

WHITE PAPER

Uncovering the Hidden Costs of Spam in the Enterprise: Email Traffic Shaping Joins the Fight Against Spam

Sponsored by: Symantec

Mark Levitt

Brian E. Burke

January 2007

IDC OPINION

For most email users, spam is a problem that has worsened rather than improved during the past year. As a result, organizations with antispam solutions are looking for cost-effective ways to further minimize the number of spam messages that reach email servers and user mailboxes. Interviews of organizations that have deployed Symantec Mail Security (SMS) 8160 appliances revealed the following benefits of adding email traffic shaping to slow down and effectively block spam:

- Cost avoidance by not having to add antispam servers, email servers, and administrators despite significant growth in spam volumes in 2005 and 2006 and steady growth in email users and subscribers
- Cost reduction by reducing the time spent by IT staff dealing with spam, email delivery, and denial of service (DoS) attacks
- Improved efficiency and customer satisfaction by reducing the amount of spam reaching user and subscriber mailboxes

IN THIS WHITE PAPER

In this IDC white paper, we look at the resurging problem of spam and what organizations are doing to augment existing antispam solutions with additional cost-effective layers of protection. We then present the benefits realized by organizations that have deployed SMS 8160 appliances in conjunction with other antispam solutions, along with a return on investment (ROI) analysis for one of the service provider customers that agreed to have its findings published anonymously.

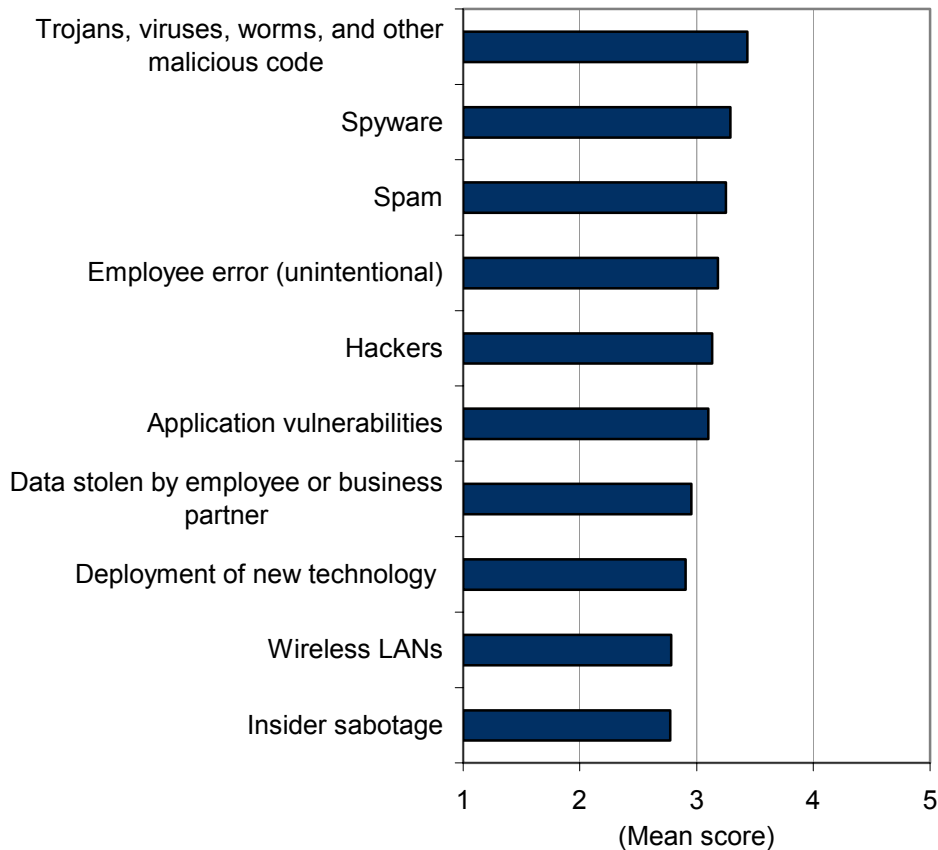
SITUATION OVERVIEW

Resurgence of Spam

Spam continues to clog networks, servers, and inboxes with unwanted, offensive, and often malicious content, and it has quickly climbed back up the priority lists of IT managers. Spam moved from a nuisance in 2002 to a full-blown IT nightmare in 2003, but as organizations implemented antispam technologies during 2003 and 2004, it started to slide back down the priority lists in many IT departments. In fact, in IDC's 2004 *Enterprise Security Survey*, spam fell to eighth place on the list of most serious threats to enterprise security (down from second place in 2003). This decline has reversed, and spam is once again considered a major security threat, ranking as the third-greatest threat to enterprise security in 2006 (see Figure 1).

