

A Single Solution for Messaging Management and Security

Introduction

From in-house project management teams to sales personnel reaching out to prospects, email and instant messaging (IM) are playing an increasingly strategic role in the enterprise. But as the popularity of these messaging technologies grows, so does the vulnerability to security threats. Further, disaster recovery and long-term archival of email and IM content is increasingly critical in an era defined by daunting legal and/or regulatory requirements.

In an effort to meet these challenges, many companies overload their email servers with a variety of antivirus, anti-spam, content filtering and backup applications. Managing this disparate group of applications not only requires more and more skilled staff, but imposes a processing load that requires frequent upgrades to email servers. This in turn results in outages to email and IM service which users are less and less willing to tolerate.

A more effective approach is to deploy an integrated solution for email and messaging management and security. This reduces server and management overhead while providing maximum uptime, assured regulatory compliance and security while minimizing capital and management costs – and maximizing employee productivity.

Growing Use, Growing Risk

Email has become a mission-critical application, used for far more than sending short and simple text communications. Especially with the growth in broadband access by consumers and telecommuters, emails are now routinely used to transmit multi-year economic forecasts; product designs, customer proposals and presentations.

As a result, email is no longer just a medium for sharing text messages, but has become a de-facto file store for critical, and often, sensitive information. This information might include attachments with patient or customer names; price lists; specifications for future products or offers to buy or sell stock.

Rather than carefully file these attachments in subdirectories on their hard drive or a network file server, many users simply create folders in their email client application and search for the critical business information within attachments simply by checking their email. For the user, this has the additional advantage of preserving the “context” (in the form of the email text) around the information being stored.

As a result, not only is the volume of business email (excluding spam) expected to grow 25-30 percent per year through 2009, but the size of the attachments is growing, dramatically increasing the size of the storage required for email.

In early 2006, a study conducted by Osterman Research Inc. showed that over the previous 12 months the mean size of the email store at the typical organization had

grown 42%. While the number of emails sent had risen only 17 percent over the previous year, and the number of emails received had increased only 20 percent, overall storage growth has risen at a higher rate primarily because of the growing number of attachments to emails, and that those attachments were increasing in size.

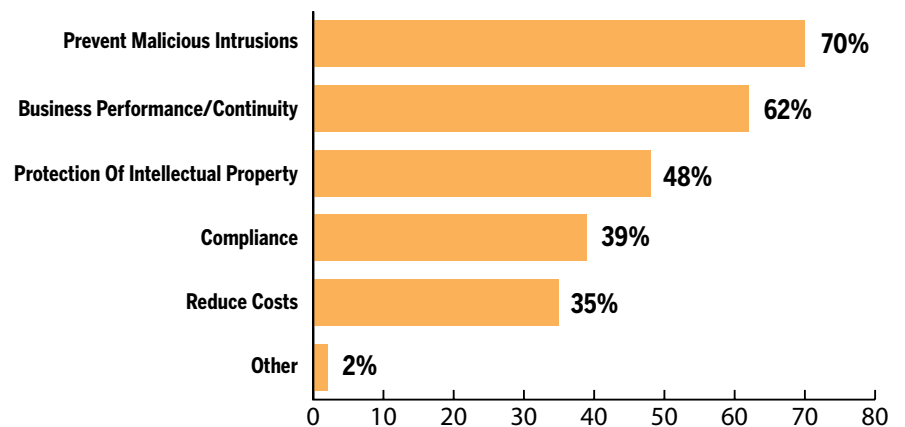
The growing volume of email messages, and the growing size of the average message, means that organizations require higher availability, performance and reliability from their email infrastructures. The increasing criticality of the information contained within emails results in a greater need to secure these systems, and the messaging traffic they carry.

These concerns were reflected in a survey of 551 technology decision-makers conducted by Ziff Davis Media on behalf of Symantec, in March, 2006. It showed that the key drivers for messaging security in their organizations are intrusion prevention, business continuity and the protection of the organization's intellectual property.

KEY DRIVERS SUPPORTING MESSAGING SECURITY STRATEGY

FIGURE 1

Q: What key drivers support your enterprise's messaging security strategy?



Hackers have noticed the popularity of email and IM, and have devised attacks which rely on these popular communications channels to spread viruses, worms, phishing attacks and other threats. Spam – which now makes up as much as 80 percent of email traffic – not only can carry viruses or other malware, but clogs corporate networks and email servers, causing either delivery delays or forcing organizations to upgrade their servers or networks to handle the extra traffic.

