GFI MailSecurity

for Exchange/SMTP

Anti-virus, directivas de contenido, detección de vulnerabilidades y anti-troyanos para el correo

La necesidad de controlar los mensajes de correo electrónico en busca de contenido peligroso, ofensivo o confidencial nunca ha sido más evidente. Los virus más mortíferos, capaces de dejar incapacitado su sistema de correo y su red corporativa en minutos, están siendo distribuidos alrededor del mundo mediante el correo electrónico en cuestión de horas. Los productos que realizan un simple escaneo anti-virus de un fabricante no proporcionan suficiente protección. Peor aún, el correo se ha convertido en la forma de instalar backdoors (troyanos) y otros peligrosos programas que ayuden a los potenciales intrusos a introducirse en su red. Los productos restringidos a un único motor anti-virus no protegerán contra debilidades de correo y ataques de esta clase.

Su única defensa es instalar un software integral exhaustivo de directiva de contenido y anti-virus para salvaguardar su servidor de correo y su red. GFI MailSecurity actúa como un cortafuegos de correo electrónico y proporciona seguridad al correo protegiéndolo de virus, vulnerabilidades y amenazas de correo, así como de los ataques por correo dirigidos a su organización.

GFI MailSecurity puede ser implementado en modo Gateway o VS API. La versión Gateway SMTP debe implantarse en el perímetro de la red como servidor retransmisor de correo y analiza el correo entrante y saliente. La versión Exchange 2000 VS-API se integra estrechamente con Exchange Server 2000/2003 y analiza los almacenes de información de Exchange.

Beneficios

¿Por qué escoger GFI MailSecurity para protegerse contra virus y malware de correo?

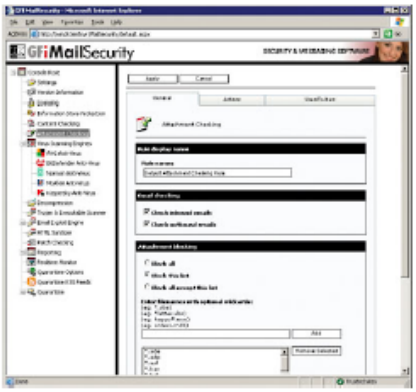
- Múltiples motores anti-virus garantizan un ratio de detección más alto y una respuesta más rápida
- Su único Escáner de Troyanos y Ejecutables detecta los ejecutables maliciosos sin necesitar de actualizaciones de virus - ¡MyDoom fue inmediatamente detectado!
- El Motor de Vulnerabilidades de Correo y el Purificador HTML desactivan las vulnerabilidades de correo y los scripts HTML

Análisis de virus utilizando múltiples motores anti-virus

GFI MailSecurity utiliza varios motores anti-virus para analizar el correo entrante. Utilizar varios escáneres reduce drásticamente el tiempo medio para obtener las firmas de virus que combatan las últimas amenazas, y por lo tanto reduce las posibilidades de una infección. La razón de esto es que una única empresa anti-virus no puede ser SIEMPRE la más rápida en responder. Para cada epidemia, las empresas anti-virus tienen diferentes tiempos de respuesta a un virus, dependiendo de donde fue descubierto el virus, etc. Mediante el uso de varios motores anti-virus, tiene muchas mejores opciones de tener al menos uno de sus motores anti-virus al dia y capaz de protegerle contra los últimos virus. Además, como cada motor tiene sus propios métodos y heurística, es probable que un motor anti-virus sea mejor detectando un virus concreto y sus variantes, mientras que otro motor anti-virus sería más potente al detectar otros virus. En general, más motores anti-virus significan mejor protección. *Nota: Investigaciones independientes mostratron que el nombre de la firma no garantiza tiempos de respuesta más rápidos; de hecho alguna de las grandes marcas se encontraban entre las más lentas.*

