Providing Multi-Tiered Security for Microsoft Exchange Environments

For most enterprise IT organizations, eradicating spam and virus-laden e-mail traffic can be a daunting task. By deploying a multi-tiered protection strategy involving the desktop, file server, mail server, gateway, and network boundary, administrators can provide a strong defense against attacks and disruptions. A select set of products from Symantec and Dell can help fortify enterprise messaging environments.

BY WERNER ZURCHER AND GARRETT P. JONES

The requirements for managing an e-mail infrastructure such as Microsoft® Exchange changed dramatically as e-mail evolved into a mission-critical application. At the same time, spam and viruses present new and constantly changing threats to e-mail security and availability. To ward off attacks and help reduce business risks, IT administrators must protect e-mail infrastructures with a combination of integrated, highly accurate antispam, antivirus, and content filtering technologies.

Preventing spam, viruses, and other unwanted content from reaching the Microsoft Exchange environment and end users can help significantly improve overall e-mail productivity, enhance network security, and reduce total cost of ownership. In addition, significant reductions of spam and viral content can also help reduce backup windows and speed data recovery.

To help ensure e-mail security and availability, Symantec best practices recommend that organizations implement a multi-tiered approach. Each tier can help reduce the potential downstream risk posed by security threats and spam. For example, Figure 1 shows the primary tiers of e-mail protection for client desktops and the Symantec® products that are available for securing each tier.

To secure e-mail systems and keep them available, organizations must be able to control and manage the flow of messaging information from start to finish. In functional terms, this means removing spam, viruses, and unwanted or unneeded content from the messaging infrastructure at the appropriate time. Multilayered defenses should complement each other by using multiple methodologies to complicate any attempts to attack. The multi-tiered strategy also can help reduce both security risks and e-mail volume while helping to ensure that messages are legitimate and “clean” before they pass to the next tier.

Network boundary tier

Large enterprise IT organizations that need to significantly reduce spam before it enters their networks may want to
deploy antispam devices at the network boundary. One of the most effective ways this can be achieved is by using the Symantec Mail Security 8160 appliance. This is a network boundary device that acts as a router, not a message transfer agent (MTA), to inspect incoming Simple Mail Transfer Protocol (SMTP) traffic. The Mail Security 8160 is designed to significantly reduce the spam volume before it affects the internal network, including any SMTP gateway defenses.

Unlike traditional defenses, the Mail Security 8160 employs inspection and traffic shaping at the TCP/IP level by sampling and analyzing SMTP packets in real time based on their content, origin, and the sender’s reputation. Over time, the appliance determines a sender’s reputation based on cumulative history and reputation of the e-mail path itself. Once the reputation is established, incoming traffic can be “shaped” based on that reputation. Traffic shaping involves dynamically controlling the speed at which SMTP packets are accepted, and therefore controlling the number of e-mail messages that can be received from known spam senders. The net result is a significant reduction in the volume of spam reaching the mail server per unit of time, as well as a significant deterrent to spammers because spam jobs become backed up on their own servers.

Typically, traffic shaping is implemented only in large, high-volume environments (usually 2,000 or more e-mail users) that handle significant e-mail volumes. The Symantec Mail Security 8160 appliance is built using a Dell™ PowerEdge™ 1850 server.

**Gateway tier**

The two primary e-mail–borne threats and disruptions are viruses and spam. Several measures can be taken to prevent viruses and spam from reaching downstream servers, storage, archives, and e-mail users.

First, the most common virus content found in e-mail is the product of mass-mailer worms. These programs use e-mail addresses found on compromised systems and automatically generate e-mail messages to replicate and distribute their payload to unsuspecting users and systems. Because e-mail messages from mass-mailer worms have no intrinsic business value, they can be deleted automatically without fear of legitimate data loss. Gateway-based antivirus scanners should be able to identify and distinguish mass-mailer worms and allow administrators to delete them.

