

# Mail Security

## INSIDE

Five Spam Blockers by the Numbers	2
For Spammers, a Picture Is Better Than 1,000 Words	3
2006 Security Survey: Threat Severity on the Rise	4
Symantec Assesses Security	9
Appliances Offer More Than Spam Defense	11
E-mail Attacks Getting Super-Focused	15

*Sponsored By:*



# Five Spam Blockers by the Numbers

WE EVALUATED FIVE ANTI-SPAM SOLUTIONS IN 2006, and for the third year running Symantec (and secret sauce Brightmail) reigns supreme in accuracy. Here's the ranking by percentage of spam blocked in our tests:

**Symantec Mail Security:** 97% accurate, 0 critical false positives, .199% non-critical false positives ([infoworld.com/4561](http://infoworld.com/4561))

**Proofpoint Protection Server:** 95% accurate, 0 critical false positives, .215% non-critical false positives ([infoworld.com/4561](http://infoworld.com/4561))

**IronPort C-Series:** 93% accurate, 0 critical false positives, .058% non-critical false positives ([infoworld.com/4194](http://infoworld.com/4194))

**Mirapoint Message Server:** 92% accurate, .46% critical false positives, 4.661% non-critical false positives ([infoworld.com/4194](http://infoworld.com/4194))

**Microsoft Antigen Spam Manager:** 82% accurate, .358% critical false positives, 2.454% non-critical false positives ([infoworld.com/4592](http://infoworld.com/4592))

Symantec, Proofpoint, and IronPort all proved quite accurate, and all three excelled at avoiding false positives. IronPort deserves special mention here, having registered only 1 false positive in nearly 10,000 messages, and this a “non-critical” one. Non-critical false positives are mass mailings that are incorrectly identified as spam, while critical false positives are personal messages that are incorrectly blocked.

Anti-spam gateways have come a long way since 2003, when we first began testing them. It's hard to find a viable commercial solution today that isn't at least 90% accurate, and the best ones exceed 95%. Microsoft Antigen's 82% accuracy is head-scratchingly behind the curve. ☞

— *Doug Dineley*

# For Spammers, a Picture Is Better Than 1,000 Words

SPAM IS AGAIN ON THE RISE, LED BY A FLOOD OF junk images that spammers have crafted over the past few months to trick e-mail filters, according to security vendors.

Called “image-based” spam, these junk images typically do not contain any text, making it harder for filters that look for known URLs or suspicious words to block them.

Instead of a typed message, users will see only an embedded .gif or .jpeg image file urging them to buy pharmaceuticals or invest in penny stocks.

Antispam vendor Cloudmark says that half of the incoming spam is now image-based on the “honeypot” systems it puts out on the Internet to lure spammers.

“About a year and a half ago, we started seeing a little bit of it, but it wasn’t until the past six months that it became a serious issue for many antispam companies,” said Adam O’Donnell, a senior research scientist with the company.

Image-based spam has jumped from about 1 percent of all spam messages in June 2005 to around 12 percent today, according to Craig Sprosts, senior product manager with IronPort Systems.

Its growth is helping to fuel a global resurgence in spamming, Sprosts said.

The total number of spam messages sent daily is up 40 percent since April, Sprosts said. Much of this new spam is coming from a “relatively small group of spammers with control over very large zombie networks,” of hijacked computers, he said.

Spammers now generate an estimated 55 billion messages per day, according to IronPort. A year ago that number was 30 billion e-mail messages per day.

The combination of greater volume and better techniques has meant more complaints for network administrators.

Administrators at Avnet have started stripping certain embedded image files out of all messages, after seeing an uptick in image-based spam two months ago, said Rob Ku-

dray, manager of messaging services with the computer distributor.

One other tactic that is helping keep in-boxes full is the spammers’ practice of constantly registering new domains. Of the 35 million domains registered in April, 32 million were never paid for and expired after five days, Sprosts said. He believes that many of those domains were used by spammers to send out their unsolicited e-mail during that five-day grace period.

This technique makes it very difficult to blacklist e-mail based on the URLs it contains. “Traditional blacklists and whitelist approaches just can’t keep up with how fast they’re registering new domains and changing the URLs in the e-mail,” Sprosts said.☞

— Robert McMillan

# 2006 Security Survey: Threat Severity on the Rise

THIS YEAR'S *INFOWORLD* SECURITY SURVEY SHOWS an alarming and growing lack of confidence among IT security professionals — for the fourth year in a row.

It would be hard to find a better example of a distressed IT pro than Brent Oxley, the owner of the Web-hosting service HostGator. In September, Oxley found himself facing a potentially fatal catastrophe.

