ESET Cyber Security

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r.o.

ESET Cyber Security byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte https://www.eset.cz.

Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována žádným prostředkem, ani distribuována jakýmkoliv způsobem bez předchozího písemného povolení společnosti ESET, spol. s r.o.

ESET, spol. s r.o. si vyhrazuje právo změny programových produktů popsaných v této publikaci bez předchozího upozornění.

Technická podpora: https://servis.eset.cz

REV. 2023-03-19

1 ESET Cyber Security 1
1.1 Co je nového ve verzi 6? 1
1.2 Systémové požadavky 1
2 Instalace 2
2.1 Typická instalace 2
2.2 Pokročilá instalace 3
2.3 Povolení systémových rozšíření 4
2.4 Povolení úplného přístupu k disku 5
3 Aktivace produktu 6
4 Odinstalace 6
5 Základní přehled 6
5.1 Klávesové zkratky 7
5.2 Kontrola stavu systému 7
5.3 Co dělat, když program nepracuje správně? 8
6 Ochrana počítače 8
6.1 Antivirová a antispywarová ochrana 8
6.1 Obecné 8
6.1 Výjimky 9
6.1 Kontrola po startu 9
6.1 Rezidentní ochrana souborového systému 9
6.1 Rozšířená nastavení 10
6.1 Konfigurace rezidentní ochrany 10
6.1 Ověření stavu rezidentní ochrany 10
6.1 Co dělat, když nefunguje rezidentní ochrana? 11
6.1 Volitelná kontrola počítače 11
6.1 Typ kontroly 12
6.1 Smart kontrola 12
6.1 Volitelná kontrola 12
6.1 Cíle kontroly 13
6.1 Profily kontroly 13
6.1 Nastavení parametrů jádra ThreatSense 14
6.1 Objekty 14
6.1 Možnosti 15
6.1 Léčení 15
6.1 Výjimky 15
6.1 Omezení 16
6.1 Ostatní 16
6.1 Nalezena infiltrace 17
6.2 Kontrola a blokování výměnných médií 18
7 Anti-Phishing 18
8 Webová a poštovní ochrana 18
8.1 Webová ochrana 19
8.1 Porty 19
8.1 Seznam URL adres 19
8.2 Poštovní ochrana 19
8.2 Kontrola protokolu POP3 20
8.2 Kontrola protokolu IMAP 20
9 Aktualizace 21
9.1 Nastavení aktualizace 21
9.1 Rozšířená nastavení 21

9.2 Jak vytvořit aktualizační úlohu ... 22
9.3 Aktualizace ESET Cyber Security na novou verzi ... 22
9.4 Aktualizace operačního systému ... 22
10 Nástroje ... 23
10.1 Protokoly ... 23
10.1 Údržba protokolů ... 24
10.1 Filtrování protokolů ... 24
10.2 Plánovač ... 25
10.2 Vytvoření nové úlohy ... 25
10.2 Kontrola jako vlastník složky ... 27
10.2 Vytvoření uživatelské úlohy ... 27
10.3 Karanténa ... 28
10.3 Vložení do karantény ... 28
10.3 Obnovení z karantény ... 28
10.3 Odesílání souborů ... 28
10.4 Spuštěné procesy ... 28
10.5 Síťová spojení ... 29
10.6 ESET LiveGrid® ... 30
10.6 Nastavení Live Grid ... 30
10.7 Odeslat soubor k analýze ... 31
11 Uživatelské rozhraní ... 31
11.1 Upozornění a události ... 32
11.1 Zobrazení upozornění ... 32
11.1 Stavy ochrany ... 32
11.2 Oprávnění ... 33
11.3 Kontextové menu ... 33
11.4 Import a export nastavení ... 34
11.5 Nastavení proxy serveru ... 35
12 Licenční ujednání s koncovým uživatelem ... 35
13 Zásady ochrany osobních údajů ... 41

ESET Cyber Security

ESET Cyber Security představuje nový přístup k plně integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ThreatSense® je rychlá a přesná. Výsledkem je inteligentní systém, který neustále chrání váš počítač před škodlivými kódy a útoky.

ESET Cyber Security je komplexní bezpečnostní řešení, které nabízí výkonnou a účinnou ochranu při zachování minimálního dopadu na výkon systému. Na základě umělé inteligence a pokročilé heuristiky dokáže ESET Cyber Security proaktivně eliminovat viry, červy, trojské koně, spyware, adware, rootkity a další internetové hrozby, aniž by došlo ke zpomalení systému.

Co je nového ve verzi 6?

ESET Cyber Security verze 6 nabízí následující aktualizace a vylepšení:

- **Podpora 64-bitové architektury**
- **Anti-Phishingová ochrana** – chrání vás před pokusy o získání hesla a dalších citlivých informací zablokováním přístupu na podvodné webové stránky, které se vydávají za legitimní.
- **Hlídání aktualizací systému** – ESET Cyber Security verze 6 přináší vylepšenou podporu systémových oznámení a bude vás pravidelně informovat o dostupných aktualizacích systému. Pro více informací se podívejte do kapitoly aktualizace operačního systému.
- **Stavy ochrany** – pomocí této možnosti můžete vypnout upozorňování na specifické stavy ochrany (například: *ochrana poštovních klientů je vypnutá*, *vyžadován restart systému*).
- **Kontrola médií** – zajišťuje kontrolu výměnných médií a umožňuje definovat jednotky, které chcete, resp. nechcete kontrolovat.
- **Síťová spojení** – tato součást zobrazuje seznam otevřených spojení a umožňuje snadné vytvoření výjimek.

Další podrobnosti o nových funkcích v ESET Cyber Security naleznete v Databázi znalostí.

Systémové požadavky

Pro plynulý běh ESET Cyber Security by měl váš systém splňovat následující hardwarové a softwarové požadavky:

	Systémové požadavky:
Architektura procesoru	Intel 64-bit, M1, M2
Operační systém	macOS 10.12 a novější
Operační paměť	300 MB
Volné místo na pevném disku	200 MB

Kromě procesorů Intel podporuje ESET Cyber Security od verze 6.10.900.0 také Apple M1 a M2 čipy (prostřednictvím emulátoru Rosetta 2).

Instalace

Před spuštěním instalace ukončete všechny programy běžící na vašem počítači. ESET Cyber Security obsahuje komponenty, které mohou způsobit konflikt s antivirovými programy jiných výrobců. Proto doporučujeme ostatní bezpečnostní software před instalací produktu ESET odebrat.

Pro spuštění instalačního průvodce postupujte takto:

- Pokud instalujete ze souboru staženého z webové stránky ESET, otevřete soubor a dvojklikem na ikonu **Instalátor** spusťte instalaci programu.
- Pokud instalujete z CD nebo DVD, vložte médium do mechaniky, otevřete médium z Plochy nebo okna **Finder** a dvojklikem na ikonu **Instalátor** spusťte instalaci programu.



Před samotným zahájením instalace instalační program nejprve automaticky ověří, zda není na webových stránkách dostupná novější verze produktu. Pokud ano, bude nabídnuta ke stažení, a poté zahájena její instalace.

Po odsouhlasení licenčních podmínek vyberte požadovaný typ instalace:

- Typická instalace
- Pokročilá instalace

Typická instalace

Typická instalace nainstaluje produkt s doporučeným nastavením, které je vhodné pro většinu uživatelů. Toto nastavení zajišťuje maximální zabezpečení počítače v kombinaci s nízkými nároky na systémové prostředky. Tento typ instalace je předvybrán jako výchozí a je doporučen pro uživatele, kteří nevyžadují specifické nastavení.

1. V okně **ESET LiveGrid** vyberte požadovanou možnost a klikněte na **Pokračovat**. Pokud se později rozhodnete, že chcete nastavení změnit, přejdete do **Nastavení LiveGrid**. Více informací o technologii ESET Live Grid najdete v našem glosáři.
2. V okně **Potenciálně nechtěné aplikace** vyberte požadovanou možnost (viz potenciálně nechtěná aplikace?) a

klikněte na **Pokračovat**. Pokud se později rozhodnete, že chcete toto nastavení změnit, použijte **Rozšířeného nastavení**.

3.Klikněte na možnost **Instalovat**. Pokud vás k tomu systém vyzve, zadejte adminstrátorské heslo do macOS, potvrďte jej a klikněte na tlačítko **Instalovat aplikaci**.

Pro dokončení instalace ESET Cyber Security:

macOS Big Sur (11)

1.Povolte systémová rozšíření.

2.Povolte úplný přístup k disku.

3.Umožněte programu ESET přidat nastavení proxy. Obdržíte následující upozornění: "ESET Cyber Security**"Chtěli byste přidat konfigurace serveru proxy**. Jakmile obdržíte toto oznámení, klikněte na **Povolit**. Pokud kliknete na **Nepovolit**, nebude ochrana přístupu na web fungovat.

macOS 10.15 a novější

1.Na macOS 10.13 a novější zobrazí operační systém upozornění, že je **blokováno systémové rozšíření**, a v hlavním okně produktu ESET Cyber Security se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Cyber Security plně fungovat, musíte ručně povolit načítání rozšíření jádra systému. To provedete v **Předvolbách systému** v sekci **Zabezpečení a soukromí**, kde povolte aplikacím vydaným společností **ESET, spol. s.r.o.** načítat rozšíření kliknutím na tlačítko **Povolit.** Další informace naleznete v Databázi znalostí.

2.Na macOS 10.14 a novějších se v hlavním okně produktu ESET Cyber Security objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Cyber Security plně fungovat, musíte aplikaci povolit **Úplný přístup k disku**. Klikněte na **Otevřít předvolby systému** > **Zabezpečení a soukromí**. Přejděte na záložku **Soukromí** a vyberte možnost **Úplný přístup k disku**. Pro povolení změn klikněte na ikonu zámku. Klikněte na ikonu + a ze seznamu vyberte aplikaci ESET Cyber Security. Zobrazí se výzva k restartování počítače. Klikněte na tlačítko **Později**. Počítač zatím nerestartujte. V oznámení produktu ESET Cyber Security klikněte na tlačítko **Spustit znovu** nebo restartujte počítač. Další informace naleznete v Databázi znalostí.

Po dokončení instalace ESET Cyber Security doporučujeme provést kontrolu počítače na přítomnost škodlivého kódu. Pro spuštění kontroly klikněte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Smart kontrola**. Pro více informací o volitelné kontrole počítače přejděte do kapitoly volitelná kontrola počítače.

Pokročilá instalace

Pokročilá instalace je určena zkušeným uživatelům, kteří chtějí během instalačního procesu měnit pokročilé nastavení.

- **Proxy server**

Pokud pro připojení k internetu používáte proxy server, pro jeho konfiguraci vyberte možnost **Používám proxy server**. Následně do pole **Adresa** zadejte IP adresu nebo název proxy serveru a vyplňte **port** (standardně 3128). V případě, že proxy vyžaduje autentifikaci, zadejte **uživatelské jméno** a **heslo**. Jestliže proxy server nepoužíváte, vyberte **Nepoužívám proxy server**. Pokud si nejste jisti, zda pro připojení k internetu proxy server používáte, vyberte možnost **Převzít nastavení ze systému**.

- **Oprávnění**
Definujte seznam privilegovaných uživatelů a skupin, které budou mít oprávnění k úpravě konfigurace programu. Ze seznamu na levé straně vyberte uživatele nebo skupinu, a následně klikněte na tlačítko **Přidat** pro přidání uživatele do seznamu **Privilegovaných uživatelů**. K zobrazení všech systémových uživatelů vyberte **Zobrazit všechny uživatele**. Pokud ponecháte seznam prázdný, všichni uživatelé budou privilegovaní.

- **ESET LiveGrid®**
Pro více informací o ESET LiveGrid přejděte do Slovníku pojmů.

- **Potenciálně nechtěné aplikace**
Pro více informací o potenciálně nechtěných aplikacích přejděte do Slovníku pojmů.

Pro dokončení instalace ESET Cyber Security:

macOS Big Sur (11)

1. Povolte systémová rozšíření.
2. Povolte úplný přístup k disku.
3. Umožněte programu ESET přidat nastavení proxy. Obdržíte následující upozornění: "ESET Cyber Security"**Chtěli byste přidat konfigurace serveru proxy**. Jakmile obdržíte toto oznámení, klikněte na **Povolit**. Pokud kliknete na **Nepovolit**, nebude ochrana přístupu na web fungovat.

macOS 10.15 a novější

1. Na macOS 10.13 a novější zobrazí operační systém upozornění, že je **blokováno systémové rozšíření**, a v hlavním okně produktu ESET Cyber Security se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Cyber Security plně fungovat, musíte ručně povolit načítání rozšíření jádra systému. To provedete v **Předvolbách systému** v sekci **Zabezpečení a soukromí**, kde povolte aplikacím vydaným společností **ESET, spol. s.r.o.** načítat rozšíření kliknutím na tlačítko **Povolit**. Další informace naleznete v Databázi znalostí.
2. Na macOS 10.14 a novějších se v hlavním okně produktu ESET Cyber Security objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Cyber Security plně fungovat, musíte aplikaci povolit **Úplný přístup k disku**. Klikněte na **Otevřít předvolby systému** > **Zabezpečení a soukromí**. Přejděte na záložku **Soukromí** a vyberte možnost **Úplný přístup k disku**. Pro povolení změn klikněte na ikonu zámku. Klikněte na ikonu + a ze seznamu vyberte aplikaci ESET Cyber Security. Zobrazí se výzva k restartování počítače. Klikněte na tlačítko **Později**. Počítač zatím nerestartujte. V oznámení produktu ESET Cyber Security klikněte na tlačítko **Spustit znovu** nebo restartujte počítač. Další informace naleznete v Databázi znalostí.

Po dokončení instalace ESET Cyber Security doporučujeme provést kontrolu počítače na přítomnost škodlivého kódu. Pro spuštění kontroly klikněte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Smart kontrola**. Pro více informací o volitelné kontrole počítače přejděte do kapitoly volitelná kontrola počítače.

Povolení systémových rozšíření

V macOS 11 (Big Sur) bylo rozšíření jádra nahrazeno systémovými rozšířeními. Pro načtení nových systémových rozšíření třetích stran je nutný souhlas uživatele.

