Comprehensive Email Protection Leveraging Over 20 Layers of Defense

MX Logic is committed to providing customers worldwide with a comprehensive email defense solution that protects their networks from the full range of email threats. MX Logic employs a powerful, 20-layer approach that includes proven spam filters, leading anti-virus engines, content and attachment filtering, and email attack protection. Because each filtering method has unique strengths designed to identify specific threats, the combination creates one of the most accurate and comprehensive filtering processes in the industry.

59 percent of respondents believe that large attachments sent through email represent a serious problem.

Osterman Research

Viruses, worms and Trojan horses cost $28 billion in economic losses in 2003.
The Radicati Group

MX Logic’s Stacked Classification Framework® designed for spam detection

To help businesses avoid the productivity- and budget-draining impact of spam, MX Logic aggregates the most effective spam filters in the industry to accurately identify and thwart spammer attacks. The following spam filters comprise the patent-pending MX Logic Stacked Classification Framework:

- **Statistical Filtering**: MX Logic’s probabilistic filtering utilizes a statistical Bayesian algorithm to determine the probability that an email message is spam based on how often elements in that message have appeared in other spam emails.
- **Industry Heuristics**: MX Logic incorporates thousands of successful industry-wide spam-fighting rules into its filtering layers.
- **Proprietary Heuristics**: MX Logic experts write and update thousands of proprietary rules to block spam using real-time data from MX Logic’s Threat Center.
- **Reputation Analysis**: Like black and white lists, reputation analysis blocks spam based on comprehensive information about the source of the message—rating the reputation of the sender based upon the percentage of spam messages sent from that IP address in the past.
- **URL Filtering**: URL filtering works by comparing embedded links found in email messages with URLs associated with identified spam.
- **Reputation-based RBL Filtering**: MX Logic assigns a level of trust to key real-time blackhole lists (RBLs), which rates the reputation of the RBL based on its accuracy at blocking spam.

**Allow and deny lists provide flexible protection**

MX Logic integrates the following domain-level black and white lists and distributed black lists:

- **Domain-level Black and White Lists**: Specifically designed to protect against spam, inappropriate content, and email attacks; domain-level black and white lists filter and block unsolicited messages.
- **Distributed Black Lists**: Providing exceptional protection against spam, distributed black lists comprise a number of real-time subscription services including the Mail Abuse Prevention System (MAPS) and MX Logic’s own global deny lists, which include multiple lists of known spammers and their IP addresses.

**Robust Architecture — Over 20 Layers of Defense**
About MX Logic
MX Logic, Inc. provides innovative email defense solutions that ensure email protection and security for enterprises, service providers, government organizations and resellers and their customers. Deployed as either a managed service or on-premise software, the company’s feature-rich suite is the industry’s most comprehensive, flexible and easy to use. Through the company’s managed service offering, MX Logic processes millions of messages per day for over 2,500 organizations, including Evite, Hyundai/Motor America, The Sports Authority, YMCA, and ServiceMaster. In addition, MX Logic is the only email defense company to offer both a managed service and a turnkey, carrier-grade software solution for service providers.

More Information:
MX Logic Sales Team
9788 W. Pyramid Court, Suite 590
Denver, CO 80122 USA
T +1.877 MXLOGIC
F +1.720.865.5757
E sales@mxlogic.com
W www.mxlogic.com

- Recipient Deny Lists (Address): This type of filtering is designed specifically to filter for content and relieve network servers from attempting repeatedly to deliver mail to invalid addresses.
- User-level Black and White Lists: Through regularly-delivered MX Logic Spam Guarantee Reports, end users have the flexibility to develop their own, personal allow and deny lists.

Email attack filtering protects critical networking infrastructure
To protect businesses against email attacks, MX Logic incorporates sophisticated protection into its filtering layers, including:
- Denial of Service (DoS) Attack Protection: MX Logic defends business networks from unplanned outages associated with DoS attacks by incorporating Email Attack Protection. DoS attacks are machine-generated email messages sent on a massive scale to overwhelm unprotected networks. This feature detects the excessive SMTP “chatter” associated with DoS attacks and immediately limits the connections it will allow from the attacking IP addresses/laws.
- Directory Harvest Attack (DHA) Protection: MX Logic’s Email Attack Protection defends networks against DHAs, which run through possible alphanumeric combinations or predefined dictionaries to identify valid email addresses on a target domain.

Content and attachment filtering techniques reduce liability
MX Logic incorporates six filtering techniques designed to control unwanted email content and attachments. The following methods protect a business’ public image and shield employees from offensive messages:
- Keyword Filtering: With Content and Attachment Filtering from MX Logic, organizations can reduce corporate liability and bandwidth waste. Content filtering technology evaluates the content of all messages based on the policies and associated actions configured by the enterprise.
- Attachment Filtering: Content and Attachment Filtering blocks unwanted attachments by type and size before they enter or exit the corporate network. Identified according to configurations set by the enterprise IT administrator, attachments can be filtered by size, MIME media type (exe, vbs, rtf, etc.), and by binary content.
- Archive and Compressed File Integrity Filtering: MX Logic can protect the business network from the bandwidth-draining effect of dangerously sized malicious archive files (e.g., zip) by locking up messaging servers. When it detects suspicious compression ratios or suspected nested archives in attachments, the feature strips the file to prevent possible network outages.
- Spam Beacon and Web Bug Detection and Blocking: MX Logic offers spam beacon and web bug detection and blocking to protect networks from attacks that use these intrusive, almost imperceptible tags embedded in HTML to give spammers the ability to confirm if their messages have been opened and target businesses for future attacks.
- Multi-level HTML Content Protection: Because malware can now take many forms, MX Logic protects its business clients with multi-level HTML content protection. This feature filters suspect HTML, JavaScript, ActiveX and applets based on defined policies.
- Fraud Protection: Using a combination of industry-leading spam-fighting methods, phishing emails and fraudulent content can be identified and filtered out of inbound email before they reach the business email network and dupe unsuspecting recipients into releasing personal or business-related information.

Sophisticated virus and worm scanning prevents infection
MX Logic’s virus and worm detection technology leverages the combination of a proprietary worm analysis engine along with two industry-leading anti-virus engines to provide defense-with-diversity protection.
- Proprietary Worm Filtering: Through sophisticated content behavior analysis, MX Logic’s proprietary worm detection technology can identify and intercept, zero-day mass-mailing worms before they enter or leave a corporate network.
- McAfee® Anti-virus: MX Logic has partnered with industry-leading anti-virus company, McAfee, to offer customers an additional layer of virus protection at their network perimeter. With this feature, viruses can be stripped from incoming email, the message can be quarantined for review, or the email can be blocked outright.
- Sophos® Anti-virus: MX Logic has also partnered with industry-leading anti-virus company, Sophos, to offer an alternative anti-virus platform, or to enable customers to double their virus protection by integrating both Sophos and McAfee.

© 2014 MX Logic, Inc. All rights reserved.