

- **GfiMailSecurity**



## E-mail anti-vírus és tartalomszűrő Exchange/Lotus/SMTP levelezőszerverekhez

Egy vállalat elektronikus levelezésének védelmekor a beérkező többszáz ezer levél közül ki kell tudni szűrni a veszélyes tartalmú vagy támadó szándékú leveleket úgy, hogy a folyamat közben az értékes és bizalmas levelek ne sérüljenek, és ne kerüljenek a kiszűrt levelek közé. A kénytelen levelek mellett a legtöbb problémát az e-mailben érkező vírusok és más rosszindulatú kódok okozzák, amelyek képesek akár lebénítani a levelezőszervert. Talán még ennél is nagyobb veszélyt jelentenek azok az e-mailben terjedő kódok, amelyek megfertőzhetik a levelezőszervert, és bizalmas adatokat, leveleket küldenek tovább a világ bármely postafiókjába. A felsorolt veszélyforrásokra nem adnak megfelelő megoldást azok a programok, amelyek csak egy hagyományos vírusirtót használnak, mert a levelekben érkező trójai és exploit programok szabályos kommunikációját a hagyományos módszerekkel nem lehet felderíteni. A levelező szervert csak egy integrált e-mail-tartalomszűrő és több motorral működő e-mail anti-vírus program tudja megvédeni. A GFI MailSecurity e-mail tűzfalként tartja távol a levelekben érkező vírusokat és más kártékony, támadó jellegű tartalmakat.

- **Vírusellenőrzés több vírusirtóval**

A GFI MailSecurity a bejövő leveleket akár 5 különböző vírusirtó segítségével ellenőrizheti. A több vírusirtó alkalmazása drasztikusan csökkenti a vírusok megszületése és felismerése között eltelt időt, ezáltal minimálisra csökkentve a fertőzés esélyét. A magyarázat nagyon egyszerű: egyik gyártó sem lehet mindig a leggyorsabb. A víruskitörésekre az egyes gyártók más-más válaszütemmel reagálnak a vírusok típusa és a megjelenésük helyének függvényében. Több vírusirtó használata esetén nagyobb az esély arra, hogy ezek közül a programok közül legalább egy képes azonosítani és megállítani a legújabb vírusokat. Fontos még kiemelni, hogy minden vírusirtó egyedi keresési mechanizmussal rendelkezik. Egyesek nagy pontossággal találnak meg egy bizonyos vírust és annak variációit, míg egy másik anti-vírus motor más vírusokat képes azonosítani. Összefoglalva: a több vírusirtó nagyobb védelmet biztosít.

- **Norman, Kaspersky, BitDefender, McAfee és AVG anti-vírus motorok**

A GFI MailSecurity alapvetően két ICSA bizonyítvánnyal rendelkező elismert és erőteljes vírusirtó motorra támaszkodik. A Norman Vírus Control az ICSA minősítés mellett 32 alkalommal nyerte el a 100% Vírus Bulletin díjat, és Checkmark bizonyítvánnyal is rendelkezik. A BitDefender szintén 100% Vírus Bulletin díjas megoldás, amely ICSA bizonyítvánnyal is rendelkezik. A fokozott biztonság érdekében azonban lehetőség van további három gyártó termékének az integrálására is. A Kaspersky, McAfee és AVG víruskeresők külön-külön beállíthatók a két alapvető vírusirtó program helyett vagy mellé, így akár egyszerre 5 megbízható anti-vírus motor védheti a levelezést. A Kaspersky, a McAfee és az AVG sok éves tapasztalata és világszerte elismert anti-vírus mérnökeinek kiváló munkája teszi még erőteljesebbé és megbízhatóbbá a GFI MailSecurity-t.

- **Spyware keresés**

A GFI MailSecurity Trojan & Executable Scanner modulja sikeresen felismeri a spyware és adware fájlokat. Az opcionális Kaspersky víruskereső motor további kiterjedt adatbázissal rendelkezik az ismert spyware, adware és trójai leírásokkal.

