



3 Ways To Kill Spam Dead

ANTISPAM OFFERINGS FACE OFF IN 'LET'S CAN SPAM' SERIES

BY FAHMIDA Y. RASHID

CRN TEST CENTER Customers are drowning in unsolicited mail. Estimates of the amount of spam sent vary, but vendor estimates for 2007 range from 79 percent of messages to as high as 95 percent. Regardless, having a good spam filter in place is essential.

Which products actually deliver? That's the question the CRN Test Center plans to answer in a series of face-offs between the industry's antispam offerings.

We're starting here with a comparison of three products: MX Logic Email Defense Service, MX Ultimate Access from MX Logic Inc., Englewood, Colo.; Sendio ICE Box eMail Integrity Services Appliance from Sendio Inc., Irvine, Calif., and Sophos ES1000 from Sophos, Burlington, Mass.

But this is just the first of many antispam appliances, software and hosted services we're reviewing in an attempt to cover the mind-boggling variety of products that are available. So if your favorite isn't covered here, be patient. Check out CRN.com on April 28 for the next installment in the "Let's Can Spam" series.

Methodology

We evaluated the products with three viewpoints in mind: the solution provider, the system administrator and the end user.

Over a two-week period, all inbound traffic passed through the test product before reaching the mail server. Reviewers manually examined all mail before and after it passed through the test system to evaluate accuracy. Each system was given time to "learn" the mail before assessing its accuracy.

Reviewers also evaluated feature set, pricing, ease of deployment, management and reporting capabilities, and the ease in which users can correct errors. Each vendor's channel program was also evaluated.

The tests were conducted on a production mail server with a mix of live spam, malware and valid mail. The mail server, a Linux machine running exim, processed mail for five different domains, for a total of 15 distinct users. The box handled, on average, 14,000 to 15,000 messages each day, although that number was significantly higher at the end and beginning



1st

SCORECARD

MX Logic Email Defense Service

MX Logic offers an accurate spam filtering solution with extensive reporting and management tools in a hosted product.

Deployment



Security



Management



Ease of Use



Features



Profit Potential



of each month, corresponding with peak activity in general spam traffic. While a bulk of the valid messages were direct, some were warnings and alerts generated by various applications and systems, and some users were subscribed to mailing lists. Users accessed their e-mail accounts in several ways, including Microsoft Outlook Express, Mozilla Thunderbird, Web mail and mutt (a text-based mail client for Unix-based systems). Hosted solutions were tested with a mail server running one domain, with seven users.

MX Logic Email Defense Service, MX Ultimate Access

The only SaaS product in this set, MX Logic's mail filtering service blew reviewers away with its simple and comprehensive management interface, high accuracy rates and distinctive features. MX Logic also boasted a comprehensive, partner-friendly channel program.

MX Logic Email Defense Service utilizes the Stacked Classification Framework, which consists of multiple layers of spam-fighting techniques, to aggregate and analyze spam-likelihood scores. Reputation filtering is the first line of defense. MX Logic looks at the mes-

▶ BAKE-OFF

sage's SPF/Sender ID record, uses blacklists, whitelists and URL filtering, examines HTML tags and JavaScript, scans for worms and viruses, uses a multilanguage filter to identify phishing messages regardless of language, and performs deep content analysis to block attachment-based spam, including PDF files and image-based spam. MX Logic also utilizes a statistical Bayesian algorithm to determine the probability that a message is spam, based on how often elements have appeared in other spam e-mails. Finally, MX Logic applies its own proprietary rules based on the company's analysis of global spam. Messages that may or may not be spam are stored in user-specific quarantines accessible online.

As a hosted solution, nothing is installed at the customer site. The domain's MX record points to MX Logic's servers, so mail first is filtered through Email Defense. Spam messages are quarantined and legitimate mail is directed to the actual mail server for delivery. As such, deployment is straightforward. An account is created with the customer's billing address, domain name and e-mail address. The system administrator gets instructions on how to change the mail server's MX records. The solution provider can handle this for a fee. Users can be created to access quarantine information. A Web-based management interface, attachment and HTML filters are selected through the MX Control Console. By default, MX Logic rejects messages flagged as High spam and quarantines Medium messages.