Na macOS 11 a novější zobrazí operační systém upozornění, že je blokováno systémové rozšíření, a v hlavním okně produktu ESET Cyber Security se objeví hlášení **Váš počítač není chráněn**. Aby mohl program ESET Cyber Security plně fungovat, musíte ručně povolit načítání rozšíření jádra systému.



Aktualizace z předchozí verze macOS na Big Sur.
Pokud máte nainstalovaný ESET Cyber Security a chcete provést aktualizaci na macOS Big Sur, povolte po aktualizaci ručně rozšíření jádra ESET. Je vyžadován fyzický přístup ke klientskému počítači – při vzdáleném přístupu je tlačítko **Povolit** zakázáno.

Pokud máte nainstalovaný ESET Cyber Security na macOS Big Sur a novějším, povolte ručně systémová rozšíření ESET. Je vyžadován fyzický přístup ke klientskému počítači – při vzdáleném přístupu je tato vypnutá.

Ruční povolení systémových rozšíření

1. Klikněte na **Otevřít předvolby systému** nebo **Otevřít předvolby zabezpečení**.
2. Pro povolení změn klikněte na ikonu zámku vlevo dole.
3. Využijte funkci Touch ID nebo klikněte na **Použít heslo** a zadejte své uživatelské jméno a heslo a poté klikněte na možnost **Odemknout**.
4. Klikněte na tlačítko **Detaily**.
5. Vyberte obě nabídky ESET Cyber Security**.app**.
6. Klikněte na tlačítko **OK**.

Pro podrobný návod si prostudujte článek v Databázi znalostí. (Obsah nemusí být dostupný ve všech jazycích.)

Povolení úplného přístupu k disku

Na macOS 10.14 se v hlavním okně produktu ESET Cyber Security objeví hlášení **Váš počítač není plně chráněn**. Aby mohl program ESET Cyber Security plně fungovat, udělte aplikaci **Úplný přístup k disku**:

1. Klikněte na **Otevřít předvolby systému**.
2. Pro povolení změn klikněte na ikonu zámku vlevo dole.
3. Využijte funkci Touch ID nebo klikněte na **Použít heslo** a zadejte své uživatelské jméno a heslo a poté klikněte na možnost **Odemknout**.
4. Vyberte ze seznamu ESET Cyber Security**.app** .
5. Tím se zobrazí oznámení o restartu ESET Cyber Security. Klikněte na tlačítko **Později**.
6. Vyberte ze seznamu možnost **ESET rezidentní ochrana souborového systému**.



Nedostupná ESET rezidentní ochrana souborového systému
Pokud v seznamu není možnost **Rezidentní ochrana souborového systému** uvedena povolte pro produkt ESET systémová rozšíření.

7. V oznámení produktu ESET Cyber Security klikněte na tlačítko Spustit znovu nebo restartujte počítač. Více si přečtete v databázi znalostí. (Obsah nemusí být dostupný ve všech jazycích.)

Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu. Pro aktivaci ESET Cyber Security klikněte na ikonu na liště menu (v horní části obrazovky) a vyberte možnost **Aktivovat produkt…**.

- **Licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX nebo XXXX-XXXXXXXX, který slouží pro identifikaci vlastníka licence a aktivaci produktu. Pokud jste si zakoupili krabicové balení, produkt aktivujte pomocí licenčního klíče, který naleznete na licenčním štítku uvnitř balení.
- Pokud máte pouze klasické licenční údaje (**uživatelské jméno a heslo**), a nevíte jak ESET Cyber Security aktivovat, klikněte na možnost **Mám uživatelské jméno a heslo, co mám dělat?** Následně budete přesměrováni na portál my.eset.com, na kterém si můžete licenční údaje převést na licenční klíč.
- Pokud si chcete produkt ESET Cyber Security nejprve vyzkoušet, vyberte možnost **Bezplatná zkušební verze**. Následně budete vyzváni k zadání e-mailové adresy. Každý zákazník si může zkušební licenci aktivovat pouze jednou.
- Pokud zatím nemáte žádnou licenci, klikněte na možnost **Zakoupit licenci**. Následně budete přesměrování na webové stránky lokálního distributora ESET.
- **Aktivovat později** – tuto možnost vyberte v případě, pokud nyní nechcete produkt aktivovat.

Odinstalace

Pro odinstalování ESET Cyber Security proveďte jeden z následujících kroků:

- Vložte instalační CD/DVD ESET Cyber Security do počítače, otevřete jej přímo z Plochy nebo okna **Finder** a dvakrát klikněte na ikonu **Odinstalovat**,
- Otevřete instalační soubor ESET Cyber Security (*.dmg*) a dvakrát klikněte na ikonu **Odinstalovat**,
- Spusťte **Finder**, otevřete složku **Aplikace**, stiskněte klávesu CTRL a klikněte na ikonu ESET Cyber Security. Z nabídky vyberte možnost **Zobrazit obsah balíčku**, otevřete složku **Contents** > **Helpers** a dvakrát klikněte na **Uninstaller**.

Základní přehled

Hlavní okno produktu ESET Cyber Security je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

- **Domů** – v přehledné formě poskytuje informace o stavu ochrany počítače, přístupu na web a poštovních klientů
- **Kontrola počítače** – umožňuje nastavit a spustit tzv. Smart nebo volitelnou kontrolu počítače a kontrolu výměnných médií
- **Aktualizace** – zobrazuje informace o aktualizacích detekčních modulů
- **Nastavení** – obsahuje možnosti nastavení ochrany počítače

- **Nástroje** – zajišťují přístup k Protokolům, Plánovači, Karanténě, Běžícím procesům a dalším funkcím programu
- **Nápověda a podpora** – poskytuje přístup k nápovědě, ESET Databázi znalostí a webové stránce společnosti ESET. Dále zde můžete přímo vytvořit dotaz na technickou podporu a v dolní části okna naleznete informace o aktivaci produktu.

Klávesové zkratky

Klávesové zkratky, které můžete používat při práci s programem ESET Cyber Security:

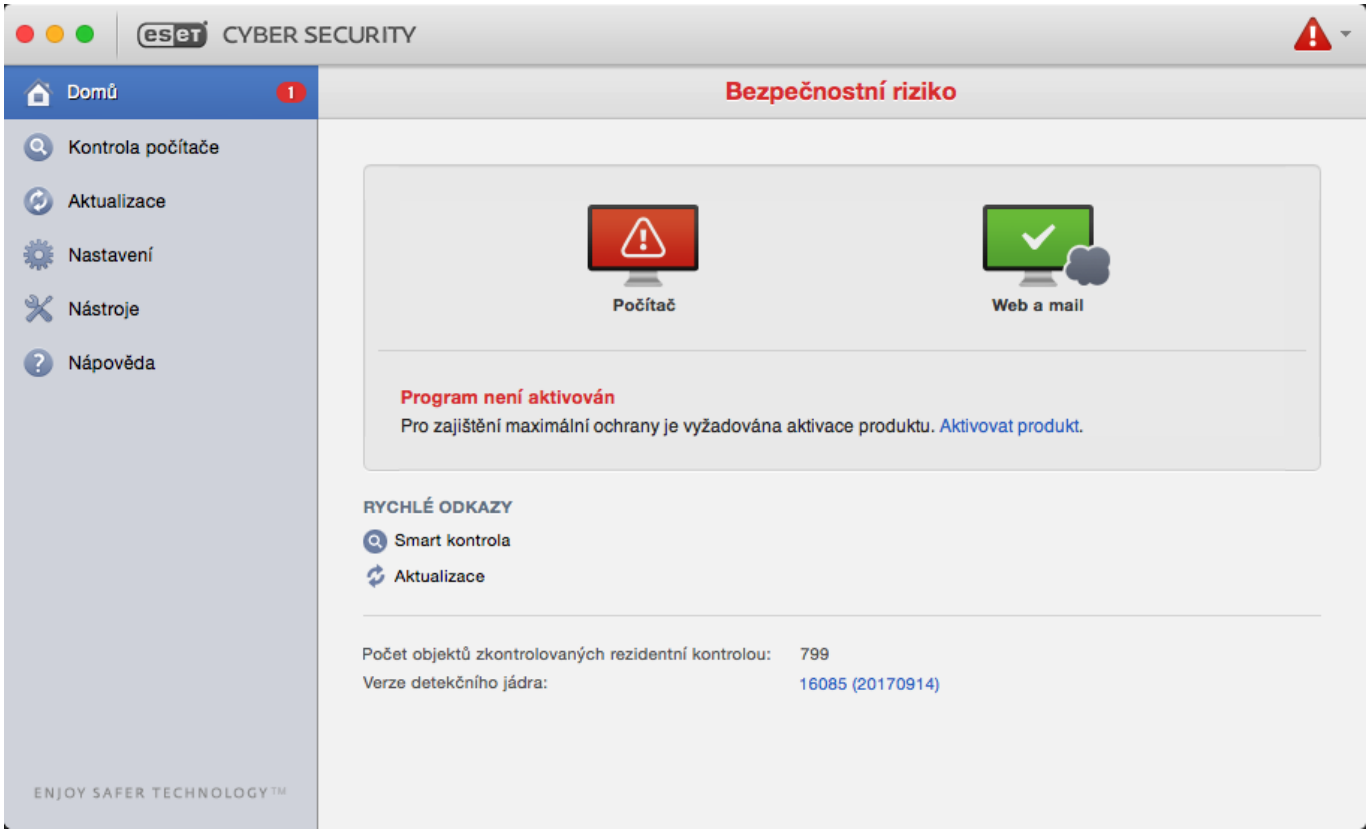
- cmd+, – zobrazí Rozšířená nastavení produktu ESET Cyber Security
- cmd+O – obnoví výchozí pozici a velikost hlavního okna ESET Cyber Security,
- cmd+Q – obnoví výchozí pozici a velikost hlavního okna ESET Cyber Security, Znovu otevřít jej můžete kliknutím na ikonu produktu ESET Cyber Security v menu baru macOS,
- cmd+W – zavře hlavní okno ESET Cyber Security

Následující klávesové zkratky můžete použít pouze v případě, že máte aktivovanou možnost **Použít standardní menu**, jejíž nastavení naleznete po kliknutí v hlavním okně programu v **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo po stisknutí klávesy *cmd+,*) > **Rozhraní**:

- cmd+alt+L – otevře Protokoly
- cmd+alt+S– otevře Plánovač
- cmd+alt+Q – otevře Karanténu

Kontrola stavu systému

Pro zjištění aktuálního stavu programu a ochrany operačního systému přejděte v hlavním menu na záložku **Stav ochrany**. V pravé části ESET Cyber Security se zobrazí stav jednotlivých modulů ochrany.



Co dělat, když program nepracuje správně?

Při plné funkčnosti ochrany má ikona stavu ochrany zelenou barvu. V opačném případě je barva červená nebo žlutá a není zajištěna maximální ochrana. Zároveň jsou na záložce **Domů** zobrazeny bližší informace o stavu jednotlivých modulů a návrh na možné řešení problému pro obnovení maximální ochrany.

Pokud uvedený návrh na řešení problému nezabral, zkuste prohledat ESET Databázi znalostí nebo kontaktujte technickou podporu ESET. Technická podpora Vám odpoví na Vaše otázky ohledně ESET Cyber Security co nejdříve.

Ochrana počítače

Nastavení počítače naleznete na záložce **Nastavení** > **Počítač**. Zobrazuje se zde stav **Rezidentní ochrany souborového systému** a **Blokování výměnných médií**. Pro vypnutí jednotlivého modulu přepněte tlačítko požadovaného modulu do stavu **VYPNUTO**. Pamatujte, že vypnutí některých modulů může snížit úroveň ochrany počítače. Pro přístup k pokročilé konfiguraci klikněte na tlačítko **Nastavit...**.

Antivirová a antispywarová ochrana

Antivirová ochrana chrání systém před útoky a manipulací se soubory, které představují potenciální hrozbu. Při detekci dokáže modul antivirové ochrany škodlivý kód zablokovat, vyléčit případně vymazat nebo umístit do karantény.

Obecné

V rozšířeném nastavení (dostupném po stisknutí kláves cmd + , v hlavním okně programu nebo po kliknutí na **Nastavení** > **Otevřít rozšířená nastavení programu…**) můžete v sekci **Hlavní** nastavit detekci těchto druhů aplikací:

- **Potenciálně nechtěné aplikace** – grayware (neboli PUA – potentially unwanted aplicatione) představují širokou škálu aplikací, které nejsou jednoznačně škodlivé jako viry nebo trojské koně. Mohou však instalovat nechtěný software, měnit chování vašeho zařízení, provádět neočekávané operace, případně akce bez vědomí uživatele. Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- **Potenciálně zneužitelné aplikace** – Existuje řada legitimních programů, které za běžných podmínek zjednodušují například správu počítačových sítí. V nesprávných rukách však mohou být zneužity k nekalým účelům bez vědomí uživatele. Například se jedná o aplikace pro zobrazení vzdálené plochy a standardně je tato možnost vypnuta.
- **Podezřelé aplikace** – Jedná se o aplikace, které jsou komprimovány pomocí packerů nebo protektorů. Ty často zneužívají autoři malware, aby se vyhnuli detekci. Packery jsou runtime samorozbalovací spustitelné soubory, které spojují několik druhů škodlivého kódu do jednoho balíčku. Nejběžnějšími packery jsou UPX, PE_Compact, PKLite a ASPack. Stejný malware může být detekován odlišně, pokud je komprimován pomocí rozdílných metod. Packery navíc dokáží v průběhu času měnit své "podpisy" ve snaze vyhnout se detekci ze strany antivirových programů.

Pro vytvoření výjimky v rezidentní a internetové ochraně klikněte na tlačítko **Nastavit...**.

Výjimky

V sekci **Výjimky** můžete vyloučit konkrétní soubory/složky, aplikace nebo adresy IP/IPv6 ze skenování.

Soubory a složky definované na záložce **Souborový systém** budou vyloučeny z kontroly souborů zaváděných při startu počítače, rezidentní ochrany souborového systému i volitelné kontroly počítače.

