

I D C V E N D O R S P O T L I G H T

Email Security and Availability: A Holistic Solution to a Critical Problem

August 2005

Adapted from *Worldwide Secure Content Management 2004–2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security* by Brian E. Burke, IDC #31598

Sponsored by Symantec

Email has grown up very rapidly in the past decade and is now considered to be a mission-critical application for conducting business. By extension, email has become indispensable as a repository of information and as a legal record. Paralleling email's growth in importance is the growth of threats to email security and availability. Spam, for example, is no longer considered a nuisance but a full-blown assault on information availability and business productivity. Viruses also continue to plague organizations' ability to maintain secure environments and can further reduce systems and network availability. Moreover, companies increasingly need to monitor and secure outbound messaging traffic to comply with both external regulatory requirements and internal corporate policies and best practices. Threats as well as regulatory demands are compelling companies to rethink their former patchwork-quilt approach to email infrastructure. This document identifies the current drivers for email security and availability, describes an "information integrity" strategy for building a resilient email infrastructure, and evaluates the role of Symantec in this market.

Email and Its Enemies

Email remains the dominant form of electronic communication and collaboration for business, but three market factors are affecting usage:

- Rising torrents of spam are reducing the usefulness of email by forcing users and IT staff to expend additional time and energy to identify and delete spam and prevent the associated reduction in productivity. Internet service providers and antispam solution vendors report that spam represented 50–95% of all inbound Internet email in 2004, somewhat higher than 2003 levels, and triple the reported 2002 levels of 15–30%. When internal business email is included in the calculation, IDC estimates that spam represented 38% of all email sent on an average day in North America in 2004.
- Viruses and related threats continue to pose major risks to enterprise security and data integrity. Malicious infection, from external and internal sources, continues to be a growing problem. In addition, spyware is increasingly attracting attention from corporate security departments, particularly when it monitors keystrokes, scans files, and snoops email. As such, organizations continue to invest heavily in antivirus software, driving market growth of more than 21% from 2002 to 2003 alone. According to a 2004 IDC survey of 600 firms across North America, 31% of respondents indicated viruses, Trojans, and malicious code as the single greatest threat, and another 10% indicated network worms as the greatest threat. Spyware ranked fourth on the list of single greatest threats in 2004, showing clear movement up the priority list of corporate security concerns.

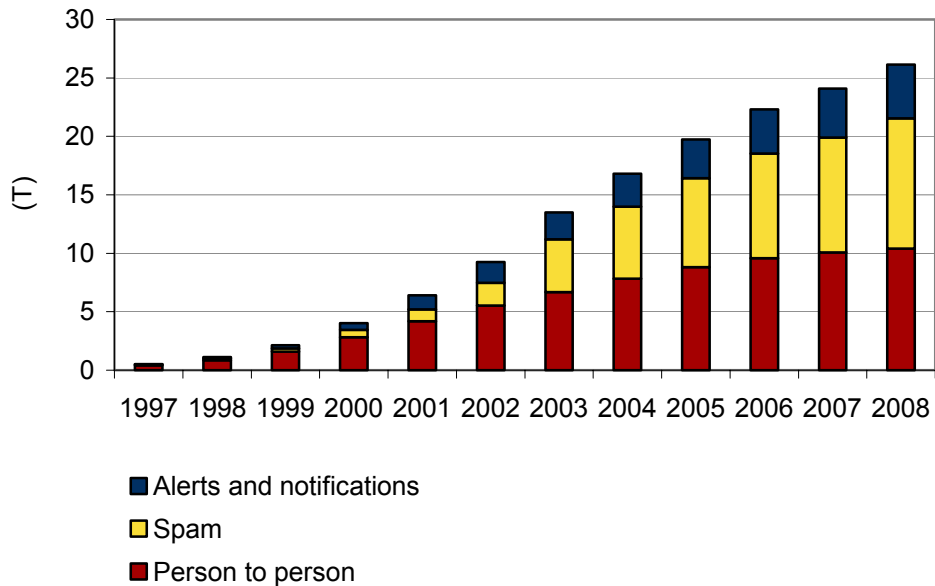
- The cost of storing and managing email throughout its life cycle is rising dramatically as the need to comply with email retention policies dictated by government and industry regulations and business requirements continues to expand. This is on top of the rising volume of all types of email. The size of business email volumes sent annually worldwide increased by 47% from 2003 and more than doubled from 2002 levels (1 petabyte [PB] = 1 million gigabytes = 1 billion megabytes). With IT departments looking to lower technology and operating costs in general, and in the case of mature systems such as email in particular, these emerging needs provide real monetary incentives for organizations to make email more efficient and cost-effective.

