

F-Secure Anti-Virus 2012

Tartalom

1. fejezet: Az els lépések.....	5
Automatikus frissítés használata.....	6
Frissítés állapotának ellen rzése.....	6
Az internetkapcsolat beállításainak módosítása.....	6
A valós idej védelmi hálózat állapotának ellen rzése.....	7
A termék eredményeinek megtekintése.....	7
Értesítési el zmények megtekintése.....	7
Az értesítések beállításainak módosítása.....	7
Valós idej védelmi hálózat.....	8
Mire szolgál a valós idej védelmi hálózat?.....	8
A valós idej védelmi hálózat el nyei.....	8
Az összegy jtött adatok.....	9
Adatvédelmi irányelveink.....	10
Közrem ködés a valós idej védelmi hálózatban.....	10
A valós idej védelmi hálózattal kapcsolatos kérdések.....	11
Honnan tudhatom, hogy érvényes-e az el fizetésem?.....	11
El fizetés aktiválása.....	11
2.	
fejezet: A számítógép védelme a kártékony szoftverekkel szemben.	13
Mik a vírusok és kártékony szoftverek?.....	14
Vírusok.....	14
Kémprogram.....	14
Rootkitek.....	14
Veszélyes program.....	15
A számítógép vizsgálata.....	15
Kártékony programok vizsgálata.....	15
Ütemezett vizsgálat.....	17
Kézi vizsgálat.....	19
Vizsgálni kívánt fájlok kiválasztása.....	21
M velet kiválasztása amikor talál valamit a program.....	24
Vírusok és kémprogramok el zményeinek megtekintése.....	27
Bels ok.....	27
A DeepGuard m ködése.....	27
A DeepGuard bekapcsolása.....	28
A DeepGuard által blokkolt programok engedélyezése.....	28
A fejlett folyamatfigyelés kikapcsolása.....	28
Védelem a káros rendszermódosítások ellen.....	29

A DeepGuard eredményeinek megtekintése.....	30
A karantén használata.....	30
Karanténba helyezett elemek megtekintése.....	31
Karanténba helyezett elemek visszaállítása.....	31
A mobil szélessáv beállításainak módosítása.....	31
Biztonsági frissítések felfüggesztve.....	32

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 részben 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 rízheti, 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 hálózatához 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 esetén 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 most** 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 **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 kódése 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 érkehetnek 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 **Egyéb > 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 **Egyéb** > **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.
Ha ez a beállítás be van kapcsolva, a termék megjeleníti a szolgáltató által küldött értesítéseket.
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 találatsszámlálóját növeljük.

A valós idej védelmi hálózatra irányuló teljes forgalom leállítás 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 lehetővé 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. Elemzésre kizárólag hordozható végrehajtható fájlok küldhet k.

Elküldhet egyéni gyanús alkalmazásokat manuálisan, amikor a termék erre kéri, vagy a termékbeállításoknál bekapcsolhatja a gyanús alkalmazások automatikus feltöltését.


A valós idej védelmi hálózat soha nem tölti fel automatikusan személyes dokumentumait.

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, mielőtt 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 erőfeszítésünkkel arra törekszünk, hogy minden, személyes azonosításra alkalmas információt eltávolítsunk, bizonyos esetekben előfordulhat, 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 műszaki 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 jtött adatokat megoszthatja leányvállalataival, alvállalkozóival, terjesztőivel és partnereivel, de kizárólag azonosíthatatlan, névtelen formátumban.

Közrem ködés a valós idej védelmi hálózatban

Segítheti 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 később is módosíthatja a termékben.

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

1. Az indítópulton kattintson a jobb gombbal a jobb szélső ikonra. Ekkor megjelenik egy előugró menü.
2. Válassza az **Általános beállítások megnyitása** lehetőséget.
3. Válassza az **Egyebek > Adatvédelem** lehetőséget.
4. Ha a valós idej védelmi hálózat közrem ködés szeretne lenni, jelölje be a részvételt biztosító jelölőnégyzetet.

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 **EI fizetés állapota** lapon látható.

Ha az el fizetés hamarosan lejár vagy már lejárt, a program teljes védelmi állapota módosul a megfelelő 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 **EI fizetések megtekintése** lehet séget.
3. Az **EI 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 lejárat i 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.

EI fizetés aktiválása

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

EI fizetés aktiválása:

1. Az indítópulton kattintson a jobb gombbal a jobb széls ikonra.
Ekkor megjelenik egy el ugró menü.
2. Válassza az **EI fizetések megtekintése** lehet séget.
3. Válasszon egyet az alábbi lehet ségek közül:
 - Kattintson az **EI fizetés aktiválása** elemre.
 - Válassza a **Kampánykód 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 illesze be a mez be.

Az új el fizet i kulcs beírása után az új el fizetés érvényességi dátuma az [El fizetés állapota](#) lapon látható.

A számítógép védelme a kártékony szoftverekkel szemben

Témák:

- [Mik a vírusok és kártékony szoftverek?](#)
- [A számítógép vizsgálata](#)
- [Belső ok](#)
- [A karantén használata](#)
- [A mobil szélessáv beállításainak módosítása](#)

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 valószínűleg *kártékony szoftver*.

Mik a vírusok és kártékony szoftverek?

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

A kártékony szoftverek:

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

A kártékony szoftverek a számítógép lelassulását vagy instabilitását is okozhatják. Elképzelhet, hogy *kártékony szoftverek* 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. Elfordulhat, hogy úgy módosítják vagy cserélik le a fájl tartalmát, hogy az kárt tesz a számítógépében.

A *vírusok* olyan programok, amelyek általában a tudta nélkül telepítődnek a számítógépére. A telepítés után a vírus megpróbálja többszörözni önmagát. A vírus:

- a számítógép erőforrásait közepes mértékben foglalja le,
- elfordulhat, hogy módosít vagy károsít fájlokat a számítógépén,
- valószínűleg felhasználja a számítógépét, hogy más számítógépeket is megfertőzzön,
- elfordulhat, hogy törvénybe ütköző célokra használja a számítógépét.

Kémprogram

A kémprogramok olyan programok, amelyek a személyes adatait gyűjtik össze.

A kémprogramok személyes információkat gyűjtenek, 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 félrevezető felugró ablak ráveszi, hogy valamire rákattintson az ablakban.

Rootkitek

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

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

Ez a termék rootkitvizsgálót is tartalmaz, amely kimondottan a rootkitek vizsgálatára szolgál, így a *kártékony szoftverek* nehezebben rejtőzhetnek el a számítógépén.

Veszélyes program

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

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

Ilyen veszélyes programok például:

- azonnali üzenetküldő 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-ellenrzések és a másolásvédelem kijátszására kialakított szoftverek.