- **Cesta** – cesta k souboru nebo složce.
- **Hrozba** – pokud je vedle vyloučeného souboru zobrazen název hrozby, pak to znamená, že daný soubor je vyloučen ze skenování této konkrétní infiltrace. V případě, že je nakažen jiným druhem infiltrace, detekce proběhne.
-  – vytvoří novou výjimku. Při definování cesty k objektu můžete použít zástupné znaky (* a ?), případně konkrétní soubor nebo složku vybrat ze stromové struktury.
-  – odstraní vybranou výjimku.
- **Standardní** – odstraní všechny výjimky.

Na záložce **Web a mail** můžete vyloučit **aplikace** nebo **IP/IPv6 adresy** z filtrování protokolů.

Kontrola po startu

Standardně se provádí během startu počítače a po aktualizaci detekčních modulů kontrola souborů zaváděných při startu počítače do operační paměti. Pro změnu nastavení parametrů skenovacího jádra ThreatSense klikněte na tlačítko **Nastavení...**. Více informací o nastavení ThreatSense naleznete v této kapitole.

Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí. Využívá metody detekce technologie ThreatSense (blíže popsáno v kapitole Nastavení parametrů skenovacího jádra ThreatSense), a může se lišit pro nově vytvořené a již existující soubory. Na vytvořené soubory se může použít hlubší úroveň kontroly.

Ve výchozím nastavení jsou kontrolovány soubory při jejich **otevření**, **vytvoření** nebo **spuštění**. Doporučujeme ponechat standardní nastavení, které poskytuje maximální možnou ochranu vašeho počítače. Standardně se rezidentní ochrana spouští ihned po startu a běží nepřetržitě na pozadí. V některých speciálních případech (například při konfliktu s jiných rezidentním štítem) ji můžete vypnout kliknutím na ikonu produktu ESET Cyber Security umístěnou v menu baru a vybráním možnosti **Vypnout rezidentní ochranu souborového systému**. Rezidentní ochranu také vypnete v hlavním okně na záložce **Nastavení** > **Počítač** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**).

Rezidentní kontrola může kontrolovat tyto typy médií:

- **Lokální disky** – systémové pevné disky;
- **Výměnná média** – CD, DVD, USB, Bluetooth atd.;
- **Síťové jednotky** – namapované síťové jednotky.

Nastavení doporučujeme měnit pouze v ojedinělých případech, například když pozorujete zpomalení při práci s daným typem média.

Konfigurovat nastavení rezidentní ochrany můžete v Rozšířeném nastavení (dostupném po stisknutí kláves *cmd + ,* v hlavním okně programu) v sekci **Rezidentní ochrana** po kliknutí na tlačítko **Nastavit** u možnosti **Rozšířená nastavení** (blíže popsáno v kapitole Rozšířená nastavení kontroly).

Rozšířená nastavení

V tomto okně můžete definovat typy objektů kontrolované skenovacím jádrem ThreatSense. Pro více informací o kontrole **samorozbalovacích archivů**, **runtime archivů** a **rozšířené heuristice** přejděte do kapitoly Nastavení parametrů skenovacího jádra ThreatSense.

Nedoporučujeme měnit hodnoty v sekci **Standardní nastavení archivů**. Změnu byste měli provádět pouze v případě, kdy řešíte konkrétní problém, například zpomalení počítače při kontrole vnořených archivů.

Rozšířenou heuristiku jádra ThreatSense můžete zapnout/vypnout pro kontrolu vytvářených a modifikovaných souborů a samostatně pro kontrolu spouštěných souborů. Změnu provedete pomocí možnosti **Zapnout rozšířenou heuristiku**. Pro snížení dopadu na výkon systému doporučujeme ponechat aktivní **Smart optimalizaci** a také technologii **ESET LiveGrid**.

Zvýšit kompatibilitu se síťovými jednotkami – po aktivování této možnosti zvýšíte rychlost při přístupu k souborům umístěných v síťové jednotce. Doporučujeme ji aktivovat, pokud pozorujete zpomalení při práci se síťovými soubory. Tato funkce využívá systémový file coordinator, který je dostupný od macOS 10.10. Mějte na paměti, že file coordinator nepodporují všechny aplikace. Například Microsoft Word 2011 jej nepodporuje, zatímco Word 2016 ano.

Konfigurace rezidentní ochrany

Rezidentní ochrana patří mezi nejdůležitější součásti, díky kterým ESET Cyber Security pomáhá udržovat počítač zabezpečený. K úpravě parametrů rezidentní ochrany přistupujte vždy s opatrností. Tato nastavení doporučujeme měnit pouze ve speciálních případech, např. v situaci, kdy nastane konflikt mezi produktem ESET a specifickou aplikací.

Po instalaci ESET Cyber Security jsou všechna nastavení optimalizována pro maximální ochranu počítače. Pro obnovení nastavení na standardní hodnoty klikněte na tlačítko **Standardní** v levé části okna **Rezidentní ochrana** (dostupném po kliknutím v hlavním okně na **Nastavení** > **Otevřít rozšířená nastavení programu…** > **Ochrana** > **Rezidentní ochrana**).

Ověření stavu rezidentní ochrany

Pro ověření funkčnosti rezidentní ochrany produktu ESET Cyber Security použijte testovací soubor eicar.com. Tento soubor je speciální neškodný objekt, který detekují všechny antivirové programy. Soubor vyvinula společnost EICAR (European Institute for Computer Antivirus Research) za účelem testování antivirových programů.

Co dělat, když nefunguje rezidentní ochrana?

V této kapitole jsou popsány problémové stavy, které mohou nastat při běhu rezidentní ochrany.

Rezidentní ochrana je vypnutá

Pokud byla rezidentní ochrana nedopatřením vypnuta uživatelem, je potřeba ji znovu aktivovat. Pro opětovné zapnutí rezidentní ochrany přejděte v hlavním menu programu na záložku **Nastavení** > **Počítač** a přepínač u položky **Rezidentní ochrana souborového systému** přepněte do polohy **ZAPNUTO**. Opětovné zapnutí je možné v hlavním okně programu na záložce **Nastavení** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

Ujistěte se, zda nemáte nainstalován další antivirový program. Mezi dvěma rezidentními ochranami může docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

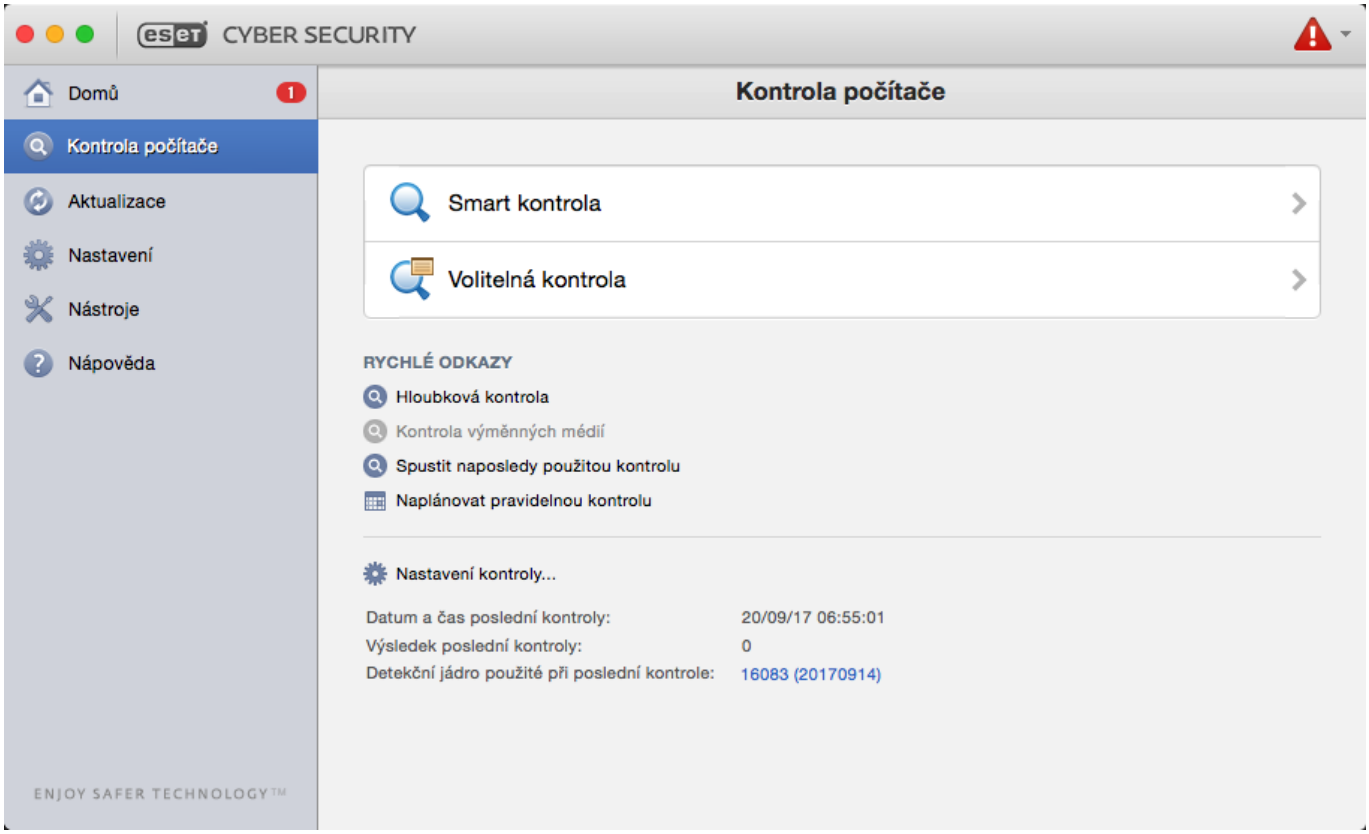
Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

Volitelná kontrola počítače

Pokud máte podezření, že je počítač nakažen (chová se nestandardně), spusťte **Smart kontrolu** pro prověření, zda počítač není infiltrován. Pro zabezpečení maximální ochrany provádějte kontrolu počítače pravidelně, ne jen při podezření na infekci. Pravidelná kontrola může odhalit infekci, která dříve prošla systémem rezidentní ochrany. To se může stát, pokud byla v některém okamžiku činnost rezidentní ochrany vypnuta, nebo detekční moduly nebyly aktuální.

Doporučujeme provádět kontrolu počítače alespoň jednou měsíčně. Pro pravidelnou kontrolu počítače můžete využít naplánované úlohy, jejichž konfiguraci naleznete v sekci **Nástroje** > **Plánovač**.



Typ kontroly

K dispozici jsou dva druhy antivirové kontroly počítače. **Smart kontrola** rychle zkontroluje systém s doporučeným nastavením kontroly. **Volitelná kontrola** umožňuje měnit parametry kontroly a také vybrat vlastní cíle (soubory, složky, média), které budou kontrolovány.

Smart kontrola

Smart kontrola je rychlá kontrola počítače, která léčí infikované soubory bez potřeby zásahu uživatele. Hlavní výhodou tohoto typu kontroly je její snadné použití bez nutnosti podrobného nastavování parametrů kontroly. Smart kontrola zkontroluje všechny soubory a složky a automaticky vyléčí nebo odstraní nalezené hrozby. Úroveň léčení je automaticky nastavena na standardní hodnotu. Pro podrobnější informace týkající se možností léčení si prostudujte kapitolu Léčení.

Volitelná kontrola

Volitelná kontrola je vhodným řešením, pokud chcete upravit všechny parametry kontroly, jako jsou cíle a další nastavení. Výhodou volitelné kontroly je možnost podrobně nastavit její parametry. Různé konfigurace můžete ukládat individuálně jako uživatelské profily kontroly. To je užitečné zejména pokud potřebujete pravidelně opakovat kontrolu se stejnými parametry.

Na záložce **Kontrola počítače** > **Volitelná kontrola** můžete vybrat **Cíle kontroly** ze stromové struktury. Cíle kontroly můžete blíže specifikovat také zadáním cesty ke složce nebo k souborům. Pokud chcete vybrané cíle pouze zkontrolovat bez léčení nebo odstranění nalezených infiltrací, zaškrtněte možnost **Kontrolovat bez léčení**. Celkově si můžete vybrat ze tří úrovní léčení, po kliknutí na tlačítko **Nastavit...** > **Léčení**.



Volitelná kontrola

Volitelnou kontrolu počítače doporučujeme zejména pokročilým uživatelům, kteří již mají předchozí zkušenost s používáním antivirových programů.

Cíle kontroly

Stromová struktura cílů kontroly slouží k výběru souborů a složek, které budou zkontrolovány. Další složky mohou být automaticky vybrány z nastavení definovaném v profilu kontroly.

Cíl kontroly můžete blíže specifikovat také zadáním cesty ke složkám nebo souborům, které chcete zahrnout do kontroly. Cíle kontroly si vyberte ze stromové struktury, která obsahuje všechny složky ve vašem počítači.

Profily kontroly

Požadované nastavení kontroly si můžete uložit do profilu pro pozdější použití. Doporučujeme vytvořit nový profil (s různými cíli kontroly, metodami a dalšími parametry) pro každou pravidelně používanou kontrolu počítače.

Vytvořit nový profil můžete na záložce **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo stiskněte klávesy *cmd+,*) > **Kontrola počítače** kliknutím na tlačítko **Upravit...** vedle vybraného profilu.



Podrobné informace související s vytvořením nového profilu kontroly naleznete v kapitole Nastavení parametrů ThreatSense, kde je popsáno nastavení kontroly.

Příklad: Předpokládejme, že chcete vytvořit vlastní profil kontroly a částečně Vám pro tento účel vyhovuje konfigurace Smart kontroly. Nechcete ale, aby byly kontrolovány runtime archivy a dále potřebujete nastavit přísné léčení. V okně **Seznam profilů kontroly počítače** zadejte název pro váš profil, klikněte na tlačítko **Přidat...** a potvrďte stiskem **OK**. Poté upravte parametry v nastavení **Jádra ThreatSense** a **Cíle kontroly**, tak aby odpovídaly vašim potřebám.

