



GFI MailSecurity

for Exchange/SMTP/Lotus

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



The need to monitor email messages for dangerous, offensive or confidential content has never been more evident. The most deadly viruses, able to cripple your email server and corporate network in minutes, are being distributed worldwide via email in a matter of hours. Products that perform single vendor anti-virus scanning do not provide sufficient protection. Worse still, email has become the means for installing backdoors (trojans) and other harmful programs to help potential intruders break into your network. Products restricted to a single anti-virus engine will not protect against email exploits and attacks of this kind.

Your only defense is to install comprehensive email content policy and anti-virus software to safeguard your mail server and network. GFI MailSecurity acts as an email firewall and provides email security by protecting you from email viruses, exploits and threats, as well as email attacks targeted at your organization.

■ Virus checking with multiple virus scanning engines

GFI MailSecurity uses multiple virus scanners to scan inbound mail. Using multiple scanners drastically reduces the average time to obtain virus signatures which combat the latest threats, and therefore greatly reduces the chances of an infection. The reason for this is that a single anti-virus company can never ALWAYS be the quickest to respond. For each outbreak, virus companies have varying response times to a virus, depending on where the virus was discovered, etc. By using multiple virus engines, you have a much better chance of having at least one of your virus engines up-to-date and able to protect against the latest virus. In addition, since each engine has its own heuristics and methods, one virus engine is likely to be better at detecting a particular virus and its variants, while another virus engine would be stronger at detecting a different virus. Overall, more virus engines means better protection.

■ Spyware detection

GFI MailSecurity's Trojan & Executable analyzer can recognize malicious files including spyware and adware. GFI MailSecurity can also detect spyware transmitted by email via the Kaspersky virus engine (optional) which incorporates a dedicated spyware and adware definition file that has an extensive database of known spyware, trojans and adware.

Benefits

Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003 and 2007

Multiple virus engines guarantee higher detection rate and faster response

Unique Trojan & Executable Scanner detects malicious executables without need for virus updates

Email Exploit Engine and HTML Sanitizer disable email exploits & HTML scripts.

■ NORMAN and BITDEFENDER virus engines are included

GFI MailSecurity is bundled with Norman Virus Control and BitDefender. Norman is an industrial strength virus engine that has received the 100% Virus Bulletin award 32 times running. It also has ICSA and Checkmark certification. BitDefender is a fast, flexible virus engine that excels in the number of formats it can scan. BitDefender is ICSA certified and has won the 100% Virus Bulletin award and the European IT Prize 2002. GFI MailSecurity automatically checks and updates the engines' definition files as they become available. The GFI MailSecurity price includes updates for one year.

■ KASPERSKY, MCAFEE and AVG virus engines (optional)

To achieve even greater security, users can add the Kaspersky, McAfee and/or AVG anti-virus engines as a third, fourth or fifth anti-virus engine. Kaspersky Anti-Virus is ICSA-certified and is well known for the high rate at which new virus signatures are released. The McAfee virus engine is particularly strong at detecting non-virus attacks such as rogue ActiveX controls. With 15 years of experience in the anti-virus industry, GRISOFT employs some of world's leading experts in anti-virus software, specifically in the areas of virus analysis and detection.

■ Trojan and executable analyzer

The GFI MailSecurity Trojan & Executable analyzer detects unknown malicious executables (for example, trojans) by analyzing what an executable does. Trojans are dangerous as they can enter a victim's computer undetected, granting an attacker access to the data stored on that computer. Anti-virus software will NOT catch unknown trojans because it is signature-based. The Trojan & Executable Scanner takes a different approach by using built-in intelligence to rate an executable's risk level. It does this by disassembling the executable, detecting in real time what it might do, and comparing its actions to a database of malicious actions. The scanner then quarantines any executables that perform suspicious activities, such as accessing a modem, making network connections or accessing the address book.

■ Attachment checking

GFI MailSecurity's attachment checking rules enable administrators to quarantine attachments based on user and file type. For example, all executable attachments can be quarantined for administrator review before they are distributed to the user. GFI MailSecurity can also scan for information leaks, for example, an employee emailing a database. You can also choose to delete attachments like .mp3 or .mpg files.



Full threat reporting for quarantined emails

When an email is quarantined, GFI MailSecurity gives a full threat report, detailing all threats identified per mail.

