



# GFI MailDefense Suite

for Exchange/SMTP/Lotus

Comprehensive anti-virus, anti-spam and anti-phishing protection for SMBs

Email is a primary means of communication but it is also used to commit fraud, sell fake goods, steal identities and cause damage to networks. Dealing with the huge amount of junk email hitting mail servers and email threats such as viruses and malware can be a nightmare.

An effective but low cost way to do so would be to install the GFI MailDefense Suite. This is a powerful package comprising two market leading GFI products that together filter and clean all inbound email for spam, viruses, malware and many other threats. With over 80,000 and 30,000 customers respectively, GFI MailEssentials, the no.1, award-winning anti-spam software, and GFI MailSecurity, the leading multiple anti-virus engine solution for SMBs, will put your mind at rest that your inbound email is rendered safe of malware and free of spam before end-users receive it.

The GFI MailDefense Suite makes use of multiple technologies – such as Bayesian filtering to remove spam and up to five anti-virus engines to detect viruses – to achieve this. It is very easy to install and configure while it ships at a price that is the lowest on the market. If you are looking for a holistic way to handle spam and viruses, then the GFI MailDefense Suite is the right tool, at the right price, for you.

**Features: GFI MailEssentials – Anti-spam, anti-phishing and email management**

## ■ Server-based anti-spam and anti-phishing

GFI MailEssentials is server-based and installs on the mail server or at the Gateway, eliminating the deployment and administration hassle of desktop-based anti-spam and anti-phishing products. Desktop-based software involves training your users to create anti-spam rule sets, and subsequently users have to spend time updating these rules. Besides, this system does not prevent your server message stores from filling up with spam.

## Benefits

### Why choose GFI MailDefense Suite to enhance your company's email security?

- 80,000 customers use #1 server anti-spam software by GFI
- Dozens of awards for GFI MailEssentials and GFI MailSecurity
- Highest spam detection rate (over 98%) and ultra low rate of false positives
- Leading multiple anti-virus software and content management functionality
- Up to five anti-virus engines providing comprehensive email security
- Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003, 2007 and Lotus Domino

## ■ Bayesian filtering technology

Bayesian filtering is widely acknowledged by leading experts and publications as the best way to catch spam. A Bayesian filter uses a mathematical approach based on known spam and ham (valid email). This gives it a tremendous advantage over other spam solutions that just check for keywords or rely on downloading signatures of known spam. GFI's Bayesian filter uses an advanced mathematical formula and a dataset which is 'custom-created' for your installation: The spam data is continuously updated by GFI and is automatically downloaded by GFI MailEssentials, whereas the ham data is automatically collected from your own outbound mail. This means that the Bayesian filter is constantly learning new spam tricks, and spammers cannot circumvent the dataset used. This results in a 98+% spam detection rate, after the required two-week learning period. In short, Bayesian filtering has the following advantages:

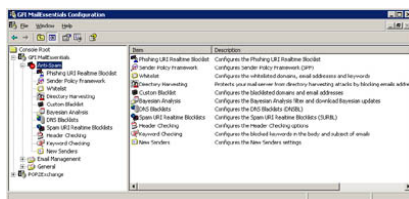
- Looks at the whole spam message, not just keywords or known spam signatures
- Learns from your outbound email (ham) and therefore greatly reduces false positives
- Adapts itself over time by learning about new spam and new valid email
- Dataset is unique to your company, making it impossible to bypass
- Multilingual and international.

## GFI MailDefense Suite



Centralized console for GFI mail products management

## GFI MailEssentials

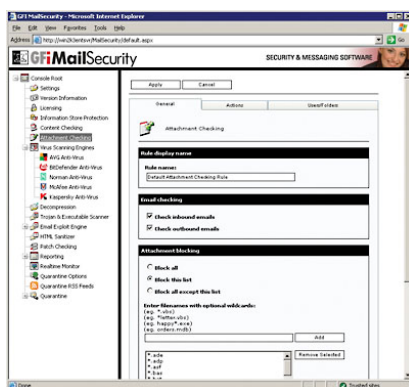


GFI MailEssentials configuration

## GFI MailSecurity



GFI MailSecurity configuration



Configure attachment checking

## Eliminate hard to catch image, PDF, Excel, ZIP and NDR spam

With spammers controlling tens of thousands of zombie machines, these large botnet armies have become one of the leading sources of spam. The Botnet/Zombie check in GFI MailEssentials eliminates hard to catch attachment spam such as image spam, PDF spam, Excel and ZIP spam. The attachment spam check filters this attachment spam quickly, efficiently and with a very low rate of false-positives. GFI MailEssentials uses a variety of technologies such as uses Bayesian Filter, DNS Blacklists, Sender URI RealTime Blocklists and Keyword Checking to keep Non-Delivery Report (NDR) spam at bay. Click here to read more about attachment spam or click here to learn more about NDR spam!

## Protect your users against the menace of phishing emails

GFI MailEssentials' anti-phishing module detects and blocks threats posed by phishing emails by comparing the content of the scam with a constantly updated database of blacklisted mails, thereby ensuring all the latest phishing emails are captured. As extra protection, it also looks for typical phishing keywords in every email sent to your organization.

## Sort spam to users' junk mail folders

GFI MailEssentials gives you the flexibility to choose what to do with spam. You can delete it, move it to a folder, forward the spam mail to a public email address or folder, or send it to individual customizable folders (for example, a "junk mail" folder) in the end-users' inboxes. This allows users to easily review mail that has been flagged as spam.

## List server for newsletter lists and discussion lists

A list server is the best method for distributing company newsletters, since it automates the process of allowing users to subscribe and unsubscribe (required by anti-spam regulations). However, until now, list servers have been expensive and difficult to administer and they did not integrate with Exchange Server. GFI MailEssentials integrates with Exchange and can use Microsoft Access or Microsoft SQL Server as the backend. Both newsletter lists and discussion lists are supported.

## Company-wide disclaimer/footer/header text

GFI MailEssentials enables you to add disclaimers to the top or bottom of an email. Text and HTML formats are supported. You can include fields/variables to personalize the disclaimer. You can also create multiple disclaimers and associate them with a user, group or domain.

**Features: GFI MailSecurity – Email anti-virus, content policies, exploit detection and anti-trojan**

## Virus checking with multiple anti-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.

## 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.

## ■ 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. Click here for pricing!

## ■ 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.

## System requirements

- Windows 2000 Server/Advanced Server (Service Pack 1 or higher) or Windows 2003 Server/Advanced Server or Windows XP, Windows Server 2008
- Microsoft Exchange server 2000 (SP1), 2003, 2007, 4, 5 or 5.5, Lotus Domino, or any SMTP/POP3 mail server
- When using Small Business Server, ensure you have installed SP2 for Exchange Server 2000 and SP1 for Exchange Server 2003
- Microsoft .NET Framework 2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS5) – World Wide Web service & SMTP service installed and running as an SMTP relay to your mail server
- Microsoft Data Access Components (MDAC) 2.8.

## Awards



Download your evaluation version from <http://www.gfi.com/maildefense/>

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 Pty Ltd  
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 2205 2000  
Fax +356 2138 2419  
sales@gfi.com

Microsoft  
GOLD CERTIFIED  
Partner

GFI  
www.gfi.com