

GFI Software product comparison

GFI MailEssentials & GFI MailSecurity vs Symantec Brightmail 6 & Anti Virus



	GFI MailEssentials & GFI MailSecurity	Brightmail 6.0 & AV
Supports Microsoft Exchange Server 2000/2003	✓	✓
Supports Microsoft Exchange Server 2007	✓	✗
Option to run as a separate gateway	✓	✓
Superior protection through multiple anti-virus engines	✓	✗
Runs on same server as mail server	✓	Not recommended
Anti-virus engines used	Norman, BitDefender, Kaspersky*, AVG*, McAfee*	Symantec
Detects spyware and adware	✓	✗
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	✓	✓
Automatic white list management	✓	✗
Detects attachments by file type	✓	✓
Technology to detect custom-made trojans	✓	✓
User based black lists	✗	✓
Spam capture rate	98%	95%

* Available at an extra cost

Testimonials

The support you have provided has been excellent, and your firm should consider it to be viewed truly as "an industry standard".

Dave Spencer
Network Administrator,
Century Foods International
Sparta, WI, USA

I only have the highest praise and accolades for GFI and their products. They have returned time and efficiency to our company.

Justin Lenkey
Systems Administrator,
GB Manufacturing Co.
Delta, Ohio, USA

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 Symantec Brightmail 6 & Anti Virus

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>

Price comparison at a glance

Total Cost of Ownership for one year (per user)	Number of users							
	10	25	50	75	100	150	200	250
GFI MailSecurity & GFI MailEssentials	\$25.76	\$21.28	\$18.22	\$17.09	\$15.83	\$14.04	\$14.04	\$14.04
Symantec Brightmail AntiSpam & Anti Virus	\$41.40	\$34.20	\$31.50	\$31.50	\$28.80	\$28.80	\$28.80	\$24.30

GFI Software product comparison



GFI MailEssentials & GFI MailSecurity vs Symantec Brightmail 6 & Anti Virus

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.

Symantec Brightmail Antispam 6 & Anti Virus contains ONLY 1 anti-virus engine

GFI MailSecurity comes with a Trojan & Executable Scanner

What is the need for a specialized Trojan & Executable scanner?

Trojan and other executable codes can be a serious threat to organizations as these give unrestricted access to the user's data. GFI uses the Trojan & Executable Scanner to detect if the executable is capable of performing any suspicious activity that can be harmful to the user's data and the organization.

Symantec Brightmail Antispam 6 & Anti Virus does not provide a separate Trojan and executable scanner

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 email 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.

Symantec does not provide protection against Directory Harvesting attacks

GFI MailSecurity can automatically sanitize HTML from embedded commands

Can HTML emails be cleaned of embedded malicious code?

The advent of HTML email has made it possible for hackers and virus writers to trigger commands by embedding them in HTML email and to plant HTML beacons in order to generate more spam. 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.

Symantec does not provide HTML sanitization from embedded commands

GFI Software product comparison



GFI MailEssentials & GFI MailSecurity vs Symantec Brightmail 6 & Anti Virus

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 whitelist management tool automatically adds outgoing mail recipients to your white list. This greatly reduces false positives, without any need for additional administration. Whitelists can also be built based on domain names, email addresses and keywords.

Sender Policy Framework

GFI MailEssentials is one of the first commercial anti-spam solutions to support the Sender Policy Framework. Because most of today's spammers' spoof email addresses, it is important to be able to check whether an email is genuine or if it has been sent from a forged sending address. The SPF module automatically checks whether the mail from a particular company was actually sent by its registered mail servers. For more on SPF, visit: <http://www.openspf.org>.

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.

Support for Microsoft Exchange 2007

GFI MailEssentials provides seamless integration with Microsoft Exchange Server 2007 in addition to previous versions. You can rest assured that GFI stays up-to-date with current releases of industry leading messaging platforms.