Searching within quarantined emails

It is possible to conduct searches within all emails that GFI MailSecurity quarantines. Such searches can be performed among inbound or outbound emails to or from a particular user, for instance. Searches can also be carried out based on sender, recipient and also quarantine reason, freeing the administrator from the need to go through all quarantined emails one by one.

Checkmark & ICSA certified

GFI MailSecurity holds Checkmark certification from West Coast Labs and ICSA certification from TruSecure.

Web-based configuration – enables remote management from any location

The product's web-based configuration allows you to configure and monitor the product and manage quarantined emails remotely from any computer that is equipped with a browser. This means that you can monitor and manage GFI MailSecurity from anywhere in the world.



System requirements

- Windows 2000 Server/Advanced Server (Service Pack 1 or higher) or Windows 2003 Server/Advanced Server or Windows XP. Note: Since Windows XP has some speed limitations installing GFI MailSecurity on a machine running Windows XP could affect its performance
- Microsoft Exchange server 2000 (SP1), 2003, 2007, 4, 5 or 5.5, Lotus Domino 4.5 and up, or any SMTP/POP3 mail server
- When using Small Business Server, ensure you have installed SP 2 for Exchange Server 2000 and SP1 for Exchange Server 2003
- Microsoft .NET Framework 1.1
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) – SMTP service & World Wide Web service.

Granular user-based email content policies/filtering

Using GFI MailSecurity's powerful content policies rules engine, you can configure rule sets based on user and keywords that allow you to quarantine potentially dangerous content for administrator approval. In this way, GFI MailSecurity can also scan for offensive content.

Custom quarantine filters

GFI MailSecurity enables you to configure a series of search folders (similar to MS Outlook Search Folders) within the 'Quarantine Store', permitting you to manage quarantined emails better and faster. For example, you can set up a folder for emails that were quarantined by virus checking and another for emails quarantined by attachment checking for a particular user, allowing you to prioritize which folders you check first: It may be more important to examine the attachment checking folder first as it is more likely to contain emails that need to be approved and forwarded to users.

Enable easy quarantine folder monitoring through RSS feeds

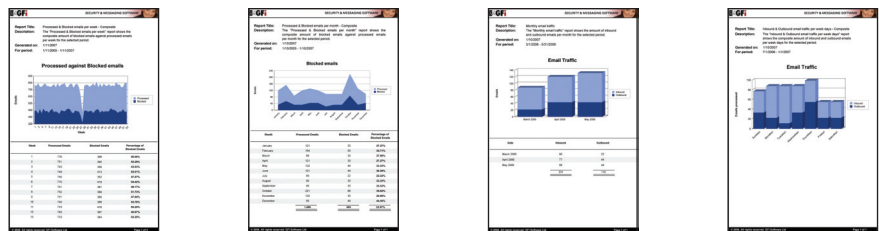
GFI MailSecurity takes advantage of the power of RSS (Really Simple Syndication) feeds to simplify your work as an administrator in keeping an eye on your email quarantine store. Through RSS feeds, you will be informed of all new quarantined objects, avoiding the need to log onto the quarantine store to check for new updates manually.

Approve/reject quarantined email using the moderator client, email client or web-based moderator

GFI MailSecurity provides several options for moderating quarantined mail. The moderator client gives you a familiar Windows interface for approving/rejecting email. The web-based moderator allows you to approve/reject emails from anywhere on your network. Alternatively, GFI MailSecurity can also forward quarantined mails to an email address, enabling you to use a public folder to distribute the quarantined items to multiple administrators.

Multiply the value of GFI MailSecurity with powerful reporting

The GFI MailSecurity 10 ReportPack is a full-fledged reporting companion to GFI MailSecurity 10. The ReportPack provides you with the easy-to-view information you need to fully understand your email security patterns. The GFI MailSecurity ReportPack offers several default and customizable reports that can be prepared on an hourly, daily, weekly or monthly basis including: Viruses blocked; Inbound email traffic; Outbound email traffic; Total inbound and outbound email traffic; Processed emails; Blocked emails and more!



Download your evaluation version from <http://www.gfi.com/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
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 2138 2418
Fax +356 2138 2419
sales@gfi.com

