

InfoWorld

February 16, 2004 ■ Issue 7

GET TECHNOLOGY RIGHT



SECURITY EXCLUSIVE

Trimming the Spam (excerpted)

CipherTrust IronMail 4.0

Easy to use and configure, the IronMail appliance produced excellent results in my tests, and with no per-user cost it should be especially cost-effective in

deployments with large numbers of users. Additional security and content control features offer extra value for the price.

IronMail offers a wide range of sophisticated features, including both anti-spam and anti-virus services and a variety of additional security features, including content checking, attachment filtering, Exchange firewall and reverse proxy capability, and intrusion detection. These features will be a boon to companies that would rather consolidate e-mail security in one place and that don't already have these features in a firewall or other appliance.

This 1U, Intel server is based on an IBM eServer xSeries 305 system. Since on-site installation support is included, administrators will have little to do other than following the preinstallation checklist.

A wizard takes you through the initial setup. From there,



CipherTrust IronMail 4.0

the IronMail appliance can be attached to the normal network, and the rest of the configuration can be accomplished through a browser. The appliance connects to CipherTrust's network for updates to filtering criteria and to share information on new trends in spam with information collected from all the other IronMail appliances.

Configuring IronMail is necessarily complex, given the large number of capabilities it offers. For instance, an admin can change the filtering order (anti-virus, anti-spam, content filtering, mail monitoring) and anti-spam filter order (Bayesian, ESP,

blacklist), and there are a number of anti-spam filters to be configured. The primary filter is the ESP (Enterprise Spam Profiler), which uses a set of 15 tools. This is a larger variety of different tools than I have seen in a single product before, which allows for considerable flexibility, although not necessarily any greater effectiveness than other solutions.

Other filters include a statistical look-up service, which creates a hash of messages (a unique identifier of the subject and body of the message) that it shares with all IronMail systems worldwide, looking at the total message frequency to

CipherTrust IronMail 4.0

CipherTrust ciphertrust.com

EXCELLENT 8.6

Manageability(25%)	8
Performance (25%)	9
Ease of use(20%)	8
Setup(20%)	9
Value(10%)	9

COST: Initial cost, \$27,000; annual costs, \$4,860

BOTTOM LINE: The IronMail 4.0 appliance is easy to set up, delivers great performance, and offers very sophisticated security features such as intrusion detection, a reverse proxy for Exchange, content filtering, and anti-virus. Logging features are complete, and adding users is easy.

determine if a message is spam or bulk.

A whitelist of usual legitimate bulk mailers is included, another extra not common to anti-spam solutions. The whitelist can cover sender or recipient, with wildcards, for any part of the system — not just anti-spam but anti-virus and content checking as well. The system can automatically add addresses to the whitelist based

on outbound messages and the number of messages in a given time. Otherwise, the approach to whitelisting is a manual process, accessible only to the admin, which is fairly cumbersome.

Attachment checking looks at both the file name in the message and the actual file, regardless of name; it can also check Zip files. The feature can look for specific attachments

and send an alert if a message is encrypted.

The content filters have a log-only mode so administrators can test new filters before deployment. Other options for processing spam and applying filters include changing the header, quarantine, forwarding normally, copying suspect messages to a second account, rewriting the subject or dropping the

message. A search feature enables users to find processed and quarantined mail sent or received that day or to look at logs of what happened to the mail.

If you're looking for a full-featured e-mail security appliance that also filters spam, CipherTrust brings an exceptional variety of capabilities to the table.

—Logan G. Harbaugh



**4800 North Point Parkway
Alpharetta, GA 30022
main: 678.969.9399
fax: 678.969.9398
toll free: 877.448.8625**