Of course it happened on Friday afternoon — and before long it turned into the biggest crisis in his company's four-year history. What started as a handful of complaints from clients was starting to number in the hundreds, and each told a similar tale: People who tried to visit any of the legitimate Web sites that HostGator's customers operated were redirected to rogue addresses that quickly dropped a virus onto the end-users' PCs.

The next 12 hours were hell. Every time Oxley's team scoured one machine clean, another system elsewhere in the network would get infected. "It was madness," said Oxley, who began to feel he was trapped in a whack-a-mole game of incursion and parry — while simultaneously attempting to deflect the wrath of customers and end-users.

## Metastasizing Threat

Oxley isn't alone. According to our survey, which polled 430 individuals responsible for their organization's security, 56 percent are at most "somewhat confident" in their enterprise's security system. And the rising tide of malware and phishing exploits is behind a great deal of that anxiety.

If 2005 marked the year that playful teenage hacker hobbyists gave way to more criminally minded professionals, 2006 is showing just how lethal this better-funded and -disciplined breed of thugs can be. Their malware is leaner and stealthier, and it burrows deeper into operating systems and applications to ferret out confidential informa-

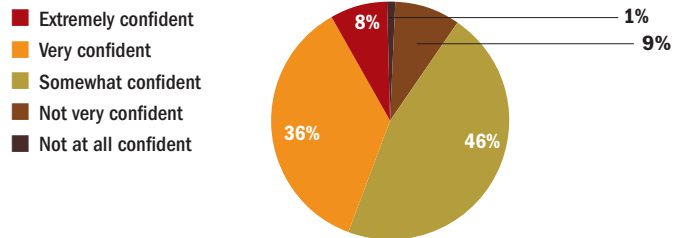
tion. You can even buy do-it-yourself malware and phishing kits online, including one called Web Attacker, which offers a maintenance contract for an extra fee. Sophisticated phishing attacks are targeting smaller enterprises, too.

"It's not getting any better, and some would argue that it's getting worse," says Ed Skoudis, co-founder of security consultancy Intelguardians and an incident handler at the SANS Institute Internet Storm Center. Speaking of the security menace facing the average enterprise today, he adds, "The threat has metastasized in a very bad way, all based on the profit motive."

The attack on HostGator bears many of the typical hallmarks of today's increasingly sophisticated security threats. And it underscores the growing number of zero-

### Level of Confidence in Enterprise Security System

Please rate your overall level of confidence in your company's enterprise security system.



Note: Based on 430 qualified respondents

day vulnerabilities in Windows — which totals at least eight this year, according to eEye Digital Security — not to mention other applications. This point isn't lost on survey respondents, 51 percent of whom rated the increasing sophistication of attacks as a top security challenge, while 50 percent said Trojans, viruses, and other malicious code represented the top threat to network security.

Eric Sites, vice president of research and development at Sunbelt Software, isn't surprised. In years past, Trojans typically loaded machines with adware that was so poorly written it would bring the PCs to a grinding halt. They were

**Rating Threat Posed to Network Security**

Please rate the items below on the threat each poses to your company's enterprise network security.

Trojans, viruses, worms, or other malicious code (regardless of source)	50%
Spyware	45%
SPAM	44%
Employee error (unintentional)	39%
Application vulnerabilities	37%
Data stolen by employee or business partner	37%
Hackers	36%
Insider sabotage	30%
Wireless LANs	30%
Deployment of new technology (e.g., wireless LAN, remote access)	27%
Business partner error (unintentional)	24%
Mobile devices (PDAs, smartphones)	24%
Casual intruders who don't fall under definitions of competitors, cyberterrorists, employees, or partners	20%
Cyberterrorism	19%
Inability to meet government regulatory mandates	16%
Competitor espionage	15%

Note: Based on 430 qualified respondents; percentages reflect responses of 4 or 5 on a 5-point scale

a nuisance, says Sites, but nothing like today's malware, which steals passwords, sends spam, and joins botnets — revealing few or no visible signs. To make matters even worse for enterprises, attackers have begun gathering at "cyberbazaars" where they can trade passwords and other information gathered via malware.

"The guys currently out there will do anything to get your money, your credit card number, or whatever private information they can sell to make money," Sites says.

**Attacks Drop, Severity Rises**

Security professionals reported a modest drop in the number of attacks on their networks during the past 12 months, with a mean of 331 attempted breaches and 39 successful ones per company. That compares favorably with the mean of 368 attempted attacks and 44 successful intrusions per company noted in last year's survey.

