F-Secure Anti-Virus 2013

Tartalom

1. fejezet: Telepítés.....5

Az els telepítés el tti teend k.....6
A termék els telepítése.....6
Alkalmazások telepítése és frissítése.....6
Súgó és támogatás.....7

2. fejezet: Az els lépések.....9

Automatikus frissítés használata.....10
Frissítés állapotának ellen rzése.....10
Az internetkapcsolat beállításainak módosítása.....10
A valós idej védelmi hálózat állapotának ellen rzése.....11
A termék eredményeinek megtekintése.....11
Értesítési el zmények megtekintése.....11
Az értesítések beállításainak módosítása.....11
Valós idej védelmi hálózat.....12
Mire szolgál a valós idej védelmi hálózat?.....12
A valós idej védelmi hálózat el nyei.....12
Az összegy jtött adatok.....13
Adatvédelmi irányelveink.....14
Közrem ködés a valós idej védelmi hálózatban.....14
A valós idej védelmi hálózattal kapcsolatos kérdések.....15
Honnan tudhatom, hogy érvényes-e az el fizetésem?.....15
M veleti központ.....15
El fizetés aktiválása.....16

3. fejezet: Bevezetés.....17

A védelem általános állapotának megtekintése.....18
Termékstatisztika megtekintése.....18
Termékfrissítések kezelése.....19
Adatbázis-verziók megtekintése.....19
A mobil szélessáv beállításainak módosítása.....19
Mik a vírusok és kártékony szoftverek?.....20
Vírusok.....20
Kémprogram.....20
Rootkitek.....21
Veszélyes program.....21

4. fejezet: A számítógép védelme a kártékony szoftverekkel szemben.23

A számítógép vizsgálata....24
Fájlok automatikus vizsgálata....24
Fájlok manuális vizsgálata....26
E-mailek vizsgálata....29
Vizsgálati eredmények megtekintése....30
Fájlok kizárása a vizsgálatból....30
Fájltípusok kizárása....30
Fájlok kizárása azok helye alapján....31
Kihagyott alkalmazások megtekintése....32
A karantén használata....32
Karanténba helyezett elemek megtekintése....33
Karanténba helyezett elemek visszaállítása....33
Bels ok....33
A DeepGuard be- vagy kikapcsolása....34
A DeepGuard által letiltott alkalmazások engedélyezése....34
A DeepGuard használata kompatibilitási módban....34
Gyanús viselkedésr l szóló figyelmeztetések beállítása....35

1

. fejezet

Telepítés

Témák:

- *Az els telepítés el tti teend k*
- *A termék els telepítése*
- *Alkalmazások telepítése és frissítése*
- *Súgó és támogatás*

Az els telepítés el tti teend k

Köszönjük, hogy az F-Secure céget választotta.

A termék telepítéséhez a következ kre van szükség:

- A telepít lemez vagy telepít csomag. Ha CD-meghajtó nélküli netbookot használ, a telepít csomagot innen töltheti le: *www.f-secure.com/netbook*.
- Az Ön el fizet i kulcsa:
- Internet-hozzáférés.

Egy másik gyártótól származó biztonsági termék megléte esetén a telepít program automatikusan megkísérli azt eltávolítani. Ha ez nem történik meg, kérjük, távolítsa el a terméket manuálisan.

Megjegyzés: Ha több fiók is be van állítva számítógépén, a telepítéskor rendszergazdai jogosultságokkal jelentkezzen be.

A termék els telepítése

Utasítások a termék telepítéséhez.

A termék telepítéséhez kövesse a következ utasításokat:

1. Helyezze be a CD-t, vagy kattintson duplán a letöltött telepít programra.

   Ha a CD lejátszása nem indul el automatikusan, a Windows Intéz ben kattintson duplán a CD-ROM ikonjára, majd kattintson duplán a telepít fájlra a telepítés elindításához.

2. Kövesse a képerny n megjelen utasításokat.

   - Ha a terméket kiskereskedelmi csomagban, CD lemezen vásárolta meg, akkor az el fizet i kulcs a Gyorstelepítési útmutató borítóján található.
   - Ha a terméket az F-Secure eStore áruházból töltötte le, akkor az el fizet i kulcs a megrendelés meger sítését tartalmazó e-mail üzenetben található.

   Az el fizetés érvényesítése és a legújabb frissítések letöltése el tt szükség lehet a számítógép újraindítására. Ha a telepítést CD-r l végzi, a számítógép újraindítása el tt ne feledje eltávolítani a telepít lemezt a meghajtóból.

Alkalmazások telepítése és frissítése

Az új el fizetés aktiválásának lépései.

Az új el fizetés aktiválásához vagy az indítópult segítségével egy új alkalmazás telepítéséhez kövesse az alábi utasításokat:

Megjegyzés: Az indítópult ikonja a Windows rendszertálcáján található.

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Megnyílik egy el ugró menü.
2. Válassza az **El fizetések megtekintése** lehet séget.
3. A **Saját el fizetések** csoportban nyissa meg az **El fizetés állapota** oldalt, és kattintson az **El fizetés aktiválása** elemre.

Ekkor megnyílik az **El fizetés aktiválása** ablak.

4. Adja meg az el fizet i kulcsot az alkalmazáshoz, és kattintson az **OK** gombra.
5. Az el fizetés érvényesítése és aktiválása után kattintson a **Bezárás** gombra.
6. A **Saját el fizetések** csoportban nyissa meg a **Telepítés állapota** oldalt. Ha a telepítés nem indul el automatikusan, kövesse az alábbi utasításokat:
   a) Kattintson a **Telepítés** gombra.
   Megnyílik a telepít ablak.
   b) Kattintson a **Tovább** gombra.
   A rendszer letölti az alkalmazást, és a telepítés megkezd dik.
   c) A telepítés befejez désekor kattintson a **Bezárás** gombra.

Az új el fizetés aktiválása megtörtént.

Súgó és támogatás

Az online terméksúgót a Súgó ikonra kattintva vagy a termék bármely képerny jén az F1 billenty lenyomásával érheti el.

A licenc regisztrálása után további szolgáltatásokra (például ingyenees termékfrissítésekre és terméktámogatásra) válik jogosulttá. A regisztrálást a *www.f-secure.com/register* oldalon hajthatja végre.

2

. fejezet

Az els lépések

Témák:

- *Automatikus frissítés használata*
- *A termék eredményeinek megtekintése*
- *Valós idej védelmi hálózat*
- *Honnan tudhatom, hogy érvényes-e az el fizetésem?*

A termék használatának megkezdéséhez szükséges lépések.

Ebb l a részb l megtudhatja, hogy miként módosíthatók az általános beállítások és kezelhet k az el fizetések az indítópultról.

Az indítópult általános beállításai az indítópulton telepített minden programra érvényesek. Ahelyett, hogy külön kellene módosítani a beállításokat az egyes programokban, egyszer en szerkesztheti az általános beállításokat, amelyeket aztán a telepített programok mindegyike használni fog.

Az indítópult általános beállításai:

- Letöltések, ahol megtekintheti, hogy milyen frissítéseket töltött le eddig, és manuálisan ellen rizheti, hogy milyen új frissítések érhet k el.
- Kapcsolat beállításai, ahol módosíthatja a számítógép internethez való csatlakozásának módját.
- Értesítések, ahol megtekintheti az eddigi értesítéseket, és megadhatja, hogy milyen típusú értesítéseket szeretne megjeleníteni.
- Adatvédelmi beállítások, ahol megadhatja, hogy engedélyezi-e a számítógép számára a Valós idej védelmi hálózathoz való csatlakozást.

Az indítópulton keresztül a telepített programokhoz tartozó el fizetések kezelésére is van mód.

Automatikus frissítés használata

Az automatikus frissítés naprakészen tartja a számítógép védelmét.

A termék letölti a legújabb frissítéseket a számítógépre, amikor az internethez csatlakozik. Észleli a hálózati forgalmat, és nem zavarja az internethasználatot még kis sebesség kapcsolat estén sem.

Frissítés állapotának ellen rzése

A legutóbbi frissítés dátumának és idejének megjelenítése.

Ha engedélyezi az automatikus frissítést, az automatikusan frissíti a terméket, amikor csatlakozik az internethez.

Annak biztosítása, hogy mindig a legújabb frissítésekkel rendelkezik:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.
3. Válassza az **Automatikus frissítések** > **Letöltések** lehet séget.
4. Kattintson az **Ellen rzés** gombra.
   A termék csatlakozik az internethez, és megkeresi a legújabb frissítéseket. Ha a védelem nem naprakész, a program letölti a legújabb frissítéseket.

   Megjegyzés: Ha modemet használ, vagy ISDN-kapcsolaton keresztül csatlakozik az internethez, a frissítéseket csak aktív kapcsolat megléte esetén tudja ellen rizni a program.

Az internetkapcsolat beállításainak módosítása

Általában nincs szükség az alapbeállítások módosítására, de a kiszolgáló internethez való kapcsolódását konfigurálhatja, így automatikusan kapja a frissítéseket.

Az internetkapcsolat beállításainak módosítása:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.
3. Válassza az **Automatikus frissítések** > **Kapcsolat** lehet séget.
4. Az **Internetkapcsolat** listában válassza ki, hogy a számítógép hogyan kapcsolódik az internethez.
   - Ha állandó hálózati kapcsolattal rendelkezik, válassza a **Folyamatos kapcsolat feltételezése** lehet séget.