GFI MailSecurity

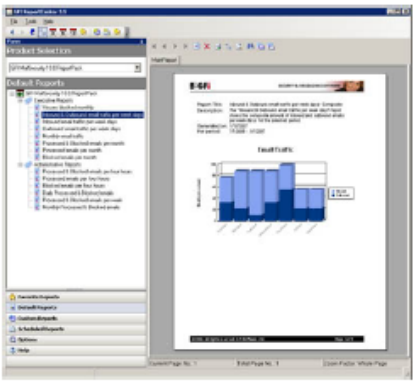
Configuración de GFI MailSecurity



Configurar el análisis de adjuntos

GFI MailSecurity admite múltiples motores anti-virus

GFI MailSecurity ReportPack



Interfaz de usuario

Escáner contra troyanos y ejecutables

El Escáner de Troyanos y Ejecutables de GFI MailSecurity detecta ejecutables desconocidos y maliciosos (por ejemplo, Troyanos) analizando qué hace el ejecutable. Los Troyanos son tan peligrosos que puede entrar en el equipo de la víctima sin ser detectados, concediendo a un atacante el acceso sin restricciones a los datos almacenados en dicho equipo. El software anti-virus NO detectará los troyanos desconocidos ya que se basa en las firmas de virus. El Analizador de Troyanos y Ejecutables utiliza una técnica diferente basada en un análisis inteligente del nivel de riesgo del ejecutable. Esto lo hace decompilando el ejecutable, detectando en tiempo real que podría hacer, y comparando sus acciones con una base de datos de acciones maliciosas. El analizador pone en cuarentena cualquier ejecutable que realice actividades sospechosas, tales como acceso a un módem, activación de conexiones de red o acceso a la libreta de direcciones.

Están incluidos los motores antivirus Norman Virus Control y BitDefender

GFI MailSecurity se entrega junto con Norman Virus Control y BitDefender. Norman Virus Control es un potente motor antivirus que ha recibido el premio 100% Virus Bulletin 32 veces consecutivas. También tiene la certificación ICSA y Checkmark. BitDefender es un motor antivirus muy rápido y flexible que sobresale en el numero de formatos que reconoce y es capaz de escanear. BitDefender está certificado por ICSA y ha ganado los premios 100% Virus Bulletin y European Information Technologies Prize 2002. GFI MailSecurity actualiza automáticamente el archivo de definición de BitDefender con los nuevos que estén disponibles. El precio de GFI MailSecurity incluye las actualizaciones por un año.

Motores anti-virus Kaspersky, McAfee y AVG (opcionales)

Para adquirir aún mayor seguridad, los usuarios pueden incluir el motor anti-virus Kaspersky, McAfee y/o AVG como un tercer, cuarto o quinto motor o para reemplazar uno de los otros motores. Kaspersky Anti-Virus está certificado por ICSA y es bien conocido por la exhaustividad no superadada de escaneo de objetos, el alto ratio en el que aparecen nuevas firmas de virus, y su tecnología heurística única que efectivamente neutraliza virus desconocidos. El motor anti-virus McAfee es particularmente potente detectando ataques que no son virus tal como pícaros controles ActiveX. Con 15 años de experiencia en la industria anti-virus, GRISOFT emplea a algunos de los expertos mundiales en software anti-virus, específicamente en las áreas de análisis y detección de virus.

Eliminación automática de los scripts HTML

La llegada del correo HTML ha hecho posible para los hackers/creadores de virus el ejecutar comandos incrustados en el correo HTML. GFI MailSecurity busca código script en el cuerpo del mensaje y deshabilita esos comandos antes de enviar el correo HTML "limpio" al destinatario. GFI MailSecurity es el único producto que le protege de los correos electrónicos HTML potencialmente maliciosos utilizando un proceso patentado por GFI, guardándole de virus HTML y de ataques lanzados vía correo HTML.

