

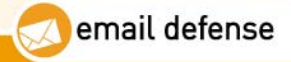


# The MX Logic® Email Defense Service

## Solution Guide

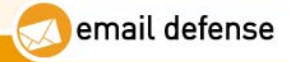
### In Review

- ☒ The Rocky Email Landscape
- ☒ The MX Logic Email Defense Service
- ☒ MX Logic's Technology
- ☒ About the Threat Center
- ☒ How Intelligent Message Filtering Works



## Table of Contents

✉ Executive Summary .....	3
✉ MX Logic® Email Defense Service – The Best Defense is a Good Offense .....	4
✉ Multiple Layers of Filtering Technology .....	7
✉ Spam Blocking .....	8
✉ Virus and Worm Scanning .....	11
✉ Fraud Protection .....	12
✉ Content and Attachment Filtering .....	13
✉ Email Attack Protection .....	14
✉ Outbound Message Filtering .....	15
✉ Convenient Administrative and Reporting Tools .....	16
✉ Sophisticated, safe external quarantine .....	18
✉ MX Logic® Disaster Recovery Services .....	19
✉ Technology Architecture .....	21
✉ A Closer Look at the MX Logic® Threat Center .....	23
✉ More about MX Logic’s Intelligent Message Processing .....	24
✉ About MX Logic .....	26



## Executive Summary

*Simple. Efficient. Powerful. Invaluable.* That's email – the way it should be. Email has transformed how we communicate with others at home, in the office, down the street and around the globe, and has become as integral to business communications as the phone and fax.

Unfortunately, this revolutionary communications tool is under constant attack, with its delivery routes polluted each day by billions of unsolicited messages ranging from the merely annoying to the truly dangerous. The cost to businesses worldwide in dealing with spam and malicious email threats has reached billions of dollars annually.

MX Logic brought its powerful email defense solutions to market in response to the escalating risks that jeopardize business email systems and networks. With its industry-leading network-perimeter protection, MX Logic successfully blocks more than 99 percent of all email threats for its customers – including service providers and their customers – using a combination of proven spam filters powered by patented spam detection technology, fraud protection, leading anti-virus engines, content and attachment filtering, and sophisticated email attack protection.

MX Logic goes beyond traditional spam prevention with multilayered technology that is positioned between the Internet and the business network to identify, quarantine, block and strip email threats before they can infiltrate the organization. Overall, by using MX Logic to filter both inbound and outbound messages, businesses can enjoy the inherent benefits of email communications and significantly reduce risk, save bandwidth, reduce storage costs, and minimize administrative costs.

This overview reviews the technology and techniques that make the award-winning MX Logic® Email Defense Service unique and effective:

- *Ease of administration and use through secure Web-based platform*
- *Patented, multilayered technology to block spam*
- *A tri-layered combination of virus and worm protection*
- *Comprehensive protection for the entire email network*
- *Sophisticated quarantine management to reduce time and risk*
- *Secure message delivery over Transport Layer Security (TLS)*



MX Logic processes billions of messages each month and proactively protects the critical messaging networks for over 35,000 organizations worldwide including EnCana, Hyundai Motor America, Internet Initiative Japan, ServiceMaster, Verio Inc., and YMCA. In addition to MX Logic's highly-accurate threat protection technology, we combine human intelligence and experience with automated filtering technology to ensure that our multiple filtering layers are updated instantly upon detecting new threats.

Named #59 in the Inc. 500 fastest growing privately held business in 2007 MX Logic is no stranger to receiving awards and recognition. The innovative service was honored as the Best Managed Email Service in the *2006 SC Magazine Reader Trust Technology Awards*, and was selected as a *2005 Product of the Year* by SearchExchange.com. In addition, the Email Defense Service was awarded the highest available rating of five stars in the *VeriTest Anti-Spam Benchmark Service Summer 2005 Report*, in the vendor-tuned portion of the test. MX Logic also posted the highest spam catch rates in the independent test, with an out-of-the-box catch rate of 99.71% and 99.76% in the vendor-tuned portion of the test.