Pokud chcete po dokončení kontroly vypnout počítač, zaškrtněte možnost **Vypnout počítač po dokončení kontroly**.

Nastavení parametrů jádra ThreatSense

ThreatSense je technologie společnosti ESET, kterou tvoří soubor komplexních metod detekce infiltrací. Tato technologie je proaktivní, poskytuje tak ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury atd.), které efektivně kombinuje, a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně a maximalizovat tak svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat také rootkity.

Technologie ThreatSense umožňuje nastavit následující parametry kontroly:

- Typy souborů a přípony, které se mají kontrolovat;
- Kombinace různých detekčních metod;
- Úrovně léčení.

Pro otevření okna s nastavením parametrů klikněte v hlavním okně programu na **Nastavení > Otevřít rozšířená nastavení programu...** (nebo stiskněte klávesy *cmd+,*) a následně klikněte na tlačítko ThreatSense **Nastavit...** a to v sekci **Ochrana po spuštění**, **Rezidentní ochrana** a **Kontrola počítače**, které používají ThreatSense technologii. Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. V rámci technologie ThreatSense můžete konfigurovat následující moduly:

- **Ochrana po spuštění** – kontrola souborů spouštěných po startu
- **Rezidentní ochrana** – ochrana počítače v reálném čase
- **Kontrola počítače** – kontrola složek a souborů
- **Ochrana přístupu na web**
- **Poštovní ochrana**

Parametry ThreatSense jsou speciálně optimalizovány pro každý modul a jejich změna může podstatně ovlivnit práci systému. Příkladem může být změna nastavení tak, aby byla vždy provedena kontrola runtime archivů, nebo zapnutí rozšířené heuristiky pro modul rezidentní ochrany souborů. Takové změny způsobí celkové zpomalení systému. Proto doporučujeme ponechat původní nastavení ThreatSense parametrů. Určitou volnost v konfiguraci ponechává modul **Kontrola počítače**.

Objekty

V sekci **Objekty** můžete definovat typy souborů, které se budou kontrolovat na přítomnost infiltrace.

- **Symbolické odkazy** – (dostupné pouze pro kontrolu počítače) kontrola speciálních typů souborů, které obsahují textovou informaci s cestou k jinému souboru či složce.
- **Soubory e-mailů** – (není dostupné v rezidentní ochraně) kontrola souborů, které obsahují e-mailové zprávy.
- **Poštovní schránky** – (není dostupné v rezidentní ochraně) kontrola uživatelských poštovních účtů. Nesprávné použití může vést ke konfliktu s vaším e-mailovým klientem. Pro více informací o výhodách a nevýhodách si přečtěte tento článek.
- **Archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v archivech (.rar, .zip, .arj, .tar, apod.).

- **Samorozbalovací archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v samorozbalovacích archivech.
- **Runtime archivy** – runtime archivy se na rozdíl od klasických archivů dekomprimují v paměti počítače. Pokud jsou vybrány (typicky UPX, ASPack, yoda, FGS, apod.), jsou rovněž kontrolovány.

Možnosti

V části **Možnosti** můžete vybrat metody, které se použijí při kontrole počítače. Dostupné jsou následující možnosti:

- **Heuristika** – heuristika používá algoritmus pro analýzu (škodlivé) aktivity programů. Hlavní výhodou heuristické detekce je její schopnost identifikovat škodlivý software, který předtím neexistoval.
- **Rozšířená heuristika** – rozšířená heuristika používá jedinečný heuristický algoritmus vyvinutý společností ESET, který dokáže detekovat červy a trojské koně napsané ve vyšších programovacích jazycích. Schopnost detekce je tak značně vyšší právě díky rozšířené heuristice.

Léčení

Nastavení léčení určuje způsob jakým kontrola vyléčí infikované soubory. K dispozici jsou tři úrovně léčení:

- **Neléčit** –- infikované soubory se automaticky nevyléčí. Program zobrazí okno s varováním a možností výběru akce
- **Standardní úroveň léčení** – program se pokusí automaticky vyléčit, nebo vymazat infikovaný soubor. Pokud není možné provést akci automaticky, program nabídne možnost výběru akce
- **Přísné léčení** – program vyléčí, nebo vymaže všechny infikované soubory (včetně archivů). Jedinou výjimku tvoří systémové soubory. Pokud je nelze vyléčit, program zobrazí okno s varováním s možností výběru akce



Soubory archivů

V přednastaveném režimu standardní úrovně léčení je vymazán celý archiv pouze v případě, když jsou všechny soubory v archivu infikované. Jestliže tedy archiv obsahuje i legitimní soubory (nenapadené), nebude vymazán. Pokud je archiv detekován v režimu přísného léčení, bude tento archiv vymazán, pokud obsahuje alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů.



Kontrola archivů

V přednastaveném režimu standardní úrovně léčení je vymazán celý archiv pouze v případě, když jsou všechny soubory v archivu infikované. Jestliže tedy archiv obsahuje i legitimní soubory (nenapadené), nebude vymazán. Pokud je archiv detekován v režimu přísného léčení, bude tento archiv vymazán, pokud obsahuje alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů.

Přípony

Přípona souboru je součástí jeho názvu, ve kterém je oddělena tečkou. Přípona označuje typ a obsah souboru. V této části nastavení parametrů ThreatSense můžete nastavit typy souborů, které budou kontrolovány.

Standardně se kontrolují všechny soubory bez ohledu na příponu. Do seznamu souborů vyloučených z kontroly může být přidána jakákoli přípona. Pomocí tlačítek + a − můžete povolit nebo zakázat kontrolu požadovaných souborů podle jejich přípon.

Vyloučení přípon je někdy nutné, pokud probíhající kontrola narušuje činnost specifického programu, který k daným typům souborů bude přistupovat. V některých případech může být vhodné vyloučit z kontroly soubory s příponou *log*, *cfg* a *tmp*. Níže uvádíme správný formát zápisu (každá přípona je na samostatném řádku):

log

cfg

tmp

Omezení

V sekci **Omezení** nastavíte maximální velikost kontrolovaných objektů a maximální hloubku kontroly v archivech (počet vnořených archivů které budou kontrolovány).

- **Maximální velikost**: určuje největší možnou velikost souborů, které budou zkontrolovány. Modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Nedoporučujeme měnit přednastavenou hodnotu, protože většinou není pro tuto změnu důvod. Doporučujeme, aby tuto hodnotu měnili jen pokročilí uživatelé, kteří potřebují vyloučení větších objektů z kontroly.
- **Maximální čas kontroly**: upravuje maximální čas věnovaný kontrole jednoho objektu. Pokud je zde nastavena hodnota, antivirový modul přestane kontrolovat objekt po uplynutí nastavené doby, bez ohledu na to, zda byla kontrola objektu dokončena či nikoli.
- **Maximální úroveň vnoření**: upravuje maximální hloubku vnoření při kontrole archivů. Pokud nejste zkušený uživatel, nedoporučujeme vám měnit přednastavenou hodnotu 10. Za běžných okolností není důvod toto nastavení měnit. Pokud se kontrola ukončí kvůli překročení počtu úrovní vnoření archivů, celý archiv zůstane nezkontrolován.
- **Maximální velikost souboru**: umožňuje nastavit maximální reálnou velikost souborů v archivech, které budou zkontrolovány. Pokud se kontrola ukončí kvůli tomuto omezení, celý archiv zůstane nezkontrolován.

Ostatní

Používat Smart optimalizaci

Se zapnutou Smart optimalizací se automaticky nastaví nejvýhodnější poměr mezi efektivitou a rychlostí skenování. který spočívá v inteligentním použití různých skenovacích metod pro různé typy souborů v rámci jednotlivých ochranných modulů. Nastavení Smart optimalizace nejsou v produktu definována napevno. Vývojový tým společnosti ESET má možnost dle uvážení měnit moduly prostřednictvím pravidelné automatické aktualizace produktu ESET Cyber Security. Pokud je Smart optimalizace vypnuta, aplikuje se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

Kontrolovat alternativní datové proudy (platí pouze pro kontrolu počítače)

Alternativní datové proudy používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho hrozeb je proto využívá pro zabránění detekce.

Nalezena infiltrace

Infiltrace se do systému mohou dostat mnoha způsoby: z internetových stránek, sdílených složek, pošty, výměnných médií (USB, externí disky, CD, DVD, diskety atd.).

Pokud váš počítač vykazuje znaky napadení škodlivým kódem, např. je pomalejší, často "mrzne" apod., doporučujeme provést následující kroky:

1. Otevřete ESET Cyber Security a klikněte na záložku **Kontrola počítače**.
2. Vyberte **Smart kontrola** (více informací v kapitole Smart kontrola).
3. Po dokončení kontroly, zkontrolujte zobrazený protokol.

Pokud chcete zkontrolovat pouze určitou část disku, vyberte možnost **Volitelná kontrola** a vyberte vlastní cíle kontroly.

Obecným příkladem postupu při řešení problému s infiltrací je situace, kdy rezidentní ochrana souborového systému s nastavenou standardní úrovní léčení najde hrozbu a pokusí se o vyléčení nebo vymazání souboru. Pokud modul rezidentní ochrany nemá nastavenou akci, která se má provést, ESET Cyber Security vás vyzve prostřednictvím okna s upozorněním k výběru akce. Obvykle jsou k dispozici možnosti **Léčit**, **Smazat** a **Ponechat**. Pokud vyberte **Ponechat**, s infikovaným souborem se neprovede žádná akce, což nedoporučujeme. Výjimkou může být situace, kdy máte jistotu, že soubor je neškodný a byl chybně detekován.

Léčení a mazání
Použijte léčení, pokud byl soubor napaden virem, který k němu přidal škodlivý kód. Infikovaný soubor se tak může v některých případech obnovit do původního stavu. Pokud však soubor obsahuje výhradně škodlivý kód, bude vymazán.



Mazání souborů v archivech
Ve výchozím režimu léčení bude celý archiv vymazán pouze tehdy, pokud obsahuje výhradně infikované a žádné "čisté" soubory. Jinými slovy, archivy se nevymazávají, pokud obsahují i neškodné (nenapadené) soubory. Opatrnost je však nutná, pokud spustíte kontrolu s nastavením **Přísné léčení**. V tomto režimu bude archiv obsahující alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů, v archivu smazán.

Kontrola a blokování výměnných médií

ESET Cyber Security nabízí volitelnou kontrolu výměnných paměťových médií po jejich vložení (CD, DVD, USB, aj.) Na macOS 10.15 dokáže ESET Cyber Security kontrolovat také další externí mediální zařízení.

Kontrola výměnných médií na macOS 11 a novějším

ESET Cyber Security nainstalovaný na macOS 11 a novějším kontroluje pouze paměťová zařízení.



Výměnná média mohou obsahovat škodlivý kód a představovat tak riziko pro počítač. Pro blokování výměnných médií klikněte na tlačítko **Nastavit...** na záložce **Nastavení** > **Počítač** > **Blokování výměnných médií** a zaškrtněte možnost **Aktivovat blokování výměnných médií**. Pro povolení konkrétních typů médií odstraňte označení u požadovaného typu média. Do nastavení se také dostanete z dialogového okna kliknutím na **Nastavení blokování médií**, které se zobrazí po vložení média do počítače, viz obrázek výše.

Přístup k CD-ROM

Pro přístup k externím CD-ROM jednotkám připojených pomocí USB kabelu odškrtněte možnost **CD-ROM**.

Anti-Phishing

Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem je získat citlivé údaje, jako například hesla k bankovním účtům, PIN kódy a jiné detaily.

Důrazně doporučujeme tuto ochranu aktivovat v rozšířeném nastavení (dostupném po stisknutí kláves cmd + , v hlavním okně programu) v sekci **Anti-Phishingová ochrana** > vybráním možnosti **Zapnout Anti-Phishingovou ochranu**. Poté zablokuje a zobrazí upozornění při detekování všech potenciálních phishingových útoků pocházejících z podezřelých webových stránek a domén.

Webová a poštovní ochrana

Nastavení webové a mailové ochrany najdete po kliknutí v hlavním okně programu na **Nastavení** > **Web a Mail**. Upravit podrobné nastavení jednotlivých modulů ochrany můžete po kliknutí na tlačítko **Nastavit...**.

- **Ochrana přístupu na web** – monitoruje HTTP komunikaci mezi webových prohlížečem a vzdálenými servery.
- **Ochrana poštovních klientů** – poskytuje kontrolu e-mailové komunikace přijímané pomocí POP3 a IMAP

protokolu.

- **Anti-Phishingová ochrana** – blokuje potenciální útoky přicházející z webových stránek a domén.



Výjimky
ESET Cyber Security nekontroluje komunikaci přenášenou šifrovanými protokoly HTTPS, POP3S a IMAPS.

Webová ochrana

Ochrana přístupu na web monitoruje veškerou komunikaci mezi webovými prohlížeči a vzdálenými servery pomocí protokolu HTTP (Hypertext Transfer Protocol).

Ve výchozím nastavení je kontrolována komunikace na standardních portech. V případě potřeby můžete definovat další porty a případně využít seznamy URL adres.

Porty

Na záložce **Porty** můžete definovat čísla portů používaných pro HTTP komunikaci. Standardně jsou přednastaveny porty 80, 8080 a 3128.

Seznam URL adres

Správa seznamů **URL adres** umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly. Webové stránky zařazené na seznamu blokovaných stránek nebudou dostupné, zatímco stránky vyloučené z kontroly nebudou kontrolovány na přítomnost škodlivého kódu.

Pokud chcete povolit přístup pouze na adresy uvedené v **Seznamu povolených adres**, aktivujte možnost **Povolit přístup pouze na URL adresy zařazené do seznamu povolených adres**.

Pro aktivování daného seznamu aktivujte možnost **Seznam je aktivní**. Pokud chcete zobrazit upozornění při přístupu na webovou stránku umístěnou na seznamu, zaškrtněte možnost **Upozornit při aplikování adresy ze seznamu**.

V seznamech můžete používat speciální znaky *** a *?*, Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám a proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Rovněž je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu.

