1.1 Porty....16
7.2.1.2 Zoznam URL adries....16
7.2.2 E-mailová ochrana....16
7.2.2.1 Kontrola protokolu POP3....17
7.2.2.2 Kontrola protokolu IMAP....17
7.3 Ochrana osobných údajov (Anti-Phishing)....17
8. Firewall....17
8.1 Režimy filtrovania....17
8.2 Pravidlá firewallu....18
8.2.1 Vytvorenie nového pravidla....18
8.3 Zóny....18
8.4 Profily....18
8.5 Protokoly....19
9. Správa zariadení....19
9.1 Pravidlá....19
10. Webová kontrola....20
11. Nástroje....21
11.1 Protokoly....21
11.1.1 Údržba protokolov....21
11.1.2 Filtrovanie protokolov....22
11.2 Plánovač....22
11.2.1 Vytváranie nových úloh....22
11.2.2 Vytvorenie úlohy definovanej používateľom....23
11.3 Live Grid....23
11.3.1 Posielanie podozrivých súborov....23
11.4 Karanténa....24
11.4.1 Pridanie súborov do karantény....24
11.4.2 Obnovenie súborov z karantény....24
11.4.3 Posielanie súboru z karantény....24
11.5 Oprávnenia....24
11.6 Prezentačný režim....25
11.7 Bežiace procesy....25
12. Používateľské rozhranie....26
12.1 Upozornenia a notifikácie....26
12.1.1 Výstražné upozornenia....26
12.1.2 Stavy ochrany....26
12.2 Kontextové menu....27
13. Aktualizácia programu....27
13.1 Nastavenie aktualizácií....27
13.1.1 Rozšírené nastavenia....28
13.2 Ako vytvoriť úlohy aktualizácie....28
13.3 Aktualizácia programu na novú verziu (upgrade)....28
13.4 Aktualizácie systému....28
14. Rôzne....29
14.1 Import a export nastavení....29
14.2 Proxy server....29
14.3 Zdielaná lokálna vyrovnávacia pamäť....29

1. ESET Endpoint Security

ESET Endpoint Security 6 predstavuje nový prístup k integrovanej počítačovej bezpečnosti. Najnovšia verzia skenovacieho jadra ThreatSense® kombinovaného s ochranou emailových klientov a firewallom spája rýchlosť a presnosť pri zabezpečovaní vášho počítača. Výsledkom je inteligentný systém, ktorý je konštantne v pohotovosti proti útokom a škodlivému softvéru, ktorý ohrozuje váš počítač.

ESET Endpoint Security 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 odstraňovať infiltrácie ako vírusy, červy, trójske kone, spyware, adware, rootkity a iné internetové útoky ovplyvňujúce výkon systému alebo narušujúce váš počítač.

ESET Endpoint Security 6 je navrhnutý pre pracovné stanice vo firmách/v podnikoch. Môže byť použitý s nástrojom ESET Remote Administrator, ktorý umožňuje hromadne meniť nastavenia viacerých pracovných staníc, ako napr. zavádzať politiky a pravidlá, sledovať zachytené infiltrácie a vzdialene ich nastavovať z iného počítača v sieti.

1.1 Čo je nové vo verzii 6

Nové grafické prostredie programu ESET Endpoint Security bolo kompletne prebudované pre lepšiu čitateľnosť jednotlivých prvkov a viac intuitívne používanie. ESET Endpoint Security vo verzii 6 prináša nasledujúce vylepšenia:

- **Firewall** – teraz už môžete vytvárať pravidlá firewallu priamo z protokolov, alebo z notifikačných okien systému IDS *(Intrusion detection system)*, prípadne priradiť toto pravidlo konkrétnemu sieťovému pripojeniu
- **Webová kontrola** – blokuje web stránky, ktoré môžu obsahovať neželaný a ofenzívny materiál
- **Ochrana prístupu na web** – kontroluje internetovú komunikáciu webových prehliadačov so servermi na sieti internet
- **Ochrana poštových klientov** – kontroluje emailovú komunikáciu prostredníctvom protokolov POP3 a IMAP
- **Anti-Phishing ochrana** – obmedzuje webstránky podozrivých z distribúcie obsahu za účelom manipulácie používateľov, aby poskytli svoje osobné údaje.
- **Správa zariadení** – umožňuje skenovať alebo blokovať zariadenia a prispôsobovať filtre a oprávnenia používateľov pre prístup a prácu s externými zariadeniami. Táto funkcionalita je dostupná od produktovej verzie 6.1.
- **Prezentačný režim** – umožňuje mať spustený ESET Endpoint Security na pozadí bez zobrazovania notifikácii či vykonávaní plánovaných úloh
- **Zdieľaná lokálna vyrovnávacia pamäť** – zvyšuje rýchlosť skenovania vo virtuálnych prostrediach

1.2 Systémové požiadavky

Pre bezproblémový chod ESET Endpoint Security je potrebné splniť nasledujúce požiadavky na hardvér a softvér:

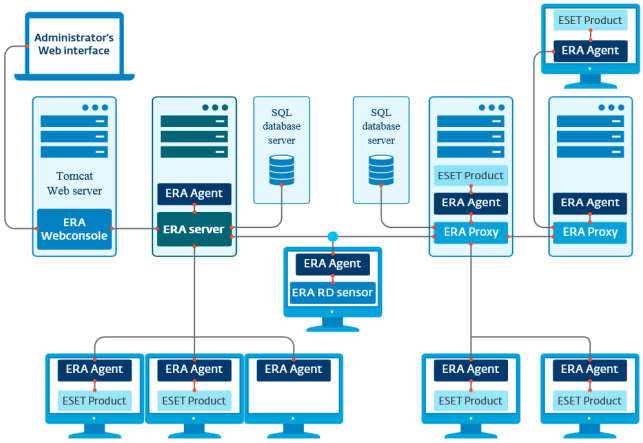
	Systémové požiadavky:
Podporované procesory	Intel 32-bit, 64-bit
Operačný systém	macOS 10.9 a novší
Pamäť	300 MB
Voľné miesto na disku	200 MB

2. Dokumentácia pre používateľov pripojených cez ESET Remote Administrator

ESET Remote Administrator je nástroj, ktorý vám umožňuje spravovať produkty od ESET pripojené do siete z jedného programu. Pomocou spravovania úloh vám umožňuje nainštalovať produkty od ESET na vzdialené počítače v sieti a okamžite reagovať na problémy, ktoré môžu vzniknúť na zariadení. ESET Remote Administrator neposkytuje ochranu proti škodlivému kódu, no spolieha sa na bezpečnostné produkty nainštalované na pripojených klientskych počítačoch.

Podporuje spojenie so všetkými platformami produktov ESET. Vaša sieť tak môže obsahovať zariadenia s operačnými systémami Microsoft Windows, macOS, Linux, ako aj operačnými systémami na mobilných zariadeniach (telefónoch a tabletoch).

Nasledujúci obrázok zobrazuje príklad siete chránenej bezpečnostnými produktmi od firmy ESET.



POZNÁMKA: Viac informácií sa nachádza k kapitole ESET Remote Administrator Používateľská príručka.

2.1 ESET Remote Administrator Server

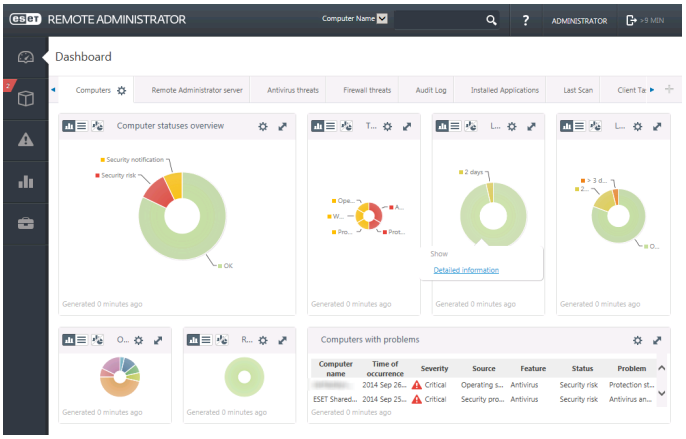
ESET Remote Administrator Server (ERAS) je hlavnou súčasťou nástroja ESET Remote Administrator 6. Úlohou servera je spracovávať všetky dáta prijaté od klientov pripojených na server (cez ERA Agenta 5). ESET Remote Administrator Agent uľahčuje komunikáciu medzi klientom a serverom. Dáta (protokoly klientov, nastavenia, replikácia agenta atď.) sú uložené v databáze (MySQL).

Predtým ako začnete spravovať klientov, musí byť ESET Remote Administrator Server (ERAS) nainštalovaný na podporovanom operačnom systéme. Pre správne spracovanie dát, vyžaduje ERAS stabilné pripojenie na databázový server, kde sú uložené dáta. Odporúčame preto nainštalovať ERAS a databázu na dva oddelené servery pre optimalizáciu výkonu. Počítač, na ktorom je ERAS nainštalovaný, musí byť nastavený na akceptovanie všetkých komunikácii z nástrojov Agent/ Proxy/RD Sensor, ktoré sú overované pomocou certifikátov. Po nainštalovaní, je ERAS prístupný cez nástroj ERA Web Console 5, z ktorého sú spravované všetky operácie nástroja ERAS.

2.2 Web Console

ERA Web Console je webové rozhranie, ktoré zobrazuje dáta z ERA Servera 5 a umožňuje správu bezpečnostných produktov ESET vo vašej sieti. Webconsole možno otvoriť v každom podporovanom webovom prehliadači. Webconsole sa používa na spravovanie všetkých klientov. Je zobrazený náhľad počítačov a zariadení v sieti a dá sa použiť na vzdialenú inštaláciu produktov ESET na pracovné stanice.

Ako vyzerá Webconsole?



V dolnej časti Webconsole sa nachádza nástroj rýchleho vyhľadávania **Quick Search**. Zadajte do tohto poľa ľubovoľný reťazec alebo **IPv4/IPv6 adresu** do poľa **Názov počítača** a kliknite na lupu alebo stlačte **Enter** pre vyhľadanie klienta. Budete presmerovaný do sekcie **Skupiny,** kde bude klient zobrazený.

2.3 Proxy

ERA Proxy je ďalším komponentom ESET Remote Administrator a slúži na tieto účely. V stredne veľkých sieťach alebo v podnikových sieťach s mnohými klientmi (napríklad 10 000 a viac klientov) môžete použiť ERA Proxy a prerozdeliť záťaž siete medzi viaceré ERA Proxy pracovné stanice a ERA Server 5. Ďalšou výhodou ERA Proxy je, že je možné ho použiť ak sa pripájate na vzdialenú pobočku firmy s pomalším pripojením. To znamená, že ERA Agent na každom klientovi nie je pripojený do ERA Serveru priamo cez ERA Proxy, ktorý je v tej istej sieti ako pobočka firmy. ERA Proxy prijíma komunikáciu z ESET klientov, spája ju a odosiela na server (alebo ďalšiu proxy). To umožňuje pripojenie viacerých klientov na vašu sieť bez obmedzenia kvality databázových dotazov.

V závislosti od nastavenia siete by malo byť možné pripojiť ERA Proxy na ďalšiu ERA Proxy a až potom na ERA Server.

Pre správnu funkciu ERA Proxy musí byť na hosťovskom počítači nainštalované okrem ERA Proxy aj ERA Agent a tiež musí byť pripojený na vyššiu úroveň siete.

2.4 Agent

Agent je nevyhnutnou súčasťou produktu ESET Remote Administrator – každé klientske riešenie (napríklad Endpoint, Smart security, atď...) komunikuje so serverom cez agenta. Agent je tá časť ESET Remote Administratora, ktorá umožňuje správu produktov ESET pomocou klientov. Agent zbiera informácie z klienta a odosiela ich na server. Ak server odosiela úlohu pre klienta, najprv ju odošle agentovi, ktorý následne tú

úlohu odošle klientovi. Všetka komunikácia na sieti sa deje medzi agentom a vyššími časťami ERA siete – serverom a proxy.

ESET Agent používa nasledujúce tri metódy pripojenia k Serveru:

1. Agent klienta je pripojený priamo na server.
2. Agent klienta je pripojený na server cez proxy.
3. Agent klienta je pripojený na server cez viaceré proxy.

ESET Agent komunikuje s produktmi ESET na klientoch, zbiera informácie a odosiela nastavenia zo servera na klientov.

POZNÁMKA: ESET Proxy má vlastného agenta, ktorý sa stará o komunikáciu medzi klientom, ostatnými proxy a serverom.