FIGURE 1

Threats to Enterprise Security



Note: Threat scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

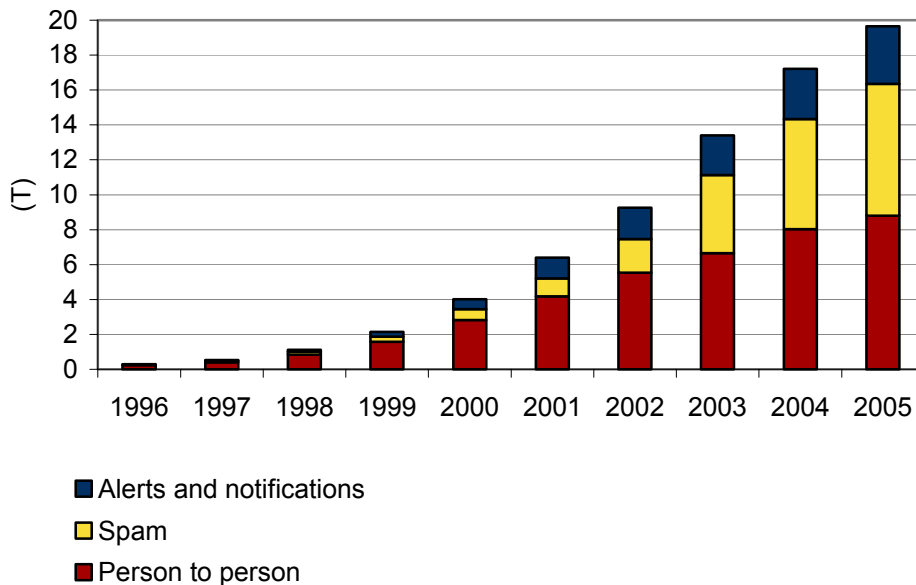
Source: IDC's 2006 *Enterprise Security Survey*

The volume of spam continues to rise at a rapid pace even as the pace of person-to-person emails has slowed (see Figure 2). The convenience and efficiency of email have been reduced by the extremely rapid growth in the volume of unsolicited commercial email. Moreover, an increasing amount of spam is being sent by a bot network of zombie machines. IDC believes that more than two-thirds of all spam sent today originates from zombie machines remotely controlled by spammers. Malicious attacks are also becoming more sophisticated (e.g., blended threats that combine spam, spyware, viruses, and other malware in their attacks), and attackers are becoming increasingly focused and targeted in their attacks. IDC sees financial gain, fraud, and identity theft continuing to be the leading drivers behind the increasing sophistication and volume of email-based attacks. Email phishing attacks are now daily occurrences for many organizations, especially for the largest financial institutions and their customers. We expect email pipelines to continue to be a favorite target for malicious attacks, including spam, worms, viruses, and blended threats.

IDC believes these factors are the primary reasons for the resurgence of spam as a major threat to enterprise security. These trends are causing the effectiveness and accuracy of first- and second-generation antispam solutions to suffer and, in turn, are contributing to spam's resurgence as a serious security threat and productivity drain for organizations of all sizes.

FIGURE 2

Worldwide Annual Total Email Messages Sent, 1996–2005



Note: This 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, 2007

Impact of Spam


The resurgence of spam is having a significant negative impact on both IT and email users. First, IT staff have to increase the amount of time spent dealing with the rising workload demands on existing email and antispam servers that can slow or even stop email traffic. Sometimes spammers flood servers with emails to slow or stop the processing of legitimate emails in what is called a DoS attack. IT often needs to deploy additional servers and administrators to handle the higher workload. In addition, IT is called away from other projects to respond to complaints about the rising number of spam messages appearing in user or subscriber mailboxes. The spam problem is essentially stealing money from budgets and IT staff time that had been intended for other projects. The spam situation is especially frustrating and disruptive for IT departments that thought that they had the spam problem under control and are now realizing that their assessment was premature. Instead of being a chronic problem that IT was successfully managing with minimal attention, spam is again an acute problem that often requires immediate attention.