Poštovní ochrana

Poštovní ochrana zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Při kontrole přijímaných zpráv jsou použity všechny pokročilé metody obsažené ve skenovacím jádře ESET Cyber Security, které jsou součástí ThreatSense. Kontrola POP3 a IMAP protokolu je nezávislá na typu poštovního klienta.

Nastavení skenovacího jádra ThreatSense – pokročilé nastavení kontroly poštovních klientů jako jsou cíle

kontroly, metody detekce atd. Pro zobrazení nastavení klikněte na tlačítko **Nastavit...**.

Přidávat upozornění do poznámky pod čarou – ESET Cyber Security může do kontrolovaných zpráv přidávat podpis s informacemi o výsledku kontroly. Tato informace je užitečná, ale není spolehlivá a nemůže být použita pro finální rozhodnutí o škodlivosti zprávy, jelikož některé zprávy mohou být škodlivým kódem pozměněny, případně se nemusí vložit do problematických zpráv v HTML. Možná nastavení jsou následující:

- Nikdy – informace nebude přidávány do žádných kontrolovaných zpráv,
- Pouze do infikovaných zpráv – informace budou přidávány pouze do infikovaných zpráv,
- **Do všech kontrolovaných zpráv** – informace budou přidávány do všech kontrolovaných zpráv.

Přidávat do předmětu příchozích a čtených infikovaných zpráv – tuto možnost vyberte, pokud chcete do předmětu zpráv přidat informaci o tom, že je škodlivá. Díky tomu se vám snáze budou takové zprávy filtrovat.

Šablona přidávaná do předmětu infikovaných zpráv – v případě potřeby si můžete v tomto poli upravit prefix, který bude přidán do předmětu infikovaných zpráv.

- %avstatus% – přidá informace o stavu infiltrace (příklad: čisté, infikováno, …)
- %virus% – přidá název hrozby
- %aspmstatus% – změní předmět na základě výsledku odchozí antispamové kontroly
- %product% – přidá název ESET produktu, který provedl kontrolu (v tomto případě ESET Cyber Security)
- %product%_url – přidá odkaz na webové stránky společnosti ESET (www.eset.com)

V dolní části tohoto okna se můžete rozhodnout, zda chcete, aby byly kontrolovány zprávy při jejich příjmu prostřednictvím POP3 a IMAP protokolu. Více informací naleznete v následujících kapitolách:

- Kontrola protokolu POP3
- Kontrola protokolu IMAP

Kontrola protokolu POP3

POP3 protokol je nejrozšířenější protokol pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET Cyber Security zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí ověřit, zda je modul zapnutý. Kontrola POP3 protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.

Aktivovat kontrolu protokolu POP3 – zapne kontrolu poštovní komunikace přes POP3 na přítomnost škodlivého kódu.

Kontrola protokolu IMAP

IMAP (Internet Message Access Protocol) je další internetový protokol pro přijímání e-mailových zpráv. IMAP má v porovnání s protokolem POP3 několik výhod. Umožňuje například připojení více klientů na stejný účet a zachovávání informace stavu zprávy, zda zpráva byla či nebyla přečtena, bylo na ni odpovězeno nebo byla vymazána. ESET Cyber Security zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro

správné fungování stačí ověřit, zda je modul zapnutý. Kontrola IMAP protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 143. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.

Aktivovat kontrolu protokolu IMAP – zapne kontrolu poštovní komunikace přes IMAP na přítomnost škodlivého kódu.

Aktualizace

Pravidelná aktualizace ESET Cyber Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program stále aktuální pomocí aktualizace detekčních i programových modulů.

Pro zobrazení informací o stavu aktualizace produktu ESET Cyber Security klikněte v hlavním menu na položku **Aktualizace**. Kromě data a času poslední úspěšné aktualizace můžete aktualizaci vynutit manuálně kliknutím na **Aktualizovat moduly**.

Pokud jsou moduly v pořádku staženy a aktuální, zobrazuje se informace **Aktualizace není potřeba – moduly jsou aktuální.** Pokud nelze program aktualizovat, zkontrolujte Rozšířené nastavení – aktualizace. Nejčastější příčinou selhání stahování aktualizací jsou nesprávně zadaná přihlašovací data (uživatelské jméno a heslo), případně chybně nastavený proxy server.

Na záložce Aktualizace naleznete rovněž číselné označení detekčního jádra, které produkt aktuálně používá. Jedná se zároveň o funkční odkaz vedoucí na webové stránky společnosti ESET s podrobnými informacemi, které aktualizace zahrnuje.

Nastavení aktualizace

Pro odstranění všech dočasně uložených aktualizačních souborů klikněte na tlačítko **Vyčistit**. Vymazat dočasné soubory doporučujeme provést v případě problémů s aktualizací.

Rozšířená nastavení

Pro deaktivaci zobrazování upozornění o provedené aktualizaci modulů aktivujte možnost **Nezobrazovat upozornění o úspěšné aktualizaci**.

Pokud chcete mít přístup k vývojářským aktualizacím, které mohou řešit váš problém, aktivujte si **Testovací aktualizace**. Vyberete-li možnost **Opožděné aktualizace**, aktualizace se budou stahovat z aktualizačního severu, na který jsou aktualizace umisťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

ESET Cyber Security zálohuje detekční a programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshot modulů vytvářely, ponechte možnost **Vytvářet zálohu modulů** zaškrtnutou. **Počet záloh** určuje počet obrazů předchozích modulů uložených na lokálním disku počítače. Pro použití starší verze modulů je třeba vrátit aktualizaci. Nejprve ji zastavte použitím tlačítka **Pozastavit aktualizace na** a vyberte dobu, na jak dlouho. Poté klikněte na tlačítko **Obnovit**, čím se vrátíte k předchozí verzi. Při použití výběru doby **Do odvolání** je třeba stahování aktualizací obnovit ručně kliknutím na tlačítko **Povolit aktualizace.** Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Pomocí možnosti **Nastavit automaticky maximální stáří detekčního jádra** definujete maximální přístupné stáří detekčních modulů. Budou-li starší, zobrazí se informace, že moduly nejsou aktuální. Předdefinovaná doporučená hodnota je sedm dní.

Jak vytvořit aktualizační úlohu

Aktualizaci můžete spustit kdykoliv ručně kliknutím na **Aktualizovat moduly** na záložce **Aktualizace** v hlavním okně ESET Cyber Security.

Aktualizaci můžete také spouštět jako naplánovanou úlohu. Pro vytvoření naplánované úlohy klikněte v hlavním okně programu na záložku **Nástroje** > **Plánovač**. Standardně jsou v ESET Cyber Security již vytvořeny tyto aktualizační úlohy:

- **Pravidelná automatická aktualizace,**
- **Automatická aktualizace po přihlášení uživatele.**

Každá z těchto úloh může být nastavena tak, aby odpovídala vašim potřebám. Kromě úpravy stávajících úloh aktualizace můžete vytvářet i nové úlohy s vlastní konfigurací. Pro bližší popis vytváření a nastavení úloh přejděte do kapitolyPlánovač.

Aktualizace ESET Cyber Security na novou verzi

Pro zaručení maximální ochrany před škodlivým kódem je důležité vždy používat (mít nainstalovanou) nejnovější verzi produktu ESET Cyber Security. Pro ověření dostupnosti nové verze produktu přejděte v hlavním okně programu na záložku **Domů**. Jakmile bude dostupná nová verze, zobrazí se na této záložce upozornění. Kliknutím na **Zjistit více…** si zobrazíte informace o nové verzi programu včetně čísla verze a seznamu změn.

Kliknutím na tlačítko **Ano** zahájíte stahování nejnovější verze, případně aktualizaci odložte na později kliknutím na **Nyní ne**.

Po vybrání možnosti **Ano** se soubor stáhne do složky se staženými soubory, případně jiné složky nastavené v internetovém prohlížeči. Po dokončení stahování soubor spusťte a postupujte podle kroků instalačního průvodce. Vaše licenční údaje (uživatelské jméno a heslo) a nastavení budou automaticky přenesena do nové instalace. Doporučujeme pravidelně kontrolovat aktualizaci zejména v případě, že jste instalovali ESET Cyber Security z CD nebo DVD.

Aktualizace operačního systému

Aktualizace systému macOS představují důležitou součást v ochraně proti škodlivému software. Pro maximální bezpečnost doporučujeme instalovat aktualizace co nejdříve po jejich vydání. ESET Cyber Security vás může upozornit na chybějící aktualizace systému v závislosti na nastavené úrovni. Po kliknutím v hlavním okně na **Nastavení** > **Zobrazit rozšířené nastavení...** (nebo stisknutím kláves *cmd+,*) > **Upozornění a události > Nastavení...** můžete změnit následující **Podmínky upozornění** v sekci **Aktualizace operačního systému**:

- **Zobrazit všechny aktualizace** – budete upozorněni pouze na instalaci všech aktualizací operačního systému
- **Zobrazit pouze doporučené** – budete upozorněni pouze na instalaci důležitých aktualizací operačního systému.

Pokud nechcete být informováni o chybějících aktualizacích systému, odškrtněte možnost **Aktualizace operačního systému**.

Informace o dostupnosti aktualizací operačního systému macOS a souvisejících aplikací jsou poskytovány systémovým nástrojem Aktualizace systému. Aktualizaci můžete spustit přímo ze zobrazeného okna nebo kliknutím na záložku **Domů** v hlavním okně ESET Cyber Security na **Instalovat chybějící aktualizace**.

Okno s upozorněním obsahuje název aplikace, verzi, velikost aktualizace, vlastnosti (vlajky) a další informace o aktualizaci. Sloupec **Vlajky** může obsahovat následující informace:

- **[doporučeno]** – výrobce operačního systému doporučuje nainstalovat tuto aktualizaci pro zvýšení bezpečnosti a stability operačního systému,
- **[restart]** – po dokončení instalace je vyžadován restart,
- **[vypnutí]** – po dokončení instalace bude nutné vypnout a znovu zapnout počítač.

Okno s upozorněním zobrazuje aktualizace získané pomocí nástroje „softwareupdate“. Aktualizace získané pomocí tohoto nástroje se mohou lišit od seznamu aktualizací poskytovaných pomocí aplikace „Aktualizace aplikací“. Pokud chcete nainstalovat aktualizace zobrazené v okně „Chybějící aktualizace systému“ a aplikace „Aktualizace aplikací“ je nezobrazuje, je nutné použít nástroje „softwareupdate“ z příkazového řádku. Pro více informací o nástroji „softwareupdate“ se podívejte do manuálu po zadání man softwareupdate do okna **Terminál**. Toto doporučujeme pouze zkušeným uživatelům.

Nástroje

Záložka **Nástroje** obsahuje nástroje, které pomáhají zjednodušit správu programu a nabízí dodatečné možnosti pro zkušené uživatele.

Protokoly

Protokoly zachycují všechny podstatné události programu a nabízejí přehled detekovaných hrozeb. Záznamy v protokolech představují důležitý nástroj pro systémové analýzy, detekci hrozeb a řešení problémů. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové informace a protokoly si můžete prohlédnout i archivovat přímo v prostředí ESET Cyber Security.

Protokoly jsou dostupné v hlavním menu ESET Cyber Security na záložce **Nástroje** > **Protokoly**. Požadovaný typ protokolu vyberte z rozbalovacího menu **Protokol** v horní části okna. Dostupné jsou následující typy protokolů:

1. **Zachycené infiltrace** – tento protokol je vhodné použít k prohlížení všech událostí týkajících se detekce infiltrací;
2. **Události** – všechny důležité akce, které provede ESET Cyber Security jsou zaznamenány v tomto protokolu. Tento protokol je určen hlavně správcům systémů a uživatelům při řešení různých problémů;
3. **Kontrola počítače** – výsledky každé kontroly počítače se zobrazují v tomto protokolu. Kliknutím na položku v protokolu zobrazíte podrobnosti vybrané kontroly počítače;
4. **Filtrované webové stránky** – tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem ochrana přístupu na web. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.

Jednotlivé události v protokolech můžete kopírovat do schránky vybráním daného protokolu a kliknutím na tlačítko **Kopírovat**.

Údržba protokolů

Nastavení protokolů ESET Cyber Security je dostupné z hlavního okna programu po kliknutí na záložku **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo stiskněte klávesy *cmd+,*) > **Nástroje** > **Protokoly**. Zde můžete nastavit tyto parametry:

- **Automaticky mazat staré záznamy protokolů** – po zaškrtnutí této možnosti se budou automaticky odstraňovat protokoly starší než určený počet dnů (ve výchozím nastavení 90 dní);
- **Automaticky optimalizovat protokoly** – tato možnost zajišťuje defragmentaci databáze protokolů podle nastavení horního limitu množství nevyužitých záznamů v procentech (ve výchozím nastavení 25 %).

Všechny související informace zobrazené v uživatelském rozhraní, zprávy o nalezených hrozbách a událostech můžete ukládat do čitelné podoby jako plain text nebo CSV (hodnoty oddělené čárkou) soubor. Pokud si chcete tyto soubory následně prohlížet v nástrojích třetích stran, vyberte možnost **Zaznamenávat do textových souborů**.

Pro definování cílové složky, do které chcete uložit protokoly, klikněte na tlačítko **Nastavit...** v **Rozšířeném nastavení**.

V závislosti na vybrané možnosti v **Textové protokoly: Upravit** můžete do protokolů ukládat tyto typy informací:

- Události typu *Nesprávné uživatelské jméno a heslo* apod. jsou zapsány do souboru eventslog.txt.
- Hrozby detekované kontrolou po spuštění, rezidentní ochranou nebo kontrolou počítače se zapisují do souboru threatslog.txt.
- Výsledky všech dokončených kontrol jsou uloženy do souboru scanlog.ČÍSLO.txt

Pro konfiguraci filtrů **Standardní záznamy protokolů kontroly počítače** klikněte na tlačítko **Upravit...** a vyberte/zrušte označení u požadovaných typů záznamů. Více podrobností o protokolech naleznete v této kapitole.

