by Paul Robichaux

Scope It   Plan It   Buy It   Solve It

Enterprise Spam Filters

Scan your email servers to prevent spam

The volume of spam messages we receive seems to be growing, with no end in sight. And little wonder: *The Wall Street Journal* recently ran an article about a spammer who makes more than $200,000 a year by filling people's email Inboxes with junk. Microsoft receives approximately 200,000 spam messages per day.

Along with the explosive growth of spam has come a corresponding growth in the number of products and services that cut down the amount of spam entering users' mailboxes. An ongoing race exists between two clever and determined forces: spammers and antispam vendors.

The technology that vendors use to fight spam varies. Keyword scans look for terms, such as "free," "XXX," or "refinance," that are often used in spam messages. Some products scan only the message headers, whereas others include the message body and attachments. Contextual analyzers flag messages according to spam indicators such as the presence of many exclamation points or dollar signs in the subject line or a blank To line coupled with a Bcc field in the header. Other products reference blacklists of known spammers' IP addresses to determine whether an email message is from a known spammer or a known spammer's ISP. Collaborative filters add spam message signatures to the filter list so that all sites that use the list can block the same spam messages. Some spam preventive procedures attempt to identify spam messages by scanning the number of capital letters or punctuation marks in the header, the number of addresses the sender is delivering the message to, and the rate at which incoming messages from the same sender arrive at a given server. Some products let you configure specific scanner settings (e.g., the keyword list, contextual analyzers, IP address blacklist sources).

Most antispam products implement more than one of these filtering methods and let you choose to delete suspected spam before it reaches your Inbox (which risks deleting legitimate email messages erroneously identified as spam), quarantine suspicious messages, or tag suspicious messages so that a client-side rule can file the message accordingly. Be prepared to spend some time experimenting to find the right mix of settings and adjusting them over time as spammers change their methods of operation.

Antispam products offer a wide range of abilities and features but in general fall into five categories: Client-side filters, appliances, Exchange plugins, standalone SMTP proxies, and hosted services. Client-side filters install on the desktop; some client-side filters run as Exchange plugins, and others act as POP3 proxy servers.

This issue's Buyer's Guide highlights appliance- and server-based antispam products. Appliances are dedicated hardware devices that install at the network perimeter and scan incoming mail. Hardware solutions tend to be more expensive than software-only solutions but generally offer easier configuration and maintenance.

Exchange plugins provide the advantage of not requiring a separate server, but you need to carefully assess such products' stability and vendor support before making a commitment. Standalone SMTP proxies sit on the network perimeter and scan all your incoming mail, which is beneficial because you don't have to make any Exchange server changes; however, not all proxies correctly handle the full set of SMTP extensions that Exchange supports. Notably, most proxies don't support the STARTTLS or 8BITMIME protocols. Hosted services act as SMTP relays: You point your DNS MX records to the vendor's servers, which accept and filter mail for your domains and relay legitimate mail back to your servers.

PAUL ROBICHAUX (getting-started@robichaux.net) is a principal engineer for 3sharp and an MCSE. He is the author of several books, including *Secure Messaging with Exchange 2000* (Microsoft Press), and creator of the http://www.exchangefaq.org Web site.

The Wall Street Journal **recently ran an article about a spammer who makes more than $200,000 a year by filling people's email Inboxes with junk.**

InstantDoc ID 38277

Contact Information	Product Name	Price	Description
SOFTWARE			
ActiveState 604-484-6400 866-866-2802 http://www.activestate.com	PureMessage	Licensed per CPU	Email-filtering software for corporate policy enforcement and spam and virus protection; features configurable filters that provide full control over the security and usage of corporate email systems at the gateway level
Brightmail 415-365-6180 http://www.brightmail.com	Anti-Spam 4.0 Enterprise Edition	$4 to $15 per user per year	Antispam software that features BrightSig, technology that automatically eliminates standard and polymorphic spam attacks at the messaging gateway and uses multipoint rules to prevent false positives; works with Windows 2000, Sun Microsystems' Solaris, Exchange, and Lotus Notes
BVRP Software 303-450-8296 http://www.bvrpusa.com	Mail Warden	$703	Antivirus and spam software for Exchange, Lotus Domino, and SLmail mail servers; combines email filtering capability with Norman Virus Control technology
Clearswift 425-460-6000 888-888-6883 http://www.clearswift.com	CS MAILsweeper for SMTP and SpamActive	$1387 for 50 users; Spam-Active is free to users with current support contracts	Policy-based content-filtering software that works with SpamActive to increase detection and prevention of spam at the gateway; is available as a value-added service to Clearswift customers with current support contracts; SpamActive is managed and delivered through Clearswift's ThreatLab
Computerized Horizons 508-799-4548 888-694-6882 http://www.declude.com	Declude JunkMail	$249 to $895	Software that supports both public spam detection and internal spam detection procedures; features multihop scanning capability, country of origin detection based on IP address, a weighting system to identify legitimate email messages, settings you can customize by user, Habeas support, and 12 actions to take against spam
DataEnter support@dataenter.co.at http://www.dataenter.co.at	XWall for Microsoft Exchange	$298	Firewall software that protects your Exchange server from viruses, spam, and dangerous attachments
GFI 919-388-3373 888-243-4329 http://www.gfi.com	GFI MailEssentials for Exchange/SMTP	$225 for 10 mailboxes	Software that provides spam protection at the server level; adds other email tools to your mail server, including disclaimers, archiving, reporting, server-based autoreplies, and POP3 downloading
GROUP Software 508-473-3332 877-476-8755 http://www.group-software.com	securiQ.Wall	Starts at $3162 for 150 users	Server-based software solution that scans email content and enterprise databases to block spam; protects against confidentiality breaches; available as a module of the securiQ suite, which performs other Exchange security functions
Hexamail info@hexamail.com http://www.hexamail.com	Hexamail Guard	$650	Antispam software that analyzes incoming and outgoing email at the Internet gateway to eliminate spam and ensure that outgoing email is legitimate; features statistical pattern-matching capability combined with advanced configurable rules
IntelliReach 781-407-9899 800-219-9838 http://www.intellireach.com	Message Manager Suite for Exchange	Starts at $4995	Software that stops spam and helps you manage an email message's full life cycle; lets you filter and audit in realtime; lets you search and secure historical email messages; protects against abusive and noncompliant email messages

