



## Email Security and Availability

How to ensure the protection and availability of email information and systems while reducing the cost of ownership

By Chris Miller  
Director of Product Management  
Symantec Network and Gateway Solutions

# Email Security and Availability

## Contents

<b>Introduction</b> .....	<b>3</b>
<b>What is Email Security and Availability?</b> .....	<b>4</b>
<b>Email Security and Availability Drivers</b> .....	<b>5</b>
<b>Email Security and Availability—How to efficiently manage email data and systems</b> .....	<b>6</b>
Step 1—Security .....	7
Step 2—Archiving .....	12
Step 3—Building a resilient foundation .....	15
<b>Introducing Email Security and Availability from Symantec</b> .....	<b>17</b>
Email Security .....	17
Availability through archiving .....	22
Symantec’s solution for a resilient email foundation .....	23
<b>Conclusion</b> .....	<b>29</b>

### Introduction

Electronic mail has transformed how we conduct business—how we exchange thoughts, ideas, proposals, and information—as well as the speed and efficiency at which we can conduct business. Email has become as important, if not more important, in our personal and business lives as the telephone itself.

Not only does it serve as an effective communications medium, allowing one-on-one and one-to-many conversations to occur virtually simultaneously and instantaneously, but it also has become the de facto record of a company's business transactions and internal operations. At the same time, it has become an avenue for threats and problems that can often jeopardize the very viability and profitability of our business.

Over the past ten years, we have gone from leveraging email as an alternate communications vehicle to depending on it as our most mission-critical application. According to the Enterprise Strategy Group, more than 75% of corporate intellectual property is stored in email. The fact that email also serves as a detailed transaction record for a company makes it valuable as evidence in a court of law, proof that companies are following regulations and a source for identifying violations of internal company policies. As a result, more companies are deciding to preserve email for longer periods of time and verify that the email is not modified during the retention period, whether because of external rules and pressures explicitly forcing them to do so or internal corporate governance guidelines. This has also increased the cost of storage required to retain necessary email messages and added complexity to email data lifecycle management.

However, the very things that make email valuable to an organization also expose it to a great deal of risk and liability. Its ubiquity and simplicity have made it the preferred method for transferring:

- Any data between users, including non-business content such as multimedia files and executables, or even company confidential information outside the corporate walls
- Threats and disruptions to thousands of users, such as viruses and spam, at high anonymity and very low cost

Consequently, we spend countless hours, budget, and resources defending and worrying about how to keep email running smoothly. IT professionals tend to look at security issues such as reducing spam or blocking viruses and at availability issues such as making sure the email application, systems, and data are there when needed separately. However, as the “checklist” of how to manage email more efficiently and cost effectively to keep up with the increase of

email volume continues to grow, IT should be looking for a more holistic approach to balancing the cost and risk associated with email. In situations like migration to new email servers or consolidation of messaging servers, organizations have opportunities to review current systems and plans to build an email infrastructure that is flexible to respond to an ever-changing IT environment. Symantec Email Security and Availability can help IT get to that goal.

### **What is “Email Security and Availability”?**

At its simplest, Email Security and Availability is about cost-effectively ensuring both the security and the availability of email. (Security and availability are the two critical sources of risk to email today.) Email Security and Availability is about protecting the data and systems from abuse and attack, while simultaneously making the systems and information highly available for business use, meeting requirements for regulatory compliance, and for legal discovery. “Systems” here refers to the underlying email architecture or messaging system itself—from the physical infrastructure (servers, storage, and network) to the application software (mail systems, message stores, and more) and the security and availability of the information that resides in it or travels through it. “Information” refers to the actual content that is transferred through and stored in the messaging systems.

The following defines how availability and security impacts data and systems:

Security and availability are very broad areas, so it’s helpful to understand the specific goals that are being addressed by Email Security and Availability.

Making email “secure” means:

- Email systems themselves are protected against intentional or inadvertent attack and disruption. Email users are protected against threats and disruptions from the Internet, such as spam and viruses.
- Data being sent to or arriving from customers, suppliers, and partners is free of malicious or inappropriate content.
- The network itself is protected against exposure to virus and worm infections that circulate through email and can affect end-user systems and internal servers.
- Company data is protected against inadvertent or intentional transfer to unauthorized persons and does not encroach on privacy restrictions (social security numbers, medical records, etc.).

## Email Security and Availability

Making email “available” means:

- Minimizing disruption to the email infrastructure itself—through performance degradation or outright failure
- Assuring that end-user systems are not compromised and taken offline by email-borne attacks
- Assuring that legitimate email is available and accessible, amid the volumes of spam and other unwanted content
- Preserving email for long-term retention based upon external regulations or internal company policies
- Providing end users with seamless access to information in email—whether in email systems or in long-term archives
- Allowing end users and legal personnel to easily and securely search through historical email and attachments
- Enabling organizations to supervise employee communications for compliance with internal or external policies

Of course IT must do all of this with a constantly growing volume of email, while IT budget growth does not happen at the same rate.

