

NetworkWorld Reprint

The leader in network knowledge ■ www.nwfusion.com

December 20, 2004 ■ Volume 21, Number 51

INWILD
THE
Anti-spam

SPAM IN THE THE SEQUEL WILD

This time, we tested
(almost) everyone

■ BY JOEL SNYDER, NETWORK WORLD LAB ALLIANCE

HOW BIG CAN A TEST GET? We found out with our latest in-depth look at the anti-spam industry. Spam is still a huge problem, and there is an equally large market opportunity to fix it.

INWILD
THE
Anti-spam

We invited every anti-spam vendor in our online Buyer's Guide (see www.nwfusion.com, DocFinder: 5047) to participate. While we expected to get eight to 10 vendors to sign up, 41 participated. We tested them all for spam catch rate (including false-positive and false-negative rates), and performance and throughput.

Then we let the products speak for themselves. Out of the 36 that made it through the first round, we felt any product with a greater-than-90% spam catch rate and lower-than-1% false-positive rate should get a more in-depth evaluation (see page 34). We still ended with a dozen excellent finalists, reflecting the growing maturity and commoditization of anti-spam products.

Analyzing the spam test results

False positives: The best scores in our test all reflect products that have gotten the science of not tagging legitimate mail as spam down to the noise level. Any false positive is a problem, and non-delivery receipts (NDR) and mailing lists caused the most problems for the anti-spam products. Many mailing lists might be unimportant, but some are critical. The same is true for NDRs. If you send a mail and it doesn't go through, your only clue is the NDR coming back from your own mail system or, sometimes, the other end. Anti-spam packages that filter these out a little too zealously (because they assume that most NDR messages are the result of a mass-mailing worm), which we found in many of the products we tested, break that feedback loop and make mail less reliable.

“The best balance [of accuracy and false positives] came from service provider Postini, which had a 97% spam catch rate and only six false positives.”

In last year's test, false-positive rates were much higher, and we said a quarantine was a critical requirement. This year, while the false-positive rate has dropped overall, we still think that most businesses using e-mail as a critical communications tool need some way to deal with false positives.

Picking our favorites

These products have proven themselves capable of doing a great job of filtering spam. It's not a question of better or worse — it's more a question of “What solves your problem best?”

When it comes to roll-your-own software, Sophos' and MailFrontier's offerings impressed us in many ways. But in the world of software-based systems, there are lots of different ways to solve the same problem. For example, if all you want is outstanding spam control, the uncluttered approach of Cloudmark might be your best bet.

On the appliance side, BorderWare was a pretty clear favorite. Although it didn't top other appliance-based anti-spam solutions in every category, it showed excellent design and implementation throughout our testing.

That said, we think Messaging Architects and CipherTrust

should also be on your short list. Barracuda's appliance has a fantastic start so early in its life cycle, but issues in management and security kept us from seeing it as an enterprise-class solution today.

If you are looking for a service, Postini gets top billing for the second year in a row. Although Advscan did a great job in filtering mail, our inability to customize it pushed it down on our preference list. With Mycom, the feature set was tremendous for a service, but some consistent delays in performance of the Web GUI and in mail delivery were a concern.

Snyder is a senior partner at Opus One in Tucson, Ariz., specializing in information security and messaging applications. He can be reached at joel.snyder@opus1.com. The author acknowledges the generous help of Chris Janton and Jan Trumbo on this project.

Accuracy

Vendor	False positives	Vendor	Spam caught
BorderWare (MS=S)	0.04%	0Spam.Net	99%
Sophos	0.04%	Netriplex	99%
BorderWare	0.04%	Vircom	98%
Postini	0.08%	Process Software	98%
CipherTrust	0.12%	Postini	97%
Symantec (MS=S)	0.16%	MailFrontier (MS=S)	97%
Symantec	0.16%	Messaging Architects	97%
Advascan	0.19%	NoSpamToday!	97%
Proofpoint	0.20%	SpamStopsHere	97%
CipherTrust (MS=S)	0.23%	BlueCat	97%
MailFrontier	0.25%	Intellireach (MS=S)	97%
Proofpoint (MS=S)	0.29%	Advascan	96%
Barracuda	0.30%	Process Software (RR)	96%
Spamfighter	0.34%	Roaring Penguin	95%
Cloudmark	0.35%	MailWise	95%
NetCleanse	0.46%	Solid Oak	95%
NetIQ	0.55%	CipherTrust (MS=S)	94%
MailFrontier (MS=S)	0.54%	Proofpoint (MS=S)	94%
Process Software (RR)	0.75%	Barracuda	94%
Mycom	0.89%	Clearswift (MS=S)	94%
Aladdin	0.92%	Symantec (MS=S)	93%
Messaging Architects	0.94%	Cloudmark	93%
Sybari	1.25%	Mycom	93%
Vircom	1.63%	Mail by Design	93%
NoSpamToday!	2.00%	Symantec	92%
Mail by Design	2.13%	Proofpoint	92%
Policy Patrol	2.16%	BorderWare (MS=S)	90%
SpamStopsHere	2.34%	Sophos	90%
Process Software	3.15%	ZixCorp	89%
Intellireach	3.32%	BorderWare	88%
Roaring Penguin	3.37%	CipherTrust	88%
Sublimemail	4.00%	Aladdin	87%
BlueCat	4.08%	Policy Patrol	87%
Clearswift	4.13%	Tethernet	85%
MailWise	4.32%	Spamfighter	83%
eSoft	4.91%	MailFrontier	81%
Intellireach (MS=S)	5.48%	NetCleanse	81%
0Spam.Net	5.52%	NetIQ	79%
ZixCorp	5.90%	Clearswift	78%
Clearswift (MS=S)	8.46%	Intellireach	62%
Netriplex	9.12%	eSoft	58%
Tethernet	14.34%	Sybari	54%
Solid Oak	19.86%	Sublimemail	47%

Key: Services, Appliances, Software