Unfortunately, this is not to say that networks are any safer — at least according to Jon Ramsey, CTO of SecureWorks, which monitors Internet attacks using about 5,000 intrusion prevention system devices. Although the volume of overall alerts has decreased, he points out that "the number of severe attacks is increasing precipitously." The

reason for the decrease in the number of attacks, according to this reasoning, is disturbing: As break-ins morph from prank to business, profit-driven attackers are less likely to waste time or take chances using outdated or ineffectual techniques.

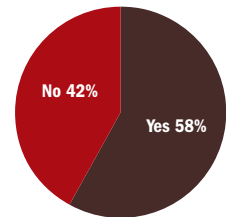
Among successful intrusions, the spoofing of an organization's identity to victimize customers — a common technique in phishing scams — was the most common, with 25 percent of respondents reporting they have been subjected to the practice, up from 23 percent last year. The increase is hardly surprising, Sunbelt's Sites says, given the advent of \$50 phishing kits that provide templates that mimic even the most minute details of the 10 most popular banking Web sites.

To make matters even worse, phishing, which was once primarily focused on large enterprises such as eBay, is now becoming a problem for much smaller organizations. SecureWorks' Ramsey says that 67 percent of the credit unions his company counts as clients have been subject to phishing attacks.

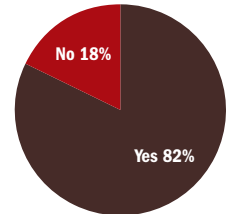
For the second year in a row, security professionals reported a drop in the number of successful attacks that targeted flaws in operating systems. Only 23 percent of respondents reported being subjected to an intrusion that targeted the operating system, down from 24

**Official Security Policy/  
Policy Training/Official  
Risk Notification Policy**

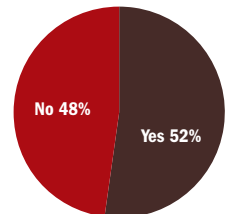
Does your company have a formal, documented security policy?<sup>1</sup>



Are your employees trained in that policy?<sup>2</sup>



Does your company have an official policy for notifying customers when their private data may be at risk?<sup>1</sup>



Note: (1) Based on 430 qualified respondents; (2) based on 249 qualified respondents

percent last year and 40 percent in 2004. Similarly, reports of exploits that hit weaknesses in Web applications, routers, or other pieces of network infrastructure either decreased or remained flat.

“Software vendors seem to have definitely gotten the message that enterprises are valuing security as a very important feature in the products they want to buy,” says John Pescatore, Gartner’s vice president for Internet security. “We see more and more software vendors using vulnerability testers.”

### Threat from Within

As predatory as today’s criminally minded hackers are, IT professionals face plenty of threats from within their own enterprises — none more glaring than their own lack of a comprehensive plan for security. No fewer than 42 percent of respondents reported that their organization had no documented security policy. (That’s a slight improvement over last year, when 46 percent of security professionals polled reported no formal policy.)

Almost as distressing is the finding that 18 percent of

those groups that do have a policy do not train their employees how to follow it. “It’s the old saying, ‘Well, I’d love to fix the plane, but I’m busy flying it across the ocean,’” Pescatore says. Although it’s true that implementing a policy can be a lot of work, the SANS Institute has taken much of the cost out of this process by offering a draft security policy on its Web site for free.

Resistance to implementing and enforcing security policies goes a long way toward explaining the long list of front-page headlines detailing privacy breaches that dominated much of the past year. In one of the better known cases, a laptop with confidential information pertaining to approximately 26.5 million veterans was stolen when the residence of a contractor with the Department of Veterans Affairs was burglarized. The incident highlights the troublesome fact that even when an organization has a strict security policy — in this case, the contractor was not authorized to take the data home — getting workers to follow it can be difficult. The episode also underscores a finding in the *InfoWorld* survey that just 55 percent of respondents deploy encryption software on PCs and handheld devices — a solution that would go a long way toward securing data that falls into the wrong hands.

The threat posed by their own employees isn’t lost on security pros, 56 percent of whom rated workers who fail to follow security policy as a significant security challenge. “We’re at the point now where we have to look and say, ‘What are we

### Top Security Challenges

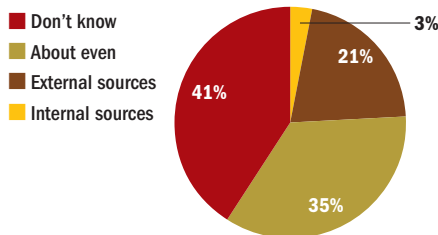
Please rate the top security challenges your company will face over the next 12 months.

