



GFI MailSecurity

for Exchange/SMTP/Lotus

Antivirus per email, criteri di controllo del contenuto, individuazione di exploit e antitrojan

L'esigenza di controllare i messaggi email alla ricerca di contenuti pericolosi, offensivi o riservati non è mai stata più evidente. I virus più letali, capaci di danneggiare il server di posta elettronica e la rete aziendale in pochi minuti, sono distribuiti in tutto il mondo via email nel giro di poche ore. I prodotti che eseguono scansioni antivirus di un solo distributore non offrono una protezione adeguata. Peggio ancora, la posta elettronica è diventata il mezzo per installare backdoor (trojan) e altri programmi dannosi che aiutano potenziali intrusi a penetrare nella rete dell'azienda. I prodotti limitati a un singolo motore antivirus non proteggeranno dagli exploit della posta elettronica e attacchi analoghi.

L'unica difesa è l'installazione di un software antivirus e dotato di criteri di controllo del contenuto email basati sull'utente, in modo da proteggere il server di posta e la rete. GFI MailSecurity funge da firewall di email e fornisce la protezione della posta da virus email, exploit e minacce, oltre che da attacchi via email diretti all'azienda.

Benefici

Perché scegliere GFI MailSecurity per proteggersi dai virus della posta elettronica e dai codici maligni?

- Perché supporta le piattaforme di messaggistica leader del settore, ivi compresi Microsoft Exchange 2000, 2003, 2007 e Lotus Domino (in inglese)
- Perché più motori antivirus garantiscono una percentuale di scoperta più alta e una risposta più rapida
- Perché l'esclusivo scanner per trojan ed eseguibili (Trojan & Executable Scanner) rileva eseguibili pericolosi senza dover aggiornare gli antivirus: MyDoom è stato individuato immediatamente!
- Per la presenza del motore per exploit di email e dell'agente sanitizzante di HTML, che disabilitano gli exploit di posta elettronica e gli script HTML

■ Controllo antivirus grazie alla presenza di più motori di scansione

GFI MailSecurity si avvale di più scanner antivirus per eseguire la scansione delle email in entrata. L'utilizzo di più scanner riduce drasticamente il tempo medio di ottenimento delle firme antivirus che combattono le minacce più recenti, cioè riduce notevolmente le probabilità d'infezione. Infatti, una singola azienda antivirus non potrà mai essere SEMPRE la più rapida a rispondere. In occasione di ogni attacco, le aziende di antivirus rispondono in tempi diversi, a seconda del luogo in cui il virus è stato scoperto, ecc. L'utilizzo di più motori antivirus aumenta le probabilità di disporre di almeno un motore aggiornato e quindi in grado di proteggere dai virus più recenti. Inoltre, poiché ogni motore è dotato di euristiche e metodi propri, mentre un motore antivirus può essere in grado di scoprire un determinato virus e le sue varianti, un altro motore antivirus può fare altrettanto con un virus diverso. Nel complesso, più motori antivirus equivalgono a una migliore protezione.

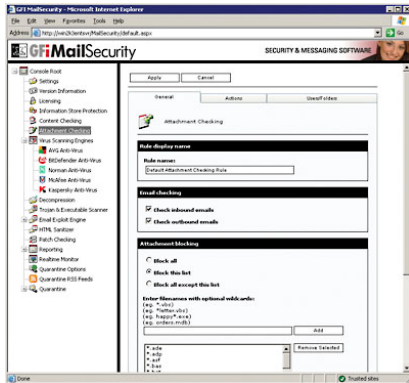
■ Scansione contro trojan ed eseguibili

Lo scanner per trojan ed eseguibili (Trojan & Executable Scanner) di GFI MailSecurity scopre gli eseguibili sconosciuti e pericolosi (ad esempio, i trojan), mediante l'analisi delle loro possibili azioni. I trojan sono pericolosi perché riescono a penetrare nel computer delle vittime a loro insaputa, garantendo all'aggressore un accesso totale ai dati memorizzati su quel computer. Il software antivirus NON cattura i trojan sconosciuti perché si basa su firme. Lo scanner per trojan ed eseguibili adotta un approccio diverso, con l'utilizzo di un'intelligenza interna che valuta il livello di rischio di un eseguibile: scompone il file eseguibile, ne analizza in tempo reale le possibili azioni e confronta queste ultime con le azioni contenute in un database di azioni pericolose. Lo scanner mette poi in quarantena qualsiasi eseguibile di attività sospette, quali, accesso a un modem, connessioni di rete o tentativi di accesso alla rubrica degli indirizzi.

