

Corporate Antispam Tools

BY CADE METZ

THE INDEPENDENT GUIDE TO TECHNOLOGY

FEBRUARY 25, 2003

EDITORS' CHOICE

Installed: CipherTrust IronMail 210 **Hosted:** Postini Perimeter Manager

None of the corporate anti-spam solutions in this roundup are flawless, but these two edged out the competition.



We like the CipherTrust IronMail 210 best. Yielding the top accuracy results in its subgroup, the appliance caught over 94 percent of the spam it encountered during testing and had a false-positive rate of only 0.24 percent. The unit also offers excellent policy configuration and guards against hack attempts. Though it requires more IT maintenance than Brightmail Anti-Spam 4.0, IronMail offers abundant controls that are much easier for the administrator to use than those of SurfControl E-mail Filter.

For companies that want the control of an in-house solution and don't mind the extra IT maintenance or cost, an installed system is the answer.

If you don't want to dedicate a lot of company resources to fighting spam, look for a hosted product. Although MessageLabs SkyScan AS requires less management and scored better on our tests than Postini Perimeter Manager, SkyScan offers no way for end users to retrieve an e-mail incorrectly identified as spam and very limited tuning options for administrators. Here, **Postini Perimeter Manager outshines the competitors.** Perimeter Manager gives both IT personnel and end users control over spam filtering. It also lets managers assign multiple levels of rights and protects against directory harvest attacks. Although Perimeter Manager generated the most false positives on our tests, its tools for retrieving them and tuning the system to your needs make this less of a problem.



Postini Perimeter Manager

500 to 1,000 users, \$17 per user per year.
Postini Inc.
www.postini.com



Postini Perimeter Manager is a balanced antispam solution that will please both administrators and end users. The hosted service combines versatile Web-based administration with leading-edge technology for detecting directory harvest attacks.

During our tests, Postini's accuracy was less than ideal. But it does a good job with the realities of administering even complex enterprises by delegating spam-fighting chores to ordinary users and designated administrators.

Directing our mail flow to Postini's spam-filtering servers allowed us to tap a global network of data centers with a different approach to attacking spam. Postini's servers look at raw SMTP packets for telltale patterns of spam activity. One advantage of this is that messages are processed in real time (as they are in the hardware-based CipherTrust IronMail 210). Another advantage is a defense against *directory harvest attacks*—a technique spammers use to gather addresses of members of your organization by running scripts against SMTP. Postini's data centers rely on Solaris and Intel x86 hardware running Oracle and proprietary software.

The administrative control offered by Postini Perimeter Manager leads the pack. The Web-based console provides good granular control of organizations and users. The solution's support for delegated administration, offering different levels of rights, is unmatched. That said, we found several of the administration screens a bit overcrowded with settings.

For basic configuration against spam, Perimeter Manager let us choose among categories to block, such as bulk e-mail, pornography, get-rich-quick schemes, and special offers. (Postini offers e-mail antivirus protection licensed from McAfee at extra cost.) You can also set whitelists and blacklists manually using the Approved and Blocked Sender features.

	Power of administration	Ease of administration	Interface	Spam defense mechanisms	Spam management	Reporting	Accuracy	OVERALL
INSTALLED								
Brightmail	●●	●●●●	●●	●●●●	●●	●●	●●	●●
CipherTrust	●●●●	●●	●●	●●●●	●●●●	●●	●●●●	●●●●
SurfControl	●●●●	●●	●●	●●●●	●●●●	●●	●●●●	●●●●
HOSTED								
Big Fish	●●	●●●●	●●●●	●●●●	●●	●●●●	●●●●	●●
MessageLabs	●●	●●●●	●●●●	●●●●	●●●●	●●●●	●●●●	●●●●
Postini	●●●●	●●●●	●●●●	●●●●	●●●●	●●●●	●●	●●●●

RED denotes Editors' Choice.

Perimeter Manager's reporting is above average though not as powerful as that of SurfControl E-mail Filter. We especially like the graphical snapshot of current e-mail activity. Beyond this, you can view e-mail traffic, blocked e-mails, and stopped viruses by IP address, domain, user, or category. For further traffic analysis, you can download any reports as CSV files via links on the report pages.

One drawback is that the traffic report is not much more than a dump of a log file. We'd prefer to see an HTML presentation of data rather than just raw text. Postini's e-mail alerts, however, are outstanding, with an option to reach wireless pagers and PDAs.

Nonadministrators can modify their own spam settings using the Postini Message Center, which is decidedly simpler and more approachable than the administrative interface. It shows quarantined

e-mail and provides options to deliver or delete messages. Better yet, you can choose to whitelist or blacklist specific addresses.

We also like Postini's support for wireless technology, unique among the products we reviewed. Using this feature, Postini can automatically forward copies of e-mail to your PDA—a basic but useful function.

