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

WHITE PAPER

The Evolution of Email Security: Symantec Brightmail Integrated Email Security Appliance

Sponsored by: Symantec

Brian E. Burke
January 2005

IDC OPINION

Email security is increasingly moving away from a focus on a single type of protection, such as antivirus, toward a focus on broad protection from a wide range of emerging threats to enterprise security. While antivirus software remains the foundation of email security, emerging threats are forcing organizations to approach email security with a more comprehensive solution. Corporate concerns about spam, viruses, worms, legal liability, regulatory compliance, and employee productivity are driving the need for a more complete solution. Moreover, there is an increasing need for integration between individual security technologies in order to reduce the cost and time associated with managing point products.

Key evolving challenges and threats regarding email security include:

- New viruses continue to employ blended threat techniques, exploiting multiple weaknesses and attacking through multiple methods (e.g., email, file transfers, and Web browsers). This forces organizations to purchase additional layers of antivirus and content security products that are being deployed the corporate gateway.

- IDC estimates the amount of spam being sent on an average day worldwide jumped from 4 billion in 2001 to 17 billion in 2004. Spam is quickly becoming both a potential legal liability and a major productivity and resource drain for corporate IT departments and users alike.

- Spam has grown from a nuisance to a major problem with rising costs in terms of lost email user and IT staff productivity, wasted network and storage resources, damage from viruses carried by spam, and liability for organizations not doing what they could to deal with the problem.

- Spyware is moving up the priority list of corporate security concerns. Spyware has the ability to monitor keystrokes, scan files on the hard drive, monitor other applications, install other spyware programs, read cookies, and change the default home page on the Web browser.

METHODOLOGY

IDC developed this bulletin using a combination of existing market forecasts and direct, in-depth, primary research. To gain insights into the challenges organizations face in managing multiple security technologies and to learn more about how Symantec's Mail Security solution set helps address these challenges, IDC conducted in-depth interviews with IT executives in various vertical industries. In addition IDC met with the Symantec team to review their goals and tactics. This report reflects all of these research perspectives.

SITUATION OVERVIEW

Evolving Threat Environment

Blended Threats

Blended threats are increasingly designed to get past point-solution security and target multiple vulnerabilities in clients and corporate networks. Unlike traditional viruses, which relied on the user to spread the infected files, blended threats are automated and are always scanning the Internet and local networks for vulnerabilities and other computers to infect; meaning they spread without user interaction. Moreover, the speed with which blended threats can spread has caused the effectiveness of point-solution security products to suffer. Recent malicious code incidents have achieved widespread propagation at rates significantly faster than many previous viruses. Worm propagation times have dropped from hours to minutes. One of the most destructive viruses of all time, the Melissa virus, took several days to spread all over the world. Today, viruses and worms need just hours or, in some cases, minutes to spread like wildfire across the world. With the rise of blended threats, there is an increasing need for integration between individual security components in order to reduce the cost and time associated with managing point products.

Blended threats are increasingly designed to get past point-solution security and target multiple vulnerabilities in clients and corporate networks.

Phishing Attacks

The recent incidents of phishing attacks on banks and their online customers have opened both consumer and corporate eyes to the increasing dangers of corporate identity theft. Phishing is clearly motivated by financial fraud and gain, and thus criminals are most often behind these attacks, rather than teenagers just trying to cause havoc. Phishing attacks use spoofed emails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, and social security numbers. IDC believes more sophisticated attackers, often from organized crime, will increasingly use phishing techniques to obtain credit card numbers, bank account information, corporate passwords, and other personal information to perpetrate identity theft. We believe the sophistication and scale of online frauds and identity thefts will continue to increase at a rapid pace.

Spyware

Spyware is no longer just a consumer nuisance; it is quickly becoming a major concern in the corporate environment. The fact that spyware can gather information about an employee or organization without their knowledge is causing corporate security departments to take notice. The more malicious type of spyware is often installed without the user's consent, as a drive-by download while web surfing, or as the result of clicking a URL link in a deceptive email. What concerns corporate security departments is that spyware can also be used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, and snoop email and other applications. Some of the more sophisticated spyware can even capture screenshots or turn on Webcams. A recent IDC survey of 600 North American organizations showed that spyware was indeed viewed as a serious threat to network security. Spyware was ranked as the fourth greatest threat to network security ahead of spam, hackers, and even cyberterrorism.