In addition, IDC sees a disturbing trend: the convergence of spam and viruses. In the past, spammers traditionally sent spam from their own ISP accounts. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to new methods to conceal their identities. Some spammers are starting to resort to outright criminality in their efforts to conceal the sources of their spam messages, using Trojan horses to turn the computers of innocent consumers and corporate users into secret spam engines. The explosive growth of cable modems and broadband connections has left consumers and remote employees open to attack. In many cases, their computers are being used as a relay for sending spam to thousands of other people. The SoBig virus is a good example of the convergence of spam and viruses.

Despite the harm that spam and viruses have caused, the associated storage burdens from these threats, and the need for regulatory compliance, email still has a reputation as a reliable and efficient tool for communication and collaboration. IDC expects email to become an invaluable collaborative tool over the next several years (see Figure 1). This trend will drive organizations to continue seeking more efficient and economical ways of managing, storing, archiving, and retrieving email files. In addition, secure content management vendors will continue to seek ways to integrate antispam and antivirus applications into more comprehensive messaging security solutions in the near future.

Figure 1

Worldwide All Email Messages Sent Annually by Type of Email, 1997–2008



Note: Data includes person-to-person email, spam (all unsolicited bulk email, regardless of whether it is intercepted by antispam scanning products or services), and email alerts and notifications sent automatically (such as return receipts; undeliverable email notices; new content postings on intranets, portals, and virtual workspaces; project task completions; and status updates).

Source: IDC, 2005

Email as an End-to-End Process

Like other enterprise applications whose maturity has required increasing process control and tighter integration, email systems need to be viewed holistically. The two linchpin areas of a comprehensive email solution are the security and availability of email-based information and the resiliency of underlying systems and infrastructure.

Information security establishes significant, reliable, and automated data reductions throughout the messaging layers, removing spam, viruses, and other unwanted content from the messaging environment at the earliest point in time. Information and system availability establishes a resilient messaging infrastructure with a reduction and policy-based migration of older, authorized email from message stores and local PST files to more cost-effective storage; continuous backup of data and recovery of critical messaging systems; and a reduction of planned and unplanned downtime of data and servers.

A holistic view of enterprise email infrastructure reveals the complementary roles of these two areas:

- **Security.** Content filtering tools not only identify spam but also can be used to filter and monitor outbound communications for policy enforcement, regulatory compliance, and inappropriate content. Antivirus tools, including those that root out spyware, will continue to find and neutralize threats. The net result will be a reduction in risk and compliance violations. Added benefits will include an overall drop in email volume and a reduction in the number of resources and costs associated with managing and archiving email.
- **Availability.** Email management tools such as archiving and retention compliance software automatically migrate and manage older email. Backup, replication, disaster recovery, and storage management tools ensure the availability of email as well as enable the monitoring, searching, and retrieval of archived email for regulatory and corporate policy compliance. Not only are storage costs from growing data reduced, but email is more readily accessible for compliance and legal purposes. Also, end users have the ability to access archived email directly from their inbox folders so they no longer need to engage IT to find or recover aging email. The net result is a more resilient enterprise email system that minimizes disruptions and ensures business continuity.

IDC believes that to maximize the value of email in the coming years as well as to control the rising costs associated with managing email infrastructure, organizations need to look at email not as a point problem but as an end-to-end process that demands a comprehensive solution to ensure the security and availability of email information and the underlying systems.

Such a comprehensive solution should be an integral component of a larger information management strategy that entails specific messaging- and document-level information security technologies. IDC defines "information management" as the soundness, security, and incorruptibility of the content, images, or data found in business communications and digital media, including email as well as application files and documents.

