ESET Cyber Security

Felhasználói útmutató

Ide kattintva megjelenítheti a dokumentum verzióját

Digital Security
Progress. Protected.

Az ESET Cyber Security terméket az ESET, spol. s r.o. fejlesztette ki

További információkért látogasson el a https://www.eset.com oldalra.

Műszaki terméktámogatás: https://support.eset.com

REV. 2024.04.12.

ESET Cyber Security

ESET Cyber Security – ez egy újszerű megoldást jelentő integrált biztonsági programcsomag. A ESET LiveGrid® keresőmotor legújabb verziója gyorsan és megbízhatóan védi számítógépét.Az eredmény egy olyan intelligens rendszer, amely szünet nélkül figyeli a számítógépet veszélyeztető támadási kísérleteket és kártevő szoftvereket.

Az ESET Cyber Security egy teljes körű biztonsági megoldás, amely a hosszú távú fejlesztések eredményeként minimális rendszerterhelés mellett kínál maximális védelmet. Az ESET Cyber Security részét képező korszerű technológia a mesterséges intelligencián alapuló elemző algoritmusok segítségével képes proaktív módon kivédeni a vírusok, férgek, trójaiak, kémprogramok, kéretlen reklámprogramok, rootkitek és más internetes károkozók támadását anélkül, hogy a rendszer teljesítményét visszafogná.

A 7-es verzió újdonságai

Az ESET Cyber Security 7-os verziója az alábbi frissítéseket és fejlesztéseket tartalmazza:

- **Nagy teljesítmény és nagyobb stabilitás**– könnyebb architektúrával rendelkezik, mindegyik komponens elszigeteltebb, csak szükség esetén indul el, és megakadályozza, hogy a teljes alkalmazás összeomoljon hiba esetén. A jobb optimalizálás gyorsabb és hatékonyabb ellenőrzést tesz lehetővé.

- **ARM-kompatibilitás**– az ARM architektúrájú Apple chip natív támogatását tartalmazza. A korábbi verziók a Rosetta 2-t használták az ARM támogatásához.

- **Új kialakítású grafikus felhasználói felület**– a sötét mód támogatása.

- **Többnyelvű telepítő**– egyetlen telepítőfájl magában foglalja az összes nyelvet.

- **Automatikus frissítések**– frissítéseket keres, majd automatikusan letölti az új verziókat, és értesíti minden frissítésről.

- **Alkalmazásbeállítások** – újratervezve és továbbfejlesztve.

Az ESET Cyber Security új funkcióival kapcsolatos további részletekért olvassa el ezt az ESET-tudásbáziscikket.

Beállítások átköltöztetése

A 7.2-es és újabb verzióktól az ESET Cyber Security 6-os verziójából származó beállítások automatikusan átköltöznek az új verzióba a frissítési folyamat során.

Az átköltöztetési folyamat után az ESET Cyber Security megjelenít egy értesítést a kezdőképernyőn, amely jelzi a beállítások sikeres átköltöztetését: **A beállítások átkerültek az új verzióba**.

> Ha már frissített az ESET Cyber Security 6-os verziójáról a 7-es vagy 7.1-es verzióra, akkor is átköltöztetheti a beállításokat, amikor egy későbbi verzióra frissít. Az utasításokért tekintse meg az ESET átköltöztetésről szóló tudásbáziscikkét.

A 7.X verzióban elérhető összes beállítás átköltözik a 6-os verzióról, kivéve a következőket:

- Jogosultsági beállítások (a 7-es verzióban nem támogatottak)

- Egyéni proxykiszolgáló a frissítésekhez (az egyéni proxy nem támogatott a 7-es verzióban)
- A karantén tartalma
- Megtisztítási szintek az ellenőrzésekhez
- Célprofilok a kézi indítású ellenőrzéshez

A következő szolgáltatások beállításait az átköltöztetési .xml fájl tárolja, és akkor tölthetők majd be, ha a funkciók megtalálhatók lesznek az ESET Cyber Security következő verziójában:

- Eszközfelügyelet
- Naplók
- Webhozzáférés-védelem
- Bemutató üzemmód

Rendszerkövetelmények

Az optimális működéséhez a rendszernek meg kell felelnie az alábbi hardver- és szoftverkövetelményeknek:

	Rendszerkövetelmények:
Processzorarchitektúra	Intel 64-bit, M1, M2
Operációs rendszer	macOS Big Sur (11.0) és újabb
Memória	300 MB
Szabad tárhely	600 MB
Más	Internetkapcsolat szükséges a termék aktiválásához vagy frissítéséhez

Az ESET Cyber Security 7-es verziója natív támogatást nyújt az ARM architektúrájú Apple chipekhez.

Telepítés

A telepítés megkezdése előtt zárja be az összes megnyitott számítógépes programot. Az ESET Cyber Security olyan összetevőket tartalmaz, amelyek ütközhetnek a számítógépre telepített más vírusirtó programokkal. Ezért azt javasoljuk, hogy távolítsa el az összes többi vírusirtó programot az esetleges problémák megelőzése érdekében.

A Telepítővarázsló elindításához nyissa meg az ESET webhelyéről letöltött fájlt, majd kattintson duplán a **Az ESET Cyber Security telepítése** ikonra. A Telepítővarázsló ekkor végigvezeti a telepítésen.

Az ESET Cyber Security-telepítőfájl letölthető az ESET HOME-ból is. További információkért olvassa el ezt az ESET-tudásbáziscikket.

Használatbavétel

Az ESET Cyber Security telepítése után megjelenik a **Használatbavételi varázsló** – ez több képernyőből áll, amelyek végigvezetik az ajánlott és kötelező lépéseken, amelyek az ESET Cyber Security hiánytalan működéséhez szükségesek.

1. Engedélyezze az **ajánlott védelmi beállításokat**, válassza ki a kívánt beállításokat, majd kattintson a **Folytatás** gombra. Az **ESET LiveGrid®** rendszerről és a **kéretlen alkalmazásokról**, a szójegyzékünkben olvashat bővebben.

2. Kötelező lépés: **ESET-rendszerbővítmények** engedélyezése. A telepítés folytatásához kövesse a képernyőn megjelenő utasításokat.

3. Kötelező lépés: **Proxykonfiguráció** hozzáadása A megjelenő riasztási ablakban válassza ki az **Engedélyezés** lehetőséget.

4. Kötelező lépés: Adjon az ESET Cyber Security számára **Teljes lemezhozzáférést**. Kövesse a képernyőn megjelenő utasításokat, és engedélyezze a teljes lemezhozzáférést.

5. Ezután a varázsló kéri az **ESET Cyber Security** aktiválását. Több aktiválási lehetőséget is ismertet az Aktiválás című fejezet.

6. **Az értesítések engedélyezése** Azt javasoljuk, hogy engedélyezze az értesítéseket, hogy folyamatosan tájékozódjon a rendszert érintő esetleges fenyegetésekről.

A ESET Cyber Security használatbavételi varázsló kihagyása
A **Beállítás később** gombra kattintva kihagyhatja a kötelező beállítást, de vegye figyelembe, hogy a védelem csak részben fog működni.

A használatbavételi varázsló újraindítása
Nyissa meg a **Finder** > **Alkalmazások** lapot > a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) az **ESET Cyber Security** ikonra > válassza ki a **Csomag tartalmának a megjelenítése** menüpontra a helyi menüben > nyissa meg a **Contents** elemet > nyissa meg a **Helpers** > **Használatbavétel** elemet. A kötelező biztonsági beállításokat manuálisan is beállíthatja a Rendszerbővítmények engedélyezése és a Teljes lemezhozzáférés engedélyezése című fejezetben leírtak követésével.

Az ESET Cyber Security telepítése után célszerű ellenőrizni, hogy a számítógép nem tartalmaz-e kártékony kódokat. A program főablakában kattintson a **Ellenőrzés** > **Ellenőrzés most** elemre. A Kézi indítású számítógép-ellenőrzés című fejezetben bővebben olvashat a kézi indítású számítógép-ellenőrzésről.

Rendszerbővítmények engedélyezése

Ha először végzi az ESET Cyber Security telepítését, engedélyeznie kell a **rendszerbővítményeket**, hogy védelmet nyújtson az ESET Cyber Security. Ez történhet a használatbavételi folyamat részeként, vagy manuálisan is **engedélyezheti a rendszerbővítményeket** az alábbiak szerint:

Kövesse az itt ismertetett lépéseket, ha macOS Ventura (13.x) vagy újabb rendszerrel rendelkezik

1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki az **Adatvédelem és biztonság** menüpontot a bal oldali menüből.
3. Görgessen le a **Biztonság** szakaszhoz, majd kattintson a **Részletek** gombra a „Néhány rendszerszoftver figyelmet igényel a használat előtt” szöveg alatt.

Ha a **„Néhány rendszerszoftver figyelmet igényel a használat előtt”** és a **Részletek**gomb nem érhető el, akkor korábban engedélyezte a rendszerbővítményeket, így nincs további teendője.

4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata** gombra, és írja be a **felhasználónevét** és **jelszavát**, majd kattintson a **Feloldás** gombra.
5. Engedélyezze az **ESET Valós idejű fájlrendszervédelem** és az **ESET Web- és e-mail-védelem** funkciót a kapcsolókra kattintva.
6. Kattintson az **OK** gombra.
7. Amikor az **ESET Web- és e-mail-védelem** figyelmeztetése felszólítja a **proxykonfiguráció hozzáadására**, válassza ki az **Engedélyezés** lehetőséget. Ha a figyelmeztetés megjelenésekor nem engedélyezi a proxykonfigurálást, akkor újra kell indítania a számítógépet a figyelmeztetés megjelenítéséshez, és újra engedélyeznie kell a proxykonfigurálást.

Részletes útmutatót ehhez a tudásbáziscikkünkben talál. A tudásbáziscikkek nem minden nyelven érhetők el.

Kövesse az itt leírt lépéseket, ha macOS Monterey (12.x) vagy korábbi rendszerrel rendelkezik

1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki a **Biztonság és adatvédelem** lehetőséget.
3. A bal alsó sarokban található lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.
4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Kattintson a **Részletek** elemre.
6. Válassza ki mindegyik **ESET Cyber Security** opciót.
7. Kattintson az **OK** gombra.

A használatbavételi varázsló újraindítása

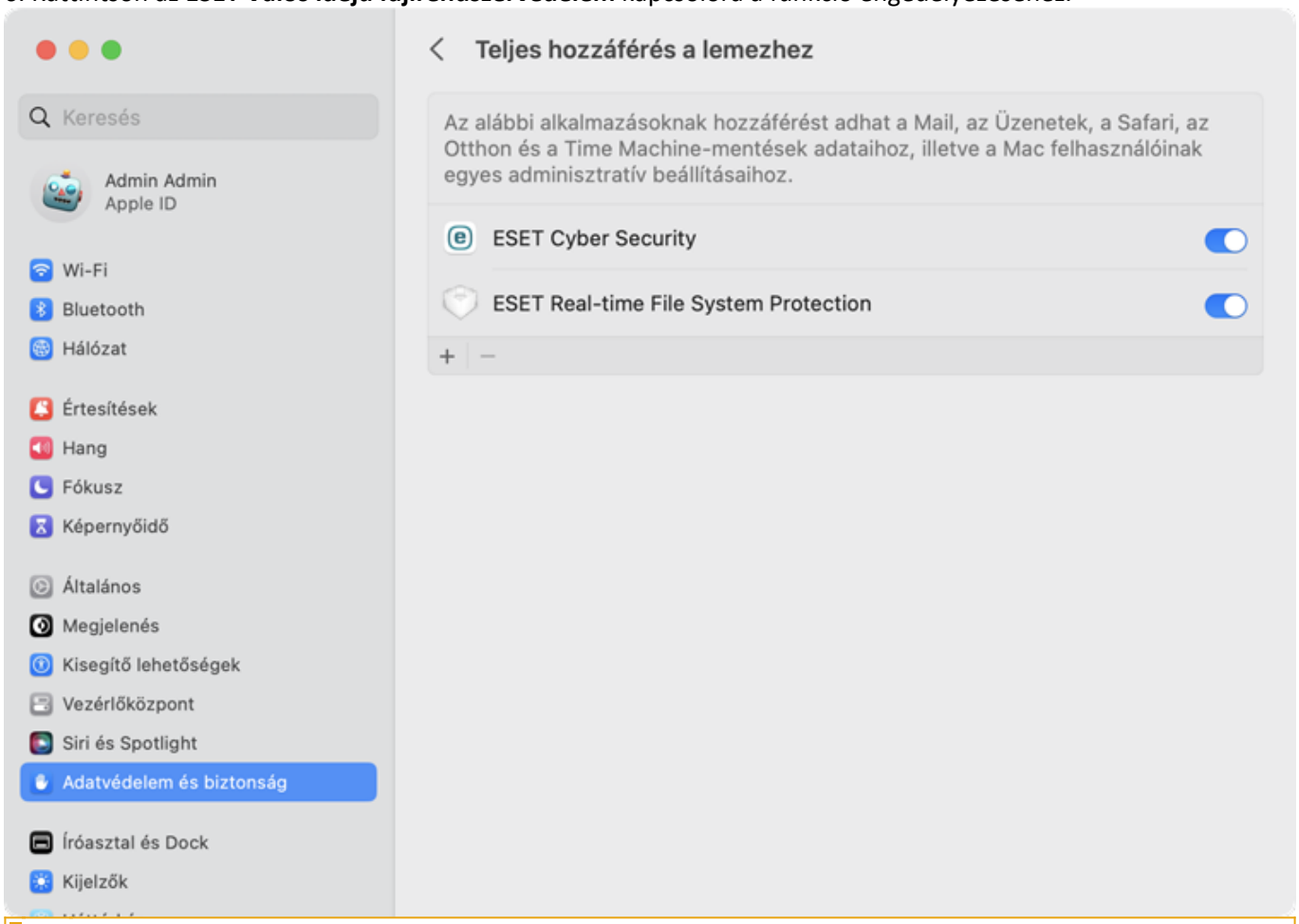
Nyissa meg a **Finder** > **Alkalmazások** lapot > a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) az **ESET Cyber Security** ikonra > válassza ki a **Csomag tartalmának a megjelenítése** menüpontra a helyi menüben > nyissa meg a **Contents** elemet > nyissa meg a **Helpers** > **Használatbavétel** elemet. A használatbavételi varázsló végigvezeti az ESET Cyber Security általi teljes védelemhez szükséges lépéseken.

A Teljes lemezhozzáférés engedélyezése

Ha először telepíti az ESET Cyber Security szolgáltatást, engedélyeznie kell a **Teljes lemezhozzáférést**, hogy védelmet nyújtson az ESET Cyber Security. Ez történhet a használatbavételi folyamat részeként, vagy manuálisan is **engedélyezheti a Teljes lemezhozzáférést** az alábbiak szerint:

Kövesse az itt leírt lépéseket, ha macOS Ventura (13.x) vagy újabb rendszerrel rendelkezik

1. Nyissa meg a **Rendszerbeállításokat**.
2. Válassza ki az **Adatvédelem és biztonság** menüpontot a bal oldali menüből.
3. Kattintson a **Teljes lemezhozzáférés** elemre, majd az ESET Cyber Security kapcsolóra a funkció engedélyezéséhez.
4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata gombra**, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Ha megjelenik egy felszólítás az ESET Cyber Security újraindítására, kattintson a **Később** gombra.
6. Kattintson az **ESET Valós idejű fájlrendszervédelem** kapcsolóra a funkció engedélyezéséhez.



Ha a **Valós idejű fájlrendszervédelem** opció nem érhető el, engedélyeznie kell a rendszerbővítményeket az ESET-termékhez.

7. Miután engedélyezte a rendszerbővítményeket és a Teljes lemezhozzáférést, indítsa újra a számítógépet. További információkért tekintse meg tudásbáziscikkünket.

Kövesse az itt leírt lépéseket, ha macOS Monterey (12.x) vagy korábbi rendszerrel rendelkezik

1. Nyissa meg a **Rendszerbeállításokat**.
2. Lépjen az **Adatvédelem** lapra, és válassza ki a **Teljes lemezhozzáférés** menüpontot a bal oldali menüből.
3. A bal alsó sarokban található lakatra kattintva engedélyezze a módosításokat a beállítási ablakban.
4. Használja a **Touch ID-t**, vagy kattintson a **Jelszó használata** gombra, és írja be a felhasználónevét és jelszavát, majd kattintson a **Feloldás** gombra.
5. Válassza ki az **ESET Cyber Security** szolgáltatást a listából.
6. Ekkor megjelenik az ESET Cyber Security újraindítását lehetővé tevő értesítés. Kattintson a **Később** gombra.
7. Válassza ki az **ESET Valós idejű fájlrendszervédelem** elemet a listában.

Ha a **Valós idejű fájlrendszervédelem** opció nem érhető el, engedélyeznie kell a rendszerbővítményeket az ESET-termékhez.

8. Kattintson az **Újrakezdés** gombra a riasztási ablakban az ESET Cyber Security újraindításához és a módosítások érvényesítéséhez, vagy indítsa újra a számítógépet. További információkért tekintse meg tudásbáziscikkünket.

A használatbavételi varázsló újraindítása
Nyissa meg a **Finder** > **Alkalmazások** lapot > a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) az **ESET Cyber Security** ikonra > válassza ki a **Csomag tartalmának a megjelenítése** menüpontra a helyi menüben > nyissa meg a **Contents** elemet > nyissa meg a **Helpers** > **Használatbavétel** elemet. A használatbavételi varázsló végigvezeti az ESET Cyber Security általi teljes védelemhez szükséges lépéseken.

Licenc aktiválása

A **Termékaktiválás** ablak a használatbavételi lépések egyikeként jelenik meg. Abban az esetben, ha a termék aktiválása nem történt meg a használatbavétel során, bármikor elvégezhető az ESET Cyber Security alkalmazásban. Az alkalmazás elindításához kattintson az ESET Cyber Security macOS menüsorán (a képernyő tetején) található ikonjára, majd válassza ki az ESET Cyber Security megjelenítése lehetőséget. A **Termékaktiválás** figyelmeztetés az **Áttekintés** szakaszban jelenik meg. A figyelmeztetés tartalmazza az **aktiválási párbeszédablakra** mutató linket. Miután megnyílt az aktiválási párbeszédablak, adja meg a következőket:

- **Aktiválás aktiválási kulccsal** – Írja be az aktiválási kulcsot, amely azonosítja az előfizetés tulajdonosát, és aktiválja az előfizetést. Az aktiválási kulcs egy egyedi karakterlánc a következő formátumban: XXXX-XXXX-XXXX-XXXX-XXXX vagy XXXX-XXXXXXXX.

- **Ingyenes próbaverzió** – Válassza ezt a lehetőséget az ESET Cyber Security vásárlás előtti kiértékeléséhez. Írja be adatait, majd kattintson a **Regisztráció** gombra az ESET Cyber Security korlátozott ideig történő aktiválásához. Minden kliens csak egyszer aktiválhatja a próbaverzió licencét.

- **Előfizetés vásárlása** — Előfizetés vásárlásához kattintson erre a lehetőségre. Ekkor átkerül a helyi ESET-forgalmazó webhelyére.