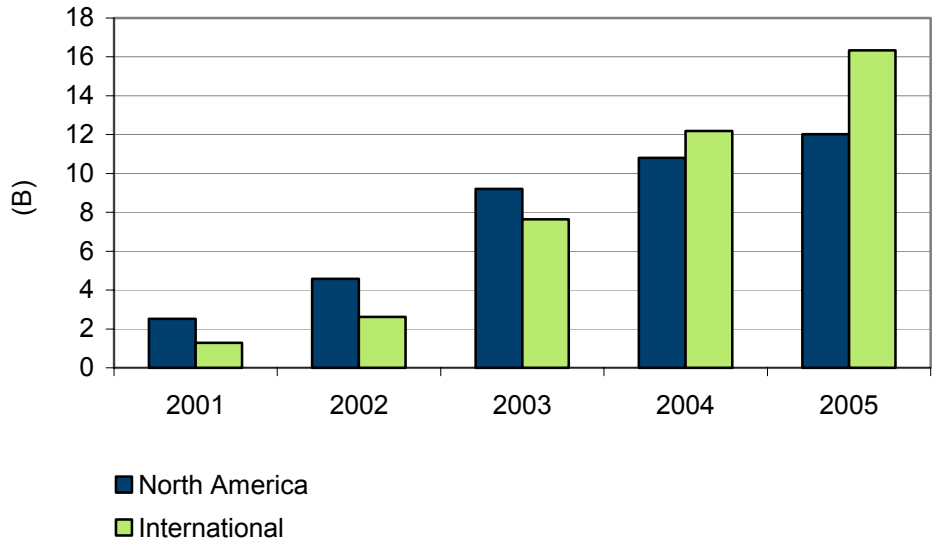
Growth of Spam

During the past two years, the volume of spam messages sent daily worldwide has jumped from 7 billion in 2002 to 23 billion in 2004, as shown in Figure 1. Internet service providers and antispam solution vendors report that spam currently represents 50–95% of all inbound Internet email, which is somewhat higher than in 2003 and triple the reported 2002 levels of 15–30%. When internal business email is included in the calculation, IDC estimates that spam represents 38% of all email sent on an average day in North America in 2004, up from 24% in 2002.

During the past two years, the volume of spam messages sent daily worldwide has jumped from 7 billion in 2002 to 23 billion in 2004

FIGURE 1

North America and International Spam Messages Sent Daily, 2001–2005



Source: IDC's Spam Study, 2003 (IT Results)

The Convergence of Spam and Virus

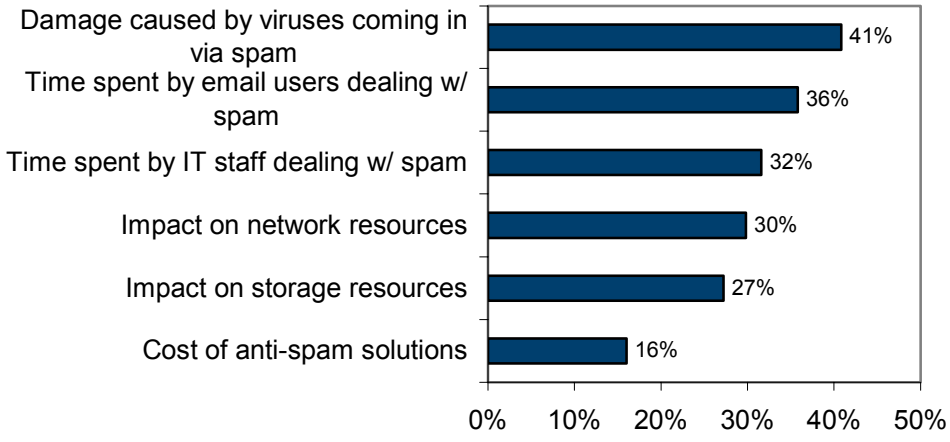
IDC's recent security survey showed that time spent due to damage caused by viruses coming in via spam is the biggest cost impact felt by organizations

Spam is increasingly viewed as a security threat, because it can carry viruses, malicious code, and fraudulent solicitations for privacy information. In fact, IDC's recent security survey showed that time spent due to damage caused by viruses coming in via spam is the biggest cost impact felt by organizations, as shown in Figure 2. IDC believes worms and viruses are increasingly using spam techniques — not just the exploitation of unprotected mail relays to maximize spread, but also the use of social engineering to trick victims into opening malicious files. In some cases senders of unsolicited commercial email (spammers) are also resorting to outright criminality in their efforts to conceal the sources of their ill-sent missives, using Trojan horses to turn the computers of innocent consumers and corporate employees into secret spam zombies. Spammers traditionally sent spam from their own ISP account. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to virus and trojan techniques to conceal their true identity.