GFI MailSecurity



Configurazione di GFI MailSecurity

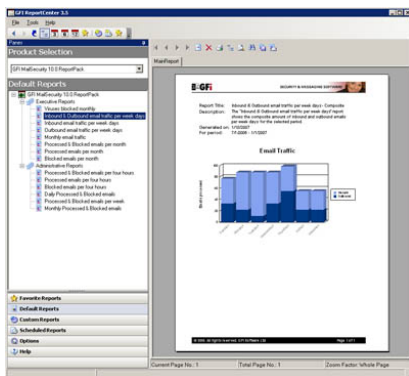


Configurazione del controllo di allegati



GFI MailSecurity supporta più motori antivirus

GFI MailSecurity ReportPack



Interfaccia utente

Inclusione dei motori antivirus Norman Virus Control e BitDefender

GFI MailSecurity è venduto in un unico pacchetto insieme a Norman Virus Control e BitDefender. Norman Virus Control è un motore antivirus di applicazione industriale che ha ricevuto il premio "100% Virus Bulletin" per 32 volte consecutive. È inoltre provvisto delle certificazioni ICSA e Checkmark. BitDefender è un motore antivirus rapido e flessibile, e primeggia per il numero di formati che è in grado di riconoscere e sottoporre a scansione. BitDefender è certificato ICSA e ha vinto i premi "100% Virus Bulletin" e "European Information Technologies Prize 2002". GFI MailSecurity ricerca e aggiorna automaticamente i file di definizione dei motori antivirus Norman Virus Control e BitDefender non appena questi si rendono disponibili. Il prezzo di GFI MailSecurity comprende aggiornamenti per un anno.

Motori antivirus Kaspersky, McAfee e AVG (facoltativi)

Per ottenere una protezione ancora maggiore, gli utenti hanno la facoltà di aggiungere i motori antivirus Kaspersky, McAfee e/o AVG come terzo, quarto e quinto motore antivirus o in sostituzione di uno degli altri motori. L'antivirus Kaspersky è certificato ICSA ed è noto per la sua insuperata profondità di scansione degli oggetti, l'alta percentuale di rilascio di nuove firme antivirus e la sua esclusiva tecnologia euristica che neutralizza efficacemente i virus sconosciuti. Il motore McAfee è particolarmente efficace nell'individuazione di attacchi non correlati a virus, come quelli collegati a controlli ActiveX maligni. Con 15 anni di esperienza nel settore degli antivirus, GRISOFT si avvale di alcuni dei principali esperti mondiali del settore dei software antivirus, in particolare nelle aree dell'analisi e scoperta dei virus.

Rimozione automatica di script HTML

L'avvento delle email in formato HTML ha consentito agli hacker e ai creatori di virus di attivare comandi incorporandoli nell'email HTML. GFI MailSecurity cerca codici di script nel testo del messaggio email e disabilita tali comandi prima di inviare l'email HTML "pulita" al destinatario. Con l'ausilio di un processo brevettato da GFI, GFI MailSecurity è il solo prodotto in grado di difendere da email HTML potenzialmente dannose, proteggendo così da virus HTML e da attacchi lanciati tramite email HTML.

Motore per la scoperta di exploit della posta elettronica

Il motore contro gli exploit di email di GFI MailSecurity (Email Exploit Engine) si basa su ricerche di prim'ordine condotte dai laboratori GFI sugli exploit di email e protegge da virus di email future e attacchi che si avvalgono di noti exploit di applicazioni o del sistema operativo. Ad esempio, GFI MailSecurity ha protetto dai virus Nimda e Klez, quando questi sono emersi per la prima volta, senza la necessità di aggiornamenti, perché questi virus utilizzano exploit noti. Presso i GFI SecurityLabs si scoprono regolarmente nuovi exploit di posta elettronica, che vengono poi automaticamente scaricati da GFI MailSecurity. GFI MailSecurity è l'unico prodotto di protezione della posta elettronica che rileva gli exploit di email.

Individuazione di spyware

Lo scanner per trojan ed eseguibili (Trojan & Executable Scanner) di GFI MailSecurity riesce a riconoscere file maligni, compresi spyware e adware (software spia e pubblicitari). GFI MailSecurity è inoltre in grado di individuare, tramite il motore antivirus Kaspersky (facoltativo), spyware trasmessi via email, poiché esso incorpora un file di definizioni spyware e adware provvisto di un ampio database di spyware, trojan e adware noti.