- Az **ESET HOME**-fiók használata – Jelentkezzen be az ESET HOME-fiókjába, és válasszon előfizetést az ESET-termék eszközén történő aktiválásához.

- **Aktiválás később** – Ha az adott időpontban nem szeretné aktiválni a licencet, kattintson erre az opcióra.

Ha többet szeretne megtudni arról, hogy hol található az aktiválási kulcs, olvassa el ezt az ESET-tudásbáziscikket.

Hol találom az előfizetésemet?

Ha az interneten vásárolt előfizetést, kapott egy e-mailt az ESET-től, amely tartalmazza az aktiválási kulcsot (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX), a nyilvános licencazonosítót (xxx-xxx-xxx), a termék nevét (vagy a termékek listáját) és a mennyiséget. Ha a termék kiskereskedelmi dobozos változatát vásárolta meg, az aktiválási kulcs a termékcsomag belsejében vagy hátoldalán található.

Ha az aktiválási kulcs nem működik, tekintse meg ezt az ESET-tudásbáziscikket.

Eltávolítás

Az ESET Cyber Security eltávolításhoz kövesse az alábbi lépéseket:

1.Indítsa el a **Findert**

2.Nyissa meg a merevlemezen található **Alkalmazások** mappát.

3.A Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) az **ESET Cyber Security** ikonra.

4.Válassza ki a **Csomag tartalmának a megjelenítése** lehetőséget a helyi menüből.

5.Nyissa meg a **Contents** > **Helpers** mappát, és kattintson duplán az **Uninstaller** ikonra.

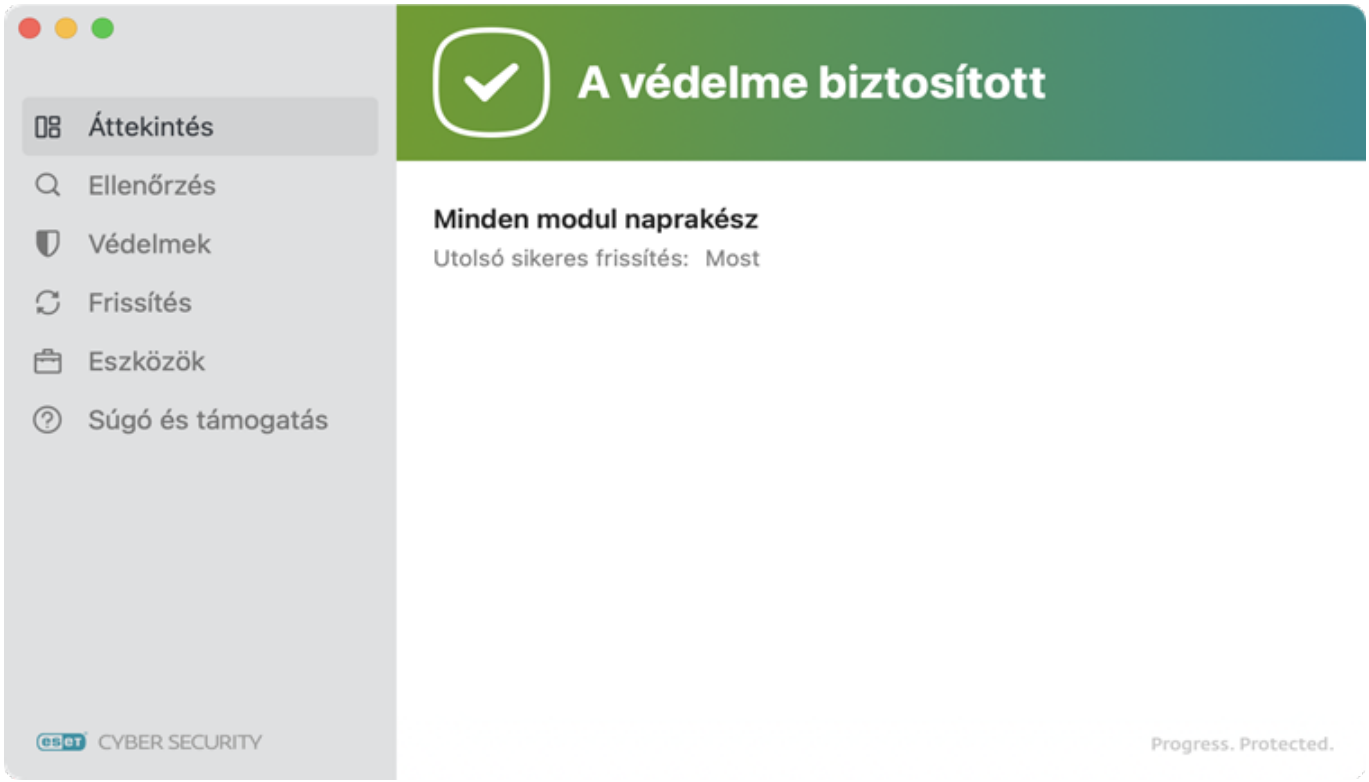
Ha megtartotta az ESET Cyber Security-telepítőfájlt (.dmg), nyissa meg, majd kattintson duplán az **Eltávolítás** gombra.

Az ESET Cyber Security használata

Az ESET Cyber Security főablaka két fő részre oszlik. A jobb oldali elsődleges ablakban a bal oldalon kiválasztott beállításnak megfelelő információk jelennek meg.

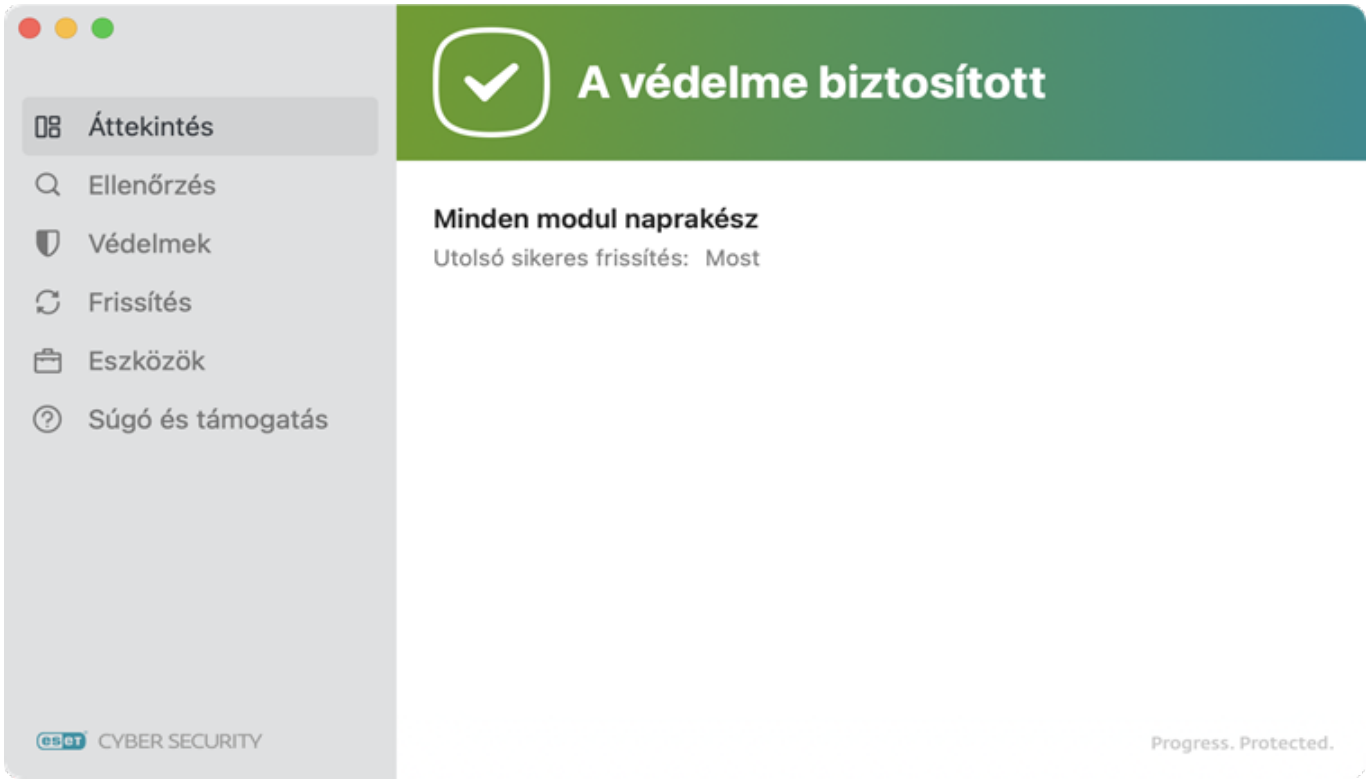
A főmenüből a következő szakaszok érhetők el:

- **Áttekintés** – Állapot-összefoglalót ad az ESET Cyber Security-modulok működéséről.
- **Ellenőrzés** – Lehetővé teszi az összes helyi lemez ellenőrzését vagy egyéni ellenőrzés futtatását.
- **Védelmek** – Lehetővé teszi a számítógép biztonsági szintjének beállítását.
- **Frissítés** – A keresőmodulok frissítéseiről jelenít meg információkat.
- **Eszközök** – Hozzáférést biztosít a naplófájlokhoz és a karanténhoz.
- **Súgó és támogatás**–Hozzáférést biztosít a súgófájlokhoz, az ESET tudásbázisához, a támogatáskérelmi űrlaphoz és a program további információihoz.



Védelem állapotának ellenőrzése

A védelem állapotának megjelenítéséhez a főmenüben kattintson a **Áttekintés** lehetőségre. Az ESET Cyber Security-modulok működésére vonatkozó állapotösszegzés megjelenik az elsődleges ablakban.



Súgó és támogatás

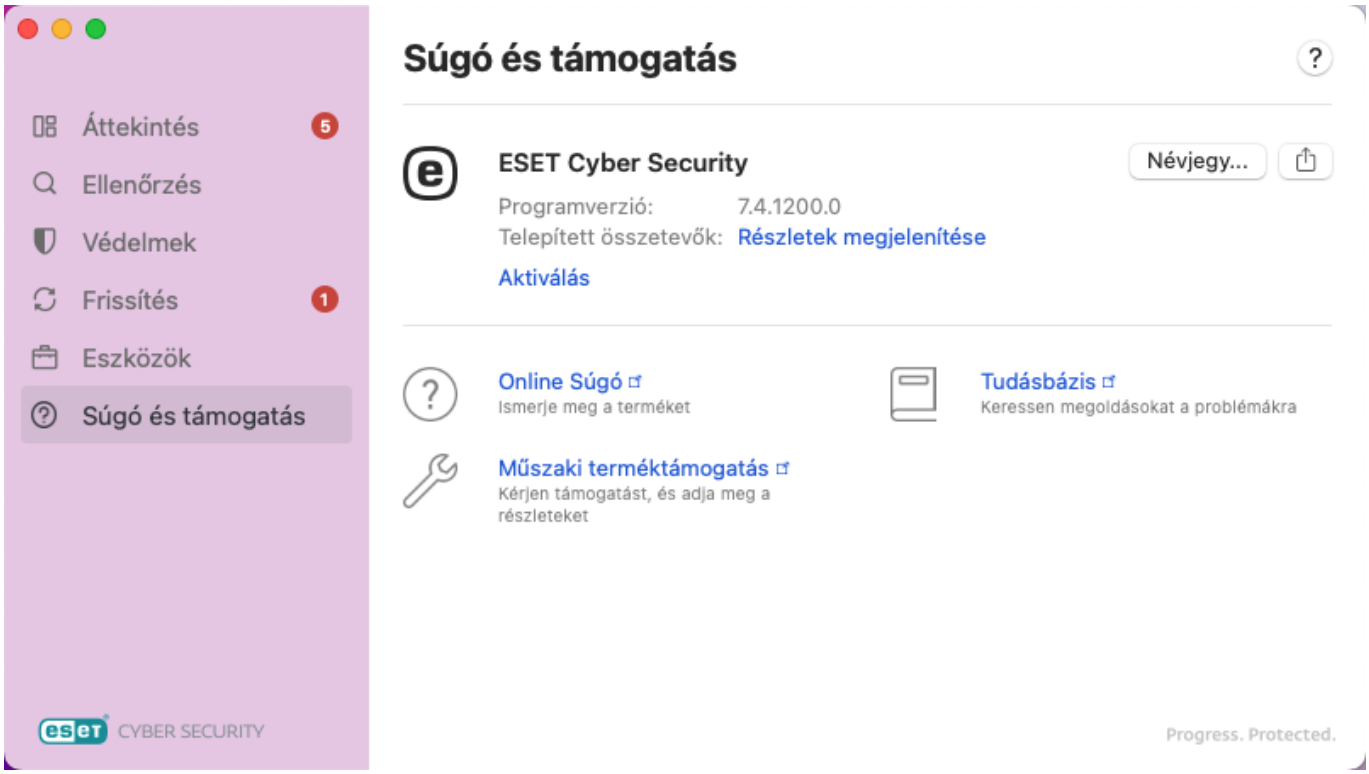
Az ESET Cyber Security súgója hibaelhárítási eszközöket és támogatási információkat tartalmaz, amelyek segítséget nyújtanak a felmerülő problémák megoldásában. A Súgó és támogatás szakasz az alkalmazás fő ablakában található. A telepített összetevők listájának megjelenítéséhez kattintson a **Részletek megjelenítése** elemre a **Telepített összetevők** szöveg mellett. **Az összes másolása** elemre koppintva a vágólapra másolhatja a listát. Ez a hibakereséshez, illetve a terméktámogatási szolgálattal folytatott kommunikáció során lehet hasznos.

Az **ESET Cyber Security** termékverziója és a termék-előfizetés azonosítója látható. Lehetőség van az előfizetés módosítására is: kattintson erre az opcióra az aktiválási ablak elindításához és a termék aktiválásához. A **Névjegy** gombra kattintva további részleteket tekinthet meg az ESET Cyber Security szolgáltatásról.

Súgóoldal – Kattintson erre a hivatkozásra az ESET Cyber Security súgójának megnyitásához.

Műszaki terméktámogatás – Ha nem tudja megoldani az adott problémát a súgóoldalaink segítségével, vegye fel a kapcsolatot az ESET műszaki terméktámogatással.

Tudásbázis – Az ESET tudásbázisában (angol nyelven) találhatók a leggyakoribb kérdésekre adott válaszok, valamint a különböző problémákra ajánlott megoldások. Az ESET műszaki szakemberei által rendszeresen frissített tudásbázis a különböző problémák megoldásának leghatékonyabb eszköze.



Beállítások importálása és exportálása

Meglévő konfiguráció importálásához vagy az ESET Cyber Security-konfiguráció exportálásához nyissa meg az ESET Cyber Security fő alkalmazásablakát, majd a képernyő bal felső sarkában található macOS-menüsorban kattintson a **Fájl** > **Beállítások importálása vagy exportálása** elemre.

Importálásra és exportálásra akkor lehet szükség, ha az ESET Cyber Security aktuális konfigurációjáról későbbi használat céljából biztonsági másolatot kell készítenie. A beállítások exportálása azok számára is hasznos, akik az

ESET Cyber Security előnyben részesített beállításait több rendszerben is szeretnék használni. A kívánt beállításokat egyszerűen átviheti egy konfigurációs fájl importálásával.

Ha konfigurációt szeretne importálni, válassza ki a **Beállítások importálása** lehetőséget, és keresse meg az importálni kívánt konfigurációs fájlt. Ha exportálni szeretne, válassza a **Beállítások exportálása** elemet, és a tallózási funkcióval jelöljön ki egy helyet a számítógépen, ahová menteni szeretné a fájlt.

Billentyűparancsok

Az alábbi billentyűparancsokat használhatja az ESET Cyber Security szolgáltatásban:

- cmd+, – az ESET Cyber Security beállításainak megadása;
- cmd+Q – az ESET Cyber Security grafikus felhasználói felülete főablakának elrejtése. Ezt a macOS menüsorán (a képernyő tetején) található ESET Cyber Security ikonra kattintva, majd **Az ESET Cyber Security megjelenítése** elemet kiválasztva nyithatja meg.
- cmd+W – az ESET Cyber Security grafikus felhasználói felülete főablakának bezárása.

Teendők, ha a program nem megfelelően működik

Ha az összes modul megfelelően működik, a zöld színű **A védelme biztosított** fejléc látható az **Áttekintés** szakaszban. Ha egy modul hibásan működik, a vörös színű **Biztonsági figyelmeztetés** fejléc vagy a narancssárga **Beavatkozás szükséges** fejléc látható. Az ESET Cyber Security megjelenít további információkat a modulról és a javasolt megoldást a problémák elhárítására. Az egyes modulok állapotának módosításához kattintson az adott értesítési üzenet alatti kék hivatkozásra.

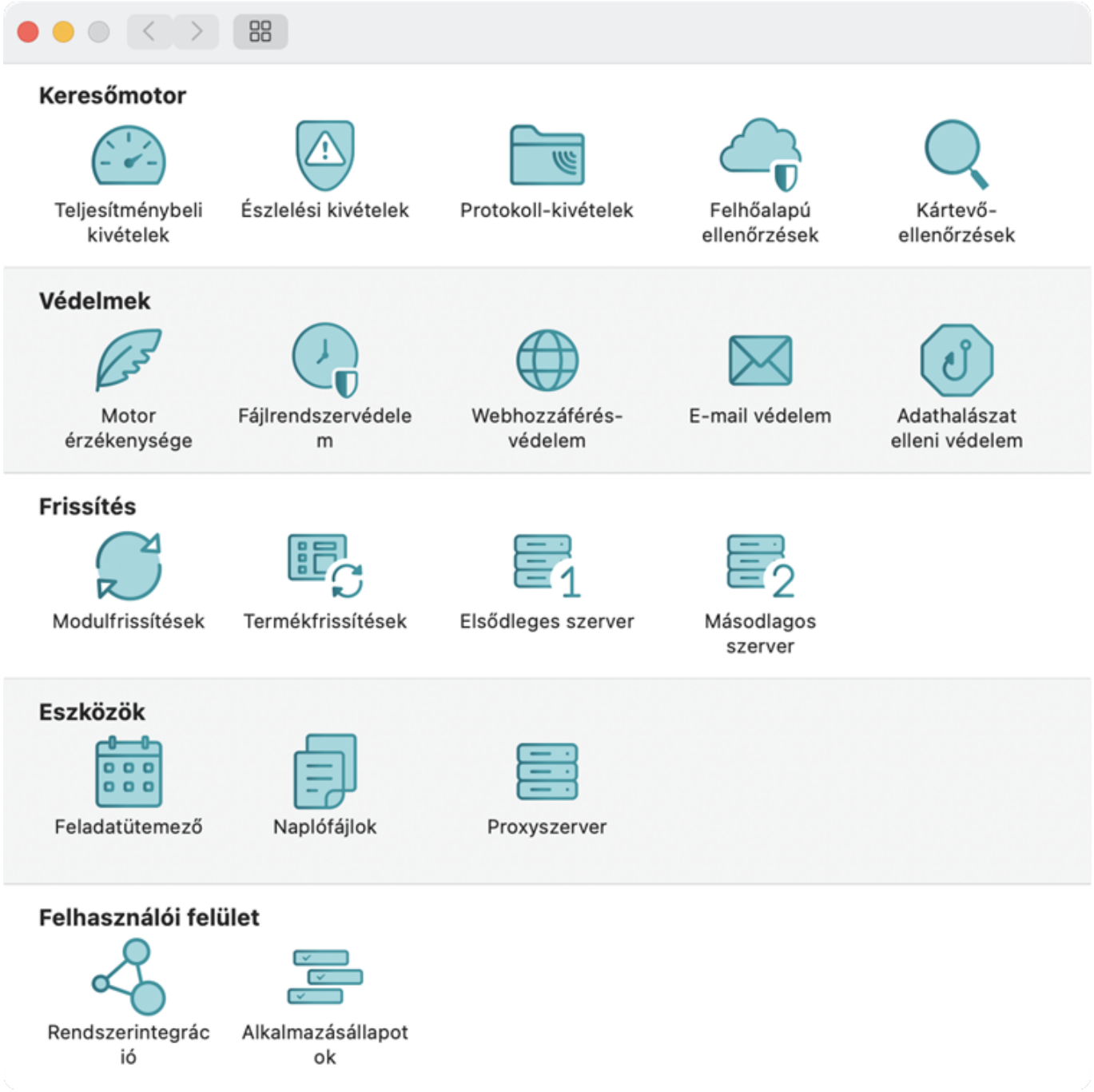
Ha a javasolt megoldásokkal nem szüntethető meg a probléma, az ESET tudásbázisában is megoldást kereshet rá, vagy lépjen kapcsolatba az ESET műszaki terméktámogatásával.