Ha szándékosan telepítette és megfelelően beállította a programot, akkor kicsi a valószínűsége, hogy problémát okozzon.

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

A számítógép vizsgálata

Valós időben, manuálisan vagy ütemezett időpontokban is vizsgálhatja a kártékony szoftvereket a számítógépen.

A használandó módszer a számítógép teljesítményét és a biztonsági szintet függően választható ki. Az összes vírus- és kémprogram-vizsgáló szolgáltatás bekapcsolása jelentős hatással lehet a régebbi számítógépek teljesítményére.

Kártékony programok vizsgálata

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

A valós idejű vizsgálat csak a saját számítógépét védi, a barátaiét nem.

1. A számítógépe megpróbál megnyitni egy fájlt.
2. A program azonnal megvizsgálja, hogy a fájl tartalmaz-e *kártékony szoftvert*, mielőtt engedélyezné a hozzáférést a fájlhoz.
3. Ha *kártékony szoftvert* talált a fájlban, a valós idejű vizsgálat automatikusan eltávolítja a *kártékony szoftvert*, mielőtt az károsíthatná a számítógépet.

A valós idejű vizsgálat hatással van a számítógép teljesítményére?

A vizsgálat általában nem vehet észre, mert csak kevés időt, és a számítógép teljesítményének kis részét veszi igénybe. A valós idejű vizsgálat erőforrás-igénye és időszükséglete többek között a fájl tartalmától, helyétől és típusától függ.

A vizsgálat több időt vesz igénybe a következő fájlok esetében:

- Tömörített fájlok, például a .zip-fájlokat.
 - 👉 **Megjegyzés:** Az ilyen fájlokat a program alapértelmezés szerint nem vizsgálja.
- Cserélhető meghajtókon, például CD-, DVD- és USB-meghajtókon lévő fájlok.

A valós idej vizsgálat lelassíthatja a számítógépet, ha:

- A számítógép meglehetősen régi vagy
- túl sok fájlt próbál megnyitni egyszerre. Jó példa erre egy olyan könyvtár megnyitása a Windows Intéző programban, amely sok fájlt tartalmaz.

A valós idej vizsgálat be- vagy kikapcsolása

Bekapcsolhatja a valós idej vizsgálatot, hogy a *kártékony szoftvereket* még azelőtt megállíthassa, mielőtt azok károsítanák a számítógépét.

A valós idej vizsgálat bekapcsolása:

1. A felületen kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehetőséget.
3. Válassza a **A valós idej vizsgálat bekapcsolása** elemet.
4. Kattintson az **OK** gombra.

Kártékony szoftverek vizsgálata az e-mail üzenetekben

A levelek vizsgálata megakadályozza, hogy *vírusokat* kapjon vagy küldjön az e-mail üzenetekben.

A levelek vizsgálata a következőket védi a számítógépét:

- *vírusok* fogadásától az e-mail üzenetekhez csatolt fájlokban,
- *vírusok* véletlenül elküldését másoknak az e-mail üzenetekhez csatolt fájlokban.

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

Az e-maileket és a mellékleteket a rendszer minden alkalommal megvizsgálja, amikor a levelező program e-maileket küld vagy fogad.

Az e-mailek vizsgálata a következő e-mail üzeneteket ellenőrzi:

- A webböngészőtől függetlenül futó különálló levelező programokkal, például a Microsoft Outlook és az Outlook Express, a Microsoft Mail vagy a Mozilla Thunderbird szoftverrel küldött e-mail üzenetek.

Az e-mailek vizsgálata a következő e-mail üzeneteket nem ellenőrzi:

- A webes levelezés e-mail üzenetei. Ide tartoznak a webböngészőben futó e-mail alkalmazások (például a Hotmail, a Yahoo! vagy a Gmail).

- 👉 **Megjegyzés:** Mindenképpen győződjön meg róla, hogy a különböző e-mail protokollok (POP3, IMAP4, SMTP) által használt portok helyesen vannak beállítva. A más portokon keresztül küldött vagy fogadott e-mail üzeneteket a program nem vizsgálja.

A számítógépe még akkor is védett a *vírusok* ellen, ha a portok nincsenek megfelelően beállítva, vagy ha webes levelezést használ. Ha megnyitja a mellékletet, a valós idej vizsgálat észleli, ha a vírust tartalmaz, és még azelőtt letiltja az adott programot, hogy a vírus kárt okozhatna.

- 👉 **Megjegyzés:** A valós idej vizsgálat csak a saját számítógépét védi, a barátaiét nem. A program csak akkor észleli a vírust, ha megnyitja a mellékletet. Ha nem nyitja meg a mellékletet, nem fog kiderülni, ha a levél *vírust* tartalmaz, így el fordulhat, hogy vírusos levelet továbbít a barátainak.

E-mailek szűrésének be- vagy kikapcsolása

Az e-mailek vizsgálatának bekapcsolásával ellenőrizheti, hogy nincsenek-e *vírusok* az e-mail üzenetekben és mellékletekben.

Az e-mailek vizsgálatának bekapcsolása:

1. A felületen kattintson a **Beállítások** elemre.

2. Válassza az **Internet > E-mailek sz rése** lehet séget.
3. Válassza **Az e-mailek sz részének bekapcsolása** lehet séget.
4. Kattintson az **OK** gombra.

Különböz e-mail protokollokhoz használt portok megadása

Ha a levelez program nem szabványos portot használ, módosítania kell az *vírusvizsgálat* portját. Ellenkez esetben az adott porton érkező e-mail üzenetekben a program nem végzi el a *vírusok* vizsgálatát.

Portok beállítása:

1. Nyissa meg a levelez alkalmazást, és ellen rizza az e-mail üzenetek küldésére és fogadására használt portokat. Jegyezze le a portok számát.
2. Nyissa meg a terméket.
3. A f lapon kattintson a **Beállítások** elemre.
4. Válassza az **Internet > E-mailek sz rése** lehet séget.
5. Kattintson a **Protokollok megjelenítése** gombra.
6. Adja meg, hogy a program mely portokat használja a POP3 e-mail protokollhoz.
7. Kattintson az **OK** gombra.

Nyomkövet cookie-k blokkolása

A nyomkövet cookie-k blokkolásával megakadályozhatja, hogy a webhelyek ellen rizzessék, mely weblapokat látogatta meg az interneten.

A nyomkövet cookie-k olyan kis fájlok, amelyek lehet vé teszik weboldalak számára, hogy rögzítsék a megtekintett webhelyeket. A nyomkövet cookie-k telepítésének megakadályozása:

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehet séget.
3. Válassza a **Nyomkövet cookie-k blokkolása** lehet séget.
4. Kattintson az **OK** gombra.

