Securing and Archiving Instant Messages:

A Critical Step for Securing Microsoft Messaging Environments

As part of a secure and productive messaging environment where users can take advantage of the latest communication tools, Symantec® IM Manager can help organizations control instant messaging (IM) while complying with legal regulations and corporate policies. IM Manager supports both public and enterprise IM networks and helps manage, secure, log, and archive IM traffic.

BY LEE WEINER AND CRAIG PHELPS

Related Categories:

Enterprise security

Instant messaging

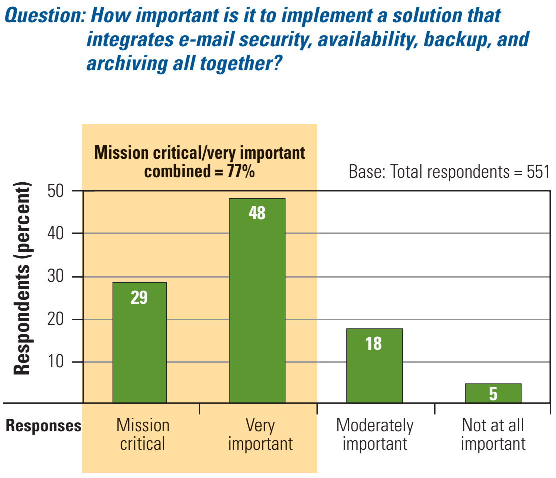
Security

Symantec

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

Instant messaging (IM) has become a key tool for enterprise communication, enabling employees to share information and collaborate in real time with colleagues, partners, and customers around the world. As a result, enterprises must find a way to safely enable IM while simultaneously satisfying the management policies, security needs, and regulatory compliance requirements associated with its use.

Dell and Symantec recognize the need for secure, highly available messaging environments supporting both e-mail and IM. For example, Figure 1 illustrates how important enterprises consider such an environment for e-mail. The first step in developing such an environment is to secure, protect, and archive Microsoft® Exchange Server deployments. This can be accomplished by implementing the Dell™ Secure Exchange Reference Architecture, which uses validated industry-standard components to simplify the deployment and scalability of secure enterprise messaging environments.[1]



***Question:** How important is it to implement a solution that integrates e-mail security, availability, backup, and archiving all together?*

Source: Survey of technology decision makers conducted by Ziff Davis Media on behalf of Symantec, March 2006. For more information, see "A Single Solution for Messaging Management and Security," by Ziff Davis Media, 2006, www.interop.com/newyork/pdfs/symantec-white-paper.pdf.

Figure 1. Survey responses on the importance of integrated e-mail solutions

[1] For more information about this architecture, see "Implementing the Dell Secure Exchange Reference Architecture," by Suman Kumar Singh and Bharath Vasudevan, *Dell Power Solutions,* November 2006, www.dell.com/downloads/global/power/ps4q06-20060452-Singh.pdf.

The second critical step is to do the same for other messaging platforms, including IM, by deploying Symantec layered messaging security along with Symantec IM Manager software.

Understanding IM security and regulations

Because enterprise IM deployments are growing rapidly and can often be unmanaged and unmonitored, IM use can expose organizations to numerous security risks, including the following:

- Blended threats that use IM to bypass traditional security software
- Identity theft, spoofing, and phishing over IM
- Advanced spyware and spam over IM
- Proprietary information security leaks over IM
- Targeted IM attacks on enterprise domains

Widespread enterprise IM use can also mean that, in some cases, archiving requirements for IM are the same as those for e-mail and other enterprise messaging systems. Important regulatory requirements relevant to IM include the following:

- **Securities and Exchange Commission (SEC) rules 17a-3 and 17a-4:** Require firms to retain all Internet communications pertaining to their business, which includes IM
- **NASD rules 3010 and 3110:** Require firms to supervise, review, and demonstrate compliance procedures for electronic correspondence, which includes IM
- **New York Stock Exchange (NYSE) rules 342 and 440:** Explicitly include IM in NYSE information memo 03-7 as a type of communication that must be archived under SEC regulations
- **Department of Defense directive 5015.2:** Sets standards for records retention, which includes IM
- **Sarbanes-Oxley Act section 404:** Includes extensive requirements for monitoring and reporting financial communication and documentation
- **Health Insurance Portability and Accountability Act:** Requires medical and pharmaceutical companies to retain patient records during clinical trials and provide for the records' privacy, which includes information shared over IM
- **Federal Energy Regulatory Commission (FERC) regulations:** Require logging and auditing transaction-related information, which includes IM

