

Email **Security** and **Availability**:

Why You Need It, How to Achieve It



Over the last 10 years, electronic mail has evolved from an occasional communications alternative to a mission-critical capability that few organizations can do without. These days, according to the Enterprise Strategy Group, more than 75 percent of corporate intellectual property is stored in email¹.

Email Security and Availability

The trouble with email

This spectacular transformation of email from incidental to business-critical has come, however, at a price. Email's chief virtues — its simplicity and ubiquity — not only expose your company to tremendous risk and liability, but also add to the cost and complexity of managing and storing your email communications.

Direct Media: Centralizing email storage and management

A provider of database services and custom media mix to support their clients' direct marketing needs, Direct Media, Inc. (DMI) does a lot of business by email. As email volumes exploded, though, employees struggled to access critical, revenue-generating information used to formulate client marketing campaigns. And the firm's storage infrastructure was severely overtaxed. DMI decision-makers understood they needed a centralized, web-based way — with archival, search, and discovery functionality — to manage their email environment.

After deploying Symantec solutions, including VERITAS Enterprise Vault and Symantec Mail Security, DMI has saved \$60,000 by eliminating the need to purchase additional email servers and storage/backup gear and cut the number of file servers from six to just one, thus significantly cutting total cost of ownership. What's more, employee productivity is up, since information search is now centralized and web-based. Help desk calls have been reduced, too, and the nightly backup window has been shortened.

DMI's data is safer, too. "Symantec protects our email system against corruption due to viruses and helps ensure the information we store is free of malicious content," says Kevin Ladd, DMI's director of infrastructure. "Symantec helps Direct Media save both time and money by reducing the amount of infected and unwanted emails we receive, and by helping us migrate older email information to less expensive storage."

Email-borne risk and liability come in two forms:

- Viruses, spam, spyware, and other malicious code, and
- Easily transmitting confidential and sensitive data to those who might misuse it.

Viruses, spam, and spyware. Infections from malicious code — viruses, Trojan horses, worms, etc. — and spyware pose serious threats to enterprise security and data integrity. In one study, 31 percent of respondents pointed to viruses, Trojans, and malicious code as their greatest security threat, and 10 percent said worms were the greatest problem².

These days, so much of email is spam — between

50 percent and 95 percent, according to Internet service providers³ — that organizations must devote substantial resources to sifting out legitimate emails from it. This effort recently has taken on particular importance because, increasingly, spam and malicious code are converging, turning PCs (corporate and consumer) into unwitting spam engines.

Confidential data exposed. More danger looms. Experts note a shift in the motivation behind attacks from those of opportunity to those intended to reap financial gain or profit, often from the compromise of confidential customer information, credit card numbers, Social Security numbers, etc.

Email systems are prime targets of such attacks. They also are often the means by which — accidentally or not — employees within organizations fail to comply with confidentiality laws and destroy customer trust via outgoing messages that contain malicious code or inappropriate content, including confidential data going to unauthorized addresses.

Too much cost and complexity. Meanwhile, managing the email lifecycle is getting costly for several reasons:

- Annual worldwide business email topped one billion gigabytes (1 exabyte) for the first time in 2004, according to IDC⁴, and email volumes continue to increase;
- In order to stay in regulatory compliance, organizations must retain emails longer, verify that they have not been altered, and ensure that they are easily accessible;
- The amount and diversity of email makes managing its storage and retrieval complex and expensive. According to Osterman Research, 65 percent of organizations consider growth in messaging storage to be a serious or very serious problem⁵.

Inadequacies of patchwork-quilt email infrastructures. Given its importance in conducting business, organizations must keep email up and running all the time. Without email, your business faces the negative impacts of lower customer satisfaction, missed deadlines, lost sales opportunities, and lost revenue.

Email Security and Availability

Yet keeping email systems reliably available, as well as secure and compliant with regulations, is difficult for today's typical email infrastructures, which generally consist of a patchwork of point solutions.

Solution: An 'information integrity' strategy

What is needed to address growing email challenges?

An email infrastructure that secures data and systems from abuse and attack while simultaneously making systems and information highly available, compliant with regulations, and capable of legal discovery. This means controlling and managing the flow of email from start to finish, thus protecting your organization against risk and ensuring continuity and reliability of operations.

How? By identifying and removing unwanted content from the messaging infrastructure as early as possible, despite constantly growing email volumes and limited IT budgets.

