



**Messaging Security,
Availability, and Control for
Small and Mid-sized Businesses**

Messaging Security, Availability, and Control for Small and Mid-sized Businesses

Contents

Executive summary	4
Introduction	5
Messaging security	6
Viruses	6
Spam	6
Phishing	7
Addressing the messaging security challenge	7
Messaging availability	10
Addressing the messaging availability challenge	10
Messaging control	12
Addressing the messaging control challenge	13
Benefits of Symantec solutions	15

Executive summary

Email has transformed business—how thoughts, ideas, proposals, and information are exchanged as well as the speed and efficiency with which business is conducted. It has become as important as, if not more important than, the telephone, serving not only as a communications medium but also as the de facto record of a company's business transactions and internal operations. Over the past 10 years, businesses have evolved from leveraging email as an alternate form of communication to depending on it as a mission-critical application.

At the same time, email poses threats and involves complexities that can jeopardize business viability and profitability. These can be organized into three groups: security, availability, and control. Security involves the impact of viruses, malware, and phishing attacks on email and instant messages; the burden of spam on the messaging environment; and the need for content filtering. Availability entails minimizing messaging downtime and its impact, as well as ensuring rapid recovery in case of a disruption. Control involves managing messaging storage, maintaining messaging software, and enabling messaging content to be discovered in response to legal needs.

In addition to email, instant messaging can spread malicious code and so must be included in messaging security and protection strategies. This white paper describes the challenges and a holistic approach to meeting them that addresses security, availability, and control. It then discusses Symantec's solutions and how they meet the business and technical requirements of businesses today.

Introduction

IT professionals tend to address security, availability, and control issues separately.

The “checklist” of issues in these areas is growing:

Security

- Ensure the messaging environment is protected from viruses, malware, and phishing.
- Reduce the impact of spam on the messaging environment.
- Prevent unauthorized transmittal of confidential information.
- Reduce volumes of unwanted email.
- Reduce threats to the network environment.

Availability

- Ensure that messaging systems are always available.
- In the event of a failure
 - Recover the messaging system quickly.
 - Recover the messaging system to a recovery point that is as close to instantaneous as possible.
 - Enable *granular* recovery, if possible (to the mailbox, folder, or message level).

Control

- Contain and manage the growth of email systems.
- Reduce the administrative burden of the email infrastructure.
- Reduce the storage space required for email.
- Develop an efficient way to retain, supervise, and discover electronic communication based on business and legal policies.

The likelihood that small and mid-sized businesses will face more or even all of these issues is increasing. Thus, a growing number of them are proactively addressing the full range of messaging security, availability, and control concerns.

Messaging security

The messaging security challenge includes protecting messaging systems from viruses, reducing the impact of spam, and addressing phishing threats.

Viruses

Worms, back doors, and Trojan horses are the primary virus threats that businesses face today, while polymorphic viruses are an emerging threat. Email continues to be the primary mechanism for propagating viruses.

A recent Symantec threat report found that worms, for example, made up 38 of the top 50 unique malicious code threats, accounting for 75 percent of the volume of the top 50 in the first six months of 2006. Most of these are mass-mailer worms, which use email addresses found on compromised systems and automatically generate emails to replicate and distribute their payload to unsuspecting users and systems. The report found that back doors were the second most frequently reported malicious code type, followed by Trojan horses.

During March and April 2006, a worldwide outbreak of two viruses, Polip and Detnat, signified that polymorphic viruses may be regaining prominence. A polymorphic virus is one that can change its byte pattern when it replicates and thereby avoid detection by simple string-scanning antivirus techniques. In essence, polymorphic viruses change their code, making their detection more dependent on technology compared with other types of malicious code. As Polip and Detnat showed, security and antivirus vendors may have difficulty detecting and protecting against these threats.

Worms and viruses use various means to transfer themselves, or propagate, from one computer to another. These propagation mechanisms can include a number of different vectors, such as email (Simple Mail Transfer Protocol), Common Internet File System (CIFS), peer-to-peer services (P2P), and remotely exploitable vulnerabilities. In the first half of 2006, malicious code that propagates via email accounted for 98 percent of the volume of the top 50 malicious code threats. During this period, 38 of the top 50 malicious code threats propagated via email, demonstrating the ongoing effectiveness of this vector.