Ütemezett vizsgálat

A *kártékony szoftverek* vizsgálata érdekében megadott időközönként vizsgálhatja a számítógépet, például naponta, hetente vagy havonta.

A *kártékony szoftverek* vizsgálata erőforrás-igényes folyamat. A számítógép teljes kapacitására szüksége van, és eltart egy kis ideig. Emiatt a vizsgálatot ajánlott olyan időpontokra ütemezni, amikor nem használja a számítógépet.

Vizsgálat ütemezése

Beállíthatja, hogy a program rendszeres időközönként ellen rizza a számítógépet.

Vizsgálat ütemezése:

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Ütemezett vizsgálat** lehet séget.
3. Válassza **Az Ütemezett frissítés bekapcsolása** lehet séget.
4. Jelölje ki, hogy melyik napokon szeretné rendszeresen elvégezni a *vírusok* és *kémprogramok* vizsgálatát.

Lehet ség

Leírás

Naponta

Vizsgálat minden nap.


Lehet ség	Leírás
Hetente	Vizsgálat a hét kijelölt napjain. Jelölje ki a jobb oldali listában, hogy melyik napokra ütemezze a program a vizsgálatot.
Havonta	Legfeljebb 3 napot jelölhet ki keresésre a hónapban. A napok kijelölése: <ol style="list-style-type: none"> Válasszon a Nap lehet ségek közül egyet. Jelölje ki a hónap egy napját a kijelölt nap melletti listában. Ismételje meg a nap megadását, ha másik napon is szeretne ütemezett vizsgálatot.

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

Lehet ség	Leírás
Indítás id pontja	A vizsgálat elindításának id pontja. Olyan id pontot érdemes választani, amikor úgy gondolja, hogy nem fogja a számítógépet használni.
Ha a számítógépet ennyi ideje nem használták	Adja meg, mennyi ideig legyen a számítógép használaton kívül, mielőtt a vizsgálat elkezdődik.

Ütemezett vizsgálat megszakítása

Az ütemezett vizsgálatot helyileg megszakíthatja, ha alkalmatlan id pontban indul el. Az ütemezett vizsgálat a következő ütemezett id pontban fog lefutni.

 **Megjegyzés:** A Web Console használatával az ütemezett vizsgálatok nem szakíthatók meg.

Az ütemezett vizsgálat észlelhető mértékben csökkentheti a számítógép teljesítményét. Az ütemezett vizsgálat megszakításához tegye a következőket:

- Kattintson **Az ütemezett vizsgálat elkezdődött** hivatkozásra a **Vírus- és kémprogramvizsgálat** értesítésén. Az értesítés körülbelül 15 másodpercig jelenik meg, azután eltűnik. Ha nem kattint az értesítésen lévő hivatkozásra, többé nem szakíthatja meg az ütemezett vizsgálatot.
- Kattintson a **Mégse** gombra a **Vírus- és kémprogramvizsgálat** ablakban.
- Kattintson a **Bezárás** gombra.


Az ütemezett vizsgálat megszakadt. A következő ütemezett vizsgálat a szokásos módon el fog indulni.

Ütemezett vizsgálat eredményeinek megtekintése


Az ütemezett vizsgálat végén ellenőrizheti, hogy található-e *kártékony szoftver* a rendszeren.

Az ütemezett vizsgálat eredményeinek vizsgálata:

- Kattintson **Az ütemezett vizsgálat befejeződött** elemre a **Vírus- és kémprogramvizsgálat** értesítésén.
- Kattintson a **Jelentés megjelenítése** hivatkozásra a vizsgálat során történt események megtekintéséhez.

 **Megjegyzés:** Ha a párbeszédpanel a **Korábbi értesítések** párbeszédpanelen nyitotta meg, a **Jelentés** gomb nem használható, a korábbi ütemezett frissítések eredményei nem pedig nem láthatók.

- Kattintson a **Bezárás** gombra a párbeszédpanel bezárásához.

 **Tipp:** Megjelenítheti a legutóbbi vizsgálat eredményeit úgy is, ha a **Beállítások > Számítógép > Ütemezett vizsgálat** lehet ségre kattint. Kattintson az **Utolsó vizsgálati jelentés megtekintése** lehet ségre.

Kézi vizsgálat

Ha úgy érzi, hogy *kártékony szoftver* fertőzte meg a gépét, kézzel is indíthat vizsgálatot.

Kézi vizsgálat típusának kiválasztása

A vizsgálatot végezheti a teljes számítógépen, kereshet adott típusú *kártékony szoftvereket*, vagy ellenőrizhet 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 fertőzött, korlátozhatja a vizsgálatot arra az egy helyre is. Az ilyen keresések sokkal gyorsabban befejeződnek, mint a teljes számítógép átvizsgálása.

Kézi vizsgálat elindítása:

1. A felületen kattintson a **Vizsgálat** alatti nyílra.
Megjelennek a vizsgálati beállítások.
2. Vizsgálat típusának kiválasztása
Ha módosítani kívánja a vizsgálat beállításait, válassza a **Vizsgálati beállítások megváltoztatása** lehetőséget.
3. Ha a **A vizsgálandó fájlok kijelölése** lehetőséget 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 következő lista a vizsgálatok különböző típusait tartalmazza:

Vizsgálat típusa	Mit vizsgál	Mikor használandó ez a típus
Teljes számítógépvizsgálat	A teljes számítógépen (a belső és a külső 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 időt. Kombinálja a kártékony programok gyors vizsgálatát és a merevlemez vizsgálatát. A rootkitek által lehetségesen elrejtett elemeket is ellenőrizi.
A vizsgálandó fájlok kijelölése	Egy adott fájlban, mappában vagy meghajtón vírusokat, kémprogramokat és veszélyes programokat	Ha azt gyanítja, hogy a számítógép egy adott helyen esetleg kártékony szoftver található, például az adott helyen lehetségesen veszélyes forrásokból letöltött elemek (például fájlcsere-rendszerekben letöltött fájlok) találhatóak. A vizsgálat ideje a vizsgált célmappa méretétől függ. A vizsgálat gyorsan befejeződik, ha például egy néhány kis méretű fájl tartalmazó mappában végzi azt.
Vírus- és kémprogramvizsgálat	A számítógép részein vírusokat, kémprogramokat és veszélyes programokat	Ez a vizsgálati típus 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 ellenőrizni a számítógép tisztaságát, mert képes a számítógépen található aktív kártékony szoftverek hatékony megkeresésére és eltávolítására.