### **Email Security and Availability Drivers**

The Internet and email have rapidly evolved and become powerful business enablers, but not without costs. Several key drivers have created the need for Email Security and Availability:

- The size of business email volumes sent annually worldwide increased 47% from 2003 to 2004 (Source: IDC Worldwide Email Usage 2004.2008 Forecast: Spam Today, Other Content Tomorrow, IDC #31782, August 2004)
- Ever-increasing volume of spam entering corporate networks, comprising 64% of total incoming email, on average. (Source: Brightmail Logistics and Operations Center monthly Spam Statistics Report)

## Email Security and Availability

- Surge in phishing attacks.
- Annual rise in the number of mass-mailer threats continues to increase year-over-year.
- Recognition in the United States, Europe, and other markets that email is a legal business record that must be preserved.
- Emerging regulations around retaining, auditing, and supervising internal and external email communications.
- Loss through employee theft or misuse of corporate information assets affecting company brand, customer trust, and legal liability.
- Increasing cases of litigation requiring discovery of email.
- Increase in storage costs, 65% of organizations consider growth in messaging storage to be a serious or very serious problem, slightly more problematic than the problem of spam itself. (Source: Osterman Research, *Messaging Security Market Trends, 2005-2008*, May 2005).

### **Email Security and Availability—How to efficiently manage email data and systems**

Email Security and Availability starts by controlling and managing the flow of email information from start to finish to protect the company against risk and ensure the unobstructed operation of business. In functional terms, it comes down to removing unwanted or unneeded content from the messaging infrastructure at the right points in time.

These right “points in time” are:

- **Incoming email**—arriving from the Internet, including spam and phishing attacks, mass-mailer worms, inappropriate or non-business content.
- **Outgoing email**—viruses or confidential or inappropriate content leaving the four walls of the corporation.
- **Internally transmitted email**—viruses or confidential or inappropriate content spread within the corporation.
- **Stored email**—email that is no longer accessed frequently but needs to be retained for medium to long periods of time

## Email Security and Availability

To achieve this control, organizations need a layered approach that starts at the earliest point of entry onto the network, working through to the end user and beyond to archiving and storage systems.

### **Step 1—Security**

As a general rule, the first step is to secure the environment. This includes: avoiding receipt of unwanted content, preventing unwanted Internet email from reaching downstream servers, and inspecting internal mail traffic.

#### ***Reliable volume reduction***

To keep the email system performance up despite an increase in email volume—especially with the current spam issue—it is important to simply avoid receiving unwanted content. Easier said than done, of course, but achievable with the right tools.

A nontechnical first line of defense can and should be user education and awareness regarding email usage policies and best practices. For example, all users should be aware of basic policies and procedures such as not replying to spam messages, not using unsubscribe links, not following links in suspicious fraud emails, not opening email attachments where there is no clear business relevance or where the intention is suspect i.e., the attachment may contain a virus or vulnerability patch, not ignoring virus hoaxes and warnings, and not allowing content based on size limitations or type such as EXEs, MP3s, AVIs, etc. But while education should play a role in the overall solution, the reality is that we do need technology to block spam and unwanted mails.

The challenge of stopping email in transit lies in the fear that legitimate data will also be lost. As a result, systems used to stop content before it reaches the network or internal mail systems must be highly reliable, i.e., they must be effective and enable the continuous flow of legitimate email.

The advantages of technology that stops content close to the source include the savings in bandwidth and storage that can be felt throughout the network—from the SMTP gateway scanners themselves to the message stores, and even down to the message archive layer. Eliminating content that serves no practical business purpose saves precious bandwidth, processing power, and storage space.

Few companies offer products that deliver this key benefit, with the exception of Symantec's patent-pending traffic-shaping technology, which will be discussed later in this paper.

### ***Protect the perimeter***

Several measures can be taken to prevent unwanted Internet email from reaching downstream servers, such as an organization's expensive message stores and data archives, as well as email users. The two primary email-borne threats are viruses and spam.

First, the most common virus content found in email is the product of mass-mailer worms. These are programs that use email addresses found on compromised systems and automatically generate emails to replicate and distribute their payload to other unsuspecting users and systems. Since mass-mailer worm emails have no intrinsic business value, they can be deleted automatically without fear of legitimate data loss. Gateway-based antivirus scanners should be able to identify and distinguish mass-mailer worms and allow administrators to delete them based on this distinguishing feature. Often referred to as "Mass-mailer Cleanup" or "Worm Purge," it is an important feature to look for in antivirus solutions.

Second, mass-mailer worms usually rely on the same variety of data or file types to deliver the payload as an attachment. These are file types such as .scr, .pif, .vbs, etc., which are typically not found in regular business transactions; but they may also include .exe files and will apply compression techniques, usually .zip. Based on these characteristics, further action can be taken to proactively protect the network environment from emerging, yet unidentified, mass-mailer threats. Attachment filtering can accomplish this through the creation of policy to delete messages when the presence of a suspect extension type, such as .scr and .pif, is detected. Also critical is the ability to identify these files within compressed containers, like .zip files, and take the appropriate action.

Third, 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, are ideal places to move unwanted spam content from active message stores (and consequently end-user mailboxes) to less expensive media that are far easier to scale and maintain. Quarantines are required because antispam systems cannot be 100% accurate. Since businesses cannot risk the loss of legitimate email, users need a place to review spam-tagged messages. However, the reliability of the antispam system can play a significant role in reducing the amount of data that is held in quarantine and minimizing the amount of data requiring review by users.

The standard metrics for antispam reliability are detection (i.e., spam catch rate) and accuracy rate against false positives (legitimate messages incorrectly identified as spam). One of the biggest challenges with many antispam systems is that detection and accuracy rates

are often dependent variables, which can mean high detection rates at the expense of lower accuracy and vice versa. It is important to look for an antispam solution that is not a collection of manual tools, but is an integrated, frequently updated response mechanism with highly accurate spam definitions and techniques based on the latest spamming methods.