Another growing challenge for storage administrators are regulations which require – or which administrators fear may require – the contents of email and IM traffic to be stored for many years. Currently, there are only a few regulations at specifically require companies to store email or instant messages for a specific period of time in specific industries, example being Security and Exchange Commission's Rule 17a-4. However, many other regulations, such as HIPAA, and Sarbanes-Oxley, require organizations to protect and control broad classes of business records and information. Since more of business communication is taking place over email or instant messenger, and these systems are carrying more regulated information, many companies are developing systems to monitor, audit and archive messaging traffic so it will comply with external or internal policies if needed.

Another major driver for archiving is the need to quickly search and retrieve information such as emails or instant messages in the event of a lawsuit or a regulatory

audit. In many cases, the ability to quickly find the piece of information to avoid a regulatory penalty (or that allows the quick settlement of a lawsuit) can more than pay for the cost of the archiving/retrieval solution.

By automatically storing email information in a searchable, centralized form, archiving also reduces the time users spend managing their mailboxes and can thus deliver significant productivity gains. Finally, an archiving solution can also reduce the risk that an employee or outsider can tamper with the stored information.

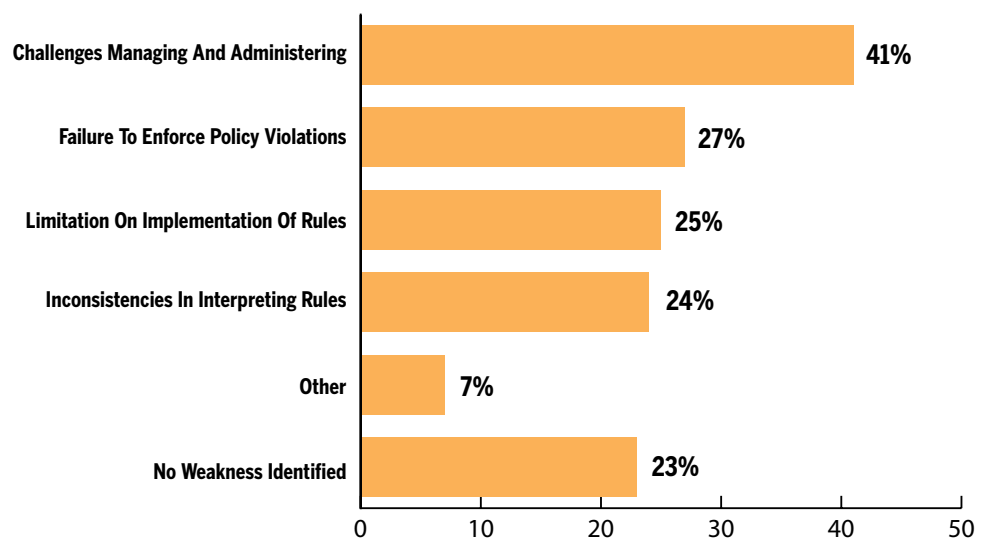
Each of the trends currently affecting enterprise email use are also beginning to affect enterprise use of IM. While IM is still mainly a consumer phenomenon, more and more organizations are using IM to communicate internally or with customers or business partners. In the financial services industry, for example, some brokers are using IM to discuss or recommend stocks to their clients. Most IM systems now allow users to attach and send files along with their IM messages. As with email, while the exact regulatory requirements are not necessarily specific to IM usage, some organizations are putting processes and technology in place to properly monitor and archive such message streams with an eye towards meeting regulatory or legal needs.

Despite the security and regulatory concerns, 70 percent of respondents admit weaknesses in managing and administering their email/messaging environments; in failing to enforce policy violations and failing to consistently interpret and enforce rules on email/messaging use.

WEAKNESSES IN MESSAGING ENVIRONMENT

FIGURE 2

Q: What weaknesses, if any, have you identified in the management of your current exchange messaging environment?