Alkalmazásbeállítások

Az ESET Cyber Security speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

A következő kategóriákba tartozó modulok beállításait konfigurálhatja:

- Keresőmotor
- Védelmek
- Frissítés
- Eszközök
- Felhasználói felület



Keresőmotor

A keresőmotor a fájlok ellenőrzésével megakadályozza a kártékony kódok bejutását a rendszerbe. Ha például a program felismer egy kártevőnek minősülő objektumot, megkezdődik a kezelése. A keresőmotor először letiltja, majd megtisztítja, törli vagy karanténba helyezi.

Az ESET Cyber Security **Keresőmotor** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Teljesítménybeli kivételek

A **Teljesítménybeli kivételek** csoportban megadhatja egyes fájlok, mappák, alkalmazások vagy IP/IPv6-címek kizárását az ellenőrzésből. Ha kizár útvonalakat (mappákat) az ellenőrzésből, sokkal kevesebb idő alatt kiszűrhetők a kártevők a fájlrendszerből.

-  – Új kivétel létrehozása. Adja meg az objektum elérési útját.
-  – A kijelölt bejegyzések eltávolítása.

Csak akkor szabad kizárni a fájlokat az ellenőrzésből, ha komoly problémákat tapasztal a valós idejű védelemmel kapcsolatban, mivel a fájlok ellenőrzésből való kizárása csökkenti az általános védelmet.

Észlelési kivételek

Ezzel a funkcióval objektumokat zárhat ki a tisztításból az észlelt elem neve, az objektum elérési útvonala vagy kivonata segítségével.

Az észlelési kizárások beállításakor bizonyos kizárási kritériumokat kell megadni. Meg kell adni egy érvényes észlelési nevet vagy SHA-1 kivonatot. Az érvényes fertőzésneveket vagy az SHA-1 kivonatokat tekintse meg a naplófájlokban, majd válassza ki az Észlelések menüpontot a Naplófájlok legördülő menüben. Ez akkor hasznos, ha egy tévesen jelentett minta észlelhető az ESET Cyber Security alkalmazásban. A valós fertőzések kizárása nagyon veszélyes – lehetőleg csak az érintett fájlokat vagy könyvtárakat zárja ki átmeneti időre. A kivételek a kéretlen alkalmazásokra, a veszélyes alkalmazások és a gyanús alkalmazásokra is vonatkoznak.

A következő típusú **kizárási feltételek** vannak:

- **Pontosan a fájl** – Fájl kizárása a megadott kivonat alapján SHA-1, függetlenül a fájl típusától, tárolási helyétől, nevétől és kiterjesztésétől.
- **Észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve alapján.
- **Elérési út és észlelt elem** – Mindegyik fájl kizárása az észlelt elem neve és elérési útja alapján (pl. `file:///Users/documentation/Downloads/eicar_com.zip`).

Csak akkor használjon észlelési kizárásokat, ha komoly problémákat tapasztal például egy kártevő észlelésével, mert a kártevők ellenőrzésből való kizárása csökkenti az általános védelmi szintet.

Protokoll-kivételek

A kivételek listájában szereplő címeken nem végez protokollszűrést a rendszer. A listára csak megbízható alkalmazásokat és címeket ajánlott felvenni.

Felhőalapú ellenőrzések

Az ESET LiveGrid® megbízhatósági rendszer engedélyezése (javasolt)

Az ESET LiveGrid® szolgáltatása összeveti az ellenőrzött fájlokat a felhőben tárolt engedélyező- és tiltólistaelemek adatbázisával, ezáltal fokozza az ESET kártevőirtó szoftvereinek a hatékonyságát.

Az ESET LiveGrid® visszajelzési rendszer engedélyezése

Az ESET víruslaborja megkapja a mintákat további elemzésre.

Minták elküldése

Az észlelt minták automatikus elküldése: A kiválasztott beállítás alapján fertőzött mintákat küldheti be az ESET víruslaborjának elemzésre és a kártevőészlelés fejlesztése céljából.

- Az összes észlelt minta
- Az összes minta a dokumentumok kivételével
- Ne küldje be

Gyanús minták automatikus elküldése: A kártevőkre hasonlító és szokatlan tulajdonságokat vagy viselkedést mutató gyanús mintákat a rendszer elküldi elemzésre az ESET víruslaborjába.

- Végrehajtható fájlok – Például a következő végrehajtható fájlok: .exe, .dll, .sys
- Tömörített fájlok – Például a következő tömörített fájltípusok: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- Szkriptek – Például a következő a szkriptfájltípusok: .bat, .cmd, .hta, .js, .vbs, .ps1
- Dokumentumok – A Microsoft Office, a Libre Office vagy más irodai eszközben létrehozott dokumentumok vagy aktív tartalommal rendelkező PDF-fájlok.
- Egyéb – Például a következő fájltípusok: .jar, .reg, .msi, .swf, .lnk

Automatikus beküldési kivételek: A kizárt fájlokat akkor sem kapja meg az ESET víruslaborja, ha gyanús kódot tartalmaznak.

Összeomlási jelentések és diagnosztikai adatok küldése

Elküldhet például olyan adatokat, mint az összeomlási jelentések vagy a modul-memóriaképek.

Segítse a termék tökéletesítését anonim használati statisztikai adatok beküldésével

Engedélyezheti az ESET-nek, hogy begyűjtse az újonnan észlelt kártevőkre vonatkozó anonim információkat (név, az észlelés dátuma és időpontja, az észlelési mód és a kapcsolódó metaadatok), az ellenőrzött fájlokat (kivonat, fájlnév, a fájl eredete, telemetria), a letiltott és gyanús URL-címeket, a termékverziót és -konfigurációt, beleértve az Ön rendszerének adatait.

E-mail-cím (nem kötelező)

E-mail-címét a program a gyanús fájlokkal együtt elküldi az ESET víruslaborjába. Az ESET munkatársai azonban csak akkor keresik fel, ha a gyanús fájlokkal kapcsolatban további információra van szükségük.

Kártevő-ellenőrzések

A kézi indítású víruskereső a vírus- és kémprogramvédelem fontos része, és a használatával ellenőrizheti a számítógépen lévő fájlokat és mappákat. Biztonsági szempontból fontos, hogy a számítógép-ellenőrzések futtatása ne csak akkor történjen meg, ha fertőzés gyanítható, hanem rendszeres időközönként, a szokásos biztonsági intézkedések részeként. A **Kártevőellenőrzések** szakaszban konfigurálhatja a kézi indítású ellenőrzési profilok beállításait:

Profilok listája – Új létrehozásához vagy meglévő eltávolításához kattintson a + vagy − gombra. Új profil hozzáadásakor írja be a profil nevét, majd kattintson az **OK** gombra. Az új profil megjelenik a Kiválasztott profil legördülő menüben, amely felsorolja a meglévő ellenőrzési profilokat.

ThreatSense-paraméterek – Az ellenőrzési profil konfigurációs beállításai, például a vezérelni kívánt fájlkiterjesztések, ellenőrizendő objektumok, alkalmazott észlelési módszerek stb.

Védelmek

Az ESET Cyber Security speciális **védelmi beállításainak** módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Motor érzékenysége

A motorérzékenység lehetővé teszi a következő kategóriák jelentési és védelmi szintjeinek konfigurálását az összes védelmi modulnál.

- **Kártevő** – rosszindulatú kód, amely a számítógépen meglévő fájlokhoz kapcsolódik

- **Kéretlen alkalmazások** – A „grayware” vagy kéretlen alkalmazások (PUA) kategória számos különböző szoftvert foglal magában. Az ilyen szoftverek nem annyira kártékonyak, mint a többi kártevő, például a vírusok és a trójaiak. További nemkívánatos szoftvereket telepíthetnek azonban, megváltoztathatják a digitális készülék viselkedését, illetve olyan tevékenységeket végezhetnek, amelyeket a felhasználó nem hagyott jóvá, vagy nem várt. A Szószedetben részletesen olvashat az ilyen típusú alkalmazásokról.

- **Gyanús alkalmazások** – Ezek olyan programok, amelyeket tömörítőprogramokkal vagy védelmi modulokkal tömörítettek. Az ilyen típusú védelmi modulokat gyakran használják a kártevőprogramok fejlesztői arra, hogy segítségükkel elkerüljék az észlelést. A tömörítő egy olyan futtatás közbeni, önkicsomagoló végrehajtható fájl, amely többféle kártevőt egyetlen csomagban egyesít. A legnépszerűbb tömörítők az UPX, a PE_Compact, a PKLite és az ASPack. Ugyanazt a kártevőt különbözőképpen észlelheti a program attól függően, hogy a tömörítést melyik tömörítővel végezték. A tömörítőkre továbbá az is jellemző, hogy „aláírásuk” idővel mutáción megy keresztül, még jobban megnehezítve ezzel a kártevő észlelését és eltávolítását.

- **Veszélyes alkalmazások** – A kereskedelemben kapható olyan törvényes szoftverek, amelyekkel a támadók visszaélhetnek, ha a felhasználó beleegyezése nélkül telepítik azokat. Ez a besorolás olyan programokat tartalmaz, mint a távoli hozzáférési eszközök. Ez a beállítás alapértelmezés szerint le van tiltva.

Fájlrendszervédelem

Az ESET LiveGrid® technológia (a ThreatSense keresőmotor beállításai című témakörben ismertetjük) használatakor a valós idejű fájlrendszervédelem eltérő lehet az újonnan létrehozott fájlok és a meglévő fájlok esetében. Nagyobb fokú felügyelet érhető el az újonnan létrehozott fájlok esetén.

A következő típusú adathordozókat zárhatja ki a Real-time ellenőrzésből:

- **Helyi meghajtók** – rendszermeghajtók
- **Cserélhető adathordozók** – USB-tárolóeszközök, Bluetooth-eszközök stb.
- **Hálózati adathordozók** – minden csatlakoztatott meghajtó

Alapértelmezés szerint a szolgáltatás az összes fájlt ellenőrzi a **fájlok megnyitása** és a **fájlok létrehozása** után. Az ESET azt javasolja, hogy tartsa meg az alapértelmezett beállításokat, mert maximális szintű valós idejű védelmet biztosítanak a számítógép számára.

Bizonyos folyamatokat is kizárhat az ellenőrzésből.

Az ESET azt javasolja, hogy az alapértelmezett beállításokat használja és csak bizonyos esetekben módosítsa az ellenőrzésből kizárandó adathordozókat, például amikor egyes adathordozók ellenőrzése jelentősen lassítja az adatátvitelt.

Webhozzáférés-védelem

A webhozzáférés-védelem a böngészők és a távoli szerverek közötti kommunikációt figyeli, és támogatja a HTTP protokollon alapuló szabályokat.

A webes szűrést úgy érheti el, hogy meghatározza a portszámokat a HTTP-kommunikációhoz és az URL-címekhez.

Webprotokollok

A webprotokollok szakaszban engedélyezheti vagy letilthatja a HTTP-protokollellenőrzést, és meghatározhatja a HTTP-kommunikációhoz használni kívánt portszámokat. Alapértelmezés szerint a 80-as, a 8080-as és a 3128-as portszám van beállítva.

URL-címek kezelése

Ebben a szakaszban megadhatók a letiltandó, engedélyezendő, illetve az ellenőrzésből kizárandó HTTP-címek. A Letiltva címek listájában szereplő webhelyeket nem fogja tudni elérni. A kizárt címek listáján szereplő webhelyek elérése közben a program nem keres kártékony kódokat.

Az engedélyezett, letiltott vagy kizárt címek listájának aktiválásához válasszon egy listát, és engedélyezze az **Lista aktiválása** opciót. Ha értesítést szeretne megjeleníteni az aktuális listán szereplő címek beírásakor, engedélyezze

az **Értesítés az alkalmazásakor** opciót.

Bármely listában használható a *(csillag) és a ?(kérdőjel) speciális szimbólum. A csillaggal tetszőleges karaktersor, a kérdőjellel pedig bármilyen szimbólum helyettesíthető. Az ellenőrzésből kizárt címek megadásakor különös figyelemmel járjon el, mert a listában csak megbízható és biztonságos címek szerepelhetnek. Szintén fontos, hogy a * és a ? szimbólumot megfelelően használja a listában.

E-mail védelem

E-mail védelem – A POP3 és az IMAP protokollon keresztül érkező e-mailes kommunikáció szabályozását biztosítja. A bejövő üzenetek vizsgálatakor az ESET Cyber Security a ThreatSense keresőmotor összes speciális ellenőrzési módszerét alkalmazza. A POP3 és az IMAP protokollon keresztül folytatott kommunikáció ellenőrzése nem függ attól, hogy milyen levelezőprogramot használ. A választható beállítások az alábbiak:

Levelezési protokollok

Itt engedélyezheti vagy letilthatja a POP3 és az IMAP protokollon keresztül érkező e-mailek ellenőrzését.

POP3-protokollszűrés

A POP3 a levelezőprogramok által a legszélesebb körben használt levélfogadási protokoll. Az ESET Cyber Security a levelezőprogramtól függetlenül képes védeni a POP3 protokollon keresztüli kommunikációt.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A modul megfelelő működéséhez ellenőrizze, hogy az IMAP-protokollszűrés engedélyezve van-e. Az automatikus IMAP-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 110-as porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

Ha engedélyezi a **POP3 protokollellenőrzés** opciót, a rendszer ellenőrzi az összes POP3 forgalmat a rosszindulatú szoftverek szempontjából.

IMAP-protokollszűrés

Az IMAP egy e-mailek fogadására szolgáló protokoll. Az IMAP a POP3 protokollnál fejlettebb funkciókkal rendelkezik. Az ESET Cyber Security a használt levelezőprogramtól függetlenül képes az IMAP protokoll védelmére.

Az ellenőrzést biztosító védelmi modul automatikusan elindul az operációs rendszer indításakor, és aktív marad a memóriában. A modul megfelelő működéséhez ellenőrizze, hogy az IMAP-protokollszűrés engedélyezve van-e. Az automatikus IMAP-ellenőrzéshez nincs szükség a levelezőprogram újrakonfigurálására. A modul alapértelmezés szerint a 143-as porton át folyó teljes kommunikációt ellenőrzi, de szükség esetén a vizsgálat további kommunikációs portokra is kiterjeszthető. A portszámokat vesszővel elválasztva kell megadni.

Ha engedélyezi az **IMAP-protokollszűrést**, akkor a program az IMAP protokollon átmenő teljes forgalmat ellenőrzi kártevő szoftvereket keresve.

E-mail-címkék

Az e-mail-címkék használata lehetővé teszi címkeüzenet hozzáfűzését az e-mail-lábjegyzethez. Az e-mailek ellenőrzése után előfordulhat, hogy a program az ellenőrzés eredményét ismertető értesítést is hozzáfűz az adott

üzenethez. A címkeüzenetek, azaz értesítő szövegek hasznos eszközként szolgálnak, de nem érdemes az üzenet biztonságának végső meghatározásához használni őket, mivel a hibásan formázott HTML-üzenetekben eltűnhetnek, illetve egyes kártevők képesek azokat meghamisítani. A választható lehetőségek az alábbiak:

- **A kimenő e-mailekhez észlelés esetén** – Csak a kártevőket tartalmazó e-mailek lesznek megjelölve ellenőrzöttként.
- **Minden e-mailhez ellenőrzéskor** – Az összes ellenőrzött e-mail címkeüzenettel lesz ellátva.
- **Soha** – Semmilyen e-mail nem lesz ellátva címkeüzenettel.

Kapott e-mail tárgyának frissítése – Jelölje be ezt a jelölőnégyzetet, ha azt szeretné, hogy az e-mail-védelem kártevőre utaló figyelmeztetést szúrjon be a fertőzött e-mailekbe. Ez a funkció lehetővé teszi a fertőzött e-mailek egyszerű szűrését. Így a címzett számára megnő az üzenetek hitelességi szintje, és fertőzés észlelése esetén értékes információk nyerhetők az adott üzenet vagy feladója veszélyességi szintjéről.

Hozzáadás az észlelt e-mail tárgyához – A sablon szerkesztésével módosíthatja a fertőzött e-mail tárgyában szereplő előtag formátumát.

ThreatSense paraméterek

A speciális víruskeresési beállítások lehetővé teszik a megtisztítási szintek, az ellenőrzési beállítások és az ellenőrzésből kizárt fájlkiterjesztések konfigurálását.

Adathalászat elleni védelem

Az Adathalászat elleni védelem további védelmet biztosít azokkal a nem szabályszerű webhelyekkel szemben, amelyek jelszavakat és más bizalmas információkat kísérelnek meg megszerezni. Az adathalászat elleni védelem alapértelmezés szerint engedélyezve van, és azt javasoljuk, hogy ne kapcsolja ki.

Frissítés

Ebben a szakaszban adhatja meg a frissítési források beállításait, például a használatban lévő frissítési szervereket és a hozzájuk tartozó hitelesítési adatokat. Az ESET Cyber Security speciális **frissítési** beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy az ESET Cyber Security elemre kattintva a macOS menüsávon, majd válassza ki a **Beállítások** lehetőséget.

Modul- és termékfrissítések

Modulfrissítések

Frissítés típusa

- **Rendszeres frissítés**. Ez az alapértelmezett frissítési típus, amely biztosítja, hogy a kereső-adatbázis és a termékmodulok automatikusan frissüljenek az ESET frissítési szerverekről.
- A **tesztelési mód** tartalmazza a legutóbbi hibajavításokat és észlelési módszereket, amelyek hamarosan elérhetők lesznek a nagyközönség számára is. Előfordulhat azonban, hogy nem mindig stabilak, ezért nem

ajánlott termelési környezetben használni őket.