     Megjegyzés: Ha a számítógép valójában nem kapcsolódik folyamatosan a hálózathoz, és igény szerinti kapcsolatra van beállítva, a **Feltételezze, hogy mindig van kapcsolat** lehet ség kiválasztása többszöri tárcsázást eredményezhet.
   - Válassza a **Kapcsolat észlelése** lehet séget, ha csak akkor kívánja letölteni a frissítéseket, amikor a program aktív hálózati kapcsolatot észlel.
   - Az **Adatforgalom észlelése** beállítás használata esetén a program csak akkor tölti le a frissítéseket, ha a termék egyéb hálózati forgalmat is észlel.

     Tipp: Ha olyan különleges hardverkonfigurációt használ, amely következtében a **Kapcsolat észlelése** lehet ség tévesen észleli az aktív hálózati kapcsolatok meglétét, válassza helyette az **Adatforgalom észlelése** beállítást.

5. A **HTTP-proxy** listában válassza ki, hogy a számítógép az internetes kapcsolathoz használ-e *proxykiszolgálót*, vagy sem.
   - Ha a számítógép közvetlenül kapcsolódik az internethez, válassza a **Nincs HTTP-proxy** lehet séget.
   - Válassza a **HTTP-proxy beállítása saját kez leg** lehet séget a *HTTP-proxy* beállításainak megadásához.
   - Válassza **A böngész HTTP-proxyjának használata** lehet séget, ha a webböngész által használt *HTTP-proxy* beállításokat kívánja használni.

A valós idej védelmi hálózat állapotának ellen rzése

A termék számos szolgáltatásának helyes m ködése függ a valós idej védelmi hálózati kapcsolattól.

Ha hálózati problémák merülnek fel, vagy ha a t zfal blokkolja a valós idej védelmi hálózat adatforgalmát, a „Leválasztva” állapotúra vált. Ha a terméknek nincsenek olyan szolgáltatásai telepítve, amelyek igényelnék a valós idej védelmi hálózat szolgáltatást, az „Nincs használatban” állapotú lesz.

Az állapot ellen rzése:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.
3. Válassza az **Automatikus frissítések** > **Kapcsolat** lehet séget.

A **Valós idej védelmi hálózat** csoportban megtekintheti a valós idej védelmi hálózat aktuális állapotát.

A termék eredményeinek megtekintése

Az **Értesítések** oldalon megtekintheti, hogy a termék milyen m veleteket hajtott eddig végre a számítógép védelmének biztosítása érdekében.

A termék akkor jelenít meg értesítést, ha végrehajt valamilyen m veletet, például blokkol egy észlelt vírust. A szolgáltatótól is érkezhetnek értesítések, például arról, hogy új szolgáltatások váltak elérhet vé.

Értesítési el zmények megtekintése

Az eddig megjelenített értesítéseket az értesítési el zményekben tekintheti meg.

Az értesítési el zmények megtekintése:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.
3. Válassza az **Egyebek** > **Értesítések** lehet séget.
4. Válassza az **Értesítési el zmények megjelenítése** lehet séget.
   Ekkor megnyílnak az értesítési el zmények.

Az értesítések beállításainak módosítása

Kiválaszthatja, hogy a termék milyen típusú értesítéseket jelenítsen meg.

Az értesítések beállításának módosítása:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.

3. Válassza az **Egyebek** > **Értesítések** lehet séget.
4. A programüzenetek be-, illetve kikapcsolásához jelölje be a **Programüzenetek engedélyezése** jelöl négyzetet, vagy törölje annak jelölését.

   Ha ez a beállítás be van kapcsolva, a termék megjeleníti a telepített programok értesítéseit.
5. A promóciós üzenetek be-, illetve kikapcsolásához jelölje be a **Promóciós üzenetek engedélyezése** jelöl négyzetet, vagy törölje annak jelölését.
6. Kattintson az **OK** gombra.

Valós idej védelmi hálózat

Ez a dokumentum a valós idej védelmi hálózatot, az F-Secure Corporation azon online szolgáltatását ismerteti, amellyel azonosíthatók a tiszta alkalmazások és webhelyek, valamint biztosítható a kártékony programok és a nem biztonságos webhelyek elleni védelem.

Mire szolgál a valós idej védelmi hálózat?

A valós idej védelmi hálózat egy olyan online szolgáltatás, amely gyors választ biztosít az internetalapú fenyegetésekkel szemben.

A valós idej védelmi hálózat közrem köd jeként segíthet nekünk az új és jöv beli fenyegetésekkel szembeni védelem meger sítésében. A valós idej védelmi hálózat statisztikai adatokat gy jt egyes ismeretlen, ártalmas vagy gyanús alkalmazásokról, illetve azoknak az adott eszközön végzett tevékenységeir l. Ezek az adatok névtelenek, és a szolgáltatás kombinált adatelemzés céljából küldi el azokat az F-Secure Corporation vállalatnak. Ezt követ en, az elemzésen átesett információk segítségével továbbfejlesztjük az eszközök legújabb fenyegetések és kártékony fájlok elleni védelmét.

A valós idej védelmi hálózat m ködése

A valós idej védelmi hálózat közrem köd jeként információkat adhat az ismeretlen alkalmazásokról és webhelyekr l, valamint a káros alkalmazásokról és webhelyekr l. A valós idej védelmi hálózat nem követi nyomon az Ön webes aktivitását, nem gy jt információt a már elemzett webhelyekr l, és nem gy jt adatokat a számítógépre telepített vírusmentes alkalmazásokról.

Ha nem szeretne ezekkel az adatokkal hozzájárulni a szolgáltatás m ködéséhez, akkor a valós idej védelmi hálózat nem gy jti a telepített alkalmazásokkal vagy a felkeresett webhelyekkel kapcsolatos információkat. A terméknek ugyanakkor az alkalmazások, webhelyek, üzenetek és más objektumok besorolása érdekében le kell kérdeznie az F-Secure kiszolgálóit. A lekérdezés kriptografikus ellen rz összeg használatával történik, amely során magát a lekérdezett objektumot nem küldi el a program az F-Secure vállalatnak. Az adatokat nem felhasználónként követjük nyomon, csupán a fájl vagy a webhely találatszámlálóját növeljük.

A valós idej védelmi hálózatra irányuló teljes forgalom leállítása nem lehetséges, mivel az a termék által biztosított védelem integrált része.

A valós idej védelmi hálózat el nyei

A valós idej védelmi hálózat gyorsabb és pontosabb védelmet tesz lehet vé a legújabb fenyegetésekkel szemben, és a valójában nem ártalmas gyanús alkalmazások esetén szükségtelenül megjelen riasztásokat is kiküszöböli.

A valós idej védelmi hálózat közrem köd jeként segíthet nekünk új és fel nem ismert kártev ket találni, valamint eltávolítani az esetleges hibásan vírusként felismert elemeket a vírusdefiníciós adatbázisból.

A valós idej védelmi hálózat minden résztvev je segítheti egymást. Amikor a valós idej védelmi hálózat gyanús alkalmazást talál eszközén, kihasználhatja a más eszközökön már észlelt alkalmazások elemzési eredményeib l származó el nyöket. A valós idej védelmi hálózat fokozza az eszköz általános teljesítményét,

mivel a telepített biztonsági terméknek nem kell újra megvizsgálnia a valós idej védelmi hálózat által már elemzett és tisztának talált alkalmazásokat. Hasonlóképpen, a valós idej védelmi hálózaton keresztül a kártékony webhelyekkel és a kéretlen tömeges üzenetekkel kapcsolatos információkat is megosztja, aminek következtében pontosabb védelmet biztosíthatunk a webhelyek biztonsági réseivel és a spamekkel szemben.

Minél több felhasználó m ködik közre a valós idej védelmi hálózatban, annál védettebbek lesznek a résztvev k.

Az összegy jtött adatok

A valós idej védelmi hálózat közrem köd jeként Ön az eszközén és az Ön által felkeresett webhelyeken tárolt alkalmazások adataival járulhat hozzá ahhoz, hogy a valós idej védelmi hálózat védelmet biztosíthasson a legújabb kártékony alkalmazásokkal és gyanús webhelyekkel szemben.

A fájlok besorolásának elemzése

A valós idej védelmi hálózat csak olyan alkalmazásokról gy jt információt, amelyek besorolása ismeretlen, illetve gyanús vagy ártalmasnak ismert fájlokról.

A valós idej védelmi hálózat anonim információkat gy jt az eszközön lév vírusmentes és gyanús fájlokról. A valós idej védelmi hálózat csak a futtatható fájlokról gy jt információt (például Portable Executable fájlok Windows platformon, amelyek kiterjesztése .cpl, .exe, .dll, .ocx, .sys, .scr és .drv lehet).

Az összegy jtött információk a következ ket tartalmazzák:

- az az elérési út, ahol az alkalmazás megtalálható az eszközön,
- a fájl mérete, valamint létrehozásának vagy módosításának dátuma,
- fájlattribútumok és jogosultságok,
- a fájl aláírási adatai,
- a fájl aktuális verziója és az azt létrehozó vállalat,
- a fájl eredete vagy letöltési URL-címe, valamint
- Az F-Secure DeepGuard és a víruskeresés elemzésének eredménye a vizsgált fájlokról, valamint
- további hasonló információk.

A valós idej védelmi hálózat soha nem gy jt információkat a személyes dokumentumokról, kivéve ha azokban vírust talál. A rosszindulatú fájlok minden típusáról összegy jti a vírus nevét és a fájl megtisztítási állapotát.