Spam

Spam has grown to unprecedented levels. In the first six months of 2006, for example, spam made up 54 percent of all monitored email traffic. In addition to managing spam volume, companies must deal with spam threats. In the first half of 2006, one out of every 122 spam messages blocked by Symantec Brightmail AntiSpam™ contained malicious code.

Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or business, often for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to conduct cybercriminal activities for profit. The adverse impact on businesses from phishing includes degraded customer confidence, reduced brand loyalty, and increased customer service calls (and costs).

Phishing is growing rapidly. Over the first six months of 2006, the Symantec™ Probe Network detected 157,477 unique phishing messages—an increase of 81 percent over the previous period. According to an earlier Symantec report, over the last half of 2005, roughly one out of every 119 email messages scanned was found to be a phishing attempt. Also in the last half of 2005, Symantec Brightmail AntiSpam blocked 1.5 billion phishing attempts, a 175 percent increase over the number of blocked phishing attempts detected in the last six months of 2004.

Addressing the messaging security challenge

Addressing messaging security involves four primary areas: 1) mail server protection (at the groupware level), 2) protection at the network perimeter (the messaging gateway), 3) instant messaging protection, and 4) granular content management.

Mail server protection

The first line of defense against viruses and spam, protection at the mail server or groupware level, provides the following capabilities:

- Scanning for viruses that enter through other vectors within the network, such as personal Web-based email, removable media such as USBs, remote laptops whose virus definitions are not current, and more
- Preventing unwanted or oversized content from being transmitted through the internal mail system
- Performing post-attack virus clean-up of message stores using the latest antivirus definitions
- Retroactively cleaning message stores to remove older, unneeded content such as internal “housekeeping” memos

As a result, mail server protection solutions, such as those for Microsoft® Exchange and Domino®, need to be able to inspect content in real time. Such inspections should take place as email is being committed to the message store, when it is being accessed from the store, and on a scheduled or on-demand basis. Sweeps of message store content based on updated virus definitions or specific content rules identify suspicious or inappropriate content.

Protection at the gateway

As the messaging environment grows and spam proliferates, protection is extended to the network perimeter, stopping threats at the entry point. Several measures can be taken to prevent unwanted email from entering the network and reaching downstream servers, such as expensive message stores and data archives, as well as email users. For example, mass-mailer worm emails, which have no intrinsic business value, can be deleted automatically via gateway-based antivirus scanners. Restricting unauthorized SMTP traffic (that is, port 25 traffic) via network and desktop firewall rules also prevents propagation of mass-mailer worms that provide their own SMTP delivery services. Spam content can be eliminated or removed from mail streams to further reduce the burden on mail systems. Spam quarantines, generally housed on a server separate from the mail infrastructure, provide lower cost storage and enable user review of the spam for legitimate email.

By implementing these measures, companies can divert or delete a large volume of data from the mail stream, ensuring that downstream systems are not overtaxed by nonbusiness content. This in turn leads to significant improvement in the overall operation of the email infrastructure.

Instant messaging protection

Instant messaging (IM) continues to grow, with users in both home and business environments estimated at 300 million in 2005. The three largest IM providers—AOL Instant Messenger, MSN Messenger, and Yahoo! Messenger—each report over 1 billion messages sent per day, and IM traffic is expected to exceed email traffic by the end of 2006.

However, IM is generally unprotected and unmonitored, leaving it vulnerable to attacks. This is particularly worrisome for corporate entities, as IM is rapidly becoming a key part of business communications, and confidential information is often exchanged on these networks. IM can be a potent vector for spreading malicious code. The infection of one computer can result in the broadcast of messages to all users contained in an IM contact list on that machine. Furthermore, social engineering tactics can be highly effective, as the parties communicating by IM are inherently trusted.

According to the *Symantec Internet Security Threat Report* (March 2006), in the second half of 2005, worms were the preferred type of malicious code on all three large IM networks, making up 91 percent of IM-related malicious code. Worms were also used to download other non-IM malicious code. For instance, a worm may send users a link to a Web page that exploits a vulnerability in a Web browser, such as the Microsoft Windows® Graphics Rendering Engine WMF SetAbortProc Code Execution Vulnerability. This allows the malicious code hosted on the Web page to be automatically installed on a computer running a vulnerable browser.