These best-of-breed antispam solutions ensure both detection and accuracy. The primary benefit—the elimination of a large subset of spam messages while in transit—minimizes the burden on the spam quarantine and the end-user reviewer. Additional benefits include greater end-user confidence in their company's antispam defenses.

Finally, in order to maintain trust with customers and partners, it is also critical that an organization not be perceived as a source of inappropriate or malicious content. There are many ways to address this.

- All outbound email should be scanned for viruses and inappropriate content. If company internal or confidential information is not to be shared with outside parties, it is important to identify this content and put the appropriate measures in place to filter the content at the mail server or gateway layer, to keep it internal. Policy guidelines and employee education and awareness are also important.
- Since today's mass-mailer worms provide their own SMTP delivery services and no longer rely on popular email programs and company mail architecture to distribute threats, it is important to put measures in place to stop unauthorized SMTP traffic (also referred to as Port 25 traffic). These include network firewall rules that restrict Port 25 access to only authorized mail systems, as well as desktop firewall rules that prevent the use of Port 25 by end-user systems (end users send and receive Internet email through the mail server, which is responsible for any actual SMTP transmissions).

By implementing these measures, a large volume of data can be diverted or deleted from the mail stream, thus ensuring that downstream systems are not overtaxed by non-business content. This in turn leads to significant improvement in the overall operation of the email infrastructure.

## Email Security and Availability

Also key to the protection of the perimeter is choice of solution form factor. Perimeter form factors include:

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

The availability of resources and expertise varies from company to company, even within larger organizations, so the choice of form factors becomes a matter of preference and convenience. Here are some benefits and criteria of choosing a solution.

### **Software**

- Deployment flexibility through support for multiple operating systems, including Windows®, Solaris™, and Linux™. This allows companies to deploy and maintain flexibly and not require specific operating system expertise in all geographic locations.
- Highly integrated solutions combining antispam, virus protection, content filtering technologies. For emergency updates or upgrades, the fewer the number of components, the easier it is to ensure compatibility and uptime.
- The vendor is responsible for both the security technology and response components. This limits finger-pointing between vendors in the solution itself.

### **Appliance**

- “Hardening” of the operating system for security: Non-essential operating system services are disabled, if not removed entirely, to limit exposure to system vulnerabilities.
- A global support contract with four-hour hardware replacement is available.
- Updates for applications and operating system can be automated.

### ***Hosted solutions***

- Proxy-based scanning, not store-and-forward mail relay, means the hosted provider should never take ownership of the message, with the exception of spam quarantining. This is accomplished by acting as a proxy between sending server and receiving server, holding the connection open long enough to complete inspection of the message, then closing out the transaction, as appropriate.

### ***Mail server protection***

In addition to having solid perimeter protection in place, it is still necessary to inspect internal mail traffic. There are many reasons why this is valuable:

- Scanning for viruses that enter through other vectors, such as personal Web-based email, removable media such as USBs, remote laptop users whose virus definitions are not current, and more.
- Preventing authorized content from being sent to unauthorized users.
- Preventing unwanted or oversized content from being sent through the internal mail system.
- Post-attack, performing virus clean-up of message stores using the latest antivirus definitions.
- Retroactive cleaning of 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®, should 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 to conduct sweeps of message store content based on updated virus definitions or specific content rules designed to identify suspicious or inappropriate content.

In the case of many viral threats, the initial outbreak stage leaves the company open to infection, as emails enter the message store, where new infections are not yet detected by the current definitions. Once definitions have been updated, it is important to run periodic scans of the message store to eliminate any malicious content and to protect users from exposure.

### Step 2—Archiving

As the business use email as a business application, companies are increasingly aware that email systems were never designed to store the amount of data that goes through the typical messaging system today. Some companies are further being asked to retain even more email than before—to comply with external regulations, adhere to internal policies, or prepare for possible legal discovery requests.

Nearly every email administrator understands the first problem—storage management for email. Email continues to arrive every day, and the volume grows dramatically from year to year. The impact on this growth to the email environment is:

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

To “solve” this problem, most IT organizations implement email quotas, restricting their users to a fixed amount of email storage (typically 25 MB to 200 MB). However, in many ways this simply shifts the problem rather than truly addressing it:

- Users must constantly ensure their email storage is below the quota and store their excess messages in separate files (e.g., .PST files on Microsoft Exchange or .NSF files on Domino)
- In many cases, these files are kept on the network file servers and thus still use storage and backup resources
- Furthermore, these files are highly susceptible to corruption and the same availability and performance problems seen on email servers
- Finally, if users store these files on their local desktops or laptops, which are often not backed up, company-critical data becomes subject to loss or theft

This is all in addition to the fact that email quotas affect user productivity, result in large numbers of support calls, and are one of the burdens of email management.

## Email Security and Availability

The real solution to this problem is to provide 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 allow 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.
- 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 to reduce the volume of information while leveraging more cost-effectively disk or tape storage for archived data.
- Allow end users to seamlessly access messages and attachments from the archive just as they access normal email.
- Index the messages and attachments so that end users can search through the (eventually large) archives of their email over time.

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

However, message archiving is not simply about storage management. Many companies view archiving as a general best practice in information management—a way to preserve critical company information based upon business needs.

Many companies that are subject to potential litigation now realize that email is a legally discoverable record and that, if forced into a lawsuit, companies are often required to produce email for the courts. It is simply not acceptable to tell a judge that email was deleted; in many cases, this can lead to fines or sanctions against the company in question.