2.5 RD Sensor

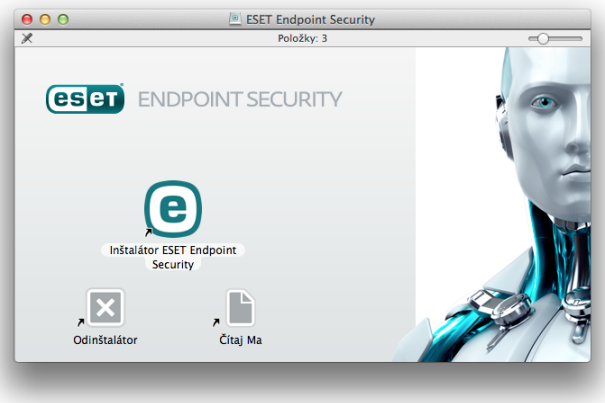
RD (Rogue Detection) Sensor je vyhľadávací nástroj, ktorý dokáže rozpoznať všetky vzdialené počítače zo siete, ku ktorej je pripojený. RD Sensor je súčasťou produktu ESET Remote Administrator. Je to pohodlný spôsob pridania nových počítačov do ESET Remote Administrator bez nutnosti ich manuálneho vyhľadávania.

RD Sensor vyhľadá počítače, ktoré sú v sieti a pošle o nich informáciu ERA Serveru. ERA Server vyhodnotí, či je nájdený počítač neznámy alebo už spravovaný.

3. Inštalácia

Inštalačného sprievodcu spustíte jednou z nasledujúcich možností:

- Ak spúšťate inštaláciu z CD alebo DVD, vložte disk do vášho počítača, otvorte ho a potom kliknite dvakrát na ikonu inštalátora.
- Ak ste stiahli súbor z internetu, kliknite dvakrát na ikonu inštalátora.



Inštalačný sprievodca vás prevedie základnými nastaveniami. Počas prvotnej fázy inštalácie inštalátor skontroluje, či nie je na internete dostupná novšia verzia produktu. Ak je dostupná nová verzia, budete môcť zvoliť možnosť, že sa pred inštaláciu stiahne najnovšia verzia produktu a potom budete pokračovať v inštalácii.

Po súhlase s licenčnou dohodou koncového používateľa si môžete zvoliť typ inštalácie:

- Typická inštalácia 6
- Pokročilá inštalácia 7
- Vzdialená inštalácia 7

3.1 Typická inštalácia

Typická inštalácia je vhodná pre väčšinu používateľov a umožňuje nastaviť základné parametre. Ich použitím zabezpečíte výbornú úroveň ochrany kombinovanú s jednoduchým používaním programu a vysokým výkonom systému. Typická inštalácia je predvolenou voľbou. Odporúčame ju použiť v prípade, že nemáte žiadne špecifické požiadavky ohľadom nastavení programu.

ESET Live Grid
Systém včasného varovania ESET Live Grid pomáha bezodkladne informovať ESET o nových infiltráciách, čím sa zabezpečí čo najrýchlejšia spätná väzba v podobe ochrany našich zákazníkov. Systém zasiela nové hrozby do vírusových laboratórií ESET, kde sa tieto vzorky analyzujú, spracovávajú a pridávajú do vírusovej databázy. Ak si želáte zmeniť nastavenia posielania podozrivých súborov, kliknite na **Nastavenia...**. Pre ďalšie informácie si pozrite kapitolu Live Grid 23.

Potenciálne nechcené aplikácie
Potenciálne nechcené aplikácie sú programy, ktoré nemusia byť škodlivé, ale môžu negatívne ovplyvňovať výkon či spoľahlivosť systému, prípadne posielajú informácie tretím stranám. Tieto aplikácie sú často súčasťou inštalačných balíkov iných programov a preto býva často obtiažne všimnúť si ich včas, tzn. počas inštalácie. Práve preto môžu byť takéto aplikácie nainštalované vďaka drobnej nepozornosti, napriek tomu, že ich zväčša sprevádza upozornenie počas inštalácie.

Po nainštalovaní programu ESET Endpoint Security vám odporúčame spustiť kontrolu počítača. V hlavnom okne programu zvoľte **Kontrola počítača** a následne **Smart kontrola**. Viac informácií nájdete v kapitole Kontrola počítača 12.

3.2 Pokročilá inštalácia

Pokročilá inštalácia je určená pre skúsených používateľov, ktorí uprednostňujú spresnenie nastavení počas procesu inštalácie.

Programové súčasti
ESET Endpoint Security umožňuje inštalovať produkt bez niektorých vybraných programových súčastí (napr. Web a e-mail ochrana). Odznačte vybranú možnosť, ak si neželáte, aby bola súčasťou 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 vášho servera alebo jeho URL a port, na ktorom proxy server počúva (štandardne 3128). Ak proxy server vyžaduje autorizáciu, je potrebné správne vyplniť polia **Meno** a **Heslo**, aby sa autorizovalo pripojenie k proxy serveru. Ak nepoužívate proxy server, označte možnosť **Pri pripojení nepoužívam proxy server**. Ak si nie ste istý(á), či používate proxy server, označte **Chcem použiť systémové nastavenia (Odporúčané)**.

Oprávnenia
V ďalšom kroku môžete nastaviť privilegovaných používateľov alebo skupiny, ktoré budú môcť upravovať nastavenia programu. Zo zoznamu používateľov vľavo vyberte používateľov a potom ich pridajte pomocou tlačidla **Pridať** do zoznamu **Oprávnení používatelia**. Pre zobrazenie zoznamu všetkých systémových používateľov (účtov) označte možnosť **Zobraz všetkých používateľov**. Ak necháte zoznam Oprávnení používatelia prázdny, všetci používatelia budú považovaní za oprávnených.

ESET Live Grid
Systém včasného varovania ESET Live Grid pomáha bezodkladne informovať ESET o nových infiltráciách, čím sa zabezpečí čo najrýchlejšia spätná väzba v podobe ochrany našich zákazníkov. Systém zasiela nové hrozby do vírusových laboratórií ESET, kde sa tieto vzorky analyzujú, spracovávajú a pridávajú do vírusovej databázy. Ak si želáte zmeniť nastavenia posielania podozrivých súborov, kliknite na **Nastavenia...**. Pre ďalšie informácie si pozrite kapitolu Live Grid 23.

Potenciálne nechcené aplikácie
Potenciálne nechcené aplikácie sú programy, ktoré nemusia byť škodlivé, ale môžu negatívne ovplyvňovať výkon či spoľahlivosť systému, prípadne posielajú informácie tretím stranám. Tieto aplikácie sú často súčasťou inštalačných balíkov iných programov a preto býva často obtiažne všimnúť si ich včas, tzn. počas inštalácie. Práve preto môžu byť takéto aplikácie nainštalované vďaka drobnej nepozornosti, napriek tomu, že ich zväčša sprevádza upozornenie počas inštalácie.

Firewall
V tomto kroku môžete vybrať režim filtrovania prichádzajúcich sieťových komunikácií. Viac informácií nájdete v kapitole Režimy filtrovania 17.

Po nainštalovaní programu ESET Endpoint Security vám odporúčame spustiť kontrolu počítača. V hlavnom okne programu zvoľte **Kontrola počítača** a následne **Smart kontrola**. Viac informácií nájdete v kapitole Kontrola počítača 12.

3.3 Vzdialená inštalácia

Vzdialená inštalácia umožňuje vytvorenie inštalačného balíčka, ktorý môže byť inštalovaný na cieľových staniciach s použitím softvéru na pripojenie na vzdialenú plochu (tzv. "remote desktop"). Po dokončení inštalácie môže byť ESET Endpoint Security spravovaný pomocou ESET Remote Administrator.

Vzdialená inštalácia pozostáva z dvoch fáz:
1. Vytvorenie balíčka pre vzdialenú inštaláciu s použitím ESET inštalátora 7
2. Inštalácia s použitím softvéru na vzdialenú správu 8

S použitím poslednej verzie produktu ESET Remote Administrator 6 môžete vykonať vzdialenú inštaláciu na klientských počítačoch s operačným systémom macOS. Podrobné informácie nájdete tomto článku databázy znalostí ESET.

3.3.1 Vytvorenie balíčka pre vzdialenú inštaláciu

Programové súčasti
ESET Endpoint Security umožňuje inštalovať produkt bez niektorých vybraných programových súčastí (napr. Web a e-mail ochrana). Odznačte vybranú možnosť, ak si neželáte, aby bola súčasťou 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 vášho servera alebo jeho URL a port, na ktorom proxy server počúva (štandardne 3128). Ak proxy server vyžaduje autorizáciu, je potrebné správne vyplniť polia **Meno** a **Heslo**, aby sa autorizovalo pripojenie k proxy serveru. Ak nepoužívate proxy server, označte možnosť **Pri pripojení nepoužívam proxy server**. Ak si nie ste istý(á), či používate proxy server, označte **Chcem použiť systémové nastavenia (Odporúčané)**.

Oprávnenia
V ďalšom kroku môžete nastaviť privilegovaných používateľov alebo skupiny, ktoré budú môcť upravovať nastavenia programu. Zo zoznamu používateľov vľavo vyberte používateľov a potom ich pridajte pomocou tlačidla **Pridať** do zoznamu **Oprávnení používateľa**. Pre zobrazenie zoznamu všetkých systémových používateľov (účtov) označte možnosť **Zobraz všetkých používateľov**. Ak necháte zoznam Oprávnení používateľa prázdny, všetci používatelia budú považovaní za oprávnených.

ESET Live Grid
Systém včasného varovania ESET Live Grid pomáha bezodkladne informovať ESET o nových infiltráciách, čím sa zabezpečí čo najrýchlejšia spätná väzba v podobe ochrany našich zákazníkov. Systém zasiela nové hrozby do vírusových laboratórií ESET, kde sa tieto vzorky analyzujú, spracovávajú a pridávajú do vírusovej databázy. Ak si želáte zmeniť nastavenia posielania podozrivých súborov, kliknite na **Nastavenia...**. Pre ďalšie informácie si pozrite kapitolu Live Grid 23.

Potenciálne nechcené aplikácie
Potenciálne nechcené aplikácie sú programy, ktoré nemusia byť škodlivé, ale môžu negatívne ovplyvňovať výkon či spoľahlivosť systému, prípadne posielajú informácie tretím stranám. Tieto aplikácie sú často súčasťou inštalačných balíkov iných programov a preto býva často obtiažne všimnúť si ich včas, tzn. počas inštalácie. Práve preto môžu byť takéto aplikácie nainštalované vďaka drobnej nepozornosti, napriek tomu, že ich zväčša sprevádza upozornenie počas inštalácie.

Firewall
V tomto kroku môžete vybrať režim filtrovania prichádzajúcich sieťových komunikácií. Viac informácií nájdete v kapitole Režimy filtrovania 17.

Súbor vzdialenej inštalácie
V poslednom kroku inštalátora vyberte cestu k cieľovému priečinku inštalačného balíčka *(esets_remote_Install.pkg)*, shell skriptu s nastaveniami *(esets_setup.sh)* a shell skriptu pre odinštaláciu *(esets_remote_UnInstall.sh)*.

3.3.2 Inštalácia na cieľovú stanicu

ESET Endpoint Security môže byť nainštalovaný na cieľovú stanicu pomocou programu Apple Remote Desktop alebo iného podobného nástroja, ktorý podporuje inštaláciu štandardných macOS balíčkov (*.pkg*). Skopírujú sa súbory a spustí sa shell skript na cieľovej stanici.

Inštalácia ESET Endpoint Security pomocou programu Apple Remote Desktop:

1. Kliknite na ikonu **Copy** v Apple Remote Desktop.
2. Kliknite na **+**, presuňte sa do umiestnenia shell skriptu *(esets_setup.sh)* a označte ho.
3. Označte **/tmp** v roletovom menu **Place items in** a kliknite na **Copy**.
4. Kliknite na **Install** a pošlite balíček na cieľovú stanicu.

Podrobné inštrukcie ohľadom administrácie klientskych staníc pomocou programu ESET Remote Administrator je možné nájsť v príručke ESET Remote Administrator.

3.3.3 Vzdialená odinštalácia

Kroky pre odinštaláciu ESET Endpoint Security z klientskych staníc:

1. Použitím príkazu **Copy Items** v programe Apple Remote Desktop nájdite odinštalačný shell skript (*esets_remote_unInstall.sh* – vytvorený spolu s inštalačným balíkom) a skopírujte ho do adresára / tmp na cieľovej stanici (teda, */tmp/ esets_remote_uninstall.sh*).
2. Zvoľte **User** pod **Run command as** a napíšte **root** do poľa **User**.
3. Kliknite na **Send**. Po úspešnej odinštalácii sa zobrazí informácia v konzole.

3.3.4 Aktualizácia staníc

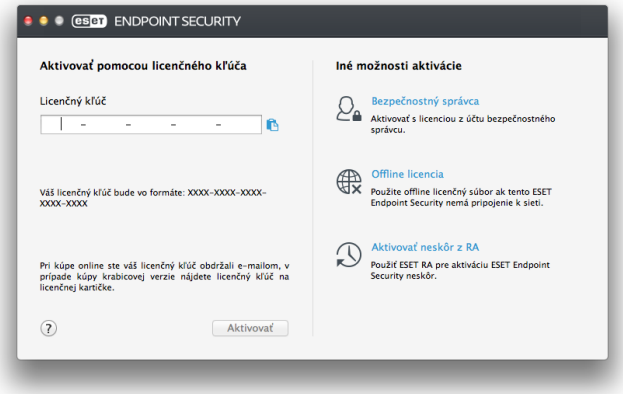
V prípade, že je k dispozícii nová verzia produktu, pre inštaláciu najnovšej verzie ESET Endpoint Security použite príkaz **Install packages** v programe Apple Remote Desktop.