- A **késleltetett frissítések** lehetővé teszik a speciális frissítési szerverekről való frissítést, amelyek a vírusadatbázisok új verzióit biztosítják legalább X órás késéssel (vagyis valós környezetben tesztelt és stabilnak tartott adatbázisok).

Modul-visszaállítás

Ha a keresőmotor egyik frissítése vagy a programmodulok feltehetően nem stabilak, illetve sérültek, visszaállhat az előző verzióra, és átmenetileg letilthatja a frissítéseket.

Modulok pillanatképének létrehozása

Az ESET Cyber Security pillanatfelvételeket készít a keresőmotorról és a programmodulokról a visszaállítás funkcióhoz való használatra. A moduladatbázis pillanatfelvételeinek létrehozásához hagyja engedélyezve a **Modulok pillanatképének létrehozása** funkciót. Ha a **Modulok pillanatképének létrehozása** funkció engedélyezve van, az első pillanatkép az első frissítés alkalmával jön létre. A következő 48 óra múlva jön létre. A **Helyben tárolt pillanatképek száma** mező meghatározza a keresőmotor pillanatképeinek tárolt számát.

> Amikor elérte a pillanatképek maximális mennyiségét (például három), a legrégebbi pillanatképet 48 óránként új pillanatfelvétel váltja fel. Az ESET Cyber Security for macOS visszaállítja a keresőmotor és a programmodulok frissítési verzióját a legrégebbi pillanatfelvételre.

Termékfrissítések

A termékfrissítések biztosítják, hogy mindig a legújabb termékverziót használja. Engedélyezze az **Automatikus frissítések** kapcsolót, hogy a termékfrissítések automatikusan települjenek a következő újraindításkor, és folyamatosan hozzáférjen a legújabb funkciókhoz és a lehető legmagasabb szintű védelemhez.

Elsődleges szerver és másodlagos szerver

Alapértelmezés szerint engedélyezve van az elsődleges és másodlagos frissítési szerverek közötti automatikus választás lehetősége. Mindkét szerver megadható, ha az automatikus kiválasztás kapcsolója le van tiltva.

Eszközök

Az ESET Cyber Security **Eszközök** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Feladatütemező

A feladatütemező segítségével beállíthat igény szerinti ellenőrzési feladatokat, amelyek automatikusan végbemennek egy meghatározott időpontban. Új ütemezett feladat létrehozásához vagy egy meglévő eltávolításához válassza ki a + vagy a − elemet. Azt is meghatározhatja, hogy mely napon vagy napokon ismétlődjön a feladat.

Naplófájlok

Naplózás részletessége

A naplózási részletesség azt határozza meg, hogy milyen részletesek legyenek a naplófájlok.

- **Kritikus figyelmeztetések** – Csak a kritikus hibákat tartalmazza (például **nem sikerült elindítani a vírusvédelmet**).
- **Hibák** – A **„Hiba a fájl letöltésekor”** és más kritikus hibák bejegyzése a naplóba.
- **Figyelmeztetések** – Kritikus hibák és figyelmeztető üzenetek bejegyzése a naplóba.
- **Tájékoztató bejegyzések** – Tájékoztató jellegű üzenetek rögzítése a naplóba (beleértve a sikeres frissítésekről szóló üzeneteket és a fent említett bejegyzéseket).
- **Diagnosztikai bejegyzések** – A fentiek mellett a program pontos beállításához szükséges információk megjelenítése.

Naplófájlok megtisztítása

Az ennél régebbi naplóbejegyzések törlése (nap) – A megadott napszámnál régebbi naplóbejegyzések automatikusan törlődnek.

Naplófájlok optimalizálása

Naplófájlok automatikus optimalizálása – Az opciót engedélyezve a naplófájlok optimalizálása automatikusan megtörténik, ha a fölösleges bejegyzések száma meghaladja a **Ha a fölösleges bejegyzések száma több mint (%)** mezőben megadott százalékos értéket. A teljesítmény és a naplók feldolgozási sebességének javítása érdekében a program eltávolítja az összes üres naplóbejegyzést. A teljesítményjavulás különösen a nagyszámú bejegyzést tartalmazó naplófájloknál látványos.

A proxyszerver beállításai

Itt adhatja meg a proxyszerver beállításait. Az itt definiált paramétereket minden olyan modul felhasználja, amely kapcsolódik az internethez.

A proxyszerver konfigurálása:

1. Engedélyezze a **Proxyszerver használata** opciót, majd írja be a proxyszerver címét a Proxyszerver mezőbe, a proxyszerver portszámát pedig a Port mezőbe.
2. Engedélyezze a **Közvetlen kapcsolat használata, ha nem érhető el proxy** funkciót, ha azt szeretné, hogy meg legyen kerülve a proxy, és közvetlenül az ESET-szerverekkel folyjon a kommunikáció.
3. Ha a proxyszerverrel folytatott kommunikációhoz hitelesítés szükséges, akkor engedélyezze **A proxyszerver hitelesítést igényel** funkciót, majd adjon meg egy érvényes **felhasználónevet** és **jelszót** a megfelelő mezőkben.

Felhasználói felület

Az ESET Cyber Security **felhasználói felület** speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombináció segítségével vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget.

Rendszerintegráció

Felhasználói felület elemei

Grafikus felhasználói felület megnyitásának engedélyezése a felhasználó számára – A beállítás letiltásával megakadályozhatja, hogy a felhasználók elérhessék a grafikus felhasználói felületet. Ez felügyelt környezetben, illetve olyan esetekben lehet hasznos, amikor meg kell őriznie a rendszererőforrásokat.

Ikon megjelenítése a menüsáv extrái között – A beállítás letiltásával eltávolíthatja az ESET Cyber Security ikonját a macOS menüsáv extrái közül (a képernyő tetején).

Értesítések

Értesítések megjelenítése az asztalon – Az asztali értesítések (például sikeres frissítési üzenetek, víruskeresési feladatok befejezése vagy új kártevők) a macOS menüsor melletti kis előugró ablakban jelennek meg. Ha engedélyezve van, az ESET Cyber Security tájékoztatja, ha új esemény következik be.

Alkalmazásállapotok

Itt adhatja meg, hogy mely alkalmazásállapotok jelenjenek meg az ESET Cyber Security-termékben. Ha az **Állapot megjelenítése** kapcsoló le van tiltva egy probléma jelentésekor, az ESET Cyber Security alkalmazás megőrzi a zöld **A védelme biztosított** állapotot.

Védelmek

Az alkalmazás főablakában található **Védelmek** opció lehetővé teszi a számítógép, az internet és az e-mailek védelmi szintjének beállítását. Mind a Számítógép-védelem, mind a Web- és e-mail-védelem szakasz védelmi modulokat tartalmaz, amelyek engedélyezhetők vagy letilthatók. Azt javasoljuk, hogy az összes modult engedélyezze, hogy teljes mértékben kiaknázhassa az ESET Cyber Security funkcióit és biztonságban tartsa a számítógépét.

A számítógép védelme

A számítógép védelmi konfigurációja a **Védelmek** > **Számítógép** szakaszban található. Ez az ablak a **Valós idejű fájlrendszervédelem** és az **ESET LiveGrid® megbízhatósági rendszer** modul állapotát jelzi. Azt javasoljuk, hogy mindkét modult engedélyezze, mivel bármelyik kikapcsolása csökkentheti a számítógép védelmi szintjét.

A váltóra kattintva engedélyezheti vagy letilthatja az **Automatikus frissítés** funkciót a **Frissítés** szakaszban. Ha az Automatikus frissítés engedélyezve van, az ESET Cyber Security megkeresi a legújabb termékfrissítéseket, és automatikusan letölti őket.

Webhozzáférés- és e-mail védelem

A webhozzáférés- és e-mail védelem eléréséhez a főmenüben kattintson a **Védelmek** > **Web és e-mail** elemre. Az egyes modulok fejlettebb beállításainak kezeléséhez nyissa meg az **Alkalmazásbeállításokat** a cmd+, billentyűkombinációval vagy a macOS menüsávján az ESET Cyber Security elemre kattintva, majd válassza ki a **Beállítások** lehetőséget. A Web- és e-mail-védelemben a következő védelmi modulok érhetők el:

- **Web** – A böngészők és a távoli szerverek közötti kommunikáció figyelése.
- **Adathalászat elleni védelem** – A webhelyekről és tartományokból származó minden potenciális adathalászati támadást letilt.
- **E-mail** – A POP3 és az IMAP protokollon keresztül érkező e-mailes kommunikáció szabályozását biztosítja.

Ellenőrzési kivételek
Az ESET Cyber Security nem ellenőrzi a következő titkosított protokollokat: HTTPS, POP3S és IMAPS.

Adathalászat elleni védelem

Az adathalászat olyan bűncselekmény, amely pszichológiai manipulációt alkalmaz (vagyis bizalmas információk kiszolgáltatására veszik rá a felhasználót). Az adathalászattal megszerezni kívánt bizalmas adatok közé tartoznak többek között a bankszámlaszámok, a hitelkártyaszámok, a PIN-kódok, illetve a felhasználónevek és a jelszók. Az adathalászatról további információt az ESET-szójegyzékben talál.

Azt javasoljuk, hogy ne kapcsolja ki az adathalászat elleni védelmet (Védelmek >Web és e-mail >Adathalászat elleni védelem). A rendszer a veszélyes webhelyekről vagy tartományokból érkező minden lehetséges adathalászati támadást letilt, és a támadásról figyelmeztető értesítést jelenít meg.

Annak teszteléséhez, hogy az adathalászat elleni védelem működik-e, olvassa el az AMTSO tesztoldalát.

Vírus- és kémprogramvédelem

A vírusvédelem a lehetséges fenyegetéseket jelentő fájlok módosításával megakadályozza a kártevők bejutását a rendszerbe. Ha a program kártékony kódot észlel, a víruskereső modul letiltja, majd megtisztítja, törli vagy karanténba helyezi a hordozó fájlt.

Valós idejű fájlrendszervédelem

A valós idejű fájlrendszer-védelem ellenőrzi az összes adathordozó-típust, és különböző események alapján elindítja az ellenőrzést. Az ESET LiveGrid® technológia (a ThreatSense keresőmotor beállításai című témakörben ismertetjük) használatakor a valós idejű fájlrendszervédelem eltérő lehet az újonnan létrehozott fájlok és a meglévő fájlok esetében. Nagyobb fokú felügyelet érhető el az újonnan létrehozott fájlok esetén.

A valós idejű fájlrendszer-védelem speciális beállításainak módosításához nyissa meg az **Alkalmazásbeállításokat** a cmd+, használatával, vagy kattintson az **ESET Cyber Security** elemre a macOS menüsávon, majd válassza ki a **Beállítások** > **Fájlrendszervédelem** lehetőséget.

Alapértelmezés szerint a szolgáltatás az összes fájlt ellenőrzi **fájlok megnyitásakor** és **fájlok létrehozásakor**. Az ESET azt javasolja, hogy tartsa meg az alapértelmezett beállításokat, mert maximális szintű valós idejű védelmet biztosítanak a számítógép számára. A valós idejű védelem indítása a rendszerindításkor történik, és folyamatos ellenőrzést biztosít. Különleges esetekben (ha például ütközés lép fel egy másik valós idejű keresővel) leállíthatja a valós idejű védelmet a fő programablakból (kattintson a **Védelmek** > **Számítógép** elemre, majd kapcsolja ki a **Valós idejű fájlrendszervédelmet**).

A következő típusú adathordozókat zárhatja ki a Real-time ellenőrzésből:

- **Helyi meghajtók** – rendszermeghajtók
- **Cserélhető adathordozók** – CD-k, DVD-k, USB-tárolóeszközök, Bluetooth-eszközök stb.
- **Hálózati adathordozók** – minden csatlakoztatott meghajtó

Bizonyos folyamatokat is kizárhat az ellenőrzésből.

Ajánlott az alapértelmezett beállításokat használni és csak bizonyos esetekben módosítani az ellenőrzésből kizárandó adathordozókat, például amikor egyes adathordozók ellenőrzése jelentősen lassítja az adatátvitelt.

Mikor érdemes módosítani a valós idejű védelem beállításain?

A valós idejű védelem elengedhetetlen az ESET Cyber Security segítségével fenntartott biztonságos rendszerhez. Legyen körültekintő a valós idejű védelem paramétereinek módosításakor. Azt javasoljuk, hogy a paramétereket

csak bizonyos esetekben módosítsa, például akkor, ha ütközés áll fenn egy adott alkalmazással.

Telepítése után az ESET Cyber Security minden beállítást optimalizál, hogy a lehető legmagasabb szintű védelmet biztosítsa a rendszer számára.

Valós idejű védelem ellenőrzése

Ha meg szeretne bizonyosodni arról, hogy a valós idejű védelem működik és képes a vírusok észlelésére, töltse le az eicar.com nevű tesztfájlt, és próbálj ki, hogy az ESET Cyber Security felismeri-e kártevőként. A tesztfájl egy ártalmatlan, az összes víruskereső program által felismerhető speciális fájl. Az Európai Institute for Computer Antivirus Research (EICAR intézet) hozta létre a fájlt a vírusirtó programok teszteléséhez.

Teendők, ha a valós idejű védelem nem működik

Itt a valós idejű védelem használata során előforduló problémákról és azok elhárítási módjáról tájékozódhat.

A valós idejű védelem le van tiltva

Ha egy felhasználó véletlenül letiltotta a valós idejű védelmet, akkor aktiválja újra a funkciót. A valós idejű védelem főmenüből történő újraaktiválásához kattintson a **Valós idejű fájlrendszervédelem** kapcsolóra az engedélyezéséhez. Alternatív megoldásként lépjen az alkalmazásbeállítások ablakába, majd kattintson a**Valós idejű védelem** kapcsolóra a valós idejű fájlrendszervédelem engedélyezéséhez.

A valós idejű védelem nem észleli és nem tisztítja meg a fájlokat a fertőzésektől

Győződjön meg arról, hogy a számítógépen nincs másik víruskereső program telepítve. Ha egyszerre két valós idejű védelmi szolgáltatást nyújtó eszköz van engedélyezve, azok ütközésbe kerülhetnek egymással. Ajánlatos az esetleges további víruskereső programokat eltávolítani a rendszerből.

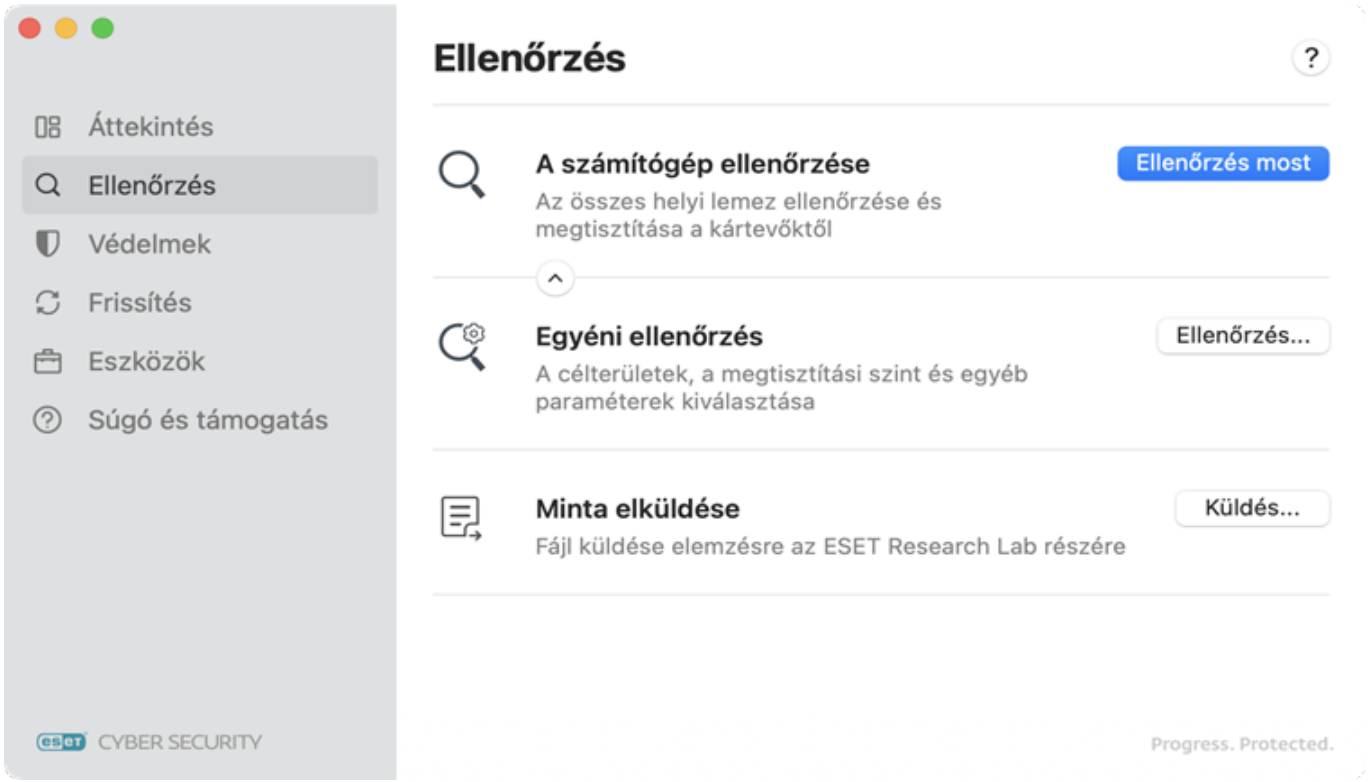
A valós idejű védelem nem indul el

Ha a rendszer indításakor nem indul el valós idejű védelem, akkor lehet, hogy ütközések állnak fenn más programokkal. Ha a valós idejű védelem nem indul el, vegye fel a kapcsolatot az ESET műszaki terméktámogatásával.

Kézi indítású számítógép-ellenőrzés

Ha azt gyanítja, hogy számítógépe fertőzött (mert rendellenesen viselkedik), válassza ki a **Ellenőrzés**lehetőséget az alkalmazás főablakában, majd kattintson az **Ellenőrzés most** gombra a számítógépen található fertőzések vizsgálatához. A maximális védelem érdekében rendszeresen futtasson számítógépes ellenőrzést a rutinszerű biztonsági intézkedések részeként, ne pedig csak akkor, ha fertőzésre gyanakszik. A rendszeres ellenőrzéssel felismerhetők az olyan fertőzések is, amelyeket a valós idejű víruskereső nem észlelt a lemezre mentésükkor. Ez akkor fordulhat elő, ha a fertőzés időpontjában a valós idejű víruskereső ki volt kapcsolva, illetve a keresőmodulok nem voltak naprakészek.

Az ESET azt javasolja, hogy havonta legalább egyszer futtasson kézi indítású számítógép-ellenőrzést.