A more holistic approach to email management will help organizations:

- Keep email (their mission-critical business application) up, running, and growing — regardless of the threat landscape
- Ensure that critical assets and information remain secure and accessible to the people who need them
- Protect network and users from risks and problems caused by unwanted or malicious email content
- Minimize the size of client and server email stores to maximize performance and uptime and reduce operational cost
- Ensure availability of historic email information for regulatory compliance and legal discovery
- Provide continuous backup and recovery of messaging data, servers, and sites
- Protect the messaging infrastructure itself against vulnerabilities and security threats

Symantec Profile

Symantec, a United States–based company founded in 1982, is a market leader in providing solutions to help individuals and enterprises ensure the security, availability, and integrity of their information. The Cupertino, California–based company held its initial public offering in June 1989 and today has operations in more than 40 countries, including global Security Response labs in the United States, Canada, New Zealand, Japan, and Australia. The company reported fiscal year 2005 earnings of \$2.6 billion. The most important strategic developments for the company of late have been the acquisition of Brightmail Inc. and the merger with VERITAS Software Corporation.

Symantec's \$370 million acquisition of Brightmail in June 2004, followed by the company's acquisition of TurnTide in July 2004, underscored the market reality that customers prefer to buy comprehensive messaging security solutions rather than point products. The acquisition of Brightmail allowed Symantec to pair its strong position in both the consumer and business security markets with Brightmail's early-to-market reputation as a technology leader in the enterprise antispam market and as an OEM partner. Brightmail's approach to fighting spam mirrors Symantec's view of combating viruses, adding additional global response infrastructure to the organization.

Symantec's recent merger with VERITAS in July 2005, in a deal valued at approximately \$11 billion, positions the merged entity as the fourth largest independent software company in the world and a major player in the infrastructure software market — particularly in email security and availability.

This merger furthers Symantec's Information Integrity vision toward the integration of security management and availability management to keep information secure and available. The merger, combined with other acquisitions, represents a significant investment in reaching the company's goal of providing software and services that offer greater information access with less risk.

VERITAS' product lines will augment Symantec's security infrastructure and management portfolio, and VERITAS' data protection, high availability, automation, and provisioning products will strengthen Symantec's capabilities to compete in this burgeoning market.

Like Symantec's recently announced email security and availability solution, the company's expanded product offerings will be able to address broader customer pains and challenges through integrated solutions for protection, filtering, archiving, retention, legal discovery, regulatory compliance, storage management, and backup and recovery of messages and information.

Challenges and Considerations

The rapid and dramatic expansion of Symantec's organization presents opportunities as well as challenges. Symantec has long been perceived as a consumer antivirus software vendor. Recent acquisitions and the merger with VERITAS continue to strengthen Symantec's capabilities to deliver on its holistic approach to enterprise security and information availability and will go a long way to change the public's perception of the company.

Most important, these acquisitions, and the merger with VERITAS in particular, have vaulted Symantec beyond its antivirus software heritage and placed it squarely in the enterprise information market. The merger provides Symantec with the product portfolio necessary to execute its ambitions to expand its addressable markets, with minimal overlap in product and service offerings.

As with all major mergers and acquisitions, it is critical for the merged entity to effectively integrate the respective organizations, as well as articulate the value proposition of an integrated Symantec-cum-VERITAS solution to its customers. Symantec will have to continue easing existing VERITAS customers' concerns regarding the support and future of VERITAS' products. While IDC hasn't seen many success cases of a merger of (almost) equals, and the potential pitfalls of such mergers are well documented in business literature, Symantec may well succeed in leveraging its purchase if it can execute on the following:

- Provide a synergistic product integration road map
- Develop a clear sales channel management strategy
- Retain critical staff
- Allay the concerns of VERITAS' customers around product support as well as upgrades and provide future product road maps

Conclusion

Increasing numbers of threats, including spam and viruses, are limiting the effectiveness of email by forcing enterprises and IT staff to expend additional time and energy to identify and mitigate these threats. The cost of storing and managing email throughout its life cycle is likewise rising, driven not only by spam and virus threats but also by growing volumes of all types of email and the need to comply with email retention regulations and business requirements. IDC believes messaging security technologies will continue to converge, and while some customers will continue to buy point solutions, these purchases will be the exception not the rule.

Going forward, IDC expects that enterprise customers will continue to gravitate toward solutions that address the convergence of system and network management with storage and security. If Symantec can successfully address its integration challenges on two fronts, organizational and technological, the company will be well positioned to capitalize on favorable demand-side forces for an end-to-end information integrity solution.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com