4. Aktivácia produktu

Po ukončení inštalácie sa zobrazí dialógové okno s ponukou na aktiváciu produktu. Existuje niekoľko možností ako aktivovať produkt. Dostupnosť nižšie uvedených aktivačných scenárov v dialógovom okne sa môže líšiť v závislosti od spôsobu distribúcie inštalačného súboru (CD, stránka ESET, ...).

Pre aktiváciu ESET Endpoint Security priamo z

programu, kliknite na ikonu programu v macOS menu bar (v hornej časti obrazovky) a vyberte možnosť **Aktivácia produktu** alebo v hlavnom okne programu kliknite na **Pomocník** > **Aktivovať produkt**.



Môžete použiť jednu z nasledujúce metód aktivácie ESET Endpoint Security:

- **Licenčný kľúč** – Jedinečný reťazec znakov XXXX-XXXX-XXXX-XXXX-XXXX , ktorý je použitý na identifikáciu vlastníka licencie a aktiváciu licencie.
- **Bezpečnostný správca** – Konto vytvorené na portáli ESET License Administrator s prihlasovacími údajmi (emailová adresa + heslo). Táto metóda vám umožní spravovať viac licencií z jedného miesta.
- **Offline licencia** – Automaticky vygenerovaný Offline licenčný súbor s informáciami o vašej licencii. Offline licenčný súbor je generovaný pomocou licenčného portálu ESET a používa sa, keď sa aplikácia nemôže pripojiť na licenčné servery v danej sieti.

Ak je váš počítač súčasťou spravovanej siete a správca siete používa ESET Remote Administrator, aktiváciu môžete vykonať aj neskôr.

POZNÁMKA: ESET Remote Administrator automaticky aktivuje pracovné stanice (aktivácia prebieha v pozadí, bez oznámení) pomocou licencie sprístupnenej správcom.

5. Odinštalácia

ESET Endpoint Security odinštalujete jednou z nasledujúcich možností:

- vložte inštalačné CD alebo DVD ESET Endpoint Security do vášho počítača, otvorte disk z pracovnej plochy alebo z okna Finder a dvojkliknite na ikonu **Odinštalátor**,
- otvorte inštalačný súbor ESET Endpoint Security *(.dmg)* a dvojkliknite na ikonu **Odinštalátor**,
- otvorte okno aplikácie **Finder**, kliknite na **Aplikácie** (alebo **Applications**), stlačte ctrl a kliknite na ikonu **ESET Endpoint Security**. Z kontextového menu vyberte možnosť **Zobraziť obsah balíka** (alebo **Show Package Contents**). Otvorte adresár **Contents** > **Helpers** a dvojkliknite na ikonu **Uninstaller**.

6. Stručný prehľad

Hlavné okno programu ESET Endpoint Security je rozdelené do dvoch častí. Časť vpravo zobrazuje informácie, ktoré podliehajú voľbe vybranej v hlavnom menu vľavo.

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

- **Stav ochrany** – zobrazuje informácie o stave ochrany vášho počítača, Firewallu, Web a Mail ochrany.
- **Kontrola počítača** – umožňuje nastaviť a spustiť On-demand kontrolu 12.
- **Aktualizácia** – zobrazí informácie týkajúce sa aktualizácií vírusovej databázy.
- **Nastavenie** – vyberte si túto možnosť, ak chcete zmeniť nastavenia úrovne zabezpečenia vášho počítača.
- **Nástroje** – slúži na prístup k Protokolom 21, Plánovaču 22, Karanténe 24 a Bežiacim procesom 25 a ďalším funkciam programu.
- **Pomocník** – obsahuje odkazy na Pomocníka, web stránku Databázy znalostí ESET, formulár slúžiaci na kontaktovanie Technickej podpory a ostatné informácie o programe.

6.1 Klávesové skratky

Tieto klávesové skratky môžu byť použité pri práci s programom ESET Endpoint Security:

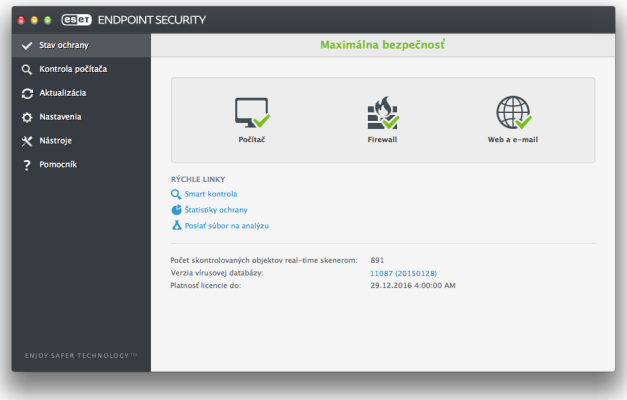
- *cmd+,* – zobrazí nastavenia programu ESET Endpoint Security,
- *cmd+O* – zmení veľkosť hlavného okna programu na pôvodnú veľkosť a presunie ho do stredu obrazovky,
- *cmd+Q* – schová hlavné okno programu, ktoré je možné znova otvoriť kliknutím na ikonu programu ESET Endpoint Security v hornej lište macOS,
- *cmd+W* – zatvorí hlavné okno programu.

Nasledujúce klávesové skratky fungujú iba v prípade, že povolíte možnosť **Používať štandardné menu** v sekcii **Nastavenie** > **Zobraziť pokročilé nastavenia ...** (alebo stlačte *cmd+,*) > **Rozhranie**:

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

6.2 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 Security.



6.3 Čo robiť ak program nepracuje správne

Ak zapnuté moduly fungujú správne, majú priradenú zelenú ikonu. Ak nie, zobrazí sa vedľa každého z nich červená ikona s výkričníkom. Ďalšie informácie sa zobrazia pod týmito ikonami spolu s navrhovaným riešením problému.

Ak sa vám nepodarí vyriešiť problém pomocou navrhovaných riešení, môžete vyhľadať riešenie v Databáze znalostí ESET alebo kontaktovať Technickú podporu ESET. Pracovníci Technickej podpory rýchlo odpovedia na vaše otázky a pomôžu vám vyriešiť váš problém.

7. Ochrana počítača

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

7.1 Antivirus a antispyware

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

7.1.1 Všeobecné

V časti **Všeobecné** (**Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Ochrana** > **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 zneužiteľné aplikácie** – sem spadajú komerčné aplikácie, legitímny softvér ako sú napr. nástroje pre vzdialený prístup. Táto možnosť je štandardne 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.

Vylúčenia z detekcie 10 nastavíte kliknutím na tlačidlo **Nastavenia...**.

7.1.1.1 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: Startup kontrola (spúšťaná pri štarte počítača), rezidentná aj kontrola počítača (On-demand).

- **Cesta** - úplná cesta k súborom alebo priečinkom, ktoré budú vylúčené z kontroly,
- **Infiltrácia** - ak je v tomto poli zobrazený názov infiltrácie, znamená to, že súbor je vylúčený z kontroly len pre túto konkrétnu infiltráciu. Ak bude tento súbor neskôr napadnutý inou infiltráciou, infiltrácia bude detegovaná antivírusovým modulom.
- **+** - zadajte cestu k objektu, ktorý bude vylúčený z kontroly (môžete taktiež použiť nahrádzajúce znaky * a ?) alebo vyberte objekt zo stromovej štruktúry,
- **−** - odstráni označený záznam,
- **Štandardné** - odstráni všetky pridané vylúčenia.

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

7.1.2 Ochrana pri štarte počítača

Štandardne sa táto kontrola spúšťa pravidelne vo forme plánovanej úlohy po prihlásení používateľa alebo po úspešnej aktualizácii vírusovej databázy. Nastavenia skenovacieho jadra ThreatSense pre túto kontrolu sú dostupné po kliknutí na tlačidlo **Nastavenia...**. O nastaveniach jadra ThreatSense sa viac dočítate v tejto sekcii 13.

7.1.3 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 13) 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 Security nachádzajúcu sa v macOS menu bar (v hornej časti obrazovky) a aktivovaním voľby **Vypnúť rezidentnú ochranu súborového systému** . Rezidentnú ochranu môžete vypnúť v hlavnom okne programu (**Nastavenie** > **Počítač** a prepnite tlačidlo modulu do polohy **VYP**).

Z rezidentnej ochrany môžu byť vynechané nasledujúce typy médií:

- **Lokálne disky** – systémové pevné disky
- **Výmenné disky** – 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 **Nastavenie** > **Zobraziť pokročilé nastavenia ...** (alebo stlačte *cmd+,*) > **Rezidentná ochrana** > **Nastavenia...** (tlačidlo vedľa možnosti **Rozšírené nastavenia**, ktoré sú bližšie popísané v sekcii Rozšírené nastavenia 11).

7.1.3.1 Rozšírené nastavenia

V tomto okne môžete nastaviť typy objektov, ktoré bude technológia ThreatSense kontrolovať. Pre viac informácií o **Samorozbaľovacích archívoch**, **Runtime archívoch** a **Rozšírenej heuristike** si prečítajte kapitolu Nastavenie parametrov skenovacieho jadra ThreatSense 13.

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

ThreatSense parametre pre vykonávané súbory – štandardne sa **Rozšírená heuristika** vykonáva pre spustené súbory. Pre zmiernenie dopadu na výkon systému odporúčame ponechať povolenú Smart optimalizáciu a ESET Live Grid.

Zvýšiť kompatibilitu sieťových zväzkov – táto funkcionalita zvýši výkon pri pristupovaní k súborom na sieti. Mala by byť povolená, ak máte spomalenia pri prístupe k sieťovým diskom. Funkcionalita 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.

7.1.3.2 Kedy je vhodné upraviť nastavenia rezidentnej ochrany

Rezidentná ochrana je najzákladnejší komponent udržania bezpečnosti v systéme. K úprave parametrov rezidentnej ochrany pristupujte 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 Security 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** (**Nastavenie** > **Zobraziť pokročilé nastavenia ...** > **Rezidentná ochrana**).

7.1.3.3 Overenie rezidentnej ochrany

Na overenie funkčnosti rezidentnej ochrany použite testovací súbor eicar.com. Tento súbor je špeciálny neškodný objekt, ktorý detegujú všetky antivírusové programy. Súbor vyvinula spoločnosť EICAR (European Institute for Computer Antivirus Research) za účelom testovania antivírusových programov.

Stav rezidentnej ochrany bez použitia ESET Remote Administrator je možné overiť pomocou príkazového riadku pripojením sa na danú pracovnú stanicu a vykonaním nasledovného príkazu:
`/Applications/.esets/Contents/MacOS/esets_daemon --status`

Stav funkčnosti rezidentnej ochrany bude zobrazený v oboch prípadoch `RTPStatus=Enabled` alebo `RTPStatus=Disabled`.

Výstup z príkazového riadku zahŕňa nasledovné údaje:

- verzia inštalovaného programu ESET Endpoint Security na vybranom počítači
- dátum a verzia vírusovej databázy
- cesta k serveru aktualizácie

POZNÁMKA: Používanie príkazového riadku je odporúčané iba pre skúsených používateľov.

7.1.3.4 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 **Nastavenie > 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**.

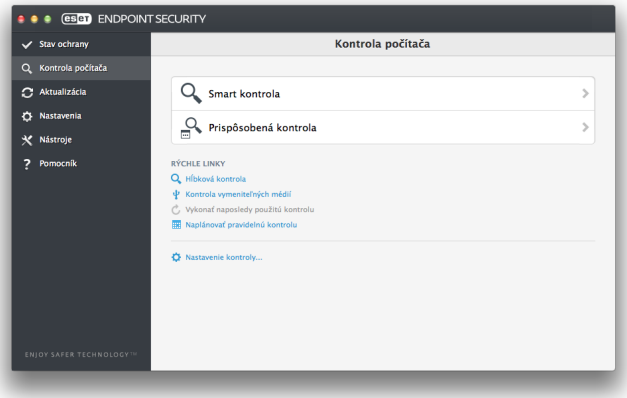
Rezidentná ochrana nedeteguje a nelieči súbory s infiltráciami
Uistite sa, že nemáte na počítači nainštalované žiadne iné antivírusové programy. Ak sú naraz zapnuté dve alebo viac rezidentných ochrán, môžu medzi nimi nastať konflikty. Odporúčame odinštalovať zo systému všetky antivírusové programy od 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.

7.1.4 Kontrola počítača

Ak máte podozrenie, že je váš počítač napadnutý malvérom, spustite antivírusovú kontrolu počítača (**Kontrola počítača** > **Smart kontrola**). Jedným z predpokladov pre udržanie čo najvyššej úrovne ochrany sú pravidelné antivírusové kontroly systému.