FIGURE 2

Factors impacting the cost of Spam

Q: On a scale of 1 to 5, please rate the cost impact the following have had on your organization
Top 2 responses represented: high [4] and very high[5]



Source: IDC's Spam Study, 2003 (IT Results)

Regulatory Compliance

The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly more critical. Government and industry regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley have placed unprecedented pressure on corporations to secure the use of their electronic communications. In many cases in which the original intent was to address a regulatory issue, the security aspect represents part of the solution. Organizations are faced with the complex task of complying with various regulations and making sure that employees do not inadvertently, or deliberately, break the law.

Government and industry regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley have placed unprecedented pressure on corporations to secure the use of their electronic communications

Each of these regulations can carry criminal penalties and/or civil penalties. Criminal means criminal prosecution of individuals as well as substantial fines. Successful criminal convictions generally lead to civil lawsuits. Civil lawsuits (especially in class action situations) can carry substantial financial penalties and damage a company's reputation with its customers. Although many regulations only fall into the civil area and would seem "toothless," the fact that they permit class action suits creates major opportunities for the legal community, especially in today's litigious society.

STEPS FOR STRONGER EMAIL SECURITY

Integrated Security Appliances

Security appliances rank among the fastest-growing segments of the worldwide IT security market. Because appliances can lower costs, ease administrative overheads, facilitate management, consolidate support, and scale efficiently, their success is not surprising. Appliances have become popular by being a simple means of delivering security software, so much so that appliance products can be found that cover many different security applications. By 2007, 80% of all gateway security solutions will be delivered via a dedicated appliance.

Security appliances rank among the fastest-growing segments of the worldwide IT security market

Why are people buying security appliances when so many excellent software-based security applications are already on the market? Simply put, convenience and ease of installation are the key advantages of security appliances. The following outline the factors that have encouraged the growth of the threat management security appliance:

- **Reduced complexity.** The all-in-one approach simplifies product selection, product integration, and ongoing support.
- **Avoidance of software installation and proliferating servers.** Customers — or more often VARs, VADs, or MSPs — can easily install and maintain the products. Increasingly, this process is handled remotely.
- **Install and forget.** The appliances are generally plug and play, with very little installation required.

- **Synergy with high-end software solutions.** Appliances are used in remote sites where an enterprise does not have security professionals on the ground. A plug-and-play appliance can be installed and then managed remotely. This management is synergistic with large, centralized software-based firewalls.

- **Less operator interaction.** Users have a tendency to play with things, and the black-box approach limits the "damage" users can do. This reduces trouble calls and improves security.

- **Troubleshooting ease.** When a box fails, it is easier to swap it out than troubleshoot. This process gets the node back online quicker, and it can also be done by a nontechnical person. This feature is especially important for remote offices without dedicated technical staff onsite.

Benefits of Integrated Solutions

There are a series of important benefits for organizations to consider when evaluating an integrated security solution.

Lower Total Cost of Ownership

Using an integrated security solution can help lower the total cost of ownership

Using an integrated security solution can help lower the total cost of ownership. A single vendor can typically offer a lower total price for an integrated solution than the sum of list prices for each component purchased from different vendor. There are also hidden costs to consider such as the need to manage and renew multiple licenses, often at different times of year. While renewals may not be an issue if organizations choose to purchase the products at the same time, the management of multiple security products could be costing an organization in administration overheads as well as the IT administration staff's time. Additionally, using one vendor's products will result in lowered internal support and training costs, as staff only need to be trained on one product.

Simplifying Administration

Integrated security solutions provide central consoles to manage multiple security products across a network

Integrated security solutions provide central consoles to manage multiple security products across a network. By using two or more vendors' products, an organization eliminates the central control functionality and introduces the issue of consolidating logs for reporting. Under a multi-vendor strategy, administrators may need to use four or more consoles to manage and update their security products. Security vendors also typically standardize their interface layouts for all security products. An integrated strategy ensures management is consistent across all security products, which again simplified administration. While it is certainly true that security vendors collaborate in providing new virus signatures that have been detected in the wild, these vendors also use different name formats for these viruses when updating their products. This can cause confusion when an organization goes to update its security products in a point-solution scenario, and can sometimes hinder effective incident response and management.