Employees underestimate importance of following security policy.....	52%
Increasing sophistication of attacks.....	51%
Business execs underestimate importance of following security policy.....	44%
Budget too small to cover necessary security purchases.....	40%
Increasing complexity of security solutions.....	39%
Increasing volume and complexity of network traffic.....	39%
Mobile clients and unmanaged devices.....	37%
Always-on environment.....	35%
Patchwork nature of network security.....	34%
Wireless devices used in the enterprise.....	33%
Network configuration management.....	31%
Lack of IT security experts within company.....	30%
Difficulty of securing Web applications.....	28%
Integrating third-party vendor software into your environment.....	27%
Complying with government security and privacy regulations.....	25%
Instant messaging used in the enterprise.....	24%
Cyberterrorism.....	20%
Outsourcing security.....	11%

Note: Based on 430 qualified respondents; percentages reflect responses of 4 of 5 on a 5-point scale

### Most Serious Threats Come From External Sources

Do you believe that the most serious threats to your company’s enterprise IT infrastructure originate from internal or external sources?



Note: Based on 430 qualified respondents

going to do about the internal threat?’” says Jim Brockett, CIO of Washington Trust Bank, referring to rank-and-file employees. He remains particularly wary of the risks of “social engineering,” in which some smooth-talking visitor posing as a PC repairman, or a customer’s long-lost relative, talks an employee into handing over confidential data, or providing physical access to the network. “It’s a constantly moving target,” he says.

### Employee Monitoring

Brockett is also vigilant to the threat that employees might pilfer data, something Dan Clements, CEO of privacy protection company CardCops, sees every day—as he lurks anonymously in online chat rooms that traffic in stolen Social Security numbers, credit card accounts, and other confidential information. “The value of the data in the underground is pulling this data from corporate America into cyberspace,” Clements says. He notes that data thieves now pay as much as \$20 for data pertaining to a single identity.

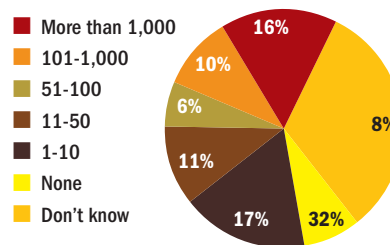
Enterprises are currently looking to a host of solutions to combat this threat from within. Alongside the anti-virus, firewall, and VPN programs they’ve been using for years to keep bad guys out, IT professionals are now using products that help keep information in. Fully 24 percent of security professionals surveyed said they deployed employee-monitoring solutions, while another 8 percent said they planned to introduce such systems during the next year. And 44 percent said they monitored or filtered outbound e-mail, with an additional 8 percent saying they would begin doing so in the next 12 months.

Brockett uses a fraud monitoring service from a company called NextSentry to prevent data theft by his employees. It notifies him whenever a worker copies information from a trusted application, such as the bank’s database, and pastes it into an untrusted one, such as a Web browser or e-mail program. The solution also blocks the use of thumb drives and other unapproved USB devices.

### Network Attacks Foiled in the Past 12 Months

How many attacks, including (but not limited to) viruses, hacks, Trojan horses, and worms, against your company’s enterprise network defenses were attempted but foiled in the past 12 months?

Mean number of network attacks foiled past 12 months = 331

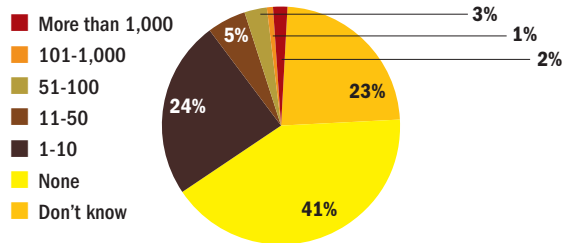


Note: Based on 430 qualified respondents

### Successful Network Attacks in the Past 12 Months

How many attacks, including (but not limited to) viruses, hacks, Trojan horses, and worms, against your company’s enterprise network defenses successfully breached in the past 12 months?

Mean number of network attacks past 12 months = 39



Note: Based on 430 qualified respondents; percentages do not add up to 100 due to rounding

Traditional technology, when properly configured, can provide important tools in the struggle to stay secure. But increasingly, according to our respondents, what’s needed are new technologies that do more than scan for malicious code or network probes. “We need to move to a behavioral-driven monitoring system,” says Dave Rand, chief technologist for Internet content security at Trend Micro. “Is the machine supposed to wake up at 3 a.m. and send e-mail or not?”

Assuming security providers are able to develop such sophisticated products— a big “if” in the minds of many IT professionals — there’s the less-than-trivial question of how they’ll be received in a market that’s already saturated with expensive security solutions. According to the survey, only 35 percent of respondents expect their security budget to grow next year.