Email security. To make email secure, your email infrastructure must:

- Shield email systems against intentional or inadvertent attack and disruption, and protect email users against threats and disruptions from the Internet, such as spam and viruses. This includes guarding your organization's network against exposure to email virus and worm infections that might impact end-user systems and internal servers.
- Guarantee that incoming and outgoing data are free of malicious or inappropriate content. This includes protecting data against inadvertent or intentional transfer to unauthorized persons and seeing to it that privacy restrictions (regarding social security numbers, medical records, etc.) are not breached.

Email availability. Ensuring the availability of email involves:

- Minimizing disruptions. Your email infrastructure must be protected from harm and down-

time — via performance degradation, outright failure, or vulnerabilities/attacks coming from the outside that may compromise end-user systems as well as email servers.

- Minimizing planned downtime. Your email infrastructure must be able to change, and as email traffic increases, the storage capacities required to support a dynamic email infrastructure must grow, too. Minimizing planned and unplanned downtime with online storage management capabilities is a requirement for many IT organizations.

- Maximizing application availability. In addition to ensuring that storage management tasks do not impact end-user's access to email, further measures must be taken to protect against hardware, software, and/or human errors. IT organizations need to ensure that both data and applications are protected. Even in the event of a failure, the application must continue satisfying end-user requests.

- Reliable delivery of legitimate email. Regardless of the volumes of spam and other unwanted content, legitimate emails must always be available and accessible.

- Data backup. Email information must be preserved through backup and replication to assure its availability, recoverability, and manageability. This is best achieved through a combination of disk- and tape-based solutions that enable not only point-in-time copies of information but also long-term storage.

- Archiving. Old emails must be retrievable long-term in accordance with organizational policies and/or regulatory requirements.

- Easy access. End users must have seamless access to email — in email systems as well as in long-term archives — and both end users and legal personnel must be able to easily and securely search through historical email and attachments.

- Policy enforcement. Employee communications must be supervised for compliance with internal and external policies.

A holistic approach. To build this sort of information integrity into your email infrastructure, you

Email Security and Availability

need to look at email issues holistically, considering security and availability needs together in order to streamline operations and reduce costs.

Whenever your organization migrates to new email servers or consolidates messaging servers, you have the opportunity to begin revamping your email infrastructure and to reduce the complexity associated with managing multiple vendors' products, licensing agreements, and support contracts across your email environment.

Implementation

Begin with security

Creating a cost-effective enterprise-wide email infrastructure begins with securing your email environment. It's an effort that entails three key steps:

Reliably reduce email volumes. The goal is to avoid receipt of unwanted content, thus reducing email volume without sacrificing legitimate messages. This is most effectively accomplished with Symantec's patent pending, traffic-shaping technology.

Defend your perimeter. The idea is to prevent unwanted Internet email from reaching downstream servers. The best solutions to achieve this include gateway-based antivirus scanners, attachment filtering, spam quarantines, an integrated and frequently-updated antispam tool, outbound email scanning, and measures to stop unauthorized SMTP traffic (network firewall rules restricting Port 25 access).

Protect your mail servers. This kind of protection enables scanning for viruses that enter through other vectors (for instance, personal Web-based email, removable media like USBs, remote laptops with outdated antivirus definitions, etc.), as well as post-attack virus clean-up of message stores using the most-recent antivirus definitions and retroactive message storage cleaning to remove older, unneeded content. It also prevents content from being sent to unauthorized users and stops unwanted or oversized content from being sent through the internal mail system. Best solutions: Inspect internal mail traffic in real time as email is being committed to or accessed

from the message store, and sweep message stores on-demand or on a schedule based on updates of virus definitions, content rules, or other considerations.

Next: Email lifecycle management and content archiving

Once your email infrastructure is secure and your users are not drowning in unwanted email, you can take on the challenges of managing exploding email volumes and complying with regulations that require email retention and ease of access.

The dark side: email quotas. While a short-term solution to this problem — establishing email quotas — may tempt you, you may be better off resisting, since email quotas create a new set of difficulties that hurt user productivity, generate large numbers of support calls, and add to the burdens of email management. Consider the following.

Users must constantly ensure their email storage is below the quota and store excess messages in separate personal email folders. Because these files (folders) often are kept on network file servers, storage and backup resources remain strained. Moreover, these files are highly susceptible to corruption and face the same availability and performance problems seen on email servers.

When end users store over-quota email files on local desktops or laptops without adequate backup or security, critical data becomes subject to loss or theft. Emails stored locally by end users also cannot be centrally managed, which can throw your organization out of compliance with regulations that require easy and quick access to email archives.

