

# GFI WHITE PAPER

## GFI Software's Email Security Solutions

### Overview

Through the recent acquisition of Katharion™, GFI Software now offers a hosted email filtering solution in conjunction with GFI MailEssentials™ and GFI MailSecurity™. GFI's hosted email filtering solution is available in two versions, which are detailed in this paper: GFI MAX MailEdge™ and GFI MAX Mail Protection™.



The first solution, **GFI MAX MailEdge™**, is designed to be used in combination with an existing on-premise anti-spam/antivirus solution, primarily GFI MailEssentials/GFI MailSecurity – although it can also be used as an add-on to any on-premise email security software or hardware product. GFI MAX MailEdge can block the most common types of spam before this junk mail reaches a customer's network, thus reducing the bandwidth and processing power required for incoming email, and effectively increasing the capacity of the installed GFI MailEssentials/GFI MailSecurity software. Equally important, GFI MAX MailEdge provides email continuity, whereby the service will automatically queue any legitimate inbound email messages that cannot be delivered, and allow customers to access and respond to those messages when the customer's email server is offline.

### **The benefits for customers**

#### **GFI MAX MailEdge**

Existing and new GFI customers will be able to take advantage of the following benefits by adding GFI MAX MailEdge.

- Through its IP reputation filters, connection throttling, directory harvesting protection, and optional greylisting, GFI MAX MailEdge can safely block up to 90% of all spam emails and email threats before they reach the customer's network.
- In addition to reducing the volume of incoming junk mail, GFI MAX MailEdge will also prevent denial of service (DOS) attacks, since a customer's mail server will only need to accept emails from the GFI MAX MailEdge service which will block most or all of those delivery attempts.
- Because GFI MAX MailEdge leverages multiple servers across distributed datacenters, it also provides customers with added security given the inherent scalability limitations and single point of failure of any on-premise solution dependent on a single server.
- In addition to these benefits, GFI MAX MailEdge provides customers with email continuity. If a customer's email server is offline due to scheduled maintenance or unexpected circumstances, GFI MAX MailEdge will continue receiving all inbound emails without interruption, and will relay them to the mail server once the server is online again. Throughout the period when the mail server is offline, users will be able to access and respond to their emails from any location via GFI MAX MailEdge's web-based interface.

GFI MAX MailEdge therefore perfectly complements GFI MailEssentials/GFI MailSecurity software installed on premise – providing the added reliability and scalability that a single software or hardware component cannot achieve, reducing the risk of a large spam run or denial of service attack, and offering continuity for an organization's email communications in the event of a technical problem or other emergency.

The second hosted email security solution, **GFI MAX MailProtection™** is a fully-fledged anti-spam and antivirus solution that requires no hardware, no software, and no maintenance on the customer's part. As a cloud-based service, GFI MAX MailProtection can be deployed in a matter of minutes from any location, and can be offered as a stand-alone solution or as part of a premium hybrid solution with on premise GFI MailEssentials/GFI MailSecurity software.



### **GFI MAX MailProtection**

GFI MAX MailProtection provides several key features and benefits in addition to those offered by GFI MAX MailEdge.

These include:

- "Zero-hour" antivirus protection
- Attachment and malware scanning
- Multi-layered spam detection
- Searchable individual hosted junk mail quarantines
- Daily spam digest messages for each end-user
- Configurable preferences for each user
- Message logging and search capabilities.

True to its software as a service (SaaS) nature, GFI MAX MailProtection works in any environment with any operating systems and mail infrastructure. Unlike an on-premise solution, the GFI MAX MailProtection service can also (in most cases) protect customers that host their mail externally.

GFI MAX MailProtection can be implemented as a replacement for an existing anti-spam/antivirus solution, or can be part of a premium hybrid solution in combination with the on-premise GFI MailEssentials/GFI MailSecurity software. This hybrid solution offers the best of both on-premise and service-based solutions, providing customers with defense in depth, extremely high accuracy in spam detection through multiple complementary technologies, robust virus protection with both zero-hour antivirus protection and up to five signature-based antivirus engines, local filtering of internal messages combined with multi-stage filtering of inbound and outbound messages, and email continuity to safeguard an organization's mission-critical communications.

### **The benefits for channel partners**

GFI channel partners can fully brand both the GFI MAX MailEdge and the GFI MAX MailProtection service. Unlike other solutions which offer partial branding, these services were designed from the ground up to support partner branding at all customer touch points. This includes the URL for the control panel, the graphics and color scheme used within the control panel, the neutral MX records used to activate the services, and even the message digest and statistics messages which are sent to end-users. This comprehensive approach allows partners to offer an OEM-style managed service offering to their customers.

These services also allow partners to easily introduce their customers to software-as-a-service (SaaS) – a model that has significant appeal and that is seeing substantial growth.



The GFI cloud-based email security services are also an effective way for many partners to transition their own businesses from a reactive and/or labor-based business model to a service-oriented model that is more predictable, more scalable, and less dependent on human capital.

Last but not least, these GFI MAX services offer an attractive recurring revenue model for partners, with margins that increase as partners add customers.