Vizsgálat típusa	Mit vizsgál	Mikor használandó ez a típus
Rootkitvizsgálat	A fontos rendszerelemek 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 megszeretne gy z dni arról, hogy nem telepített rootkitet.

Kártékony szoftver automatikus tisztítása

Ha a vizsgálat során a program *kártékony szoftver* jelenlétét észleli, engedélyezheti, hogy a program automatikusan döntsön a számítógép tisztításáról, vagy minden egyes elem esetében személyesen dönthet.

1. Válassza a következők valamelyikét:

Lehet ség

Automatikus kezelés (ajánlott)


Elemenként szeretném eldönteni

Következmény

A program minden egyes *kártékony szoftver* esetében dönt a teend kr l a számítógép tisztítása érdekében.

A program minden egyes *kártékony szoftver* esetében rákérdez, hogy mi a teend .


2. Kattintson a **Tovább** gombra.

- Ha az **Automatikus kezelés (ajánlott)** elemet választotta, megjelenik egy ablak, melyben a kártékony programok automatikus kezelésének eredménye látható.
 -  **Megjegyzés:** Ha egy kártékony program mellett az látható, hogy még nincs feldolgozva, akkor a fert zött fájl archívumban (pl. .zip fájlban) található, és nem kezelhet automatikusan. A fert zött fájl törléséhez meg nyitni az archívumot, és kézzel kell bel le törölni a fájlt. Ha az archívum tartalma nem fontos, törölheti az egész archívumot.
- Ha az **Elemenként szeretném eldönteni** lehet séget választotta, minden észlelt kártékony programhoz külön kell megadnia a m veletet.

3. Kattintson a **Befejezés** elemre a Vizsgálat varázsló párbeszédpanel bezárásához.

Kézi vizsgálat eredményeinek megtekintése

A vizsgálat befejezése után megtekinthet egy jelentést a vizsgálat eredményeir l.

-  **Megjegyzés:** Érdemes megtekinteni ezt a jelentést, mert a program nem mindig azt a m veletet hajtja végre, amit kiválasztott. Ha például a tisztítás lehet séget választotta egy fert zött fájl esetén, de a *vírus* nem távolítható el a fájlból, akkor a termék valamilyen más m veletet hajt végre a fájlban.

A jelentés megjelenítése:

1. Kattintson a **Jelentés megjelenítése** hivatkozásra.

A jelentés tartalma:

- Talált *kártékony szoftverek* száma
- A talált *kártékony szoftverek* típusa és internetes hivatkozások a *kártékony szoftverek* leírásaihoz.
- Az egyes *kártékony szoftverre* alkalmazott m velet.
- A keresésb l kihagyott elemek.
- A kártékony programok vizsgálatokra használt vizsgálómodulok.

- ☞ **Megjegyzés:** A vizsgált fájlok száma attól függ, hogy a program megvizsgálja-e a tömörített fájlok tartalmát a vizsgálat során. Ha a tárolt fájlok vizsgálata korábban már megtörtént, a vizsgálat eredményeit a gyorsítótár memóriájába mentheti.

2. Kattintson a **Befejezés** elemre a **Vizsgálat varázsló** párbeszédpanel bezárásához.

- ☞ **Tipp:** Megjelenítheti a legutóbbi vizsgálat eredményeit úgy is, ha a **Beállítások > Számítógép > Kézi vizsgálat** lehet ségre kattint. Kattintson az **Utolsó vizsgálati jelentés megtekintése** lehet ségre.

Vizsgálni kívánt fájlok kiválasztása

Megadhatja, hogy mely fájltypusokat és a számítógép mely részeit szeretné ellen rizni a kézi és ütemezett vizsgálatok során.

- ☞ **Megjegyzés:** Szerkessze a kézi vizsgálat beállításait az ütemezett vizsgálat során vizsgálandó fájlok és mappák kiválasztásához.

Kétféle lista határozza meg, hogy mely fájlokban keres *vírusokat* a program a kézi és az ütemezett vizsgálatok során:

- Az Ellen rzött fájltypusok lista minden fájl tartalmaz, vagy csak meghatározott fájltypusokat.
- A vizsgálatból kizárt fájlok listái a vizsgálatból kimaradó fájltypusokat határozzák meg. A listák fájltypusai kizárt típusok, amelyek akkor sem lesznek ellen rizve, ha szerepelnek az ellen rizend fájltypusok listájában.

Az ellen rzött és kizárt fájltypusok listáival definiálhatja, hogy a számítógép mely részei lesznek a különböző módszerekkel ellen rizve:

- Megteheti azt, hogy felvesz minden fájl a keresésbe, majd a kivételek listájával adja meg azokat a meghajtókat, mappákat vagy fájlokat, amelyekr l tudja, hogy biztonságosak, és ezért nem igényelnek ellen rzést.
- Megadhatja azoknak a fájltypusoknak a listáját is, amelyeket ellen rizni kíván, így csak a megadott fájltypusok szerepelnek a vizsgálatban.

Fájlok hozzáadása

Kijelölheti a fájltypusokat, amelyekben *vírusokat* és *kémprogramokat* szeretne keresne a kézi vagy ütemezett vizsgálat során.

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Kézi vizsgálat** lehet séget.
3. A **Vizsgálati beállítások** csoportban válasszon a következ beállítások közül:

Csak az ismert fájlok vizsgálata (gyorsabb)

Csak a fert zéseknek leginkább kitett fájltypusok, 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 (zip, arj, lzh stb.) tartalmának vizsgálata

Tömörített fájlok és mappák vizsgálata.

Fejlett heurisztika használata (lassabb)

Az új vagy ismeretlen kártékony szoftverek megtalálása érdekében az összes elérhető heurisztika használata a vizsgálat során.

- ☞ **Megjegyzés:** Ha ezt a lehetőséget választja, a vizsgálat több időt vesz igénybe, és több hamis találat (vagyis gyanúsként feltüntetett, de ártalmatlan fájlal) járhat.

4. Kattintson az **OK** gombra.

A **Vizsgálati beállítások** meghatározzák, hogy mely fájlok szerepeljenek a jövőbeni kézi és ütemezett vizsgálatokban.

- ☞ **Megjegyzés:** A kizárt elem listán lévő összes fájl típus vagy hely felülírja az itt megadott beállításokat. A kizárt elemek listában lévő fájl típusokat a program akkor sem vizsgálja, ha itt bejelölte azokat.

Fájltípusok kizárása

A kézi és az ütemezett vizsgálatból a fájlokat fájl típus alapján zárhatja ki.