Az ellenőrzést az alkalmazásbeállítások **Eszközök** > **Feladatütemező** szakaszában konfigurálhatja ütemezett feladatként.

Egyéni ellenőrzés

Az alkalmazás főablakának bal oldali menüjében keresse meg az **Ellenőrzés** elemet, kattintson a nyíl ikonra az **Egyéni ellenőrzés** és a **Minta elküldése** opció megjelenítéséhez.

Egyéni ellenőrzés

Ez az opció akkor optimális megoldás, ha be szeretné állítani az ellenőrzés paramétereit (például a célterületeket vagy az ellenőrzési módszereket). Az egyéni ellenőrzés futtatásának előnye a paraméterek részletes beállításának lehetősége.

Kattintson az **Ellenőrzés** gombra az **Egyéni ellenőrzés** szakaszban az egyéni ellenőrzési ablak megnyitásához. Húzza át az ellenőrizni kívánt fájlokat az ablak kijelölt területére. Megadhat egy **ellenőrzési célterületet** is a **Böngészés** gombra kattintva, majd a felvenni kívánt mappához vagy fájlokhoz lépve.

A hárompontos menüikonra kattintva további lehetőségeket jeleníthet meg: **Ellenőrzési profil kiválasztása** és **Kizárások beállítása**.

Ellenőrzési profil kiválasztása

Itt kiválaszthatja a kívánt **ellenőrzési profilt** és beállíthatja a **megtisztítási szintet**.

Ellenőrzési profilok

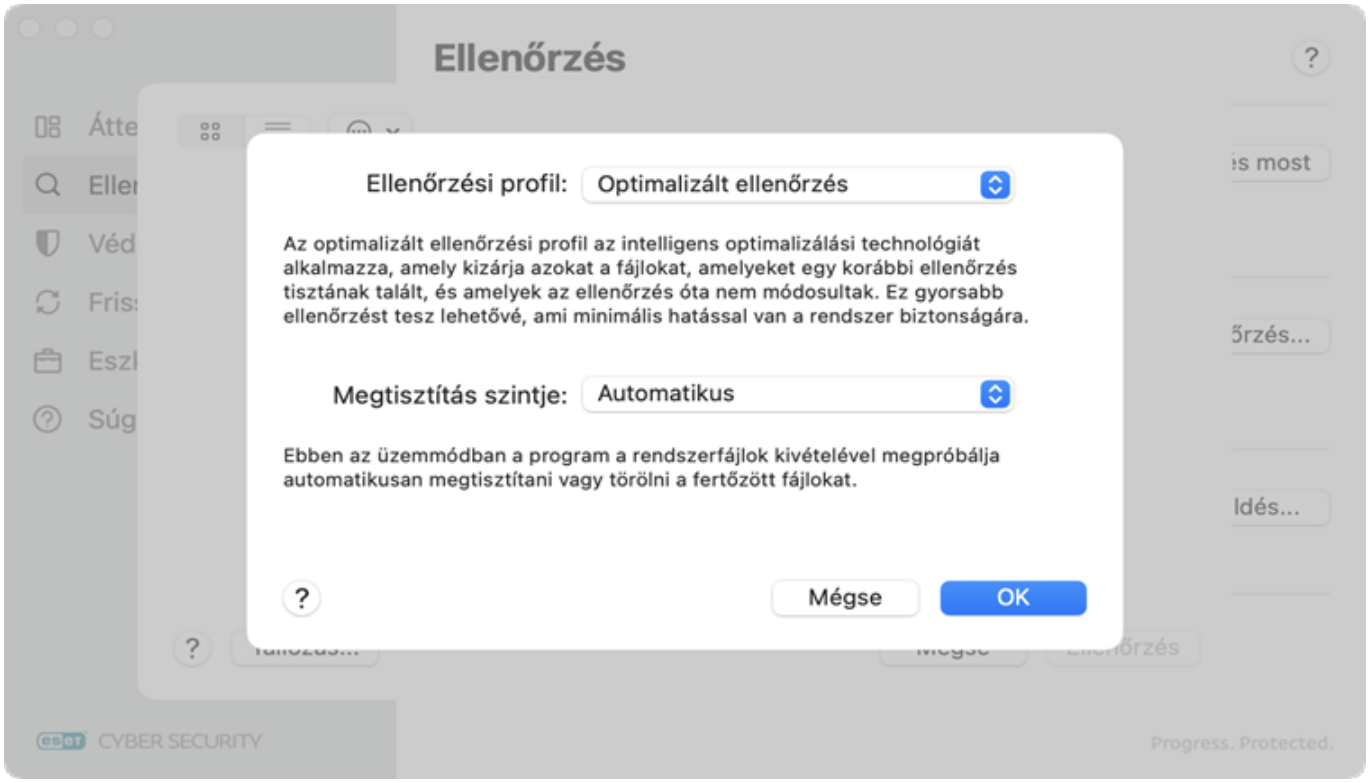
Az **optimalizált ellenőrzéssel** gyorsan elindítható a számítógép ellenőrzése, és felhasználói beavatkozás nélkül megtisztíthatók a fertőzött fájlok. Fő előnye az egyszerű kezelhetősége anélkül, hogy részletesen be kellene

állítani az ellenőrzést. Az optimalizált ellenőrzés az összes mappa minden fájlját ellenőrzi, és automatikusan megtisztítja vagy törli az észlelt kártevőket tartalmazó fájlokat. Az intelligens ellenőrzési profil az Intelligens optimalizálási technológiát alkalmazza, amely kizárja azokat a fájlokat, amelyeket egy korábbi ellenőrzés tisztának talált, és amelyek az ellenőrzés óta nem módosultak.

A **mélyreható ellenőrzési** profil nem használja az intelligens optimalizálást, így egyetlen fájl sincs kizárva az ellenőrzésből.

Automatikus megtisztítás szintje

Itt kiválaszthatja, hogy a kereső hogyan kezelje a fertőzött fájlokat. Ha többet szeretne megtudni a megtisztítási szintekről, olvassa el a Megtisztítás című részt.



Kizárások beállítása

Az ellenőrzésből kizárni kívánt fájlok vagy mappák hozzáadása. Húzza a kizárni kívánt fájlokat a megjelenített ablak kijelölt területére.

> A számítógép **egyéni ellenőrzése** a víruskereső programok használatában tapasztalattal rendelkező felhasználóknak ajánlott.

Minta elküldése

Ez az opció lehetővé teszi, hogy fájlt küldjön a ESET kutatólaborjába elemzés céljából. A mintafájl beküldésével kapcsolatos további részletekért tekintse meg a Minta elküldése című részt.

A ThreatSense keresőmotor beállításai

A ThreatSense egy szabadalmaztatott ESET-technológia, amely számos összetett kártevő-felismerési módszer együtteséből áll. Ez a proaktív technológia az új kártevők elterjedésének korai szakaszában is védelmet nyújt. A ThreatSense számos módszer (kódelemzés, kódemuláció, általános definíciók stb.) összehangolt alkalmazásával jelentős mértékben növeli a rendszer biztonságát. A ThreatSense technológiával sikeresen elkerülhetők a rootkitek okozta fertőzések is.

A ThreatSense technológia beállítási lehetőségeivel több ellenőrzési paraméter megadható, például az alábbiak:

- Az ellenőrizendő fájltípusok és kiterjesztések
- Különböző észlelési módszerek kombinációja
- A megtisztítás mértéke stb.

A ThreatSense-konfigurációkat az Alkalmazásbeállításokban módosíthatja (nyissa meg a cmd+, billentyűkombinációval, vagy a macOSmenüsávján kattintson az ESET Cyber Security elemre, majd válassza ki a **Beállítások** lehetőséget. A különböző biztonsági körülmények eltérő konfigurációkat igényelhetnek. Ennek érdekében a ThreatSense külön beállítható az alábbi védelmi modulokhoz:

- Valós idejű fájlrendszervédelem
- Kártevő-ellenőrzések
- Webhozzáférés-védelem
- E-mail védelem

A ThreatSense paraméterei minden modulhoz speciálisan optimalizáltak, és módosításuk jelentősen befolyásolhatja a rendszer működését. Ha például engedélyezi, hogy a program mindig ellenőrizze a futtatás közbeni tömörítőket, vagy bekapcsolja a kiterjesztett heurisztikát a Valós idejű fájlrendszervédelem modulban, a rendszer lelassulhat. Ezért a Számítógép ellenőrzése modul kivételével az összes modul esetében ajánlott a ThreatSense paramétereit az alapértelmezett értékeken hagyni.

Ellenőrzési beállítások

Az ellenőrzési beállítások az Alkalmazásbeállítások lapon konfigurálhatók a következő védelmi moduloknál: Valós idejű fájlrendszervédelem, Kártevőellenőrzések, Webhozzáférés-védelem és E-mail-védelem. A védelmi modulok mindegyikéhez kiválaszthatja a rendszerellenőrzés során alkalmazott módszereket. A választható lehetőségek az alábbiak:

- **Heurisztika** – A heurisztika a programok (kártékony) tevékenységének felismerésére szolgáló algoritmust használ. Fő előnye, hogy a korábban még nem létező, új kártevő szoftvereket is képes felismerni.

- **Kiterjesztett heurisztika** – A kiterjesztett heurisztika az ESET saját, a számítógépes férgek és trójai programok felismerésére optimalizált, magas szintű programozási nyelveken fejlesztett heurisztikus algoritmusa. A kiterjesztett heurisztikának köszönhetően a program észlelési képessége jelentősen megnőtt.

• **Optimalizálás** – Ha ez engedélyezve van, az Optimalizálás biztosítja a leghatékonyabb ellenőrzési szintet, miközben fenntartja a legmagasabb ellenőrzési sebességet. A különböző védelmi modulok intelligensen ellenőriznek, különböző ellenőrzési módszereket alkalmazva bizonyos fájltípusokra.

Automatikus megtisztítás szintje

A megtisztítási szintek az Alkalmazásbeállítások lapon konfigurálhatók a következő védelmi moduloknál: Valós idejű fájlrendszervédelem, Kártevőellenőrzések, Webhozzáférés-védelem és E-mail-védelem. Az egyes szintek határozzák meg, hogy a kereső hogyan tisztítja meg a fertőzött fájlokat. A következő megtisztítási szintek állnak rendelkezésre:

• **Nincs megtisztítás** – A fertőzött fájlok megtisztítása nem megy végbe automatikusan. A program megjelenít egy figyelmeztető ablakot, és a felhasználó választhat a műveletek közül.

• **Normál megtisztítás** – A program megkísérli a fertőzött fájlok automatikus megtisztítását vagy törlését. Ha a megfelelő művelet automatikus kiválasztására nincs lehetőség, felkínál néhány utóműveletet. Az utóműveletek akkor is megjelennek, ha egy előre definiált művelet nem hajtható végre.

• **Automatikusan megtisztít** – A program megtisztítja vagy törli az összes fertőzött fájlt (a tömörített fájlokat is beleértve). A rendszerfájlok kivételt képeznek. Ha egy fájl nem tisztítható meg, a program értesíti erről a felhasználót, és kéri, hogy adja meg a végrehajtandó művelet típusát.

• **Aprólékos megtisztítás** – Ebben az üzemmódban a program megpróbálja automatikusan megtisztítani vagy törölni az összes fertőzött fájlt.

• **Törlés** – Az összes fertőzött fájl törlése.

Tömörített fájlok ellenõrzése
A Normál megtisztítási szint használata esetén a program csak akkor törli a kártevőt tartalmazó teljes tömörített fájlt, ha az abban lévő összes fájl fertőzött. A program nem törli a tömörített fájlt, ha az szabályos, valamint fertőzött fájlokat is tartalmaz. Ha az Automatikusan megtisztít módban a program egy fertőzött tömörített fájlt észlel, akkor is törli a teljes tömörített fájlt, ha nem fertőzött fájlokat is tartalmaz.

Kivételek

A kiterjesztés a fájlnév ponttal elválasztott része. A kiterjesztés meghatározza a fájl típusát és tartalmát. Az ellenőrzésből kizárandó fájlok típusait az Alkalmazásbeállítások lapon határozhatja meg a következő védelmi moduloknál:

- Valós idejű fájlrendszervédelem
- Kártevő-ellenőrzések
- Webhozzáférés-védelem
- E-mail védelem

A program alapértelmezés szerint kiterjesztéstől függetlenül ellenőrzi az összes fájlt. Az ellenőrzésből kizárt fájlok listájára bármilyen kiterjesztés felvehető. A plusz [+] és mínusz [−] gombbal engedélyezheti vagy letilthatja adott kiterjesztésű fájlok ellenőrzését.

A fájlok ellenőrzésből való kizárására akkor lehet szükség, ha bizonyos fájltípusok ellenőrzése akadályozza a program megfelelő működését. Például tanácsos kizárni a log, a cfg és a tmp fájlokat. A fájlkiterjesztéseket a következő formátumban kell megadni:

- log
- cfg
- tmp

Frissítés

Az ESET Cyber Security rendszeres frissítésével tartható fenn a biztonság maximális szintje. A Frissítés modul a legfrissebb keresőmodulok letöltésével biztosítja, hogy a program mindig naprakész legyen.

A főmenü **Frissítés** parancsára kattintva megjelenítheti az ESET Cyber Security aktuális frissítési állapotát, beleértve az utolsó sikeres frissítés dátumát és időpontját, valamint azt, hogy szükség van-e frissítésre. Új frissítések kereséséhez kattintson a **Frissítés keresése** gombra. Ha rendelkezésre áll egy termékfrissítés, megjelennek az aktuális és az elérhető verzió adatai, valamint a frissítés mérete és kiadási dátuma. Választhat a **Frissítés most** és a **Frissítés újraindításkor** műveletek közül. Az egyes termékverziókkal kapcsolatos további részletek megtekintéséhez kattintson a **Változásnapló megtekintése** hivatkozásra.

Az ESET Cyber Security frissítése új verzióra

A maximális védelem biztosításához fontos, hogy az ESET Cyber Security legújabb verzióját telepítse. Annak érdekében, hogy mindig rendelkezzen a legújabb verzióval, ajánlott bekapcsolni **a termék automatikus frissítéseit** (fő alkalmazásmenü > **Védelmek** > **Számítógép**).

Eszközök

Az **Eszközök** lapon található modulok segítik a program adminisztrációjának egyszerűsítését, és további lehetőségeket kínálnak a tapasztalt felhasználóknak. A lapon az alábbi eszközök láthatók:

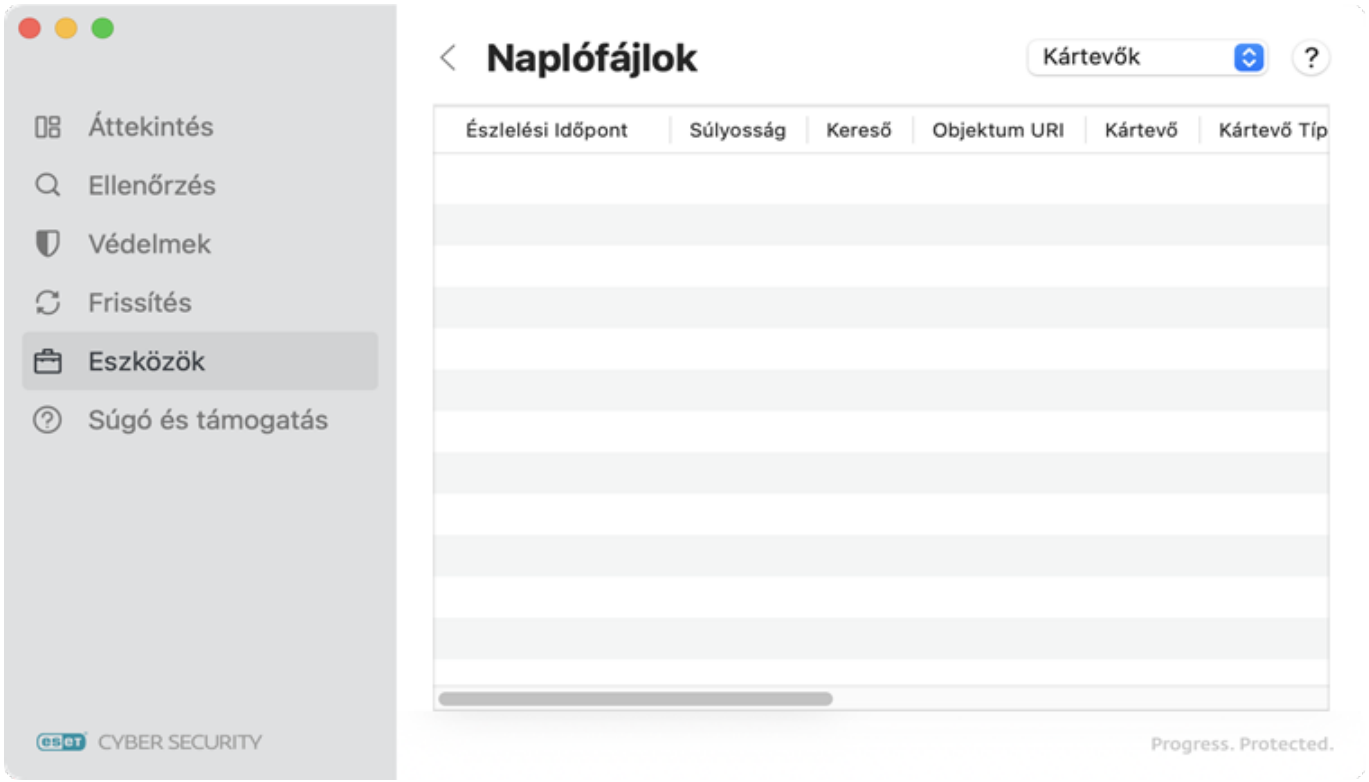
- Naplófájlok
- Karantén

Naplófájlok

A Naplófájlok lap a fontos programeseményekről tájékoztatást, az észlelt kártevőkről áttekintést nyújt. A naplózás elengedhetetlen a rendszerelemzéshez, a kártevők észleléséhez és a hibaelhárításhoz. A naplózás a háttérben folyik aktívan, felhasználói beavatkozás nélkül. Az információkat az aktuális naplórészletességi beállításoknak megfelelően rögzíti. A szöveges üzenetek és a naplófájlok közvetlenül az ESET Cyber Security-programkörnyezetből is megtekinthetők, és archiválhatók a naplók.

