ONE PRODUCT. FIVE DEFENDERS.
FIVE ANTIVIRUS ENGINES. ONE CHOICE.

ENHANCE YOUR EMAIL DEFENSES
TODAY WITH GFI MAILSECURITY

Multiple AV email security product

Thousands of customers

Excellent pricing

Outstanding security performance

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 antivirus and email exploit protection on their network. Such is the range of virus variants appearing daily that products which use a single antivirus 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 antivirus engines running on the email server.

With multiple antivirus engines you:

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

BENEFITS

- Support for most industry leading messaging platforms including Microsoft Exchange 2000, 2003, 2007, 2010 and Lotus Domino
- Multiple antivirus engines guarantee higher detection rate and faster response
- Trojan and Executable Scanner detects malicious executables without need for virus updates
- Email exploit engine and HTML sanitizer disable email exploits and HTML scripts.

GFI MailSecurity™

Email security for Exchange Server/SMTP/Lotus

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 over 30 times running. The Norman Sandbox analyzes the behavior of suspicious files in cases where signature-based analysis falls short. BitDefender is a very fast and flexible award-winning antivirus engine that can recognize and scan a strikingly wide range of formats. 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 (optional)

To achieve even greater security, users can add the Kaspersky, McAfee and/or AVG antivirus engines as a third, fourth or fifth antivirus engine or as a replacement to one of the other engines. AVG also gives you the option of using LinkScanner to analyze suspicious hyperlinks in email bodies.

Trojan and executable analyzer

GFI MailSecurity's trojan and executable scanner detects unknown malicious executables (for example, trojans) by analyzing what an executable does.

Spyware detection

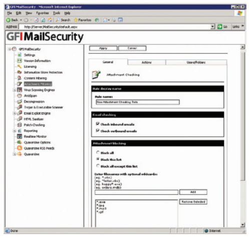
GFI MailSecurity's trojan and executable analyzer can recognize malicious files including spyware and adware. GFI MailSecurity can also detect spyware transmitted by email via the Kaspersky virus engine (optional) which incorporates a dedicated spyware and adware definition file that has an extensive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

Attachment checking

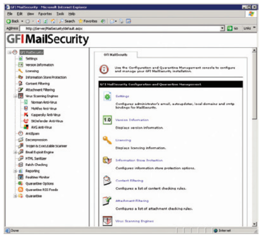
GFI MailSecurity's attachment checking rules enable administrators to quarantine attachments based on user and file type. For example, all executable attachments can be quarantined for administrator review before they are distributed to the user. GFI MailSecurity can also scan for information leaks, 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.



Configure attachment checking



GFI MailSecurity configuration

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:

- Full scan of internal emails
- Custom quarantine filters
- Norman AV Sandbox and optional AVG LinkScanner provide outstanding malware detection
- Dashboard
- 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
- Email exploit detection engine
- Automatic removal of HTML scripts.

KASPERSKY ANTI-VIRUS

bitdefender secure your every bit

McAfee®

AVG Internet Security

NORMAN®

System requirements

- Windows 2003 Server/Advanced Server, Windows XP, Windows Server 2008
- Microsoft Exchange Server 2010, 2007, 2003, 2000 (SP1), 5.5, 4.5, Lotus Domino 4 and up, or any SMTP/POP3 mail server
- Microsoft .NET Framework 2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) – SMTP service and World Wide Web service
- Microsoft Data Access Components (MDAC) 2.8.

Download your free trial from http://www.gfi.com/mailsecurity

Microsoft GOLD CERTIFIED Partner

GFI MailSecurity™

Email security for Exchange Server/SMTP/Lotus

Contact us

Malta	**UK**	**USA**	**Asia Pacific - South Australia**
Tel: +356 2205 2000	Tel: + 44 (0)870 770 5370	Tel: +1 (888) 243-4329	Tel: +61 8 8273 3000
Fax: +356 2138 2419	Fax: + 44 (0)870 770 5377	Fax: +1 (919) 379-3402	Fax: +61 8 8273 3099
sales@gfi.com	sales@gfi.co.uk	ussales@gfi.com	sales@gfiap.com

For more GFI offices please visit http://www.gfi.com/company/contact.html

GFI® www.gfi.com