**GFI MailEssentials and GFI MailSecurity are already blocking spam and malware for my organization. Why should I purchase GFI MAX MailEdge?**

GFI MAX MailEdge is useful in the following scenarios:

- You are using GFI MailEssentials and GFI MailSecurity, but you are wasting too much bandwidth due to a high volume of junk mail.
- Your organization receives a large volume of email traffic, most of which is spam, causing email queues to build up and potentially delaying email delivery because your current email infrastructure cannot cope with the volume of messages.
- You would like to ensure that no emails are lost when your mail server goes offline.
- You want users to be able to continue sending and receiving emails when your mail server goes offline.
- You want to mitigate the risk of Denial of Service (DOS) attacks or Distributed Denial of Service (DDOS) attacks on your email infrastructure.
- You would like to become familiar with the benefits of a fully hosted email security solution.
- You would like to have the benefits of a hosted solution, while continuing to scan internal emails in your Exchange Server.
- You would like to be able to manage the solution from any location via a web-based control panel.

**GFI MailEssentials and GFI MailSecurity are already blocking spam and malware for my organization. Why in addition to the reasons listed above should I purchase GFI MAX MailProtection?**

- You would like to move to a fully hosted email security solution.
- You would like to add an additional level of spam detection.
- You would like to minimize the bandwidth consumed by incoming junk mail.
- You would like to complement your existing signature-based antivirus protection with a zero-hour antivirus solution.



- You would like to use an externally hosted spam quarantine for each user.
- You would like to have each user receive a daily spam digest message.
- You would like to delegate some responsibilities of spam handling (setting the aggressiveness of the filter, maintaining whitelists or blacklists, review of quarantine/digests etc.), to end-users.
- You would like a solution that works regardless of your infrastructure – Apple, Linux/UNIX, Windows – and regardless of what mail server you use, now or in the future.
- You would like to offload the spam and virus filtering demands from your network and from your mail server.

### **I am buying GFI MAX MailEdge. Do I still need GFI MailEssentials and GFI MailSecurity?**

GFI MAX MailEdge performs various tests during the transmission of incoming email messages. Up to 90% of inbound junk mail messages can be safely blocked via these checks. However, GFI MAX MailEdge is not designed as a comprehensive spam and virus filter – it is designed as a first layer of defense against incoming email threats, and as a continuity solution in case of a problem with a customer's mail server or network. The remaining spam emails that are not blocked by GFI MAX MailEdge require additional tests related to the contents of each individual email message. That analysis is performed by GFI MailEssentials and GFI MailSecurity or comparative products.

Just as importantly, GFI MAX MailEdge does not provide any antivirus defense beyond the blocking or throttling of messages from disreputable source IP addresses. GFI MailSecurity can detect all malware emails, since it scans the message body and attachments using up to five virus scanning engines – providing a far greater level of assurance against email-borne threats.

### **Can you provide me a breakdown of the features provided by each solution?**

The following table illustrates better the features provided by each GFI solution:



Core Features	Software Solutions		Hosted Services Solutions	
	GFI MailSecurity	GFI MailEssentials	GFI MAX MailEdge	GFI MAX MailProtection
<b>Virus and threat detection</b>				
Inbound virus scanning	Up to 5 engines			Zero-hour AV
Outbound virus scanning	Up to 5 engines			Zero-hour AV
Malware scanning	✓			✓
Attachment blocking based on user and file type	✓			✓
Email exploit protection	✓			Q1 2010
Scanning of Microsoft Exchange information store	✓			
<b>Spam detection</b>				
DNS-based IP blacklists		✓		✓
DNS-based URI blacklists		✓		✓
Multi-layered inbound spam filtering		✓		✓
Multi-layered outbound spam filtering		✓		✓
Anti-phishing		✓		✓
NDR blocking		✓	✓	✓
<b>Network protection</b>				
Directory harvest attack prevention		✓	✓	✓
Denial of service protection	Limited	Limited	✓	✓
Connection throttling			✓	✓
Greylisting		Planned	✓	✓
Load balanced delivery with automatic failover			✓	✓



## GFI Software's Email Security Solutions

Core Features	Software Solutions		Hosted Services Solutions	
	GFI MailSecurity	GFI MailEssentials	GFI MAX MailEdge	GFI MAX MailProtection
Email continuity – inbound queue and on-demand mail service			✓	✓
<b>Administration</b>				
Multi-lingual control panel		✓	Q1 2010	Q1 2010
Attachment and content filtering	✓			Q1 2010
Multiple methods for account synchronization	✓	✓	✓	✓
Searchable individual quarantines		-		✓
Individual junk mail digests		Limited		✓
Individual whitelists/blacklists by sender, subject, and source IP		✓	✓	✓
Message logging and search		Limited		✓
Hierarchical management capabilities			✓	✓
Full partner branding of control panel			✓	✓
<b>Other features</b>				
Outbound disclaimers and signatures		✓		✓
Scanning and policy application for internal mail		✓		
Integrated list server		✓		
Archive of messages to SQL database		✓		



## GFI Software's Email Security Solutions

Core Features	Software Solutions		Hosted Services Solutions	
	GFI MailSecurity	GFI MailEssentials	GFI MAX MailEdge	GFI MAX MailProtection
Special handling of messages from new senders		✓		
Works in Windows, Linux/UNIX, and Apple environments			✓	✓

© 2010. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.