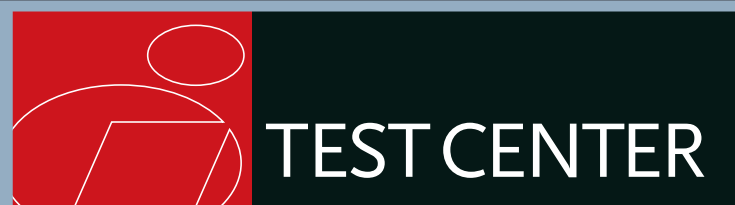


InfoWorld

June 16, 2003 ■ ISSUE 24

GET TECHNOLOGY RIGHT



SECURITY

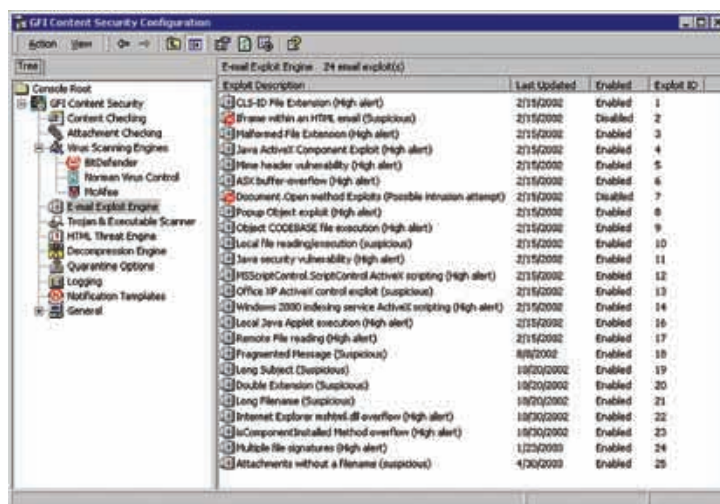
Return to Sender

Leading mail scanners rev their engines **BY DAN MORTON**

FIREWALLS are a good first line of network defense, but they typically don't inspect connections for malicious code. Because of this, scanning e-mail as it enters the network has become an enterprise must.

Companies have traditionally looked to server-based solutions to fulfill their e-mail anti-virus needs. Such solutions integrate with an existing mail server and inspect e-mail content as it passes through. Today, e-mail scanners that act as stand-alone gateways are also available, thereby offering enterprises the option of blocking incoming viruses before they even touch the mail server. I tested both types of anti-virus scanners in this roundup.

Although gateway solutions require additional hardware, they are easier to configure and they leave the mail server unfettered. Server-based products typically scan mailbox stores in addition to incoming and outgoing e-mail messages, thereby providing an extra layer of protection. Products that scan mail stores can catch viruses that slip



GFI MailSecurity for Exchange/SMTP was the only solution tested that scans for specific kinds of attacks on the mail server.

through the mail server before signatures are updated.

I tested solutions from GFI Software, Gordano, Network Associates, Sophos, Symantec, and Trend Micro, using the test virus developed by the European Institute for Computer Anti-Virus Research (EICAR) to mimic malicious code embedded in e-mail bodies, in uncompressed attachments, and in compressed attachments. The

EICAR test virus is harmless, so it wouldn't pose a risk if it escaped my test network, but it provided a good test of each virus scanner's detection capabilities.

All of the solutions in this roundup use a signature database to detect viruses. The scanning engine compares an e-mail file against the database, which is essentially a list of known viruses and their footprints. When a virus

is found, the program starts a treatment procedure. First, it attempts to remove the virus from the file. Failing this, the program quarantines the file or — if the administrator chooses — deletes the file, sending the administrator and the intended recipient an indication of what has happened.

All of these products are built on mature anti-virus scanning engines, so I wasn't surprised that each was capable of catching the simulated viruses I threw at it. Although all six products performed on par with one another in terms of identifying viruses, one ultimately provides stronger protection than the rest, due to its use of multiple scanning engines.

Multiple scanning engines improve the chances of detection, of course, because any given virus may be listed in one vendor's signature database but not in another's. GFI MailSecurity uses three separate scanning engines to identify viruses. The rest of the solutions I tested rely on only one.

Not that the other products don't offer extras. All of the server-based solutions perform scanning of mail stores. And nearly all of the six solutions tested provide the ability to configure rules for alerting administrators of outbreaks.