Furthermore, the old method of producing email (by restoring data from tapes) is often cost-prohibitive and time-consuming. In many cases, manual tape restoration costs \$2,000 to \$5,000 per tape, resulting in total charges in typical litigation cases exceeding \$200,000 per case. For companies in highly litigious industries such as consumer products, this is untenable.

Companies are also being forced by external regulations to retain email. Regulations such as the Securities and Exchange Commission Rule 17(a)–4(f) in the U.S. specify that, for certain

## Email Security and Availability

companies, email must be retained specifically on non-erasable media for long periods of time. And increasingly, companies want to be prepared for the next regulation or legal interpretation, rather than having to scramble to react.

Finally, organizations are realizing that regardless of external forces, it is simply a “best practice” to control information and preserve it. Email has become the source and destination of the lion’s share of company intellectual property. Because of this, companies want to retain email for internal purposes—whether to be able to search it later or simply so they can monitor it for inappropriate usage or company policy violations.

In this way, the ideal message archiving solution will further enable the following:

- Automatic archiving of “journaled” email so that the email is guaranteed to be captured
- Indexing of the information as it is archived to facilitate future discovery
- Secure search capabilities across the organization, allowing authorized personnel to perform company-wide information requests
- Specialized tools to assist in the capture, search, and review processes of legal discovery
- Sampling and workflow around regulated supervision of employee email

Setting spam and viruses aside, email and other corporate intellectual property can consume 30–50% of corporate storage resources. Left unmanaged, this can literally cost millions of dollars per year in storage and administration. Content archiving takes control of managing older content to enable:

- Lower total cost of ownership of frontline mail environments
- Instant search and retrieval of content by users
- Compliance with legal and corporate retention requirements
- Faster platform migrations
- Increased server consolidation and storage optimization

### Step 3—Building a resilient foundation

Equal in importance to maintaining the security and availability of email information is the need to build the email infrastructure on a resilient foundation – one that is robust in its ability to meet growing demands, resistant to failure, and able to quickly recover when failure occurs. Many corporations have opportunities to plan for infrastructure that supports future needs of the business growth, such as when they need to migrate to new version of messaging servers or when they consider consolidation of servers.

When considering how to build infrastructure that has higher availability for email:

- Email administrators must identify, understand and respond to a large range of problems that could disrupt email access. They need to monitor and react to potential outages automatically, according to well-defined response policies.
- The business needs the ability to keep functioning and communicating in the face of a disaster. It is critical to have well-defined plans and steps to recover the system, as well as the technologies to protect data and systems and minimize downtime and disruption.
- IT organizations need to proactively maintain, upgrade, and otherwise manage the various IT infrastructure components that contribute to service delivery, including server operating systems, network components, and storage systems.

One of the keys to addressing availability in the email infrastructure starts with ensuring protection of the data via a proven backup and recovery solution. Enterprise level backup solutions need to deliver high performance data protection that scales to protect the largest environments.

To minimize the business disruption and protect data, backup software must offer a single management tool to consolidate all backup and recovery operations, while providing cutting-edge management, alerting, reporting, and troubleshooting technologies. It is also important that organizations take advantage of both tape and disk storage with its advances in disk and snapshot-based protection, off-site media management, and automated disaster recover. To reduce the impact on business critical systems, organizations need to look at online database and application aware backup and recovery for the specific messaging system that is used in email infrastructure.

Further, it is essential to protect the system from disruption. Such solutions, including VERITAS Bare Metal Restore, automate and streamline the server recovery process, making it unnecessary to manually reinstall operating systems or configure hardware. With simple commands, complete server and data restores can be accomplished in a fraction of the time without extensive training or tedious administration.

Another key area is to build a highly scalable storage management environment. Rather than relying on traditional, time consuming and expensive methods of scaling—i.e. by adding additional servers or disk space as performance gets impacted or space runs out with the increase of email data—it's important to begin to view your email environment more holistically as a system of unified and available resources that can be leveraged and shared across the entire messaging network.

Storage management and clustering software are the key technologies that should be employed for building this scalable email infrastructure. They allow ever-increasing demands to be met, not simply by adding more systems or volumes, but by intelligently identifying and utilizing existing, untapped resources in the environment, ultimately maximizing the value of total cost of ownership around the email environment.

Through the right storage management solution, administrators are also able to perform nearly all storage-related tasks online (such as RAID reconfiguration, defragmentation, file system resizing and volume resizing), without having to take storage offline to perform these regular maintenance functions, thus not causing impact to business operations.

Also, clustering technology should be able to mirror data for redundancy and automatically migrate data from failing disks to healthy disks to cut downtime from unplanned events, or to quickly move an application from a failed server to a healthy server.

## Introducing Email Security and Availability from Symantec

By combining products and services with VERITAS, the leader in availability solutions, the new Symantec is now able to offer a comprehensive solution that enables Email Security and Availability. These unique technologies and services control and manage the flow of email information from start to finish, helping protect an organization against risks, ensuring uptime of systems and users, satisfying compliance and document retention requirements while at the same time minimizing the total cost of ownership for email. Here is how Symantec's technology and service offerings map to the layered approach described earlier.