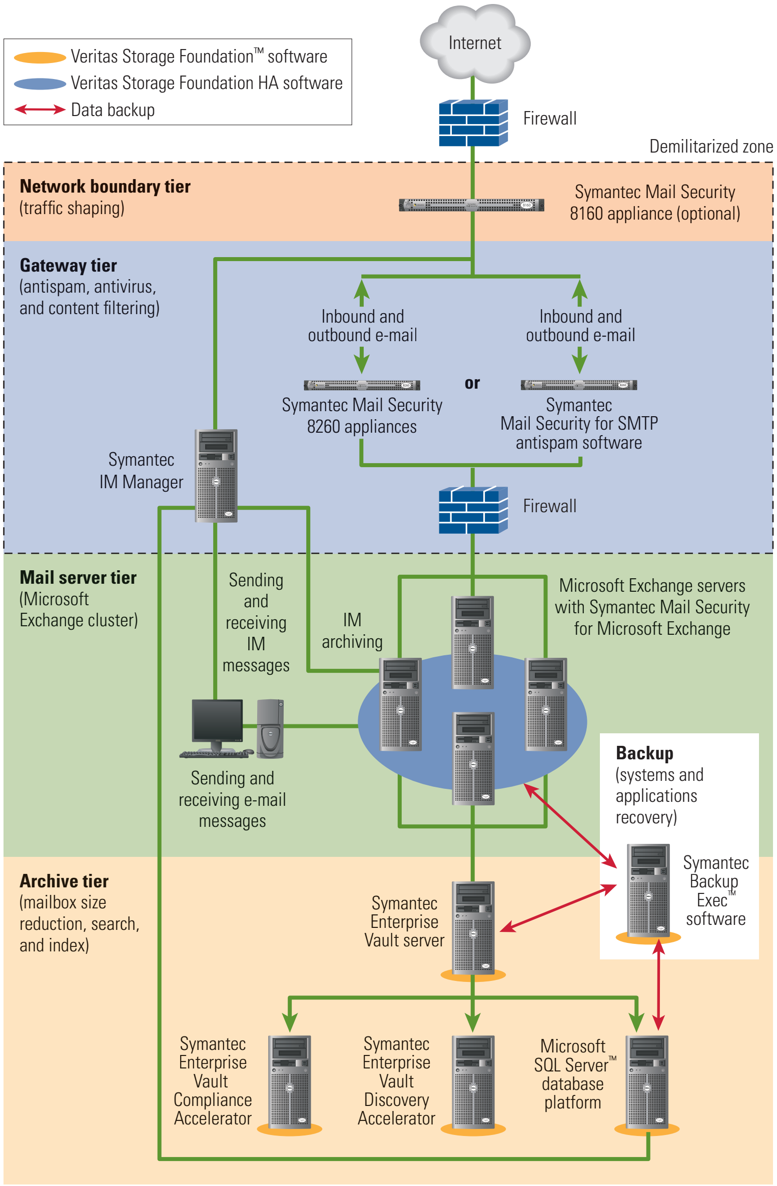


Figure 2. Symantec layered messaging security architecture

- **Federal Communications Commission (FCC) regulations:** Require extensive record keeping and storage, including supervising and indexing books and records
- **Corporate IM communication policies:** May require monitoring and controlling IM as part of general employee communications policies

Implementing Symantec layered messaging security and Symantec IM Manager can help protect organizations against IM-based threats such as viruses, worms, and malware and help enable compliance with legal and corporate requirements.