About halfway through the test, a user on the test domain received about 300 messages an hour, of which 98 percent were denied, 1 percent was delivered and 1 percent was quarantined. This was a turnaround from the first day of testing, when about 20 percent of messages in quarantine were actually valid messages, and about a dozen spam messages showed up in the user's inbox. Since the service depends on the DNS entry having the updated MX record, some spam messages can bypass Email Defense and hit the mail server directly in the initial 24 hours. Towards the end of the test, the user reported having only one message every few days in quarantine that was fit to release and whitelist, and only one spam message squeaked through each day.

MX Logic offers a Message Continuity feature, where mail is queued if the mail server is down. Users can log in and read and reply to their messages even during an outage. Some solution providers use this feature as part of a planned migration, when moving one mail server to another.

The channel program has three tiers and is based on how much managed service support the partner wants or needs: F1, F2 and F3.

Margins can vary from 20 to 40 points, depending on the partner's MSP readiness.

Partners all have dedicated managers with MX Logic to provide field-based sales training, joint sales calls and market development. The Partner Portal offers deal registration and specific customer subscription information.

Sophos ES1000

The ES1000 from Sophos had very high accuracy results from the onset and quickly became a reviewer favorite during testing. Despite Sophos' strong partner program, MX Logic's program was more attractive, bumping the Sophos appliance down to second place.

The ES1000 is a 1U appliance weighing 26 pounds with an Intel Celeron D 2.93-GHz processor, 1 Gbyte of memory and a 160-Gbyte SATA hard drive. The ES1000 is capable of processing up to 20,000 messages per hour. It is a high-availability, managed appliance platform, relying on realtime security updates to scan and identify spam.

If a hosted solution ever decided to move onto a box, it would resemble the Sophos ES1000, since the customer doesn't need to worry about administration and monitoring. Sophos support centers proactively monitor every Sophos e-mail appliance using built-in sensors to measure unit temperature, disk space utilization and update status. The ES1000 performs self-maintenance activities automatically and allows administrators to monitor the box remotely.

The ES1000 was designed with ease of use in mind; deployment is no exception. Reviewers received the activation key before the unit arrived, and were able to get the appliance set up with DNS settings, domains, internal mail hosts and basic policy in less than 30 minutes. At the end of the setup wizard, the appliance conducted diagnostics tests.

The key selling point for the ES1000 is its Web-based management interface. The dashboard presents summary statistics, such as the day's total mail volume, blocked mail, detected spam and found viruses. It's easy to tell at a glance what viruses have been blocked.

Sophos has three levels in its partner program: Platinum, Gold and Silver. While

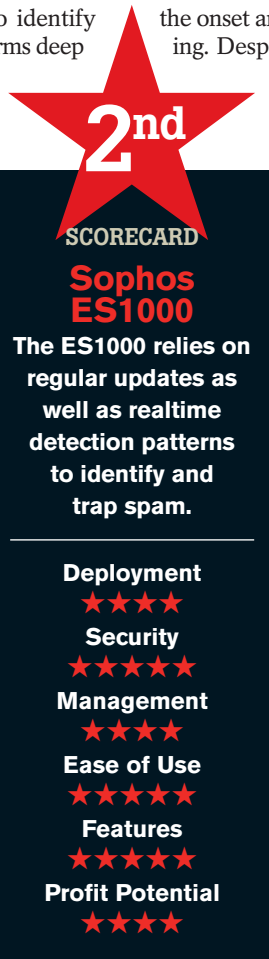
there is no cost to join the program, platinum partners commit \$750,000 in annual license sales and gold partners to \$250,000. All partners have access to lead management programs.

Sendio ICE Box eMail Integrity Services Appliance

Sendio approached spam filtering differently. The method works—reviewers received zero spam during the testing period. From a user standpoint, this is great, as the inbox is always clean and there are no false negatives where spam slips past, but reviewers felt uneasy with the company's approach.