A naplófájlok az ESET Cyber Security főmenüjéből érhetők el az **Eszközök** > **Naplófájlok** lehetőséget választva. Jelölje ki a kívánt naplótípust az ablak jobb felső részén található legördülő listában. A választható naplók az alábbiak:

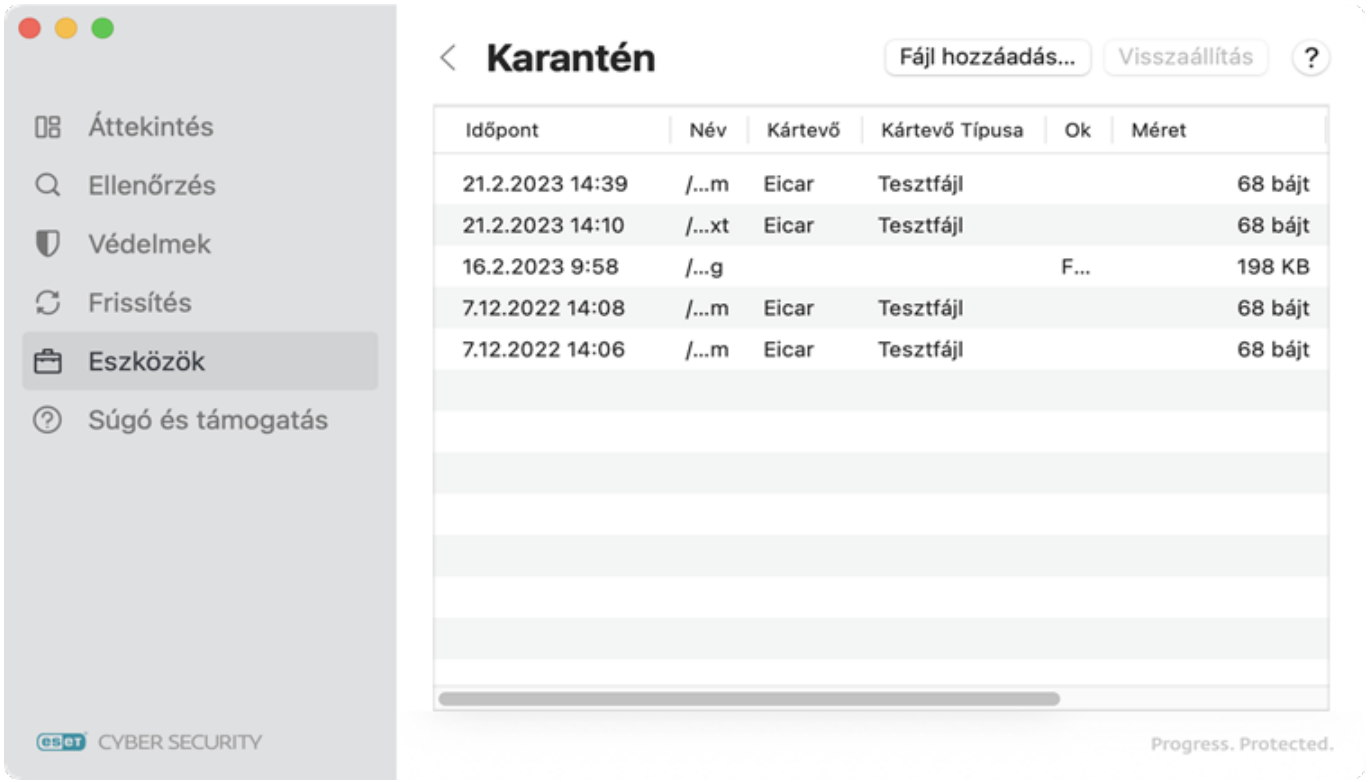
- **Észlelések** – A fertőzések észlelésével kapcsolatos eseményekre vonatkozó információk.
- **Számítógép ellenőrzése** – Ebben a naplóban megjelenítheti az összes befejezett ellenőrzés eredményét. Az egyes bejegyzésekre duplán kattintva megjelennek az adott kézi indítású számítógép-ellenőrzés részletes adatai.
- **Események** – Segít a rendszergazdáknak és a felhasználóknak a problémák elhárításában. A program az ESET Cyber Security által végrehajtott összes fontos műveletet rögzíti az eseménynaplókban.
- **Szűrt webhelyek** – A Webhozzáférés-védelem által blokkolt webhelyek listája. . Ezekben a naplókban látható az idő, az URL-cím, az állapot, az IP-cím, a felhasználó és az adott webhely felé kapcsolatot megnyitó alkalmazás.
- **Elküldött fájlok** – Az elemzésre elküldött minták rekordjait tartalmazza.



Karantén

A karantén fő célja a fertőzött fájlok biztonságos tárolása. A fájlokat akkor kell a karanténba helyezni, ha nem tisztíthatók meg, ha törlésük kockázattal jár vagy nem ajánlott, illetve ha az ESET Cyber Security tévesen észlelte őket.

A karanténmappában lévő fájlokat egy táblázatban láthatja, amely jelzi a karanténba helyezés dátumát és időpontját, a fertőzött fájl eredeti helyének elérési útját, a fájl bájtban megadott méretet, a karanténba helyezés okát (például a felhasználó vette fel) és a fertőzések számát (például azt, hogy egy több fertőzést is hordozó tömörített fájlról van-e szó). A karanténba helyezett fájlokat tartalmazó karanténmappa (*/Library/Application Support/Eset/Security/Cache/Quarantine*) az ESET Cyber Security eltávolítása után is a rendszerben marad. A karanténba helyezett fájlok tárolása biztonságos titkosított formában történik, és az ESET Cyber Security telepítése után ismét visszaállíthatók.



Karantén fájlok

Az ESET Cyber Security automatikusan karanténba helyezi a törölt fájlokat (ha nem tiltotta le ezt a beállítást a riasztási ablakban). Kattintson a **Fájl hozzáadása** gombra a gyanús fájlok manuális karanténba helyezéséhez. Manuálisan húzza át a fájlt vagy a mappát úgy, hogy a fájlra vagy mappára kattint, az egérmutatót a megjelölt területre viszi, miközben az egér gombját lenyomva tartja, majd engedje fel az egér gombját.

Visszaállítás a karanténból

Jelölje ki a karanténba helyezett fájlt, majd kattintson a **Visszaállítás** gombra az eredeti helyére történő visszaállításához. Ez a funkció úgy is elérhető, hogy a Control billentyűt lenyomva tartva kattint (vagy a jobb gombbal kattint) egy adott fájlra a **Karantén** ablakban, majd a **Visszaállítás** elemre kattint. A helyi menüben megtalálható a **Visszaállítás megadott helyre** menüpont is, amellyel a törlés helyétől eltérő mappába is visszaállíthatók a fájlok.

Fájl elküldése a karanténból

Ha karanténba helyezett egy, a program által nem észlelt gyanús fájlt, vagy ha a szoftver tévesen jelölt meg fertőzöttként (például a kód heurisztikus elemzésével), majd helyezett a karanténba egy fájlt, kérjük, küldje el azt az ESET víruslaborjába. A karanténban lévő fájl elküldéséhez a Control billentyűt lenyomva tartva kattintson (vagy a jobb gombbal kattintson) a fájlra, majd válassza ki a **Minta elküldése** menüpontra a helyi menüben. A mintafájl beküldésével kapcsolatos további részletekért tekintse meg a Minta elküldése című részt.

Minta beküldése elemzésre

Az alkalmazás főablakának bal oldali menüjében válassza ki az **Ellenőrzés** elemet, kattintson a nyíl ikonra a **Minta elküldése** opció megjelenítéséhez.

Ez az opció lehetővé teszi, hogy kiválasszon egy gyanúsan viselkedő fájlt a számítógépén vagy egy gyanús internetes webhelyet, és elküldheti elemzésre az ESET kutatólaborjába.

Mielőtt leadna mintákat az ESET-nek
A beküldött mintának meg kell felelnie legalább egynek az alábbi feltételek közül:
- Az Ön által használt ESET-termék nem észleli a mintát
- A program tévesen kártevőként észlelte a mintát
- A minta nem személyes fájl; az ESET nem fogad el személyes fájlokat (ha azt szeretné, hogy az ESET ellenőrizze a kártevők jelenlétét bennük) mintaként, és az ESET kutatólaborja nem hajt végre egyéni ellenőrzést a felhasználók számára.

Kattintson a **Küldés** gombra az elemzésre elküldeni kívánt fájl megadásához. A **Minta elküldése elemzésre** űrlapon adja meg a következőket:

- **Beküldés oka** – válasszon a helyi menüből.
- **Minta** – adja meg az elküldeni kívánt fájl elérési útját, vagy húzza a fájlt a megjelölt területre.
- **Kapcsolat**– Adja meg elérhetőségét, hogy kapcsolatba léphessünk Önnel, ha további információra van szükségünk a fájlról; nem kell megadnia az e-mail-címét, ha engedélyezi az Elküldés névtelenül kapcsolót.

A **Tovább** gombra kattintva eljuthat az utolsó lépéshez, ahol további információkat adhat meg a mintafájlról, például a kártevő általi fertőzésre utaló jeleket vagy hibajelenségeket és a fájl eredetét. További információk megadásával elősegíti, hogy laboratóriumaink azonosítsák és feldolgozzák a mintákat.

Előfordulhat, hogy az ESET nem ad választ
Az ESET csak akkor válaszol, ha további információkra van szüksége. Szervereink fájlok tízezreit fogadják naponta, így nem tudunk válaszolni minden egyes üzenetre.
Ha a minta valóban egy kártékony alkalmazás vagy webhely, bekerül a vírusdefiníciós adatbázis valamelyik későbbi ESET-frissítésébe.

Végfelhasználói licencszerződés

Hatályos 2021. október 19-től.

FONTOS: Kérjük, hogy a letöltés, telepítés, másolás vagy használat előtt olvassa el figyelmesen a termék használatára vonatkozó alábbi feltételeket. **A SZOFTVER LETÖLTÉSÉVEL, TELEPÍTÉSÉVEL, MÁSOLÁSÁVAL VAGY HASZNÁLATÁVAL ÖN ELFOGADJA EZEKET A FELTÉTELEKET, ÉS TUDOMÁSUL VESZI AZ ADATVÉDELMI SZABÁLYZATOT.**

Végfelhasználói licencszerződés

Jelen végfelhasználói licencszerződés („a Szerződés”) alapján, amely egyfelől az ESET, spol. s r. o. (székhelye: Einsteinova 24, 85101 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532; („ESET” vagy „a Gyártó”), másfelől Ön mint természetes vagy

jogi személy („Ön” vagy „a Végfelhasználó”) között jött létre, Ön jogosult a jelen Szerződés 1. pontjában meghatározott szoftver használatára. A jelen Szerződés 1. pontjában meghatározott Szoftver az alábbiakban megadott feltételeknek megfelelően adathordozón tárolható, e-mailben küldhető, az internetről vagy a Gyártó szervereiről letölthető, illetve más forrásokból beszerezhető.

JELEN SZERZŐDÉS VÉGFELHASZNÁLÓI JOGOSULTSÁGOKRA VONATKOZIK, ÉS NEM ÉRTÉKESÍTÉSI SZERZŐDÉS. Az értékesítési csomagban található szoftvermásolat és a fizikai adathordozó, valamint a jelen Szerződés alapján a Végfelhasználó által készíthető bármely másolat továbbra is a Gyártó tulajdonát képezi.

Ha az „Elfogadom” vagy egyéb, jóváhagyásra szolgáló gombra kattint a Szoftver telepítése, letöltése, másolása vagy használata közben, illetve bármilyen alkalmazásáruházból való telepítésekor, azzal elfogadja a jelen Szerződés feltételeit és jóváhagyja az Adatvédelmi szabályzatot. Ha nem ért egyet a Szerződés és vagy az Adatvédelmi szabályzatot bármely rendelkezésével, azonnal kattintson a megszakításra szolgáló gombra, szakítsa meg a letöltést vagy a telepítést, illetve semmisítse meg vagy küldje vissza a Szoftvert, a telepítési adathordozót, valamint a kapcsolódó dokumentációt és a vásárlási számlát a Gyártónak vagy abba az üzletbe, ahol a Szoftvert beszerezte.

ÖN ELFOGADJA, HOGY A SZOFTVER HASZNÁLATÁVAL KIFEJEZI, HOGY A JELEN SZERZŐDÉST ELOLVASTA, MEGÉRTETTE, ÉS RENDELKEZÉSEIT ÖNMAGÁRA NÉZVE KÖTELEZŐ ÉRVÉNYŰNEK ISMERTE EL.

1. **Szoftver**. A jelen Szerződésben a „Szoftver” kifejezés a következőt jelenti: (i) a jelen Szerződéshez mellékelt számítógépes program és annak összes komponense; (ii) a lemezek, CD-ROM-ok, DVD-k, e-mailek és mellékleteik vagy más adathordozók tartalma, amelyhez a jelen Szerződés tartozik, beleértve az adathordozón nyújtott vagy e-mailben küldött, illetve interneten letölthető Szoftver tárgykódját; (iii) minden kapcsolódó írásbeli használati utasítás vagy a Szoftverhez tartozó egyéb dokumentáció, beleértve többek között a szoftver bármilyen leírását, specifikációját, tulajdonságainak vagy működésének ismertetését, a működési környezet leírását, amelyben a Szoftvert használják, a Szoftver telepítési vagy használati útmutatóit, a Szoftver megfelelő használatára vonatkozó bármilyen leírást („Dokumentáció”); (iv) a Szoftver másolatai, lehetséges hibáinak javításai, kiegészítései, bővítményei, módosított verziói, összetevőinek frissítései (ha vannak), amelyekhez a Gyártó a jelen Szerződés 3. pontja szerint Önnek használati engedélyt adott. A Szoftver kizárólag végrehajtható tárgykód formájában szerezhető be.

2. **Telepítés, Számítógép és Licenckulcs**. Az adathordozón biztosított, e-mailben küldött vagy az internetről, illetve a Gyártó szervereiről letöltött vagy más forrásból megszerzett Szoftvert telepíteni kell. A Szoftvert megfelelően konfigurált számítógépre kell telepíteni, amely legalább a Dokumentációban közölt követelményeknek megfelel. A telepítési módszer leírása a Dokumentációban található. A Szoftvert futtató Számítógépre nem telepíthető olyan számítógépes program vagy hardver, amely kedvezőtlen hatással lehet a Szoftverre. A Számítógép olyan hardver – korlátozás nélkül ideértve a személyi számítógépeket, laptopokat, munkaállomásokat, tenyérszámítógépeket, okostelefonokat, kézi elektronikus készülékeket, illetve egyéb elektronikus eszközöket –, amelyre a Szoftver készült, és amelyre telepíteni fogják, illetve amelyen használni fogják a Szoftvert. A Licenckulcs szimbólumok, betűk, számok, illetve speciális jelek egyedi sorozata, amelyet a Végfelhasználó kap annak érdekében, hogy legálisan használhassa a Szoftvert vagy annak egy adott verzióját, illetve kiterjeszthesse a Licencet a jelen Szerződéssel összhangban.

3. **Licenc**. Amennyiben Ön elfogadja a jelen Szerződés rendelkezéseit, az érvényességi időn belül megfizeti a licencdíjat, és megfelel az itt előírt összes feltételnek, a Gyártó az alábbi jogokat (a továbbiakban „a Licenc”) biztosítja az Ön számára: a) Telepítés és használat:

a) **Telepítés és használat.** Nem kizárólagos és nem átruházható jogot szerez a Gyártótól arra, hogy a Szoftvert egy számítógép merevlemezére vagy más tartós adattárolásra alkalmas adathordozóra telepítse, a Szoftvert számítógépes rendszerek memóriájába telepítse, és ott tárolja, valamint megjelenítse azt.

b) **A licencek számának kikötése.** A Szoftver használatára vonatkozó jogosultságot a Végfelhasználók száma

határozza meg. Egy Végfelhasználónak kell tekinteni a következőt: (i) a Szoftver telepítése egyetlen számítógépre, vagy (ii) ha a licenc terjedelme az e-mail postafiókok számához kötött, a Végfelhasználó egy olyan számítógép-használót jelent, aki levelezőprogramon (Mail User Agent, levelezési felhasználói ügynök, „Levelezőprogram") keresztül fogad e-mailt. Ha egy Levelezőprogram e-mailt fogad, majd azt automatikusan továbbítja több felhasználónak, akkor a Végfelhasználók számának meghatározása az alapján történik, hogy ténylegesen hány felhasználó kapja meg a továbbítással az e-mailt. Ha a levelezési szerver levelezési kapuként működik, a Végfelhasználók száma megegyezik azon levelezésiszerver-használók számával, akiknek a kapu szolgáltatást nyújt. Csak egy számítógépre szükséges licencet szerezni, ha meghatározatlan számú e-mail-cím (alias) van átirányítva egy felhasználónak, és csak egyetlen felhasználó fogadja őket, továbbá a kliens nem továbbítja automatikusan az üzeneteket nagyszámú felhasználóhoz. A Licenc egyidejűleg csak egy számítógépen használható. A Végfelhasználó csak abban a mértékben jogosult megadni a Licenckulcsot a Szoftvernek, amennyi joga van használni a Szoftvert a Gyártó által adott Licencek száma alapján. A Licenckulcs bizalmas jellegű, Ön nem oszthatja meg harmadik féllel, illetve nem engedélyezheti a Licenckulcs használatát harmadik félnek, kivéve akkor, ha a jelen Szerződés vagy a Gyártó ezt megengedi. Ha a Licenckulcs illetéktelenekhez kerül, haladéktalanul értesítse a Gyártót.

c) **Otthoni/üzleti változat.** A Szoftver Otthoni verziója kizárólag privát, illetve nem kereskedelmi környezetben használható otthoni és családi használatra. A Szoftver Üzleti verzióját kereskedelmi környezetben való használatra lehet beszerezni, valamint a Szoftver levelezési szervereken, levelezési átjárókon vagy internetes átjárókon való használatához.

d) **A licenc érvényességi időszaka.** A Szoftver használatára vonatkozó jogosultság korlátozott időtartamra szól.

e) **Számítógép-gyártói (OEM-) szoftver.** A számítógép-gyártói (OEM) besorolású szoftver használata arra a számítógépre van korlátozva, amelyen beszerezte. amellyel megvásárolta azt, és másik számítógépre nem vihető át.

f) **Kereskedelmi forgalomba nem hozható termék és próbaverzió.** A „kereskedelmi forgalomba nem hozhatóként" minősített Szoftver és a próbaverzió nem lehet díjköteles, és kizárólag a Szoftver funkcióinak ellenőrzésére és tesztelésére, valamint szemléltetési célra használható.

g) **A licenc lejárata.** A Licenc az érvényességi időszak végén automatikusan lejár. Ha Ön nem teljesíti a jelen Szerződés bármely rendelkezését, a Gyártónak jogában áll felmondani a Szerződést bármely jogosultság vagy az ilyen esetekben a Gyártó számára elérhető jogorvoslati lehetőség megsértése nélkül. A Licenc felmondása esetén a Szoftvert, illetve az összes biztonsági másolatot haladéktalanul törölnie kell, meg kell semmisítenie, vagy a saját költségén vissza kell küldenie az ESET címére vagy abba az üzletbe, ahol a Szoftvert beszerezte. A Licenc lejárata esetén a Gyártónak szintjén jogában áll felmondania a Végfelhasználó jogosultságát a Szoftver olyan funkcióinak használatára, amelyek a Gyártó vagy harmadik felek szervereihez való kapcsolódást igényelnek.