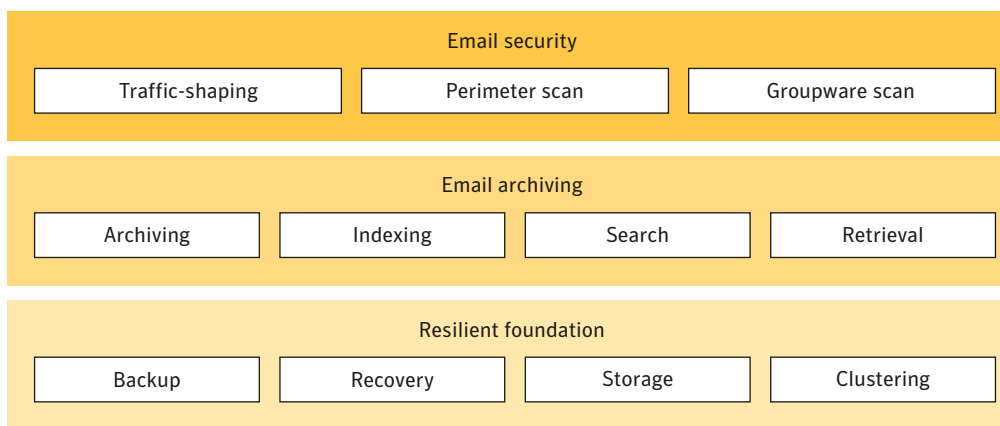


Figure 1: Symantec's email security and availability approach

### Email security

Email security is comprised of three key elements: volume reduction, perimeter protection, and groupware protection. But before discussing each layer of protection, it is important to understand how Symantec can be on top of the ever-changing security threat landscape and help customers be protected from email-borne threats.

### Symantec's Global Intelligence Network and Security Response

At the heart of Symantec's organization is the industry leading scalable security research infrastructure—the Symantec Global Intelligence Network—that aggregates, analyzes, and delivers timely security notifications on security threats worldwide. Symantec Global Intelligence Network gathers malicious code data from over 150 million antivirus desktop, 20,000 Intrusion Detection (IDS) software, firewall sensors in over 180 different countries with over 43,000 managed security

devices. Symantec's global Security Response Centers monitor Probe Network, an extensive array of over 2 million decoy email addresses and analyze latest spamming tactics across the globe. Combined with Symantec's vulnerability database of over 10,500 entries, this infrastructure provides Symantec's Security Response analysts an unparalleled source of data with which to identify emerging trends in attacks and malicious code activity. Symantec Security Response centers—located in North America, Asia, Australia, China, and Europe—are manned by researchers who represent a cross section of the most highly regarded security experts in the industry, offering customers 24x7 coverage for important security events. The diversity of threats and security risks handled by the Symantec Security Response analysts place it at the forefront of security research.

Symantec™ Mail Security product line leverages Symantec Security Response's timely security content updates to help organizations proactively predict and respond to any security threats. Powered by the Symantec's Global Intelligence Network and Security Response, information and recommended actions on the latest security threats can be updated via Symantec's robust, distributed network of LiveUpdate™ systems worldwide, reaching all customers, regardless of geographic location or time zone.

### ***Volume reduction***

#### **Symantec™ Mail Security 8100 Series appliance**

As discussed earlier in this paper, the first line of defense for unwanted email content should occur outside of the messaging infrastructure, before the data can impact internal servers, including the SMTP mail gateways. In Symantec's Email Security and Availability solution, that first line of defense is the Symantec Mail Security 8100 Series appliance.

The Symantec Mail Security 8100 Series appliance employs a unique approach to spam deterrence by evaluating sender reputation and using traffic-shaping on the inbound SMTP stream. It samples and analyzes SMTP packets in real time, makes a determination about a sender's "reputation," then applies traffic-shaping to deter "unwanted" senders from continuing to send unwanted content to the protected company's network. "Sender reputation," in this sense, comes down to whether the sending server (determined by IP addresses) sends "legitimate" email or mostly spam email.

Unlike typical gateway antispam scanners, the Symantec Mail Security 8100 Series appliance does not take any action on individual emails, but rather on the cumulative history and reputation of the mail path itself. The result is that it uses a large number of statistical inputs to determine a reputation and, once established, applies "traffic-shaping" to the sender's connection. This

means a spam sender is assigned a painfully slow connection to the protected environment, which makes sending emails to that environment not very cost-effective.

Ironically, rather than the spammer being able to tie up the system resources and bandwidth of a legitimate environment, the spammer's resources are tied up trying to send to the environment, but at negligible resource cost for the customer. The net result is that the customer's mail servers appear to be on the verge of collapse, and the spammer will drop the domain as a future destination for spam messages, thereby reducing the spam volume significantly.

### **The benefits of the Symantec Mail Security 8100 Series appliance**

Considering that 60–70% of incoming email is spam, the practice of traffic-shaping translates to a 50% reduction in overall email volume, without risk of actual mail loss. As a result, there's a corresponding reduction in messages that:

- Need to be processed by downstream email scanners and gateways
- Are stored in expensive, volume-sensitive message stores
- Require reviewing by end users through a spam quarantine
- Need to be archived, should there be legal requirements to archive all received email, including spam, for a set period of time

These significant volume reductions can further translate into savings in the overall number and size of servers required to scale to the problem, including gateway scanning devices and mail servers. In practical terms, reducing spam from 70% of traffic to less than 20% is like turning the clock back on spam to about the year 2000. At a bare minimum, it will improve overall performance and scalability of existing systems, and ease the burden on back-end systems and users.

The next step in the process of achieving Email Security and Availability is to focus on perimeter protection.

### ***Protect the perimeter***

Symantec's perimeter solutions span across the key form factors (software, appliance, and hosted solutions) as well as across key operating systems (Windows, Solaris, and Linux), thereby offering flexibility in choosing the right fit for the needs of every organization.