Motor de detección de debilidades de correo

El Motor de Vulnerabilidades de Correo de GFI se basa en la destacada investigación sobre vulnerabilidades de correo de GFI, y le protege de futuros virus y ataques de correo que utilicen aplicaciones conocidas o vulnerabilidades del sistema operativo. Por ejemplo, GFI MailSecurity le habría protegido frente a los virus Nimda y Klez la primera vez que surgieron sin necesidad de ninguna actualización, porque estos virus utilizan debilidades conocidas. GFI SecurityLabs encuentra regularmente nuevas debilidades de correo, y estas son automáticamente descargadas por GFI MailSecurity. GFI MailSecurity es el único producto de seguridad de correo que protege contra las debilidades de correo.

Detección de software espía (spyware)

El Escáner de Troyanos y Ejecutables de GFI MailSecurity puede reconocer archivos maliciosos incluyendo spyware y adware. GFI MailSecurity también puede detectar spyware transmitido por correo mediante el motor anti-virus Kaspersky (opcional) que incorpora un archivo de definición spyware y adware que disponen de una extensa base de datos de spyware, troyanos y adware conocidos.

Análisis de adjuntos

Las reglas de comprobación de adjuntos de GFI MailSecurity permiten a los administradores poner en cuarentena los adjuntos en base al usuario y al tipo de archivo. Por ejemplo, todos los adjuntos ejecutables pueden ser puestos en cuarentena para revisión administrativa antes de que sean distribuidos a los usuarios. GFI MailSecurity también puede buscar contenido ofensivo y fugas de información, por ejemplo, un empleado enviando por correo una base de datos. También puede escoger eliminar los adjuntos, como archivos .mp3 o .mpg.

Multiplique el valor de GFI MailSecurity con poderosos informes

GFI MailSecurity 10 ReportPack es un completo complemento de generación de informes para GFI MailSecurity 10. Desde informes de tendencias para los gestores (ROI) a informes desplegables diarios para el personal técnico; GFI MailSecurity ReportPack proporciona a los administradores información fácil de examinar que necesitan para comprender completamente sus patrones de seguridad de correo. ¡La completa automatización y la programación personalizada le permiten autentica funcionalidad instalar-y-olvidar! El ReportPack de GFI MailSecurity ofrece varios informes predefinidos y personalizables que pueden ser preparados cada hora, día, semana o mes, incluyendo:

- Virus bloqueados
- Tráfico entrante de correo
- Tráfico saliente de correo
- Tráfico completo entrante y saliente de correo
- Correos procesados
- Correos bloqueados
- ¡Y más!

Exhaustiva directiva/filtrado de contenido de correo basada en usuarios

Utilizando el poderoso motor de directivas de contenido de GFI MailSecurity puede configurar conjuntos de reglas basadas en el usuario y en palabras que le permiten poner en cuarentena archivos peligrosos para aprobación administrativa. De esta forma, GFI MailSecurity también puede buscar contenido ofensivo.

Requerimientos del sistema

- Windows 2000 Server/Advanced Server (Service Pack 1 o superior) o Windows 2003 Server/Advanced Server o Windows XP. **Nota:** Como Windows XP tiene algunas limitaciones de velocidad, instalar GFI MailSecurity en un equipo Windows XP puede afectar su rendimiento.
- Microsoft Exchange server 2000 (SP1), 2003, 4, 5 ó 5.5, Lotus Notes 4.5 y superior, o cualquier servidor de correo SMTP/POP3.
- Cuando utilice Small Business Server, asegúrese de haber instalado SP2 para Exchange Server 2000 y SP1 para Exchange Server 2003.
- Microsoft .NET Framework 1.1/2.0.
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – Servicio SMTP y servicio World Wide Web.
- Microsoft Data Access Components (MDAC) 2.8.

Premios

Descargue su versión de evaluación de http://www.gfihispana.com/es/mailsecurity/

www.cromlec.com

cromlec
...al servei de les persones

Microsoft GOLD CERTIFIED Partner

GFI
www.gfi.com