Implementing Symantec layered messaging security

Symantec layered messaging security deploys different types of protection at defined tiers inside the messaging architecture (see Figure 2):

- **Network boundary tier:** Reduces spam volume outside the network
- **Gateway tier:** Filters e-mail and IM messages outside the network, at the messaging environment perimeter
- **Mail server tier:** Filters e-mail messages inside the network

The separate but interdependent aspects of the messaging infrastructure enable layered functions to provide mutually reinforcing protections. Symantec recommends removing unwanted content from the messaging system at the earliest possible point; the critical interception points are entry and departure points for external e-mail and IM messages (in the gateway tier) and distribution points for internal e-mail and IM messages (in the mail server tier).

Securing IM with Symantec IM Manager

Symantec IM Manager is designed to help enterprises manage, secure, log, and archive IM traffic. It can help deliver real-time threat protection; rapid deployment; enterprise-class scalability, reliability, and management; and regulatory compliance for enterprise IM use. IM Manager offers comprehensive support for public and enterprise IM networks—including certified integrations with the IM software of industry leaders such as Microsoft, IBM, AOL, ICQ, Reuters, Yahoo!, and Jabber—and includes granular policy controls for text messaging, file transfers, audio, video, voice over IP (VoIP), application sharing, and other real-time communication capabilities associated with IM. Figure 3 provides an overview of key Symantec IM Manager features.

IM Manager can also help provide preemptive, automatic threat identification and protection against IM viruses, worms, and malware through the patent-pending Symantec Real-Time Threat Protection System (RTTPS). RTTPS IM threat protection goes beyond traditional reactive security systems and safeguards. Instead, it monitors enterprise IM traffic and searches for network anomalies and potential malicious behavior. Once a potential threat is recognized, the RTTPS predictive protection filter can identify the new threat signature and stop the potential outbreak by blocking it at the point of propagation.

Delivering comprehensive enterprise messaging management

Deploying Symantec layered security in conjunction with the Dell Secure Exchange Reference Architecture and Symantec IM Manager can help provide a comprehensive, secure, and highly available messaging environment that incorporates antivirus, antispam, archiving, backup, and recovery capabilities. Symantec IM Manager can help provide these capabilities for IM deployments by enabling organizations to manage IM traffic; improve security by scanning IM messages for viruses, worms, malware, and other threats; and comply with regulatory requirements for IM tracking and archiving. Dell and Symantec plan to continually enhance these tools and the Dell Secure Exchange program as enterprise messaging requirements evolve.

Function	Symantec IM Manager features
Managing IM traffic	• *User management and access control:* Controls IM user, group, and domain access to disparate IM systems, including integration with enterprise directory structures • *Priority-based policy enforcement:* Establishes consistent IM usage policy enforcement, including real-time content filtering, granular file transfer, and advanced client feature controls • *Real-time analytics and reporting:* Tracks and analyzes IM usage and growth patterns with real-time alerting and notifications, trend reporting, and custom monitoring
Controlling IM security and usage	• *Zero-day protection:* Helps detect and protect against zero-day attacks with patent-pending technology • *Automatic threat updates:* Automatically updates virus and spam signatures from the Symantec Security Response Team • *Virus scanning and file transfer control:* Scans file transfers and uses the Symantec AntiVirus™ Scan Engine to help prevent infected or confidential files from traversing networks
Complying with legal and corporate IM requirements	• *Rich message archive:* Selectively captures and retains IM conversations with direct links to employee data from the corporate directory for enhanced retention and discovery • *Integration with Symantec Enterprise Vault software:* Integrates with Enterprise Vault for enterprise retention and discovery and comprehensive messaging management • *Real-time content filtering:* Blocks messages and notifies administrators when messages containing restricted phrases or inappropriate content are sent

Figure 3. Key Symantec IM Manager features

Lee Weiner is a senior product manager in the Enterprise Messaging Management Group at Symantec.

Craig Phelps is a security strategist in the Dell Enterprise Product Group. He is a Certified Information Systems Security Professional (CISSP) and received his B.A., B.S., and M.B.A. from Brigham Young University.

FOR MORE INFORMATION

Dell and Symantec:
www.dell.com/symantec

Dell Secure Exchange:
www.dell.com/secure_exchange

Zurcher, Werner, and Garrett P. Jones. "Providing Multi-Tiered Security for Microsoft Exchange Environments." *Dell Power Solutions,* May 2006. www.dell.com/downloads/global/power/ps2q06-20060298-Symantec.pdf