# GFi MailSecurity

## for Exchange/SMTP

Email anti-virus, content policies, exploit detection and 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 granular user-based email content policy and anti-virus software to safeguard your mail server and network. GFI MailSecurity acts as an email firewall and provides mail security by protecting you from email viruses, exploits and threats, as well as email attacks targeted at your organization.

GFI MailSecurity may be deployed in Gateway or VS API mode. The gateway version should be deployed at the perimeter of the network as an email relay server and scans inbound and outbound mail. The VS API version integrates seamlessly with Exchange Server 2000/2003 and scans the Exchange information stores.

### Virus checking with multiple virus scanning engines

GFI MailSecurity uses multiple virus scanners to scan inbound email. 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. *Note: Independent research showed that brand names are no guarantee for faster response times; in fact some of the big brand names were found to be among the slowest.*

### Features & benefits

Multiple virus engines guarantee higher detection rate and faster response

Unique Trojan & Executable Scanner detects malicious executables without need for virus updates – MyDoom was detected immediately!

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

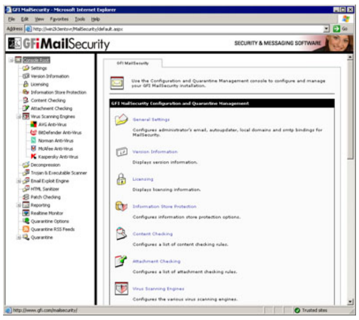
Unbeatable price: USD 500 (25), USD 1650 (100) and USD 7500 (1000) mailboxes.

### Scan against trojans and executables

The GFI MailSecurity Trojan & Executable Scanner 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 unrestricted 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.

### Norman Virus Control & BitDefender virus engines are included

GFI MailSecurity is bundled with Norman Virus Control and BitDefender. Norman Virus Control 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 very fast and flexible virus engine that excels in the number of formats it can recognize and scan. BitDefender is ICSA certified and has won the 100% Virus Bulletin award and the European Information Technologies Prize 2002. GFI MailSecurity automatically checks and updates the Norman Virus Control and BitDefender definition files as they become available. The GFI MailSecurity price includes updates for one year.



Use the Configuration and Quarantine Management console to configure and manage your GFI MailSecurity installation.

**GFI MailSecurity Configuration and Quarantine Management**

General Settings
Configures administrator's email, autoupdater, local domains and smtp bindings for MailSecurity.

Version Information
Displays version information.

Licensing
Displays licensing information.

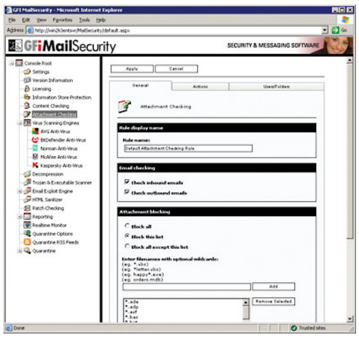
Information Store Protection
Configures information store protection options.

Content Checking
Configures a list of content checking rules.

Attachment Checking
Configures a list of attachment checking rules.

Virus Scanning Engines
Configures the various virus scanning engines.

GFI MailSecurity configuration


GFI MailSecurity - Microsoft Internet Explorer
Address http://win2k3entsvr/MailSecurity/default.aspx
GFiMailSecurity
SECURITY & MESSAGING SOFTWARE
Console Root
Attachment Checking
Apply
Cancel
General
Actions
Users/Folders
Add
Remove Selected
Done
Trusted sites

Attachment Checking

**Rule display name**

Rule name: Default Attachment Checking Rule

**Email checking**

☑ Check inbound emails
☑ Check outbound emails

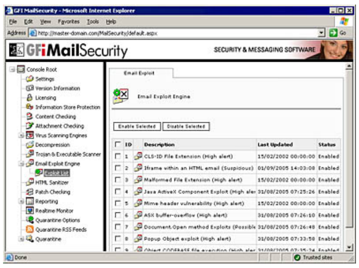
**Attachment blocking**

○ Block all
● Block this list
○ Block all except this list

Enter filenames with optional wildcards:
(eg. *.vbs)
(eg. *letter.vbs)
(eg. happy*.exe)
(eg. orders.mdb)