Indeed, any email files (such as MS Outlook PST files) kept exclusively on local desktop systems or on end-users' laptops are nearly impossible to manage and secure.

Email lifecycle management and content archiving systems. A better alternative can be provided by email lifecycle management and content archiving systems that centralize email storage, so these files can be managed and kept secure.

Email Security and Availability

These enterprise-wide solutions automatically migrate email messages and attachments based on organizational policy (such as date, size) to a secondary — and often less expensive — storage location (which can also be online disk storage). Messages also can be proactively and automatically expired, deleted, or migrated to a third tier of storage. Further, the information in messages can be compressed and implemented in single-instance storage to reduce the volume while cost-effectively leveraging disk or tape storage for archived data.

This approach offers plenty of benefits, including:

- Automatic archiving and indexing of ' journaled' email so it's guaranteed to be captured and able to be retrieved in the future using specialized tools to assist in legal discovery processes (capture, search, review), thus ensuring that your organization is in compliance with legal and corporate retention requirements;
- Secure search capabilities across the organization, so users can perform instant search and retrieval of content and authorized personnel can quickly respond to information requests;
- Sampling and workflow around regulated supervision of employee email;
- Faster platform migrations as well as increased server consolidation and storage optimization;
- Lower total cost of ownership of frontline mail environments.

Finally: Build a resilient foundation

Once your email information storage is secure, manageable, and in compliance, it's time to ensure it is also robust, scalable enough to meet accelerating demands, resilient against failure, and able to recover quickly when failure occurs. Achieving this kind of resilience requires an ability to identify, understand, and proactively respond to a vast range of problems before they can disrupt your email services.

You'll need to be able to automatically monitor and react to potential outages according to well-defined response policies.

You'll need to keep functioning and communicating amidst disaster. This requires well-defined disaster recovery plans to restore system functionality as well as technologies to protect data and systems and minimize downtime and disruption — or to failover to a replicated site.

You should be able to efficiently manage your storage resources without taking your system offline. And you should be able to proactively maintain, upgrade, and manage the IT infrastructure components that contribute to service delivery, including server operating systems, network components, and storage systems.

Backup/recovery tools. An email infrastructure with this kind of resilience requires a backup/recovery environment that can provide very quick recovery — in the minutes that disk-based backup with snapshots can handle, rather than the hours that tape backup requires. These tools must be able to scale to protect large environments and use a single management interface that consolidates all backup/recovery operations. And they also have to deliver alerting, reporting, and troubleshooting technologies, and be application-aware for the particular messaging system used in your email infrastructure.

Storage virtualization. Email infrastructure resilience also depends on a storage management environment that enables the separation of your storage space from your physical hardware, so that storage/disk hardware can be added, physically relocated, virtual snapshots taken, RAID layouts changed, unused storage reclaimed — all without taking data or applications offline. This sort of virtual storage management environment can be scaled holistically as a system of unified and available resources shared across your entire messaging network.

Storage virtualization enables the use of disparate hardware and local or SAN-attached disks to hold redundant copies of email in case of disk, array, SAN, or even site failures. Good storage virtualization tools will automatically migrate data from failing disks to healthy disks, to avoid downtime from unplanned events.

High availability clustering technology. To quickly move an application from a failed server to a healthy server to minimize downtime or add incremental compute cycles as requirements dic-

Email Security and Availability

tate, you'll need high availability clustering to mirror not only the data, but also the email application for redundancy.

Solutions that combine security and availability

By combining products and services with VERITAS, the leader in availability solutions, the new Symantec is now able to offer a wide-ranging solution set that enables comprehensive enterprise-wide email security and availability.

2,200 vendors and 2 million decoy email addresses scanned on a daily basis for spam, phishing, and email security threats.

Symantec's email security solutions, all derived from the Symantec Global Intelligence Network, include three lines of defense:

The first line of defense. Symantec Mail Security 8100 Series appliances reduce spam volume up to 80 percent by stopping it before it reaches the network, thus containing administrative overhead, network bottlenecks, mail infrastructure costs, and storage requirements.