A valós idej védelmi hálózat segítségével arra is lehet ség van, hogy a gyanús alkalmazásokat elemzésre küldje. Az elküldend alkalmazások csak hordozható végrehajtható fájlok lehetnek. A valós idej védelmi hálózat soha nem gy jt adatokat személyes dokumentumairól, és azokat nem küldi automatikusan elemzésre.

Fájlok küldése elemzésre

A valós idej védelmi hálózat segítségével arra is lehet ség van, hogy a gyanús alkalmazásokat elemzésre küldje.

Amikor a termék megjeleníti az erre vonatkozó lehet séget, manuálisan, egyénileg elküldheti a gyanús alkalmazásokat. Elemzésre kizárólag hordozható végrehajtható fájlok küldhet k. A valós idej védelmi hálózat személyes dokumentumait soha nem tölti fel.

A webhely besorolásának elemzése

A valós idej védelmi hálózat nem követi nyomon az Ön internetes tevékenységét, és nem gy jt adatokat a már elemzett webhelyekr l, hanem az internetböngészés közben ellen rzi, hogy a felkeresett webhelyek biztonságosak-e. Amikor ellátogat egy webhelyre, a valós idej védelmi hálózat ellen rzi annak biztonságosságát, és értesítést jelenít meg, ha a webhely gyanús vagy ártalmas besorolású.

Ha a felkeresett webhely kártékony vagy gyanús tartalmat vagy egy ismert biztonsági rést tartalmaz, a valós idej védelmi hálózat a webhely teljes URL-címét begy jti, hogy a weblap teljes tartalmát elemezni tudja.

Ha egy olyan webhelyre látogat, amely még nincs besorolva, a valós idej védelmi hálózat begy jti a tartomány és az altartomány nevét, és egyes esetekben a felkeresett oldal elérési útját is a webhely elemzése és besorolása érdekében. Az adatvédelem érdekében minden olyan URL-paramétert eltávolítunk, amely személyes azonosításra alkalmas adatokat tartalmazhat.

Megjegyzés: A valós idej védelmi hálózat magánhálózatokban nem végzi el a weblapok besorolását vagy elemzését, így soha nem gy jt adatokat a magánhálózati IP-címeken (például vállalati intraneteken).

A rendszeradatok elemzése

A valós idej védelmi hálózat az operációs rendszer nevét és verzióját, az internetkapcsolattal kapcsolatos információkat, valamint a valós idej védelmi hálózat használatával kapcsolatos statisztikai adatokat (például a webhelybesorolás lekérdezéseinek számát és a lekérdezés átlagos válaszadási idejét) gy jti össze annak érdekében, hogy nyomon követhessük és továbbfejleszthessük a szolgáltatást.

Adatvédelmi irányelveink

Az adatok átvitelét biztonságosan végezzük, és automatikusan eltávolítunk azokból minden esetleges személyes információt.

A valós idej védelmi hálózat eltávolítja az azonosításra alkalmas adatokat, miel tt elküldené azokat az F-Secure vállalatnak, és az illetéktelen hozzáférés elleni védelem érdekében az átvitel során minden összegy jtött információt titkosít. Az összegy jtött adatok feldolgozása nem egyenként történik, hanem más közrem köd k információival együtt, csoportosan. Minden adat elemzése statisztikai módszerekkel és névtelenül történik, ami azt jelenti, hogy semmilyen információ nem lesz köthet Önhöz semmilyen módon.

Az összegy jtött adatok között nem szerepel semmilyen személyes azonosításra alkalmas információ. A valós idej védelmi hálózat nem gy jti össze személyes IP-címeit vagy személyes információit, például e-mail címeit, felhasználóneveit és jelszavait. Habár minden er feszítésünkkel arra törekszünk, hogy minden, személyes azonosításra alkalmas információt eltávolítsunk, bizonyos esetekben el fordulhat, hogy az összegy jtött információk között maradnak ilyen adatok. Ezekben az esetekben az ilyen akaratlanul összegy jtött adatokat nem használjuk fel.

Szigorú biztonsági intézkedésekkel és fizikai, felügyeleti és m szaki óvintézkedésekkel biztosítjuk az átvitel, tárolás és feldolgozás alatt álló adatok védelmét. Az adatokat biztonságos helyeken és az általunk felügyelt, irodáinkban vagy alvállalkozóink irodáiban található kiszolgálókon tároljuk. Az összegy jtött információkhoz kizárólag az erre jogosult személyzet férhet hozzá.

Az F-Secure az összegy jött adatokat megoszthatja leányvállalataival, alvállalkozóival, terjeszt ivel és partnereivel, de kizárólag azonosíthatatlan, névtelen formátumban.

Közrem ködés a valós idej védelmi hálózatban

Segíheti a valós idej védelmi hálózat által biztosított védelem továbbfejlesztését, ha információkkal szolgál a kártékony programokkal és webhelyekkel kapcsolatban.

A valós idej védelmi hálózatban való részvételt a telepítés során állíthatja be. Az alapértelmezett beállításokkal közrem ködik a valós idej védelmi hálózatban. A beállítást kés bb is módosíthatja a termékben.

A valós idej védelmi hálózat beállításainak módosításához kövesse az alábbi utasításokat:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **Általános beállítások megnyitása** lehet séget.
3. Válassza az **Egyebek** > **Adatvédelem** lehet séget.
4. Ha a valós idej védelmi hálózat közrem köd je szeretne lenni, jelölje be a részvételt biztosító jelöl négyzetet.

A valós idej védelmi hálózattal kapcsolatos kérdések

Elérhet ségi adatok a valós idej védelmi hálózattal kapcsolatban felmerült kérdések esetére.

A valós idej védelmi hálózattal kapcsolatos további kérdéseivel az alábbi elérhet ségekhez fordulhat:

F-Secure Corporation

Tammasaarenkatu 7

PL 24

00181 Helsinki

Finland

http://www.f-secure.com/en/web/home_global/support/contact

A jelen irányelvek legújabb változata mindig elérhet webhelyünkön.

Honnan tudhatom, hogy érvényes-e az el fizetésem?

Az el fizetés típusa és állapota az **El fizetés állapota** lapon látható.

Ha az el fizetés hamarosan lejár vagy már lejárt, a program teljes védelmi állapota módosul a megfelel indítópultikonon.

Az el fizetés érvényességének ellen rzése:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **El fizetések megtekintése** lehet séget.
3. Az **El fizetés állapota** lehet séget választva megtekintheti a telepített programokhoz tartozó el fizetések adatait.
4. A **Telepítési állapot** elemre kattintva megtudhatja, hogy milyen programok érhet k el telepítésre.

Az el fizetés állapota és lejárati ideje a program **Statisztika** lapján is megtekinthet . Ha lejárt az el fizetése, meg kell újítania az el fizetést, hogy továbbra is kapjon frissítéseket és használhassa a terméket.

Megjegyzés: Ha lejárt az el fizetése, a rendszertálcán villog az állapotikon.

M veleti központ

A m veleti központ minden olyan fontos értesítést megjelenít, amely számot tart az Ön figyelmére.

Ha el fizetése lejárt vagy hamarosan lejár, a m veleti központ értesítést küld róla. A m veleti központ által küldött üzenet háttérszíne és tartalma az el fizetés típusától és állapotától függ:

- Ha el fizetése hamarosan lejár és nem áll rendelkezésre ingyenes el fizetés, az üzenetben fehér háttérel egy **Aktiválás** gomb látható.
- Ha el fizetése hamarosan lejár és nem áll rendelkezésre ingyenes el fizetés, az üzenetben sárga háttérrel egy **Vásárlás** és egy **Kulcs megadása** gomb látható. Ha már vásárolt új el fizetést, a **Kulcs megadása** gombra kattintva megadhatja el fizet i kulcsát, és aktiválhatja új el fizetését.
- Ha el fizetése lejárt és nem áll rendelkezésre ingyenes el fizetés, az üzenetben piros háttérrel egy **Aktiválás** gomb látható.

- Ha lejárt az el fizetése és nem áll rendelkezésre ingyenes el fizetés, az üzenetben piros háttérrel egy **Vásárlás** és egy **Kulcs megadása** gomb látható. Ha már vásárolt új el fizetést, a **Kulcs megadása** gombra kattintva megadhatja el fizet i kulcsát, és aktiválhatja új el fizetését.

Megjegyzés: A m veleti központ **Értesítési el zmények megjelenítése** hivatkozásával a termék értesítései jeleníthet k meg, nem pedig a m veleti központ korábbi üzenetei.

El fizetés aktiválása

Ha új el fizet i kulccsal vagy kampánykóddal rendelkezik egy termékhez, aktiválnia kell azt.

El fizetés aktiválása:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
   Ekkor megjelenik egy el ugró menü.
2. Válassza az **El fizetések megtekintése** lehet séget.
3. Válasszon egyet az alábbi lehet ségek közül:
   - Kattintson az **El fizetés aktiválása** elemre.
   - Válassza a **Kapmpánykód aktiválása** lehet séget.
4. A megnyíló párbeszédpanelen adja meg az új el fizet i kulcsot vagy kampánykódot, és kattintson az **OK** gombra.

   Tipp: Ha az el fizet i kulcsot e-mailben kapta meg, másolja ki az üzenetben található kulcsot, majd illessze be a mez be.

Az új el fizet i kulcs beírása után az új el fizetés érvényességi dátuma az **El fizetés állapota** lapon látható.