In addition, the following are common to all Symantec solution offerings:

- Symantec's industry-leading antispam technologies and response, which offer a 95% effectiveness rate (Source: eWeek 2003) and an accuracy of 99.9999% (Source: Yankee Group Report 2004), achieved through over 20 filtering technologies, its global BLOC (Source: Brightmail Logistics and Operations Centers) response infrastructure, and frequent 5- to 10-minute update intervals. In addition, Sender Reputation Lists leverage the Probe Network™ to identify known spam sources on the Internet to provide added certainty along with a stacked classification verdict system
- Symantec's award-winning NAVEX™ antivirus technologies and response, which ensures consistent virus protection and updating across all supported platforms, using multiple detection technologies, including heuristics, and is supported by our global Symantec™ Security Response operations centers, with both scheduled and on-demand updating on a weekly, daily, and hourly basis
- 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 based on customizable rules for attachment name and extension or by message size, subject line, and message body content to assist in stopping early-hour attacks or to prevent the transmission of unwanted or inappropriate email content
- The flexibility to treat spam differently based on antispam engine verdict, i.e.. deleting "spam" messages, but quarantining "suspected spam" messages for further review
- Symantec's Web-based Spam Quarantine, which removes spam messages from the messaging environment, yet makes them available to administrators and end users for further processing and review

### **The benefits of Symantec's perimeter protection**

As the second line of defense after the Symantec Mail Security 8100 Series appliance, Symantec's appliance and software-based perimeter solutions offer the following benefits:

- Harmful Internet email-borne content doesn't reach end-user desktops, spread infection, or disrupt the network
- Significantly fewer unwanted messages enter the downstream mail environment
- With flexible spam handling and high accuracy, fewer messages require end-user review
- Fewer non-business emails are archived

Clearly, applying a further 95% reduction on the remaining spam volumes minimizes the negative impact on downstream message stores, archives, and end users. In addition, removing mass-mailer worm emails can limit the volume spikes caused by these attacks and prevent additional unwanted data from clogging message stores and inboxes. The perimeter protection layer is clearly one of the most critical layers in enhancing network security and improving the availability of email.

### ***Protect the groupware environment***

Where Symantec's perimeter protection plays a key role in minimizing the negative impacts of Internet email traffic, Symantec™ Mail Security for Microsoft® Exchange and Symantec™ Mail Security for Domino® ensure that internal message traffic is also free of malicious or inappropriate content.

Both solutions are tightly integrated into their respective mail environments, using vendor-supported APIs and ensuring maximum capability and minimum conflicts with the underlying messaging architecture.

Similar to our perimeter protection solutions, Symantec Mail Security for Exchange and for Domino leverage the same core antivirus technology and response, as well as updating flexibility. For smaller organizations, or even some larger organizations that have standardized from mail server to gateway using either a Domino or an Exchange infrastructure, there's an added option of enabling the same antispam technologies and response as used in the perimeter protection solutions, providing the flexibility in deployment required by diverse organizations.

In addition to core scanning services, Symantec Mail Security for Microsoft Exchange and for Domino offer similar content inspection capabilities, such as subject line and message body filtering, attachment stripping, and restrictions on message size. Such capabilities can be used

to enforce email usage policies as well as minimize exposure to regulatory penalties or even lawsuits due to inappropriate content being sent through internal email.

### ***The benefits of Symantec groupware protection***

This third layer in the Email Security and Availability solution further contributes to data reduction by eliminating unwanted, internally sent content, and early-stage mass-mailer worm messages.

It is particularly well-suited for the early-stage real-time detection of email policy violations, such as sending inappropriate or unauthorized content to internal or external users.

Following this final stage of message store scanning and cleansing, archiving systems can then add its value to the Email Security and Availability chain.

### **Availability through archiving**

Symantec Enterprise Vault is the industry-leading solution for automatically and seamlessly archiving, indexing, searching, and retrieving information, while keeping Microsoft® Exchange servers running at optimal efficiency and providing users with easy access to their archived data. Enterprise Vault provides the following functionality:

- **Store**—Automatically move email, file system, Microsoft SharePoint®, and instant messaging content from expensive operational storage locations to a more cost-effective online vault, without impacting end-user access to the data. Users can access archived information directly from their email client such as Outlook or Web browser and can even access it while offline, using the optional Offline Vault option. IT can also automatically discover, collect, migrate, and eliminate PST files by moving the content to the vault. In addition to Microsoft Exchange mailboxes, Enterprise Vault can also archive Exchange Journals and Public Folders.
- **Manage**—Archived data is automatically compressed, duplicate copies are removed, and data is retained based upon business policies. Data can be migrated over time to tertiary storage, including tape repositories managed by Symantec NetBackup.
- **Discover**—End users, compliance departments, legal professionals, and corporate risk management functions can securely search through messages, files, and attachments with minimal effort. In addition, legal departments can manage the process of legal discovery review through the optional Discovery Accelerator, while compliance officers can supervise employee communications through the Compliance Accelerator module.