Postini's solution offers plenty of customization if you need it, but digging into the administrative features is largely optional. The other hosted products in this review are turnkey solutions and don't let you delegate as much control to different groups. And as more and more spammers make use of directory harvesting, other antispam solution providers will have to catch up with a problem Postini has already solved with its innovative technology. ☰

PERFORMANCE TESTS

How We Tested



Every corporate antispam solution we tested did a better job than the personal products, but don't expect any of them to solve your spam problems completely overnight. Several of the vendors claim that over time their solutions improve, as users and administrators train the software to tell the difference between wanted and unwanted e-mail. To test corporate antispam products, PC Magazine Labs built a production-caliber e-mail environment that inundated each tool with an average of 2,500 e-mail messages over several days. (Note that these tests used a different setup from the one in the Personal Antispam Tools section.) As e-mail traffic flowed into the e-mail accounts of a group of PC Magazine editors and labs staff, a duplicate of each message was diverted to the test domain and copied to a Microsoft Exchange 2000 Server with Service Pack 3. The message IDs in the header information were not modified, which is important for tools that rely on header analysis as a defense mechanism.

We categorized all unsolicited bulk-marketing e-mail as spam, with one exception. Much of the e-mail that we in the media business receive is *gray spam*—unsolicited but relevant industry newsletters and press releases—which we excluded from our calculations. Every vendor except Brightmail was inconsistent in whether it placed newsletters in the quarantine queue or sent them to the e-mail in-boxes. Because you can adjust most antispam software to your preferences, over time this problem would probably disappear.

We categorized all unsolicited bulk-marketing e-mail as spam, with one exception. Much of the e-mail that we in the media business receive is *gray spam*—unsolicited but relevant industry newsletters and press releases—which we excluded from our calculations. Every vendor except Brightmail was inconsistent in whether it placed newsletters in the quarantine queue or sent them to the e-mail in-boxes. Because you can adjust most antispam software to your preferences, over time this problem would probably disappear.

We relied on some metrics used in the science of epidemiology. The *false-positive* percentage is the percentage of legitimate e-mail an antispam tool has incorrectly identified as spam and quarantined. The *false-negative* percentage is the percentage of actual spam the tool has identified as legitimate mail and delivered to the in-boxes. We also show you graphically which portions of both the in-boxes and the quarantine queue were correctly and incorrectly identified.

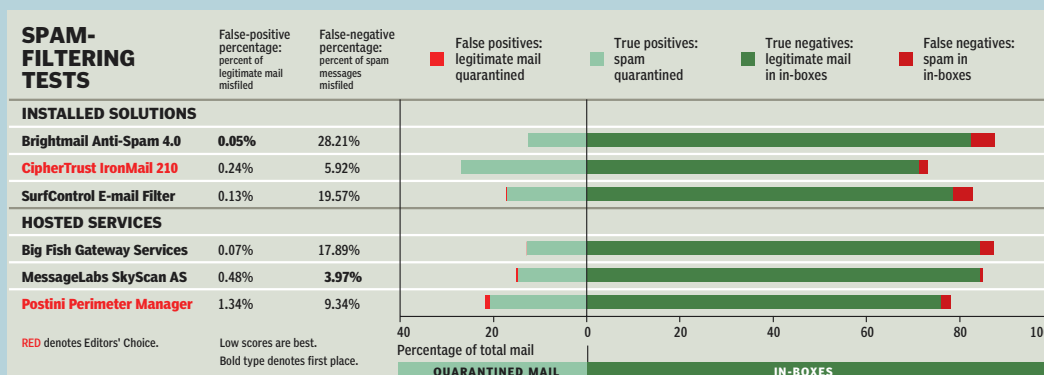
Low false-positive scores were the norm across all the solutions. Although Postini Perimeter Manager had a relatively high false-positive rate (1.34 percent), we traced this back to a single e-mail it identified as spam that was proved valuable to our test users, who circulated it. This created a ripple effect, inflating the false-positive score. Without it, Postini's false-positive percentage would have decreased 24 percent. This incident illustrates the importance of good management tools and end user tools that let employees retrieve quarantined legitimate e-mails and use whitelists.

Results from Brightmail Anti-Spam 4.0 require some interpretation, as it uses a unique methodology to diagnose spam. Relying on a very specific definition of spam, it quarantined only one false positive across all our test accounts. But this definition was not as sensitive as the those of the other products, yielding an unacceptably high false-negative rate.

Even one-tenth of a percent difference in these scores could have a big effect on an organization that receives thousands of messages per day. Yet these performance results should be only one factor in your buying decision. We like Postini's excellent management tools and white-list capability enough to recommend it above MessageLabs SkyScan AS.

Finally, each product needs to do a better job of diagnosing the rising problem of spam in non-Latin alphabets, such as those used by most Asian languages. These languages use double-byte or multibyte character sets whose increased complexity produce added challenges for spam detection algorithms.—*Analysis written by Sahil Gambhir*

▼ Each bar shows the total set of e-mail examined. The left side of the chart is e-mail the product identified as spam. The right side of each bar is e-mail delivered to the users' in-boxes. The green portions of each bar show how much of the mail a product correctly identified as either spam (light green) or legitimate mail (dark green). The red portions of each bar show mail incorrectly identified as either spam (false positives) or legitimate mail (false negatives). The table to the left of the chart shows false-positive percentages (the number of legitimate messages misdiagnosed) and false-negative percentages (misdiagnosed spam).



Posted from PC Magazine with permission from Ziff Davis Media Inc. by Reprint Management Services.

Copyright 2003 Ziff Davis Media Inc. All Rights Reserved.

#445746 Managed by Reprint Management Services, (717) 399-1900. To purchase reprints online, visit www.reprintbuyer.com.