Contact Information	Product Name	Price	Description
SOFTWARE continued…			
Lightspeed Systems 661-324-4291 877-447-6244 http://www.lightspeed systems.com	Total Traffic Control	$5495 as software only	Spam Blocker software module provides whitelists, blacklists, Realtime Blackhole List (RBL) queries, message-header scanning, and advanced statistical sampling of spam and legitimate email to create a spam-pattern comparison file; Web-based reports are searchable by sender, receiver, and subject line
LogSat Software 407-650-3008 http://www.logsat.com	Spam Filter	$200	Software for ISPs and companies running SMTP servers; works as a proxy to an incoming SMTP server; forwards nonspam messages to the Message Transfer Agent (MTA); you can specify domain exclusions to identify specific domains as spam senders; runs on Windows and Linux
Mail-Filters.com 650-655-7700 800-555-1212 http://www.mail-filters.com	SpamCure	$1 to $5 per mailbox per month	Spam-filtering software that provides 11 test categories; you can customize the filter to detect unwanted email by domain or by user
NetIQ 408-856-3000 888-323-6768 http://www.netiq.com	NetIQ MailMarshal for SMTP	Pricing starts at $600 per 100 users	Server-based email-scanning software that enforces your organization's acceptable-use policy; protects against viruses, spam, and loss of confidential data; provides transparent perimeter security; a Win2K Datacenter Server–certified email-scanning solution
Nemx Software 613-831-2010 http://www.nemx.com	Power Tools for Exchange 2000 Advanced and Internet Editions	Advanced Edition starts at $999; Internet Edition starts at $795	Software that provides email content management for Exchange 2000 Server; RBL technology provides realtime information to identify and eliminate external and internal email threats; increases overall Exchange performance; integrates into Exchange 2000 architecture without requiring proxy servers or hardware and soft-ware upgrades
Network Associates 972-308-9960 888-847-8766 http://www.network associates.com	McAfee SpamKiller Enterprise	Contact vendor for pricing	Filters email to defend against unwanted messages; conducts more than 750 tests and heuristic scans to analyze messages and identify spam; after identifying spam, determines the appropriate action; lets you reject messages or log them for further review; doesn't require special configuration; scalable to your growing network
PlexObject Solutions 847-705-5183 http://www.plexobject.com	PlexMailer 1.4	$495 for 50 users	Java-based antispam software that uses blacklists to scan email contents and headers; includes an analysis engine that produces a detailed report of spam message-routing information; identifies concealed headers and email addresses from which the spam originated
Red Earth Software 309-279-1189 http://www.policypatrol.com	Policy Patrol Enterprise 2.0	From $375 for 10 users	Software that uses multiple realtime blacklists and scans header, content, and number of recipients; lets you delete, quarantine, or tag a spam message; uses whitelists to minimize false positives