## HostGator Strikes Back

Meanwhile, back at HostGator, Oxley and his team finally gained the upper hand when it figured out that the attackers were penetrating HostGator's defenses via a previously unknown hole in a Web site management application called cPanel. Once inside, the criminals used HostGator's servers as a beachhead to exploit a separate zero-day weakness in the way Microsoft Windows uses VML (Vector Markup Language) to render graphics. All told, the predators infected more than 200 machines that served the majority of the 500,000 domains that HostGator runs. (They also targeted at least two other hosting services, according to Oxley, who declines to name them.)

Although Oxley's team finally resolved the episode, Oxley himself, like many of our survey respondents, is still looking over his shoulder. "The biggest risk we have," he says, "is waking up one morning and finding there's an exploit bad enough to put all the Web hosting companies out of business."

It would be nice to ascribe statements like that to professional paranoia. Unfortunately, as many of Oxley's peers can attest, his concern is all too real. 🦹

— Dan Goodin

# Symantec Assesses Security

AS THE INTERNET HAS EVOLVED INTO A VAST DIGITAL information and commerce hub, so too have the crimes perpetrated therein. Petty Web site vandalism and shotgun-style DoS (denial-of-service) attacks have paved the way for sophisticated data thefts and targeted phishing scams.

As reported by IDGNS, Symantec has released its most recent Internet Security Threat Report, which provides a grim reminder of just how dangerous the untamed Internet can be. The research covers the first half of 2006.

For now, Symantec reports that home users suffer the worst of cyberthieves' plots, accounting for 86 all targeted attacks. Financial services businesses follow, according to the report.

Net crooks' techniques have come a long way, making them all the more difficult to spot and track. "Symantec has identified increased attacks aimed at client-side applications, increased use of evasive tactics to avoid detection, and ... smaller, more targeted attacks focusing on fraud, data theft, and criminal activity."

Following are some of the numerical highlights from Symantec's Internet Security Threat Report:

## U.S. Gives as Good as it Gets

- 6,110 - Average number of DoS attacks Symantec observed per day during the first half of 2006
- 54% - Percentage of worldwide DoS attacks targeting the U.S.
- 42% - Percentage of bot command-and-control servers in the U.S., the highest percentage of any country
- 37% - Percentage of worldwide attacks originating from the U.S., the highest of any country

## Holes ...

- 2,249 - Number of new vulnerabilities documented by Symantec in the first half of 2006

- 18% - Increase in number of new vulnerabilities over the second half of 2005
- 47 - Number of vulnerabilities found in Mozilla browsers
- 38 - Number of vulnerabilities found in Internet Explorer
- 47% - Percentage of Web browser attacks targeting Internet Explorer, the more frequently attacked browser
- 80% - Percentage of vulnerabilities Symantec deemed "easily exploitable (up from 79%)
- 78% - Percentage of easily exploitable vulnerabilities that affected Web applications.
- 28 - Average window of exposure, in days, for enterprise vulnerabilities
- 9 - Average window of exposure, in days, for IE — the highest of any browser
- 2 - Average window of exposure, in days, for Opera
- 1 - Average window of exposure, in days, for Mozilla

## ... and Patches

- 89 - Average number of days for Sun to develop patches for its OSes
- 53 - Average number of days for HP to develop patches for its OSes
- \* 37 - Average number of days for Apple to develop patches for its OSes
- 13 - Average number of days for Microsoft to develop patches for its OSes
- 13 - Average number of days for Red Hat to develop patches for its OSes

## Trojans and Viruses and Worms, Oh My


- 8% - Percentage of new distinct malicious code samples detected by Symantec honeypots in the first half of 2006
- 5 - Number of the top ten new reported malicious code families that were Trojans. The most prevalent for the period was the Polip virus.

- 38 - Number of the top 50 malicious code samples that were worms
- 75% - Percentage of the worms making up the volume of top 50 malicious code reports
- 6,784 - Number of new Win32 viruses and worms documented by Symantec
- 22% - Percentage of bots accounting for the top 50 malicious code reports, up from 20%
- 30 - Number of the top 50 malicious code samples that expose confidential information

### **Return to Sender**

- 157,477 - Number of unique phishing messages detected by the Symantec Probe Network in the first half of 2006
- 81% - Increase in the number of unique phishing messages since the second half of 2005
- 54% - Percentage of monitored e-mail traffic that was spam in the first half of 2006, up from 50%
- 58% - Amount of detected worldwide spam originating in the U.S.