Ease of Updates

Organizations with an integrated security solution are typically only required to download one file per update, rather than one or more files per product. Vendors also

typically release program version upgrades at different times of the year. An integrated solution allows an organization's administrator to keep a straightforward schedule in terms of updates. New signature updates are currently available every few days, and this trend is increasing rather than decreasing. To manage and download these files across multiple systems could become very confusing and time consuming. By using an integrated solution that offers a universal update for multiple security products, deployment of the update across a network will ensure that disruption to network resources is minimized. This is important considering signature updates can exceed 5 megabytes, with the size and frequency only set to increase.

Support

When an organization purchases a license, it is not simply buying the product, but also access to updates and technical support. Whether a single user or large corporation, a large outbreak will give rise to the need to contact someone for assistance. With increasing complexity of new viruses, it is becoming harder to protect and clean all possible viruses and variances of viruses. Access to round-the-clock support is critical to managing outbreaks. Organizations with an integrated solution also gain benefits from using one vendors support team. This is important in terms of consistent technical support as well as escalation processes.

SYMANTEC'S NEW APPROACH TO EMAIL SECURITY

Corporate Overview

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, Calif., Symantec has operations in more than 35 countries. Symantec provides security solutions for all tiers of a network: at the gateways between the network and the outside world, at the servers that act as the network's vital organs, and at end-user devices including desktop PCs, laptops and handhelds. Symantec announced the acquisition of Brightmail on May 19, 2004.

Symantec Mail Security Overview

Symantec Mail Security 8200 Series

The Symantec Mail Security 8200 Series appliances enable organizations to cost-effectively secure the organization from email-based threats using a combination of Symantec Brightmail AntiSpam, Symantec AntiVirus, volume management, attack prevention, content filtering, encryption, anti-forgery and archiving functionality. Symantec Brightmail AntiSpam technology filters spam with a 95% effectiveness rate and eliminates the impact of false positives with a high accuracy rate. Symantec's Brightmail Logistics Operations Centers (BLOC) analyze spam across the globe and provide secure, automatic spam filter updates every 10 minutes to help thwart attacks. Symantec AntiVirus technologies, leveraging the global research and

response expertise of Symantec Deepsight and Symantec Security Response, ensures business uptime by protecting against email-borne threats. Additionally, content compliance features allow organizations to gain control over inbound and outbound email content, enabling them to enforce internal or regulatory email content policies.

Symantec Mail Security 8100 Series

To further reduce spam volume and cut email infrastructure costs in large organizations and ISP's, Symantec also provides the Symantec Mail Security 8100 Series appliance. Using Turntide TCP Traffic Shaping technology, the Symantec Mail Security 8100 Series reduces up to 50% of overall mail volume before it reaches the network. Traffic Shaping, performed at the protocol level, manages the quality of service that each email sender is given so that legitimate business email continues and spam is slowed or stopped. By limiting the number of spam messages a spammer can send, spam remains on the spammers servers rather than the targeted organization, reversing the cost of spam so that the spammer, rather than the organization, incurs the consequences of high spam volumes. Symantec Mail Security 8160 can be coupled with any email security gateway solution, including Symantec Mail Security 8200 Series appliance, to provide a comprehensive multilayered approach to combat spam that is easy to deploy and manage. The solution is powered by Brightmail technology and response.

CHALLENGES/OPPORTUNITIES

Symantec's dominance in the client antivirus market could present an obstacle since some organizations prefer to use more than one vendor for antivirus protection. Symantec can overcome this obstacle by positioning the mail security solution as a comprehensive integrated solution that will not only improve security, but reduce the time and cost associated with managing multiple point solutions. Symantec should also look to expand the current outbound scanning features of the mail security solution to a more robust solution that can address compliance with industry and government regulation, protection of intellectual property, and enforcing corporate policies. Expanding secure email (encryption) capabilities also represents a great opportunity for Symantec.

CONCLUSION

IDC believes antispam will continue to converge with antivirus over the next year. Our survey results clearly show that the majority of executives (two out of three) view antispam as part of a larger network security solution. We believe some customers may continue to buy point solutions, but this will be the exception, not the rule. Antispam will continue to be an important adoption driver in the messaging security implementation; however, IDC believes it will become a feature of email security and not a distinct market. We also expect outbound email to become more of a concern in IT departments as organization are forced to comply with various industry and government regulations.

Copyright Notice