Contact Information	Product Name	Price	Description
SOFTWARE continued…			
Sunbelt Software 727-562-0101 888-688-8457 http://www.sunbelt-software.com	iHateSpam	Priced per mailbox on a sliding scale; approximately $4 to $12 per mailbox	Server-based antispam software that filters spam at the gateway; can optionally route messages to a folder in a user's mailbox; user can create personal whitelists and blacklists; lets you use policies to set custom rules, whitelists, and blacklists at the server level; supports Exchange 2000
SurfControl 831-431-1400 800- 368-3366 http://www.surfcontrol.com	SurfControl E-mail Filter 4.5	$18 per user for 500 users	Software that combines antivirus, antispam, and email-auditing features; offers optional plug-in components
Sybari Software 631-630-8500 800-239-1095 http://www.sybari.com	Sybari Spam Manager	Contact vendor for pricing	Content-filtering software module for spam, offensive language, and confidential information
Tech Mavens 408-733-5804 http://www.tech-mavens.com	MavenFilter	$295	Server-based email-filtering software with Web-based interface that lets you review blocked messages and unblock legitimate messages
Trend Micro 408-257-1500 888-588-7363 http://www.trendmicro.com	InterScan eManager	Contact vendor for pricing	A server-based plugin for InterScan Messaging Security Suite; blocks spam and filters messages according to message body and attachment content; supports full auditing and reporting
Vircom 514-845-1666 http://www.vircom.com	VOP Anti-Spam Gate Enterprise 2.0	Starts at $1995	Email gateway with antispam protection for any mail server; features Vircom Sieve antispam script technology that's automatically updated 24 × 7 by Vircom; comes with 1-year customer support and auto-updates to Sieve scripts
	VOP modusGate Enterprise 2.0	Starts at $1995	Email gateway with antispam and antivirus protection for any mail server; features Vircom Sieve antispam script technology that's automatically updated 24 × 7 by Vircom; comes with 1-year customer support and auto-updates to Sieve scripts and antivirus definitions
	VOP modusMail Enterprise 2.0	Starts at $1995	Email server with Sieve-based antispam and antivirus capabilities; features Vircom Sieve antispam script technology that's automatically updated 24 × 7 by Vircom; comes with 1-year customer support and auto-updates to Sieve scripts and antivirus definitions
APPLIANCES			
BorderWare Technologies 905-804-1855 877-814-7900 http://www.mxtreme.com	MXtreme Mail Firewall	Starts at $6000	Appliance that provides mail security and protects email systems with a layered security model that guards against OS hacks, malformed messages, viruses, employee misuse, and spam
CipherTrust 678-969-9399 877-448-8625 http://www.ciphertrust.com	IronMail	Starts at $15,000	Appliance that protects enterprise email systems against viruses, spam, and intruders; provides message privacy and policy enforcement; antispam technologies include blacklists, reverse DNS lookup, local deny lists, signatures and policies, content filtering, header analysis, and anomaly detection

Contact Information	Product Name	Price	Description
APPLIANCES continued…			
Cobion 781-229-5844 http://www.cobion.com	OrangeBox Mail	Starts at $1895	A 19" standalone appliance that prevents intellectual property, confidential documents, or offensive language from leaving the corporate domain through outgoing email; keeps spam or inappropriate content from coming in; analyzes message text and attachments, regardless of format or compression; passes or blocks messages according to user-defined policy
Corvigo 650-472-9570 877-429-5076 http://www.corvigo.com	MailGate	$10,000	Network appliance that uses a proprietary artificial intelligence (AI) engine to filter spam; quarantines spam at the edge of the network; lets you configure across the enterprise or per user; can manage 100 to 10,000+ mail accounts
ESCOM 703-620-4823 http://www.escom.com	Active SMTP (ASMTP) Model D-1 Appliance	$5900	Appliance that protects any SMTP and Extended SMTP (ESMTP) server; Exchange-compatible; dynamically finds and quarantines spam from dial-up connections, relays, and forged addresses; features content-filtering, virus-risk filtering, and Web-based management capabilities; can handle 100,000 messages per hour; offers a free 30-day onsite evaluation; software release also available
Network Associates 800-847-8766 http://www.mcafeesecurity.com	WebShield	Starts at $5000	Gateway appliance that scans SMTP, HTTP, FTP, and POP3 traffic; features RBL support; filters URLs and SMTP message content
Roaring Penguin Software 613-851-4379 http://www.canit.ca	CanIt Spam Trap	Starts at $4 per user	Server-based antispam scanner; hardware appliance comes with CanIt Spam Trap software preinstalled
SERVICES			
MessageLabs 952-830-1000 877-324-4913 http://www.messagelabs.com	SkyScan AS	Sixty cents per user per month (for 1000 users)	Filtering service that uses heuristics scanning to build a knowledge base of spam techniques and behavior; also filters email by using criteria to suit specific businesses; can eliminate false positives
Postini 650-482-5130 888-584-3150 http://www.postini.com	Postini Perimeter Manager	Contact vendor for pricing	Service that protects corporate email from spam, viruses, and SMTP-based network intrusions; uses heuristics-based filtering to identify and quarantine spam; provides realtime monitoring and reporting and disaster-recovery features
Singlefin 619-222-1362 866-566-3346 http://www.singlefin.net	Singlefin Spam Filter	$49.95 per month	Enterprise email gateway protection services block spam and viruses before they enter the network; won't block legitimate email; uses advanced algorithms to identify spam