3

. fejezet

Bevezetés

Témák:

- *A védelem általános állapotának megtekintése*
- *Termékstatisztika megtekintése*
- *Termékfrissítések kezelése*
- *Mik a vírusok és kártékony szoftverek?*

Ez a termék megvédi számítógépét a vírusoktól és más veszélyes alkalmazásoktól.

A termék automatikusan átvizsgálja a fájlokat, elemzi az alkalmazásokat és telepíti a frissítéseket. Nem igényel semmilyen felhasználói beavatkozást.

A védelem általános állapotának megtekintése

Az **Állapot** lap a telepített termékszolgáltatások és azok aktuális állapotának gyors áttekintését biztosítja.

Az **Állapot** lap megnyitása:

A f lapon kattintson az **Állapot** elemre.

Megnyílik az **Állapot** lap.

Az ikonok a program és a hozzá tartozó biztonsági funkciók állapotát jelenítik meg.

Állapotikon	Állapot neve	Leírás
	OK	A számítógép védelme aktív. A funkció be van kapcsolva, és megfelel en m ködik.
	Információ	A termék értesítést küld egy funkció speciális állapotáról. Ilyen például, ha egy funkció épp frissítés alatt áll.
	Figyelmeztetés	A számítógép védelme nem teljes. Például a termék régóta nem lett frissítve, vagy egy funkció állapota figyelmet igényel.
	Hiba	A számítógép nem védett Például lejárt az el fizetése, vagy egy kritikus fontosságú funkció ki van kapcsolva.
	Kikapcsolt	Egy nem kritikus funkció ki van kapcsolva.

Termékstatisztika megtekintése

Megtekintheti a program által a telepítés óta végzett m veleteket a **Statisztika** lapon.

A **Statisztika** lap megnyitása:

A f lapon kattintson a **Statisztika** elemre.

Megnyílik a **Statisztika** oldal.

- Az **Utolsó sikeres frissítésellen rzés** a legutóbbi frissítés id pontját jeleníti meg.
- A **Vírus- és kémprogramvizsgálat** megjeleníti, hogy hány fájlt vizsgált és tisztított meg a termék a telepítés óta.
- **Alkalmazások** - Megjeleníti, hogy a DeepGuard hány programot engedélyezett vagy tiltott le a telepítés óta.

- A **T zfalkapcsolatok** a telepítés óta engedélyezett és blokkolt kapcsolatok számát jeleníti meg.
- A **Levélszemét és adathalászat sz rése** a termék által érvényesként és levélszemétként azonosított e-mailek számát jeleníti meg.

Termékfrissítések kezelése

A termék automatikusan naprakészen tartja a védelmi funkciókat.

Adatbázis-verziók megtekintése

Az utolsó frissítések dátumát és a verziószámokat az **Adatbázis-frissítések** lapon tekintheti meg.

Az **Adatbázis-frissítések** lap megnyitásához:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza az **Egyéb beállítások** > **Adatbázis-verziók** lehet séget.

Az **Adatbázis-verziók** lapon a vírus- és kémprogram-definíciós adatbázis, a DeepGuard, illetve a levélszemét- és adathalászat-sz rés frissítésének utolsó dátuma és az ahhoz kapcsolódó verziószám látható.

A mobil szélessáv beállításainak módosítása

Döntse el, hogy letölti-e a biztonsági frissítéseket, ha mobil szélessávot használ.

Megjegyzés: Ez a funkció csak Microsoft Windows 7 rendszerben érhet el.

Alapértelmezés szerint a biztonsági frissítések mindig letölt dnek, ha saját hálózatát használja, más hálózatok elérésekor azonban a program felfüggeszti a frissítéseket. Ennek az az oka, hogy a csatlakozás költsége hálózatonként, például országonként eltér . Érdemes ezt a beállítást változatlanul hagyni, ha utazás közben is változatlan sávszélességgel és költségekkel számol.

Megjegyzés: Ez a beállítás csak mobil szélessávú csatlakozáskor van érvényben. Ha a számítógép rögzített vagy vezeték nélküli hálózathoz csatlakozik, a termék automatikusan frissül.

A beállítás módosítása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza az **Egyéb beállítások** > **Mobil szélessáv** > **Biztonsági frissítések letöltése** lehet séget.
3. Válassza ki a mobil csatlakozáshoz használni kívánt frissítési beállítást:
   - **Csak a saját hálózatban**

     A frissítések a saját hálózatban mindig letölt dnek, más hálózat használatakor azonban a program felfüggeszti ket. Javasoljuk, hogy ezt a beállítást válassza, így a tervezett költségeken belül tarthatja naprakészen a terméket.
   - **Soha**

     Nem lesznek letöltve a frissítések, ha mobil szélessávú kapcsolatot használ.
   - **Mindig**

     A frissítések a használt hálózattól függetlenül mindig letölt dnek. Akkor válassza ezt a beállítást, ha a költségekt l függetlenül mindig naprakészen kívánja tartani a számítógép védelmét.

4. Ha minden alkalommal külön szeretne dönteni, amikor nem saját hálózatban van, válassza a **Rákérdezés minden alkalommal a saját hálózat elhagyásakor** lehet séget.

Biztonsági frissítések felfüggesztve

Ha saját hálózaton kívüli mobil szélessávot használ, a biztonsági frissítések felfüggeszthet k.

Ilyenkor a **Felfüggesztve** értesítés jelenik meg a képerny jobb alsó sarkában. A frissítéseket a program felfüggeszti, mert például a csatlakozás költsége hálózatonként változik a különböz országokban. Érdemes ezt a beállítást változatlanul hagyni, ha utazás közben is változatlan sávszélességgel és költségekkel számol. Ha mégis a beállítás módosítása mellett dönt, kattintson a **Módosítás** hivatkozásra.

Megjegyzés:

Ez a funkció csak Microsoft Windows 7 rendszeren érhet el.

Mik a vírusok és kártékony szoftverek?

A kártékony szoftverek kimondottan azért készülnek, hogy károsítsák a számítógépét, az Ön tudomása nélkül törvénybe ütköz célokra használják vagy információkat lopjanak el arról.

A kártékony szoftverek:

- átvehetik a webböngész irányítását,
- átirányíthatják a keresési kísérleteket,
- nemkívánt hirdetéseket jeleníthetnek meg,
- eltárolhatják a meglátogatott webhelyek címét,
- személyes információkat, például banki adatokat lophatnak el,
- levélszemetet küldhetnek a számítógépr l és
- más számítógépeket támadhatnak meg a számítógépr l.

A kártékony szoftverek a számítógép lelassulását vagy instabilitását is okozhatják. Elképzelhet , hogy *kártékony szoftver*ek támadták meg a számítógépét, ha az hirtelen lelassult, és gyakran összeomlik.

Vírusok

A vírusok általában olyan programok, amelyek csatolni tudják magukat fájlokhoz, és meg tudják magukat többszörözni. El fordulhat, hogy úgy módosítják vagy cserélik le fájlok tartalmát, hogy az kárt tesz a számítógépében.

A *vírus*ok olyan programok, amelyek általában a tudta nélkül telepít dnek a számítógépére. A telepítés után a vírus megpróbálja többszörözni önmagát. A vírus:

- a számítógép er forrásait közepes mértékben foglalja le,
- el fordulhat, hogy módosít vagy károsít fájlokat a számítógépén,
- valószín leg felhasználja a számítógépét, hogy más számítógépeket is megfert zzön,
- el fordulhat, hogy törvénybe ütköz célokra használja a számítógépét.

Kémprogram

A kémprogramok olyan programok, amelyek a személyes adatait gy jtik össze.

A kémprogramok személyes információkat gy jtenek, beleértve:

- a megtekintett internetes oldalakat,
- a számítógépen található e-mail címeket,
- jelszavakat vagy

- hitelkártyaszámokat.

A kémprogramok szinte mindig a felhasználó kifejezett engedélye nélkül telepítik magukat. A kémprogramok telepítése a hasznos programokkal együtt történhet, vagy akkor, ha egy félrevezet felugró ablak ráveszi, hogy valamire rákattintson az ablakban.

Rootkitek

A rootkitek olyan programok, amelyek más, nehezen megtalálható *kártékony szoftver*eket hoznak létre.

A rootkitek fájlokat és folyamatokat rejtenek el. Általában azért teszik ezt, hogy a kártékony folyamatokat elrejtsék a számítógépen. Ha egy rootkit *kártékony szoftver*t rejt el a számítógépén, akkor nem egyszer észrevenni, hogy a számítógépen egy kártékony szoftver található.

Ez a termék rootkitvizsgálót is tartalmaz, amely kimondottan a rootkiteket vizsgálja, így a *kártékony szoftver*ek nehezebben rejt zhetnek el a számítógépén.

Veszélyes program

A veszélyes programok célja nem feltétlenül a károkozás, de nem megfelel használat esetén kárt tehetnek a számítógépben.

A veszélyes programok nem a kártékony szoftverek közül kerülnek ki. Ezek a programok általában hasznos, de esetenként veszélyes m veleteket hajtanak végre.

Ilyen veszélyes programok például:

- azonnali üzenetküld szolgáltatások, például az IRC (IRC – Internet Relay Chat, internetes csevegés),
- a két számítógép közötti internetes fájlátvitelre használt programok,
- internetes telefonprogramok, például a VoIP (*Voice over Internet Protocol*),
- Távoli hozzáférést biztosító szoftverek, például a VNC,
- scareware-ek, amelyek megpróbálják megijeszteni vagy becsapni a felhasználót, hogy megvásároljon valamilyen hamis biztonsági szoftvert vagy
- a CD-ellen rzések és a másolásvédelem kijátszására kialakított szoftverek.