The second line of defense. Symantec perimeter solutions include

- Symantec Brightmail AntiSpam — combining effective spam catching with a high accuracy rate that prevents false positives.
- Symantec Hosted Mail Security — incorporating Symantec's market-leading anti-spam and antivirus technologies, backed by Symantec Security Response, in a hosted environment.
- Symantec Mail Security for SMTP — providing high-performance, integrated mail protection against virus threats, spam, and other unwanted content at the earliest point of network entry, the Internet email (SMTP) gateway.
- Symantec Premium AntiSpam — an add-on subscription service powered by Brightmail technology delivering the industry's highest accuracy rate against false positives (99.9999%) for Symantec Mail Security and Symantec AntiVirus Enterprise Edition customers.

The third line of defense. Symantec groupware protection includes Symantec™ Mail Security for Microsoft® Exchange, providing high-performance integrated mail protection against virus threats, spam, and other unwanted content for Microsoft Exchange 2000/2003 servers; and Symantec™ Mail Security for Domino, which does the same for Lotus Domino environments.

Symantec's email security and availability approach			
email security			
Traffic-shaping	Perimeter scan	Groupware scan	
email archiving			
Archiving	Indexing	Search	Retrieval
Resilient foundation			
Backup	Quick Recovery	Storage Virtualization	Clustering

These unique technologies and services control and manage the flow of email information from start to finish, helping protect your organization against risks, ensuring uptime of systems and users, satisfying compliance and document retention requirements — all while minimizing your total cost of email infrastructure ownership.

Symantec enterprise security solutions. Behind Symantec's unmatched security capabilities stands the Symantec Global Intelligence Network, which gathers malicious code data from more than 150 million desktop antivirus sensors and 20,000 intrusion detection (IDS) software and firewall sensors in 180 countries, and collects and analyzes data from 4,300 monitored and managed security devices around the world. The network leverages one of the world's largest vulnerability databases—covering 18,000 applications and operating systems from more than

Email Security and Availability

Perimeter protection form factors: Which is best for you?

- Software-based solutions require installation of application software on customer-provided hardware and operating system.
- Appliance-based solutions deliver pre-installed application software on a vendor-maintained operating system and hardware.
- Hosted solutions locate the software and systems off-premise at a hosted provider and Internet email streams are redirected through this environment to be scanned.

Symantec enterprise availability solutions. Symantec's VERITAS availability products curb disruptions and provide reliable data backup and recovery, a flexible archiving framework, and high data availability levels with these key solutions:

- VERITAS Enterprise Vault — providing a flexible archiving framework to enable the discovery of content held within email, file system, and collaborative environments.
- VERITAS NetBackup — delivering high-performance data protection that scales to protect the largest UNIX, Windows, Linux, and NetWare environments from desktop to data center to vault.
- VERITAS Backup Exec — a complete backup solution for mixed platform workgroups needing protection for Windows NT, Windows 2000, and Novell NetWare environments
- VERITAS Storage Foundation for Windows — providing easy-to-use online disk storage management for enterprise Windows environments by enabling high availability of data, optimized storage I/O performance, protection of current storage investments, and freedom of choice for future storage hardware investments.
- Symantec (VERITAS) Storage Foundation High Availability (HA) for Windows — providing uninterrupted and consistent access to mission-critical information with easy-to-use, online storage management tools for heterogeneous enterprise environments. A Dynamic Multipathing option increases application availability by load balancing and providing availability

through the storage area network. The FlashSnap option enables point-in-time snapshots for disk-based recoveries in the event of failure or corruption. And VERITAS Cluster Server™ provides high availability for applications and databases monitoring the health and performance of the resource and automatically restarting the resource on another available server.

When email is mission-critical. Once email becomes a mission-critical part of your organization, you have no choice but to defend it against abuse and attack, and keep it resilient and reliable. You'll also have to ensure that your email information storage complies with corporate, legal, and regulatory policies, and that email ownership costs are kept under control.

The better you're able to do this, the more competitive advantage your organization will be able to derive from its email infrastructure.

Symantec's Email Security and Availability solutions can help.

Symantec solutions reduce risk to email systems and data, and ensure uptime and performance of both systems and users of email while satisfying regulatory and corporate policy requirements. Symantec solutions also can lower overall costs of ownership.

That's because Symantec solutions significantly reduce cost burdens at all layers of the email infrastructure. And Symantec's Email Security and Availability solutions provide flexible deployment options across a range of form factors, integration points, and operating environments so you can tailor solutions to your needs and keep your email infrastructure running securely, reliably, and economically.

Footnotes: ¹Email Security and Availability: A Holistic Solution to a Critical Problem, International Data Corporation, August 2005

²Ibid.

³Ibid.

⁴Ibid.

⁵Messaging Security Market Trends, 2005-2008, Osterman Research, May 2005