1. A f lapon kattintson a **Beállítások** elemre.
2. Tegye az alábbiak egyikét:
 - Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehetőséget.
 - Válassza az **Számítógép > Kézi vizsgálat** elemre.
3. Kattintson a **Kihagyott elemek listájának megnyitása** gombra.
4. Fájltípus kizárása:
 - a) Kattintson a **Fájltípusok** fölé.
 - b) Válassza az **Az alábbi kiterjesztés fájlok kivételével** lehetőséget.
 - c) Írja be a kizárni kívánt fájl típus azonosító fájl kiterjesztést a **Hozzáadás** gomb melletti mezőbe. A kiterjesztés nélküli fájlok megadásához írja be a „.” karaktert. Használhatja a „?” helyettesítő karaktert egyetlen karakter helyettesítéséhez vagy a „*” karaktert tetszőleges számú karakter helyettesítéséhez. Például a futtatható fájlok kizárásához írja be az exe szöveget a mezőbe.
 - d) Kattintson a **Hozzáadás** gombra.
5. Ismételje meg az előző 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 kijelölt fájl típusok nem szerepelnek a későbbi valószínű vizsgálatokban.

Fájlok kizárása azok helye alapján


Megadhatja azoknak a mappáknak vagy meghajtóknak a kivétel listáját, amelyekben nem kíván kézi vagy ütemezett *vírusvizsgálatot* végezni.

- ☞ **Megjegyzés:** A vizsgálatból kizárt fájlok, mappák vagy meghajtók nem lesznek megvizsgálva, még akkor sem, ha típusuk szerint szerepelnének a vizsgált fájl típusok között.

A hely alapján kizárt fájlok, mappák vagy meghajtók listájának megadása:

1. A f lapon kattintson a **Beállítások** elemre.
2. Tegye az alábbiak egyikét:
 - Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehetőséget.
 - Válassza az **Számítógép > Kézi vizsgálat** elemre.

3. Kattintson a **Kihagyott elemek listájának megnyitása** gombra.
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 kijelölt fájlok, meghajtók és mappák nem szerepelnek a kés bbi valós idej és kézi vizsgálatokban.

Kihagyott alkalmazások megtekintése

Megtekintheti azokat az alkalmazásokat, amelyeket kizárt a valós idej , kézi és ütemezett vizsgálatokból. Ezeket az alkalmazásokat eltávolíthatja a kivételek listájából, így azok szerepelni fognak a kés bbi vizsgálatokban.

A vizsgálatból alkalmazások megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.
2. Tegye az alábbiak egyikét:
 - Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehet séget.
 - Válassza az **Számítógép > Kézi vizsgálat** elemre.
3. Kattintson a **Kihagyott elemek listájának megnyitása** elemre.
4. Kattintson az **Alkalmazások** fülre.

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

5. Alkalmazás visszaállítása, hogy az szerepeljen a kés bbi kézi vagy ütemezett keresésekben:
 - a) Válassza ki azt az alkalmazást, amelyet ismét fel kíván venni a keresésbe.
 - b) Kattintson az **Eltávolítás** gombra.
6. Kattintson az **OK** gombra a **Kizárás a vizsgálatból** párbeszédpanelen.
7. Kattintson az **OK** gombra a kilépéshez.


Tömörített fájlok és mappák vizsgálata

Végezhet ellen rzést a tömörített fájlokban rejt zköd *vírus* megkereséséhez.

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Kézi vizsgálat** lehet séget.
3. Tömörített fájlok és mappák, például .zip fájlok, például .zip fájlok vizsgálatához jelölje be a **Tömörített fájlok (zip, arj, lzh stb.) tartalmának vizsgálata** jelöl négyzetet.
A tömörített fájlok vizsgálata valamennyivel több id t vesz igénybe.
4. Kattintson az **OK** gombra.

M velet kiválasztása amikor talál valamit a program

Ha a program *vírusokat* talál és nem állította be, hogy a program automatikusan kezelje a *vírusokat*, akkor eldöntheti, hogy a program tisztítsa, törölje, tegye karanténba vagy csak tiltsa le figyelmen kívül a talált vírusokat.

-  **Megjegyzés:** A **Vizsgálat varázsló** ezen lépése kimarad, ha beállította a programot, hogy mindig automatikusan kezelje a *vírusokat* a kézi és ütemezett keresések során, vagy ha azt állította be, hogy automatikusan kezelje a mostani vizsgálat során talált *kártékony szoftvereket*.


Megjelenik a fert zött fájlok listája és a fájlokban talált *vírusok* amelyeket a program ezen fájlokban talált. Ezek kezelése *vírusok* eltávolítása a számítógépr l:

1. Válassza ki az elvégzend feladatot fert zött fájlok esetén.
Ha további részleteket szeretne megtudni a fert zésr l, kattintson a **Fert zés** oszlopban található hivatkozásra.
2. Kattintson a **Tovább** gombra a m veletek alkalmazásához.
3. A befejezéshez kattintson a **Tovább** gombra.

Ha a program *kémprogramot* talál a kézi vagy ütemezett vizsgálat során, a **Vizsgálat varázsló** következ lépése a *kémprogram* eltávolítása.

Valós idej vizsgálat során végezhet intézkedések

A **Végrehajtandó m velet** oszlopban látható, hogy milyen intézkedéseket végezhet a fert zött fájlok a valós idej vizsgálat során.

-  **Megjegyzés:** A fájlok mellett a beállításjegyzék bejegyzéseiben vagy a folyamatokban is lehet fert zés.

A következ m veletek végezhet k el a *vírusokon*:

Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Automatikus fert tlenítés	A program megpróbálja fert tleníteni az összes <i>vírust</i> az összes fert zött fájlban, amelyet a valós idej vizsgálat során talál.
Karanténba helyezés automatikusan (alapérték)	A program által a valós idej vizsgálat során talált összes fert zött fájl karanténba kerül, ahol már nem okozhat kárt a számítógépen.
Automatikus átnevezés	A program átnevezi az összes fert zött fájl, amelyet a valós idej vizsgálat során talál.
Automatikus törlés	A program törli az összes fert zött fájl, amelyet a valós idej vizsgálat során talál.
Csak jelentés	A termék bejegyzi az észlelt vírusokat a logfile.log fájlba, figyelmeztetéseket küld a Policy Manager szolgáltatásnak, eseményeket ad hozzá a Windows eseménynaplójához, és e-mail értesítéseket küld (az Általános>Felügyelet szakaszban lév Figyelmeztetések lap beállításai szerint).


A következ m veletek végezhet k el *kémprogramok* esetén:

Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Automatikus karanténba helyezés	A program által a valós idej vizsgálat során talált összes fert zött fájl karanténba kerül, ahol már nem okozhat kárt a számítógépen.
Automatikus eltávolítás	A termék eltávolítja az összes <i>kémprogramot</i> , amelyet a valós idej vizsgálat során talál.



Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Csak jelentés (alapérték)	A termék nem módosítja a valós idej vizsgálat során talált kémprogramokat, bejegyzi az észlelt elemeket a logfile.log fájlba, figyelmeztetéseket küld a Policy Manager szolgáltatásnak, eseményeket ad hozzá a Windows eseménynaplójához, és e-mail értesítéseket küld (az Általános>Felügyelet szakaszban lév Figyelmeztetések lap beállításai szerint).

Kézi vagy ütemezett vizsgálat során végezhet intézkedések

A **Végrehajtandó m velet** oszlopban látható, hogy milyen intézkedéseket végezhet a fert zött fájlkon a kézi vagy ütemezett vizsgálatok során.


 **Megjegyzés:** A fájlok mellett a beállításjegyzék bejegyzéseiben vagy a folyamatokban is lehet fert zés.

A következ m veletek végezhet k el *vírusok*okon:

Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Teend k megkérdezése (alapérték)	A termék rákérdez, hogy mit tegyen, ha egy kézi vizsgálat során <i>vírusokat</i> talál.
Automatikus fert tlenítés	A program megkísérli automatikusan fert tleníteni az összes fert zött fájlt, amelyet a kézi vagy az ütemezett vizsgálat során talál.  Megjegyzés: Nem mindig lehetséges a vírusok tisztítása a fájlkból. Ha nem lehetséges, a fájl karanténba kerül (kivéve, ha a hálózaton vagy cserélhet meghajtón található), hogy a vírus ne károsíthassa a számítógépet.
Karanténba helyezés automatikusan	A termék által a kézi vagy ütemezett vizsgálat során talált összes fert zött fájl karanténba kerül, ahol már nem okozhat kárt a kiszolgálón.
Automatikus átnevezés	A program automatikusan törli az összes fert zött fájlt, amelyet a kézi vagy ütemezett vizsgálat során talál.
Automatikus törlés	A program automatikusan törli az összes fert zött fájlt, amelyet a kézi vagy ütemezett vizsgálat során talál.
Csak jelentés	A program a kézi vagy ütemezett vizsgálat során talált összes fert zött fájlt érintetlenül hagyja, és a vírusok és kémprogramok észlelését rögzíti a vizsgálati jelentésben.  Megjegyzés: Ha a valós idej vizsgálat nincs bekapcsolva, a kártékony programok kárt okozhatnak a számítógépen, ha ezt a lehet séget választja.

A következ m veletek végezhet k el *kémprogramok* esetén:

Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Teend k megkérdezése (alapérték)	A termék rákérdez, hogy mit tegyen, ha egy kézi vizsgálat során <i>kémprogramokat</i> talál.
Karanténba helyezés automatikusan	A termék által a kézi vagy ütemezett vizsgálat során talált összes kémprogram karanténba kerül, ahol már nem okozhat kárt a kiszolgálón.
Automatikus eltávolítás	A termék eltávolítja az összes kémprogramot, amelyet a kézi vagy ütemezett vizsgálat során talál.

Végrehajtandó m velet	Mi történik a fert zött fájlokkal
Csak jelentés	A termék a kézi vagy ütemezett vizsgálat során talált összes kémprogramot érintetlenül hagyja, és az észlelést rögzíti a vizsgálati jelentésben.  Megjegyzés: Ha a valós idej vizsgálat nincs bekapcsolva, a kártékony programok kárt okozhatnak a számítógépen, ha ezt a lehet séget választja.

Alapértelmezett m veletek a valós idej vizsgálatához

Az **Alapértelmezett m velet** oszlopban látható, hogy a valós idej vizsgálat során mely alapértelmezett m veletek választhatók ki a fert zött fájlokhoz.



A következ alapértelmezett m veletek közül választhat, ha a program kártékony szoftvert talál:

Alapértelmezett m velet	Mi történik, ha a program kártékony szoftver jelenlétét észleli
Engedély kérése minden esetben	A program rákérdez, hogy mit tegyen, ha kártékony szoftvert észlel egy valós idej vizsgálat során.
Ha nem egyértelm , kérdezzen	Ha a program nem tudja azonosítani a kártékony szoftvert, rákérdez, hogy mit tegyen vele.

Alapértelmezett m veletek kézi és ütemezett vizsgálatokban

Az **Alapértelmezett m velet** oszlopban látható, hogy a kézi és ütemezett vizsgálatok során mely alapértelmezett m veletek választhatók ki a fert zött fájlokhoz.

A következ alapértelmezett m veletek közül választhat, ha a program kártékony szoftvert talál:

Alapértelmezett m velet	Mi történik, ha a program kártékony szoftver jelenlétét észleli
Teend k megkérdezése	A program rákérdez, hogy mit tegyen, ha egy kézi vizsgálat során kártékony szoftvert észlel.
Automatikus fert tlenítés	A program megpróbálja automatikusan fert tleníteni az összes fert zött fájlt, amelyet a kézi vagy ütemezett vizsgálat során talál.  Megjegyzés: Nem mindig lehetséges a vírusok tisztítása a fájlkból. Ha nem lehetséges, a fájl karanténba kerül (kivéve, ha a hálózaton vagy cserélhet meghajtón található), hogy a vírus ne károsíthassa a számítógépet.
Karanténba helyezés automatikusan	A program által a kézi vagy ütemezett vizsgálat során talált összes fert zött fájl karanténba kerül, ahol már nem okozhat kárt a számítógépen.
Automatikus átnevezés	A program automatikusan törli az összes fert zött fájlt, amelyet a kézi vagy ütemezett vizsgálat során talál.
Automatikus törlés	A program automatikusan törli az összes fert zött fájlt, amelyet a kézi vagy ütemezett vizsgálat során talál.
Csak jelentés	A program a kézi vagy ütemezett vizsgálat során talált összes fert zött fájlt érintetlenül hagyja, és a vírusok és kémprogramok észlelését rögzíti a vizsgálati jelentésben.  Megjegyzés: Ha a valós idej vizsgálat nincs bekapcsolva, a kártékony programok kárt okozhatnak a számítógépen, ha ezt a lehet séget választja.

A DeepGuard alapértelmezett m veletei

Az **Alapértelmezett m velet** oszlopban látható, hogy mely alapértelmezett m veletek választhatók a DeepGuard eszközhöz.