Filtrování protokolů

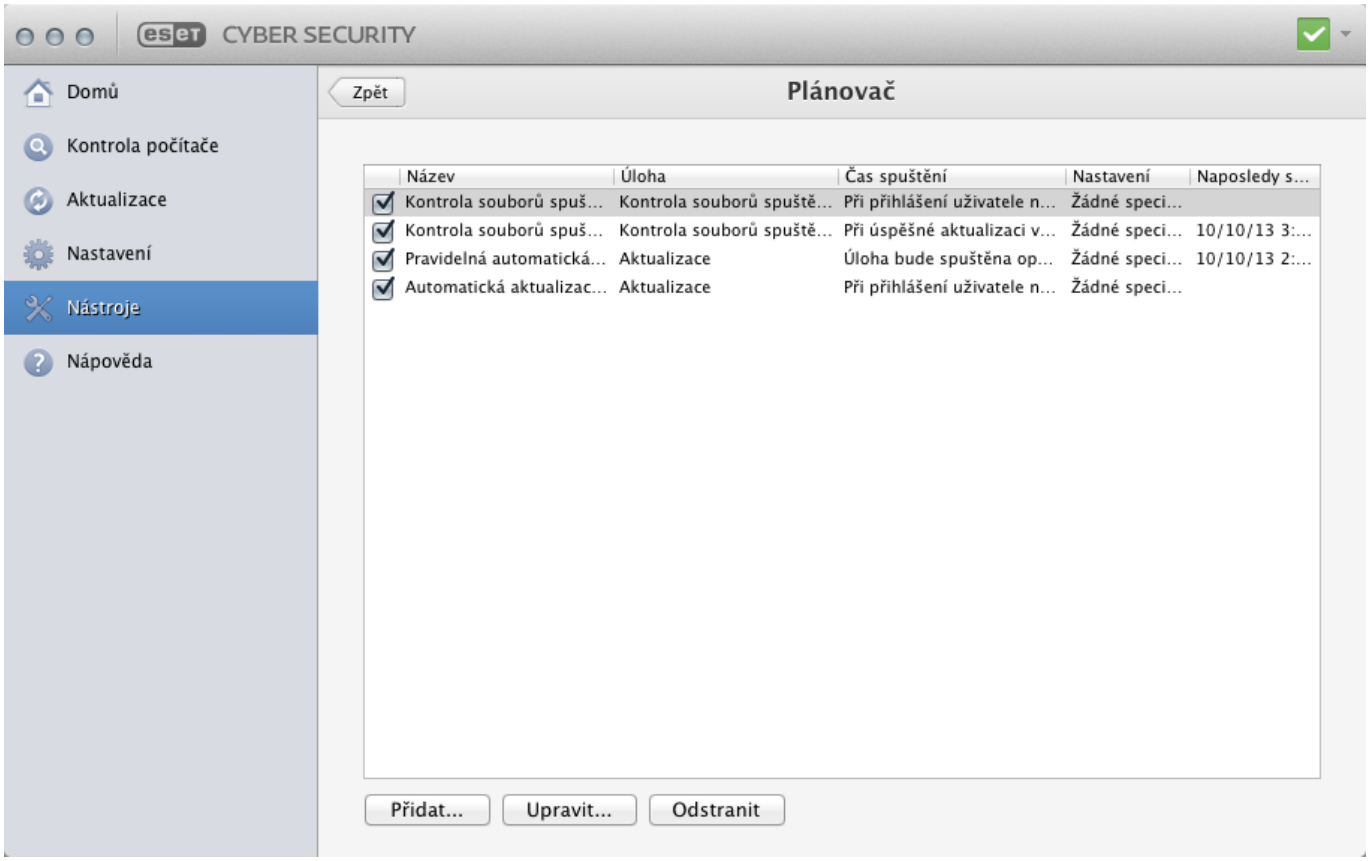
Protokoly obsahují různé druhy záznamů. Použitím filtru můžete zobrazit protokoly pouze zaznamenávající pouze záznamy specifické události.

Vybírat můžete z následujících druhů protokolů:

- **Kritická upozornění** – kritické chyby systému (např. nespuštění antivirové ochrany);
- **Chyby** – chyby typu *"Chyba při stahování souboru aktualizace"* a kritická upozornění;
- **Varování** – varovné zprávy a všechny výše uvedené záznamy;
- **Informační záznamy** – informační zprávy (např. o úspěšné aktualizaci) a všechny výše uvedené záznamy;
- **Diagnostické záznamy** – informace důležité pro ladění programu a všechny výše uvedené záznamy.

Plánovač

Plánovač najdete v hlavním okně ESET Cyber Security na záložce **Nástroje**. Obsahuje seznam všech naplánovaných úloh a vlastnosti konfigurace, jako je přednastavené datum a čas profil kontroly atp.



Plánovač spravuje a spouští naplánované úlohy s nastavenými parametry a vlastnostmi. Parametry úlohy jsou datum, čas nebo jiné podmínky spuštění stejně jako profil kontroly.

Standardně se v plánovači zobrazují tyto naplánované úlohy:

- Údržba protokolů (po aktivování možnosti **Zobrazovat systémové úlohy** v nastavení Plánovače),
- Kontrola souborů spouštěných při startu počítače po přihlášení uživatele,
- Kontrola souborů spouštěných při startu počítače po úspěšné aktualizaci detekčních modulů,
- Pravidelná automatická aktualizace,
- Automatická aktualizace po přihlášení uživatele.

Pro úpravu nastavení již existující naplánované úlohy (předdefinované nebo vytvořené uživatelem) vyberte danou úlohu a klikněte na tlačítko **Upravit...**. Případně stiskněte klávesu CTRL, klikněte na úlohu a vyberte možnost **Upravit...**.

Vytvoření nové úlohy

Pokud chcete vytvořit novou úlohu v Plánovači, klikněte na tlačítko **Přidat...** nebo klikněte pravým tlačítkem kamkoli do seznamu úloh a z kontextového menu vyberete **Přidat...**. Vytvořit můžete pět typů naplánovaných

úloh:

- **Spuštění aplikace**
- **Aktualizace**
- **Údržba protokolů**
- **Volitelná kontrola počítače**
- **Kontrola souborů spouštěných po startu**

Spuštění aplikace

Po vybrání možnosti **Spuštění aplikace** můžete spouštět programy jako systémový uživatel "nobody." Oprávnění pro běh aplikací spouštěným pomocí plánovače je definováno v systému macOS. Pro změnu uživatele zadejte na začátek cesty k aplikaci jméno uživatele oddělené dvojtečkou (:). Pomocí této možnosti můžete spustit aplikaci pod uživatelem **root**.

Příklad: Spuštění úlohy jako uživatel

V tomto příkladu si ukážeme, jak spustit pod uživatelem **UserOne** v definovaný čas kalkulačku:

1. V **plánovači** klikněte na tlačítko **Přidat úlohu**.
2. Zadejte název úlohy. Jako **typ úlohy** vyberte možnost **Spustit aplikaci**. V sekci **Spuštění úlohy** vyberte možnost **Jednou** pro jednorázové spuštění úlohy. Pokračujte kliknutím na tlačítko **Další**.
3. Klikněte na tlačítko Procházet a vyberte aplikaci Kalkulačka.
4. Na začátek cesty zadejte **UserOne:** (UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator') a pokračujte kliknutím na tlačítko **Další**.
5. Vyberte čas, kdy chcete úlohu spustit, a pokračujte kliknutím na tlačítko **Další**.
6. Rozhodněte se, co se stane, pokud se úlohu nepodaří v daném čase spustit, a klikněte na tlačítko **Další**.
7. Klikněte na tlačítko **Dokončit**.
8. Plánovač v produktu ESET spustí v definovaný čas kalkulačku.

Příklad: Aktualizační úloha

V tomto příkladu si ukážeme, jak vytvořit aktualizační úlohu, který se spustí v konkrétní čas.

1. Z rozbalovacího menu **Naplánovaná úloha** vyberte možnost **Aktualizace**.
2. Do pole **Název úlohy** zadejte její název.
3. V rozbalovacím menu **Spustit úlohu** vyberte frekvenci úlohy. V závislosti na vybrané frekvenci budete vyzváni k uvedení konkrétních parametrů aktualizace. Pokud vyberete možnost **Definované uživatelem**, v dalším kroku bude nutné nastavit datum a čas ve formátu cron (pro více informací se podívejte se do kapitoly Vytvoření uživatelské úlohy).
4. V dalším kroku nastavte, jaká akce se provede v případě, že úlohu nebylo možné provést v naplánovaném čase.
5. V dalším kroku se zobrazí souhrnné informace o přidávané naplánované úloze. Po kliknutí na tlačítko **Dokončit** se nově vytvořená úloha přidá do seznamu naplánovaných úloh.

ESET Cyber Security obsahuje předdefinované naplánované úlohy, které jsou nezbytné pro správné fungování produktu. Tyto úlohy byste neměli modifikovat, a proto jsou ve výchozím nastavení skryté. Pro zobrazení těchto úloh klikněte v hlavním okně programu na záložku **Nastavení** > **Otevřít rozšířená nastavení programu…** (nebo stiskněte klávesy *cmd+,*). Následně klikněte na **Nástroje > Plánovač** a zaškrtněte možnost **Zobrazovat systémové úlohy**.

Kontrola jako vlastník složky

Kontrolu složek můžete spustit pod uživatelem, který je její vlastník:

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

Jako aktuálně přihlášený uživatel můžete kontrolovat `/tmp` složku:

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

Vytvoření uživatelské úlohy

Při tvorbě **uživatelem definované úlohy** zadávejte datum a čas v rozšířeném cron formátu (řetězec obsahující šest polí oddělených mezerou):

```
minuta(0-59) hodina(0-23) den v měsíci(1-31) měsíc(1-12) rok(1970-2099) den v
týdnu(0-7)(neděle = 0 nebo 7)
```

Příklad:

```
30 6 22 3 2012 4
```

Speciální znaky podporované v cron formátu:

- hvězdička (`*`) – nahrazuje všechny hodnoty v poli, např. hvězdička ve třetím poli (den v měsíci) znamená každý den
- spojovník (`-`) – definuje rozsah; např. `3-9`
- čárka (`,`) – odděluje položky v seznamu; např. `1,3,7,8`
- lomítko (`/`) – definuje přírůstky v rozsahu; např. `3-28/5` ve třetím poli (den v měsíci) znamená třetí den v měsíci a pak každých 5 dní.

Názvy dnů (Monday-Sunday) a měsíců (January-December) nejsou podporovány.



Spouštění příkazů

Pokud definujete den v měsíci i den v týdnu, úloha se provede pouze v případě, že se obě hodnoty shodují.

Karanténa

Hlavní funkcí karantény je bezpečně uschovat infikované soubory. Soubory jsou uloženy do karantény v případě, že nemohou být léčeny, pokud není bezpečné a doporučené jejich odstranění (systémové soubory) nebo pokud je ESET Cyber Security detekoval nesprávně (tzv. falešný poplach).

Do karantény můžete také ručně přidat libovolný soubor. Tento postup je vhodný, pokud soubor vykazuje podezřelou aktivitu, ale není detekován rezidentní ochranou. Soubory v karanténě můžete následně odeslat na analýzu do virové laboratoře ESET.

Soubory uložené v karanténě můžete zobrazit v přehledné tabulce, která obsahuje datum a čas přidání souboru do karantény, cestu k původnímu umístění souboru, velikost souboru v bajtech, důvod přidání (např. přidaný uživatelem) a počet infiltrací (např. pokud se jedná o archiv obsahující více infikovaných souborů). Karanténa s uloženými soubory () zůstává na disku i po odinstalaci ESET Cyber Security. Soubory jsou v karanténě uloženy v bezpečném šifrovaném formátu a můžete je obnovit například v případě nesprávné detekce.

Vložení do karantény

ESET Cyber Security automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nevypnuli v okně s upozorněním). V případě potřeby můžete kliknutím na tlačítko **Přesunout...** do karantény přesunout libovolný podezřelý soubor. K tomuto účelu můžete použít také kontextové menu karantény. Podržte klávesu CTRL, klikněte pravým tlačítkem na soubour, který chcete přesunout do karantény, v záložce **Služby** vyberte možnost **Přidat soubory do karantény**.

Obnovení z karantény

Soubory z karantény můžete obnovit do svého původního umístění kliknutím na tlačítko **Obnovit**. Obnovení souboru můžete provést v okně karantény kliknutím pravým tlačítkem myši na daný soubor (při stisknuté klávese CTRL) a vybráním možnosti **Obnovit**. Kontextové menu karantény nabízí také možnosti **Obnovit do...**, pomocí které můžete soubor obnovit do jiného než původního umístění.

Odesílání souborů

Pokud jste do karantény umístili podezřelý soubor, který nebyl detekován, nebo pokud byl soubor naopak nesprávně označen jako infikovaný a následně umístěn do karantény, pošlete ho prosím do virové laboratoře společnosti ESET. Stiskněte klávesu CTRL, klikněte pravým tlačítkem na soubor v karanténě a z kontextového menu vyberte možnost **Odeslat soubor k analýze**.

Spuštěné procesy

Nástroj **Spuštěné procesy**, který je součástí produktu ESET Cyber Security, zobrazuje běžící procesy ve vašem počítači a poskytuje podrobné informace o běžících procesech díky technologii ESET LiveGrid.

- **Proces** – jméno běžícího procesu. Pro zobrazení všech běžících procesů v počítači můžete také použít nástroj Sledování aktivity, který najdete v systému macOS (*/Aplikace/Utility*).

- **Úroveň rizika** – ve většině případů určí ESET Cyber Security na základě technologie ESET LiveGrid® úroveň rizika jednotlivých objektů (souborů, procesů apod.). Úroveň rizika je vyhodnocena použitím několika heuristických metod, které zjistí charakteristiku každého objektu a váhu možné nebezpečné aktivity. Na základě těchto metod je objektu přiřazena úroveň rizika. Známé aplikace vyhodnocené jako čisté jsou označeny zeleně a jsou dále automaticky vyjmuty z kontroly počítače. Díky tomu dochází ke zrychlení rezidentní i uživatelsky spuštěné kontroly. Pokud je aplikace označena jako neznámá (žlutá), nemusí jít ještě o škodlivou aplikaci. Obvykle se jedná o novou verzi aplikace. V případě, že nedokážete sami rozhodnout, zda je aplikace škodlivá, můžete ji odeslat na analýzu do virové laboratoře ESET. Pokud bude aplikace označena jako škodlivý kód, bude její detekce přidána do jedné z dalších aktualizací detekčního jádra.
- **Počet uživatelů** – množství uživatelů používající tuto aplikaci. Tato informace je poskytována technologií ESET LiveGrid®.
- **Datum nalezení** – doba, kdy byla aplikace poprvé zaznamenána technologií ESET LiveGrid®.
- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu.