### **Bad Apples**

- 8 - Number of adware programs among the top 10 reported security risks
- 3 - Number of “misleading applications” among the top 10 new security risks. 

— *Ted Samson*

# Appliances Offer More Than Spam Defense

WHILE SPAM CONTINUES TO BE A PROBLEM, CONSUMING network bandwidth and users' time, it is not the only security issue facing e-mail administrators. DHAs (directory harvest attacks) try to find valid e-mail addresses by sending random e-mails to thousands or millions of possible users at a domain; phishing scams try to collect users' login information with phony eBay or Amazon.com update messages; users send or receive e-mail with objectionable content — or share information that shouldn't be released outside the company.

Recognizing these growing threats, anti-spam appliances are moving beyond spam protection. I tested two devices, Proofpoint Protection Server and Symantec Mail Security, both of which provide excellent anti-spam performance and help to secure your e-mail systems

against other risks. The appliances offer drop-in simplicity of installation and excellent integration with any e-mail server already in use, and they help enforce e-mail policies, ensure regulatory compliance, and stop the transmission of proprietary data.

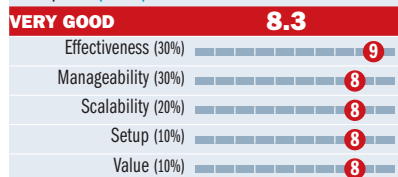
Pricing on these products can be difficult to figure out, but it's an important consideration. Proofpoint offers three different appliance models; Symantec, two. Additional per-user, per-year costs for subscriptions vary with the number of users and the features enabled. Symantec comes out as

the price leader in all of the per-user, per-year costs, especially because their content filtering, e-mail firewall, and regulatory compliance features are included in the base price. At 5,000 users, the cost per user, per year for all features is \$10.37 for Symantec, and \$57.56 for Proofpoint.



## Proofpoint Protection Server v.3.2.2.40

Proofpoint [proofpoint.com](http://proofpoint.com)



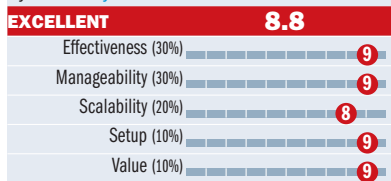
**COST:** 500 users: \$6,750 for hardware, \$57.56 per user, per year for all features; 1,000 users: \$9,750 for hardware, \$53.31 per user, per year for all features; 5,000 users: \$9,750 for hardware, \$30.75 per user, per year for all features

**PLATFORMS:** SMTP

**BOTTOM LINE:** Proofpoint Protection Server provides excellent performance and an extensive feature set, along with easy setup and good ease-of-use. Performance was excellent, with three bulk false positives and a catch rate of more than 95 percent. Although bettered slightly by the Symantec system, which has a lower cost per user, Proofpoint is still a very good e-mail security choice.

## Symantec Mail Security 4.1.1-3

Symantec [symantec.com](http://symantec.com)



**COST:** 500 users: \$1,995 for hardware, \$18.70 per user, per year for all features; 1,000 users: \$4,995 for hardware, \$14.15 per user, per year for all features; 5,000 users: \$4,995 for hardware, \$10.37 per user, per year for all features

**PLATFORMS:** SMTP

**BOTTOM LINE:** Symantec Mail Security offers best-in-class performance with a spam catch rate of more than 97 percent and four false positives, all bulk. It is very easy to use and has a relatively low cost per user, with regulatory compliance and digital asset security features standard. Great policy-driven filtering and e-mail firewall features add value to the basic anti-spam and anti-virus functionality.

## Cutting False Positives

Performance in anti-spam filtering is measured in two areas: the percentage of spam caught and the number of false positives. There are two types of false positives — bulk e-mails and critical false positives, which are e-mails that end-users need to see but are erroneously tagged as spam.

Both the Proofpoint and Symantec products produced excellent statistics, with better than 95 percent of spam caught and no critical false positives out of more than 8,000 messages processed. Each had a few — three for Proofpoint, four for Symantec — bulk false positives, but these were relatively unimportant; bulk e-mails tend to repeat and are thus easily whitelisted, a task users can do for themselves. The zero

critical false positive rate is much more important than the catch rate because too many critical false positives negate productivity gains by forcing users to sort through quarantined files for e-mails they need.

Both appliances can quarantine spam, throw the message away, or mark message headers to indicate that the messages are definitely or probably spam. This allows for differing responses based on spam-confidence levels — you could throw away messages with high confidence and quarantine ones that are probably spam, while allowing the rest through into the user’s inbox.