Pravidelné kontroly môžu detegovať aj infiltrácie, ktoré neboli pri ukladaní na pevný disk identifikované rezidentným modulom. Uvedená situácia môže nastať v prípade, ak bola počas ukladania súboru vypnutá rezidentná ochrana, prípadne nebola aktualizovaná vírusová databáza.



Odporúčame vám spúšťať kontrolu počítača prinajmenšom 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*na hlavné okno ESET Endpoint Security, ikonu v Docku, ikonu na macOS menu bar lište (v pravej hornej časti obrazovky) alebo ikonu aplikácie v priečinku */Applications*.

7.1.4.1 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.

7.1.4.1.1 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 14.

7.1.4.1.2 Prispôsobená kontrola

Prispôsobená kontrola je vhodným riešením ak chcete upraviť parametre kontroly ako sú ciele a metódy kontroly. Výhodou prispôsobenej kontroly je možnosť podrobne špecifikovať jej parametre. 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, kliknutím na **Nastavenia...** > **Liečenie**.

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

7.1.4.2 Ciele kontroly

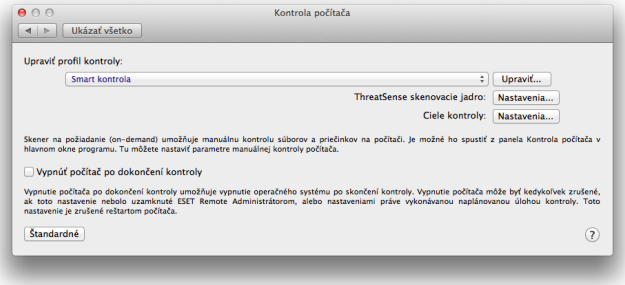
Stromová štruktúra cieľov kontroly slúži na výber súborov a adresárov, ktoré budú predmetom antivírusovej kontroly. Adresáre môžu byť označené tiež podľa nastavení profilu.

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.

7.1.4.3 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 **Nastavenie** > **Zobraziť pokročilé nastavenia ...** > **Kontrola počítača** a kliknite na **Upraviť...** vedľa zoznamu aktuálnych profilov.



Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite sekciu Nastavenie parametrov skenovacieho jadra ThreatSense 13, 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 a navyše chcete aplikovať metódu prísneho liečenia. V okne **Zoznam profilov kontroly počítača** napíšte názov pre váš profil, kliknite na **Pridať...** a potvrďte stlačením **OK**. Potom upravte parametre v nastaveniach **ThreatSense skenovacie jadro** a **Ciele kontroly**, tak aby zodpovedali vašim potrebám.

Ak si želáte automaticky vypnúť počítač po spustení kontroly počítača, označte možnosť **Vypnúť počítač po dokončení kontroly**.

7.1.5 Nastavenie skenovacieho jadra ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácie. Táto technológia je proaktívna, teda poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. K odhaleniu hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické vzorky, vírusové vzorky), ktoré efektívne kombinuje a zvyšuje tým bezpečnosť systému. Skenovacie jadro je schopné kontrolovať niekoľko dátových tokov paralelne a tak maximalizovať svoj výkon a účinnosť detekcie. Technológia ThreatSense dokáže účinne odstraňovať aj rootkity.

Samotné nastavenia technológie ThreatSense umožňujú používateľovi nastaviť viaceré parametre kontroly:

- Typy súborov a prípony, ktoré budú skontrolované
- Kombinácie rôznych metód detekcie
- Úrovne liečenia, atď.

Okno nastavení otvoríte kliknutím na **Nastavenie** > **Zobraziť pokročilé nastavenia ...** (alebo stlačením *cmd+,*) a následným kliknutím na tlačidlo ThreatSense skenovacie jadro **Nastavenia...**, ktoré sa nachádza v moduloch **Ochrana pri štarte počítača**, **Rezidentná ochrana** a **Kontrola počítača**. Všetky tieto moduly využívajú technológiu ThreatSense (pozrite nižšie). Rôzne scenáre si vyžadujú rôzne nastavenia. Technológia ThreatSense je nastaviteľná zvlášť pre tieto moduly:

- **Ochrana pri štarte počítača** – Kontrola súborov spúšťaných pri štarte počítača
- **Rezidentná ochrana** – Rezidentná ochrana súborového systému
- **Kontrola počítača** – On-demand kontrola počítača
- **Ochrana prístupu na web**
- **E-mailová ochrana**

Parametre ThreatSense sú špeciálne optimalizované pre každý modul a ich zmena môže značne ovplyvniť chovanie systému. Príkladom môže byť zmena nastavení tak, aby bola vždy vykonaná kontrola runtime archívov alebo zapnutie rozšírenej heuristiky pre modul rezidentnej ochrany súborov. Takéto zmeny spôsobia celkové spomalenie systému. Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky moduly ochrany, okrem modulu kontroly počítača.

7.1.5.1 Objekty

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

- **Symbolické linky** – (dostupné iba pre On-demand kontrolu) kontroluje špeciálne typy súborov, ktoré obsahujú reťazec textu definovaný operačným systémom ako cesta k inému súboru alebo priečinku,
- **Poštové súbory** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje špeciálne súbory, v ktorých sa nachádza stiahnutá elektronická pošta,
- **Schránky poštových súborov** – (nie je dostupné pre Rezidentnú kontrolu) kontroluje používateľských poštových schránok v systéme. Nesprávne použitie tejto voľby môže viesť ku konfliktu s vašim poštovým 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 (UPX, ASPack, yoda, FGS, atď.).

7.1.5.2 Metódy

V časti **Metódy** nastavujete, ktoré metódy sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú tieto voľby:

- **Zapnúť heuristiku** - heuristika používa algoritmus na analýzu (škodlivej) aktivity programov. Hlavnou výhodou heuristickej detekcie je jej schopnosť identifikovať škodlivý softvér, ktorý predtým neexistoval, alebo nebol pridaný do vírusovej databázy.
- **Zapnúť rozšírenú heuristiku** - rozšírená heuristika používa jedinečný heuristický algoritmus vyvinutý spoločnosťou ESET, ktorý dokáže detegovať červy a trójske kone napísané v zložitých programovacích jazykoch. Schopnosť detekcie je tak značne vyššia práve vďaka rozšírenej heuristike.

7.1.5.3 Liečenie

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

- **Neliečiť** - infikované súbory sa automaticky nevyliečia. Program zobrazí okno s varovaním s možnosťou manuálneho výberu akcie.
- **Štandardná úroveň liečenia** - program sa pokúsi automaticky vyliečiť, alebo vymazať infikovaný súbor. Ak nie je možné vykonať akciu automaticky, program ponúkne možnosť manuálneho výberu akcie.
- **Prísne liečenie** - program vylieči, alebo vymaže všetky infikované súbory (vrátane archívov). Jedinou výnimkou sú systémové súbory. Ak ich nie je možné vyliečiť, program zobrazí okno s varovaním s možnosťou manuálneho výberu akcie.

Upozornenie: V prednastavenom režime štandardnej úrovne liečenia je zmazaný celý archív len ak sú všetky súbory v archíve infikované. Ak teda archív obsahuje aj legitímne súbory (nenapadnuté vírusom), nebude vymazaný. Ak je archív zdetegovaný v režime prísneho liečenia, archív bude vymazaný ak obsahuje aspoň jeden súbor s infiltráciou, bez ohľadu na stav ostatných súborov v archíve.

7.1.5.4 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 narúša 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

7.1.5.5 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 úrovní 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.

7.1.5.6 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 zadefinované napevno. Vývojársky tím firmy ESET ich má možnosť podľa uváženia meniť prostredníctvom pravidelnej automatickej aktualizácie. Pokiaľ je Smart optimalizácia vypnutá, pri skenovaní súborov sa aplikujú výlučne iba nastavenia zadefinované užívateľom v nastaveniach skenovacieho jadra ThreatSense jednotlivých ochranných modulov.

Kontrolovať alternatívne dátové prúdy (platí iba pre 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.

7.1.6 Našla sa infiltrácia

Infiltrácie sa na systém môžu dostať z najrôznejších prístupových bodov - internetových stránok, zdieľaných adresárov, pošty, vymeniteľných médií (USB, externé disky, CD, DVD, atď.).

Ak váš počítač vykazuje znaky napadnutia škodlivým softvérom, napr. je pomalší, často "mrzne", atď., odporúčame nasledovné kroky:

1. Otvorte ESET Endpoint Security a kliknite na **Kontrola počítača**.
2. Kliknite na **Smart kontrola** (pre viac informácií si pozrite sekciu Smart kontrola) 12.
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 kontrolované na prítomnosť vírusov.

Ako obecný príklad postupu ESET Endpoint Security pri riešení problému s infiltráciou uveďme prípad, kedy 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, Zmazať** 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.

Zmazávanie 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.

7.2 Web a e-mail

Nastavenia modulov web a mail ochrany nájdete v časti **Nastavenie** > **Web a mail**. Rozšírené nastavenia jednotlivých modulov zobrazíte kliknutím na tlačidlo **Nastavenia...**.

- **Ochrana prístupu na web** - monitoruje HTTP komunikáciu medzi internetovými prehliadačmi a vzdialenými servermi.
- **Ochrana poštových klientov** - poskytuje kontrolu e-mailovej komunikácie prijatej cez protokoly POP3 a IMAP.
- **Ochrana osobných údajov** - blokuje potenciálne útoky typu *phishing* prichádzajúce z webstránok alebo domén, ktoré sú uložené v ESET databáze malvéru.
- **Webová kontrola** - blokuje web stránky, ktoré môžu obsahovať neželaný a ofenzívny materiál.

7.2.1 Ochrana prístupu na web

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

Filtrovanie webu dosiahnete definovaním portov pre HTTP komunikáciu 16 a/alebo URL adries 16.

7.2.1.1 Porty

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

7.2.1.2 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 skenované.

Ak chcete povoliť prístup iba k URL adresám uvedeným v zozname **Povolené URL**, označte voľbu **Obmedziť 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 *(hviezdička) a ?(otáznik). Hviezdička 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.

7.2.2 E-mailová ochrana

Ochrana poštových klientov poskytuje kontrolu emailovej komunikácie prijatej cez protokoly POP3 a IMAP. Pri skúmaní prichádzajúcich správ používa program všetky pokročilé metódy skenovania, ktoré ponúka skenovacie jadro ThreatSense. Detekcia škodlivých programov tak nastáva ešte pred ich porovnaním s databázou vzoriek vírusov. Kontrola komunikácie prijatej cez protokoly POP3 a IMAP nie je závislá od typu vášho poštového klienta.

ThreatSense skenovacie jadro: Nastavenia – pokročilé nastavenia skeneru vám umožňujú nastaviť ciele kontroly, metódy detekcie atď. Kliknutím na **Nastavenia...** sa zobrazí okno detailných nastavení skenera.

Pridávať do odosielaných správ – po skontrolovaní emailovej správy môže byť k nej pridaná informácia o výsledku kontroly. Na tieto upozornenia sa nemožno úplne spoliehať, nakoľko nemusia byť doplnené do problematických HTML správ a taktiež môžu byť sfalšované vírusmi. K dispozícii sú nasledovné možnosti:

- **Nepridávať do správ** – nebudú pridané žiadne upozornenia,
- **Pridávať len do infikovaných správ** – iba správy obsahujúce škodlivý softvér budú označené ako skontrolované,
- **Pridávať do všetkých kontrolovaných správ** – program pridá upozornenia do všetkých skontrolovaných správ.

Pridávať poznámku do predmetu prijatých a čítaných infikovaných správ – zapnite túto možnosť, ak si želáte pridať varovanie o víruse do infikovaného emailu. Toto umožňuje jednoduché filtrovanie medzi infikovanými emailovými správami. Toto tiež zvyšuje úroveň dôveryhodnosti pre príjemcu správy. Ak je detegovaná infiltrácia, tak sa poskytnú hodnotné informácie o hrozbe od konkrétneho odosielateľa.

Pridávať do predmetu odosielaných infikovaných správ – upravte túto šablónu, ak si želáte zmeniť prefix predmetu infikovaného emailu. Táto funkcionalita nahradí predmet správy *"Ahoj"* prefixom *"[virus]"* na nasledovný formát: *"[virus] Ahoj"*. Premenná %VIRUSNAME% znamená detegovanú hrozbu.

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 17
- Kontrola protokolu IMAP 17

7.2.2.1 Kontrola protokolu POP3

POP3 protokol je najrozšírenejší protokol slúžiaci na príjem emailovej komunikácie prostredníctvom poštového klienta. ESET Endpoint Security 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 poštového 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 POP3 protokolu** označená, všetka komunikácia prúdiaca cez POP3 je monitorovaná pre škodlivý softvér.