Early warnings of a virus outbreak — a high number of infected messages in a short amount of

time — can help administrators limit the damage by setting new policies on the firewall or mail server. An alert can typically take the form of an e-mail, an SNMP trap, a numeric page, or a Windows event log entry. Only Sophos MailMonitor lacked rules-based alerts.

GFI MailSecurity for Exchange/SMTP

GFI MailSecurity is a great, dual-purpose package that can be installed as an e-mail gateway or as a server-based solution. In my testing, GFI MailSecurity integrated easily with my existing Exchange system and provided excellent security.

MailSecurity's administration interface integrates well with the MMC (Microsoft Management Console) architecture. The monitoring application runs separately from the management console and provides critical information about the status of MailSecurity.

MailSecurity is equipped to use three scanning engines — BitDefender, Norman Virus Control, and McAfee — all of which were capable of detecting my test cases right out of the box. A quarantining feature allows you to isolate infected mail for analysis, and a rules-based engine allows you to

configure alerts for outbreaks. MailSecurity even includes a separate engine to scan for common e-mail exploits such as malicious JavaScript. I was very pleased with the high level of security offered by MailSecurity.

GMS Boundary Protection

GMS (Gordano Messaging Suite) is a complete e-mail solution that includes POP (Post Office Protocol), IMAP (Internet Message Access Protocol), and SMTP support. It also includes options for Web mail and IM. Because the anti-virus tools are integrated with the mail server — which takes over all relevant e-mail ports when installed — I found it difficult to integrate them into my existing Exchange system.

Installation did not go as smoothly with GMS as it did with other products. For GMS to work, SMTP service must be turned off and set to manual, but the installer failed to do this automatically. After I manually turned off the SMTP service, the installer still thought it was running. The installation worked in spite of this.

GMS is administered exclusively through a Web interface that requires Java, thereby ruling out palmtop administration.

GMS caught all of my test cases out of the box. Anti-virus is supported through Gordano's own anti-virus scanning engine. The product also features anti-spam, content-filtering tools. Overall, I found GMS' security features to be solid. As with some of the other products reviewed here, GMS includes outbreak alerts in addition to the standard disinfection and quarantine features.

MailMonitor for Exchange

Sophos' MailMonitor is a server-based scanner that provides tight integration with Exchange, allowing administrators to manage both the anti-virus solution and the mail server from the MMC. Although it proved perfectly capable of detecting viruses — catching all of my test viruses in its default configuration — MailMonitor lacks Web management tools and multiple scanning engines.

Installing MailMonitor is a multistep process, requiring you to install Sophos' Anti-Virus first. Thanks to reasonable default settings, however, I was able to get the package installed quickly. MailMonitor also requires the user to manually add the administration snap-in to the MMC list. This procedure is well documented in the supplied installation guide;

following these instructions, I had the server performing real-time scanning of incoming e-mail as well as scheduled scans of all mailboxes on the mail server with little more than a few clicks of the mouse.

MailMonitor's virus-handling capabilities don't go beyond the basics. Failing to disinfect a message, MailMonitor will quarantine the message for later review. The quarantine report lists the critical fields of quarantined e-mails (time, sender, recipient, subject, ID number) and allows the administrator to disinfect, delete, or deliver the message. Finally, a sample can be e-mailed to Sophos for further analysis.

McAfee WebShield SMTP

McAfee WebShield is an easy-to-install, easy-to-administer gateway solution for any SMTP mail server. I found that it handles security quite well, catching all my test viruses and providing extra security features such as content filtering and outbreak management.

Installation of WebShield went smoothly. Before finishing, the installer asks several questions, such as an estimate of daily message traffic, designed to tailor the solution to your security needs. I particularly liked the installer's scan of existing mail-server stores.

E-mail Anti-Virus Solutions

Although many solutions improve anti-virus protection through mail-store scanning and outbreak alerts, only GFI MailSecurity leverages multiple scanning engines.

	TYPE	NUMBER OF SCANNING ENGINES	MAIL-STORE SCANNING?	CONTENT/SPAM FILTERING	OUTBREAK MANAGEMENT	FREE AUTOMATIC UPDATES	MANAGEMENT INTERFACE	PRICE PER USER
GFI MailSecurity	Server/Gateway	3	Yes	Yes	Yes	Yes	Windows	\$6.99 for 500 users
GMS Boundary Protection	Server*	1	Yes	Yes	Yes	Yes	Web	\$11.92 for 1,000 users**
MailMonitor	Server	1	Yes	Yes	No	Yes	Windows	\$11.50 for 500 users
McAfee WebShield	Gateway	1	No	Yes	Yes	Yes	Windows	\$11.73 for 500 users
ScanMail	Server	1	Yes	Yes	Yes	Yes	Windows, Web	\$21.90 for 500 users
Symantec AntiVirus	Gateway	1	No	Yes	Yes	Yes	Web	\$11.60 for 500 users

* Solution installs its own mail server.