The Comprehensive Solution

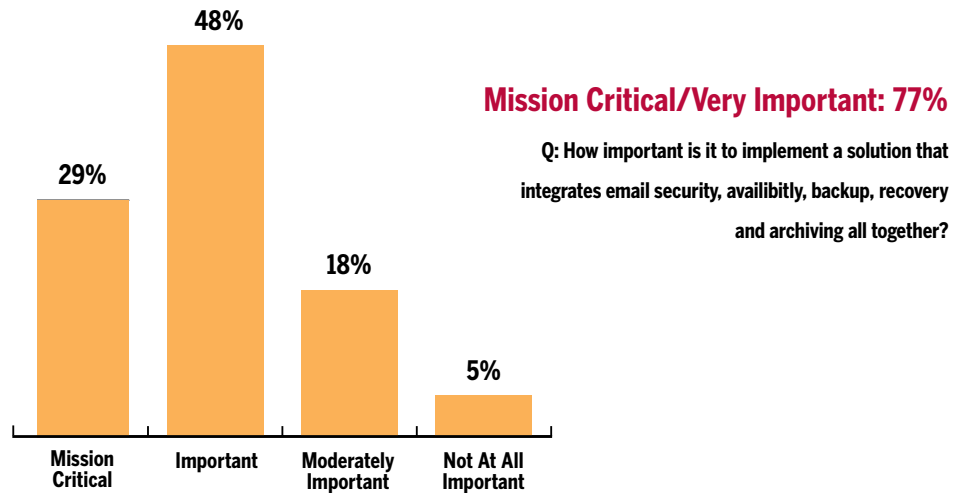
For many email administrators, just keeping up with security, availability and regulatory requirements of their messaging environments can be overwhelming. Some are now managing, tracking and maintaining as many as 40 applications on their email servers. This requires them to upgrade their email servers to handle these multiple applications. Inefficient storage management also forces them to constantly add storage to handle the archiving of older emails/messages, and (even worse) hire

enough trained staff to manage these multiple applications.

Almost eight in 10 would instead prefer a solution that integrates email security, availability, backup/recovery/archiving.

