



## MX Logic® Multiple Layers of Email Defense

Spam now accounts for more than 85% of all email traffic.

MX LOGIC® THREAT CENTER

Spam cost organizations with no filtering protection upwards of \$1,000 per mailbox per year.

FERRIS RESEARCH

MX Logic is committed to providing easy to administer network-edge managed security services that protect the entire corporate messaging infrastructure from email threats. Primary to the effectiveness of the MX Logic® Email Defense Service is the Stacked Classification Framework® spam detection system, which is powered by patented technology and combines the most effective spam-fighting filters and techniques in the industry.

### SPAM FILTERING TECHNOLOGY

Through an aggregation and analysis of spam-likelihood scores, our solution blocks over 99 percent of spam while maintaining industry-leading low false positive rates (legitimate email misidentified as spam). As new techniques and filters are developed, we add them to the Framework, further ensuring spam-filtering effectiveness. And, our sophisticated quarantine reduces false positives and IT administrator burden by allowing end users to customize filtering policies and manage their own quarantine. Our multiple spam filters include:

- **IP Reputation Connection Manager:** This filter operates at the front of the Stacked Classification Framework and rates the reputation of every incoming message, based on IP reputation data collected on an on-going basis by MX Logic. Connections are dropped for all messages which originate from IP addresses that are determined to carry a reputation for sending spam.
- **Deep Content Analysis<sup>SM</sup>:** This filtering module enables MX Logic to protect customers from increasing volume of messages that carry infected attachments. The filter blocks the most prevalent attachment-based spam, PDF spam, but has also been developed with the infrastructure necessary to address any future attachment spam variations. PDF spam specifically is the latest generation of image spam using graphics instead of other masking techniques to conceal an unsolicited advertisement's call to action. With PDF Spam, the images are embedded within attached .pdf documents instead of within the body copy of the message. The Deep Content Analysis filter enables MX Logic to analyze the content of the attachment to determine if it contains spam or malware before the message can reach the customer's network.
- **Premium Anti-Spam Multi-Language Filter:** This filter provides MX Logic with a global view of spam traffic, which enables us to defend against real-time spam attacks and rapidly identify zero-hour spam, regardless of language. The filter is also effective at identifying image-based spam and phishing emails, and is continually updated based on real-time feedback provided by a global network of users.
- **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.
- **Sender Policy Framework (SPF)/Sender ID:** For inbound messages, MX Logic can check if the message has an associated SPF/Sender ID record. If there is an SPF/Sender ID record, it can help determine if the email sender's domain is from a list of IP addresses authorized to send email from that domain.
- **Proprietary Heuristics:** MX Logic experts write and update thousands of proprietary rules to block spam using real-time data from the MX Logic® Threat Center.

## KEY BENEFITS

- Stacked Classification Framework utilizing patented technology
- More than 12 spam-filtering layers
- Email Attack Protection defends against spammer intrusion
- Domain-level black and white lists
- Distributed black lists
- Sophisticated virus and worm scanning



- **Reputation Analysis:** Reputation Analysis votes on the probability that the message is 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:** Within the Stacked Classification Framework, MX Logic compares a message's sending IP address against those on key real-time blackhole lists (RBLs), which contain IP addresses that are associated with known spammers and are considered fraudulent.

#### MULTIPLE ALLOW AND DENY LISTS PROVIDE FLEXIBLE PROTECTION

MX Logic integrates the following domain-level black and white lists and distributed black lists into its comprehensive service to fight spam and other email threats:

- **Distributed blackhole lists:** Providing exceptional protection against spam, distributed blacklists comprise a number of real-time subscription services including the Mail Abuse Prevention System (MAPS) and MX Logic global deny lists, which include multiple lists of known spammers and their IP addresses.
- **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.
- **Domain-level allow and deny lists:** Specifically designed to protect against spam, inappropriate content, and email attacks, domain-level allow and deny lists filter and block unsolicited messages.
- **User-level allow and deny lists:** Through regularly-delivered MX Logic Spam Quarantine 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 spammer intrusion, MX Logic incorporates sophisticated email attack protection into its filtering layers, which includes:

- **Denial of Service (DoS) Attack Protection:** Using Email Attack Protection, MX Logic defends business networks from unplanned outages associated with DoS attacks. This feature detects the excessive SMTP "chatter" associated with these machine-generated, large scale attacks and blocks them from attempting to overwhelm unprotected networks.
- **Directory Harvest Attack (DHA) Protection:** This feature 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 the following six filtering techniques designed to control unwanted email content and attachments in order to protect your business integrity and reduce legal liability:

- **Keyword filtering:** Content filtering technology evaluates the content of all messages based on the policies and associated actions configured by the enterprise.
- **Attachment filtering:** Attachment Filtering blocks unwanted attachments by size, by MIME media type (.exe, .vbs, .mp3, etc.), and by binary content before they enter or exit the corporate network.
- **Archive and compressed file integrity filtering:** Protecting businesses from the bandwidth-draining effect of dangerously-sized malicious archive files (e.g., .zip) that can lock up messaging servers, MX Logic detects suspicious compression ratios or suspected nested archives in attachments and strips the file to prevent possible network outages.
- **Spam beacon and Web bug detection and blocking:** This technique protects networks from these intrusive, almost imperceptible tags embedded in HTML that give spammers confirmation and information about targeted end users.
- **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 are identified and filtered 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

Virus and worm detection technology from MX Logic leverages the combination of a proprietary worm analysis engine along with three industry-leading anti-virus engines to provide defense-with-diversity protection.

- **Proprietary worm filtering:** Through sophisticated content behavior analysis, MX Logic's proprietary WormTraq® detection technology rapidly identifies and intercepts zero-hour mass mailing worms before they enter or leave a corporate network.
- **Leading signature-based virus scanning engines:** MX Logic leverages leading signature-based virus scanning engines with a combination of protection from Authentium®, McAfee® and Sophos®. Our technology detects, quarantines, blocks and strips viruses and worms at the network perimeter before they can enter and damage a customer's corporate messaging infrastructure.

Find out how you can leave the management of your online security solutions to us and enjoy a safer, more secure network and business environment by calling 1.877.MXLOGIC or visiting us at [www.mxlogic.com](http://www.mxlogic.com).



#### ABOUT MX LOGIC

MX Logic is a leading provider of managed email and Web security services that deliver enterprise-grade performance without enterprise-level complexity and cost. Our easy-to-use, award-winning services reduce risk and liability, lower overall IT costs, and increase productivity. MX Logic services are available through our industry-leading partner network. For more information, visit [www.mxlogic.com](http://www.mxlogic.com).

#### More information:

MX Logic Sales Team  
 9781 S. Meridian Blvd. Suite 400  
 Englewood, CO 80112 USA  
 T: +1.877.MXLOGIC  
 F: +1.720.895.5757  
 E: [sales@mxlogic.com](mailto:sales@mxlogic.com)  
 W: [www.mxlogic.com](http://www.mxlogic.com)