



GFI MailSecurity

for Exchange/SMTP

Email content checking, exploit detection, anti-Trojan & anti-virus



Necesitatea monitorizării e-mailurilor pentru detectarea conținutului periculos, neplăcut sau confidential, este evidentă. Cei mai periculoși virusi, capabili să paralyzeze sistemul de mail și rețeaua în câteva minute, se propagă în întreaga lume într-un interval de ordinul orelor. Produsele care scanează cu un singur motor de scanare nu mai sunt suficiente. Mai mult, virusi de mail pot instala programe backdoor sau alte programe daunatoare care ajută intrușii să patrundă în rețea. Produsele care oferă doar funcția de antivirus nu oferă protecție pentru atacuri de acest tip.

Rezolvarea problemei constă în instalarea unei soluții complete de filtrare a conținutului/analiza punctelor slabe și antivirus pentru a proteja serverul de mail și rețeaua. GFI MailSecurity acționează ca un firewall pentru e-mail și protejează împotriva virusilor și amenințărilor ce sosesc prin e-mail, atacurilor orientate la adresa rețelei organizației. GFI MailSecurity este disponibil în două versiuni. Versiunea pentru SMTP trebuie instalată ca un mail relay server și scanează atât mesajele care intră cât și cele care ies din rețea. Versiunea ce folosește VS API se integrează cu Exchange Server 2000/2003 și scanează Information Store. Ambele variante pot fi instalate simultan pentru a obține protecție maximă.

Filtrarea conținutului e-mailurilor

Folosind motorul cu reguli de verificare a conținutului, se pot trimite în carantina mesajele pe baza utilizatorului sau a tipului de fișiere atasate, pentru a fi aprobate de către administrator. Toate atasamentele executabile sunt trimise în carantina pentru aprobare înainte de a fi trimise utilizatorilor. De aceea, față de produsele ce oferă doar capabilități antivirus, GFI MailSecurity dispune și de filtrarea conținutului pentru a preveni eficient acțiunea virusilor, worms, sau alte tipuri de atacuri. Pe lângă verificarea atasamentelor, GFI MailSecurity scanează și conținutul mesajelor pentru conținut daunător (pentru care o companie poate fi data

în judecată) și scurgeri de informații (transmiterea de informații confidențiale). Puteți de asemenea să alegeți ștergerea fișierelor .mp3 și .mpg, deoarece acestea ocupă lățimea de bandă și încarcă spațiul pe disc detinut de serverul de mail.

Verificare antivirus cu multiple motoare de scanare

GFI MailSecurity este independent de motorul de scanare și poate folosi mai multe asemenea motoare în același timp. Tehnologia de scanare pentru mesaje poate fi combinată cu alte motoare antivirus, oferind o mai bună securitate. Deoarece fiecare motor de scanare are puncte tari și puncte slabe, mai multe motoare se pot completa pentru a oferi un nivel ridicat de securitate,

Analizează executabile și troieni

GFI MailSecurity Trojan and Executable Scanner detectează executabile malicioase necunoscute prin analizarea rezultatului rularii acestora. Troienii sunt periculoși pentru că pot intra nedetectați în calculator oferind acces atacatorilor asupra datelor existente. Programele anti-virus nu detectează troieni necunoscuți deoarece se bazează pe fișiere de definiții. Motorul de scanare realizează decompilarea executabilului, aflând astfel în timp real ceea ce face și compară cu acțiuni malicioase cunoscute și trimite în carantina fișierele cu activitate suspectă cum ar fi accesarea modemului, stabilirea unor conexiuni în rețea sau accesarea address book.

Avantaje și beneficii

Motoare multiple de scanare garantează o rată mare de detecție și răspuns rapid.

Trojan & Executable Scanner detectează executabile malicioase fără actualizarea semnăturilor.

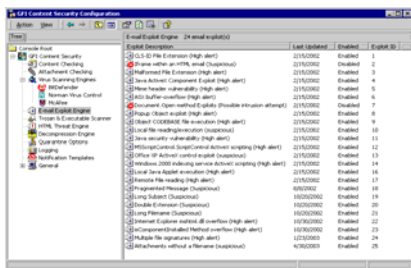
Motorul împotriva exploit-urilor și a amenințărilor HTML dezactivează exploit-urile din email și scripturi HTML.

Pret accesibil: 375€ (25), 950€ (100) sau 3750€ număr nelimitat de adrese.