Ha szándékosan telepítette és megfelel en beállította a programot, akkor kicsi a valószín sége, hogy problémát okozzon.

Ha a veszélyes program a tudta nélkül települt a rendszerre, akkor valószín leg károkozási szándékkal került oda, ezért el kell távolítani.

4

. fejezet

A számítógép védelme a kártékony szoftverekkel szemben

Témák:

- *A számítógép vizsgálata*
- *Fájlok kizárása a vizsgálatból*
- *A karantén használata*
- *Bels ok*

A vírus- és kémprogramvizsgálat a kiszolgálót veszélyeztet , a személyes információk megszerzésére vagy az illegális tevékenységekre irányuló programok ellen védi a számítógépet.

Alapértelmezés szerint a program azonnal kezeli az összes kártékony szoftvert, amint megtalálja ket, így nem okozhatnak kárt.

Alapértelmezés szerint a vírus- és kémprogramvizsgálat a helyi merevlemezeken, a hordozható adattárolókon (például hordozható meghajtókon vagy CD-ken) és a letöltött tartalmakban végez automatikus vizsgálatot. A program az e-mailek automatikus vizsgálatára is beállítható.

A vírus- és kémprogramvizsgálat olyan változásokat is keres a számítógépen, amelyek *kártékony szoftverekre* utalhatnak. Ha a program bármilyen veszélyes rendszerváltoztatási kísérletet, például a rendszerbeállítások változtatását vagy fontos rendszerfolyamatok változtatását észleli, a DeepGuard leállítja a programot, mivel az valószín leg *kártékony szoftver*.

A számítógép vizsgálata

A vírus- és kémprogramvizsgálat bekapcsolt állapotban automatikusan átvizsgálja a számítógépet veszélyes fájlok után kutatva. Szükség esetén végezhet még manuális és ütemezett vizsgálatot is.

A vírus- és kémprogramvizsgálatot célszer folyamatosan bekapcsolt állapotban tartani. Ha szeretné biztosan tudni, hogy nincs a számítógépén veszélyes fájl, vagy ha a valós idej vizsgálatból kizárt fájlokat is szeretné ellen rizni, akkor végezzen manuális vizsgálatot is.

Ütemezett vizsgálat beállításával el re megadhatja az id pontokat, amikor szeretné, hogy a vírus- és kémprogramvizsgálat eltávolítsa számítógépér l a veszélyes fájlokat.

Fájlok automatikus vizsgálata

A valós idej vizsgálat úgy védi a számítógépet, hogy ellen riz minden megnyitott fájlt, és letiltja a hozzáférést azokhoz a fájlokhoz, amelyek *kártékony szoftvereket* tartalmaznak.

Amikor a számítógép megpróbál hozzáférni egy fájlhoz, a valós idej vizsgálat ellen rzi a fájlt a hozzáférés engedélyezése el tt. Ha a valós idej vizsgálat veszélyes tartalmat észlel, a fájlt a karanténba helyezi, miel tt még bajt okozhatna.

Lehet negatív hatása a valós idej vizsgálatnak a számítógép teljesítményére?

A vizsgálat általában nem vehet észre, mert csak kevés id t, és a számítógép teljesítményének kis részét veszi igénybe. A valós idej vizsgálat er forrás-igénye és id szükséglete többek között a fájl tartalmától, helyét l és típusától függ.

A vizsgálat több id t vesz igénybe a következ fájlok esetében:

- Cserélhet meghajtókon, például CD-, DVD- és USB-meghajtókon lév fájlok.
- Tömörített fájlok, például a *.zip*-fájlokat.

  Megjegyzés: A tömörített fájlokat a program alapértelmezés szerint nem vizsgálja.

A valós idej vizsgálat lelassíthatja a számítógépet, ha:

- Olyan számítógépet használ, amely nem felel meg a rendszerkövetelményeknek.
- Egyidej leg sok fájlhoz próbál hozzáférni, például megnyit egy olyan mappát, amely számos ellen rzend fájlt tartalmaz.

A valós idej vizsgálat be- vagy kikapcsolása

A valós idej vizsgálatot ajánlott bekapcsolva hagyni, hogy megállíthassa a *kártékony programokat*, miel tt még azok kárt tehetnének a számítógépben.

A valós idej vizsgálat be- vagy kikapcsolása:

1. A f lapon kattintson az **Állapot** elemre.
2. Kattintson **Az ezen az oldalon lév beállítások módosítása** elemre.

   Megjegyzés: A biztonsági szolgáltatások kikapcsolásához rendszergazdai jogosultság szükséges.

3. Kapcsolja be vagy ki a **Vírus- és kémprogramvizsgálat** funkciót.
4. Kattintson a **Bezárás** gombra.

Káros fájlok automatikus kezelése

A valós idej vizsgálat képes automatikusan, felhasználói beavatkozás nélkül kezelni a veszélyesként észlelt fájlokat.

Ha szeretné, hogy a valós idej vizsgálat automatikusan kezelje a veszélyes fájlokat:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Káros fájlok automatikus kezelése** lehet séget.

Ha nincs engedélyezve a káros fájlok automatikus kezelése, a valós idej vizsgálat ilyen fájl észlelése esetén megkérdezi, hogy mit szeretne tenni.

Kémprogramok kezelése

A vírus- és kémprogramvizsgálat azonnal letiltja a kémprogramokat, amint azok megpróbálnak elindulni.

Miel tt még el tudna indulni a kémprogram, a termék letiltja azt, és megkérdezi Önt, hogy mit szeretne tenni.

Kémprogram észlelése esetén az alábbi m veletek közül választhat:

Végrehajtandó m velet	Mi történjen a kémprogrammal?
Automatikus kezelés	A termék eldönti a talált kémprogram alapján, hogy melyik az ideális m velet.
Kémprogram karanténba helyezése	Karanténba helyezi a kémprogramot, ahol az már nem okozhat kárt a számítógépen.
Kémprogram törlése	Eltávolítja a kémprogramhoz kapcsolódó összes fájlt a számítógépr l.
Csak a kémprogram letiltása	Letiltja a kémprogramhoz való hozzáférést, de továbbra is a számítógépen hagyja azt.
Kémprogram kizárása a vizsgálatból	Hagyja futni a kémprogramot, és kizárja azt a kés bbi vizsgálatokból.

Veszélyes programok kezelése

A vírus- és kémprogramvizsgálat azonnal letiltja a veszélyes programokat, amint azok megpróbálnak elindulni.

Miel tt még el tudna indulni a veszélyes program, a termék letiltja azt, és megkérdezi Önt, hogy mit szeretne tenni.

Veszélyes program észlelése esetén az alábbi m veletek közül választhat:

Végrehajtandó m velet	Mi történjen a veszélyes programmal
Csak a veszélyes program letiltása	Letiltja a veszélyes programhoz való hozzáférést, de továbbra is a számítógépen hagyja azt.
Veszélyes program karanténba helyezése	Karanténba helyezi a veszélyes programot, ahol az már nem okozhat kárt a számítógépen.
Veszélyes program törlése	Eltávolítja a veszélyes programhoz kapcsolódó összes fájlt a számítógépr l.
Veszélyes program kizárása a vizsgálatból	Hagyja futni a veszélyes programot, és kizárja azt a kés bbi vizsgálatokból.

Nyomkövet cookie-k automatikus eltávolítása

A nyomkövet cookie-k eltávolításával meggátolhatja a webhelyeket abban, hogy kövessék, milyen más webhelyeket látogat meg az interneten.

A nyomkövet cookie-k olyan kisméret fájlok, amelyekkel a webhelyek rögzíteni tudják, hogy Ön milyen más webhelyeket keres fel. Kövesse az utasításokat, ha szeretné számítógépét ezekt l a fájloktól mentesen tartani.

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Nyomkövet cookie-k eltávolítása** lehet séget.
4. Kattintson az **OK** gombra.

Fájlok manuális vizsgálata

Igény esetén manuálisan is végezhet vizsgálatot. Ez például akkor lehet hasznos, ha küls eszközt csatlakoztat a számítógéphez, és szeretné biztosan tudni, hogy nem található rajta kártékony program.

Manuális vizsgálat indítása

A vizsgálatot végezheti a teljes számítógépen, kereshet adott típusú *kártékony szoftver*eket, vagy ellen rizhet egy adott helyet is.

Ha arra gyanakszik, hogy egy adott típusú *kártékony szoftver* van a gépén, rákereshet csak arra a típusra is. Ha arra gyanakszik, hogy a számítógép egy adott helye fert zött, korlátozhatja a vizsgálatot arra az egy helyre is. Az ilyen keresések sokkal gyorsabban befejez dnek, mint a teljes számítógép átvizsgálása.

Kézi vizsgálat elindítása:

1. A f lapon kattintson a **Vizsgálat** alatti nyílra.

   Megjelennek a vizsgálati beállítások.

2. Vizsgálat típusának kiválasztása

   Válassza a **Vizsgálati beállítások megváltoztatása** lehet séget, ha testre szeretné szabni, hogy a manuális vizsgálat hogyan ellen rizze számítógépén a vírusokat és más veszélyes alkalmazásokat.

3. Ha a **Vizsgálandó hely kiválasztása** lehet séget választja, egy ablak jelenik meg, amelyben kiválaszthatja a vizsgálandó helyeket.
   Megnyílik a **Vizsgálat varázsló** párbeszédpanel.