** Vendor does not sell 500-user license.

Although most viruses enter companies through their e-mail systems, this is by no means the only method of infection.

I was able to configure the program in very short order. For the most part, the default options were acceptable to the test network.

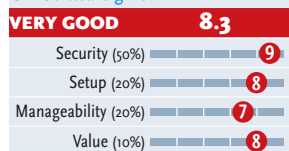
WebShield uses a Windows-based administration interface. Although the interface does not integrate with the MMC, it is nice to look at and is easy to use. Furthermore, the interface can be used to administer several different servers via the network. Although not as handy or secure as a Web interface, it does get the job done nicely.

WebShield was capable of identifying all of my test viruses in its default configuration. When an infected e-mail was caught, the product popped up a warning with pertinent information for the administrator. WebShield uses a single scanning engine to detect viruses. It also includes a feature for identifying virus outbreaks, allowing administrators to define a threshold number of

viruses within a given period of time before sending an administrative alert.

GFI MailSecurity for Exchange/SMTP 7.2

infoworld.com/reviews
GFI Software gfi.com



COST: \$6.99 per user for 500 users

PLATFORMS: Windows 2000 and XP

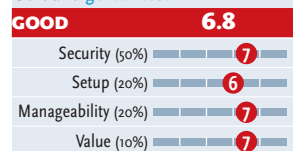
BOTTOM LINE: Multiple scanning engines and e-mail-exploit protection set GFI MailSecurity apart from the rest. Providing content filtering and outbreak management features, it's also easy to install and configure, and it can work as a gateway or integrated with the mail server. The only thing missing is a Web interface for remote management.

ScanMail for Exchange

Despite a dubious default setting to omit scans of message bodies, I

GMS Boundary Protection Version 9

infoworld.com/reviews
Gordano gordano.com



COST: \$11.92 per user for 1,000 users

PLATFORMS: Windows NT and later, Solaris, Linux, AIX.

BOTTOM LINE: GMS Boundary Protection is a complete mail solution in its own right. The anti-virus component is configured for the GMS mail server, making it difficult to integrate with existing SMTP servers. Nevertheless, anti-virus capabilities are solid, including outbreak alerts as well as disinfection and quarantine capabilities.

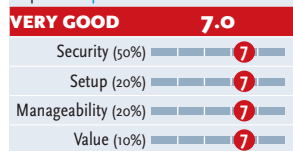
found Trend Micro's server-based ScanMail to be a good product for companies with multiple mail servers. Installation proceeded smoothly. ScanMail can install itself remotely on any number of servers via Windows administrative shares. The installer also runs a quick scan of the existing e-mail system to ensure that it is virus-free.

ScanMail has two separate administration interfaces: Windows- and Web-based. Both interfaces allow for the administration of several mail servers from one console. Although the Windows-based interface is faster, I found the Web-based interface to be easier to use.

ScanMail's security is on par with most competitors. It was the only product that did not detect all three test cases out of the box, but this was due to an ill-advised default setting. After I enabled message-body scanning, the

MailMonitor for Exchange 3.70

infoworld.com/reviews
Sophos sophos.com



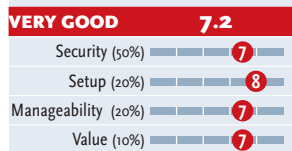
COST: \$11.50 per user for 500 users

PLATFORMS: Windows NT 4 and higher

BOTTOM LINE: MailMonitor is a solid, server-based anti-virus solution featuring an intuitive management interface and tight integration with Exchange. The addition of multiple scanning engines, outbreak alerts, and a Web interface would be welcome. But what MailMonitor lacks in cutting-edge features, it makes up for in maturity.

McAfee WebShield SMTP 4.5

infoworld.com/reviews
Network Associates mcafee.com



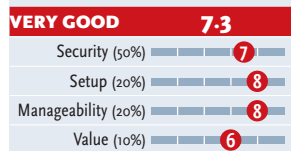
COST: \$11.73 per user for 500 users.

PLATFORMS: Windows NT 4 and later

BOTTOM LINE: A great server-based anti-virus solution for organizations using McAfee on client desktops, due to integrated client-server management. The setup routine and administration interface really shine on this product. However, the limitation of a single scanning engine and the lack of a Web management interface hold it back.