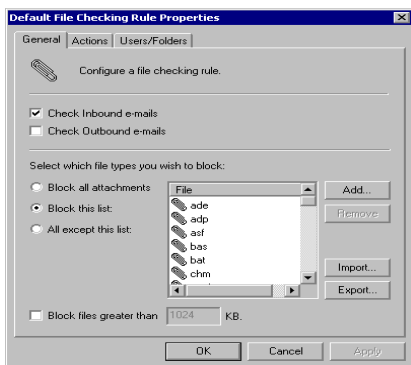
Include motoare de scanare de la Norman Virus Control si BitDefender

GFI MailSecurity include Norman Virus Control 5 si BitDefender. Norman Virus Control are un motor de scanare care a primit certificarea Virus Bulletin 100% de 23 ori la rând, si este certificat ICSA si Checkmark. BitDefender este un motor de scanare foarte rapid si flexibil care exceleaza prin numarul de formate pe care le recunoaste si poate scana. BitDefender este certificat ICSA. GFI MailSecurity actualizeaza automat definitiile de virusi pentru Norman Virus Control si BitDefender, având inclus in pret posibilitatea actualizari timp de un an.



Optional, motor de scanare McAfee si Kaspersky

Pentru o mai buna securitate, este posibila si utilizarea motorului de scanare de la McAfee si/sau cel de la Kaspersky. Motorul Kaspersky este certificat ICSA si a castigat numeroase premii din partea revistelor de specialitate: PC Magazine, PC World, etc. Este recunoscut pentru complexitatea scanarii, rata marita de aparitie a noilor definitii precum si a tehnologiei euristice unice care neutralizeaza practic virusii necunoscuti. Adaugarea motorului Kaspersky este foarte eficienta din punct de vedere al pretului. Motorul McAfee de scanare este foarte bun pentru a detecta Troieni, controale ActiveX si programe backdoor.

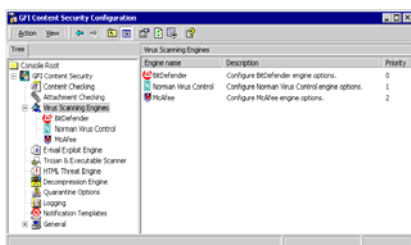


Protectie anti-spam la nivel de server

GFI MailEssentials for Exchange/SMTP ofera protectie anti-spam la nivel de server si elimina necesitatea instalarii de soft aditional anti-spam. Include de asemenea un set de metode eficiente de eliminare a spam-ului din retea. GFI MailEssentials realizeaza arhivarea mailurilor, rapoarte despre mesaje, raspunsuri automate la nivel de sever, download POP3. Se integreaza cu GFI MailSecurity.

Motor de detectie a exploit-urilor din email

Acest motor reprezinta un rezultat al cercetarilor GFI in domeniu si va protejeaza impotriva viitorilor virusi de email si atacuri ce folosesc exploit-uri necunoscute ale sistemelor de operare. Laboratoarele de securitate ale GFI descopera noi exploit-uri la nivel de email care sunt descarcate automat de GFI MailSecurity.

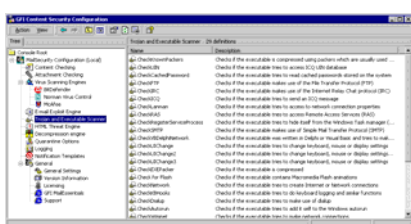


Eliminarea automata a scripturilor HTML

Posibilitatea de a transmite e-mail in format HTML a permis hackerilor sa declanseze comenzi prin inserarea lor in e-mailurile in format HTML. GFI MailSecurity verifica prezenta script-urilor in corpul mesajelor si dezactiveaza aceste comenzi inainte de a trimite e-mailul catre destinatar. GFI MailSecurity protejeaza impotriva acestor mesaje printr-un proces patentat, care actioneaza impotriva virusilor HTML si a atacurilor lansate prin intermediul e-mailurilor in format HTML.

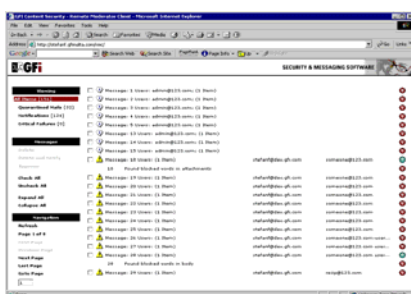
Aprobarea/respingerea mesajelor din carantina folosind clientul moderator, de mail sau bazat pe Web

GFI MailSecurity ofera cateva optiuni pentru gestiunea mesajelor din carantina. Clientul ofera o interfata simpla de aprobare/respingere a mesajelor. Moderatorul Web-based permite aprobarea/respingerea mesajelor de oriunde din retea. GFI MailSecurity permite folosirea unui director public pentru distribuirea mesajelor din carantina catre mai multi administratori.