As a result, businesses need a tool that enables management and policy enforcement of secure instant messaging. Such a solution should include the following capabilities:

- Centralized management
- Protection against zero-day attacks (attacks that take advantage of a vulnerability before a fix is available)
- Automatic updating of virus and spam signatures
- Real-time content filtering
- Features that enable discovery of information in IM records

Content management

Management of email and instant messaging content is another key dimension of email security. Because email and instant messages often contain confidential or sensitive information, managing the sending and receiving of this information is paramount. Distribution of company confidential information needs to be limited to employees and approved contractors, often at a granular level. At the same time, sensitive information such as payroll information needs to be restricted to only certain internal parties. Distribution of any information on retail customers, such as credit card numbers, must also be restricted. These decisions are typically implemented via the establishment and enforcement of policies, and content filtering tools are typically configured to manage content at the SMTP gateway and on the groupware server.

Symantec solutions for messaging security

At the mail server (groupware) level, Symantec offers Symantec™ Mail Security for Microsoft Exchange. Installed on the server with the mail store, this software provides antivirus, antispyware, and content-filtering protection. At the messaging (SMTP) gateway, when spam is a serious problem, Symantec solutions provide functionality similar to gateway protection. Symantec offers this protection in various forms to suit user needs, including a security appliance (Symantec Mail Security 8200 Series), integrated software that IT administrators can install on their SMTP server (Symantec Mail Security for SMTP), or a Symantec hosted solution (Symantec Hosted Mail Security). To provide secure instant messaging, Symantec offers Symantec IM Manager to manage, secure, log, and archive corporate IM traffic using granular policy controls. For more information on these offerings, see www.symantec.com/enterprise/solutions/key_products.jsp?solid=emm.

Messaging availability

The second major challenge that small and mid-sized businesses face involves messaging system availability. These businesses need their messaging systems to be available all the time. If the systems do fail, they need to be quickly restored and the data recovered to a recovery point that is as close as possible to the present.

An ideal solution is to install and maintain a completely redundant messaging system. In this approach, hardware and software are duplicated to maintain a complete set of backup systems, best located in a second location. This arrangement includes synchronous replication in a clustered configuration of servers with automatic failover and mirrored storage to enable almost instantaneous recovery, with little or no data loss. However, because of the duplication of solution components and the need to maintain two independent sites, this solution is prohibitively expensive for most if not all small and mid-sized businesses.

Addressing the messaging availability challenge

Whether the backup is performed at a single site or multiple locations, the recovery point objective, recovery time objective, and the ability to recover at a granular level are key considerations.

Single-location backup

For small and mid-sized businesses with a single location, the base level of messaging backup involves backing up data to tape and storing the tape offsite. The backup can then be used to restore data after a failure.

While businesses demand that email is protected and available, the amount of email data is growing exponentially. IT is faced with the challenge of backing up this critical Microsoft Exchange data within the existing backup window and recovering it quickly.

The objective of traditional backups is to minimize downtime of the enterprise messaging environment while providing the quickest possible data recovery in case of a system crash, database corruption, loss of a single mailbox, or other forms of data loss. In order to maintain the availability of Exchange and protect its mission-critical data stores, companies go to great lengths to protect their Exchange environments. Today, this protection is primarily accomplished through online backups of the Exchange database and a separate time-consuming backup of individual mailboxes for granular recovery.

Continuous data protection redefines traditional Exchange protection by eliminating daily Exchange backup windows. With continuous protection, Exchange transaction logs are protected and consolidated into easily managed recovery points automatically to help ensure Exchange databases are protected up to the latest complete transaction log.

Multiple-location backup

Continuous data protection also provides advantages for businesses with multiple locations. The hardware at various sites can be replicated by a single piece of hardware at a secondary site. Hence, if hardware at any one of multiple locations fails, recovery can be accomplished from a single centralized location. Rather than doubling expenditures to achieve seamless backup and recovery, this approach requires only an incremental additional investment.

Recovery point, recovery time, and recovery granularity

As Exchange has become mission critical in most organizations, the need for more frequent recoveries of Exchange data beyond daily backups has increased. It is no longer acceptable for many organizations to be able to recover Exchange mailboxes, messages, folders, and databases only from the previous night's backups. Continuous protection for Exchange enables these backups to occur more often to help ensure Exchange recoveries are always possible at intervals specified by the IT administrator.

Also, it's imperative that Exchange mail messages, mailboxes, and folders can be restored individually without having to restore the entire Exchange database—and without time-consuming mailbox backups.