ScanMail for Exchange 6.1

infoworld.com/reviews
Trend Micro trendmicro.com



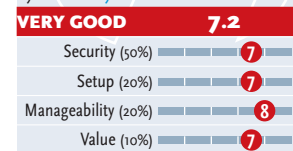
COST: \$21.90 per user for 500 users

PLATFORMS: Windows NT 3.51 and later

BOTTOM LINE: ScanMail is rich in security features, easy to set up and administer, and manageable by both Windows and Web clients, but it falls short in value, costing significantly more than competing solutions. By default, ScanMail does not scan the bodies of incoming e-mails; this ill-advised setting hampered its performance out-of-the-box.

Symantec AntiVirus for SMTP Gateways 3.1

infoworld.com/reviews
Symantec symantec.com



COST: \$11.60 per user for 500 users

PLATFORMS: Windows NT 4 and later, Solaris 7 and later

BOTTOM LINE: Symantec AntiVirus is a solid implementation of an e-mail gateway, but it's slightly hampered by a single scanning engine and the lack of built-in quarantining, which is available separately. Provides content-filtering and outbreak management features, and the Web interface allows management from anywhere on the Internet.

Overall, I was satisfied with all the products reviewed here... The inclusion of multiple scanning engines and the ability to act as either a server-side or gateway solution, however, are what earned GFI MailSecurity the top spot.

product was able to detect all my test viruses.

ScanMail also has an outbreak alert feature. When a certain number of viruses is detected within a certain amount of time, the system sends an alert to the administrator. I found the configuration for outbreak alerting to be both easy to use and powerful.

Symantec AntiVirus for SMTP Gateways

Even though it requires the purchase of an additional Symantec product to isolate infected messages for analysis, which limits the options for handling infected messages to repairing or deleting them, Symantec AntiVirus is a good gateway solution. I found that it integrated easily with my existing e-mail setup.

Symantec AntiVirus installed with a few minor glitches. Because it is a gateway product, it defaults to using the SMTP port. It would not install until I manually disabled the Windows SMTP server. Other than this, the defaults helped make installation easy.

For administration, Symantec AntiVirus supports both 128-bit secure and insecure Web interfaces without the use of Java. I found this to be particularly helpful for the on-the-go administrator because the product can be administered from a palmtop computer. Furthermore, the administrative interface is well laid-out, well-documented, and easy to use.

Symantec AntiVirus caught all my test cases out of the box. It also integrates anti-spam features into the package, providing a basic set of content-filtering tools. For outbreak management, the product can be configured to send an e-mail message to an administrator when a specific infected-message threshold has been reached.

Overall, I was satisfied with all the products reviewed here. The differences in score reflect the extra features and overall maturity of some products. Sophos' MailMonitor and Trend Micro's ScanMail are solid, yet basic, server-based e-mail anti-virus

solutions. Both Symantec AntiVirus and McAfee WebShield are great e-mail anti-virus gateway solutions. The Gordano product provides a complete e-mail anti-virus solution. The inclusion of multiple scanning engines and the ability to act as either a server-side or gateway solution, however, are what earned GFI MailSecurity the top spot.

Of course, any recommendation must be weighed against a corporation's existing anti-virus infrastructure. There are benefits to taking the single-vendor approach, and many of these vendors provide centralized management of their anti-virus solutions for e-mail servers, file servers, and client systems. If you're already using anti-virus products from one of these vendors, you should think strongly about how well a solution from another vendor would fit into the system.

Any recommendation must also be evaluated carefully for how it will fit into the corporate network. If your organization has an e-mail

server with excess capacity, and you would prefer to avoid reconfiguring the network, then a server-based solution makes the most sense. But if you're running an overloaded mail server and are willing to do some network reconfiguration, you would benefit from a gateway solution. Most shops could use some flexibility in this respect, and GFI MailSecurity deserves high marks for being configurable to run in either server or gateway mode.

Finally, keep in mind that even though most viruses enter companies through their e-mail systems, e-mail is by no means the only method of infection. Internet-based worms and traditional file-based viruses continue to be huge threats to corporate security. For this reason, every company needs a comprehensive anti-virus infrastructure that extends from Internet and e-mail gateways to file servers and end-user desktops.

Dan Morton (dmorton@hawaii.edu) is a network specialist at the University of Hawaii's Advanced Network Computing Laboratory.