4. **Adatgyűjtésre és internetkapcsolatra vonatkozó követelmények.** A Szoftver megfelelő működtetéséhez, valamint az Adatvédelmi szabályzatnak megfelelő adatgyűjtés céljából internetkapcsolat szükséges, és rendszeres időközönként csatlakoznia kell a Gyártó vagy a harmadik fél szervereihez. Az internetkapcsolatra és az adatgyűjtésre a Szoftver alábbi funkcióihoz van szükség:

a) **A Szoftver frissítései.** A Gyártó jogosult, de nem köteles időnként kiadni frissítéseket („Frissítések") a Szoftverhez. Ez a funkció a Szoftver általános beállításai között engedélyezve van, és a Frissítések ezért automatikusan települnek, kivéve ha a Végfelhasználó letiltotta a Frissítések automatikus telepítését. A frissítések biztosításához szükség van a Licenc eredetiségének ellenőrzésére, ideértve a Számítógépre vonatkozó információkat és/vagy annak ellenőrzését, hogy megfelel-e az Adatvédelmi szabályzatnak az a platform, amelyre a Szoftver telepítve van.

A Frissítések biztosítására az Életciklus végéről szóló szabályzat („EOL szabályzat") vonatkozik, amely a https://go.eset.com/eol weboldalon érhető el. Nem biztosítunk Frissítéseket, miután a Szoftver vagy bármely

funkciója elérte az EOL szabályzatban meghatározott Életciklus végét.

b) **Kártevők és információk továbbítása a Gyártónak.** A Szoftver olyan funkciókat tartalmaz, amelyek mintákat gyűjtenek a vírusokról és egyéb kártékony számítógépes programokról, a gyanús, problémás, kéretlen vagy veszélyes objektumokról, többek között fájlokról, URL-címekről, IP-csomagokról vagy Ethernet-keretekről („Kártevők"), majd a mintákat elküldik a Gyártónak, beleértve, de nem kizárólag a telepítési folyamatra, arra a számítógépre és/vagy platformra vonatkozó adatokkal, amelyen a Szoftver telepítve van, valamint a szoftver működésével és funkcióival („Adatok") együtt. Ezek az Adatok és Kártevők magukban foglalhatják a Végfelhasználóval vagy a Szoftvert futtató számítógép más felhasználóival kapcsolatos adatokat (beleértve a véletlenszerűen vagy nem szándékosan megszerzett személyes adatokat is), valamint a kártevők által érintett fájlokat a kapcsolódó metaadatokkal együtt.

Az információkat és a kártevőket a szoftver következő funkciói gyűjthetik:

i. A LiveGrid megbízhatósági rendszer végzi a kártevőkkel kapcsolatos egyirányú kivonatok gyűjtését és elküldését a Gyártónak. Ez a funkció a Szoftver általános beállításai között engedélyezhető.

ii. A LiveGrid visszajelzési rendszer hajtja végre a kártevők gyűjtését és elküldését a Gyártónak a kapcsolódó metaadatokkal és információkkal együtt. Ezt a funkciót a Végfelhasználó aktiválja a Szoftver telepítése során.

A Gyártó a kapott Adatokat és Kártevőket kizárólag a Kártevők elemzésére és tanulmányozására, a Szoftver fejlesztésére, valamint a Licenc eredetiségének ellenőrzésére használja, és megfelelő intézkedésekkel biztosítja a kapott Adatok és Kártevők bizalmas kezelését. A Szoftver fent említett funkciójának aktiválásával Ön hozzájárul ahhoz, hogy a Gyártó összegyűjtsön és feldolgozzon Kártevőket és Adatokat az Adatvédelmi szabályzatot és a vonatkozó jogszabályokat betartva. Ez a funkció bármikor kikapcsolható.

A jelen Szerződés értelmében szükség van az olyan adatok gyűjtésére, feldolgozására és tárolására, amelyek lehetővé teszik a Gyártónak az Ön beazonosítását az Adatvédelmi szabályzatnak megfelelő módon. Ön elfogadja, hogy a Gyártó saját eszközeinek segítségével ellenőrizheti, hogy Ön a jelen Szerződés előírásainak megfelelően használja-e a Szoftvert. Ön elfogadja azt is, hogy a jelen Szerződés értelmében szükség van az Ön adatainak átvitelére a Szoftver és a Gyártó számítógépes rendszerei, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei által működtetett számítógépes rendszerek között folyó kommunikáció során a Szoftver működésének biztosításához, a Szoftver használatához szükséges engedélyezés, valamint a Gyártó jogainak védelme érdekében.

A Szerződés megkötését követően a Gyártó, illetve a Gyártó forgalmazói és támogatási hálózatának részét képező üzleti partnerei jogosult az Önt azonosító alapvető adatok átadására, feldolgozására és tárolására számlázási célból, a jelen Szerződés végrehajtása érdekében, valamint azért, hogy az értesítések továbbíthatók legyenek az Ön Számítógépére.

Az adatvédelemről, a személyes adatok védelméről és az Önt mint adatalanyt megillető jogokról az Adatvédelmi szabályzat tartalmaz részletes információkat, amely a Gyártó webhelyén található, és közvetlenül a telepítési eljárás során érhető el. A szoftver súgójában is talál erről információkat.

5. **A Végfelhasználó jogainak gyakorlása**. Ön a Végfelhasználó jogait kizárólag személyesen vagy alkalmazottjai útján gyakorolhatja. Végfelhasználóként a Szoftvert csak a saját tevékenységének biztosítására és csak azon Számítógépek vagy számítógépes rendszerek védelmére használhatja fel, amelyekre vonatkozóan a Licencet megszerezte.

6. **A jogok korlátozása.** A Szoftvert nem másolhatja, nem terjesztheti, nem nyerheti ki az összetevőit, és nem készíthet belőle semmilyen származtatott tartalmat. A Szoftver használatakor az alábbi korlátozásokat kell betartania:

a) Biztonsági másolatként készíthet a Szoftverről egy másolatot tartós adattárolásra alkalmas adathordozón, feltéve, hogy a biztonsági másolatot később más számítógépen nem telepíti vagy nem használja. A Szoftver bármilyen, ettől eltérő módon történő másolása a jelen Szerződés megszegését jelenti.

b) Ön a jelen Szerződésben kifejezetten megengedett eseteken kívül nem jogosult a szoftvert és annak másolatait használni, módosítani, lefordítani, többszörözni és a használati jogát átruházni.

c) Ön a Szoftvert nem értékesítheti, használatát nem adhatja tovább, nem adhatja sem bérbe, sem kölcsön más személynek, illetve nem veheti bérbe más személytől, és nem használhatja kereskedelmi szolgáltatások nyújtásához.

d) Ön a Szoftvert nem jogosult visszafordítani, visszafejteni, vagy egyéb módon megkísérelni a Szoftver forráskódjának megszerzését, azon eseteket kivéve, melyek körében az e rendelkezés által előírt korlátozást a törvény kifejezetten tiltja.

e) Ön elfogadja, hogy a Szoftvert kizárólag olyan módon használja fel, amely megfelel az alkalmazandó jogszabályok előírásainak, amelyek alapján a Szoftvert használja, ideértve kivétel nélkül a szerzői jogról szóló törvényben és az egyéb szellemi alkotásokra vonatkozó jogszabályokban található korlátozásokat is.

f) Elfogadja, hogy a Szoftvert és annak funkcióit csak úgy használhatja, hogy azzal más Végfelhasználókat nem korlátoz e szolgáltatások elérésében. A Gyártó fenntartja magának a jogot az egyes Végfelhasználóknak nyújtott szolgáltatások hatókörének korlátozására annak érdekében, hogy a szolgáltatások használatát a lehető legnagyobb számú Végfelhasználó számára biztosíthassa. A szolgáltatások hatókörének korlátozása azt is magában foglalja, hogy a Gyártó teljes mértékben megakadályozhatja a Szoftver bármely funkciójának használatát, és törölheti a Szoftver egy adott funkciójával kapcsolatos Adatokat és információkat a Gyártó vagy harmadik fél által üzemeltetett szerverekről.

g) Ön beleegyezik abba, hogy nem folytat semmiféle olyan tevékenységet a Licenckulccsal kapcsolatban, amely megszegné a jelen Szerződés feltételeit, illetve amelynek következtében olyan személy kapná meg a Licenckulcsot, aki nem jogosult a Szoftver használatára. Ilyen tevékenység például a használt vagy nem használt Licenckulcs bármilyen formában való átadása, engedély nélküli másolása, megkettőzött vagy generált Licenkulcsok továbbadása, illetve a Szoftver használata olyan Licenkulccsal, amely nem a Gyártótól származik.

7. **Szerzői jogok**. A Szoftver és minden jogosultság, beleértve korlátozás nélkül a benne foglalt jogcímeket és szellemi tulajdonjogot, az ESET és/vagy a Licencet adó partnerei tulajdonát képezik. E jogokat a vonatkozó nemzetközi egyezmények rendelkezései és a használat helye szerinti ország alkalmazandó nemzeti jogszabályai védik. A Szoftver szerkezete, felépítése és kódja az ESET és/vagy a Licencet adó partnerei üzleti titkának és bizalmas információinak minősül. A 6(a) pontban foglalt esetet kivéve tilos a Szoftver másolása. A jelen Szerződés szerint másolt példányoknak is minden esetben tartalmazniuk kell a Szoftverrel megegyező szerzői jogokra és egyéb jogcímekre vonatkozó értesítéseket. Ha visszafordítja, visszafejti, vagy egyéb módon megkísérli a Szoftver forráskódjának megszerzését a jelen Szerződés rendelkezéseinek megszegésével, az úgy tekintendő, hogy az ezúton szerzett összes információ létrejöttének pillanatában automatikusan és visszavonhatatlanul a Gyártóra átruházza azt, a Gyártónak a jelen Szerződés megsértésével kapcsolatos jogaival együtt.

8. **Fenntartott jogok**. A Gyártó fenntartja magának a Szoftverre vonatkozó összes jogot, azokat kivéve, amelyeket Ön a Szoftver Végfelhasználójaként a jelen Szerződés keretei között gyakorolhat.

9. **Többnyelvű verzió, több adathordozón biztosított szoftver, több másolat**. Ha a Szoftver több platformot vagy nyelvet támogat, vagy ha Ön több példánnyal rendelkezik, a Szoftvert csak annyi számítógéprendszeren és azokkal a verziókkal használhatja, amelyekre a Licencet megszerezte. Ön nem jogosult a Szoftver nem használt verzióit vagy példányait értékesíteni, bérbe adni, haszonbérbe adni vagy a használatát továbbadni, kölcsönadni, illetve más személyre átruházni.

10. **A Szerződés hatálybalépése és megszűnése.** A jelen Szerződés attól a dátumtól érvényes, amikor Ön elfogadja a Szerződés feltételeit. Ön a Szerződést bármikor megszüntetheti a Szoftver, az összes biztonsági másolat és a gyártótól vagy üzleti partnereitől kapott kapcsolódó anyag végleges törlésével, megsemmisítésével vagy a saját költségen történő visszaküldésével. A Szoftver és bármely funkciójának használatára vonatkozó jog az EOL szabályzat hatálya alá tartozhat. Miután a Szoftver vagy bármely funkciója eléri az EOL szabályzatban meghatározott Életciklus végét, megszűnik a Szoftver használatára vonatkozó joga. A Szerződés megszűnésének módjától függetlenül a 7., 8., 11., 13., 19. és 21. pontban foglalt rendelkezések korlátlan ideig érvényben maradnak.

11. **VÉGFELHASZNÁLÓI JOGNYILATKOZATOK**. VÉGFELHASZNÁLÓKÉNT ÖN TUDOMÁSUL VESZI, HOGY A SZOFTVERT ANNAK „ADOTT ÁLLAPOTÁBAN”, MINDENFÉLE KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁS NÉLKÜL KAPJA, AZZAL, HOGY AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG SEM A GYÁRTÓ, A LICENCET ADÓ PARTNEREI VAGY LEÁNYVÁLLALATAI, SEM A SZERZŐI JOGOK JOGOSULTJAI NEM VÁLLALNAK KIFEJEZETT VAGY VÉLELMEZETT JÓTÁLLÁST, KÜLÖNÖSKÉPPEN, DE NEM KIZÁRÓLAGOSAN ADÁSVÉTELHEZ KAPCSOLÓDÓ JÓTÁLLÁST, MEGHATÁROZOTT CÉLRA VALÓ ALKALMASSÁGOT, VALAMINT ARRA VONATKOZÓ JOGSZAVATOSSÁGOT, HOGY A SZOFTVER NEM SÉRTI HARMADIK SZEMÉLYEK SZABADALMI, SZERZŐI, VÉDJEGYRE VONATKOZÓ VAGY EGYÉB JOGAIT. SEM A GYÁRTÓ, SEM MÁS FÉL NEM VÁLLAL JÓTÁLLÁST AZÉRT, HOGY A SZOFTVERBEN TALÁLHATÓ FUNKCIÓK MEGFELELNEK AZ ÖN ELVÁRÁSAINAK, ILLETVE HOGY A SZOFTVER MŰKÖDÉSE ZAVARTALAN ÉS HIBAMENTES LESZ. A KÍVÁNT EREDMÉNY MEGVALÓSÍTÁSÁRA ALKALMAS SZOFTVER KIVÁLASZTÁSA, TELEPÍTÉSE ÉS HASZNÁLATA, ILLETVE A SZOFTVERREL ÖN ÁLTAL ELÉRT EREDMÉNY TELJES MÉRTÉKBEN AZ ÖN FELELŐSSÉGE ÉS KOCKÁZATA.

12. **További kötelezettségvállalás kizárása**. A jelen Szerződés a benne kifejezetten felsoroltakon kívül a Gyártóra és a Licencet adó partnereire nem ró további kötelezettségeket.

13. **KORLÁTOZOTT FELELŐSSÉGVÁLLALÁS**. AZ ALKALMAZANDÓ JOGSZABÁLYOK ÁLTAL MEGENGEDETT MÉRTÉKIG A GYÁRTÓ, ILLETVE ALKALMAZOTTAI ÉS LICENCET ADÓ PARTNEREI SEMMILYEN ESETBEN SEM FELELŐSEK BÁRMIFÉLE BEVÉTEL- VAGY NYERESÉGKIESÉSÉRT, MEGHIÚSULT ÉRTÉKESÍTÉSI LEHETŐSÉGÉRT, ADATVESZTÉSÉRT, HELYETTESÍTŐ TERMÉKEK VAGY SZOLGÁLTATÁSOK BESZERZÉSÉBŐL FAKADÓ KÖLTSÉGEKÉRT, TULAJDONBAN BEKÖVETKEZETT VAGY SZEMÉLYT ÉRINTŐ KÁRÉRT, ÜZLETI FORGALOM KIESÉSÉÉRT, ÜZLETI INFORMÁCIÓ ELVESZTÉSÉRT VAGY BÁRMIFÉLE SPECIÁLIS, KÖZVETLEN, KÖZVETETT, ESETI, GAZDASÁGI, FEDEZETI, BÜNTETŐJOGI VAGY KÖVETKEZMÉNYKÁRÉRT, FÜGGETLENÜL A KÁROKOZÁS MIKÉNTJÉTŐL, ÉS ATTÓL, HOGY AZ SZERZŐDÉSBŐL, SZÁNDÉKOS KÁROKOZÁSBÓL, GONDATLANSÁGBÓL, VAGY MÁS, FELELŐSSÉGET MEGALAPOZÓ TÉNYBŐL ERED, HA EZEK A SZOFTVER TELEPÍTÉSÉNEK, A HASZNÁLATÁNAK VAGY HASZNÁLHATATLANSÁGÁNAK OKÁN MERÜLTEK FEL, MÉG ABBAN AZ ESETBEN IS, HA A GYÁRTÓT VAGY A LICENCET ADÓ PARTNEREIT, ILLETVE LEÁNYVÁLLALATAIT ELŐZŐLEG ÉRTESÍTETTÉK AZ ILYEN KÁR BEKÖVETKEZTÉNEK LEHETŐSÉGÉRŐL. MIVEL EGYES ORSZÁGOK ÉS JOGSZABÁLYOK NEM TESZIK LEHETŐVÉ A FELELŐSSÉG KIZÁRÁSÁT, A KORLÁTOZÁSÁT VISZONT IGEN, A GYÁRTÓ, ANNAK ALKALMAZOTTAI ÉS A LICENCET ADÓ PARTNEREI, ILLETVE LEÁNYVÁLLALATAI FELELŐSSÉGE A LICENCÉRT FIZETETT DÍJ MÉRTÉKÉRE KORLÁTOZÓDIK.

14. A jelen Szerződés egyetlen rendelkezése sem érinti annak a félnek a jogait, aki a jogszabályok értelmében fogyasztónak minősül.

15. **Terméktámogatás**. Az ESET vagy az ESET által meghatalmazott harmadik felek jótállás vagy jognyilatkozatok nélkül, saját döntésüknek megfelelően terméktámogatást nyújtanak. Nem biztosítunk terméktámogatást, miután a Szoftver vagy bármely funkciója elérte az EOL szabályzatban meghatározott Életciklus végét. A terméktámogatás előkészületeként a Végfelhasználónak biztonsági másolatot kell készítenie az összes meglévő adatról, szoftverről és a program összetevőiről. Az ESET vagy/és az ESET által meghatalmazott harmadik felek nem vállalnak felelősséget az adatok, a tulajdon, a szoftver vagy a hardver terméktámogatás következtében keletkező sérüléséért vagy elvesztéséért, illetve a veszteség miatt. Az ESET vagy/és az ESET által meghatalmazott harmadik felek fenntartják a jogot, hogy eldönthessék, miszerint a probléma megoldása túllépi-e a terméktámogatás hatáskörét. Az ESET fenntartja a jogot, hogy saját hatáskörében elutasítsa, felfüggessze vagy befejezze a

terméktámogatás nyújtását. Technikai terméktámogatás céljából szükség lehet Licencadatokra, Adatokra és egyéb adatokra az Adatvédelmi szabályzatnak megfelelően.

16. **A licenc átadása.** A szoftver egyik számítógéprendszerről átvihető egy másikra, feltéve ha az nem ellentétes a Szerződés feltételeivel. Ha nem ütközik a Szerződés feltételeivel, a Végfelhasználó csak a Gyártó jóváhagyásával jogosult véglegesen átadni a Licencet és a jelen Szerződésből fakadó minden jogosultságot másik Végfelhasználónak azzal a feltétellel, hogy (i) az eredeti Végfelhasználó nem tartja meg a Szoftver egyetlen másolatát sem; (ii) a jogosultságok átadása közvetlen, vagyis az eredeti Végfelhasználóról az új Végfelhasználóra történik; (iii) az új Végfelhasználónak vállalnia kell a jelen Szerződés szerint az eredeti Végfelhasználót érintő minden jogosultságot és kötelezettséget; (iv) az eredeti Végfelhasználónak át kell adnia az új Végfelhasználó részére a Szoftver eredetiségének ellenőrzését lehetővé tevő összes dokumentációt a 17. pontban leírtak szerint.