### ***The benefits of Symantec's Enterprise Vault***

As described previously, message archiving solutions provide benefits in three core areas:

- **Increased email availability**—Enterprise Vault reduces the amount of data stored in primary messaging servers and file servers, reducing corruption and performance problems that are observed when these servers reach capacity thresholds. Furthermore, by archiving data, preserving access to it for long-term retention, and providing search capabilities, end-user access to data is retained.
- **Reduced email costs**—Enterprise Vault reduces costs throughout the email environment. First, by archiving older or less frequently accessed data to less expensive storage, Enterprise Vault reduces primary storage costs in the environment. Perhaps more importantly, backup costs are then reduced because the static, archived data no longer has to be frequently backed up. IT reduces support costs through elimination of PST files and email quotas, while reducing migration cost and time by reducing the amount of data to be moved in transitioning to a new version of Microsoft Exchange or consolidating email servers, for example.
- **Controlled email risk**—By retaining email based upon business policies, Enterprise Vault also allows organizations to address concerns around regulatory or internal risk. This includes reducing risk associated with not being able to produce information for litigation, reducing risk of non-compliance with data retention regulations, or reducing risk of unauthorized employee communications.

### **Symantec's solution for a resilient email foundation**

#### ***Data protection***

The need to recover data is critical in any email environment, whether due to a system outage or other unplanned event. As was discussed earlier in this paper, a majority of mission-critical data can reside in the email infrastructure. VERITAS NetBackup can be used for backup and recovery of the information in an Exchange or Notes® environment.

NetBackup™ for Microsoft Exchange Server simplifies database backup and recovery without taking the Exchange server offline or disrupting local or remote systems. A multi-level backup and recovery approach ensures continued availability of Exchange services and data during backups. Central administration, automation options, and support for all popular storage devices create the flexibility administrators need to maximize performance.

NetBackup™ for Lotus Notes provides high performance backup and recovery of Lotus Notes/Domino environments. Lotus services and data remain available during backup because the database is not taken offline. Administrators may schedule automatic, unattended backups for local or remote Lotus Notes® clients across the network and can backup and restore at the database and transaction log level.

NetBackup provides:

- Complete, non-disruptive protection of Exchange database and mailbox components, including incremental mailbox backup.
- Backup method flexibility for scheduled, unattended backups.
- Rapid, granular recovery of databases and mailboxes, including support for performing individual message restores.
- Advanced features, including Single Instance Store (SIS), global exclusion, and storage group multiplexing. Volume Shadow Copy Services (VSS) integration and off-host backups are available when combined with the NetBackup™ Advanced Client.
- Alternate restoration techniques allowing Lotus data restoration to either an alternate system or an alternate directory.
- Advanced Lotus integration support for partitioned Lotus servers and Lotus clustering.

### ***Benefits of Symantec (VERITAS) NetBackup***

As the recognized leader for enterprise-class backup and recovery, VERITAS NetBackup is designed to help provide complete data protection for the most complex UNIX, Windows, Linux and NetWare® environments. Intuitive graphical user interfaces help enable organizations to manage all aspects of backup and recovery and to help maintain consistent backup policies that are deployed across the enterprise. VERITAS NetBackup software provides database- and application-aware backup and recovery solutions for Oracle®, IBM® DB2, UDB, Microsoft® SQL Server, Microsoft Exchange Server, Microsoft SharePoint Portal Server, SAP NetWeaver, Sybase, Informix and Lotus Notes and Domino Server.

### Product highlights

- **End-To-End Data Protection**—Data protection for all environments, from desktop to datacenter to vault.
- **Single Solution for All Platforms**—NetBackup helps you consolidate and standardize your backup and recovery operations, protecting all major UNIX variants, Windows, Linux, and NetWare systems.
- **Unlimited Scalability**—Centralized management and control, high-performance technology and a flexible multi-tier architecture enable NetBackup software to adapt to the growing needs of the modern data center.
- **Unparalleled Performance**—Synthetic backups consume less network bandwidth and decrease the impact on the application host since files are backed up only once. Multiplexing up to 32 different data streams to a single tape drive helps to realize the maximum rated throughput of your storage hardware.
- **Management and Reporting**—The NetBackup Operations Manager delivers web based management and reporting for large NetBackup enterprise users. Provides real-time monitoring, historical reporting, administration, alert management and troubleshooting assistance.
- **Advanced Data Protection**—Perform low impact, high performance backup and restores with the NetBackup Advanced Client. This consolidated suite of snapshot-based technologies enables FlashBackup, Instant Recovery, Offhost and Block-Level Incremental data protection.
- **Automate Disaster Recovery**—The NetBackup Vault option automates the disaster recovery process by helping to simplify tape rotation and the creation and management of tape duplicates for offsite vaulting. NetBackup Bare Metal Restore streamlines the server recovery process. NetBackup Administration Console provides a single point of management that enables backup administrators to manage a larger number of servers more efficiently.
- **Extensive Media Management**—Allows users to share an automated tape library between heterogeneous systems—UNIX, Windows, Linux, NetWare or network attached storage (NAS)—allowing NetBackup users to more effectively leverage their expensive tape and drive resources.

- **Security**—Secure your backup data by selecting from NetBackup software's 40-, 56-, 128-, or 256-bit encryption. NetBackup software's low-impact encryption option ensures the data is secure before it leaves the client. NetBackup Access Control offers the flexibility to restrict or provide specific access levels to NetBackup software's administrative functionality.
- **Storage Networking**—NetBackup software supports a broad range of tape library, tape drive and Storage Area Network (SAN) interconnect technologies from leading vendors. Dynamically share individual tape drives over SCSI or a SAN, or utilize the optional NetBackup for NDMP agent to help protect popular network attached storage (NAS) devices.

### ***Storage management and clustering***

Symantec (VERITAS) Storage Foundation High Availability (HA) for Windows extends the native data management capabilities of Windows® 2000 and Windows Server 2003. The resulting logical disk/volume capabilities provide the basis for a highly scalable storage environment for Microsoft Exchange. Further, Global Cluster and Volume Replicator ensures recovery of the Exchange infrastructure.