7.2.2.2 Kontrola protokolu IMAP

IMAP (Internet Message Access Protocol) je ďalší internetový protokol pre prijímanie emailových správ. IMAP má v porovnaní s POP3 zopár výhod, ako napríklad možnosť viacerých klientov pripojiť sa na tú istú poštovú schránku a zachovať informácie stavu správy (napríklad, či správa bola alebo nebola prečítaná, odpovedaná alebo vymazaná). ESET Endpoint Security 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 poštového 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 IMAP protokolu** označená, všetka komunikácia prúdiaca cez IMAP je monitorovaná pre škodlivý softvér.

7.3 Ochrana osobných údajov (Anti-Phishing)

Pojmom *phishing* sa definuje kriminálna činnosť využívajúca tzv. sociálne inžinierstvo (manipulačné techniky snažiace sa o získanie dôverných informácií). Cieľom je získať citlivé údaje ako napríklad heslá k bankovým účtom, PIN kódy a iné.

Odporúčame ponechať voľbu **Zapnúť ochranu osobných údajov** zapnutú (**Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Ochrana** > **Ochrana osobných údajov**). Všetky potenciálne útoky prichádzajúce z webstránok alebo domén, ktoré sú v databáze hrozieb, budú zablokované. Upozorní vás na to výstražná notifikácia.

8. Firewall

Personálny firewall zabezpečuje kontrolu všetkých spojení medzi sieťou a daným systémom, pričom umožňuje na základe definovaných pravidiel tieto jednotlivé spojenia povoliť alebo zablokovať. Chráni pred útokmi zo vzdialených počítačov a umožňuje blokovanie niektorých služieb. Tiež zabezpečuje antivírusovú kontrolu protokolov HTTP, POP3 a IMAP.

Základné a rozšírené nastavenia firewallu sa nachádzajú v časti **Nastavenie** > **Firewall**.

Možnosť **Zablokovať všetku komunikáciu** môžeme prirovnať k úplnému odpojeniu počítača od siete. Každá prichádzajúca a odchádzajúca komunikácia je firewallom bez upozornenia používateľa zablokovaná. Použitie takéhoto blokovania je vhodné pri podozrení na možné kritické bezpečnostné riziká s nutnosťou odpojenia systému od siete.

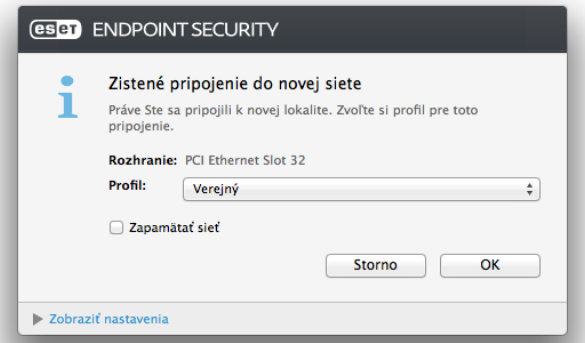
8.1 Režimy filtrovania

ESET Endpoint Security môže pracovať v troch režimoch filtrovania. Správanie firewallu záleží od zvoleného režimu. Nastavením režimu sa ovplyvní potreba interakcie používateľa. Nastavenia firewallu nájdete v Pokročilých nastaveniach ESET Endpoint Security (stlačte *cmd+,*) > **Firewall**.

Všetka komunikácia zablokovaná - všetky prichádzajúce aj odchádzajúce spojenia budú blokované.

Automatický s výnimkami - prednastavený režim. Je určený pre používateľov, ktorí potrebujú rýchle a pohodlné používanie firewallu bez nutnosti definovania pravidiel. Povoľuje všetky komunikácie z daného systému smerom do siete a blokuje všetky nové prichádzajúce komunikácie zo siete. Výnimkami môžu byť vami vytvorené pravidlá.

Interaktívny – 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 zakázať, pričom toto rozhodnutie môže byť trvalé - firewall vytvorí nové pravidlo. V tom prípade bude každá komunikácia tohto typu v budúcnosti povolená alebo zablokovaná podľa tohto pravidla.



Ak si želáte mať zaznamenané všetky spojenia blokované firewallom, označte voľbu **Zapisovať všetky zablokované spojenia do protokolu**. Firewall protokoly si môžete pozrieť v časti **Nástroje** > **Protokoly**. Z roletového menu **Protokol** vyberte **Personálny firewall** .

8.2 Pravidlá firewallu

Pravidlá predstavujú zoznam podmienok, podľa ktorých sú testované všetky sieťové spojenia a následne sú na ne uplatnené definované akcie. Môžete teda definovať, aká akcia sa má vykonať so spojením spĺňajúcim podmienky daného pravidla.

Prichádzajúce spojenie je inicializované na vzdialenej strane a snaží sa nadviazať spojenie s lokálnou stranou. V prípade odchádzajúceho spojenia je situácia opačná, teda lokálna strana nadväzuje spojenie so vzdialenou.

V prípade zistenia neznámej komunikácie je potrebné zvážiť, či ju povoliť alebo zamietnuť. Nevyžiadané, nezabezpečené alebo úplne neznáme spojenia predstavujú pre systém bezpečnostné riziko. Pri takejto komunikácii je vhodné venovať pozornosť hlavne vzdialenej strane a aplikácii, ktorá sa pokúša nadviazať spojenie. Mnohé infiltrácie odosielajú súkromné dáta alebo sťahujú iné škodlivé aplikácie na používateľské stanice. Práve tieto skryté spojenia je možné pomocou personálneho firewallu odhaliť a zakázať.

Štandardne sa aplikácie podpísané spoločnosťou Apple automaticky pripájajú do siete. Ak si to želáte vypnúť, urobte tak pomocou možnosti **Povoliť softvéru podpísanému spoločnosťou Apple automaticky pristupovať do siete**.

8.2.1 Vytvorenie nového pravidla

Záložka **Pravidlá** obsahuje zoznam všetkých pravidiel vygenerovaných konkrétnymi aplikáciami. Pravidlá sú pridávané automaticky na základe vašej reakcie na nové spojenia.

1. Nové pravidlo vytvoríte kliknutím na tlačidlo **Pridať...**. Zadajte názov pravidla a presuňte (tzv. drag and drop) ikonu aplikácie na biely štvorec v strede okna alebo kliknite na **Prehľadávať...** a nájdite aplikáciu v priečinku */Applications*. Ak chcete aplikovať pravidlo na všetky aplikácie nainštalované na vašom počítači, označte možnosť **Všetky aplikácie** .
2. V nasledujúcom kroku zvoľte **Akciu** (povoliť alebo zakázať spojenie medzi zvolenou aplikáciou a sieťou) a **Smer** spojenia (prichádzajúce, odchádzajúce alebo oba). Ak si želáte zaznamenať všetky spojenia týkajúce sa tohto pravidla do protokolu, označte voľbu **Logovať pravidlo**. Firewall protokoly si môžete pozrieť v časti **Nástroje** > **Protokoly**. Z roletového menu **Protokol** vyberte **Personálny firewall**.
3. V kroku **Protokol/Porty** vyberte protokol, cez ktorý aplikácia komunikuje a port služby alebo rozsah portov vo formáte *od-do*.
4. Posledným krokom je výber **Cieľa** (IP adresa, rozsah IP adries, podsieť, lokálna sieť alebo internet).

8.3 Zóny

Zóny predstavujú zoskupenia sieťových adries, ktoré spolu tvoria jednu logickú skupinu. Napríklad skupina sieťových adries počítačov v rámci pobočky firmy. Na každú adresu danej skupiny sa následne aplikujú rovnaké pravidlá, definované spoločne pre celú skupinu.

Zóny vytvoríte kliknutím na tlačidlo **Pridať...**. Zadajte **Názov** a **Popis** zóny, vyberte profil, ku ktorému bude táto zóna patriť a pridajte IP adresy, rozsah adries, WiFi SSID alebo konkrétne rozhranie.

8.4 Profily

Profily sú ďalším účinným nástrojom na ovplyvňovanie správania ESET Endpoint Security. Pre každé pravidlo je možné definovať, v akom profile bude platiť. Ak nie je pre pravidlo vybraný žiaden profil, pravidlo bude platiť v každom profile. Ak vyberiete profil, budú aplikované iba pravidlá pre tento profil a globálne pravidlá (s nezadaným profilom).

8.5 Protokoly

Firewall ukladá dôležité udalosti do logovacieho súboru, ktorý je možné prezerať priamo z hlavného okna ESET Endpoint Security po kliknutí na **Nástroje** > **Protokoly**. Z roletového menu **Protokol** následne vyberte **Firewall**.

Protokoly sú užitočným zdrojom informácií pri hľadaní chýb a odhaľovaní prienikov do vášho systému. Protokol firewallu obsahuje tieto údaje:

- Čas, kedy daná udalosť nastala
- Názov udalosti
- Zdrojovú sieťovú adresu
- Cieľovú sieťovú adresu
- Protokol sieťovej komunikácie
- Aplikované pravidlo
- Komunikujúca aplikácia
- Používateľ

Analýzou týchto údajov môžeme odhaliť pokusy o narušenie bezpečnosti systému. Príliš časté spojenia z rôznych neznámych lokalít, hromadné pokusy o nadviazanie spojenia, komunikujúce neznáme aplikácie či nezvyčajné čísla portov môžu pomôcť v odhalení útoku a minimalizovaní jeho následkov.

9. Správa zariadení

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

Podporované externé zariadenia:
- Diskové úložisko (HDD alebo USB výmenné médiá)
- CD/DVD
- USB tlačiareň
- Obrazové zariadenie
- Sériový port
- Sieť
- Prenosné zariadenie

Ak je vložené zariadenie, ktoré je blokované existujúcim pravidlom, zobrazí sa notifikácia a prístup k zariadeniu nebude umožnený.

Protokol zapisuje všetky incidenty, ktoré spúšťajú funkcionalitu Správy zariadení. Záznamy protokolu môžete vidieť v hlavnom menu ESET Endpoint Security v časti **Nástroje** > Protokoly 21.

9.1 Pravidlá

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

Kliknutím na **Povoliť správu zariadení** aktivujete túto funkcionalitu v ESET Endpoint Security. Po povolení Správy zariadení môžete upravovať pravidlá. Zaškrtávacím políčkom vľavo od názvu pravidla zapínate a vypínate dané pravidlo.

Pravidlá pridáte alebo zmažete tlačidlami + alebo −. Pravidlá sú zoradené podľa priority s najvyššou prioritou na vrchu. Poradie zmeníte označením a potiahnutím (drag and drop) pravidla v zozname alebo kliknutím na ⚙ a výberom jednej z možností.

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

Niektoré vymeniteľné médiá môžu byť povolené alebo blokované pre používateľa alebo skupinu používateľov podľa vybraných parametrov nastavených v pravidle. Zoznam pravidiel pozostáva z niekoľkých parametrov, ako sú meno, typ zariadenia, akcia vykonaná po pripojení média a závažnosť vytvorených protokolov.

Názov

Pre lepšiu identifikáciu vložte do poľa **Názov** popis pravidla. Možnosťou **Pravidlo zapnuté** zapínate a vypínate dané pravidlo – toto sa vám môže zísť ak nechcete pravidlo zmazať navždy.

Typ zariadenia

Vyberte typ externého zariadenia z rozbaľovacieho menu. Informácia o type zariadenia je zbieraná z operačného systému. Úložné zariadenia môžu byť externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty, ktoré neposkytujú informáciu o používateľovi, iba o jeho akciách. Z toho vyplýva, že môžu byť blokované len globálne pre všetkých používateľov.

Akcia

Prístupové práva k zariadeniam bez úložiska môžu byť povolené alebo blokované. Práva k zariadeniam s úložiskom môžu byť nasledovné:
Čítanie/Zápis – Všetky práva nad externým zariadením
Iba na čítanie – Používateľ pristupuje k súborom, ale nemôže do nich zapisovať či ukladať súbory na zariadenie
Blokovať – Prístup k zariadeniu nebude povolený

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 výrobcu alebo ID
Model – Názov daného zariadenia
Sériové číslo – Externé zariadenia majú zvyčajne svoje vlastné sériové číslo. V prípade CD/DVD sa jedná o sériové číslo daného média, nie CD mechaniky.

POZNÁMKA: Ak sú vyššie spomenuté popisy prázdne, pravidlo bude tieto polia počas filtrovania ignorovať. Parametre vo všetkých poliach okna rozlišujú malé a veľké písmená a nepoužívajú špeciálne znaky (*, ?).

TIP: Pre zistenie parametrov zariadenia pripojeného k počítaču najprv vytvorte pravidlo pre povolenie daného typu zariadení a po pripojení zariadenia k počítaču zistite jeho parametre v Protokole správcu zariadení 21.