Symantec solutions for messaging availability

Symantec Backup Exec™ 11d with Exchange Agent provides continuous and granular backup and recovery, while enabling asynchronous replication. Hence, this solution is suitable for small and mid-sized businesses with a single location or multiple locations. Symantec has developed new technology (patent pending) in Backup Exec 11d, which enables users to make only a single-pass full or incremental backup of Exchange, dramatically decreasing the time needed to back up mailboxes while also reducing the storage required. You can now recover critical Exchange data in seconds, including individual emails, individual mailboxes, public folders, calendars, and contacts, from a fast single pass Exchange database backup—with or without continuous protection. Tailored specifically for Microsoft Exchange environments, this solution enables Web-based file retrieval using a standard Web browser. Its centralized management features provide scalable management of distributed backup and remote servers. For more information, see www.symantec.com/Products/enterprise?c=proinfo&refId=57.

Messaging control

Email systems were not designed to store the amount of data that passes through the typical messaging system today. Some companies also must retain even more email to comply with external regulations, adhere to internal policies, or prepare for possible legal discovery requests. The impact on businesses includes the following:

- High cost due to increased storage and backup costs
- Lower availability and performance because messaging servers typically slow down when they reach near capacity, and long backup windows are required to back up the large amount of email data

To address this problem, most IT organizations implement email quotas, restricting each user to a fixed amount of email storage (typically 25 to 200 megabytes). Even with these quotas, a business that must store email for a great number of users requires a large amount of storage space. In Microsoft Exchange, a copy of the email that is stored on the server for each user resides in an offline store (OST) file. (Users can synchronize the OST and mailbox folders located on the server,

enabling them to work offline.) As OST files increase in size, Exchange performance deteriorates—another reason why administrators place quotas on email storage.

As a result, users must constantly ensure that email storage on their OST file is below the quota. As they approach this quota, users typically store their excess messages in separate personal folders on their desktops or laptops (for example, PST files in Microsoft Outlook). If users do not back up these files, they could permanently lose their data in case of a computer malfunction. Studies have shown that data on most laptops is not backed up. Also, if the computer is lost or stolen, confidential or sensitive data could fall into the wrong hands. Not surprisingly, many laptops are lost or stolen every year.

Over time, even these PST files grow to unmanageable sizes, primarily because they also include email attachments. Hence, many users archive all or portions of the data in these PST files to a removable medium such as a CD to save disk space on their desktop or laptop. If these media are lost or stolen, confidential or sensitive data could be at risk.

Email quotas affect user productivity, result in large numbers of support calls, and are one of the burdens of email management.

Addressing the messaging control challenge

Effective practices

An effective solution for messaging control provides the benefit of email quotas (storage management) without the problems—allowing administrators to minimize the size of primary storage and leverage more cost-effective secondary storage without burdening the user or losing critical data. Archiving systems allows email administrators to:

- Automatically migrate email messages and attachments based upon policy, such as date and size, to a secondary—and often less expensive—storage location (which also improves Exchange performance)
- Proactively and automatically expire or delete messages, or migrate to a third tier of storage, based upon business policies
- Compress the information and implement single-instance storage (SIS), which eliminates duplicate emails and attachments, to reduce the volume of information while leveraging disk or tape storage for archived data
- Allow end users to seamlessly access messages and attachments from the archive just as they would normal email

- Index the messages and attachments so that end users can search the (eventually large) archives of their email over time

In this way, message archiving solutions allow businesses to provide users with a seemingly infinite mailbox (no quotas) while cost-effectively controlling storage usage on the primary messaging servers.