Second, email users faced with significant numbers of spam in their mailboxes after a period of time during which spam had largely disappeared are again wondering whether email will ever shake the problem of spam. Users are again at risk of losing confidence in email as they are forced to spend time separating legitimate emails from spam. Unless spam can be brought under control in a long-lasting way, users may turn more often to other communications options such as instant messaging and voice calling.


The next section looks at an antispam solution that is designed to block the rising volumes of spam at the network level, before the spam has a chance to have an impact on email and antispam servers and user/subscriber mailboxes.

Symantec

Symantec Corporation, headquartered in Cupertino, California, was founded in 1982 and held its initial public offering in June 1989. With over 15,500 employees, Symantec has operations across the United States, as well as in Canada, New Zealand, Japan, and Australia.

In 2004, Symantec acquired Brightmail, the leading antispam solutions vendor in the market. Also in 2004, Symantec acquired TurnTide and its  traffic-shaping appliance technology. The Symantec Brightmail AntiSpam engine was then integrated with the traffic-shaping capabilities of the TurnTide appliance, and the resulting product was renamed the Symantec Mail Security 8160.

Symantec Mail Security 8160

The SMS 8160 stops spam before it enters the network by identifying spammers via its patent-pending IP reputation analysis technology, reducing the number of emails from suspicious IP addresses that can reach antispam and email servers. Symantec estimates that its 8160 can reduce total  mail volume by up to 50% while ensuring the continuous flow of legitimate email. By shaping email traffic at the TCP protocol level, the 8160 severely limits the number of emails that spammers can force into

corporate networks, which significantly reduces administrative overhead, network bottlenecks, and mail infrastructure costs. The SMS 8160 can scale to meet the needs of growing businesses, processing up to 30 million emails per day. It can be coupled with any antispam gateway solution, including SMS 8200 and 8300 Series appliances and Symantec Brightmail AntiSpam software with automatic updates, to provide a comprehensive multilayered approach to combat spam.

The SMS 8160 appliance is designed to improve both the effectiveness and the efficiency of an organization's existing antispam defenses by:

- ☒ Reducing the number of TCP/IP sessions that spammers can establish to an organization's inbound SMTP message transfer agents (MTAs)
- ☒ Reducing the volume of spam that an IP session suspected of sending spam is able to transmit to an inbound MTA, by reducing both the bandwidth allocated to individual TCP/IP transmission channels and the number of email messages that may be transmitted per session
- ☒ Reducing the computing resources that have to be devoted to inbound SMTP MTAs and message content-based antispam defenses
- ☒ Reducing the amount of disk storage that has to be devoted to spam quarantine

SMS 8160 ROI Analysis

Before we look at the quantitative findings from our ROI analysis, we start with the overall feedback that the Symantec customers shared about their experiences with the SMS 8160 appliances. Every customer saw a 40–90% reduction in the volumes of spam messages reaching their networks, which means that antispam and email servers had to process many fewer emails. For others, the impact was a rise from 80–95% effectiveness in blocking spam. Most of the organizations hadn't conducted their own formal ROI analysis, but they could see that the Symantec appliances made a significant difference. Customer confidence in the effectiveness of the SMS 8160 to help IT address the spam problem is clear in the following comment from one of the organizations interviewed: "You would have to pry this from my cold dead hands."

When it was time to calculate the numbers, the challenge, as in any ROI analysis, was to assign dollar values to the changes in the environment before and after deployment of the appliances. We found that many of the changes were difficult to quantify because organizations did not always choose to take action as a result of the benefits. For example, several of the organizations interviewed had antispam and email servers that were struggling to keep up with the rising spam volumes in 2005 and 2006. IT staffs worried that increased server workloads would lead to email server delivery slowing or stopping, antispam solutions letting spam through when overloaded, and costly network resources being consumed at greater quantities. Sometimes these fears were realized, and IT had to spend a significant amount of time dealing with these events in crisis mode. The fear of these events occurring and the consequences felt in calls from subscribers or executive email users were sufficient reasons for these organizations to invest in appliances that added a layer of antispam protection at the network level.