Závažnosť zapisovanie do protokolu:

Vždy – Vytvára protokol zo všetkej komunikácie pre potreby hľadania závad a riešenia problémov
Žiadne – Nebudú vytvorené žiadne protokoly
Diagnostická – Vytvára protokol z komunikácie dôležitej pre ladenie programu a všetky nasledujúce úrovne
Informácie – Zobrazované budú informačné správy napríklad o úspešnej aktualizácií a všetky nasledujúce úrovne
Upozornenie – Zobrazované budú varovné správy, chyby a kritické chyby

Zoznam používateľov:

Pravidlo môže byť obmedzené len na určitých používateľov alebo skupín používateľov ich pridaním do Zoznamu používateľov:
Upraviť... – Otvorí **Editor Identity**, v ktorom môžete pridať používateľov alebo skupiny používateľov. Zo zoznamu používateľov vľavo vyberte používateľov a potom ich pridajte pomocou tlačidla **Pridať** do zoznamu **Vybratí používatelia**. Pre zobrazenie zoznamu všetkých systémových používateľov (účtov) označte možnosť **Zobraz všetkých používateľov**. Ak necháte zoznam Vybratí používatelia prázdny, všetci používatelia budú považovaní za oprávnených.

POZNÁMKA: Nie všetky typy zariadení sa dajú kontrolovať pomocou používateľských pravidiel (napríklad zobrazovacie zariadenia neposkytujú informácie o používateľoch ale len o akciách).

10. Webová kontrola

Webová kontrola vám umožňuje konfigurovať nastavenie, ktoré chráni firmu pred rizikom právnej zodpovednosti. Webová kontrola riadi prístup k webovým stránkam, ktoré môžu obsahovať potenciálne neprístojný obsah alebo môžu porušovať intelektuálne vlastníctvo iných osôb/spoločností. Jej cieľom je zamedziť zamestnancom prístup na tieto stránky ako aj na stránky, ktoré môžu negatívne ovplyvniť ich produktivitu. Webová kontrola umožňuje blokovať webové stránky, ktoré môžu obsahovať potenciálne neprístojný obsah. Okrem toho môžu zamestnávatelia alebo systémoví administrátori zakázať prístup na 27 predvolených kategórii a viac než 140 podkategórií web stránok.

V predvolenom nastavení je modul Web control vypnutý. Aktivovať ho možno takto: kliknite **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Webová kontrola** and označte možnosť **Povoliť webovú kontrolu**.

Okno s pravidlami zobrazuje existujúce pravidlá, či už podľa URL alebo podľa kategórie. Zoznam pravidiel obsahuje niekoľko vlastností ako meno, typ blokovania, akciu, ktorá sa má vykonať po aplikovaní pravidla a úroveň závažnosti pri logovaní do protokolu 21.

Kliknite na tlačidlo  pre vytvorenie nového pravidla. Dvojkliknutím na pole **Názov** zvoľte popis pravidla pre jeho lepšiu identifikáciu.

Zaškrtávacie políčko v ľavom stĺpci zoznamu zapína a vypína pravidlo. Toto je užitočné, ak si želáte pravidlo použiť neskôr a nechcete ho natrvalo vymazať.

Typ

Akcia podľa URL – prístup na konkrétnu adresu web stránky. Dvojkliknite na **URL/Kategória** a vložte príslušnú adresu URL web stránky.
V zoznamoch URL adries je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Pre webové adresy, na ktoré je možný prístup pomocou rôznych domén vytvorte samostatnú skupinu (napríklad examplepage.com, examplepage.sk). Keď pridáte adresu do zoznamu, celý obsah nachádzajúci sa na danej doméne (napríklad sub.examplepage.com) bude blokovaný na základe vášho nastavenia akcie podľa URL.
Akcia podľa kategórie – Dvojkliknite na **URL/ Kategória** a vyberte príslušné kategórie.

Identita

Umožňuje vybrať používateľov v systéme, na ktorých bude aplikované pravidlo.

Akcia

Povoliť – prístup na URL/kategóriu bude povolená
Blokovať – blokuje prístup na URL/kategóriu

Závažnosť (pre účely filtrovania 22 protokolov)

Vždy – zapisuje všetky udalosti
Žiadne – nebude vytvorený žiadny protokol
Diagnostická – protokoly potrebné akurát tak k ladeniu programu
Informácie – zobrazuje napr. informačné správy o úspešnej aktualizácii a všetky nasledujúce úrovne
Upozornenie – zaznamenáva kritické chyby a varovné hlásenia

11. Nástroje

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

11.1 Protokoly

Protokoly obsahujú informácie o všetkých dôležitých udalostiach v programe, ktoré sa vyskytli a poskytuje ucelený prehľad o zistených hrozbách. Zapisovanie protokolov je dôležitý nástroj pri analýze systému, detegovaní hrozieb a riešení problémov. Zapisovanie protokolov je aktívne na pozadí a nevyžaduje zásah používateľa. Informácie sú zaznamenávané na základe nastavenej úrovne zachytávania protokolov. Je možné zobraziť textové správy a protokoly priamo v prostredí ESET Endpoint Security, ako aj archivovať protokoly.

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

1. **Zachytené hrozby** – Zvoľte túto možnosť pre zobrazenie informácií týkajúcich sa zachytených infiltrácií.
2. **Udalosti** – Táto možnosť je určená pre systémových administrátorov a používateľov pre riešenie problémov. Všetky dôležité akcie vykonané v ESET Endpoint Security sú zaznamenané v protokoloch udalostí.
3. **Kontrola počítača** – Výsledky všetkých ukončených kontrol sú zobrazené v tomto okne. Dvojklikom na záznam zobrazíte detaily príslušnej On-demand kontroly počítača.
4. **Správa zariadení** – Obsahuje záznamy externých médií alebo zariadení, ktoré boli pripojené k počítaču. Iba zariadenia s pravidlom budú zaznamenané. Ak sa pravidlo nezhoduje s pripojeným zariadením, záznam v protokole nebude pre dané zariadenie vytvorený. Taktiež tu môžete vidieť detaily ako napr. typ zariadenia, sériové číslo, výrobcu a veľkosť média (ak je dostupná).
5. **Firewall** – Protokol personálneho firewallu obsahuje všetky vzdialené útoky zachytené personálnym firewallom. Tu nájdete informácie o všetkých útokoch na váš počítač. V stĺpci *Udalosť* je typ zisteného útoku. V stĺpci *Zdroj* sú podrobnejšie informácie o útočníkovi. V stĺpci *Protokol* je komunikačný protokol použitý pri útoku.
6. **Webová kontrola** – Zobrazuje web stránky a kategórie, ktoré boli buď blokované alebo povolené nastaveniami webovej kontroly.
7. **Filtrované stránky** – v tomto zozname nájdete webstránky, ktoré boli zablokované Ochranou prístupu na web 16 alebo Webovou kontrolou 20. V týchto protokoloch môžete vidieť čas, URL, stav, IP adresu, používateľa a aplikáciu, ktorá otvorila spojenie ku konkrétnej webstránke.

Pre skopírovanie zobrazených informácii do pamäte kliknite pravým tlačidlom myši na konkrétny záznam v protokole a potom na **Kopírovať...**.

11.1.1 Údržba protokolov

Nastavenia protokolov ESET Endpoint Security sú dostupné z hlavného okna programu. Kliknite na **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Nástroje** > **Protokoly**. Môžete špecifikovať nasledovné možnosti pre protokoly:

- **Automaticky mazať staré záznamy protokolov** - Záznamy v protokoloch staršie ako zadaný počet dní sú automaticky vymazané.

- **Automaticky optimalizovať protokoly** - Umožní automatickú defragmentáciu protokolov, ak je prekročené určité percento nepoužívaných záznamov.

Všetky dôležité informácie zobrazené v GUI, hrozby a udalosti, môžu byť uložené vo formáte pre čítanie textových formátov, ako obyčajný text alebo CSV (Comma-separated values). Ak chcete, aby sa tieto súbory k dispozícii pre spracovanie pomocou nástrojov tretích strán, označte možnosť **Povoliť záznamy do textových súborov**.

Tieto protokoly sa ukladajú do priečinka, ktorý je možné nastaviť kliknutím na tlačidlo **Nastavenia...** v časti **Rozšírené nastavenia**.

Je možné označiť konkrétne možnosti ukladania protokolov v časti **Textové súbory protokolov** > **Upraviť...**:

- **Udalosti** ako *Neplatné používateľské meno a heslo*, *Vírusová databáza nemôže byť aktualizovaná*, atď. sú uložené do súboru *eventslog.txt*.
- **Hrozby** zachytené modulmi Startup kontrola, rezidentná ochrana alebo Kontrola počítača sa ukladajú do súboru s názvom *threatslog.txt*.
- Výsledky dokončenej **Kontroly počítača** sa ukladajú do formátu *scanlog.NUMBER.txt*.
- Zariadenia blokované Správou zariadení sú spomenuté v devctllog.txt
- Udalosti týkajúce sa **Firewallu** sa ukladajú do firewalllog.txt
- Blokované stránky modulom **Webová kontrola** nájdete v súbore webctllog.txt

Je možné nastaviť filtrovanie v časti **Štandardné záznamy kontroly počítača** kliknutím na tlačidlo **Upraviť...**. Tu povoľte resp. zakážte typ protokolu podľa vášho uváženia. Viac informácii o typoch a filtrovaní protokolov sa dočítate v kapitole Filtrovanie protokolov 22.

11.1.2 Filtrovanie protokolov

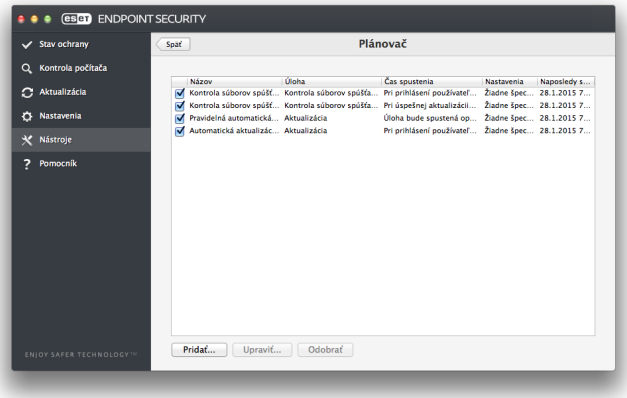
Protokoly uchovávajú informácie o dôležitých systémových udalostiach. Funkcia filtrovania protokolov vám umožňuje zobraziť záznamy týkajúce sa špecifickej udalosti.

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

11.2 Plánovač

Plánovač nájdete v hlavnom menu ESET Endpoint Security v záložke **Nástroje**. **Plánovač** obsahuje zoznam všetkých naplánovaných úloh a naplánovaných atribútov ako prednastavený čas, dátum a profil pri kontrole.



Štandardne sa v Plánovači nachádzajú nasledovné úlohy:

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

Pre zmenu konfigurácie existujúcej naplánovanej úlohy (štandardné aj definované používateľom) stlačte ctrl, kliknite na úlohu, ktorú chcete zmeniť a zvoľte **Upraviť...**, prípadne zvoľte úlohu a kliknite na tlačidlo **Upraviť...**.

11.2.1 Vytváranie nových úloh

Pre vytvorenie novej úlohy v Plánovači, kliknite na tlačidlo **Pridať...** alebo stlačte ctrl, kliknite na prázdne miesto v zozname a zvoľte **Pridať...** z kontextového menu. Dostupných je 5 typov úloh:

- **Spustenie aplikácie**
- **Aktualizácia**
- **Údržba protokolov**
- **Kontrola počítača**
- **Kontrola súborov spúšťaných pri štarte**

POZNÁMKA: Voľbou **Spustenie aplikácie** spustíte

programy pod systémovým používateľom "nobody". Práva pre spúšťanie aplikácií cez **Plánovač** sú definované systémom macOS.

Keďže aktualizácia je najčastejšie používanou úlohou, vysvetlíme si, ako pridať novú:

1. Z roletového menu **Plánovaná úloha** zvoľte **Aktualizácia**.
2. Zadajte názov do poľa **Názov úlohy**.
3. Frekvenciu opakovania zadajte zvolením hodnoty v roletovom menu **Vykonanie úlohy**. Na základe zadanej frekvencie budete upozornení na rozdielne nastavenia aktualizácie. Ak zvolíte hodnotu **Definované používateľom**, budete vyzvaní na zadanie dátumu a času vo formáte *cron*. (Pre viac podrobností prejdite na kapitolu Vytvorenie úlohy definovanej používateľom 23.)
4. V nasledujúcom kroku zadajte, aká akcia sa vykoná v prípade, že nie je možné spustiť alebo dokončiť úlohu v naplánovanom čase.
5. Následne sa zobrazí okno s informáciami o naplánovanej úlohe. Kliknite na tlačidlo **Ukončiť**. Nová plánovaná úloha bude pridaná do zoznamu aktuálnych plánovaných úloh.

Štandardne obsahuje systém dôležité plánované úlohy pre zaistenie správneho fungovania produktu. Tieto by nemali byť menené a štandardne sú skryté. Pre zmenu tejto možnosti a zviditeľnenia týchto úloh kliknite na **Nastavenie** > **Zobraziť pokročilé nastavenia...** (prípadne stlačte cmd+,) > **Plánovač** a zvoľte možnosť **Zobrazovať systémové úlohy**.