17. **A Szoftver eredetiségének ellenőrzése.** A Végfelhasználó a Szoftver használatára vonatkozó jogosultságát az alábbi módok valamelyikén igazolhatja: (i) a Gyártó vagy a Gyártó által kinevezett harmadik fél által kibocsátott licenctanúsítvánnyal; (ii) írásbeli licencszerződéssel, amennyiben készült ilyen szerződés; (iii) a Gyártó által e-mailben küldött licencadatokkal (felhasználónév és jelszó). A Szoftver eredetiségének ellenőrzése céljából szükség lehet Licencadatokra és a Végfelhasználó személyazonosítására alkalmas adatokra az Adatvédelmi szabályzatnak megfelelően.

18. **Licencek adása hatóságok és az Amerikai Egyesült Államok kormánya számára.** A Szoftver a jelen Szerződésben rögzített licencjogosultságokkal és korlátozásokkal biztosítható a hatóságok, többek között az Amerika Egyesült Államok kormánya számára.

19. **A kereskedelmi felügyeleti törvények betartása**.

a) Ön vállalja, hogy nem fogja közvetve vagy közvetlenül exportálni, újraexportálni, továbbítani vagy más módon elérhetővé tenni a Szoftvert, nem fogja semmilyen módon használni, illetve nem vesz részt olyan tevékenységben, amelynek következtében az ESET vagy holdingtársaságai, leányvállalatai és holdingtársaságainak leányvállalatai, valamint a holdingtársaságai által irányított jogalanyok („Társult vállalatok”) megsértenének kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük. Kereskedelmi felügyeleti törvénynek minősül

i. minden olyan törvény, amely szabályozást, korlátozást, illetve licencelési követelményeket szab meg áruk, szoftverek, technológiai termékek, illetve szolgáltatások exportálásának, újraexportálásának vagy továbbításának vonatkozásában, és amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik, valamint

ii. minden olyan gazdasági, pénzügyi, kereskedelmi vagy egyéb jellegű szankció, korlátozás, embargó, importálási vagy exportálási tilalom, tiltás források vagy eszközök továbbításának vagy szolgáltatások nyújtásának vonatkozásában, illetve ezekkel egyenértékű intézkedés, amelyet az Amerikai Egyesült Államok, Szingapúr, az Egyesült Királyság, az Európai Unió vagy bármely tagállama, illetve bármely olyan ország kormányzata, állami vagy szabályozó hatósága rendelt vagy fogadott el, ahol a Szerződés értelmében kötelezettségeket kell végrehajtani, illetve ahol az ESET vagy bármely társult vállalata be van jegyezve vagy működik.

(a fenti i. és ii. pontban említett jogi aktusok együttesen „Kereskedelmi szabályozási törvények”).

b) Az ESET jogában áll azonnali hatállyal felfüggeszteni vagy felmondani a jelen Feltételek szerinti kötelezettségeit abban az esetben, ha:

i. Az ESET – észszerű feltételezés révén – megállapítja, hogy a Felhasználó megsértette vagy nagy valószínűséggel megsértette a Szerződés 19 a) cikkelyét; illetve

ii. a Végfelhasználó, illetve a Szoftver kereskedelmi felügyeleti törvények hatálya alá esik, és ennek eredményeképpen az ESET – észszerű feltételezés révén – megállapítja, hogy a Szerződés szerinti kötelezettségeinek további teljesítése következtében az ESET vagy Társult vállalatai megsérthetnek kereskedelmi felügyeleti törvényeket, vagy ezek értelmében negatív következményeket kellene elszenvedniük.

c) A Szerződés egyik rendelkezése sem azzal a szándékkal jött létre és nem értelmezhető úgy, hogy bármely felet réveszi vagy kötelezi a vonatkozó kereskedelmi felügyeleti törvényekkel össze nem egyeztethető vagy azok értelmében büntetendő vagy tiltott cselekedek végrehajtására vagy bizonyos cselekedek mellőzésére (illetve arra, hogy beleegyezzenek ilyen cselekedek végrehajtásába vagy bizonyos cselekedek mellőzésébe).

20. **Értesítések**. Minden értesítést, a visszaküldendő Szoftvert és Dokumentációt a következő címre kell küldeni: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Az ESET fenntartja a jogot arra, hogy értesítse Önt a jelen Szerződés, az Adatvédelmi szabályzat, az EOL szabályzat és a Dokumentáció bármilyen módosításáról a Szerződés 22. cikkelye szerint. Az ESET küldhet Önnek e-maileket, alkalmazáson belüli értesítéseket a Szoftveren keresztül, illetve közzétehetünk közleményeket a webhelyünkön. Ön beleegyezik abba, hogy elektronikus formában jogi tájékoztatást fog kapni az ESET-től, beleértve a Feltételek, a Különleges feltételek vagy az Adatvédelmi irányelvek módosításával kapcsolatos értesítéseket, olyan szerződéses ajánlatokat/jóváhagyásokat vagy meghívásokat, amelyeket kezelnie kell, értesítéseket és egyéb jogi közleményeket. Az ilyen elektronikus kommunikációt írásban átvettnek kell tekinteni, kivéve akkor, ha a vonatkozó jogszabályok más kommunikációs formát írnak elő.

21. **Alkalmazandó jog**. A jelen Szerződésre a Szlovák Köztársaság törvénye az irányadó, és a szerződés a szerint értelmezendő. A Végfelhasználó és a Gyártó ezennel megállapodnak abban, hogy az alkalmazandó jog és az ENSZ által elfogadott „Nemzetközi árukereskedelmi szerződésekről szóló egyezmény” ütközése esetén az ütköző rendelkezések nem alkalmazhatók. A Gyártóval fennálló, illetve a Szoftver használatával kapcsolatos minden jogvita vagy követelés tekintetében Ön kifejezetten aláveti magát a Pozsonyi I. sz. Kerületi Bíróság kizárólagos joghatóságának, továbbá kifejezetten aláveti magát a nevezett bíróság illetékességének az ilyen jogviták rendezésében.

22. **Általános rendelkezések**. Amennyiben a jelen Szerződés bármely rendelkezése érvénytelen vagy kikényszeríthetetlen, az nem érinti a Szerződés többi részének érvényességét. A többi rendelkezés továbbra is érvényes és végrehajtható marad az itt lefektetett feltételek szerint. A jelen Szerződés angol nyelven íródott. Amennyiben a Szerződésről bármilyen fordítás készül kényelmi okokból vagy bármely más célból, illetve bármilyen ellentmondás van a jelen Szerződés különböző nyelvi változatai között, az angol változat az irányadó.

Az ESET fenntartja a jogot arra, hogy bármikor módosítsa a Szoftvert és felülvizsgálja a jelen Feltételek pontjait, a függelékeket, a mellékeleteket, az Adatvédelmi szabályzatot, az EOL szabályzatot és a dokumentációt, illetve azok bármely részét a releváns dokumentum frissítésével (i) a Szoftver vagy az ESET megváltozott üzleti eljárásainak megfelelően, (ii) törvényi, szabályozási vagy biztonsági okokból vagy (iii) a visszaélések vagy károk megakadályozása érdekében. A Szerződés módosításáról Ön minden esetben értesítést fog kapni e-mailben, alkalmazáson belüli értesítés útján vagy egyéb elektronikus úton. Ha nem ért egyet a Szerződés javasolt módosításaival, a 10. cikkely szerint felmondhatja a módosításról szóló értesítés kézhezvételétől számított 30 napon belül. Hacsak nem mondja fel a Szerződést ezen határidőn belül, a javasolt változtatások elfogadottnak tekinthetők és kötelezővé válnak Önre nézve attól a naptól kezdve, amikor az értesítést kézhet kapta a változásról.

Az Ön és a Gyártó között létrejött jelen Szerződés jelenti a Szoftverre vonatkozó teljes szerződést, és hatályon kívül helyezi a Szoftverre vonatkozóan tett minden korábbi jognyilatkozatot, megállapodást, kötelezettségvállalást, kommunikációt vagy hirdetést.

EULAID: EULA-PRODUCT-LG; 3537.0

Adatvédelmi szabályzat

A személyes adatok védelme különösen fontos az ESET, spol. s r. o. számára (székhelye: Einsteinova 24, 851 01 Bratislava, Slovak Republic; bejegyezve az I. sz. Pozsonyi Kerületi Bíróság cégjegyzékében; iktatási szám: 3586/B; cégjegyzékszám: 31333532) adatkezelőként („ESET” vagy „Mi”). Szeretnénk megfelelni az EU általános adatvédelmi rendelete (GDPR) alapján jogilag szabványosított átláthatósági követelménynek. Ezért közzétesszük a jelen Adatvédelmi szabályzatot azzal a céllal, hogy tájékoztassuk ügyfelünket („Végfelhasználó” vagy „Ön”) mint adatalanyt a személyes adatvédelem következő témáiról:

- A személyes adatok feldolgozásának jogi alapja,
- Adatmegosztás és titoktartás,
- Adatbiztonság,
- Az Önt adatalanyként megillető jogok,
- Az Ön személyes adatainak feldolgozása,
- Partnerinformációk.

A személyes adatok feldolgozása

Az ESET által nyújtott és a termékeinkbe integrált szolgáltatások működését a VÉGFELHASZNÁLÓI LICENCSZERZŐDÉSszabályozza, viszont néhány szolgáltatás különös figyelmet igényel. Szeretnénk további információkat biztosítani Önnek az adatgyűjtésről a szolgáltatásaink nyújtásával kapcsolatban. A Végfelhasználói licencszerződésben és a termékdokumentációműködésére és funkcióira vonatkozó információkat is. A szolgáltatások működtetése érdekében a következő információkat kell gyűjtenünk:

- Frissítési és egyéb statisztikai adatok, amelyek közé olyan információk tartoznak, mint a telepítési folyamat és az Ön számítógépe, ideértve azt a platformot, amelyre a termékünket telepíti, valamint a termékeink működésével és funkcióival kapcsolatos információk, például az operációs rendszer, hardverekkel kapcsolatos információk, telepítési azonosítók, licencazonosítók, IP-cím, MAC-cím, a termék konfigurációs beállításai.
- Kártevőkkel kapcsolatos egyirányú kivonatok, amelyek az ESET LiveGrid® megbízhatósági rendszer részét képezik. A rendszer összeveti az ellenőrzött fájlokat a felhőben tárolt engedélyező- és tiltólistaelemek adatbázisával, ezáltal fokozva a kártevőirtó szoftvereink hatékonyságát.
- Az ESET LiveGrid® visszajelzési rendszer által biztosított gyanús minták és metaadatok. Ez a rendszer lehetővé teszi, hogy az ESET azonnal választ adjon a végfelhasználók igényeire, és hogy biztosítsuk a hatékonyságunkat a legújabb kártevőkkel szemben. A következők elküldését kérjük Öntől:
    - kártevők, például minták vírusokról és egyéb kártékony szoftverekről, valamint gyanús, problémás, kéretlen vagy veszélyes objektumokról, például végrehajtható fájlokról, illetve az Ön vagy a termékünk által levélszemétként megjelölt e-mailek;
    - a helyi hálózathoz csatlakozó eszközökkel kapcsolatos információk, például az eszközök típusa, gyártója, modellszáma, illetve neve;
    - internethasználattal kapcsolatos információk, például IP-cím és földrajzi adatok, IP-csomagok, URL-címek és Ethernet-keretek;
    - összeomlási memóriaképek és a bennük található információk.

Más célból nem kívánunk adatokat gyűjteni, viszont néha lehetetlen ezt elkerülni. Előfordulhat, hogy maguk a kártevők tartalmaznak véletlenül begyűjtött adatokat (amelyek begyűjtéséről Önnek tudomása van, vagy azt jóváhagyta), illetve hogy fájlnevek vagy URL-címek részét képezik. Nem célunk, hogy az ilyen információk rendszereink vagy folyamataink részét képezzék, illetve nem dolgozzuk fel őket a jelen Adatvédelmi szabályzatban leírtak szerint.

- Licencelési információkra, például licencazonosítóra és személyes adatokra – például név, vezetéknév, cím, e-mail-cím – szükséges számlázási célokra, a licenc eredetiségének ellenőrzéséhez, valamint a szolgáltatások biztosításához.
- Szervizelés, illetve segítségnyújtás biztosításához szükség lehet az Ön által leadott terméktámogatási kérelmekben foglalt elérhetőségekre és adatokra. Attól függően, hogy Ön milyen csatornát választ a velünk történő kapcsolatfelvételre, összegyűjthetjük az Ön e-mail-címét, telefonszámát, a licencelési információkat, a termékadatokat és a támogatási eset leírását. Egyéb információk megadására is megkérhetjük a terméktámogatás megkönnyítése céljából.

Adatmegosztás és titoktartás

Adatait nem osztjuk meg harmadik felekkel. Az ESET azonban világszerte jelen van a kapcsolt vállalkozások, illetve partnerek révén, amelyek forgalmazói, szolgáltatói és terméktámogatási hálózatunk részét képezik. A kapcsolt vállalkozások és partnerek megkaphatják, illetve visszaküldhetik az ESET által feldolgozott licencelési, számlázási és műszaki terméktámogatási információkat a Végfelhasználói licencszerződés teljesítése céljából, így például a szolgáltatások és a terméktámogatás biztosítása érdekében.

Az ESET az Európai Unióban (EU) történő adatfeldolgozást preferálja. Azonban az Ön tartózkodási helyétől (termékeink és/vagy szolgáltatásaink EU-n kívüli használata) és/vagy az Ön által választott szolgáltatástól függően előfordulhat, hogy az adatait az EU-n kívüli országba kell továbbítani. Például harmadik féltől származó szolgáltatásokat használunk a felhőalapú szolgáltatásokkal kapcsolatban. Ezekben az esetekben gondosan választjuk ki szolgáltatóinkat, és biztosítjuk a megfelelő szintű adatvédelmet szerződéses, műszaki és szervezeti intézkedésekkel. Rendszerint megállapodunk az EU-s szabványos szerződési feltételekben, ha szükséges, kiegészítő szerződéses rendelkezésekkel.

Egyes EU-n kívüli országok, például az Egyesült Királyság és Svájc esetében az EU már meghatározta az adatvédelem összevethető szintjét. Az adatvédelem összevethető szintje miatt az adatok ezen országokba történő továbbítása nem igényel külön engedélyt vagy megállapodást.

Az adatalany jogai

Minden Végfelhasználó jogai számítanak, és szeretnénk tájékoztatni Önt arról, hogy minden Végfelhasználó (minden EU-s és nem EU-s országból származó) rendelkezik az alábbi jogokkal az ESET-nél. Az Önt mint adatalanyt megillető jogok gyakorlása érdekében forduljon hozzánk a támogatási űrlapon keresztül vagy e-mail útján a következő címen: dpo@eset.sk. Személyazonosítás céljából a következő információkat kérjük Öntől: Név, e-mail-cím és – ha rendelkezésre áll – licenckulcs vagy ügyfélszám, valamint vállalati hovatartozás. Kérjük, tartózkodjon attól, hogy bármilyen egyéb személyes adatot, például születési dátumot küldjön nekünk. Szeretnénk felhívni a figyelmét arra, hogy a kérésének feldolgozásához, valamint személyazonosítási célokból fel fogjuk dolgozni a személyes adatait.

Jogosult visszavonni a hozzájárulását. A hozzájárulás visszavonásának joga a csak a beleegyezésen alapuló adatkezelés esetén alkalmazható. Ha személyes adatait az Ön hozzájárulása alapján dolgozzuk fel, Önnek jogában áll a hozzájárulását indokolás nélkül bármikor visszavonni. Hozzájárulásának visszavonása csak a jövőben lép érvénybe, vagyis nem érinti a visszavonás előtt feldolgozott adatok jogszerűségét.

Jogosult tiltakozni. A feldolgozás ellen való tiltakozáshoz való jog az ESET vagy egy harmadik fél jogos érdekén alapuló adatkezelés esetén alkalmazandó. Amennyiben személyes adatait jogos érdek védelme érdekében dolgozzuk fel, akkor Önnek mint adatalanynak jogában áll bármikor kifogást emelni az általunk megnevezett jogos érdek és személyes adatainak feldolgozása ellen. A kifogásolás csak a jövőben lép érvénybe, vagyis nem érinti a kifogásolás előtt feldolgozott adatok törvényszerűségét. Amennyiben személyes adatait direktmarketing céljából dolgozzuk fel, nem szükséges indokolni a kifogásolást. Ez vonatkozik a profilalkotásra is, amennyiben az ilyen jellegű direktmarketinghez kapcsolódik. Minden más esetben arra kérjük Önt, hogy röviden tájékoztasson

bennünket az ESET személyes adatainak feldolgozásához fűződő jogos érdekével kapcsolatos panaszairól.

Kérjük, vegye figyelembe, hogy egyes esetekben a hozzájárulás visszavonása ellenére jogunk van arra, hogy a személyes adatait egy másik jogalap alapján továbbra is feldolgozzuk, például egy szerződés teljesítése céljából.

Joga van a hozzáféréshez. Ön mint adatalany bármikor díjmentesen lekérheti az ESET által tárolt adatairól szóló információkat.

Jog van a helyesbítéshez. Ha véletlenül helytelen személyes adatokat dolgozunk fel Önről, jogában áll ezt helyesbíteni.

Joga van a törléshez és az adatkezelés korlátozásához. Ön mint adatalany jogosult kérelmezni személyes adatainak törlését, illetve azt, hogy személyes adatainak feldolgozása korlátozott mértékben történjen meg. Ha például személyes adatait a hozzájárulásával dolgozzuk fel, de visszavonja a hozzájárulását, és nincs más jogalap – például szerződés –, akkor azonnal töröljük személyes adatait. A személyes adatait akkor is töröljük, amint a megőrzési időszak végén már nincs rájuk szükség az esetükben megadott célokból.

Ha személyes adatait kizárólag direktmarketing céljából használjuk fel, és Ön visszavonta a hozzájárulását, vagy kifogást emelt az ESET jogos érdekével szemben, akkor a személyes adatainak feldolgozását olyan mértékben korlátozzuk, hogy kapcsolattartási adatait belefoglaljuk a belső tiltólistánkba annak érdekében, hogy elkerüljük a kéretlen kapcsolatfelvételt. Ellenkező esetben az Ön személyes adatai törlődnek.

Kérjük, vegye figyelembe, hogy az adatait a törvényhozó vagy felügyeleti hatóságok által megadott adatmegőrzési kötelezettségek és határidők lejártáig tárolnunk kell. Az adatmegőrzési kötelezettségek és időszakok a szlovákiai jogszabályokból is származhatnak. Ezt követően a megfelelő adatok rutinszerűen törlődnek.

Joga van az adathordozhatósághoz. Örömmel biztosítjuk Önnek mint adatalanynak az ESET által feldolgozott személyes adatokat xls formátumban.

Jogosult panaszt emelni. Ön mint adatalany bármikor jogosult panaszt benyújtani egy felügyeleti hatósághoz. Az ESET vállalatra a szlovák törvények az irányadók, és az Európai Unió tagjaként kötelességünk betartani az adatvédelmi rendelkezéseket. Az érintett adatfelügyeleti hatóság a Szlovák Köztársaság Személyes Adatvédelmi Hivatala, amely a következő helyen található: Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Partnerinformációk

Amennyiben gyakorolni szeretné az adatalanyként Önt megillető jogait, vagy ha bármilyen kérdése vagy kételye van, írjon nekünk a következő címre:

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