Vizsgálatok típusai

A vizsgálatot végezheti a teljes számítógépen, adott típusú kártékony szoftvereken vagy egy megadott helyen is.

A következ lista a vizsgálatok különböz típusait tartalmazza:

Vizsgálat típusa	Mit vizsgál	Mikor használandó ez a típus
Vírus- és kémprogramvizsgálat	A számítógép részein vírusokat, kémprogramokat és veszélyes programokat	Ez a vizsgálattípus sokkal gyorsabb, mint a teljes vizsgálat. Csak a rendszer azon részeit vizsgálja, amelyek telepített programfájlokat tartalmaznak. Ez a keresési típus akkor ajánlott, ha gyorsan szeretné ellen rizni a számítógép tisztaságát, mert képes a számítógépen található aktív kártékony szoftverek hatékony megkeresésére és eltávolítására.
Teljes számítógépvizsgálat	A teljes számítógépen (a bels és a küls merevlemezeken) vírusokat, kémprogramokat és veszélyes programokat	Ha teljesen biztos szeretne lenni abban, hogy nem találhatók kártékony szoftverek vagy veszélyes programok a számítógépén. Ez a vizsgálati típus igényli a legtöbb id t. Kombinálja a kártékony programok gyors vizsgálatát és a merevlemez

Vizsgálat típusa	Mit vizsgál	Mikor használandó ez a típus
		vizsgálatát. A rootkitek által lehetségesen elrejtett elemeket is ellen rzi.
A vizsgálandó fájlok kijelölése	Egy adott fájlban, mappában vagy meghajtón vírusokat, kémprogramokat és veszélyes programokat	Ha azt gyanítja, hogy a számítógép egy adott helyén esetleg kártékony szoftver található, például az adott helyen lehetségesen veszélyes forrásokból letöltött elemek (például fájlcserél rendszerekb l letöltött fájlok) találhatók. A vizsgálat ideje a vizsgált célmappa méretét l függ. A vizsgálat gyorsan befejez dik, ha például egy néhány kis méret fájlt tartalmazó mappában végzi azt.
Rootkitvizsgálat	A fontos rendszerelemeket tartalmazó helyeket, ahol egy gyanús elem biztonsági problémát vethet fel. Rejtett fájlokat, mappákat, meghajtókat vagy folyamatokat vizsgál	Ha azt gyanítja, hogy egy rootkit települhetett a számítógépre. Ha például a program nemrégiben kártékony szoftvert észlelt a számítógépen, és meg szeretne gy z dni arról, hogy nem telepített rootkitet.

Vizsgálat a Windows Intéz programban

A Windows Intéz programban *vírusok*at, *kémprogram*okat, és *veszélyes program*okat kereshet a lemezeken, a mappákban és a fájlokban.

Lemez, mappa vagy fájl vizsgálata:

1. Mozgassa az egérmutatót arra a lemezre, mappára vagy fájlra, amelyben vizsgálatot szeretne végezni, és kattintson a jobb gombbal.
2. A jobb kattintásra megjelen helyi menüben kattintson a **Mappák vírusvizsgálata** parancsra. (Ennek neve attól függ en változik, hogy éppen lemezt, mappát vagy fájlt ellen riz.)
   Megnyílik a **Vizsgálat varázsló** ablak, és elindul a vizsgálat.

Ha a program *vírus*t vagy *kémprogram*ot talál, a **Vizsgálat varázsló** segít elvégezni az eltávolítási lépéseket.

Vizsgálandó fájlok kijelölése

Kijelölheti a fájltípusokat, amelyekben *vírus*okat és *kémprogram*okat szeretne keresne a kézi vagy ütemezett vizsgálat során.

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza az **Egyéb beállítások** > **Kézi vizsgálat** lehet séget.
3. A **Vizsgálati beállítások** csoportban válasszon a következ beállítások közül:

Csak az ismert fájlok vizsgálata	Csak a fert zéseknek leginkább kitett fájltípusok, például a végrehajtható fájlok vizsgálata. Ha ezt a beállítást választja, a vizsgálat gyorsabb lesz. A program a következ kiterjesztés fájlokat vizsgálja: `.ani`, `.asp`, `.ax`, `.bat`, `.bin`, `.boo`, `.chm`, `.cmd`, `.com`, `.cpl`, `.dll`, `.doc`, `.dot`, `.drv`, `.eml`, `.exe`, `.hlp`, `.hta`, `.htm`, `.html`, `.htt`, `.inf`, `.ini`, `.job`, `.js`, `.jse`, `.lnk`, `.lsp`, `.mdb`, `.mht`, `.mpp`, `.mpt`, `.msg`, `.ocx`, `.pdf`, `.php`, `.pif`, `.pot`, `.ppt`, `.rtf`, `.scr`, `.shs`, `.swf`, `.sys`, `.td0`, `.vbe`, `.vbs`, `.vxd`, `.wbk`, `.wma`, `.wmv`, `.wmf`, `.wsc`, `.wsf`, `.wsh`, `.wri`, `.xls`, `.xlt`, `.xml`, `.zip`, `.jar`, `.arj`, `.lzh`, `.tar`, `.tgz`, `.gz`, `.cab`, `.rar`, `.bz2` és `.hqx`.

Tömörített fájlok vizsgálata	Tömörített fájlok és mappák vizsgálata.
Fejlett heurisztikus eljárás használata	Az új vagy ismeretlen kártékony szoftverek megtalálása érdekében az összes elérhet heurisztika használata a vizsgálat során. **Megjegyzés:** Ha ezt a lehet séget választja, a vizsgálat több id t vesz igénybe, és több hamis találattal (vagyis gyanúsként feltüntetett, de ártalmatlan fájllal) járhat.

4. Kattintson az **OK** gombra.

Megjegyzés: A kizárt elemek listájához hozzáadott fájlokat a termék nem vizsgálja meg akkor sem, ha itt megadja ket vizsgálandóként.

A veszélyes fájlok észlelésekor elvégzend m velet beállítása

Adja meg, hogy hogyan szeretné kezelni a termék által észlelt veszélyes fájlokat.

A manuális vizsgálat során talált veszélyes elemeken végrehajtandó m velet megadása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza az **Egyéb beállítások** > **Kézi vizsgálat** lehet séget.
3. A **Ha vírus vagy kémprogram található** beállításnál válassza az alábbi lehet ségek egyikét:

Lehet ség	Leírás
Teend k megkérdezése (alapérték)	A manuális vizsgálat során talált összes elemhez külön-külön megadhatja a kívánt teend t.
Fájlok tisztítása	A termék megkísérli automatikusa megtisztítani a manuális vizsgálat során talált összes fert zött fájlt. **Megjegyzés:** Ha nem sikerül megtisztítani egy fert zött fájlt, a termék azt karanténba helyezi (kivéve, ha az hálózaton vagy cserélhet adathordozón található), ahol az már nem okozhat kárt a számítógépben.
Fájlok karanténba helyezése	A termék karanténba helyezi a manuális vizsgálat során talált összes veszélyes fájlt, ahol azok már nem okozhatnak kárt a számítógépben.
Automatikus törlés	A termék törli a manuális vizsgálat során talált összes veszélyes fájlt.
Csak jelentés	A termék érintetlenül hagyja a manuális vizsgálat során talált összes veszélyes fájlt, és naplózza az észlelésüket a vizsgálati jelentésben. **Megjegyzés:** Ha a valós idej vizsgálat nincs bekapcsolva, a kártékony programok kárt okozhatnak a számítógépen, ha ezt a lehet séget választja.

Megjegyzés: Az ütemezett vizsgálat során talált veszélyes fájlokat a termék automatikusan megtisztítja.

Vizsgálat ütemezése

Ha tudja, hogy egy adott id pontban nem fogja használni a számítógépet, beállíthatja, hogy ekkor történjen a fájlok automatikus vizsgálata, valamint a vírusok és más veszélyes programok eltávolítása. Vagy rendszeres vizsgálatot is beállíthat, ha gondoskodni szeretne a számítógép tisztaságáról.

Vizsgálat ütemezése:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza az **Egyéb beállítások** > **Ütemezett vizsgálat** lehet séget.
3. Kapcsolja be az **Ütemezett vizsgálat** funkciót.
4. Adja meg a vizsgálat kezd id pontját.

Lehet ség	Leírás
Naponta	Naponta végezzen vizsgálatot a számítógépen
Hetente	A hét választott napjain végezzen vizsgálatot a számítógépen. Válassza ki a napokat a listából.
Havonta	A hónap választott napjain végezzen vizsgálatot a számítógépen. A napok kiválasztása: 1. Válasszon a **Nap** lehet ségek közül egyet. 2. Jelölje ki a hónap egy napját a kijelölt nap melletti listában.

5. Válassza ki a vizsgálat indítási id pontját a kijelölt napokhoz.

Lehet ség	Leírás
Indítás id pontja	Meghatározott id pontban indítja a vizsgálatot.
Ha a számítógépet ennyi ideje nem használták	Akkor indítja a vizsgálatot, ha a számítógép nincs használatban egy bizonyos ideig.

Az ütemezett vizsgálat a manuális vizsgálat beállításaival fut azzal a kivétellel, hogy minden alkalommal megvizsgálja a tömörített fájlokat, és automatikusan törli a veszélyes tartalmakat.

E-mailek vizsgálata

Az e-mailek vizsgálata megvédi számítógépét az e-mailben kapott veszélyes fájloktól.

Ahhoz, hogy a termék ellen rizni tudja az e-mailek vírusmentességét, a vírus- és kémprogramvizsgálatnak bekapcsolt állapotban kell lennie.