11.2.2 Vytvorenie úlohy definovanej používateľom

Predtým, ako vyberiete tento typ úlohy (**Definované používateľom**), musíte nastaviť niekoľko parametrov potom, čo z roletového menu **Vykonanie úlohy** vyberiete túto možnosť.

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 (*) - výraz sa musí zhodovať so všetkými hodnotami v poli; to znamená, že hviezdička v 3. poli (deň v mesiaci) znamená ľubovoľný deň.
- pomlčka (-) - definuje rozsah; napríklad 3-9
- čiarka (,) - oddeľuje položky v zozname; 1, 3, 7, 8
- lomka (/) - definuje vzostupnosť rozsahu; 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.

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

11.3 Live Grid

Systém včasného varovania Live Grid slúži na okamžité a nepretržité informovanie spoločnosti ESET o nových infiltráciách. Obojsmerný systém včasného varovania Live Grid má jediný účel - zlepšenie ochrany, ktorú vám môžeme poskytnúť. Najlepší spôsob ako zabezpečiť, aby sme vedeli o nových hrozbách okamžite ako sa objavia, je cez prepojenie na našich zákazníkov, ktorí v tejto súvislosti vystupujú v úlohe "vírusovej polície". Sú dve možnosti:

1. Môžete sa rozhodnúť nezapnúť si Systém včasného varovania Live Grid. Neprídete tak o žiadnu funkcionalitu vášho softvéru...
2. Môžete si nastaviť Systém včasného varovania Live Grid, aby odosielal anonymné informácie o nových hrozbách a o tom, kde sa škodlivý kód nachádza. Takýto súbor sa pošle na detailnú analýzu a môže prispieť k rozšíreniu vírusovej databázy a k vylepšeniu detekcie.

Systém včasného varovania Live Grid zbiera anonymné informácie z vášho počítača priamo súvisiace s novými hrozbami. Tieto informácie môžu obsahovať vzorku, alebo kópiu súboru, v ktorom bola zistená hrozba, cestu k tomuto súboru, názov súboru, dátum a čas, proces, akým sa hrozba objavila na vašom počítači a informácie o vašom operačnom systéme. Žiadna z týchto informácií V ŽIADNOM PRÍPADE nebude použitá za iným účelom, než je skorá reakcia na nové infiltrácie.

Prístup k nastaveniam Live Grid nájdete v časti **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **ESET LiveGrid**. Pre aktiváciu LiveGrid označte možnosť **Povoliť ESET LiveGrid Reputačný systém (odporúča sa)**.

11.3.1 Posielanie podozrivých súborov

Možnosť spracovávania podozrivých súborov umožňuje upraviť spôsob, akým sa potenciálne hrozby posielajú do laboratórií ESET na analýzu. Ak si neželáte odosielať tieto súbory automaticky, odznačte možnosť **Posielanie podozrivých súborov** v časti **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Nástroje** > **Live Grid** > **Nastavenia...**).

Ak nájdete podozrivý súbor, máte možnosť ho okamžite poslať na analýzu do našich laboratórií kliknutím na **Nástroje** > **Poslať súbor na analýzu** v hlavnom okne programu. Ak sa naozaj jedná o škodlivú aplikáciu, jej detekcia bude pridaná do najbližšieho vydania vírusovej databázy.

Posielanie anonymných štatistických informácií – Systém včasného varovania Live Grid zbiera anonymné informácie z vášho počítača priamo súvisiace s novými hrozbami. Tieto informácie môžu obsahovať názov infiltrácie, dátum a čas detekcie, verziu produktu ESET, typ vášho operačného systému a nastavenie umiestnenia. Štatistika sa posiela na servery ESET raz, prípadne dvakrát za deň.

Príklad zasielanej štatistickej 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 – vám umožní vylúčiť niektoré súbory a priečinky zo zasielania. Napríklad môže byť užitočné vylúčenie dokumentov, ktoré by mohli obsahovať osobné informácie ako napr. textové dokumenty alebo tabuľky. Najbežnejšie typy takýchto úborov sú už vylúčené štandardným nastavením programu (.doc atď.). Do zoznamu vylúčených súborov sa dajú pridávať aj ďalšie typy súborov.

Kontaktný e-mail (nepovinný údaj) – váš kontaktný e-mail môže byť zasielaný spolu s podozrivými súbormi pre prípad, že by boli potrebné doplnkové informácie na vykonanie analýzy. Na váš e-mail bude zaslaná odpoveď len v tom prípade, že bude potrebné získať ďalšie informácie.

11.4 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 Security falošne označil ako infikované.

Je možné uložiť ľubovoľný súbor do karantény. Toto je odporúčané pri súboroch, ktoré sa správajú podozrivo, ale nie sú detegované antivírusovým skenerom. Súbory v karanténe môžete odosielať na analýzu do Vírusového laboratória ESET.

Súbory uložené v priečinku karantény je možné zobraziť 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 Security. Súbory v karanténe sú uložené v bezpečnej kryptovanej forme a môžu byť obnovené po opätovnej inštalácii ESET Endpoint Security.

11.4.1 Pridanie súborov do karantény

ESET Endpoint Security automaticky ukladá zmazané súbory do karantény (ak ste túto možnosť neodmietli vo výstražnom okne). Ak si želáte pridať súbor do karantény manuálne, z okna **Karanténa** kliknite na tlačidlo **Presunúť...** a vyberte konkrétny súbor.

11.4.2 Obnovenie súborov z karantény

Súbory uložené do karantény je možné obnoviť na ich pôvodné miesto. Pre tento účel použite tlačidlo **Obnoviť**. Obnovenie je tiež dostupné z kontextového menu po stlačení ctrl, kliknutí na príslušný súbor v okne **Karanténa** a kliknutí na **Obnoviť**. Kontextové menu (ctrl+klik na záznam) tiež ponúka možnosť **Obnoviť do...**, ktorá vám umožňuje obnoviť súbor na iné miesto než to pôvodné, z ktorého bol vymazaný.

11.4.3 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 zvoľte možnosť **Poslať súbor na analýzu** z kontextového menu.

11.5 Oprávnenia

Nastavenia ESET Endpoint Security 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.

Pre špecifikáciu privilégií používateľov prejdite na **Nastavenie** > **Zobraziť pokročilé nastavenia...** (prípadne stlačte cmd+,) > **Oprávnenia**.

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

POZNÁMKA: Ak je zoznam Vybratých používateľov prázdny, všetci používatelia majú povolenie vykonávať zmeny v programe.

11.6 Prezentačný režim

Prezentačný režim je funkcia určená pre používateľov, ktorí musia neprerušovane používať svoj softvér a neželajú si byť vyrušovaní notifikáciami a dialógovými oknami, taktiež požadujú minimálne vyťaženie procesora antivírusom. Prezentačný režim možno použiť aj pri prezentáciách, ktoré by mohli byť prerušené notifikáciami programu. Zapnutím prezentačného režimu budú zakázané všetky notifikácie programu a aktivity plánovača. Samotná ochrana beží ďalej v pozadí, ale nevyžaduje žiadne zásahy používateľa.

Kliknite na **Nastavenie** > **Počítač** a kliknite na **Prezentačný režim** pre manuálne zapnutie prezentačného režimu.

Po zaškrtnutí možnosti **Automaticky zapnúť prezentačný režim pri spustení aplikácie v režime na celú obrazovku** sa Prezentačný režim automaticky zapne po spustení aplikácie na celú obrazovku a po jej skončení sa vypne. Táto možnosť je užitočná pre okamžité spustenie prezentačného režimu po spustení aplikácie na celú obrazovku alebo začatí prezentácie.

Môžete si tiež zvoliť možnosť **Automaticky vypnúť prezentačný režim po X minútach** zaškrtnutím tejto možnosti a zvolením požadovaného časového úseku.

Zapnutie prezentačného režimu môže predstavovať potenciálne bezpečnostné riziko, a preto sa ikonka ochrany na lište zmení na oranžovú.

POZNÁMKA: Ak je osobný firewall v interaktívnom režime a zapnete prezentačný režim, môžu sa vyskytnúť problémy s pripojením sa do internetu. To môže byť problematické ak napríklad spustíte program, ktorý sa pripája do internetu. Je to spôsobené tým, že za bežných okolností by si firewall vyžiadal používateľské potvrdenie pripojenia (ak nie sú definované žiadne pravidlá alebo výnimky pre spojenia), ale v prezentačnom režime sú všetky vyskakovacie okná vypnuté. Riešením je definovať pravidlá alebo výnimky pre každú aplikáciu, ktorá by mohla mať konflikt s týmto správaním sa alebo zvoliť si iný režim filtrovania 18 v osobnom firewalle. Majte tiež na pamäti, že ak pri zapnutom prezentačnom režime pracujete s aplikáciou alebo stránkou, ktorá predstavuje potenciálne riziko, bude zablokovaná. Nezobrazí sa žiadne vysvetlenie alebo varovanie, lebo sú vypnuté všetky akcie vyžadujúce zásah používateľa.

11.7 Bežiace procesy

Reputácia spustených procesov zobrazuje spustené programy a procesy na vašom počítači a zabezpečuje pohotovú a neustálu informovanosť spoločnosti ESET o nových infiltráciách. Vďaka technológii ESET Live Grid ponúka ESET Endpoint Security detailnejšie informácie ohľadom bežiacich procesov.

- **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 Security stupeň rizika pomocou technológie Live Grid na základe heuristických pravidiel a kontroly každého subjektu pre prítomnosť škodlivého kódu. Potom na základe týchto výsledkov pridelí 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 Live Grid.
- **Čas objavenia** – doba, odkedy bol proces objavený technológiou ESET Live Grid.
- **ID aplikačného bundle** – 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 bundle** – názov výrobcu alebo proces aplikácie,
- **Verzia súboru** – informácia od vydavateľa aplikácie,
- **Meno produktu** – názov aplikácie, obvykle obchodné meno.

12. Používateľské rozhranie

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

- Pre zobrazenie úvodného obrázku pri štarte systému, zvoľte možnosť **Zobrazovať úvodný obrázok pri štarte**.
- Možnosť **Ponechať aplikáciu v Docku** umožňuje zobrazenie ikonky ESET Endpoint Security v macOS docku a prepínanie medzi ESET Endpoint Security a inými spustenými aplikáciami stlačením *cmd+tab*. Zmeny sa uplatnia po reštarte ESET Endpoint Security (obvykle po reštarte počítača).
- Možnosť **Používať štandardné menu** vám umožňuje používať niektoré klávesové skratky (pozri Klávesové skratky 9) a zobrazovať štandardné položky v menu (rolety Používateľské rozhranie, Nastavenia a Nástroje) v macOS menu bar (horný okraj obrazovky).
- Pre zobrazovanie popiskov (tzv. tooltips) k tlačidlám a voľbám programu ESET Endpoint Security zapnite možnosť **Zobrazovať popis tlačidiel**.
- Možnosť **Zobrazovať skryté súbory** vám umožňuje vidieť skryté súbory v nastaveniach **Cieľov kontroly** v **Kontrole počítača**.
- Ikona produktu ESET Endpoint Security je štandardne zobrazená v paneli s ponukami (Menu Bar Extras), ktorý sa nachádza v pravej časti macOS Menu Baru. Túto možnosť vypnete pomocou voľby **Zobraziť ikonku v doplnkoch panelu s ponukami**. Zmena sa prejaví po reštarte aplikácie ESET Endpoint Security, resp. po reštarte počítača.

12.1 Upozornenia a notifikácie

Sekcia **Upozornenia** vám umožňuje nastaviť, ako sa budú správať výstražné upozornenia a systémové notifikácie v ESET Endpoint Security.

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 časti 26.

Zvolenie možnosti **Zobrazovať upozornenia na pracovnej ploche** zapne výstražné okná, ktoré nepotrebujú 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 (štandardne 4 sekundy).

Od verzie ESET Endpoint Security 6.2 môžete zabrániť zobrazovaniu niektorých **Stavov ochrany** v hlavnom okne programu (okno **Stav ochrany**). Viac sa dozviete v kapitole Stavy ochrany 26.

12.1.1 Výstražné upozornenia

ESET Endpoint Security 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 (**Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Upozornenia** > **Nastavenia...**) zobrazuje zoznam všetkých výstražných dialógov, ktoré spúšťa ESET Endpoint Security. Pre povolenie alebo vypnutie jednotlivých notifikácií použite zaškrtávacie políčka pri **Názve hlásenia**. Navyše je možné definovať **Podmienky zobrazenia**, ktoré určujú, kedy sa zobrazia hlásenia o nových verziách programu a operačného systému.

12.1.2 Stavy ochrany

Aktuálny stav ochrany ESET Endpoint Security môžete meniť aktivovaním a deaktivovaním stavov v časti **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Upozornenia** > **Zobraziť na obrazovke Stav ochrany: Nastavenia...**. Stav rôznych funkcií programu bude zobrazený alebo schovaný z hlavnej obrazovky ESET Endpoint Security (okno **Stav ochrany**).

