GFI product comparison:
GFI MailEssentials®
vs.
ESET Mail Security for Microsoft® Exchange Server

GFI *Mail*Essentials®

Web filtering functionality

Features	GFI MailEssentials	ESET Mail Security for Microsoft® Exchange Server
Integrates with Microsoft® Exchange Server 2003/2007/2010/2013	✓	✓
Scans incoming and outgoing emails	✓	✓
Spam capture rate	99%+	99%+
Scans internal emails within Exchange Server	✓	✓
Remote AD support	✓	✓
Multi Server Support	✓	✓
Centralized Quarantine	✓	✓
Centralized Reporting	✓	✓
Synchronized Configuration	✓	✓
Automatic product updates and patching	✓	✓
Number of antivirus engines available	5	1
Antivirus engines used	VIPRE, BitDefender, Kaspersky*, Avira*, McAfee*	ESET
Malware, spyware and greyware	✓	✓
Custom technology to detect email exploits	✓	✗
Protection against malicious HTML emails	✓	✗
Active Directory integrated content checking policies (user and group)	✓	✓
Attachment true file-type detector	✓	✓
Phishing protection	✓	✓
Sender Policy Framework (SPF)	✓	✓
Directory Harvesting with native Active Directory lookups	✓	✗
Bayesian analysis	✓	✓
Uses multiple Spam URI Real-time Blocklist (SURBL)	✓	✓
Uses multiple Spam DNS Real-time Blocklist (DNSBL) servers	✓	✓
Outbound email auto whitelisting	✓	✗

Users can classify emails as spam/good emails	✓	✗
Personal Blocklist/Whitelist	✓	✗
Virtualization	✓	✓

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

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

GFI MailEssentials earned the 'VBSpam+ Award' for its spam catch rate of 99.79%.
www.virusbtn.com

Multiple antivirus scanning engines

GFI MailEssentials 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 antivirus 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 at least one of your virus engines being quickly 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 antivirus engine is not enough here:
http://www.gfi.com/whitepapers/why-one-virus-engine-is-not-enough.pdf

GFI MailEssentials comes bundled with VIPRE and BitDefender antivirus engines

Do I need to buy the antivirus engines separately?

VIPRE and BitDefender antivirus engines are included in the base price of GFI MailEssentials and the user is not required to buy these separately. Both these engines are ICSA certified and have won the VB100 and AV-Comparatives awards. Also, GFI MailEssentials updates VIPRE and BitDefender definition files automatically, multiple times a day.

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 whitelist. 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 MailEssentials' SpamRazer technology determines if an email is spam by utilizing email reputation, bulk email detection, spamming technique detection and extensive content analysis; while Bayesian filtering uses a mathematical approach based on known spam and ham (legitimate email). Combining these technologies yields a spam detection rate of more than 99% and lowers the false positive rate.

GFI MailEssentials has been awarded the VBSpam+ with since it manages to achieve 0 false positives and a high spam detection rates of 99+%.

GFI MailSecurity comes with a Trojan and Executable Scanner

What is the need for a specialized Trojan and 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 and 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.

ESET Mail Security for Microsoft® Exchange Server does not provide a separate Trojan and executable scanner.

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.

GFI MailEssentials 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. ESET Mail Security for Microsoft® Exchange Server does not offer this feature.

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

GFI MailEssentials ships with full-fledged reporting capabilities. From trend reports for management (ROI) to daily drill-down reports for technical staff; GFI MailEssentials 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! GFI MailEssentials 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 inbound email traffic

- Processed emails

- Blocked emails

GFI provides you with extra value!

Do you need to use auto replies or maybe need to monitor emails?

Apart from anti-spam and antivirus, with GFI products you also get other email server related features that provide extra value:

- Log to MS SQL Server or (MS SQL Server Express)

- List Server (Newsletter and discussion)

- Auto-replies

- Email monitoring

There is no need to purchase extra software.

GFI®

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit http://www.gfi.com/contactus