Second, spam content can be eliminated or removed from the internal mail streams to further reduce the burden on mail systems. Spam quarantines, generally housed on a server separate from the mail infrastructure, are ideal places to move unwanted spam content from active message stores (and consequently end-user mailboxes) to less-expensive media. Quarantine servers are easier to scale and maintain than mail servers because they have fewer functions. Anti-spam systems are not 100 percent accurate and businesses cannot risk the loss of legitimate e-mail, so spam quarantines provide a place to review spam-tagged messages. However, the reliability of the antispam system can play a significant role in reducing the amount of data that is held in quarantine and minimizing the amount of data requiring review.

Finally, an organization must not be perceived as a source of inappropriate or malicious content. All outbound e-mail should be scanned for viruses and inappropriate content. Also, organizations can put measures in place to stop unauthorized Internet e-mail (SMTP) traffic by defining network firewall rules that restrict outbound SMTP e-mail to only authorized e-mail servers. They can also establish desktop firewall rules that prevent the generation of SMTP e-mail protocol messages by end-user systems. Figure 2 shows how the multiple technologies provided with Symantec Mail Security 8200 Series

![Figure 1. Multi-tiered approach to e-mail protection](image)

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeping spam and other unwanted e-mail from reaching mail servers</td>
<td>Brightmail AntiSpam technology uses more than 20 spam-prevention techniques to block spam. The embedded Symantec antivirus technology features real-time scanning. Virus protection capabilities also include mass-mailer cleanup, which automatically removes e-mail messages associated with mass-mailer worms.</td>
</tr>
<tr>
<td>Reducing e-mail infrastructure costs</td>
<td>E-mail firewall technologies, which include Directory Harvest Attack Prevention and Sender Reputation, are designed to restrict connections from spam-sending servers.</td>
</tr>
<tr>
<td>Controlling outbound content</td>
<td>Content-compliance features help administrators control outbound e-mail content. Besides controlling viruses, administrators can manage sensitive e-mail content and enforce content rules to conform with corporate and regulatory policies.</td>
</tr>
</tbody>
</table>

![Figure 2. Security challenges and solutions for the gateway tier](image)
The continually changing landscape of threats—including spam, viruses, phishing, and spyware—requires tools that automatically keep up with the latest antispam and antivirus policies and rules.

was detected, and the accuracy rate, which shows what percentage of messages were correctly identified as legitimate (thus avoiding spam “false positives”). Symantec Mail Security 8200 Series appliances and Symantec Brightmail AntiSpam software are designed to provide highly effective and accurate antispam technology.

Furthermore, the continually changing landscape of threats—including spam, viruses, phishing, and spyware—requires tools that automatically keep up with the latest antispam and antivirus policies and rules. SymantecMail Security 8200 Series appliances and Brightmail AntiSpam software include an integrated virus and spam signatures update mechanism that is frequently and automatically updated. Mail Security 8200 Series appliances deliver antispam, antivirus, content filtering, e-mail firewall, and quarantine capabilities and are available in the following models:

- **Mail Security 8220**: Built on a Dell OptiPlex™ desktop and designed for environments with less than 100 users
- **Mail Security 8240**: Built on a Dell PowerEdge 850 server and designed for environments with 100 to 1,000 users
- **Mail Security 8260**: Built on a Dell PowerEdge 1850 server and designed for environments with more than 1,000 users

**Mail server tier**

The mail server tier processes outbound e-mail and processes and stores inbound and internal e-mail. Even with solid perimeter protection in place, messaging environments require inspection of internal e-mail traffic and stored messages. This is necessary because viruses can enter through other vectors such as through personal, Web-based e-mail or removable media (for example, USB drives of computers with outdated virus definitions). Also, post-attack virus cleanup of message stores (after early-stage virus infestations) using the latest antivirus definitions is critical.

Symantec Mail Security for Exchange enables administrators to inspect content in real time as e-mail is being committed to and accessed from the Exchange Information Store—which comprises both the private and public Exchange information databases. Administrators also can conduct sweeps of Information Store content on a scheduled or on-demand basis using updated virus definitions or specific content rules that are designed to identify suspicious or inappropriate content. Figure 3 explains common challenges that IT departments face when inspecting internal traffic and how Symantec Mail Security for Exchange can help address those challenges.

**Desktop tier**

At the innermost tier of the network, desktop users interact with Microsoft Exchange and other inboxes. At this tier, security threats and viruses are often launched by users who remain unaware of malicious activity. Consequently, having protection at the desktop level is a critical component of a tiered defense strategy. The Symantec antivirus, anti-spamware, and personal firewall software tools—Symantec Antivirus Corporate Edition and Symantec Client Security—are designed to stop the launch of threats delivered through e-mail at the desktop tier.

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanning for viruses that enter the network by bypassing the network boundary and gateway tiers</td>
<td>Viruses can enter the network through personal, Web-based e-mail or removable media such as USB drives. Mail Security for Exchange can scan mail downstream of the gateway servers to help ensure that new threats are exposed and handled.</td>
</tr>
<tr>
<td>Ensuring redundancy in e-mail inspection</td>
<td>Although inbound e-mail is a common delivery mechanism, viruses can enter e-mail systems from other sources. Running defenses at the gateway can provide coverage of inbound e-mail, but not all threats can be detected and removed at that tier—virus detection and cleanup also should be performed at the mail server tier.</td>
</tr>
<tr>
<td>Preventing unauthorized content from being sent to unauthorized users</td>
<td>Typically, companies carefully secure internal Web sites from unauthorized individual or departmental access. However, information from a secured Web site can be downloaded to a desktop system and easily forwarded to virtually anybody. This possibility exposes data to unauthorized users both inside and outside the company. Mail Security for Exchange incorporates rules-based content filtering to help prevent unwanted content from entering—and confidential information from leaving—the network.</td>
</tr>
<tr>
<td>Enforcing e-mail usage policies</td>
<td>Companies enforce e-mail policies to prevent inappropriate language in e-mail and unwanted or oversized attachments (such as MP3 music files; AVI and other video file types; and file types commonly used for delivery of viruses, such as executables). Mail Security for Exchange is designed to enforce these policies at the mail server tier to help prevent internally introduced and inappropriate e-mail from propagating inside and outside the company.</td>
</tr>
</tbody>
</table>

Figure 3. Security challenges and solutions for the mail server tier
Although desktop protection tools are highly customizable and individually effective, they cannot offer organization-wide protection because they protect individual desktop computers only. Comprehensive enterprise protection is possible only with a multi-tiered approach.

**Architectural overview**

For organizations supporting between 1,000 and 2,000 e-mail users, Symantec recommends implementing e-mail protection at the desktop, mail server, and gateway tiers. In high-volume e-mail environments of 2,000 or more users, additional protection should be implemented at the network boundary tier. Symantec and Dell recommend the following e-mail security products for each tier:

- **Desktop tier**: Symantec antivirus, anti-spyware, and personal firewall software
- **Mail server tier**: Symantec Mail Security for Microsoft Exchange
- **Gateway tier**: Symantec Mail Security 8260 appliance
- **Network boundary tier**: Symantec Mail Security 8160 appliance

Figure 4 shows the recommended architecture for a multi-tiered e-mail security approach for companies with more than 1,000 employees.

**E-mail protection on multiple levels**

E-mail plays a critical role in today’s mission-critical enterprise applications. By filtering out spam and viruses at multiple levels of the e-mail infrastructure, enterprise IT organizations can help prevent disastrous security intrusions and help keep e-mail systems running efficiently. Symantec’s offerings can be configured to address the security and availability needs of a multilayer e-mail infrastructure comprising the network boundary tier, the gateway tier, the mail server tier, and the desktop tier. This comprehensive approach provides appropriate tools to enhance e-mail security and enables high availability in mission-critical messaging environments.

**Werner Zurcher** is the director of product management in the Global Solutions Group at Symantec. Over the past 11 years, he has held various product management positions at VERITAS and Symantec, including Microsoft Windows® product line manager. Werner has degrees in Electrical Engineering and Computer Science from Brown University.

**Garrett P. Jones** is the Symantec global alliance manager in the Dell Enterprise Product Group and has also worked in the Dell Advanced Systems Group. Garrett has a B.A. in Business Economics from The University of Texas at Austin.

For more information:

**Dell and Symantec**

www.dell.com/symantec

**Symantec security products**

enterprisesecurity.symantec.com/esa