

GFI Software product comparison

GFI MailEssentials & GFI MailSecurity vs **Trend Micro ScanMail Suite for Microsoft Exchange**



	GFI MailEssentials & GFI MailSecurity	Trend Micro ScanMail Suite for Microsoft Exchange
Exchange Server 2000/2003 Integration	✓	✓
Exchange Server 2007 Integration	✓	✓
Option to run as a separate gateway	✓	✓
Superior protection through multiple anti-virus engines	✓	✗
Anti-virus engines used	Norman, BitDefender, Kaspersky*, AVG*, McAfee*	Trend Micro
Detects malware, spyware and greyware	✓	✓
Self-learning Bayesian anti-spam technology	✓	✗
Protection against Directory Harvesting attacks	✓	✗**
Sender Policy Framework (SPF) anti-spam technology	✓	✗**
Cleanses HTML emails from harmful scripts	✓	✓
Protection against email phishing attacks	✓	✓
Uses multiple Spam URI Real-time Block List (SURBL) servers as an additional anti-spam technology	✓	✗**
Uses multiple Spam DNS Real-time blacklist (DNSBL) servers as an additional anti-spam technology	✓	✗**
Technology to protect the mail server against Denial of Service (DoS) attacks	✓	✗*
Active Directory integrated content policies	✓	✓
Outbound email auto whitelisting	✓	✓
Detects attachments by file type	✓	✓
User can classify emails as spam/good emails	✓	✗

* Available at an extra cost

* Available at an extra cost in TrendMicro Control Manager

** Available at an extra cost in TrendMicro InterScan Messaging Suite

Who we are

GFI is a market leader in security software, offering high performance solutions at unbeatable prices to small and medium sized businesses.

Products like GFI MailEssentials, the leading spam filter product on the market, has over 80,000 customers; GFI MailSecurity was the first to apply multiple anti-virus engines to combat viruses; while GFI WebMonitor is the no. 1 web filter for Microsoft ISA Server. GFI FAXmaker remains the best fax server solution around.

GFI leads the way in the SMB sphere, combining price, quality and innovative technology in all products.

The GFI difference

- 80,000 satisfied customers
- Unbeatable price-performance
- Over 60 awards
- More than 98% spam capture rate because of its Bayesian filtering technology
- Lowest false positives through various technologies focused at eliminating false positives
- Server-based install, no client software required
- Support for leading message platforms including Microsoft Exchange Server 2007

GFI Software product comparison

GFI MailEssentials & GFI MailSecurity vs *Trend Micro ScanMail Suite for Microsoft Exchange*



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.

Read more about Bayesian filtering here: <http://www.gfi.com/whitepapers/why-bayesian-filtering.pdf>

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 and so on.

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.

Read more about why one anti virus engine is not enough here:

<http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf>

Anti False Positives technology

GFI MailEssentials includes various technologies focused at eliminating false positives. When GFI MailEssentials was developed particular attention was given to the false positive issue as opposed to focusing only on spam detection. The automatic white list management tool automatically adds outgoing mail recipients to your white list. This greatly reduces false positives, without any need for additional administration. White lists can also be built based on domain names, email addresses and keywords.

GFI Software product comparison



GFI MailEssentials & GFI MailSecurity vs Trend Micro ScanMail Suite for Microsoft Exchange

Eliminate hard to catch image, PDF, Excel and ZIP 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 anti-spam 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

SURBL and PURBL

GFI MailEssentials checks email content against Spam URI Real-time Blocklist (SURBL) servers. Administrators can configure multiple SURBL servers, add their own and also define the priority of which server should be checked first. More information on SURBL can be found at <http://www.surbl.org>. The Phishing URI Realtime Blocklist (PURBL) feature of GFI MailEssentials detects phishing emails by comparing URIs present in the email to a database of URIs that are known to be used in phishing attacks, and also by looking for typical phishing keywords in the URIs.

Powerful reporting

The GFI MailSecurity ReportPack is a full-fledged reporting companion to GFI MailSecurity. 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. Full automation and custom scheduling allow you true install-and-forget functionality! The GFI MailSecurity ReportPack offers several default and customizable reports that can be prepared on an hourly, daily, weekly or monthly basis including:

- Viruses blocked
- Inbound email traffic
- Outbound email traffic
- Total inbound and outbound email traffic
- Processed emails
- Blocked emails

GFI Software product comparison



GFI MailEssentials & GFI MailSecurity vs Trend Micro ScanMail Suite for Microsoft Exchange

GFI MailSecurity makes use of multiple anti-virus engines

Is multiple anti-virus engine scanning better than single anti-virus engine scanning?

GFI MailSecurity can use up to five anti-virus engines namely, Norman, BitDefender, Kaspersky, McAfee, and AVG. Using multiple anti-virus engines ensures that at least one of the engines is updated and can detect the latest viruses. Each engine has its own unique technology and methods. Thus, multiple anti-virus engine scanning ensures better protection.

Symantec, on the other hand, uses just a single anti-virus scanning engine which means its virus protection feature may not be as effective as GFI in responding to latest threats at all times.

GFI MailSecurity comes bundled with Norman and BitDefender anti-virus engines

Do I need to buy the anti-virus engines separately?

Norman and BitDefender anti-virus engines are included in the base GFI MailSecurity product and the user is not required to buy these separately. Both these engines are ICSA certified and have won the 100% Virus Bulletin award. Also, GFI MailSecurity updates Norman and BitDefender definition files automatically as and when they become available.

GFI MailSecurity prevents Directory Harvesting attacks

How is Directory Harvesting attacks prevention useful to me?

Directory Harvesting is another technique used by spammers. Spammers often try to guess recipient addresses by generating multiple random email addresses at a domain; they then send their spam mail to all those addresses.

GFI MailEssentials checks the validity of ALL the email addresses included in the mail sent, either via a query to Active Directory or through support for LDAP, and if addresses are not valid, the email is marked as spam.

GFI MailSecurity provides RSS feeds for quarantined emails

How simple it is to track quarantine emails?

It is much easier to track all the quarantine emails by using GFI MailSecurity. It allows the administrator to subscribe to RSS (Really Simple Syndication) feeds of quarantined emails. For instance, if an email addressed to the CEO is quarantined, the administrator gets notified about it by a pop-up. Trend Micro notifies the administrator only through an email or pager.

GFI is focused on the SMB Segment

A "focused" approach is better than "one size fits all"

GFI has designed its products keeping in view the requirements of Small and Medium Businesses (SMB). GFI products (GFI MailEssentials and GFI MailSecurity) are focused and offer a comprehensive package for the SMB market. This focus has helped SMBs by providing specific features and the best possible tools at the best possible price in order to better manage their emailing infrastructure. On the other hand, Trend Micro tries to cater to all the market segments and as a result it does not cater to all the needs of any particular segment.