*.ade
*.adp
*.asf
*.bas

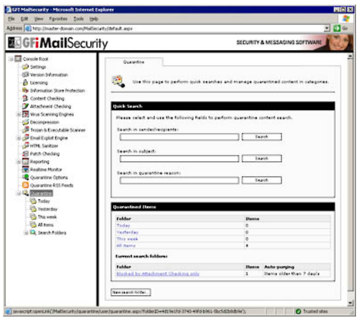
Configure attachment checking


GFI MailSecurity - Microsoft Internet Explorer
Address http://master-domain.com/MailSecurity/default.aspx
GFiMailSecurity
SECURITY & MESSAGING SOFTWARE
Console Root
Email Exploit Engine
Exploit List
Email Exploit
Enable Selected
Disable Selected
Done
Trusted sites

Email Exploit Engine

| ID | Description | Last Updated | Status |
|---|---|---|---|
| 1 | CLS-ID File Extension (High alert) | 15/02/2002 00:00:00 | Enabled |
| 2 | Iframe within an HTML email (Suspicious) | 01/09/2005 14:03:00 | Enabled |
| 3 | Malformed File Extension (High alert) | 15/02/2002 00:00:00 | Enabled |
| 4 | Java ActiveX Component Exploit (High aler | 31/08/2005 07:25:26 | Enabled |
| 5 | Mime header vulnerability (High alert) | 15/02/2002 00:00:00 | Enabled |
| 6 | ASX buffer-overflow (High alert) | 31/08/2005 07:26:10 | Enabled |
| 7 | Document.Open method Exploits (Possible | 31/08/2005 07:26:48 | Enabled |
| 8 | Popup Object exploit (High alert) | 31/08/2005 07:33:58 | Enabled |
| 9 | Object CODEBASE file execution (High aler | 31/08/2005 07:35:24 | Enabled |

Exploit engine quarantines emails with OS application exploits


GFI MailSecurity - Microsoft Internet Explorer
Address http://master-domain.com/MailSecurity/default.aspx
GFiMailSecurity
SECURITY & MESSAGING SOFTWARE
Console Root
Quarantine
Today
Yesterday
This week
All items
Search Folders
Search
New search folder...
javascript:openLink('/MailSecurity/quarantine/user/quarantine.aspx?folderID=4d19e1fd-3740-49fd-b961-5bc5d2b8db9e');
Trusted sites

Use this page to perform quick searches and manage quarantined content in categories.

**Quick Search**

Please select and use the following fields to perform quarantine content search.

Search in sender/recipients:
Search in subject:
Search in quarantine reason:

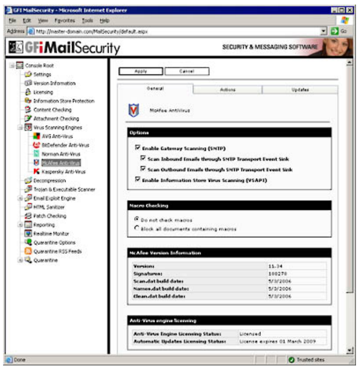
**Quarantined Items**

| Folder | Items |
|---|---|
| Today | 0 |
| Yesterday | 0 |
| This week | 0 |
| All items | 4 |

Current search folders:

| Folder | Items | Auto-purging |
|---|---|---|
| Blocked by Attachment Checking only | 1 | Items older than 7 day/s |

Quarantine Store


GFI MailSecurity - Microsoft Internet Explorer
Address http://master-domain.com/MailSecurity/default.aspx
GFiMailSecurity
SECURITY & MESSAGING SOFTWARE
Console Root
Virus Scanning Engines
McAfee Anti-Virus
Apply
Cancel
General
Actions
Updates
Done
Trusted sites