Stav ochrany môžete schovať pre nasledujúce funkcie a moduly:

- Firewall
- Anti-Phishing
- Ochrana prístupu na web
- E-mailová ochrana
- Prezentačný režim
- Aktualizácia operačného systému
- Vypršanie licencie
- Vyžaduje sa reštart počítača

12.2 Kontextové menu

Integrácia kontextového menu môže byť povolená v časti **Nastavenie** > **Zobraziť pokročilé nastavenia...** (prípadne stlačte cmd+,) > **Kontextové menu** zvolením možnosti **Používať kontextové menu**. Možnosti kontextového menu budú dostupné v okne **Finder** po stlačení tlačidla CTRL a kliknutí na ľubovoľný súbor alebo priečinok.

13. Aktualizácia programu

Pravidelné aktualizácie ESET Endpoint Security sú kľúčom k udržaniu čo najvyššej úrovne bezpečnosti. Aktualizačný modul zabezpečuje, aby bola vírusová databáza programu vždy aktuálna.

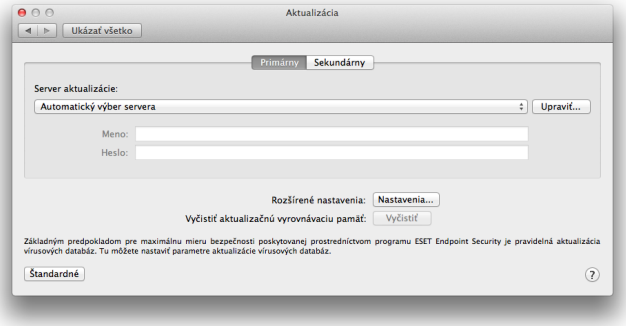
Ak kliknete v hlavnom menu programu na **Aktualizácia,** zistíte momentálny stav aktualizácie vírusovej databázy, vrátane času a dátumu poslednej úspešnej aktualizácie ako aj informáciu o prípadnej potrebe aktualizovať. Takisto tu nájdete možnosť manuálneho spustenia procesu aktualizácie - **Aktualizovať vírusovú databázu**.

Za normálnych okolností (pravidelné úspešné aktualizácie) je v okne **Aktualizácia** v zobrazená správa **Aktualizácia nie je potrebná – vírusová databáza je aktuálna**. Ak to tak nie je, program nie je aktualizovaný a zvyšuje sa riziko infiltrácie. Ak nie je možné aktualizovať vírusovú databázu, je potrebné skontrolovať nastavenia aktualizácie 27 – častá príčina je, že boli nesprávne zadané licenčné údaje 8, alebo že nie je správne nastavená sieť 29.

Tiež sa tu nachádza verzia vírusovej databázy v programe. Toto numerické označenie je zároveň aktívny odkaz na stránku ESET s informáciami o pridaných vzorkách v rámci danej aktualizácie.

13.1 Nastavenie aktualizácií

V predvolenom nastavení je **Server aktualizácie** nastavený na možnosť **Automatický výber servera**. V tomto prípade je zabezpečené, že sa budú aktualizácie vírusovej databázy sťahovať zo serverov ESET z minimálnou sieťovou záťažou.



Pre pridanie nového aktualizačného servera kliknite na **Upraviť...** a vložte adresu nového servera do poľa **Aktualizačný server**. Ak zvolíte iný aktualizačný server, uistite sa u prevádzkovateľa tohto aktualizačného servera, či nie je potrebné zadať aj **Meno** a **Heslo** pre prístup k tomuto serveru - inak aktualizačné súbory nemusia byť stiahnuté.

ESET Endpoint Security umožňuje nastaviť alternatívny alebo tzv. "failover" server pre aktualizácie. **Primárny** server môže byť váš mirror server a ako **Sekundárny** môžete použiť štandardný ESET server pre aktualizácie. Sekundárny server sa musí líšiť od Primárneho, inak nebude použitý. Ak nezadáte Sekundárny server, Meno a Heslo, funkcionalita záložného aktualizačného servera nebude fungovať. Môžete zvoliť aj **Automatický výber servera** a zadať vaše Meno a Heslo – program automaticky vyberie najvhodnejší server pre aktualizácie.

Režim proxy vám umožňuje aktualizovať vírusovú databázu cez proxy server (napr. cez lokálny HTTP proxy). Tento server sa môže ale nemusí zhodovať s globálnym proxy serverom, ktorý sa používa pre všetky programové komponenty vyžadujúce pripojenie. Nastavenia globálneho proxy servera mali byť definované počas inštalácie alebo v nastaveniach pre proxy server 29.

Sťahovanie aktualizácií z proxy servera nastavíte nasledovne:

1. zvoľte z rozbaľovacej ponuky **Spojenie pomocou proxy servera**
2. kliknite na **Detegovať** aby program vyplnil IP adresu a port (štandardne **3128**)
3. ak komunikácia s proxy serverom vyžaduje autentifikáciu, zadajte platné **Meno** a **Heslo** do príslušných polí.

ESET Endpoint Security deteguje nastavenia proxy zo Systémových nastavení macOS. Tieto môžu byť nakonfigurované v macOS pod > **Systémové nastavenia** > **Sieť** > **Rozšírené** > **Proxy**.

Ak povolíte možnosť **Použiť priame pripojenie ak nie je k dispozícii HTTP proxy**, ESET Endpoint Security sa

pokúsi automaticky spojiť s aktualizačnými servermi bez použitia proxy. Túto možnosť odporúčame mobilným používateľom s laptopmi MacBook.

Ak program nevie stiahnuť aktualizáciu vírusovej databázy, skúste vyčistiť aktualizačnú "cache" a aktualizačné súbory stlačením tlačidla **Vyčistiť**.

13.1.1 Rozšírené nastavenia

Ak si neželáte zobrazovať upozornenie po každej úspešnej aktualizácii vírusovej databázy, označte možnosť **Nezobrazovať upozornenia o úspešnej aktualizácii**.

Možnosť **Predbežné aktualizácie** umožňuje sťahovanie modulov vo fáze testovania. Toto môže pomôcť pri riešení najnovších problémoch s produktom. **Oneskorená aktualizácia** aktualizuje vírusovú databázu a moduly o niekoľko hodín neskôr po tom, čo boli vydané.

ESET Endpoint Security poskytuje zálohu a obnovu modulov (tzv. rollback) vírusovej databázy. Aby sa vytvorili obrazy (snapshoty) vírusových databáz, ponechajte možnosť **Povoliť zálohovanie modulov** zaškrtnutú. Ak máte podozrenie, že nová aktualizácia vírusovej databázy alebo programových modulov môže byť nestabilná alebo poškodená, môžete vrátiť vírusovú databázu do predchádzajúceho stavu a zakázať aktualizácie na určený časový interval. Prípadne môžete povoliť predtým zakázané aktualizácie. Ak sa vykoná obnova modulov zo zálohy, použite roletové menu **Nastaviť dobu pozastavenia aktualizácie modulov na** pre nastavenie dokedy majú byť vypnuté aktualizácie. Vyberte možnosť **Do zneplatnenia**, ak si želáte zapnúť pravidelné aktualizácie manuálne. Keďže táto možnosť predstavuje potenciálne bezpečnostné riziko, označenie tejto možnosti neodporúčame.

Nastaviť maximálny čas neaktuálnosti databázy automaticky – Umožňuje vám nastaviť čas (v dňoch), po ktorom bude vírusová databáza hlásená ako neaktuálna. Prednastavená hodnota je 7 dní.

13.2 Ako vytvoriť úlohy aktualizácie

Aktualizácie možno spúšťať manuálne kliknutím na **Aktualizovať vírusovú databázu** v okne **Aktualizácia** v hlavnom menu.

Aktualizácie možno spúšťať aj ako plánované úlohy. Pre nakonfigurovanie plánovanej úlohy kliknite na **Nástroje** > **Plánovač**. Štandardne sú v ESET Endpoint Security aktivované tieto aktualizačné úlohy:

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

Každá z týchto úloh môže byť nastavená tak, aby zodpovedala vašim potrebám. Okrem úpravy existujúcich úloh aktualizácie môžete vytvárať aj nové úlohy aktualizácie s vlastnou konfiguráciou. Pre bližší popis vytvárania a nastavenia úloh aktualizácie si pozrite sekciu nazvanú Plánovač 22.

13.3 Aktualizácia programu na novú verziu (upgrade)

Z dôvodu zaručenia maximálnej ochrany je dôležité používať najnovšiu verziu produktu ESET Endpoint Security. Ak si želáte overiť, či je k dispozícii novšia verzia produktu, kliknite na **Domov** z hlavného menu na ľavej strane. Ak je dostupná nová verzia, kliknite na **Zistiť viac...**.

Po kliknutí na **Stiahni** bude inštalačný súbor stiahnutý do vášho priečinka **Downloads** alebo iného priečinka, ktorý je prednastavený vašim internetovým prehliadačom. Po dokončení sťahovania súboru spustite súbor a postupujte podľa krokov inštalačného sprievodcu. Vaše licenčné dáta budú automaticky prenesené do novej inštalácie.

Dostupnosť novej verzie produktu odporúčame pravidelne overovať, najmä ak máte program nainštalovaný z CD alebo DVD.

13.4 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 Security vás bude notifikovať o chýbajúcich aktualizáciách na základe úrovne zobrazovania, ktorú si nastavíte. Dostupnosť notifikácií si môžete upraviť v sekcii **Nastavenie** > **Zobraziť pokročilé nastavenia...** (prípadne stlačte cmd+,) > **Upozornenia > Nastavenia...**. Použite voľbu **Podmienky zobrazenia**, ktorá sa nachádza v riadku **Aktualizácie operačného systému**.

- **Všetky aktualizácie** - upozornenie sa zobrazí po každej chýbajúcej aktualizácii
- **Iba odporúčané aktualizácie** - budete informovaný iba o odporúčaných aktualizáciách

Ak nechcete byť informovaný o chýbajúcich aktualizáciách, zrušte označenie voľby **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 Security > 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 upozornení zobrazuje aktualizácie získané pomocou nástroja príkazového riadku 'softwareupdate'. Aktualizácie získané týmto nástrojom sa môžu líšiť od aktualizácií získaných aplikáciou 'Software updates'. Ak si želáte nainštalovať všetky dostupné aplikácie zobrazené v okne 'Missing system updates' a taktiež tie, ktoré nie sú zobrazené aplikáciou 'Software updates', musíte použiť nástroj príkazového riadku 'softwareupdate'. Viac sa dozviete o tomto nástroji v manuáli 'softwareupdate' a to zadaním príkazu `man softwareupdate` do okna **Terminálu**. Táto možnosť je určená iba pre skúsených používateľov.

14. Rôzne

14.1 Import a export nastavení

Možnosť importovať a exportovať nastavenia ESET Endpoint Security 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 Security pre neskoršie použitie. Export nastavení je užitočný pri nastavovaní vlastnej preferovanej konfigurácie ESET Endpoint Security 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.

14.2 Proxy server

Nastavenia proxy servera môžete upravovať v sekcii **Nastavenie** > **Zmeniť pokročilé nastavenia...**. Nastavenia proxy servera vykonané na tejto úrovni platia ako globálne nastavenia proxy servera pre celý ESET Endpoint Security. Tu nastavené parametre sa použijú vo všetkých moduloch, ktoré potrebujú pripojenie na Internet. ESET Endpoint Security podporuje Basic Access a NTLM (NT LAN Manager) typy pripojenia.

Ak chcete upraviť nastavenia proxy servera na tejto úrovni, označte možnosť **Používať proxy server** a potom zadajte adresu proxy servera do poľa **Proxy server** a číslo portu, cez ktorý sa bude proxy server pripájať (štandardne 3128).

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

14.3 Zdielaná lokálna vyrovnávacia pamäť

Ak si želáte túto funkcionalitu zapnúť, choďte do **Nastavenie** > **Zobraziť pokročilé nastavenia...** > **Zdielaná lokálna vyrovnávacia pamäť** a označte možnosť **Povoliť ESET Zdielanú lokálnu vyrovnávaciu pamäť**. Táto funkcionalita zvyšuje výkon vo virtuálnych prostrediach tým, že predchádza duplicitnej kontrole na sieti. Každý súbor bude kontrolovaný len raz a uložený v lokálnej vyrovnávacej pamäti (cache). Pri novej kontrole bude ESET Endpoint Security hľadať kontrolované súbory vo vyrovnávacej pamäti. Ak nájde zhodné súbory, vylúči ich z kontroly.

Nastavenia obsahujú:

- **Server** – Názov alebo IP adresa počítača, na ktorom sa nachádza vyrovnávacia pamäť.
- **Port** – Číslo portu použitého pre komunikáciu (rovnaké ako pri zdieľaní lokálnej vyrovnávacej pamäte; štandardne 3537).
- **Heslo** – Zadajte heslo (nepovinné)

NOTE: Podrobné inštrukcie k inštalácii a nastaveniu Zdielanej pamäte nájdete v Používateľskej príručke. Príručka je dostupná iba v angličtine.