When IT staffs started identifying the steps they needed to take to address the rising server workloads and spam volumes reaching subscriber and email user mailboxes, it became easier to weigh the benefits and costs of deploying SMS 8160 appliances.

The largest areas of benefits for the organizations interviewed were:

- ☒ **Cost avoidance.** This involved customers not having to add antispam servers, email servers, and IT administrators and help desk staff despite significant growth in spam volumes and steady growth in email users (enterprises) and subscribers (service providers). One customer was able to avoid replacing 4 of 12 older servers dedicated to antispam blocking as a result of the appliances reducing the volume of emails sent to invalid addresses in the customer's domain that the antispam servers needed to process.
- ☒ **Cost reduction.** This involved customers reducing the time spent by IT staff dealing with spam, email delivery, and DoS attacks. One customer was able to repurpose one of three engineers dedicated to messaging infrastructure and support due to the reduction in spam problems as a result of using the 8160 appliances.
- ☒ **Improved efficiency and customer satisfaction.** This involved customers experiencing a lifting of the burden imposed by spam on IT and email users and subscribers. One customer experienced a drop of 75% in complaints about spam. Others reported hearing from fewer subscribers threatening to drop the services because of spam, and one even started receiving thank-you notes from subscribers receiving many fewer spam emails.

For a more detailed view of the ROI findings, we present a summary of the ROI analysis for one of the service provider customers that permitted us to publish the findings that show a five-year ROI of 256% and a payback period of 1.1 years. Benefits consisted of significant technology reduction and avoidance and IT staff productivity gains as a result of having the appliances in place over a five-year period. The largest cost component was from the annual mailbox fee associated with the appliance. Given the significant number of emails that the appliances can process, the model assumes that once an organization has two or three appliances for redundancy purposes, it will be unlikely that this or other service providers with even millions of subscribers will need to purchase additional appliances over time (see Table 1).

TABLE 1**ROI Analysis of a Symantec Mail Security 8160 Service Provider Customer**

	Initial	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Benefits (cost savings and avoidance)	–	\$800,803	\$1,038,341	\$1,233,924	\$1,322,507	\$1,449,530	\$5,845,105
Costs (depreciated and expensed)	\$29,750	\$469,250	\$581,250	\$710,850	\$791,490	\$878,850	\$3,461,440
Net profit before taxes	(\$29,750)	\$795,553	\$878,424	\$882,007	\$735,391	\$755,000	\$4,016,625
Net profit after taxes	(\$17,850)	\$477,332	\$527,054	\$529,204	\$441,234	\$453,000	\$2,409,975
Net cash flows after taxes	(\$17,850)	\$13,332	\$105,721	\$170,271	\$236,861	\$268,680	\$777,015
Five-year return on investment	256%						
Payback	1.1 years						

Notes:

- Initial column represents cost outlays that typically are not balanced by benefits that are counted starting in year 1.
- Benefits include avoidance of additional email and other antispam servers and email and help desk staff as subscriber and email volumes grow and avoidance of subscriber churn due to spam.
- Costs include appliance acquisition, mailbox fees, and administration and maintenance by IT staff.
- Hardware, software, and external services costs are expensed if US\$50,000 or less and are otherwise depreciated.
- Financial analysis assumptions: 40% federal and state taxes, 15% discount rate, and three-year straight-line depreciation.
- The figures presented in this table are the result of an independent financial assessment conducted by IDC based on customer interviews and industry information.

