



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 products and services 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 and 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 of 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 with two anti-spam engines, 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 out-of-the-box filtering with the Spam Razer filtering, IP reputation and Bayesian filtering to remove spam and up to five anti-virus engines to detect viruses and malware – to achieve this. It is very easy to install and configure while it ships at a on the best price in the market. If you are looking for a comprehensive way to deal with spam and viruses, then the GFI MailDefense Suite is the right tool, at the right price, for you.

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

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

■ SpamRazer: An additional anti-spam engine

The latest version of GFI MailEssentials includes a new, second anti-spam engine, SpamRazer, which provides a second layer of protection. It has been designed to be very simple to use and due to frequent updates, SpamRazer will require no tweaking or training for it to be fully effective whilst filtering the latest spam attacks such as NDR spam, CNN spam, MSNBC spam and many more. Not only will administrators benefit from out-of-the-box filtering but they will not need to tweak GFI MailEssentials each time a new attack is out. With SpamRazer filtering, IP reputation filtering, Bayesian and other advanced anti-spam technologies, the spam capture rate is well over 98%. GFI MailEssentials has a market-leading low rate of false positives thereby ensuring that good and important emails are not deleted.

■ Precise real time dashboard

GFI MailEssentials also ships with a precise, real-time dashboard that gives administrators a graphical view of the software's status and as well as the server's email flow. Components shown on the dashboard are the status of key services provided by GFI MailEssentials, statistics of email flow and blocked spam and also POP2Exchange logging.

■ Improved performance

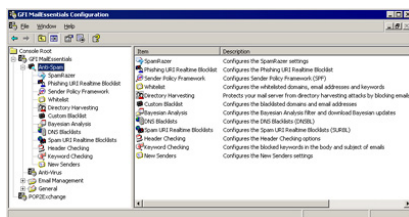
GFI MailEssentials hooks into Exchange server at the SMTP protocol level and the Exchange server does not need to download all the email before the software can determine whether an email is spam or a genuine message. This feature saves bandwidth and processing power.

GFI MailDefense Suite

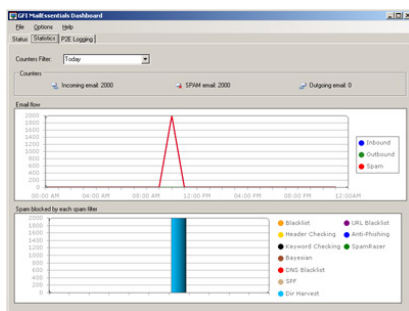


Centralized console for GFI mail products management

GFI MailEssentials



GFI MailEssentials anti-spam filters

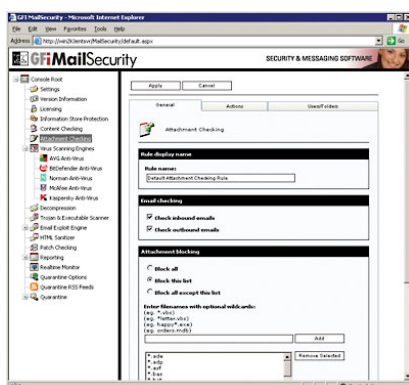


GFI MailEssentials dashboard – statistics tab

GFI MailSecurity



GFI MailSecurity configuration



Configure attachment checking

Inbuilt spam reporting

Administrators can now use GFI MailEssentials's reporting function to send a daily report to the users within the organization that shows how many emails were received by that individual and how many emails are identified as spam and filtered. This snapshot of email traffic shows the end-user how effective the anti-spam engine is and that the bulk of spam sent to him or her was successfully captured. The report also gives a full list of those emails identified and filtered as spam.

Eliminate hard to catch NDR, MSNBC and CNN 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 two anti-spam filter engines and a variety of technologies such as Bayesian Filtering and IP reputation filtering to keep Non-Delivery Report (NDR), CNN spam, MSNBC spam and many more at bay. or

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.

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