Anti-spam for Exchange, anti-phishing and email management

Anti-spam software for Exchange/SMTP server

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to businesses every day, anti-spam software is a vital component of your network security strategy. Spam wastes network users’ time and network resources, and can also be dangerous. GFI MailEssentials offers anti-spam for Exchange server and other email servers and eliminates the need to install and update anti-spam software on each desktop.

GFI MailEssentials offers a fast set-up and a high spam detection rate using Bayesian filtering and other methods – no configuration required, very low false positives through its automatic whitelist, and the ability to automatically adapt to your email environment to constantly tune and improve spam detection. GFI MailEssentials will eliminate over 98% of the spam from your network! GFI MailEssentials also detects and blocks phishing emails through a system of Uniform Resource Identifier (URI) and keyword checks. In addition to anti-spam filtering and anti-phishing protection, GFI MailEssentials also adds email management tools to your mail server: disclaimers, mail monitoring, Internet mail reporting, list server, server-based auto replies and POP3 downloading.

GFI MailEssentials awarded Checkmark Premium Certification (Dec 06)

- 98% spam detection rate!
- 100% valid email identification rate!

Get your FREE 30-day eval version of GFI MailEssentials today!

Highest spam detection rate (98%) because of its Bayesian filtering technology
Lowest false positives through its patent pending auto whitelist feature
Server-based install, no client software required
Allows users to review email marked as spam from junk mail folder
#1 server anti-spam solution at unbeatable pricing – over 60,000 installations!
GFI MailEssentials for Exchange/SMTP – Features

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.

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.

Downloads updates to spam profile database
GFI MailEssentials can download updates to the Bayesian spam profile database from the GFI site, ensuring that it recognizes the latest spam and spamming techniques. GFI maintains the spam profile database by working with a number of spam collection organizations that continually supply spam samples.

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.

**Easy tuning of the Bayesian engine via public folders**
Administrators can easily tune the Bayesian engine by dragging and dropping spam or ham to the appropriate public folder. GFI MailEssentials learns from the spam and ham that it picks up from these folders and further improves its spam detection rate. Administrators can control access to this feature through the use of Public Folder security.

**Allow users to whitelist or blacklist via public folders**
GFI MailEssentials allows users to whitelist or blacklist senders simply by dragging and dropping the appropriate mail to a public folder. This gives users more control and reduces administration. Administrators can control access to this feature through the use of Public Folder security.

**Email header analysis & keyword checking**
GFI MailEssentials intelligently analyzes the email header and identifies spam based on message field information. It detects forged headers, encoded IP's, spam mutation, spam sent from invalid domains, and more. It also enables you to configure keywords to check for spam using keyword checking.

**3rd party DNS blacklists (DNSBL) checking**
GFI MailEssentials supports DNS blacklists (real time black hole lists), which are databases of known spammers. If the sending mail server is on one of these lists, it marks the email as spam. GFI MailEssentials supports popular third party blacklists such as ORDB, SpamHaus, Spambase and also enables administrators to configure custom RBL servers.

**Support for multiple 3rd party SURBL servers**
GFI MailEssentials checks email content against 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.

**Automatic whitelist management reduces false positives**
Whitelist enable you to ensure that email from particular senders or domains are never flagged as spam, permitting more stringent anti-spam rules. GFI MailEssentials includes a patent-pending automatic whitelist management tool, which automatically adds outgoing mail recipients to your whitelist. This greatly reduces false positives, without any need for additional administration. Whitelists can also be built based on domain names, email addresses and keywords.

**Instant view of emails from new senders**
The New Senders feature provides users with an instant view of emails sent from people they never had previous contact with, thereby helping users to better organize emails in their email client. If an email is not found to be spam by the GFI MailEssentials anti-spam modules and is also not on the whitelist, then the New Senders module has the ability to move the email to a user's subfolder, for example, Inbox/NewSenders.

**Eliminates directory harvesting**
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 they are not all valid, marks the mail as spam.

**Reports on spam filtering and email usage**
The database-driven reporting engine allows you to create advanced reports on your inbound and outbound email. You can report on the amount of spam filtered and on rules which caught most spam. You can also generate reports on user, domain and mail server usage.

**Support for SPF - the Sender Policy Framework**
As 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. This can be done via the Sender Policy Framework (SPF), which allows users to test whether a particular email originates from its claimed source. GFI MailEssentials is one of the first commercial anti-spam solutions to support this framework. Its 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.

**Set priorities for each anti-spam module**
You can configure which method of capturing spam is to be given priority, and create your own hierarchical list. For example, the administrator can select that the whitelisting anti-spam feature must be applied first to all incoming mail, then Bayesian scanning, and so on.

**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.

**Email monitoring**
The email monitoring feature enables you to keep a central store of the email communications of a particular person or department. By configuring the email to be copied to an email address, all email can be stored in an Exchange or Outlook store, making searching for email or content easy.

**Email archiving to a SQL database**
GFI MailEssentials can archive all inbound and outbound mail to a Microsoft SQL Server database. You can search for a particular email or an entire email thread via the included web interface. Mail archiving is essential for back-up and search reasons.

**Seamless integration with Exchange Server 2000/2003 & 5.5**
GFI MailEssentials integrates seamlessly with Microsoft Exchange 2000/2003: It installs on the Exchange SMTP service and does not require gateway configuration. Via the SMTP protocol, it also works with Exchange 5.5, Lotus Notes and other popular SMTP/POP3 servers.

**NEW! – Checkmark certified**
GFI MailEssentials holds Checkmark certification from West Coast Labs and more awards.

**Content checking, anti-virus & anti-trojan**
Get anti-virus, email content checking and anti-trojan protection for your mail server with the GFI MailEssentials & GFI MailSecurity Suite. GFI MailSecurity for Exchange/SMTMP is an email content checking, exploit detection, threats analysis and anti-virus solution that removes all types of email-borne threats before they can affect your email users.

**Other features:**
- Whitelisting of emails by keyword
- Blocking foreign language spam based on character set
- Email monitoring of particular user or department email communications
- Fake non-delivery reports (NDRs)
- Personalized server-based auto replies with tracking number
- POP3 downloader
- Web interface for searching email archive.

**You're in good company...**
Many leading companies have chosen GFI MailEssentials. Here are just a few: Toyota, IBM, Schuff International, PerotSystems, British Midlands, B&W Speakers and many more.

**System requirements**
- Windows 2000/2003 - Pro, Server or Advanced Server or Windows XP Professional.
- IIS5 SMTP service installed and running as an SMTP relay to your mail server.
- Microsoft Exchange server 2000, 2003, 4, 5 or 5.5, Lotus Notes 4.5 and up, or an SMTP/POP3 mail server.
- For the list server feature, Microsoft Message Queueing Services is required.