



The need for greater security is compelling organizations to consider using managed security service providers for some or all of their IT security needs.

ABERDEEN GROUP, 2008

WHY WE'RE DIFFERENT?

- We are a managed service
- We protect at the network perimeter
- We provide around-the-clock email traffic monitoring and protection with the MX Logic® Threat Center
- We offer a combination of spam-detection techniques
- We integrate multi-layer anti-virus filtering
- We support message loss prevention
- We require no hardware or software purchases
- We require no ongoing maintenance fees
- We provide rapid implementation

MX Logic®

MX Logic Advantage over Appliances

Traditionally, anti-spam and anti-virus email solutions were delivered as a plug-in appliance. These are boxes which plug into the corporate network and contain software that scans and filters messages for spam, viruses or other mail-based problems.

While there was a time when the appliance solution was considered the smart choice, today managed services offer such unique capabilities and scalability that a growing number of organizations are realizing this form factor is a better choice for anti-spam, anti-virus and other email protection.

A MANAGED SERVICE HAS SIGNIFICANT BENEFITS

MX Logic is a managed service that works at the network perimeter. Quite simply, this means malware is detected and removed from the email stream before it ever reaches a customer's infrastructure. This greatly reduces the burden on the customer email server as well as its administrator and users. Additionally, MX Logic can offer perimeter protection for Denial of Service (DoS) and Directory Harvest Attacks (DHAs). These attacks are deflected by MX Logic and again, the customer's firewall and mail server are not impacted.

Finally, the MX Logic® Threat Center uses industry-leading technology and a staff of threat experts that monitor billions of messages a month looking for patterns in spam, identifying new types of spam threats, and adjusting the various spam filtration mechanisms to maintain the highest level of spam detection and a minimum number of false positives (legitimate emails marked as spam). These are benefits not available in any desktop software at any price.

COMPREHENSIVE EMAIL DEFENSE BASED ON MULTIPLE LAYERS OF FILTERING

MX Logic ensures industry-leading filtering accuracy using a multilayered strategy that combines more than 20 forms of spam, virus, content, attachment, and email attack filtering technology. Primary to the effectiveness of the MX Logic® Email Defense Service is our 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. Our filtering layers include:

- **IP Reputation Connection Manager** 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.
- **Deep Content AnalysisSM** 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.
- **Premium Anti-Spam Multi-Language Filter** Utilizes a sophisticated fingerprinting system and global spam submission network to identify foreign language, image-based, and other emerging spam types quickly and effectively.
- **Statistical 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.

STAGGERING STATISTICS

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

MX LOGIC® THREAT CENTER

More than 65% of PCs are infected with some kind of spyware – many within minutes of being turned on for the first time.

SANS INSTITUTE

55% of all companies will experience an email outage greater than four times annually.

INDUSTRY REPORTS



- **Sender Policy Framework (SPF)/Sender ID** Checks each message for an associated SPF/Sender ID record, which if present, 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** Uses thousands of proprietary rules to block spam using real-time data from the MX Logic® Threat Center.
- **Reputation Analysis** Votes on the probability that the message is spam based on comprehensive information about the source of the message.
- **URL filtering** Compares embedded links found in email messages with URLs associated with identified spam.
- **Reputation-based Real-time Blackhole List filtering** Compares a message's sending IP address against those on key real-time blackhole lists (RBLs), which are associated with known spammers and are considered fraudulent.

Each of these filtering technologies analyzes messages differently. The SCF then allows each to "vote" on the probability that a particular message is spam. The votes are then combined and analyzed by our patented algorithm-based technology, resulting in a high rate of spam filtering accuracy. These filters are constantly monitored, evaluated and modified by the MX Logic Threat Center to maintain maximum effectiveness.

MULTILAYER ANTI-VIRUS, CONTENT FILTERING KEEPS NETWORK SAFER

MX Logic provides far more than general spam filtering. The MX Logic Email Defense Service provides multilayer anti-virus filtering that includes third-party, signature-based engines from McAfee®, Sophos® and Authentium®. MX Logic provides zero-hour protection through its proprietary WormTraq® worm detection technology, which is designed to quickly detect and stop mass mailing worms like So Big, Sober.z and Storm Worm outbreaks. MX Logic maintains its commercial engine signatures on a five minute priority update to stop virus-laden mail before it gets to the customer.

The Email Defense Service also includes content and attachment policy enforcement to further protect the customer from outside their network perimeter and protection from fraud/phishing emails. In addition, businesses can also implement outbound message filtering, which enables them to proactively integrate email policy enforcement for all messages leaving the corporate network.

MESSAGE LOSS PREVENTION INCLUDED

In addition to email threat protection, MX Logic also helps businesses minimize downtime and information loss with two email disaster recovery services. Both MX Logic® Message Continuity and the MX Logic® Fail Safe Service engage automatically whenever MX Logic detects a loss in connectivity with the customer email server. Message Continuity provides Web-based email access during outages, while the Fail Safe Service is a storage-only solution. At the conclusion of the email outage, all email is spooled to the customer. The benefits of mail spooling during planned or unplanned outages are unavailable with any software package.

ULTIMATE MANAGEMENT AND CONTROL

MX Logic provides administration controls through its intuitive, easy-to-use administrative console, the MX Control ConsoleSM, and offers advanced reporting, group and individual policy management, 24x7 customer support Web-based console, reporting features, group and individual policy capability, and more.

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 extensive partner network. Visit us at www.mxlogic.com.

Contact Information:

TELECOMWORX
3878 Saint Clair Court
Monrovia, Maryland 21770
o 301.253.9900
f: 1.888.266.6450
m: 301.471.8320
e: matt_brunk@telecomworx.com
www.telecomworx.com