Pokud kliknete na některý proces, v dolní části okna se zobrazí následující informace:

- **Soubor** – umístění souboru v počítači,
- **Velikost souboru** – fyzická velikost souboru na disku,
- **Popis souboru** – popis souboru v operačním systému,
- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu,
- **Verze souboru** – informace o verzi souboru od poskytovatele aplikace,
- **Název produktu** – jméno aplikace nebo její obchodní jméno.

Síťová spojení

V tomto dialogovém okně naleznete seznam síťových spojení, které probíhá na vašem počítači. ESET Cyber Security vám o každém spojení poskytuje detailní informace a umožňuje přímo z toho okna vytvořit blokovací pravidlo pro spojení.

Vytvořit blokovací pravidlo pro toto spojení

Pro vytvoření blokovacího pravidla klikněte pravým tlačítkem myši na spojení a z kontextového menu vyberte možnost **Vytvořit blokovací pravidlo** pro toto spojení. Následně vás ESET Cyber Security provede **vytvořením blokovacího pravidla**, kdy:

1. Vyberte **Profil**, ve kterém má být pravidlo platné a zadejte jeho název. Dále se rozhodněte, zda být platné pouze pro konkrétní aplikaci nebo všechny aplikace.
2. Vyberte akci – vytváříte-li blokovací pravidlo, ponechte možnost blokovat. Dále vyberte směr, pro který se pravidlo aplikuje. V případě potřeby můžete vybráním možnosti **Zaznamenat do protokolu** aktivovat zápis informace o aplikování pravidla do protokolu.
3. Vyberte komunikační protokol a port. Vybrat si můžete z předdefinovaných služeb nebo zadat rozsah portů.
4. Definujte cíl a vyplňte další vyžadovaná pole (v závislosti na výběru).

ESET LiveGrid®

Systém včasného varování ESET LiveGrid® zajišťuje okamžité informování společnosti ESET v případě výskytu nových hrozeb. Obousměrný systém včasného varování ESET LiveGrid® má jediný účel – zlepšení ochrany, kterou vám můžeme poskytnout. Nejlepší způsob, jak zajistit, abychom věděli o nových hrozbách ihned po jejich vypuštění na internet, je spojením s našimi uživateli. Vyberte si jednu z následujících možností:

1. Můžete se rozhodnout, že nechcete zapínat systém včasného varování ESET LiveGrid. Nepřijdete o žádnou funkcionalitu programu a ochrana vašeho počítače bude na vysoké úrovni. V některých případech může produkt reagovat na nové hrozby se zpožděním – dokud nedojde k aktualizaci detekčního jádra.
2. Můžete systém včasného varování ESET LiveGrid nakonfigurovat pro odesílání anonymních informací o nových hrozbách společně s informací, kde byl soubor detekován. Tyto informace mohou být odeslány do virových laboratoři ESET k bližší analýze. Jejich analýza nám pomůže vylepšovat detekční schopnosti programu a aktualizovat detekční moduly.

ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace mohou obsahovat vzorek nebo kopii souboru, ve kterém byla zjištěna hrozba, cestu k tomuto souboru, jeho název, datum a čas, jméno procesu, který k souboru přistoupil, a informace o vašem operačním systému.

I když je pravděpodobnost, že mohou být příležitostně odhaleny informace o vás nebo vašem počítači (uživatelská jména v adresářích apod.), v ESET Threat Lab nebude ŽÁDNÁ získaná informace použita za jiným účelem, než k pomoci okamžitě reagovat na nové hrozby.

Pro konfiguraci technologie LiveGrid klikněte v hlavním okně programu na záložku **Nastavení** > **Otevřít rozšířená nastavení programu…** (nebo stiskněte klávesy *cmd+,*) > **Nástroje** > **ESET LiveGrid®**. Vyberte možnost **Aktivovat systém včasného varování** a klikněte na tlačítko **Nastavit...**.

Nastavení Live Grid

Standardně ESET Cyber Security odesílá podezřelé soubory do virové laboratoře ESET pro detailní analýzu. Pokud si nepřejete soubory posílat, odškrtněte možnost **Odeslat podezřelé soubory**.

Pokud naleznete podezřelý soubor, můžete jej okamžitě odeslat na analýzu do virové laboratoře ESET kliknutím v hlavním okně programu na **Nástroje** > **Odeslat soubor k analýze**. V případě, že se jedná o škodlivou aplikaci, její detekce bude přidána v další aktualizaci detekčního jádra.

Odesílat anonymní statistické informace – ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace obsahují jméno hrozby, datum a čas detekce, verzi produktu ESET, verzi operačního systému a vaši aktuální pozici. Statistické informace se většinou do laboratoře ESET odesílají dvakrát za den.

Vyloučit tyto soubory – pomocí této možnosti můžete vyloučit vybrané typy souborů, které nechcete odesílat do virové laboratoře ESET. Například dokumenty a tabulky obsahující důvěryhodné informace. Standardně jsou vyloučeny soubory s příponou .doc, .rtf a další. Do seznamu výjimek můžete přidat vlastní typy souborů.

Kontaktní e-mail (nepovinný údaj) – na zadané e-mailové adrese vás mohou kontaktovat specialisté z virové laboratoře ESET za účelem získání dalších informací. Pokud nejsou vyžadovány další informace, standardně nebudete kontaktováni.

Odeslat soubor k analýze

V případě, že jste detekovali na svém zařízení soubor s podezřelým chováním, můžete jej odeslat na analýzu do virové laboratoře ESET.



Před odesláním vzorku do společnosti ESET

Vzorky zasílejte pouze v případě, kdy splňuje jedno z následujících kritérií:

- Soubor není produktem ESET detekován
- Vzorek je detekován nesprávně jako hrozba
- Mějte na paměti, že osobní soubory nepřijímáme jako vzorky (neprovádíme jejich kontrolu za uživatele)
- Nezapomeňte vyplnit předmět a přiložte maximální možné množství informací o daném vzorku (jak jste se k němu dostali, odkud jste obdrželi odkaz, screenshot apod.)

Vzorek k analýze zašlete pomocí formuláře v produktu, který naleznete po kliknutí na **Nástroje** > **Odeslat soubor k analýze**.

Ve formuláři **Odeslat soubor k analýze** vyplňte následující:

Soubor – cesta k souboru nebo URL adresa.

Komentář – popište důvod zaslání souboru.

Kontaktní e-mail – na uvedené adrese vás budou kontaktovat pracovníci virové laboratoře ESET, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné.



Pravděpodobně neobdržíte žádnou zpětnou vazbu

Na zadanou e-mailovou adresu vás budou pracovníci virové laboratoře ESET kontaktovat pouze v případě, kdy budou potřebovat více informací. Denně do společnosti ESET chodí několik desítek tisíc souborů, a není možné na každý e-mail reagovat.
Pokud se ukáže, že se jedná o nebezpečnou aplikaci nebo webovou stránku, její detekce bude přidána v některé z nejbližších aktualizací.

Uživatelské rozhraní

Prostřednictvím možností pro konfiguraci uživatelského rozhraní si můžete přizpůsobit pracovního prostředí programu vašim potřebám. Pro jejich zobrazení klikněte v hlavním menu na **Nastavení** > **Otevřít rozšířená nastavení programu…** (případně stiskněte klávesy *cmd+,* v hlavním okně programu) v sekci **Uživatel** > **Rozhraní**.

- Pro zobrazování úvodního obrázku produktu ESET Cyber Security při spuštění systému zaškrtněte možnost **Zobrazit úvodní obrázek při startu**.
- Po vybrání možnosti **Ponechat aplikaci v Docku** se ikona ESET Cyber Security® zobrazí v docku macOS a pro přepínání mezi ESET Cyber Security a ostatními běžícími aplikacemi bude možné použít klávesy *cmd+tab*. Změna nastavení ESET Cyber Security se projeví po restartu počítače.
- Pomocí možnosti **Použít standardní menu** aktivujete používání klávesových zkratek (viz kapitolu Klávesové zkratky). Dále se v menu baru macOS zobrazí standardní nabídky aplikace (Uživatelské rozhraní, Nastavení a Nástroje).

• Pokud chcete povolit zobrazování nápovědy pro některá tlačítka ESET Cyber Security, zaškrtnete možnost **Zobrazovat nápovědu tlačítek**.

• Pro zobrazení a možnost výběru skrytých souborů ke kontrole v části **Cíle kontroly** na záložce **Kontrola počítače** zaškrtněte možnost **Zobrazovat skryté soubory**.

• Standardně se ikona ESET Cyber Security zobrazuje v menu baru v pravém horním rohu obrazovky. Pokud nechcete tuto ikonu zobrazovat, deaktivujte možnost **Zobrazit ikonu v rozšířeném menu baru**. Změna tohoto nastavení se projeví po restartování produktu ESET Cyber Security (případně počítače).

Upozornění a události

Nabídka **Upozornění a události** v sekci **Uživatel** nabízí možnosti pro úpravu zobrazování upozornění týkajících se hrozeb a systémových zprávy v ESET Cyber Security.

Vypnutím možnosti **Zobrazovat výstražná upozornění** se přestanou zobrazovat všechna okna s upozorněními, a proto je vhodné tuto možnost vypnout pouze v určitých situacích. Většině uživatelů doporučujeme ponechat tuto možnost zapnutou. Pokročilé možnosti máme popsané v této kapitole.

Zaškrtnutím možnosti **Zobrazovat upozornění na pracovní ploše** zapnete zobrazování oken s upozorněními, které nepotřebují interakci uživatele (standardně se zobrazují v pravém horním rohu obrazovky). Pokud chcete nastavit dobu zobrazení tohoto upozornění upravte hodnotu v poli **Upozornění zavřít automaticky po X sekundách** (výchozí hodnota je 5 sekund). Pokud chcete při běhu aplikací v režimu celé obrazovky zobrazovat pouze upozornění vyžadující odezvu uživatele, zaškrtněte položku **Povolit režim celé obrazovky**. Tato možnost je vhodná během prezentací, při hraní her nebo při jiných činnostech s aplikacemi, které běží v režimu celé obrazovky.

Od verze ESET Cyber Security 6.2 můžete potlačit zobrazování konkrétních **stavů ochrany** v hlavním okně programu. Více informací naleznete v kapitole stavy ochrany.

Zobrazení upozornění

ESET Cyber Security zobrazuje dialogová okna s informacemi o nových aktualizacích programových komponent, aktualizacích operačního systému a také při vypnutí určitých částí programu, vymazání protokolů apod. Potlačit zobrazování každého upozornění můžete kliknutím na **Příště nezobrazovat**.

Seznam dialogových oken, které zobrazuje ESET Cyber Security naleznete po kliknutí v hlavním okně na **Nastavení** > **Otevřít rozšířená nastavení programu…** > **Upozornění a události** > **Rozšířená nastavení: Nastavit…**. Pro zapnutí či potlačení každého oznámení použijte zaškrtávací pole vedle **jména dialogového okna**. Dále můžete definovat **Podmínky zobrazení** a ovlivnit, způsob zobrazení oznámení o nových verzích programu a dostupnosti aktualizací operačního systému.

Stavy ochrany

Informace o stavu ochrany produktu ESET Cyber Security se zobrazují v hlavním okně na záložce Stav ochrany. V případě potřeby můžete zobrazování konkrétních stavů ochrany potlačit. Pro jejich zapnutí nebo vypnutí klikněte v hlavním okně programu na **Nastavení** > **Otevřít rozšířená nastavení programu…** > **Upozornění a události**. Následně klikněte na tlačítko **Nastavit** u položky **Zobrazit v hlavním okně na záložce Stav ochrany**.

Můžete skrýt stav následujících funkcí programu:

- Anti-Phishing
- Ochrana přístupu na web
- Ochrana poštovních klientů
- Aktualizace operačního systému
- Platnost licence
- Vyžadován restart systému

Oprávnění

Správné nastavení ESET Cyber Security může být velmi důležité pro podnikovou bezpečnost. Neoprávněné změny mohou ohrozit stabilitu a stav ochrany systému. Můžete tedy nastavit, kteří uživatelé budou mít oprávnění měnit nastavení programu.

Pro definování oprávněných uživatelů přejděte do **Nastavení> Otevřít rozšířená nastavení programu…** (nebo stiskněte *cmd+,*) > **Oprávnění**. Vyberte ze seznamu uživatele nebo skupinu a klikněte na tlačítko **Přidat**. Všechny systémové účty zobrazíte po zaškrtnutí možnosti **Zobrazit všechny uživatele**. Pro odebrání uživatele ze seznamu oprávněných uživatelů jej vyberte a klikněte na tlačítko **Odebrat.**



Informace k aktualizaci
Pokud ponecháte seznam oprávněných uživatelů prázdný, všichni uživatelé budou automaticky považováni za oprávněné ke změně nastavení programu.

