

ENTERPRISE SPAM TOOLS

F I R S T L O O K S

THE INDEPENDENT GUIDE TO TECHNOLOGY

NOVEMBER 11, 2003



Postini Perimeter Manager™

Nobody has as rich a hosted antispam service as Postini. Postini Perimeter Manager is essentially a mail management operating system with a Web interface, including elaborate tools and facilities unmatched by any other product or service we tested.

Postini is available only as a hosted solution. The company has licensed its spam-scoring technology to Trend Micro, which implements it in its Spam Prevention Service, which we also tested, but this is a small part of the Postini service.

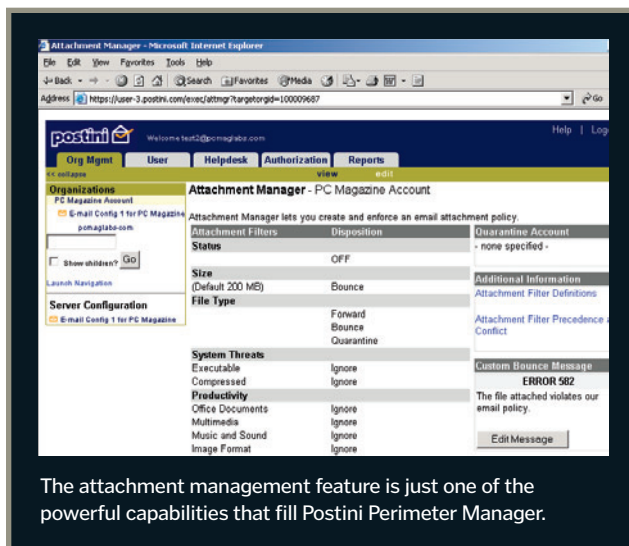
One standout feature is the ability to delegate capabilities to users and groups over and above global policies set for organizations. For example, an administrator would normally set a particular level of sensitivity to types of spam for the organization as a whole. Administrators can allow specific users and groups to modify their threshold levels. They can also allow or deny users access to the spam quarantine.

Wherever you look in Perimeter Manager, there's another capability beyond what you would expect in a simple antispam tool. You can set policies for attachment handling in the organization (for instance, blocking troublesome files, like PIF and SCR, which are usually associated with worms), and specify different size limits on attachments for different groups. You can also give specific management capabilities to help desk personnel in your organization, letting them grant or deny user privileges.

A set of APIs keeps your network directory in sync with the Postini directory; or you can use bulk import/export. There's even a server-side scripting language for performing bulk operations.

Unique to Postini's software is the scoring system. The administrator (or users, if the admin allows) sets a series of sensitivity levels for general spam, as well as subsets of spam types (Sexual Content, Make Money Fast, Commercial Offers, and Racist Content). Setting a sensitivity level higher or lower to one of the categories will increase or decrease the chances that such a message will be tagged as spam.

Perimeter Manager looks at a lot more than just the content.



The attachment management feature is just one of the powerful capabilities that fill Postini Perimeter Manager.

For instance, it checks for signs of falsified mail headers, and it performs heuristic analysis of the actual SMTP traffic coming from the server. Any of these other considerations could block a message before it ever gets to the content-based scoring system. Perimeter Manager also scans every message for viruses and worms, potentially saving money on such costs at the gateway.

Performance was right in line with the pack. Without tweaking, the package caught 84.9 percent of our spam messages. Its false-positive rate was a little high (1.4 percent), but these were all newsletters whose senders could be white-listed, not messages from individuals.

If you're uncomfortable with a hosted solution, you'll need to look elsewhere. Similarly, if you're paranoid about false positives, you may be better off with BrightMail's package. But you can't beat Postini for sheer administrative power.

Postini Perimeter Manager

Direct price: \$15-\$20 per user per year. Postini Inc., 888-584-3150, www.postini.com. ●●●●●

Several Approaches, Including Some that Work

BY LARRY SELTZER

Client-side spam utilities like Norton AntiSpam 2004 are fine for home users, but any business large enough to have a mail server needs something more: a server-side solution that traps spam before it hits employees' in-boxes. Leaving each worker to comb through messages each morning is a productivity killer, not to mention the possible legal ramifications of inappropriate material reaching an employee's desktop.

The accuracy with which a program identifies spam is the most important characteristic of these products, but it's not the only consideration. In this story, we also focus on administrative features and look at different types of products, including hosted services, gateway-level filters, and one that integrates directly into Microsoft Exchange.

For this roundup, we gathered five recent enterprise-class solutions and invited back our Editors' Choice winner (Postini Perimeter Manager) from our previous spam feature ("Slam the Spam," February 25) to see how the latest build compares. To test the products in this roundup, we redirected e-mail from a Ziff Davis Media catch-all account to Microsoft Exchange servers with each product installed.

We acknowledge that our four-day test window for each product didn't net the sheer volume of mail a large enterprise would see in the same time frame, so as the saying goes, your mileage may vary. (For example, we are not saying that Brightmail Anti-Spam 5.1 will catch 88.9 percent of spam for your organization with a 0 percent false-positive rate, as it did for us.) But since we performed the same test methodology for all of the products, our results can be used to compare each solution

to see how it fares relative to the others.

We ran each product in its default configuration, without the tweaking and tuning an administrator would do to adjust the threshold just right for his organization. In general, when compared with the personal spam-blocking utilities we've tested to date, these enterprise solutions allow more spam through. But that's because the developers are being more sensitive to false positives; snaring a legitimate inquiry from a customer is more costly than letting a few more spam messages through.

Except for iHateSpam, which blocked legitimate mail as well as some newsletters, every product's false positives (legitimate mail snagged as spam) can be attributed to newsletters in our e-mail mix. It's important to note, however, that the same type of newsletters that were labeled as spam also managed to get to our in-box.