The appliance functions on a simple rule: If mail is not for a valid account, it's dropped at the onset. This included mail addressed to former employees or made-up names. This wasn't a default option on other products. Sendio, for example, uses Sender Address Verification, where the message sender is matched against the recipient's Accept List.

The ICE Box stores incoming messages into a temporary folder. If the sender is new to ICE Box, it sends a challenge e-



▶ BAKE-OFF

mail back. The e-mail is politely worded, explaining it wanted to verify the sender's identity to stop spam. All the sender has to do is send a reply and the e-mail address is added to the approved-sender list.

The ICE Box monitors only mail coming from the outside, not intraoffice mail. This is handy, since the ICE Box can be configured to automatically kill mail that only looks like it came "from" the domain.

For end users, this is a breeze, since the chances of a spammer responding to the ICE Box challenge are close to nil as they use automated and anonymous mailers. But it does mean users are banking on the people sending them e-mail to recognize and respond to the challenge message.

For the solution provider, deployment is very straightforward: The partner tells Sendio the customer's IP address and what holes are open in the firewall. When Sendio ships the box, it's literally plug-and-go.

The ICE Box hardware is much more robust than the Sophos, with a 3-GHz Intel Pentium 4 processor, two 160-Gbyte hard drives, two NIC cards and 1 Gbyte of memory.

During testing, users had to log in to the temporary folder a few times to find the addresses and approve them so that error alerts would be delivered properly. Bulk messages also were manually approved. Logging into the ICE Box, users still have



SCORECARD
Sendio ICE Box
The ICE Box stops spam cold. But relying on senders to verify their identity means many valid messages may never get through.

Deployment ★★★★★
Security ★★★★★
Management ★★★★★
Ease of Use ★★★★★
Features ★★★★★
Profit Potential ★★★★★



to sift through a list of messages to try to find the occasional valid message.

Sendio has three tiers in its partner program: Diamond, Double Diamond and 5 Diamond.

Bottom Line

The MX Logic solution reminded us why SaaS is so popular. The mail-filtering service proved to be accurate, it learned quickly to decipher between spam and legitimate mail, was easy to configure and straightforward to manage, and it gives solution providers a wide range of revenue opportunities.

The Sophos ES1000 had high accuracy rates and an exceptionally thorough management and reporting console. The Sophos channel program was robust, but it's hard for an appliance vendor to match the flexibility a SaaS vendor can offer.

The Sendio ICE Box delivers on its promise better than anyone else: It stops spam cold. We're concerned about users missing messages because they didn't notice it in their temporary folders or because the challenge e-mail went to the sender's own spam folder. In a perfect world where everyone knows about the ICE Box, this wouldn't be an issue, but sadly, that day has not yet come. ■

Shopping The Ingredients

VENDOR	PRODUCT	LIST PRICE	PARTNER INCENTIVES	PROGRAM PARTNERS	PROGRAM COSTS	DISTRIBUTORS
■ MX Logic Englewood, Colo. (877) MX-LOGIC (695-6442) www.mxlogic.com	MX Logic Email Defense Service, MX Ultimate Access	Depends on number of seats, starts at \$0.73 per user per month	Highly competitive margins, customer programs to speed up the sales cycle	1,000	None for live sales training and Web-based sales and technical training	Ingram Micro, Alternative Technology
■ Sendio Irvine, Calif. (949) 274-4375 www.sendio.com	Sendio ICE Box eMail Integrity Services Appliance	\$1,995	Number of programs through the year; rebates for govern- ment and education; SPIFF between \$250-500 per unit	50	None	DoxElectronics, DataMatrix Systems, Dempsey Bluevar, Zyrka, Mobilizz
■ Sophos Burlington, Mass. (866) 866-2802 www.sophos.com	Sophos ES1000	\$3,295	Protection and guaranteed margins for registered deals, SPIFF and special incentive programs	1,000	None for Web and on-premise partner training. Costs for on-premise Sophos technical training can be waived depending on level and relationship	None