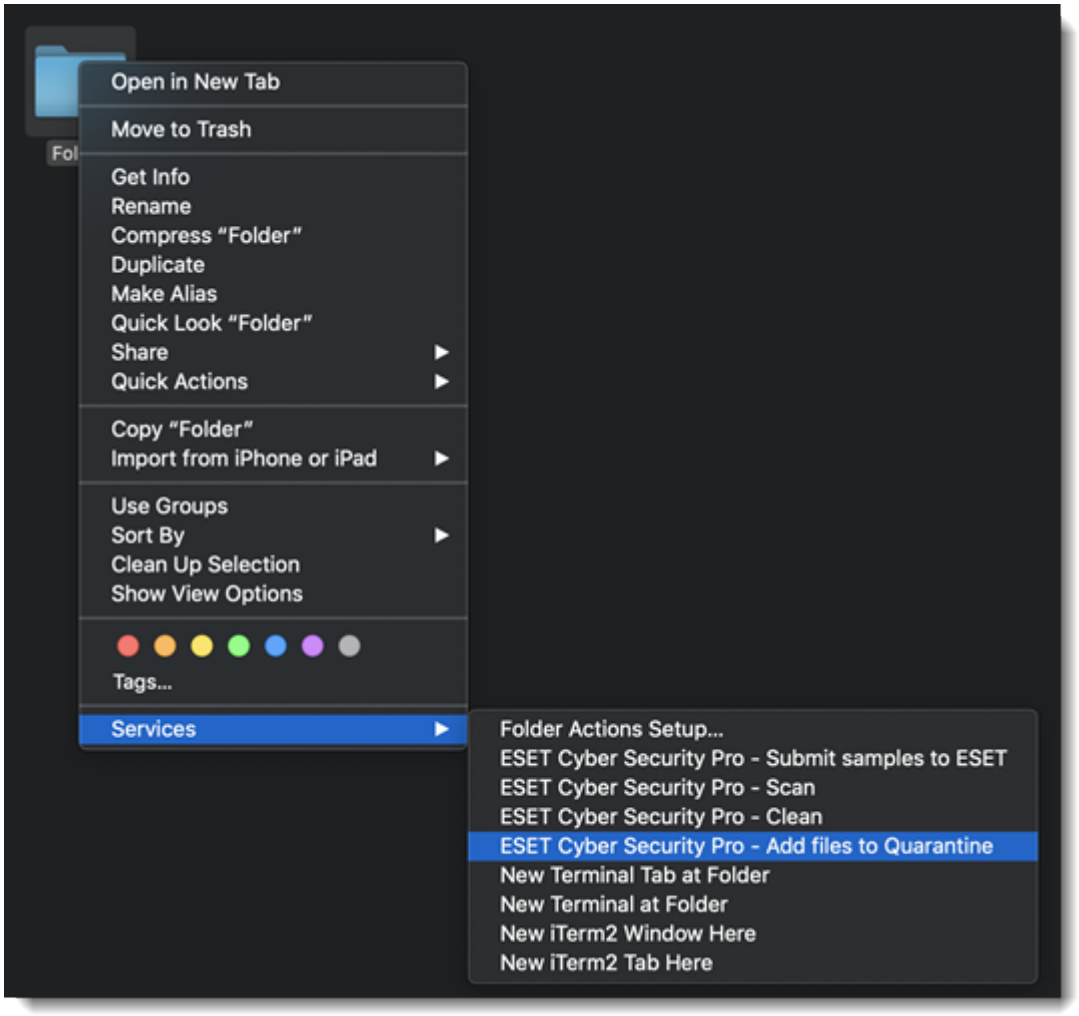
Kontextové menu

Integraci kontextového menu do systému můžete zapnout po kliknutím na **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo stiskněte *cmd+,*), kdy v sekci **Uživatel** > **Kontextové menu** vyberte možnost **Integrovat do kontextové nabídky**. Pro provedení změn je nutné provést odhlášení uživatele nebo restartovat počítač. Možnosti kontextového menu se zobrazí, když v okně **Finder** stisknete klávesu CTRL a myší kliknete na jakýkoli soubor.

Můžete se rozhodnout, které možnosti chcete v kontextovém menu zobrazit. Vybráním možnosti **Pouze kontrolovat** budete schopni zkontrolovat daný soubor. Pomocí možnosti **Pouze léčit** se v kontextovém menu zobrazí možnost pro vyléčení souboru. Tato možnost je platná pouze pro soubory, které byly napadeny virem, který k nim přidal škodlivý kód. Infikovaný soubor se tak může v některých případech obnovit do původního stavu. Pokud však soubor obsahuje výhradně škodlivý kód, bude vymazán.

Pokud vyberete možnost **Vše**, v kontextovém menu budou k dispozici následující možnosti:

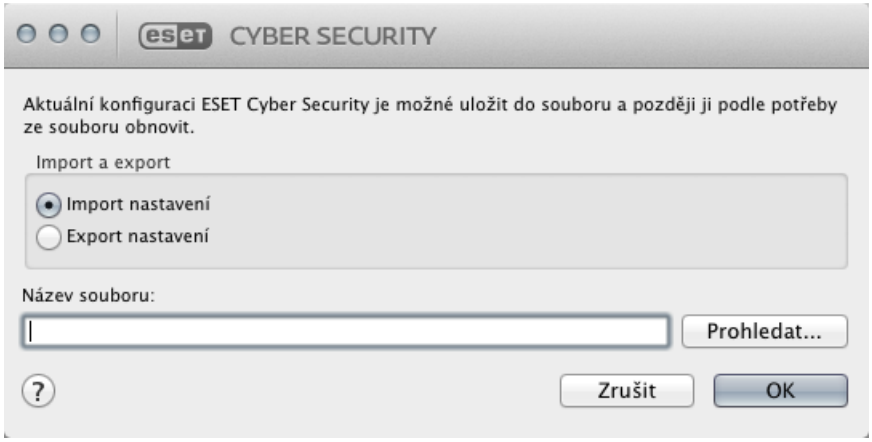
- Odeslat soubor k analýze
- Kontrolovat
- Léčit
- Přidat soubory do karantény



Import a export nastavení

Pro importování nebo exportování konfigurace ESET Cyber Security přejděte v hlavním okně na záložku **Nastavení** a klikněte na možnost **Import a export nastavení**.

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET Cyber Security a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích, kdy stačí pouze naimportovat daný .xml soubor.



Pro importování nastavení vyberte možnost **Import**, klikněte na tlačítko **Procházet...** vyberte soubor, který chcete importovat. Pro exportování nastavení vyberte možnost **Export**, zadejte název souboru a vyberte umístění pro

uložení souboru.

Nastavení proxy serveru

Nastavení proxy serveru provedete klikem na **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo stiskem kláves *cmd+,*) > v sekci **Různé** vyberte **Proxy Server**. Zde můžete určit globální nastavení proxy serveru. Parametry se použijí pro jakýkoliv modul ESET Cyber Security, který požádá o připojení k internetu. ESET Cyber Security podporuje Basic Access a NTLM (NT LAN Manager) způsoby autentifikace.

Po zaškrtnutí možnosti **Použít proxy server** vyplňte do pole **Proxy server** adresu a port proxy serveru (standardně 3128). Případně můžete kliknout na tlačítko **Vyhledat** a pokud máte v systému proxy nastavenou, údaje by se měly automaticky vyplnit.

Pokud proxy server vyžaduje autentifikaci, zadejte do odpovídajících polí **Uživatelské jméno** a **Heslo**.

Licenční ujednání s koncovým uživatelem

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem (dále jen „Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 (dále jen "ESET" nebo "Poskytovatel") a Vámi, fyzickou anebo právnickou osobou (dále jen "Vy" anebo "Koncový uživatel") Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko "Přijímám" "Přijímám..." nebo při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy. V případě, že s některými podmínkami této Smlouvy nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci,

popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software (dále jen „Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva (dále jen „Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent (dále jen „MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Business Edition**. Pro použití Software na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. OEM Software se váže na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv

ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro následující funkce Softwaru:

a) **Aktualizace Software**. Poskytovatel může čas od času vydat aktualizaci Software ("Update"), avšak není povinný poskytovat Update. Tato funkce je při standardním nastavení Software zapnutá, proto se Update nainstaluje automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Update zakázal. Pro účely poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

b) **Zasílání infiltrací a informací Poskytovateli.** Software obsahuje funkce, které slouží ke shromažďování vzorků počítačových virů a jiných škodlivých počítačových programů a podezřelých, problematických nebo potenciálně nežádoucích nebo nebezpečných objektů, jako jsou soubory, adresy URL, IP pakety a ethernetové rámce (dále jen "Infiltrace") a jejich následnému odeslání Poskytovateli, mimo jiné včetně informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, a/nebo informací o operacích a funkcích Softwaru a informací o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení (dále jen "Informace"). Informace a Infiltrace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) o Koncovém uživateli a/nebo jiných uživatelích počítače, na kterém je Software nainstalován, a soubory postižené Infiltracemi, včetně přidružených metadat.

Informace a Infiltrace mohou být shromažďovány následujícími funkcemi Softwaru:

i. Funkce Reputační systém LiveGrid zahrnuje shromažďování a odesílání jednosměrných hodnot hash, které souvisejí s Infiltracemi, Poskytovateli. Tato funkce je povolena v rámci standardního nastavení Softwaru.

ii. Funkce Systém zpětné vazby LiveGrid zahrnuje shromažďování a odesílání Infiltrací s příslušnými metadaty a Informacemi Poskytovateli. Tuto funkci aktivuje Koncový uživatel během procesu instalace Softwaru.

Poskytovatel bude obdržené Informace a Infiltrace používat pouze pro účely analýzy a zkoumání Infiltrací, zlepšování ověřování pravosti Softwaru a Licence a přijme veškerá vhodná opatření, aby zajistil, že obdržené Infiltrace a Informace zůstanou v bezpečí. Po aktivaci této funkce Softwaru mohou být Infiltrace a Informace shromažďovány a zpracovávány Poskytovatelem, jak je uvedeno v Zásadách ochrany osobních údajů a v příslušných právních předpisech. Tyto funkce můžete kdykoliv deaktivovat.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu. Tímto souhlasíte s přijímáním oznámení a zpráv, mimo jiné včetně marketingových informací.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody**. Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJE APLIKOVATELNÉ PRÁVO, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULI ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory

mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru**. Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi (dále jen „přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována (dále jen „zákony o kontrole vývozu“) a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována (dále jen „sankční zákony“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19.a Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo

vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Všechny oznámení, včetně Software a Dokumentací je potřebné doručit na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. V případě rozporů mezi jazykovými verzemi této Dohody má přednost anglická verze. Změny této Dohody jsou možné jen v písemné formě, přičemž za Poskytovatele musí takovouto změnu podepsat statutární zástupce anebo osoba k tomuto úkonu výslovně zplnomocněná.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

EULA ID: HOM-ECS-20-01

Zásady ochrany osobních údajů

Společnost ESET spol. s r.o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsaná v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. Abychom dosáhli tohoto cíle, zveřejňujeme zde tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků ("Koncový uživatel" nebo "Vy") o následujících tématech:

- Zpracování osobních údajů
- Důvěrnost údajů,
- Práva subjektu údajů.

Zpracování osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v Licenčním ujednáním s koncovým uživatelem ("EULA"), ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané ve smlouvě EULA a dokumentaci k produktu, například služby aktualizace/upgradu, ESET LiveGrid®, ochranu proti zneužití dat, podporu atd. Aby všechny tyto služby fungovaly,

potřebujeme shromažďovat následující informace:

- Aktualizace a další statistiky zahrnující informace o procesu instalace a vašem počítači, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako je operační systém, údaje o hardwaru, ID instalace, ID licencí, IP adresa, MAC adresa a nastavení konfigurace produktu.

- Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jako součást reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu.

- Podezřelé vzorky a metadata jako součást systému zpětné vazby ESET LiveGrid®, který umožňuje společnosti ESET okamžitě reagovat na potřeby našich koncových uživatelů a udržet akceschopnost tváří v tvář nejnovějším hrozbám. Jsme závislí na tom, že nám zasíláte:

  - infiltrace, jako jsou potenciální vzorky virů a jiných škodlivých programů, a podezřelé; problematické, potenciálně nežádoucí nebo nebezpečné objekty, jako jsou spustitelné soubory nebo e-mailové zprávy, které jsou nahlášeny koncovým uživatelem jako nevyžádané nebo označené naším produktem; údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;

  - údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;

  - údaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;

  - Nemáme v úmyslu, aby byly součástí našich systémů nebo aby byly zpracovány pro účely uvedené v těchto Zásadách ochrany osobních údajů.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. Kontaktní informace a údaje obsažené ve vašich požadavcích na podporu mohou být vyžadovány za účelem poskytování podpory. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory.

- Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb.

- Za účelem poskytování podpory mohou být vyžadovány kontaktní informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory.

Důvěrnost údajů

ESET je společnost s celosvětovou působností. V rámci naší distribuční, servisní a podpůrné sítě využíváme přidružené subjekty a partnery. Informace, které společnost ESET zpracovává, mohou být přenášeny k přidruženým subjektům nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb, podpora nebo fakturace. Na základě vaší polohy a služeb, které si zvolíte, může být potřeba přenést vaše údaje do země, kde neplatí rozhodnutí Evropské komise o odpovídající ochraně. I v takovém případě každý přenos informací podléhá právním předpisům o ochraně údajů a probíhá pouze v případě potřeby. Bez výjimky musí být stanoveny standardní smluvní doložky, závazná firemní pravidla nebo jiná vhodná ochrana.

Děláme vše pro to, aby nedocházelo k uchovávání dat delší dobu, než je nezbytné k poskytování služeb podle smlouvy EULA. Naše doba uchovávání může trvat déle než platnost vaší licence, a to z toho důvodu, abychom vám poskytli čas pro snadné a pohodlné obnovení. Minimalizované a pseudonymizované statistiky a další data ze služby ESET LiveGrid® mohou být dále zpracovávány pro statistické účely.

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat dozorčí orgány i subjekty údajů. Jako subjekt údajů máte právo podat stížnost u dozorčího orgánu.

Práva subjektu údajů

Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Za podmínek stanovených příslušnými zákony o ochraně údajů máte jako subjekt údajů nárok na následující práva:

- právo požádat společnosti ESET o přístup k vašim osobním údajům,
- právo na opravu vašich osobních údajů, pokud jsou nepřesné (máte také právo na doplnění neúplných osobních údajů),
- právo požadovat vymazání vašich osobních údajů,
- právo požadovat omezení zpracování vašich osobních údajů,
- právo podat námitky proti zpracování,
- právo podat stížnost, stejně tak
- právo na přenositelnost dat.

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Vedoucí pracovník ochrany osobních údajů
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk