

Introducing Symantec Email Security and Availability

for Microsoft Exchange

The Symantec® Email Security and Availability solution for Microsoft Exchange is designed to protect both the systems and the information in Microsoft® Exchange e-mail infrastructures. This solution prescribes a layered hierarchy—implementing e-mail security mechanisms at key points within the network—to filter out unwanted messages and keep e-mail systems running efficiently.

BY WERNER ZURCHER AND GARRETT P. JONES

Related Categories:

E-mail technology

Microsoft Exchange

Security

Symantec

Visit www.dell.com/powersolutions
for the complete category index.

Enterprises that depend on e-mail for employee, customer, and partner communications require no-compromise security and high availability for their e-mail infrastructure as well as for the information that passes through the messaging system and is ultimately archived. However, security and availability are interdependent variables that are often achieved at the expense of one another: high security is often traded off in exchange for high availability, and vice versa.

The Symantec Email Security and Availability solution for Microsoft Exchange is designed to reduce the volume of spam e-mail, eliminate the risk of virus infection, automatically manage the e-mail life cycle through archiving, and keep an enterprise e-mail infrastructure resilient against failure. As a result, this integrated, multilayer approach can help reduce costs and simplify management of the e-mail environment and life cycle.

Figure 1 illustrates the components of the Symantec Email Security and Availability solution, which layers different types of protection at various levels of the e-mail architecture. This approach focuses on server products and does not encompass desktop protection options.

Increasing e-mail security

The first layer of the Symantec Email Security and Availability solution for Microsoft Exchange is designed to provide e-mail security by reducing incoming e-mail volume, securing the perimeter, and filtering e-mail internally.

Reducing e-mail volume

The first line of defense against unwanted e-mail content is deployed outside the messaging infrastructure—before the data can affect internal servers, including the Simple Mail Transfer Protocol (SMTP) mail gateways. This first line of defense is provided by the Symantec Mail Security 8160 appliance.

This appliance, which integrates Symantec software on a Dell™ PowerEdge™ 1850 server, helps prevent spam by evaluating sender reputation and using traffic shaping on the inbound SMTP stream. If a significant amount of incoming e-mail is spam, traffic shaping can help reduce the overall e-mail volume by blocking the transmission of SMTP traffic from known spammers and Internet hosts that they have commandeered, without affecting other e-mail transmissions.

Securing the perimeter

The network perimeter is a critical area for enhancing network security. As the second line of defense after the Symantec Mail Security 8160 appliance, the perimeter solution—incorporating Symantec software as well as Symantec Mail Security 8200 Series appliances—combines state-of-the-art spam and virus detection with turnkey operation. The following Symantec Mail Security 8200 Series appliances are available:

- **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

Symantec's perimeter components include a mass-mailer cleanup capability to remove entire messages and prevent unnecessary virus notifications based on the presence of a mass-mailer worm; the ability to block e-mail based on customizable rules; the ability to process spam based on antispam engine verdicts (for example, deleting spam messages but quarantining suspected spam messages for further review); and a Web-based Spam Quarantine server, which removes spam messages from the messaging environment but makes them available for further processing and review. By blocking spam and other unwanted e-mail messages, Symantec's perimeter protection reduces the volume of e-mail that must be distributed and processed internally.

Filtering e-mail internally

While Symantec's perimeter protection plays a key role in minimizing the negative impact of Internet e-mail traffic, Symantec Mail Security for Microsoft Exchange is designed to keep internal message traffic free of malicious or inappropriate content. This software is tightly integrated with Exchange using Microsoft-supported application programming interfaces, helping to ensure maximum performance and minimum conflicts with the underlying messaging architecture. Similar to the perimeter protection components, Symantec Mail Security for Microsoft Exchange leverages the same core antivirus technology, updates, and response mechanism. In addition to core scanning services, Mail Security for Microsoft Exchange offers content inspection capabilities, such as subject-line and message-body filtering, attachment stripping, and restricted message size.

Archiving e-mail and increasing content accessibility

The second layer of the Symantec Email Security and Availability solution for Microsoft Exchange archives e-mail. Archiving helps ensure that e-mail content is accessible and available whenever it is needed. This layer utilizes VERITAS Enterprise Vault™ software to archive, index, search, and retrieve information. The archiving

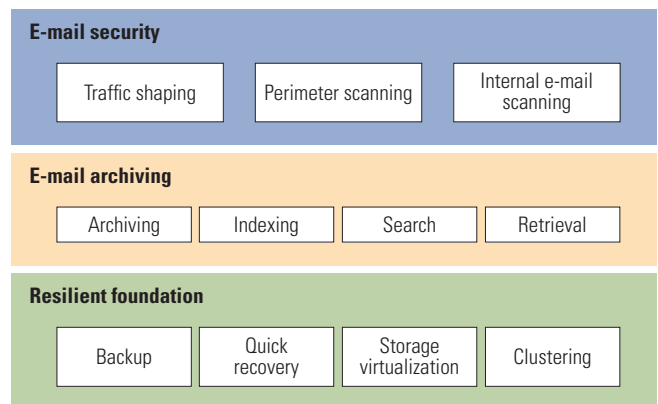


Figure 1. Components of the Symantec Email Security and Availability solution

process is designed to be automatic and seamless. Enterprise Vault implements user-defined policies to automatically archive e-mail, file system content, instant messaging, and other content from operational storage locations to a cost-effective online vault—without affecting end-user access to the data. Users can access archived information directly from their e-mail clients or Web browsers and can access it while offline by using the Offline Vault option.

IT administrators can automatically discover, collect, migrate, and eliminate Microsoft Personal Folders (.pst) files by moving the content to the vault. Enterprise Vault can also archive Exchange Journals and Public Folders, in addition to Microsoft Exchange mailboxes. Archived data is automatically compressed, duplicate copies are removed, and data is retained based upon business policies. Users, compliance departments, legal professionals, and corporate risk management functions can securely and easily search through messages, files, and attachments.

Message archiving using Enterprise Vault can provide benefits in three core areas:

- **Enhanced e-mail availability:** Enterprise Vault is designed to reduce the amount of data stored in primary messaging servers and file servers, helping to minimize corruption and performance problems that are observed when these servers reach capacity thresholds. By archiving data for long-term retention and providing search capabilities, Enterprise Vault can help maintain end-user access to data.
- **Minimized e-mail cost:** Enterprise Vault is designed to reduce primary storage costs throughout the e-mail environment by archiving outdated or infrequently accessed data to low-cost storage. This approach helps reduce backup costs significantly because archived data does not require frequent backups. Support and migration costs also can be minimized through elimination of e-mail quotas and .pst files and reduction in the amount of data to be moved during upgrades and server consolidation.

- Compliance with e-mail retention policies and regulations:** Enterprise Vault is designed to facilitate e-mail retention by following defined business rules to meet legal discovery and corporate or regulatory requirements.

Enterprise Vault can be integrated with Symantec Mail Security appliances and software. If an enterprise is legally required to keep a copy of all the e-mail it receives, a Web-based Spam Quarantine server that is fed spam and other junk e-mail messages by Symantec Mail Security can deliver the junk e-mail to Enterprise Vault for journaling. In this way, Symantec Mail Security 8200 Series appliances or Symantec Mail Security software can forward all SMTP e-mail communication to Enterprise Vault servers for journaling.

Building a resilient foundation

The third layer of the Symantec Email Security and Availability solution for Microsoft Exchange is designed to enhance e-mail system availability. Symantec offers various products to match varying organizational needs for information availability. Symantec Backup Exec™ and VERITAS Storage Foundation™ software form the lower tiers of the Symantec availability hierarchy. Backup Exec and Storage Foundation are designed to enable near-instantaneous recovery from storage device failures and quick recovery for application logic or data corruption. Backup Exec can be used as a data backup management tool to send data to tape as usual, but it also can be used to create on-disk backups, on-disk snapshots, and backups that are staged on disk and then migrated to tape.

For enterprises that require comprehensive protection and fast recovery when failures occur, Symantec offers VERITAS Storage Foundation High Availability (HA) for Windows. This advanced solution works with existing hardware and infrastructure components to enable cost-effective clustering capabilities designed to provide high-availability disaster recovery and business continuity for business-critical applications and databases. Alternatively, organizations may consider deploying Microsoft Cluster Service (MSCS), a component of Microsoft Windows® server operating systems designed to provide high availability.

Figure 2 provides a view of the Symantec Email Security and Availability solution in relation to the overall network topology. In Figure 2, the various tiers—network boundary, gateway, mail server, and archive—are shown in relation to the Symantec products that can be deployed at each tier.

Enhancing management of Exchange environments

Symantec Email Security and Availability for Microsoft Exchange is a comprehensive e-mail system solution that is designed to help ensure the security, availability, and resilience of e-mail systems and information, while helping to reduce the total cost of maintenance of the e-mail infrastructure. This solution takes a multilayered approach to

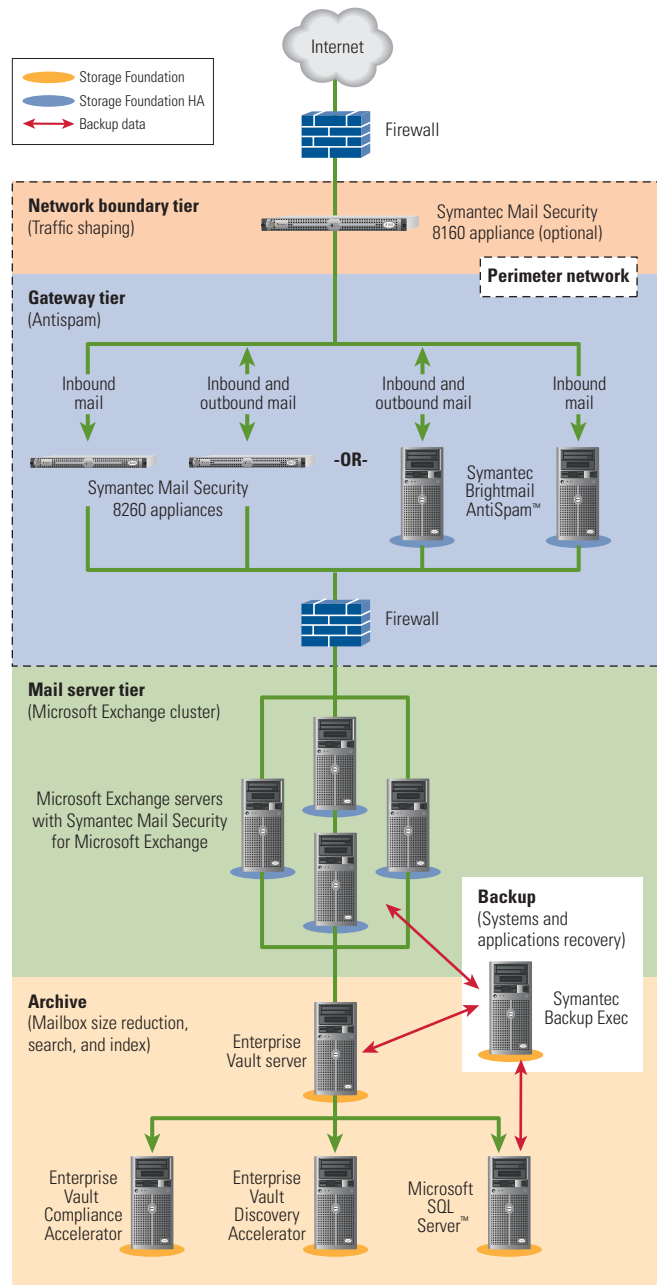



Figure 2. Network topology incorporating the Symantec Email Security and Availability solution for Microsoft Exchange

e-mail security, incorporating antivirus, antispam, archiving, backup and recovery, and storage management capabilities. 

Werner Zurcher is the director of product management in the Global Solutions Group at Symantec. 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. Garrett has a B.A. in Business Economics from The University of Texas at Austin.