Trimiterea automata in carantina a fisierelor Microsoft Word ce contin macro-uri

GFI MailSecurity protejeaza impotriva virusilor macro din documente Word sau Excel prin trimiterea automata in carantina a acestor documente. Puteti permite transmiterea de documente Word si Excel prin mail, deoarece GFI MailSecurity le va trimite in carantina daca pot fi distructive.



Detecteaza ascunderea sau modificarea extensiilor

Atasamentele ce contin script-uri (spre exemplu .vbs) pot fi mascate ca fiind alte tipuri de fisiere. GFI MailSecurity detecteaza si trimite in carantina astfel de fisiere ce contin script-uri sau fisiere executabile. Cu GFI MailSecurity, puteti bloca/trimitere in carantina fisierile pe baza tipului de fisier (de exemplu, executabil) pentru ca utilizatorii sa nu treaca de sistemul de securitate prin redenumirea extensiei.

Certificat Checkmark si ICSA

GFI MailSecurity detine certificat Checkmark de la West Coast Labs si certificat ICSA de la TruSecure. Checkmark demonstreaza ca produsul indeplineste standardele prin oferirea unei solutii de securitate. Certificatul Checkmark detinut de GFI MailSecurity declara ca produsul a detectat un procent de 100% din virusii actuali cu care a fost testat de compania independenta West Coast Labs.

Reguli usor de configurat, bazate pe utilizator
Interfata bazata pe MMC a GFI MailSecurity permite crearea de reguli pentru verificarea continutului si a atasamentelor, si aplicarea lor utilizatorilor sau grupurilor de utilizatori. Regulile pot folosi utilizatorii Active Directory, reducând efortul administrativ.

Reviews

Earns top spot in review of email security solutions

- InfoWorld reviewer Dan Morton has selected GFI MailSecurity for Exchange/SMTP as the best email scanner out of the six solutions he tested, including products by Gordano, Network Associates, Sophos, Symantec, and Trend Micro. GFI MailSecurity got a 'Very Good' rating and was awarded the top score of 8.3 points for its performance. "The differences in score reflect the extra features and overall maturity of some products," wrote the reviewer. "The inclusion of multiple scanning engines and the ability to act as either a server-side or gateway solution, however, are what earned GFI MailSecurity the top spot."

- *InfoWorld, June 2003*



GFI MailSecurity awarded ICSA certification – GFI MailSecurity has been awarded anti-virus certification from ICSA Labs. The certification provides independent confirmation that the email security product protects networks against email viruses.

- *ICSA Labs, May 2002*



GFI MailSecurity awarded Checkmark

– GFI MailSecurity has been awarded Anti-Virus Checkmark Level 1 certification from West Coast Labs. The certification ensures that GFI MailSecurity meets the Checkmark program's rigorous standards for detecting in-the-wild viruses.

- *West Coast Labs, April 2002*



Analiza lexicala

Modulul de verificare a continutului suporta scanare lexicala a e-mailurilor, permitând specificarea unor combinatii de cuvinte folosind operatorii AND si OR.

Clientii GFI sunt firme mari...

Multe firme cunoscute au ales sa foloseasca GFI MailSecurity for Exchange/SMTP. Iata doar cateva dintre acestea: NASA, Banca Centrala Europeana, MG Rover Group, Caterpillar PerotSystems, Port of Tilbury London Ltd, Mexx International BV (Olanda) si multe altele.

System requirements

Gateway mode:

- Windows 2000/2003 - Pro, Server or Advanced Server

- or

Windows XP (Note that if you use Windows 2000/2003 Pro or XP, you will only be able to accept a maximum of 10 inbound SMTP connections simultaneously, therefore Windows 2000/2003 Server is recommended).

- IIS5 SMTP service installed and running as an SMTP relay to your mail server.

- Microsoft Exchange Server 2003, 2000, 4, 5 or 5.5, Lotus Notes 4.5 and up, or an SMTP/POP3 mail server.

VS API mode:

- Windows 2000/2003 Server or Advanced Server.

- Exchange 2003 or Exchange 2000 Server with SP1 or higher, Exchange SP 2 recommended.

- If using Small Business Server, ensure you have installed Service Pack 2 for Exchange.

CS-SOFTWARE International SRL

Str. Izv. Crisului nr. 7, Sector 4, Bucuresti.

Tel: (021) 450.39.49, Fax: (021) 450.54.27, Mobil: 0722-25.22.11, 0744-55.22.11

E-mail: info@norman.ro, suport@norman.ro.

Web: www.norman.ro, www.css.ro

CUI: R 5247967, Nr. Inreg: J40/1387/1994