- **Trojan & Executable Scanner**

A GFI MailSecurity Trojan & Executable Scanner analizálja a futtatható állományokat, és beépített intelligencia segítségével képes megállapítani az állományok veszélyességi szintjét. Visszafejti a kódot és megvizsgálja, hogy mit szeretne tenni az adott program, majd az eredményeket összeveti a tiltott tevékenységeket leíró adatbázissal. A kereső minden olyan programot karanténba helyez, amely gyanúsán viselkedik, ok nélkül próbál hozzáférni a modemhez, címjegyzékhez vagy a hálózathoz.

## ■ Csatolt állományok vizsgálata

A GFI MailSecurity tartalomszűrő szabályrendszere segítségével a felhasználók és csatolt állományok típusa alapján a beérkező állományok karanténba helyezhetőek. Például: minden csatolt futtatható alkalmazás a karanténba kerül és csak ellenőrzés után férhetnek hozzá a felhasználók. A GFI MailSecurity tartalomszűrője csökkenti az adatszivárgás esélyét, felügyeli a kimenő levélforgalmat is, és beavatkozik, ha visszaélést észlel (például ha egy alkalmazott adatbázist küld ki e-mailben).

## ■ HTML szkriptek automatikus eltávolítása

A HTML-levelek küldésének lehetősége a hackerek és vírusok előtt is újabb kapukat nyitott, de a GFI MailSecurity képes ellenőrizni és kiszűrni a káros kódsorokat, így a címzethez már csak a biztonságos tartalom érkezik meg.

## ■ Felhasználó szintű, szabályrendszer-alapú tartalomszűrés

A felhasználó- (címtár-) és kulcsszó-alapú, erőteljes tartalomszűrő és szabályrendszer gondoskodik arról, hogy a kétes tartalom előbb karanténba kerüljön, és csak az ellenőrzés után jusson a felhasználóhoz.

## ■ Egyéni, RSS-felügyelt karantén-szabályok

A karanténelemek gyorsabb és egyszerűbb kezelését segíti, a Microsoft Outlook Keresési mappákhoz hasonló szolgáltatás, mely a karanténmappákra is alkalmazható. Lehetőség van külön mappába gyűjteni a vírusgyanús leveleket és a gyanús mellékleteket tartalmazó leveleket későbbi ellenőrzés céljából, így hamarabb kerülhetnek a felhasználóhoz. Az RSS-csatornák segítségével még egyszerűbbé válik a mindennapi munka, mert nem kell folyamatosan belépni és ellenőrizni az új elemeket a karanténban, hanem csak az RSS-csatornákat kell szemmel tartani.

## ■ Egyszerűsített karantén-menedzsment

A GFI MailSecurity számos eszközt kínál a karanténba került elemek kezelésére. A dedikált adminisztrációs kliens a megszokott Windowsalkalmazások rugalmasságát biztosítja, míg a webalapú kliens a hálózat bármely pontján elérhető, karanténba került levelek azonnal elfogadhatók vagy elutasíthatóak. Lehetőség van az Outlook Nyilvános Mappa szolgáltatásának használatára is, amellyel a karantén-menedzsment szétsztható az adminisztrátorok között.

## ■ Riportolási lehetőségek

A GFI MailSecurity Reportpack egy ingyenes kiegészítő programcsomag, mellyel a management részére bemutató riportok készíthetőek. Az egyszerűen áttekinthető jelentések segítenek értelmezni és értékelni az alkalmazott szabályokat. Az előre definiált riportok módosítása révén új, egyéni riportsablonok készíthetőek óránkénti, napi, heti vagy havi ütemezésben, amelyek automatikusan le is kérhetőek.

## ■ Rendszerkövetelmények:

- Windows 2000 Server/Advanced Server, Windows 2003 Server/Advanced Server/SBS, Windows XP
- Microsoft Exchange Server 2000, 2003, 2007, 5.5, Lotus Notes, vagy más SMTP szerver
- Small Business Server alapokon, Exchange Server 2000 esetén SP2, Exchange Server 2003 esetén SP1 telepítés
- .NET Framework 1.1
- Microsoft Messaging Queueing Service
- IIS SMTP service