Az e-mailek vizsgálatának bekapcsolása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Káros e-mail mellékletek eltávolítása** lehet séget.
4. Kattintson az **OK** gombra.

Mikor vizsgálja meg a program az e-mail üzeneteket és csatolásokat?

A vírus- és kémprogramvizsgálat a beérkez e-mailekb l is el tudja távolítani a veszélyes tartalmakat.

A vírus- és kémprogramvizsgálat eltávolítja a levelez programokba - például a Microsoft Outlook és Outlook Express, a Microsoft Mail vagy a Mozilla Thunderbird programba - érkez veszélyes e-mail üzeneteket. A termék minden egyes alkalommal átvizsgálja az új, titkosítatlan e-mail üzeneteket és mellékleteket, amikor a levelez program üzeneteket fogad a POP3 protokollon keresztül.

A vírus- és kémprogramvizsgálat nem tudja ellen rizni a mellékleteket a böngész ben futó webes levelez programokban, ideértve a Hotmail, a Yahoo! mail és a Gmail szolgáltatást. Nem kell azonban aggódnia, mert még akkor is védett a *vírusokkal* szemben, ha nincsenek el zetesen eltávolítva a veszélyes mellékletek, vagy ha webes levelez programot használ. Az e-mail mellékletek megnyitásakor ugyanis a valós idej vizsgálat eltávolítja a veszélyes tartalmakat, miel tt még kárt okozhatnának.

Megjegyzés: A valós idej vizsgálat csak az Ön számítógépét védi, barátainak nem nyújt védelmet. Ez a vizsgálati mód csak megnyitáskor ellen rzi a csatolt fájlokat. Vagyis ha webes levelez programot használ, és továbbküld egy üzenetet, miel tt megnyitná a mellékletét, el fordulhat, hogy fert zött tartalmat küld a barátainak.

Vizsgálati eredmények megtekintése

A vírusok és kémprogramok el zményeinél megtekintheti a termék által eddig talált összes veszélyes fájlt.

Id nként el fordulhat, hogy a termék veszélyes tartalom észlelésekor nem tudja végrehajtani a megadott teend t. Ha például a fájlok tisztítását adta meg, és nem sikerül megtisztítani a fájlt, a termék karanténba helyezi azt. A vírusok és kémprogramok el zményei között ezt az információt is láthatja.

Az el zmények megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Kattintson a **Korábbi eltávolítások megtekintése** elemre.

A vírusok és kémprogramok el zményeinél az alábbi információk jelennek meg:

- A veszélyes fájl észlelésének dátuma és id pontja
- A kártev neve és helye a számítógépen
- A végrehajtott m velet

Fájlok kizárása a vizsgálatból

Esetenként el fordulhat, hogy ki kell zárnia bizonyos fájlokat vagy alkalmazásokat a vizsgálatból. A kizárt elemeket nem vizsgálja a program, hacsak el nem távolítja ket a kizárt elemek listájáról.

Megjegyzés: A valós idej és a manuális vizsgálathoz külön kizárási lista tartozik. Ha például kizár egy fájlt a valós idej vizsgálatból, akkor ezt a fájlt manuális vizsgálatkor ellen rzi a program; hacsak külön ki nem zárja a manuális vizsgálatból is.

Fájltípusok kizárása

A típus szerinti kizárás lehet vé teszi, hogy bizonyos kiterjesztéssel rendelkez fájlokat kizárjon a kés bbi vizsgálatokból.

Kizárni kívánt fájltípusok hozzáadása vagy eltávolítása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Attól függ en, hogy valós idej vagy manuális vizsgálatból szeretne-e fájltípust kizárni, hajtsa végre az alábbiak egyikét:

- Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget, ha a valós idej vizsgálatból szeretne fájltípust kizárni.
- Válassza az **Egyéb beállítások** > **Kézi vizsgálat** lehet séget, ha a kézi vizsgálatból szeretne fájltípust kizárni.

3. Kattintson a **Fájlok kizárása a vizsgálatból** elemre.
4. Fájltípus kizárása:
   a) Kattintson a **Fájltípusok** fülre.
   b) Válassza **Az alábbi kiterjesztés fájlok kivételével** lehet séget.
   c) Írja be a kizárni kívánt fájltípust azonosító fájlkiterjesztést a **Hozzáadás** gomb melletti mez be.

      A kiterjesztés nélküli fájlok megadásához írja be a „.” karaktert. Használhatja a „?” helyettesít karaktert egyetlen karakter helyettesítéséhez vagy a „*” karaktert tetsz leges számú karakter helyettesítéséhez.

      Például a futtatható fájlok kizárásához írja be az exe szöveget a mez be.
   d) Kattintson a **Hozzáadás** gombra.
5. Ismételje meg az el z lépést az összes olyan kiterjesztés esetén, amelyet ki kíván hagyni a vizsgálatból.
6. Kattintson az **OK** gombra a **Kizárás a vizsgálatból** párbeszédpanelen.
7. Kattintson az **OK** gombra az új beállítások alkalmazásához.

A megadott típusú fájlokat a termék kihagyja a kés bbi vizsgálatokból.

Fájlok kizárása azok helye alapján

Ha hely szerint zár ki fájlokat, a megadott meghajtók vagy mappák tartalmát kihagyja a program a vizsgálatból.

Kizárt helyek hozzáadása vagy eltávolítása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Attól függ en, hogy a valós idej vagy a manuális vizsgálatból szeretne-e helyet kizárni, végezze el az alábbiak egyikét:
   - Válassza a **Számítógép** > **Vírus- és kémprogramvizsgálat** lehet séget, ha a valós idej vizsgálatból szeretne helyet kizárni.
   - Válassza a **Számítógép** > **Manuális vizsgálat** lehet séget, ha a manuális vizsgálatból szeretne helyet kizárni.
3. Kattintson a **Fájlok kizárása a vizsgálatból** elemre.
4. Fájl, meghajtó vagy mappa kizárása:
   a) Kattintson az **Objektumok** fülre.
   b) Válassza az **Objektumok (fájlok, mappák stb.) kizárása** lehet séget.
   c) Kattintson a **Hozzáadás** gombra.
   d) Jelölje ki a vizsgálatból kizárni kívánt meghajtót vagy mappát.

      Megjegyzés: Egyes meghajtók lehetnek cserélhet meghajtók, például CD- vagy DVD-meghajtók, illetve hálózati meghajtók. A hálózati meghajtók és az üres cserélhet meghajtók nem zárhatók ki.

   e) Kattintson az **OK** gombra.
5. Ha más fájlokat, meghajtókat vagy mappákat is ki szeretne zárni a vizsgálatból, ismételje meg az el z lépést.
6. Kattintson az **OK** gombra a **Kizárás a vizsgálatból** párbeszédpanelen.
7. Kattintson az **OK** gombra az új beállítások alkalmazásához.

A megadott fájlokat, meghajtókat vagy mappákat a termék ki fogja hagyni a kés bbi vizsgálatokból.

Kihagyott alkalmazások megtekintése

Megtekintheti a vizsgálatból kizárt alkalmazásokat, és eltávolíthatja ket a kizárt elemek listájáról, ha szeretné, hogy a kés bbiekben a program megvizsgálja ket.

Ha a valós idej vagy a manuális vizsgálat kémprogramként vagy veszélyes programként észlel egy alkalmazást, de Ön tudja róla, hogy biztonságos, kizárhatja az alkalmazást a vizsgálatból, hogy ne jelenjen meg több figyelmeztetés.

Megjegyzés: Ha az alkalmazás vírusként vagy más kártékony szoftverként viselkedik, nem lehet kizárni.

Az alkalmazások közvetlen kizárása nem lehetséges. Új alkalmazásokat csak úgy tud felvenni a kizárási listára, ha a vizsgálat során ezt a lehet séget választja.

A vizsgálatból alkalmazások megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Attól függ en, hogy a valós idej vagy a manuális vizsgálat kizárási listáját szeretné-e megtekinteni, végezze el az alábbiak egyikét:
   - Válassza a **Számítógép** > **Vírus- és kémprogramvizsgálat** lehet séget a valós idej vizsgálatból kizárt alkalmazások megtekintéséhez.
   - Válassza a **Számítógép** > **Manuális vizsgálat** lehet séget a manuális vizsgálatból kizárt alkalmazások megtekintéséhez.
3. Kattintson a **Fájlok kizárása a vizsgálatból** elemre.
4. Kattintson az **Alkalmazások** fülre.

   Megjegyzés: Csak a kémprogramok és a veszélyes programok zárhatók ki, a vírusok nem.

5. Ha ismét meg szeretne vizsgálni egy kizárt alkalmazást:
   a) Jelölje ki az ismét megvizsgálni kívánt alkalmazást.
   b) Kattintson az **Eltávolítás** gombra.
6. Kattintson az **OK** gombra a **Kizárás a vizsgálatból** párbeszédpanelen.
7. Kattintson az **OK** gombra a kilépéshez.

A karantén használata

A karantén egy olyan tároló, amelyben biztonságosan tárolhatók a veszélyes fájlok.

A karanténban elhelyezett fájlok nem terjedhetnek tovább, és nem okozhatnak semmilyen kárt a számítógépében.

A karanténban elhelyezhet *kártékony szoftvereket*, *kémprogramokat* és *veszélyes programokat*, hogy azok ne jelentsenek veszélyt a számítógépére. Ha szükséges, kés bb visszaállíthatja a karanténban elhelyezett programokat vagy fájlokat.