Controllo di allegati

Le regole di controllo degli allegati di GFI MailSecurity consentono agli amministratori di mettere in quarantena gli allegati in base all'utente e al tipo di file. Ad esempio, è possibile mettere in quarantena tutti gli allegati eseguibili affinché siano rivisti dall'amministratore prima di essere distribuiti all'utente. GFI MailSecurity può inoltre eseguire la scansione alla ricerca di fughe di informazioni - ad esempio, un dipendente che manda un database via email. È anche possibile scegliere di eliminare allegati come file .mp3 o .mpg.

■ Valore aggiunto per GFI MailSecurity grazie al potente strumento di creazione di rapporti

Il ReportPack di GFI MailSecurity rappresenta un prodotto complementare, del tutto sviluppato, per GFI MailSecurity. Dai rapporti sull'andamento finanziario (ROI) per il personale dirigente ai rapporti drill-down giornalieri per quello tecnico, il ReportPack di GFI MailSecurity fornisce le informazioni desiderate grazie a una semplice visualizzazione, in modo da comprendere appieno i modelli di protezione della posta elettronica. La pianificazione personalizzata e totalmente automatizzata consente una vera funzionalità del tipo "installa e dimentica"! Il ReportPack di GFI MailSecurity offre numerosi rapporti predefiniti e personalizzabili, che possono essere elaborati con i seguenti intervalli: ogni ora, giornalmente, settimanalmente o mensilmente, compresi quelli su:

- virus bloccati
- traffico email in entrata
- traffico email in uscita
- traffico email in entrata e in uscita totale
- email elaborate
- email bloccate
- e molto altro!

■ Filtraggio e criteri granulari di controllo del contenuto email basato sull'utente

Il potente motore di regole dei criteri di controllo del contenuto di GFI MailSecurity consente la configurazione di set di regole per utente e parola chiave, e quindi di mettere in quarantena contenuti e allegati potenzialmente pericolosi, ai fini della successiva approvazione dell'amministratore. In questo modo, GFI MailSecurity è anche in grado di eseguire la scansione alla ricerca di contenuto offensivo.

■ Personalizzazione dei filtri di quarantena

GFI MailSecurity consente di configurare una serie di cartelle di ricerca (simili alle Cartelle ricerche di MS Outlook) all'interno dell'Archivio di quarantena ("Quarantine Store") e quindi di gestire in modo migliore e più rapido le email messe in quarantena. Ad esempio, si può impostare una cartella per le email messe in quarantena dal controllo antivirus e un'altra per quelle messe in quarantena dal controllo di allegati di un determinato utente, consentendo di creare priorità relativamente alle cartelle da controllare per prime: può essere più importante esaminare prima la cartella di controllo degli allegati, poiché questa ha una maggiore probabilità di contenere email in attesa di essere approvate e inoltrate agli utenti.

■ Facile monitoraggio delle cartelle di quarantena con i feed RSS

GFI MailSecurity si serve delle potenzialità dei feed RSS (Really Simple Syndication) per agevolare il lavoro di controllo dell'archivio di quarantena delle email da parte dell'amministratore. Con l'ausilio dei feed RSS, si viene informati su tutti i nuovi oggetti messi in quarantena, evitando di doversi collegare all'archivio di quarantena per ricercare i nuovi elementi manualmente.

■ Configurazione basata sul web, per la gestione remota da qualsiasi locazione

La configurazione basata su internet del prodotto permette di impostare e controllare il prodotto e gestire le email messe in quarantena da qualsiasi computer dotato di un browser, in modalità remota. Di conseguenza, è possibile controllare e gestire GFI MailSecurity da qualsiasi parte del mondo.

Requisiti di sistema

- Windows 2000 Server, Advanced Server (Service Pack 1 o superiore) oppure Windows 2003 Server, Advanced Server o Windows XP
- Microsoft Exchange Server 2000 (SP1), 2003, 2007, 4, 5 o 5.5, Lotus Domino oppure un server di posta SMTP o POP3
- Se ci si avvale di Small Business Server, accertarsi di aver installato il Service Pack 2 (SP2) per Exchange Server 2000 e il Service Pack 1 (SP1) per Exchange Server 2003
- Microsoft .NET Framework 1.1 o 2.0
- MSMQ: Microsoft Messaging Queuing Service (Servizio di accodamento messaggi di Microsoft)
- Internet Information Services (IIS): servizi SMTP e World Wide Web
- Microsoft Data Access Components (MDAC) 2.8.

Premi



Scaricate la copia di valutazione da <http://www.gfi-italia.com/italia/mailsecurity/>

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com