Source: IDC, 2007

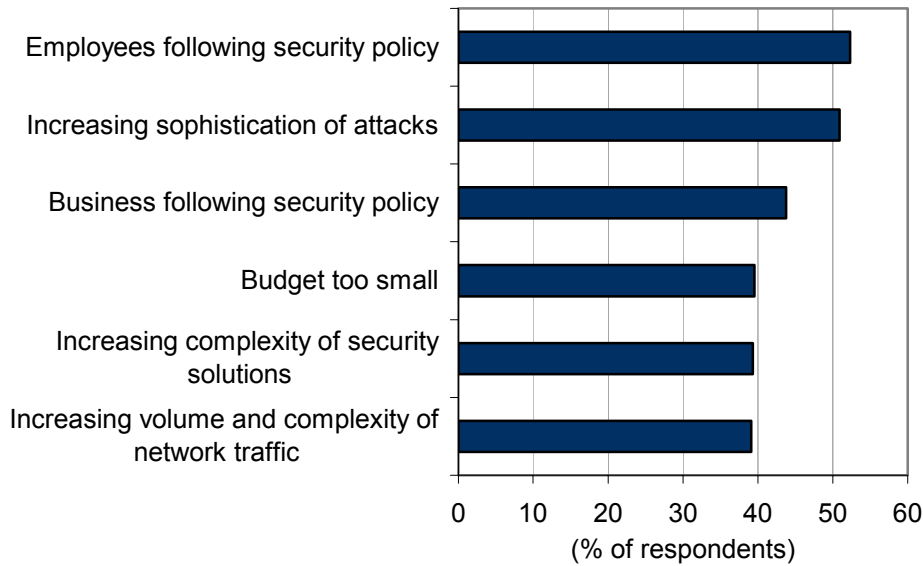
Future Security Challenges

IDC expects the threat environment to continue to evolve from a mischievous hobby to a money-making criminal venture that will attract a new breed of sophisticated hackers and organized crime. IDC believes this profit-driven motivation will cause the number of email threats to increase in sophistication, frequency, and severity.

Our recent survey results confirm these beliefs (see Figure 3). The increasing sophistication of attacks is listed as the second-greatest security concern over the next 12 months. Survey respondents also cited the increasing volume and complexity of network traffic as a major concern. IDC believes the increasing sophistication of attacks combined with the increasing volume and complexity are key factors leading to the ineffectiveness of first- and second-generation antispam solutions. As a result, many organizations are considering new technologies, such as the SMS 8160 appliance, to help deal with the increasing onslaught of spam, viruses, and other unwanted email traffic.

FIGURE 3

Future Security Challenges



Source: IDC's 2006 *Enterprise Security Survey*

The SMS 8160 customers that we interviewed saw no end to the growth of spam volumes on the one hand and the number of email users and subscribers on the other. For service providers in the business of selling hosted email services, controlling spam even as the volumes increase will be critical if they are to be successful in growing their own businesses, which see revenues rise when subscribers join and fall when subscribers drop. Keeping existing subscribers satisfied and demonstrating a reputation for effective spam control will be keys to attracting and keeping additional subscribers. For enterprises, keeping email users and management from complaining about spam in their mailboxes and protecting networks, servers, and PCs from the threats carried by spam will continue to be some of IT's most visible responsibilities.

Challenges and Opportunities

One of the key selling points of appliances for the customers interviewed and for most buyers is that they require little to no attention. Once installed and configured, appliances work tirelessly and invisibly in the background. SMS 8160 appliances are no different in blocking spam messages. One issue that customers raised was that sometimes a little visibility would be helpful. For example, email users or subscribers who realize that their ability to send or receive emails is being blocked contact IT to ask why and to fix the situation. Unlike with other antispam solutions with spam quarantines, email users do not know that their inbound or outbound email has been identified and blocked as spam. When IT receives a complaint, it is sometimes at a loss as to why a particular person's email is being blocked because the SMS 8160

acts on the email traffic based on IP reputations that are known to the appliance but are not known or easily found by IT. As a result, IT starts out in the dark and may need to spend a fair amount of time trying to confirm that the email sent from a particular IP address is being blocked by the appliance because it is on a list of suspected spammer origination sites. The appliance is nearly always working as designed because the blocked email was sent from a user's PC that has been taken over by a zombie that is sending out spam at a level that the appliances determine to be worthy of shutting down. Once IT knows what is happening, it can help the user clean the zombie from the PC or whitelist the IP address to get the user up and running quickly. In future versions of the SMS 8160, customers would like to see reports and other access tools, like those found in other antispam solutions, that keep IT informed about what is happening.

CONCLUSION

As people who live in cold climates know well, layering provides the best protection against the pernicious and invasive threats to health and welfare. IT departments again facing the need to address rising spam volumes will do well to look at network-level solutions such as the Symantec Mail Security 8160 appliance to deflect a significant portion of spam so that other antispam defenses are better able to do their jobs in protecting server and PC performance and IT staff and user productivity at enterprise and service provider organizations.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.