A következ alapértelmezett m veletek közül választhat, ha a DeepGuard a rendszer módosításának kísérletét észleli:

Alapértelmezett m velet	Mi történik, ha a program kártékony szoftver jelenlétét észleli
Engedély kérése minden esetben	A DeepGuard még akkor is rákérdez, hogy engedélyezni vagy tiltani kívánja-e az összes figyelt m veletet, ha biztonságosnak ítélte az alkalmazást.
Ha nem egyértelmű, kérdezzen	A DeepGuard csak akkor kérdez rá, hogy engedélyezni vagy tiltani kívánja-e a figyelt m veleteket, ha nem tudta eldönteni, hogy az alkalmazás biztonságos-e vagy sem
Automatikus kezelés	A DeepGuard kérdés nélkül automatikusan letiltja a nem biztonságos alkalmazásokat, a biztonságos alkalmazásokat pedig engedélyezi.

Vírusok és kémprogramok el zményeinek megtekintése

A vírusok és kémprogramok el zményei a program által a talált vírusokkal és kémprogramokkal végzett m veleteket mutatják.

Az el zmények megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehet séget.
3. Kattintson a **Vírusok és kémprogramok el zményeinek megtekintése** lehet séget.

Megnyílnak a vírusok és kémprogramok el zményei.

Belső k

A DeepGuard elemzi a fájlok tartalmát és a programok m kódését, és blokkolja az új és ismeretlen *vírusokat*, *férgeket* és egyéb káros programokat, amelyek lehetségesen ártalmas módosításokat próbálnak végrehajtani a számítógépen.

Veszélyes rendszerváltozások lehetnek 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 folyamatosan figyeli a változásokat, és minden olyan programot ellen riz, amely változtatást próbál végrehajtani a rendszeren.

A DeepGuard m kódése

Ha a DeepGuard olyan programot észlel, amely a rendszerre feltehetően veszélyes módosításokat próbál végrehajtani, akkor a programot egy biztonsági zónában engedi csak futni, hacsak kifejezetten nem engedélyezte vagy tiltotta le a programot korábban.

A biztonsági zónában a program nem veszélyezteti a számítógépét. A DeepGuard elemzi, hogy a program milyen módosításokat kísérelt meg végrehajtani, és ezek alapján eldönti, hogy a program *kártékony szoftver*-e, vagy sem.

A DeepGuard a következők alapján automatikusan engedélyezi vagy letiltja a programot, vagy megkérdezi, hogy engedélyezze vagy letiltsa-e a program működését:

- a program milyen valószínűséggel *kártékony szoftver* és
- mit állított be, mit tegyen a DeepGuard, ha feltehetően káros rendszerváltoztatási kísérletet észlel.

A DeepGuard bekapcsolása

A DeepGuard bekapcsolásával megakadályozhatja a gyanús programokat abban, hogy káros rendszermódosításokat végezzenek a számítógépén.

A DeepGuard bekapcsolása előtt ellenőrizze, hogy Windows XP rendszer esetén a Service Pack 2 szervizcsomag telepítve van a számítógépre.

A DeepGuard bekapcsolása:

1. A fő lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > DeepGuard** lehetőséget.
3. Válassza az **A DeepGuard bekapcsolása** lehetőséget.
4. Kattintson az **OK** gombra.

A DeepGuard által blokkolt programok engedélyezése

A DeepGuard által letiltott programoknak engedélyezheti a rendszer módosítását.

Néha a DeepGuard akkor is letilt néhány biztonságos programot, ha használni szeretné és tudja, hogy biztonságos. Ez azért történik, mert a program olyan rendszerváltozásokat próbál végrehajtani, amelyek akár káros is lehetnek. Az is előfordulhat, hogy a DeepGuard előugró ablak megjelenésekor véletlenül letiltott egy programot. A letiltott programokat úgy engedélyezheti, hogy módosítja a hozzá tartozó engedélyeket az Alkalmazások listában.

A DeepGuard által blokkolt program engedélyezése:

1. A fő lapon kattintson a **Feladatok** elemre.
2. Válassza az **Alkalmazás indításának engedélyezése** lehetőséget. Ekkor megjelenik a **Figyelt alkalmazások** listája.
3. Kattintson az **Engedély** oszlopra, hogy az engedélyezett és a letiltott programokat külön csoportba rendezze a program.
4. Jelölje ki az engedélyezni kívánt programot, majd kattintson a **Részletek** gombra.
5. Az **Engedély** területen jelölje ki az **Engedélyezés** lehetőséget.
6. Kattintson az **OK** gombra.
7. Kattintson a **Bezárás** gombra.

A kijelölt program most már futhat és végrehajthatja a rendszermódosításokat.

A fejlett folyamatfigyelés kikapcsolása

A maximális védelem érdekében a DeepGuard ideiglenesen módosítja a futó programokat.

A továbbfejlesztett folyamatfigyelés problémákat okozhat az olyan programokkal kapcsolatban, amelyek ellenőrzik saját épségüket vagy eredetiségüket. A csalást megelőző eszközökkel rendelkező online játékok például ellenőrzik, hogy futásuk közben nem módosítják-e őket.

A fejlett folyamatfigyelés kikapcsolása:

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > DeepGuard** lehet séget.
3. Törölje a **Fejlett folyamatfigyelés használata** lehet séget.
4. Kattintson az **OK** gombra.

Védelem a káros rendszermódosítások ellen

Ha a DeepGuard észleli, hogy egy program esetleg káros rendszermódosításokat próbál végrehajtani, és nem tudja eldönteni, hogy a program biztonságos-e vagy sem, a **Rendszermódosítási kísérlet** párbeszédpanel jelenik meg.

A Rendszermódosítási kísérlet párbeszédpanel akkor jelenik meg, ha például a következő m veletek valamelyikét adta meg, és a DeepGuard eszköznek ezt a m veletet kell végrehajtania, ha potenciálisan veszélyes rendszermódosítási kísérletet észlel:

- **Engedély kérése minden esetben** vagy
- **Ha nem egyértelmű, kérdezzen.**

A DeepGuard megjelenítheti ezt a párbeszédpanelt például akkor, amikor szoftvert telepít.

Annak eldöntéséhez, hogy a rendszermódosítást megkísérli program megbízható-e, tegye a következőket:

1. Ha bizonytalan a módosítási kísérlet forrásával kapcsolatban, kattintson a **Részletek** gombra a program részletes adatainak megtekintéséhez.

A Technikai részletek szakasz a következőkről nyújt információt:

- A módosítást megkísérli program nevét,
- a program helyét,
- a program által megkísérelt módosítást, valamint
- egy *kockázati pontszámot*, amely megmutatja, mennyire valószínű, hogy a program *kártékony szoftver*.
 - az alacsony pontszám azt jelzi, hogy a program valószínűleg ártalmatlan,
 - a magas pontszám pedig azt, hogy a program valószínűleg *kártékony szoftver*.

