

"Highest Performance  
Lowest Price"

**Microsoft**  
**GOLD CERTIFIED**  
Partner

# GFI MailSecurity

Leading email security for Exchange/SMTP/Lotus

- **No. 1** multiple AV email security product
- Over **30,000** customers
- Unbeatable pricing
- Outstanding security performance

## The leading SMB email security product with up to five virus scanners

The ever-increasing volume of viruses and other malware serves to highlight how important it is for companies to have adequate anti-virus and email exploit protection on their network. Such is the range of virus variants appearing daily, products that use a single anti-virus engine to scan inbound email do not provide sufficient protection at either server or desktop level. What you do need to protect the network from viruses is a product such as GFI MailSecurity that provides not one, but up to five anti-virus engines running on the email server.

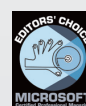
With multiple anti-virus engines you:

- Reduce the average time to obtain virus signatures which combat the latest threats
- Take advantage of all their strengths because no single AV scanner is the best
- Virtually eliminate the chances of an infection
- Get a product that is cheaper than any single AV engine solution.

### 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 or as a replacement to one of the other engines.

## Trojan and executable analyzer

The GFI MailSecurity Trojan & Executable analyzer detects unknown malicious executables (for example, trojans) by analyzing what an executable does.

## 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.

## 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.

## GFI MailSecurity ReportPack

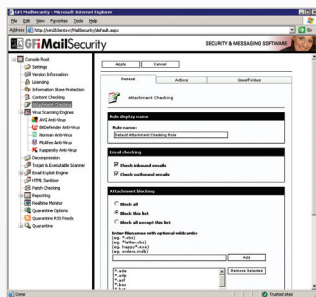
From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI MailSecurity ReportPack provides you with the easy-to-view information you need to fully understand your email security patterns.

## 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.

## Other features:

- Custom quarantine filters
- Enable easy quarantine folder monitoring through RSS feeds
- Web-based configuration – enables remote management from any location
- Approve/reject quarantined email using the moderator client, email client or web-based moderator
- Full threat reporting for quarantined emails
- Searching within quarantined emails



Configure attachment checking



GFI MailSecurity configuration

## System requirements

- Windows 2000 Server/Advanced Server (Service Pack 1 or higher) or Windows 2003 Server/Advanced Server or Windows XP.
- 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 1.1/2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) – SMTP service & World Wide Web service.
- Microsoft Data Access Components (MDAC) 2.8.



For more information and to download your evaluation version please visit <http://www.gfi.com/mailsecurity/>

In association with:



Concentrix Limited

20 Granite Way, Mountsorrel  
Loughborough, LE12 7TZ  
UK

tel: +44 (0)1509 410500

email: [info@concentrix.co.uk](mailto:info@concentrix.co.uk)

url: [www.concentrix.co.uk](http://www.concentrix.co.uk)