Prodotto con **diversi antivirus** per la protezione della posta elettronica

Migliaia di clienti

Prezzi **fantastici**

Prestazioni di protezione **eccellenti**

Prodotto per la protezione della posta elettronica provvisto di un massimo di 5 scanner antivirus

Il volume sempre maggiore di virus e altro malware serve a evidenziare l'importanza, per le aziende, di dotarsi di una protezione della rete dai virus e dagli exploit della posta elettronica. Le varianti della gamma di virus che appaiono tutti i giorni sono talmente numerose che i prodotti che si avvalgono di singoli motori antivirus per eseguire la scansione delle e-mail in entrata non offrono una protezione sufficiente, a livello di server o di client desktop. Per proteggere la rete da virus serve un prodotto come GFI MailSecurity, che è dotato non di un singolo motore antivirus, ma fino a 5 motori in esecuzione sul server di posta elettronica.

Con più motori antivirus è possibile:

- ridurre il tempo medio di ottenimento delle firme antivirus che combattono le ultimissime minacce
- trarre vantaggio da tutti i loro punti di forza, perché nessun singolo scanner antivirus, singolarmente preso, è il migliore
- eliminare praticamente le probabilità d'infezione
- avvalersi di un prodotto dal prezzo inferiore a qualsiasi soluzione antivirus a motore singolo.

VANTAGGI

- Compatibilità con le piattaforme di messaggistica leader nel settore, incluse Microsoft Exchange 2000, 2003, 2007, 2010 e Lotus Domino
- Diversi motori antivirus che garantiscono una percentuale di scoperta più alta e una risposta più rapida
- Scanner per trojan ed eseguibili che individua eventuali file eseguibili dannosi senza l'esigenza di aggiornamenti antivirus
- Il motore contro gli exploit di e-mail (Email Exploit Engine) e l'agente sterilizzante di HTML (HTML Sanitizer) disabilitano gli exploit di posta elettronica e gli script HTML.

GFI MailSecurity™

Protezione della posta elettronica per Exchange, SMTP e Lotus

Inclusione dei motori antivirus Norman e BitDefender

GFI MailSecurity è venduto in un unico pacchetto insieme a Norman Virus Control e BitDefender. Norman è un motore antivirus di applicazione industriale che ha ricevuto il premio "100% Virus Bulletin" più di 30 volte consecutive. La sandbox di Norman analizza il comportamento di file sospetti nei casi di mancata riuscita dell'analisi basata su firme. BitDefender è un motore antivirus pluripremiato rapido e flessibile in grado di riconoscere e sottoporre a scansione una vastissima gamma di formati. GFI MailSecurity controlla e aggiorna in modo automatico i file di definizione dei motori non appena gli stessi si rendono disponibili. Il prezzo di GFI MailSecurity comprende aggiornamenti per un anno.

Motori antivirus Kaspersky, McAfee e AVG (facoltativi)

Per aumentare ulteriormente la protezione, gli utenti possono aggiungere i motori antivirus Kaspersky, McAfee e AVG come terzo, quarto o quinto motore antivirus o in sostituzione di uno degli altri motori. AVG offre inoltre l'opzione di avvalersi di LinkScanner per analizzare collegamenti ipertestuali sospetti nel testo delle e-mail.

Analizzatore di trojan ed eseguibili

Lo scanner per trojan ed eseguibili (Trojan Executable Scanner) di GFI MailSecurity rileva gli eseguibili sconosciuti e pericolosi (ad esempio, i trojan) analizzandone le potenziali azioni.

Individuazione di spyware

L'analizzatore di trojan ed eseguibili di GFI MailSecurity è in grado di riconoscere file maligni, compresi spyware e adware (software spia e pubblicità). GFI MailSecurity è inoltre in grado di individuare spyware trasmesso via posta elettronica, mediante il motore antivirus facoltativo Kaspersky, che incorpora un file dedicato di definizioni spyware e adware provvisto di un ampio database di spyware, trojan e adware noti.

Controllo degli 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 vengano rivisti dall'amministratore prima di essere recapitati all'utente. GFI MailSecurity può inoltre rilevare fughe di informazioni, ad esempio quando un dipendente invia un database tramite posta elettronica. È anche possibile scegliere di eliminare allegati quali file .MP3 o .mpg.

ReportPack di 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.

Filtraggio e criteri granulari di controllo del contenuto della posta elettronica in base all'utente

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

Altre funzionalità:

- Scansione completa delle e-mail interne
- Personalizzazione dei filtri di quarantena
- Sandbox di Norman AV e Link Scanner di AVG facoltativo che forniscono una migliore scoperta del malware
- Pannello degli strumenti
- Facile monitoraggio delle cartelle di quarantena con i feed RSS
- Configurazione basata sul web, per la gestione remota da qualsiasi luogo
- Approvazione o rifiuto di messaggi messi in quarantena con l'ausilio del client moderatore, quello di posta elettronica o il moderatore basato sul web
- Rapporti completi sulle minacce delle e-mail messe in quarantena
- Motore per la scoperta degli exploit della posta elettronica
- Rimozione automatica di script HTML

Configurazione del controllo di allegati

Configurazione di GFI MailSecurity

Requisiti di sistema

- Windows 2000 Server, Advanced Server (Service Pack 1 o versioni successive), Windows 2003 Server/Advanced Server, Windows XP o Windows Server 2008
- Microsoft Exchange Server 2010, 2007, 2003, 2000 (SP1), 5.5, 4.5, Lotus Domino 4 e superiori o qualunque server di posta SMTP e/o POP3
- Microsoft .NET Framework 2.0
- MSMQ – Microsoft Messaging Queuing Service (Servizio di accodamento messaggi di Microsoft)
- Internet Information Services (IIS): servizio SMTP e servizio World Wide Web
- Microsoft Data Access Components (MDAC) 2.8.

Per ulteriori informazioni e per scaricare la versione di valutazione gratuita, visitare il sito http://www.gfi-italia.com/mailsecurity/

Microsoft GOLD CERTIFIED Partner

GFI MailSecurity™

Protezione della posta elettronica per Exchange, SMTP e Lotus

Contatti

Geco Sistemi Srl
Via Delle Rose, 7, 24040
Lallio (BG),
Italy

Tel: +39 035 200382
Tel: + 39 035 200710
Email: info@gecosistemi.com
Url: www.gecosistemi.com

© 2011 GFI Software - Windows 7, 2008, Vista, 2003, XP, 2000 ed NT sono marchi di Microsoft Corporation. GFI MailSecurity è un marchio commerciale registrato e GFI e il logo GFI sono marchi commerciali di GFI in Germania, negli Stati Uniti, nel Regno Unito e in altri paesi. Tutti i prodotti e le aziende citati nel presente documento possono essere marchi commerciali dei rispettivi proprietari.

GFI www.gfi-italia.com