2. Válasszon egyet az alábbi lehet ségek közül:

Kiválasztás

**Megbízom a programban.
Engedélyezze a folytatást**

Ha Ön...

úgy gondolja, hogy a program biztonságos. A program nagyobb valószínűséggel biztonságos, ha:

- alacsony a *kockázati pontszám*,
- egy végrehajtott m velet eredményeképpen megjelenik a párbeszédpanel,
- felismeri a programot, vagy
- a programot egy megbízható forrásból kapta.

**Nem bízom a programban.
Maradjon blokkolva**

azt gyanítja, hogy a program nem biztonságos. A program nagyobb valószínűséggel nem biztonságos, ha:

- magas a *kockázati pontszám*,
- nem ismeri a programot, vagy
- ismeri a programot, és úgy gondolja, hogy gyanús.

3. Válassza a **Ne jelenjen meg többé ez a párbeszédpanel ehhez a programhoz** ha azt szeretné, hogy a DeepGuard végrehajtsa a programhoz rendelt döntést a jövőbeli rendszermódosítási kísérletek során.

Ez a beállítás csak akkor jelenik meg, ha a **Engedély kérése minden esetben** m veletet adta meg a rendszer módosítási kísérletek esetére.

Amikor a DeepGuard legközelebb észleli ezt a programot, nem kérdezi meg, mi a teendő, hanem a korábbi felhasználói döntést alkalmazza.

4. Ha el szeretné küldeni a rendszer módosítást megkísérlő program mintáját, tegye a következőt:

- a) Kattintson a **Minta elküldése az F-Secure vállalatnak** elemre.
Megjelenik egy párbeszédpanel, amely elmagyarázza a küldés feltételeit.
- b) Alaposan olvassa el a feltételeket, és kattintson az **Elfogadom** gombra, ha elfogadja a feltételeket, és el szeretné küldeni a mintát.

Elküldhet egy mintát:

- ha a DeepGuard automatikusan blokkol egy programot, amiről Ön tudja, hogy biztonságos, vagy
- amikor megjelenik egy **Rendszer módosítási kísérlet** párbeszédpanel, és azt gyanítja, hogy a program *kártékony szoftver* lehet.

A rendszer elküldi az F-Secure vállalatnak azon program elektronikus másolatát, amelyet lehetséges biztonsági veszélyként azonosított.

A DeepGuard eredményeinek megtekintése

Egy kis értesítés jelenik meg, ha a DeepGuard automatikusan megakadályozza, hogy egy program módosítsa a rendszert.

Az értesítések olyan kis értesítő ablakok, amelyek a számítógép képernyőjének jobb alsó sarkában láthatók. Akkor jelennek meg például, ha a DeepGuard letiltotta egy program használatát. Ezek az értesítések csupán tájékoztató jellegűek, és semmilyen beavatkozást nem igényelnek. A Korábbi értesítések listában megtekintheti az összes értesítést.

Ha egy telepíteni vagy futtatni próbált program nem működik, ez azért lehetséges, mert a DeepGuard megakadályozta, hogy a program módosítsa a rendszert. Ebben az esetben megjeleníthet egy kis értesítést arról, hogy a DeepGuard mikor blokkolta a programot. Így tudni fogja, hogy miért nem működik megfelelően a program.

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, később visszaállíthatja a karanténban elhelyezett programokat vagy fájlokat.


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

- Általában törölheti a karanténban lévő *kártékony szoftvereket*.
- A legtöbb esetben törölheti a karanténban elhelyezett *kémprogramokat*. Elfordulhat, hogy a karanténban lévő *kémprogram* egy legális szoftver része, és ha eltávolítja azt, a program nem fog megfelelően működni. Ha meg kívánja tartani a szoftvert, akkor visszaállíthatja a karanténban lévő *kémprogramot*.
- A karanténban elhelyezett *veszélyes programok* lehetnek legális szoftverek is. Ha saját kezével telepítette a programot, visszaállíthatja azt a karanténból. Ha a *veszélyes program* a tudta nélkül telepítődött a számítógépére, akkor nagyon valószínű, hogy kártékony szándékkal lett telepítve, ezért ajánlott törölnie.

Karanténba helyezett elemek megtekintése

A karanténban lévő elemekről további információt is megtudhat.

A karanténban lévő elemek adatainak megtekintése:

1. A f lapon kattintson a **Beállítások** elemre.
2. Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehet séget.
3. Kattintson a **Karantén megnyitása** elemre.
A **Karantén** lapon látható a karanténban tárolt elemek teljes száma.
4. Ha a karanténban lévő elemek részletes adataira kíváncsi, kattintson a **Részletek** elemre.
A tartalmat a kártékony programok neve vagy a fájl elérési útja alapján rendezheti.
Az első 100 elem listáján megjelenik a karanténban lévő elemek típusa, neve és a telepített fájlok elérési útja.
5. Ha a karanténban lévő egyes elemekről 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.
2. Válassza a **Számítógép > Vírus- és kémprogramvizsgálat** lehet séget.
3. Kattintson a **Karantén megnyitása** elemre.
4. Jelölje ki a karanténban lévő, visszaállítandó elemeket.

 **Tipp:** A karanténban lévő összes elem visszaállításához kattintson a jobb oldali panel **Feladatok** csoportjában az **Feladatok** elemre.


5. Kattintson a **Visszaállítás** gombra.

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 érhető el.

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

2. Válassza az **Központi kezelés** > **Mobil szélessáv** elemet.

3. Válassza ki a mobil csatlakozáshoz használni kívánt frissítési beállítást:

- **Csak a saját hálózatban (ajánlott)**

A frissítések a saját hálózatban mindig letöltődnek, más hálózat használatakor azonban a program felfüggeszti őket. Javasoljuk, hogy ezt a beállítást válassza, így a tervezett költségeken belül tarthatja naprakészen a terméket.

- **Mindig**

A frissítések a használt hálózattól függetlenül mindig letöltődnek. Akkor válassza ezt a beállítást, ha a költségektől függetlenül mindig naprakészen kívánja tartani a számítógép védelmét.

- **Soha**

Mobil szélessáv használatakor semmilyen biztonsági frissítés nem töltődik le, még saját hálózaton belül sem. A következő esetekben célszerű ezt a beállítást választani:

- Ha csak átmenetileg használja a mobil kapcsolatot, egyébként rendszeresen rögzített vagy vezeték nélküli hálózaton keresztül csatlakozik.
- Ha a mobil kapcsolat adatforgalma korlátozott, és másra kívánja felhasználni a sáv szélességet.

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

Biztonsági frissítések felfüggesztve

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

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

Megjegyzés:

Ez a funkció csak Microsoft Windows 7 rendszeren érhető el.