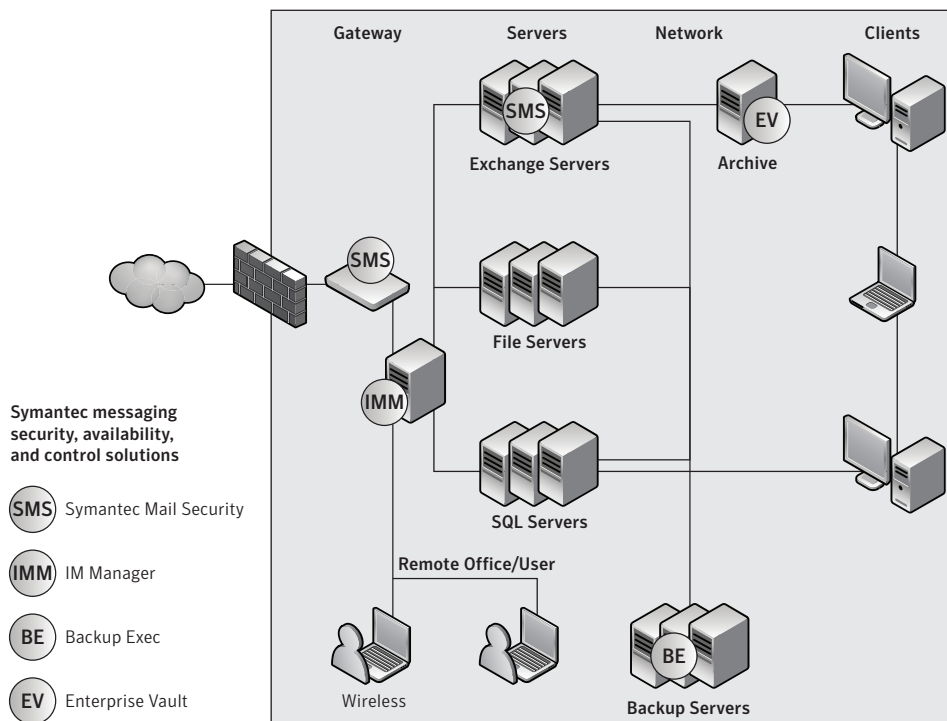
Symantec solutions for messaging control

Symantec Enterprise Vault™ automatically archives messaging data to secondary storage as needed, improving Microsoft Exchange performance and reducing storage costs. With this solution, users no longer need to consider quotas, and they can access any archived mail at any time within the Exchange or Outlook interface. Enterprise Vault automatically backs up both OST and PST files and enables timely recovery. By using SIS, this solution reduces storage space by 50 percent or more via the elimination of duplicate emails and attachments.

Many small and mid-sized businesses today are unable to cost-effectively locate emails required by legal proceedings (for example, all emails that mention a particular product, or those between defined users between a defined set of dates). Enterprise Vault facilitates this process, while providing control over messaging growth, remote user data backup, and storage costs. Via the Discovery Accelerator, Enterprise Vault reorganizes messaging data into base data (that is, body data or target data), and metadata in the SIS process provides Web-based keyword and other search capabilities. This facilitates the discovery of email when required by subpoena, other legal proceedings, or regulatory requirements. For more information, refer to www.symantec.com/enterprise/solutions/key_products.jsp?solid=emm.

Benefits of Symantec solutions

Working with multiple vendors to address messaging security, availability, and control requires significant in-house expertise and resources. Moreover, as threats evolve over time, the effective combination of solutions evolves, posing a moving target for IT administrators. The figure illustrates how complementary Symantec solutions (Symantec Mail Security, Symantec IM Manager, Symantec Backup Exec, and Symantec Enterprise Vault) address these issues.



Symantec provides messaging solutions at the gateway, mail server, backup server, and network archive locations.

Implementing Symantec's messaging security, availability, and control solutions helps small and mid-sized businesses realize the following benefits:

- Minimize downtime and consequent costs due to virus, malware, phishing, or other security breaches
- Reduce email-borne security risks by blocking spam and ensuring that stored messages (both email and IM) are legitimate and clean

Messaging Security, Availability, and Control for Small and Mid-sized Businesses

- Minimize adverse impacts on company brand, customer trust, and legal liability through employee theft or misuse of corporate information assets
- Minimize archiving, backup, and storage costs
- Ensure high availability, optimized operations, fast backup, and the ability to rapidly recover messaging systems
- Improve employee productivity
- Increase IT efficiencies, thus reducing staff requirements
- Simplify and streamline the management and maintenance of messaging systems, thereby lowering total administrative costs
- Enable accurate forecasting of IT budget spending and support strategic company initiatives and growth
- Ensure legal, regulatory, and industry compliance, enabling corporate governance and automated policy assessment
- Enable compliance with service-level agreements within a company's business units and departments

Symantec offers small and mid-sized businesses the industry's leading email, instant messaging, and archiving solutions, which work together to provide unmatched comprehensive protection. With these solutions, you can effectively manage and monitor your Windows messaging systems and ensure your systems and data remain secure and readily available at all times.

About Symantec

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.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, Backup Exec, Brightmail AntiSpam, and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Other names may be trademarks of their respective owners. Printed in the USA. 11/06 11567287