Ha nincs szüksége egy karanténban lév elemre, törölheti azt. Ha töröl egy elemet a karanténból, akkor az véglegesen el lesz távolítva a számítógépér l.

- Általában törölheti a karanténban lév *kártékony szoftvere*ket.

- A legtöbb esetben törölheti a karanténban elhelyezett *kémprogram*okat. El fordulhat, hogy a karanténban lév *kémprogram* egy legális szoftver része, és ha eltávolítja azt, a program nem fog megfelel en m ködni. Ha meg kívánja tartani a szoftvert, akkor visszaállíthatja a karanténban lév *kémprogram*ot.
- A karanténban elhelyezett *veszélyes program*ok lehetnek legális szoftverek is. Ha saját kez leg telepítette a programot, visszaállíthatja azt a karanténból. Ha a *veszélyes program* a tudta nélkül telepít dött a számítógépére, akkor nagyon valószín , hogy kártékony szándékkal lett telepítve, ezért ajánlott törölnie.

Karanténba helyezett elemek megtekintése

A karanténban lév elemekr l további információt is megtudhat.

A karanténban lév elemek adatainak megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Karantén megtekintése** lehet séget.
   A **Karantén** lapon látható a karanténban tárolt elemek teljes száma.
4. Ha a karanténban lév elemek részletes adataira kíváncsi, kattintson a **Részletek** elemre.

   A tartalmat a kártékony programok neve vagy a fájl elérési útja alapján rendezheti.

   Az els 100 elem listáján megjelenik a karanténban lév elemek típusa, neve és a telepített fájlok elérési útja.
5. Ha a karanténban lév egyes elemekr l további részletekre kíváncsi, kattintson az **Állapot** oszlopban az adott elemhez tartozó ⓘ ikonra.

Karanténba helyezett elemek visszaállítása

A szükséges elemeket visszaállíthatja a karanténból.

Visszaállíthat fájlokat vagy alkalmazásokat a karanténból, ha szüksége van rájuk. Csak akkor állítson vissza elemeket a karanténból, ha biztos benne, hogy azok nem veszélyesek. A visszaállított elemek visszakerülnek az eredeti helyükre.

Karanténba helyezett elemek visszaállítása

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Karantén megtekintése** lehet séget.
4. Jelölje ki a karanténban lév , visszaállítandó elemeket.
5. Kattintson a **Visszaállítás** gombra.

Bels ok

A DeepGuard elemzi a fájlok tartalmát és az alkalmazások viselkedését, és folyamatosan figyeli a nem megbízhatóként azonosított alkalmazásokat.

A DeepGuard blokkolja az új, még ismeretlen *vírusok*at, *férgek*et és a rendszer módosítását megkísérl más veszélyes programokat, illetve letiltja az internet-hozzáférést a gyanús alkalmazások számára.

Ha a DeepGuard észleli, hogy egy alkalmazás potenciálisan káros módosítást próbál végezni a rendszeren, akkor az alkalmazás futtatását egy biztonságos zónába helyezi át, ahol az nem tud ártani a számítógépnek. A DeepGuard elemzi, hogy az alkalmazás milyen módosításokat próbált végezni, és az eredmény alapján eldönti, hogy az alkalmazás *kártev* programnak min sül-e. Ha *kártev nek* min sül, a DeepGuard letiltja az alkalmazást.

A DeepGuard által potenciálisan károsként észlelt rendszermódosítások a következ k:

- a rendszerbeállítások (Windows beállításjegyzék) változásai,
- kísérletek a fontos rendszerprogramok, például az olyan biztonsági programok kikapcsolására, mint ez a szoftver és
- a fontos rendszerfájlok szerkesztésére irányuló kísérletek.

A DeepGuard be- vagy kikapcsolása

A DeepGuard szolgáltatást ajánlott bekapcsolva hagyni, hogy meggátolhassa a gyanús alkalmazásokat abban, hogy potenciálisan káros módosításokat végezzenek a rendszerben.

Ha Windows XP rendszert használ, gy z djön meg arról, hogy telepítve van a Service Pack 2 szervizcsomag, miel tt bekapcsolja a DeepGuard szolgáltatást.

A DeepGuard be- vagy kikapcsolása:

1. A f lapon kattintson az **Állapot** elemre.
2. Kattintson **Az ezen az oldalon lév beállítások módosítása** elemre.

   Megjegyzés: A biztonsági szolgáltatások kikapcsolásához rendszergazdai jogosultság szükséges.

3. Kapcsolja be vagy ki a **DeepGuard** szolgáltatást.
4. Kattintson a **Bezárás** gombra.

A DeepGuard által letiltott alkalmazások engedélyezése

Meghatározhatja, hogy a DeepGuard mely alkalmazásokat engedélyezze, illetve tiltsa le.

Id nként el fordulhat, hogy a DeepGuard egy olyan alkalmazást tilt le, amelyet Ön futtatni szeretne, mert tudja róla, hogy biztonságos. Ez azért történik, mert az alkalmazás potenciálisan káros rendszermódosításokat próbált végezni. Emellett az is el fordulhat, hogy véletlenül tiltotta le az alkalmazást, amikor a DeepGuard korábban kérdést jelenített meg azzal kapcsolatban.

A DeepGuard által letiltott alkalmazás engedélyezése:

1. A f lapon kattintson az **Eszközök** elemre.
2. Kattintson az **Alkalmazások** gombra.
   Ekkor megjelenik a **Figyelt alkalmazások** listája.
3. Keresse meg az engedélyezni kívánt alkalmazást.

   Megjegyzés: Az oszlopfejlécekre kattintva átrendezheti a listát. Kattintson például az **Engedély** fejlécre, ha szeretné gyorsan megtekinteni az engedélyezett vagy letiltott programokat.

4. Válassza az **Engedélyezés** lehet séget az **Engedély** oszlopban.
5. Kattintson a **Bezárás** gombra.

Ezután a DeepGuard már engedélyezni fogja az alkalmazásnak, hogy rendszermódosításokat hajtson végre.

A DeepGuard használata kompatibilitási módban

A maximális védelem érdekében a DeepGuard ideiglenesen módosítja a futó programokat. Egyes programok ellen rzik, hogy nem lettek-e módosítva vagy manipulálva, és ezért nem lettek-e inkompatibilisek ezzel a

szolgáltatással. Ilyenek például a csalás elleni védelemmel ellátott online játékok, amelyek futáskor figyelik a rajtuk végzett módosításokat. Ha ilyen problémát tapasztal, bekapcsolhatja a kompatibilitási módot.

A kompatibilitási mód bekapcsolása:

1. A f lapon kattintson a **Beállítások** elemre.

   Megjegyzés: A beállítások módosításához rendszergazdai jogosultság szükséges.

2. Válassza a **Számítógép biztonsága** > **DeepGuard** lehet séget.
3. Válassza a **Kompatibilitási mód használata** lehet séget.
4. Kattintson az **OK** gombra.

Gyanús viselkedésr l szóló figyelmeztetések beállítása

A DeepGuard figyeli a nem megbízhatóként azonosított alkalmazásokat. Ha egy figyelt alkalmazás megpróbál hozzáférni az internethez, rendszermódosításokat kísérel végrehajtani vagy más módon gyanús viselkedést tanúsít, a DeepGuard letiltja.

Ha a DeepGuard beállításainál a **Figyelmeztetés megjelenítése gyanús viselkedés esetén** lehet séget választotta, akkor a DeepGuard értesíti, ha potenciálisan káros alkalmazást észlel, vagy ha ismeretlen megbízhatósági besorolású alkalmazás indul el.

A DeepGuard által letiltott alkalmazással kapcsolatos teend meghatározása:

1. Kattintson a **Részletek** gombra a program további adatainak megtekintéséhez.
   Az adatok között az alábbiakat láthatja:
   - Az alkalmazás helye
   - Az alkalmazás megbízhatósági besorolása a valós idej védelmi hálózatban
   - Az alkalmazás elterjedtsége
2. Döntse el, hogy megbízik-e a DeepGuard által letiltott alkalmazásban:
   - Válassza a **Megbízom az alkalmazásban, és folytatni szeretném a m veletet** lehet séget, ha nem szeretné, hogy le legyen tiltva az alkalmazás.

     Az alkalmazás nagyobb eséllyel biztonságos, ha:

     - A DeepGuard egy Ön által indított m velet miatt tiltotta le az alkalmazást.
     - Ön felismeri az alkalmazást.
     - Az alkalmazás megbízható forrásból származik.
   - Válassza a **Nem bízom az alkalmazásban, maradjon blokkolt** lehet séget, ha az alkalmazást letiltva szeretné tartani.

     Az alkalmazás nagyobb eséllyel veszélyes, ha:

     - Nem általánosan elterjedt.
     - Ismeretlen megbízhatósági besorolású.
     - Az Ön számára is ismeretlen.
3. Ha szeretné, hogy elemezzünk egy gyanús alkalmazást:
   a) Válassza az **Alkalmazás jelentése az F-Secure részére** (Report the application to F-Secure) lehet séget.
   A termék ekkor megjeleníti a jelentés elküldésének feltételeit.
   b) Kattintson az **Elfogadom** gombra, ha elfogadja a feltételeket, és el szeretné küldeni a mintát.

   A mintaküldés az alábbi esetekben javasolt:

- Ha a DeepGuard olyan alkalmazást tilt le, amelyr l Ön tudja, hogy biztonságos.
- Ha gyanítja, hogy az alkalmazás *kártékony szoftver*.