McAfee AntiVirus

**Options**

☑ Enable Gateway Scanning (SMTP)
☑ Scan Inbound Emails through SMTP Transport Event Sink
☑ Scan Outbound Emails through SMTP Transport Event Sink
☑ Enable Information Store Virus Scanning (VSAPI)

**Macro Checking**

● Do not check macros
○ Block all documents containing macros

**McAfee Version Information**

| | |
|---|---|
| Version: | 11.34 |
| Signatures: | 180278 |
| Scan.dat build date: | 5/3/2006 |
| Names.dat build date: | 5/3/2006 |
| Clean.dat build date: | 5/3/2006 |

**Anti-Virus engine licensing**

| | |
|---|---|
| Anti-Virus Engine Licensing Status: | Licensed |
| Automatic Updates Licensing Status: | License expires 01 March 2009 |

The McAfee anti-virus engine

### 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 or as a replacement to one of the other engines. Kaspersky Anti-Virus is ICSA-certified and is well known for the unsurpassed depth of its object scanning, the high rate at which new virus signatures are released and its unique heuristic technology that effectively neutralizes unknown viruses. 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.

### Automatic removal of HTML scripts

The advent of HTML email has made it possible for hackers/virus writers to trigger commands by embedding them in HTML email. GFI MailSecurity checks for script code in the email message body and disables these commands before sending the "cleaned" HTML email to the recipient. GFI MailSecurity is the only product to protect you from potentially malicious HTML email using a GFI patented process, safeguarding you from HTML viruses and attacks launched via HTML email.

### Email exploit detection engine

GFI's Email Exploit Engine builds on GFI's leading research on email exploits, and safeguards you from future email viruses and attacks that use known application or operating system exploits. For example, GFI MailSecurity would have protected you against the Nimda and Klez viruses when they first emerged without needing any updates, because these viruses use known exploits. GFI SecurityLabs regularly finds new email exploits, and these are automatically downloaded by GFI MailSecurity. GFI MailSecurity is the only email security product to detect email exploits.

### Spyware detection

GFI MailSecurity's Trojan & Executable Scanner 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.

### 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.

### 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.

### 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.

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

GFI MailSecurity provides several options for moderating quarantined email. 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 emails to an email address, enabling you to use a public folder to distribute the quarantined items to multiple administrators.

### 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.

### Full threat reporting for quarantined emails

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

### Server-based anti-spam

GFI MailSecurity's companion product, GFI MailEssentials for Exchange/SMTP offers spam protection at server level and eliminates the need to install and update anti-spam software on each desktop. GFI MailEssentials includes a number of effective methods to virtually eliminate spam from your network. It also provides disclaimers, Internet email reporting, server-based auto replies and POP3 downloading. GFI MailEssentials integrates seamlessly with GFI MailSecurity and both are available as a suite.

### Other features:

- Automatic quarantining of Microsoft Office documents with macros
- Detects attachment extension hiding & renaming
- User-based, flexible rules configuration
- Scans embedded emails
- Lexical analysis.

### You're in good company...

Many leading companies have chosen GFI MailSecurity for Exchange/SMTP. Here are just a few: NASA, European Central Bank, MG Rover Group, Caterpillar, PerotSystems, Port Of Tilbury London Ltd, Mexx International BV (Netherlands) and many more.

## Reviews

**GFI MailSecurity continues to meet Checkmark standards** - 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 which are continuously being developed to ensure that they are an accurate reflection of real-world situations and changing technology advances.

*- West Coast Labs, April 2005*

**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*

## 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, 4, 5 or 5.5, Lotus Notes 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 1.1/2.0.
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – SMTP service & World Wide Web service.
- Microsoft Data Access Components (MDAC) 2.8.

**Download your evaluation version from http://www.gfi.com/mailsecurity/**

GFI Software
Unit 2, St. John's Mews
St. John's Rd, Hampton Wick
Kingston-upon-Thames
Surrey KT1 4AN, 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 Software
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 40 3068 1000
Fax +49(0) 700 3068 1010
sales@gfisoftware.de

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 05 Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft GOLD CERTIFIED Partner

www.gfi.com