Featurewise, the two appliances are well-matched. Both products have flexible policy-based engines for dealing with e-mails that violate rules relating to language — explicit, harassing, or vulgar language, or messages containing words or phrases that shouldn’t be discussed with anyone outside the company — or the sending of documents that shouldn’t leave the company.

Symantec has a slight edge in its range of responses to violations, but either system will make security officers happy. Both Proofpoint and Symantec also offer granular and flexible role-based administration to allow auditing of e-mails that have been stopped due to policy violations.

To stop DHAs, the appliances can import user information from Active Directory, Exchange, Notes/Domino serv-

ers, or standard LDAP directory servers. They can also reject e-mail addressed to invalid users.

Symantec provides a very simple, easy-to-use directory synchronization function that uses auto-discovery and auto-fill-in to reduce the necessary steps for synchronizing to just one: entering an administrator log-in and password. It is the easiest directory synchronization tool I’ve ever used — although Proofpoint’s directory synch isn’t too far behind, with only a couple of additional fields to fill in and good documentation of the necessary syntax.

### Proofpoint Protection Server v.3.2.2.40

Proofpoint Protection Server is available in three versions: a basic version (the Messaging Security Gateway X200) with limited functionality that retails for \$1,995, with bundled anti-spam/anti-virus/compliance modules priced at \$8,995 a year; the P600, priced at \$6,750, with support for 500 users; and the P800, which supports 1,000 to 5,000 users or more, priced at \$9,750.

I tested the P800 version, which comes with a content compliance module, but anti-spam, anti-virus, regulatory compliance, and digital asset security modules are each priced separately. (Depending on whether your company has a lot of intellectual property to protect, you may or may not need the regulatory compliance or digital asset security modules.) Performance was excellent, with only three bulk false positives and a catch rate of more than 95 percent.



Proofpoint Protection Server v.3.2.2.40

## Crunching the Numbers

Both appliances performed very well when cracking down on unwanted e-mail; Proofpoint had fewer bulk false positives, and Symantec caught a higher percentage of spam.

	Total messages	False positives (critical)	False positives (bulk)	Total spam	Spam caught	Spam not caught	Percent spam caught	Valid messages
<b>Proofpoint Protection Server v.3.2.2.40</b>	8,363	0	3	6,969	6,640	329	95.28%	1,391
<b>Symantec Mail Security 4.1.1-3</b>	7,484	0	4	5,469	5,343	126	97.70%	2,137

The Proofpoint appliance is simple to configure, using either a keyboard, monitor, and mouse, a serial console, or a Web browser pointing at the default IP address to configure network settings. After initial configuration has been completed, the rest of the process is done via the clean, clear browser interface.

Importing users from Active Directory, Exchange Server, Lotus Notes/Domino, a file, or an LDAP server to set up DHA prevention and Web mail/quarantine access is straightforward, although setting up an LDAP query through Exchange/AD required some experimenting to get the query and log-in information right. You can allow users to access their own quarantine or limit access to the administrator only, depending on company policy and preference.

The system sends an e-mail digest of quarantine either to the administrator or to each user; the user can click on links in the e-mail to release a message, whitelist the sender, or delete the message. Releasing a message from quarantine is separate from designating a safe sender — releasing a message doesn't automatically add the sender to the whitelist, which means another step for the admin. There is also no way to see the message in the e-mail or by clicking on a link, so if you're not sure whether the message is spam from the sender or header, you have to open the quarantine through the browser, log in, and search for the message.

The e-mail firewall has a flexible policy engine that can limit the rate at which SMTP messages are accepted, based on the IP address of the sender or the spam score of the messages received from that address in the past. The policy engine has several different dictionaries, which allow you to set differing policies for potentially offensive language, phishing attacks, or words or phrases that might indicate leaks of proprietary data, using a custom dictionary. You can also scan for attachments — either by type (extension) or by name — and quarantine messages or forward them to a policy auditor, as desired.

With all these granular settings, and apart from its higher price and relatively minor management quirks, Proofpoint Protection Server is a solid e-mail security system.



Symantec Mail Security 4.1.1-3

### Symantec Mail Security 4.1.1-3

The Symantec Mail Security appliance is available in two versions, the 8240 (which I tested) and 8260, priced at \$1,995 and \$4,995, respectively. Content checking and e-mail security features are included in the base price; anti-spam and anti-virus functionality are priced per user, per year. With a spam catch rate of more than 97 percent and four false positives, all bulk, this appliance's performance is outstanding.

The appliance is easy to install, with initial network configuration accomplished via either a keyboard, monitor, and mouse, a serial terminal, or a browser using the default IP address. Basic configuration is easily done via the browser interface, which is wizard-driven and includes the simplest directory synchronization I've ever used, with auto-discovery of existing Active Directory, Exchange, or LDAP servers and automatic field fill-in.