Rapid storage growth is a fact of life for most Exchange implementations. Storage Foundation HA for Windows offers a modular approach to addressing the wide range of potential threats to email availability. Organizations can implement the different components in a phased approach or depending on their specific needs. Using VERITAS Storage Foundation HA for Windows, you can create a highly available, resilient storage environment by:

- Creating storage that automatically expands to meet growing data needs (such as a storage volume for a transaction log).
- Designing storage configurations that use mirroring or mirroring/striping combinations to protect from the loss of a single disk.
- Identifying and addressing storage “hotspots” that slow overall application performance.
- Creating point-in-time images for rapid recovery from logical errors or data corruption.

To protect the Exchange infrastructure from site-wide disasters, Global Cluster and Volume Replicator options can be used to create a disaster recovery environment that enables the fast failover of the entire Exchange environment (or an entire data center). Because the secondary, disaster recovery site does not need to match the primary site exactly and can be used for other purposes, companies can leverage DR investments and control the costs of supporting disaster recovery by:

- Using lower-cost or lower-capacity storage at the off-site recovery location.
- Using a single data center as an off-site recovery location for multiple other data center locations.
- Using the recovery site to run non-critical services, such as development and testing, that can be interrupted, stopped and replaced with critical applications in case of a global failover. The following sections discuss how to use the Storage Foundation HA for Windows to specifically address different types of threats to Exchange availability.

However, you cannot protect Exchange data from all sources of logical errors. Data corruption, user errors, and viruses all present risks that are nearly impossible to eliminate. The best defense is to undo the effect of these errors quickly and effectively, with minimal data loss. VERITAS Storage Foundation offers another alternative: point-in-time snapshots of Exchange databases and transaction log files using the FlashSnap option. A FlashSnap snapshot is an independently-addressable volume that mirrors the production volumes. By splitting the mirror, the FlashSnap option creates a point-in-time image of the data that can be used as a backup source, offloading the backup process from the production environment, or can be used to create quick recovery images.

Organizations can protect Exchange environments from a wide range of component failures by implementing local and campus clustering for availability. Storage Foundation HA for Windows integrates VERITAS Cluster Server (VCS) technology, which provides highly flexible, scalable failover clustering with workload management capabilities. In a VCS cluster, multiple servers are linked with shared storage and private Ethernet heartbeats. Each system in the cluster can access the storage of any other system.

For business continuity in the face of a broader disruption, the best protection is the ability to resume operations, nearly instantly and without data loss, at an alternate site located a significant distance from the primary site. Using Storage Foundation with the Global Cluster and Volume Replicator options, you can replicate data between two separated sites, and switch application services between them with a single mouse click.

## Email Security and Availability

The combination of VERITAS NetBackup and Storage Foundation HA for Windows (with Global Cluster and Replication options) offers organizations that depend on Microsoft Exchange a single solution for building a resilient email foundation.

### **Key benefits of Storage Foundation HA:**

- Maximize uptime of messaging data and applications
- Reduce planned or unplanned downtime
- Enable high availability solution for local, metropolitan or global clustering from within a single product
- Ability to test disaster recovery solution without impacting production applications
- Optimize and plan cluster configuration and policies through portable modeling and simulation tool

### **Conclusion**

In most organizations today, the email environment has become the heart of its operations. And the health and well-being of that heart can affect end-user productivity, as well as the ability of the business to function and thrive. Over the last few years, the arteries of email have become literally clogged by spam, viruses, and anything else that can be sent by email. Its very viability is put at risk by the kinds of things that are fed into it. Email Security and Availability is the path to recovery for email, by reducing the intake of unwanted and potentially dangerous content before it enters the system, while at the same time exercising its stores and taking off excess weight that can cause further palpitations or even failure.

Symantec's Email Security and Availability solutions are unique in their ability to reduce risk to email systems and data, and to ensure uptime and performance of both systems and users of email while satisfying regulatory and corporate policy requirements. Especially important is the impact Symantec's solutions have on lowering the overall costs of ownership by significantly reducing the burden at all layers of the email infrastructure, including storage costs and the operational costs associated with attempting to scale infrastructure and maximize the performance. Flexible deployment options across a range of form factors, integration points, and operating environments allow companies to tailor solutions to their needs, rather than to shop for point solutions from multiple vendors. Achieving higher levels of security and availability around the mission-critical business application is the key to building the resilient infrastructure that enables corporations to keep their business up, running and growing.

## 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](http://www.symantec.com).

Symantec has worldwide operations in more than 40 countries. 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  
408 517 8000  
800 721 3934  
[www.symantec.com](http://www.symantec.com)

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Live Update, Symantec Mail Security, Symantec Mail Security 8100 Series, Symantec Mail Security for Domino, Symantec Mail Security for Microsoft Exchange, and Symantec Security Response are trademarks of Symantec Corporation. Domino, IBM, Lotus Notes, and Notes are trademarks of International Business Machines Corporation in the United States, other countries, or both. Microsoft, Microsoft Exchange, Microsoft SharePoint, Windows, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Netware is a registered trademark of Novell, Inc., in the United States and other countries. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Solaris is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries. Other brand and product names are trademarks of their respective holder(s). Any technical information that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. The technical information is being delivered to you as-is and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at the risk of the user. Copyright © 2005 Symantec Corporation. All rights reserved.  
07/05 10429770