**IMPORTANCE OF SOLUTION THAT INTEGRATES EMAIL SECURITY
 AVAILABILITY, BACKUP, RECOVERY AND ARCHIVING**

FIGURE 3

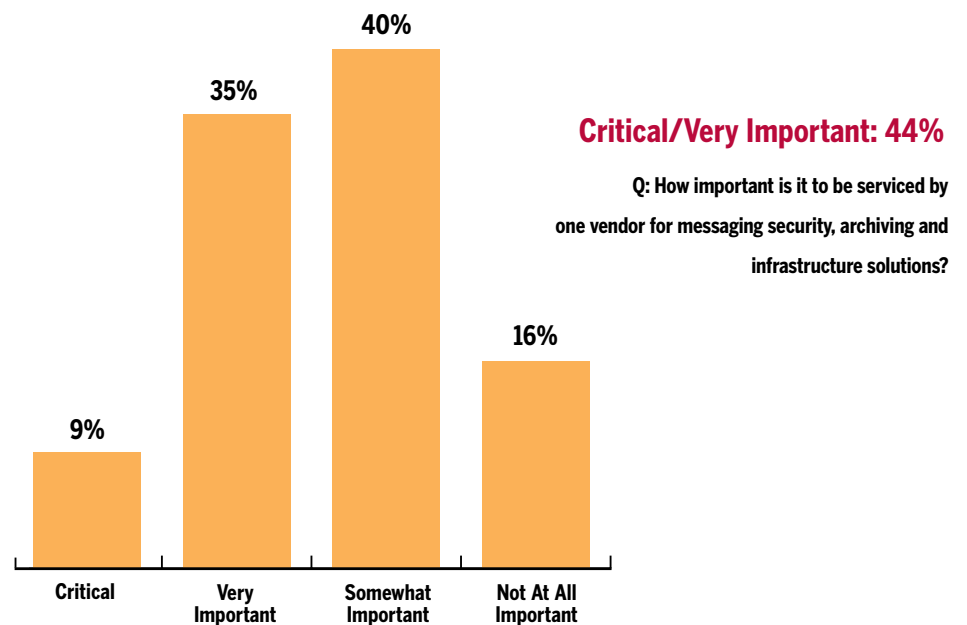


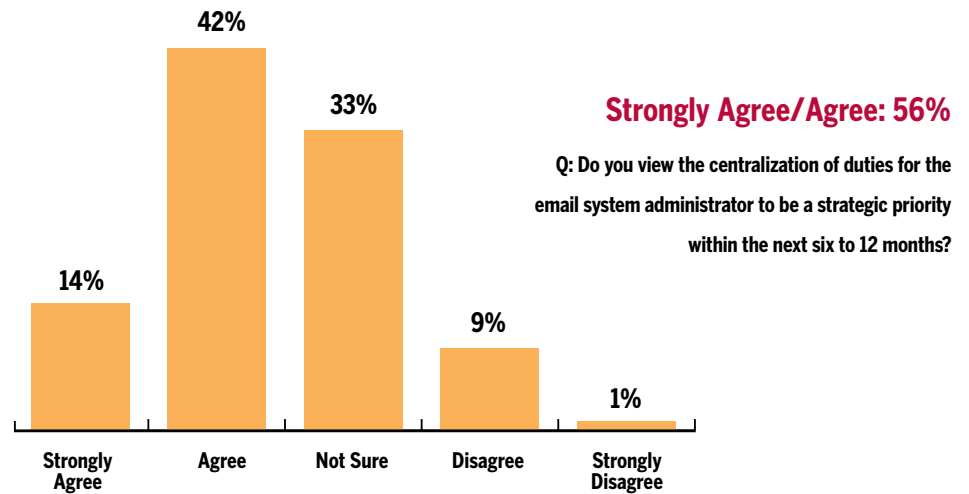
Nearly half want one vendor for messaging security, archiving and infrastructure management.

And more than half called centralization of email administration a priority.

**IMPORTANCE OF BEING SERVICED BY ONE VENDOR FOR MESSAGING
 SECURITY, ARCHIVING AND INFRASTRUCTURE SOLUTIONS**

FIGURE 4





Symantec offers a comprehensive email security and messaging management solution that addresses these key customer requirements. The combined security, management and data backup solution is provided from a single vendor. This comprehensive solution set reduces the incoming flow of email by blocking spam; identifies and blocks malware and viruses in both email and IM; and can help ensure regulatory compliance through content filtering. It can even reduce the costs of regulatory compliance through archiving software which allows older, less important data to be stored on lower-cost media, and to be indexed for quick and easy retrieval when needed.

This solution set is comprised of products that can be deployed in the location and form most appropriate for each customer: Outside the network or at the SMTP gateway; or as software, an appliance or a service.

Working at the edge of the network, the **Symantec Mail Security 8160 Appliance** stops spam before it enters the network and can clog the messaging infrastructure. This “antispam router” can be used in combination with an antispam solution at the SMTP gateway, such as the Symantec Mail Security 8200 Series appliances, to provide a comprehensive and multi-layered approach to combat spam.

Symantec also offers a software solution for the Internet gateway in the form of **Symantec Mail Security for SMTP** using Brightmail antispam technology. It leverages multiple effective technologies, globally distributed operations centers, a network of decoy accounts that monitors spam, and a real-time filter delivery mechanism.

Those who want to avoid the cost and management overhead of managing their own email security can choose **Symantec Hosted Mail Security**, a hosted solution that requires no onsite hardware, software, or ongoing administration. It allows only filtered email that is free of spam and viruses to reach corporate email servers, while content compliance features make it easy to control sensitive email content and enforce content rules.

Symantec offers protection for leading message environments through **Symantec Mail Security for Microsoft Exchange**, which provides high-performance, integrated mail protection against virus threats, spam, and security risks, and enforces company policies on Microsoft Exchange 2000/2003 servers. **Symantec Mail Security for**

Domino provides high-performance, integrated mail protection against virus threats, spam, security risks, and other unwanted content on Domino databases.

Symantec IM Manager is designed to help protect the IM traffic that is increasingly important to organizations. IM Manager is a software proxy that allows organizations to identify all IM use, create policies to manage this use, scan and remove all security risks, and archive all IM communications. It seamlessly manages, secures, logs and archives corporate IM traffic in compliance with internal or external data retention policies.

To meet the increased demand for information storage and retrieval, **VERITAS Enterprise Vault** provides lifecycle management for email and other corporate data including IM. It ensures compliance with retention and discovery policies by acting as a secure repository for electronic information. Its easy and rapid search and retrieval of content reduces the cost of content retrieval, recovery, and administration, while its storage optimization technology reduces message and information stores by 50 percent or more.

Symantec also has availability solutions such as backup (in the form of **VERITAS NetBackup** or **Backup Exec**); volume management, quick recovery and fault tolerance for Windows servers (**VERITAS Storage Foundation**); application clustering (**VERITAS Storage Foundation HA for Windows**) to ensure the continuity of email services.

Summary

Faced with constant pressures to secure and manage more data without increasing their budgets, IT managers want to deal with fewer vendors, not more. They also want to centralize the management and security of critical IT services such as email and messaging. Symantec's Enterprise Messaging Management solutions help customers protect and manage their email and messaging traffic from the time it hits the network gateway until it is archived on tape. The benefits for IT administrators are lower capital and operational expenses, and greater assurance they're protecting corporate information assets and meeting key regulatory requirements.

About Symantec Corp.

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.