The single configuration complaint I have with Symantec Mail Security is that the only way to bypass the strong password requirement is to set the password manually via console. There's no way to uncheck an "enforce strong passwords" box in the browser interface, and the password requirements are a pain, with dictionary checking and minimum character requirements. As an added annoyance, there's no guidance other than a failure message when you try to use a password that doesn't meet the requirements.

Security policies, however, are easy to configure and are very flexible, with a wide range of responses variable by type of policy, user, filter criteria, or incoming/outgoing messages. You can filter messages based on inappropriate content, possible leakage of proprietary data, attachment type, or content, and you can select a different response for different groups of users. For example, you could quarantine messages for one group of users and save a copy for others, drop inappropriate messages, notify an auditor of possible leaked data, and so forth.

For e-mail security, the e-mail firewall can throttle traffic based on sender IPs or based on spam messages, viruses, or

DHAs over a threshold of messages per hour. In addition, Symantec can integrate with Exchange via a plug-in to provide a dedicated spam folder, a feature Proofpoint doesn't offer. With this plug-in, users can move messages to and from the spam folder, automatically whitelisting messages moved out and blacklisting ones moved into the folder. This is a simpler process for most end-users, compared with logging in to the appliance through the browser interface.

### Beyond Spam

Previous versions of Symantec Mail Security, formerly known as Brightmail Anti-Spam, have consistently rated well in my testing, and this version continues the trend. Proofpoint did slightly better in filtering performance, but Symantec has the edge in ease-of-use and flexibility of configuration.

This is not to say that Proofpoint is hard to use or insufficiently flexible — both of these products are capable performers, and either should suit any organization looking for power and simplicity. The Symantec appliance wins out with slightly better ease-of-use, a better spam catch rate, and lower pricing, but if you find pricing for Proofpoint that's lower than what we were quoted for this review, you could choose it without fear of missing any features. 🐾

— Logan G. Harbaugh

# E-mail Attacks Getting Super-Focused

AT THE VIRUS BULLETIN CONFERENCE, ALEX SHIPP of messaging security company MessageLabs gave a presentation on targeted Trojan horse/industrial espionage attacks that was sobering. According to Shipp, MessageLabs is seeing an explosion in the number of very targeted attacks — typically between one and ten e-mails, compared to 10,000 or more for Warezov or another mass-mailed Trojan attack.

How hard is that to pick up? Well, MessageLabs will get more e-mails for a single Warezov variant on a single day than it will for ALL the targeted attacks for an entire year, Shipp said.

What they lack in quantity, however, the targeted attacks make up for in quality. Shipp noted that those behind targeted attacks will spend a great deal of time researching companies and their targets before even sending an e-mail. At the most basic level, the targeted attacks often use subject lines that key off some recent current event — bird flu, a prominent arrest, and so on. The most sophisticated targeted attacks might actually come by way of a compromised business partner, in which entire e-mail threads are intercepted by the hackers, then an attack e-mail is made up, posing as an email from the compromised business partner, sent to the correspondent within the target company and referencing content culled from the thread. The message might contain a Word or Excel document containing a zero day exploit that won't trigger antivirus software or gateway detection tools, and that will install a backdoor or downloader on the compromised system.

Shipp told of one attack that just targeted employees in a company's Research and Development group, but nobody else. Who wouldn't feel comfortable opening something that specific?!

Who's being targeted? A surprising variety of companies with "information that people want to steal:" law firms, pharmaceutical companies, petrochemical, news, tech,

medical research and even human rights organizations. Mostly these are "name brand" companies, but the attackers can go after smaller firms as well, depending on what they're after.

Most of the attacks are coming from Asia: China, Taiwan, and so on. But some are U.S. based as well.

Not surprisingly, antivirus firms often overlook these super-targeted, small scale attacks. In an example of one targeted attack from May, 2006, only four antivirus firms had signatures to detect the malicious code used in the attack by October, 2006.

Antivirus firms might have to slog 9GB of virus samples each day. "One email sent to one person that wasn't even part of your customer base, and that you'll never see again and none of your customers will either? The works hard enough on the AV guys anyway. There's just no time to do anything."

How do you know if your company is being targeted? Shipp said that if you're an IT security person working at a company of any size and with any valuable IP, and you don't know for sure that you already have been targeted by one of these attacks, you're already a victim. The only question is which systems on your network are owned, which data is being leaked, and how you can discover the compromised systems.

Good luck! ☞

— Paul F. Roberts