## A Rocky Email Landscape

According to the MX Logic® Threat Center, over 80 percent of all email traffic is spam, and that figure is expected to rise despite industry and legislative efforts to curb its growth. In fact, IDC noted that in 2007 for the first time spam email volumes exceeded person-to-person email volumes sent worldwide. With this unprecedented growth, there is good reason to be concerned that email will continue to be a breeding ground for computer viruses, unsolicited commercial or junk email and inappropriate content.

The ensuing bandwidth waste is another issue facing networks that are already pushing capacity. Spam, driven in large part by image-based spam, accounts for 1.7 quadrillion bytes of storage and bandwidth per day. That's the equivalent of 1.1 billion 1.5Mb DSL connections operating 24/7.<sup>1</sup> This barrage of unwanted email is costing U.S. companies up to \$71 billion annually to lost productivity caused by spam.<sup>2</sup>

Unwanted email and malicious code causes frustration and aggravation, but more importantly, they have the power to jeopardize network security, employee productivity, and corporate integrity.

## MX Logic® Email Defense Service – The Best Defense is a Good Offense

The MX Logic Email Defense Service is a comprehensive, perimeter-based solution that blocks over 99 percent of email threats – including spam, viruses, worms and harmful

<sup>1</sup> Unified Communications, January 2007

<sup>2</sup> Nucleus Research, 2008



content and attachments – before they can enter and damage internal messaging networks.

The multilayered, cost-effective solution offers rapid activation and is easy to configure and manage, helping to reduce IT-related costs and corporate liability, while increasing employee productivity. Positioned between the Internet and the business network, the Email Defense Service leverages the most effective technologies and techniques within more than 20 layers of filters to identify, quarantine, block and strip email threats.

With effortless configuration, your business can integrate the MX Logic network border protection technology to begin reducing the risk, expenses, and wasted time associated with unwanted email.

#### **Incorporate effortless policy-setting and administration**

Using the MX Control Console<sup>SM</sup>, administrators can effortlessly fine-tune email defense policies. With this administration and reporting tool, businesses have the flexibility to establish email protection policies, set domain-level rules, enable group policies filtering, and decide which type of email should be allowed and which should be denied. Real-time, daily, weekly and monthly reports also allow IT staff members to quickly analyze and track email traffic and trends in order to improve overall performance and isolate issues before they become problems.

#### **Integrate email protection outside of your network**

MX Logic network-perimeter protection is proven to be the most effective way to defend the entire enterprise email system from unwanted and unsolicited email using a precise combination of spam filtering, fraud protection, virus and worm blocking, content and attachment filtering, and email attack protection.

#### **Reduce maintenance and additional hardware or software purchases**

Unlike appliances and software solutions that require integration, migration and a significant amount of ongoing maintenance, our service is effortless and highly effective – requiring no additional hardware or software or the constant diligence needed to apply and integrate updates, new patches and filters.

#### **Eliminate on-going email monitoring with Threat Center protection**

As new email threats are detected by the MX Logic<sup>®</sup> Threat Center, new rules for blocking those threats are seamlessly integrated into our filtering layers to automatically protect our customers. Within our sophisticated streaming data environment, our technologists and our technology monitor the global state of email for spam, viruses, worms and other email threats 24 hours a day, seven days a week.

#### **Reduce IT-related costs**

Because MX Logic filters and blocks threats before they can enter the corporate network and then stores suspect messages in a safe, offsite queue, businesses can



eliminate risk and unnecessary costs associated with the additional storage and bandwidth required to deliver and store the unwanted email, and the risks of server overload.

### **Increase employee productivity and control**

With MX Logic blocking over 99 percent of spam, employees spend virtually no time sifting through junk email to find legitimate messages. And, in the fight against false positives, our Spam Quarantine Reports allow end users to take action on their own spam quarantine and determine how items captured by the filter should be handled in the future.

### **Safeguard business integrity**

MX Logic® Outbound Message Filtering and our disaster recovery services – MX Logic® Message Continuity and the MX Logic® Fail Safe Service provide additional layers of network protection.

- Outbound Message Filtering helps businesses to safeguard and protect valuable proprietary or private information, and be assured that potentially harmful viruses and worms or offensive messages will not be transmitted outside the organization via email.
- Both Message Continuity and MX Logic Fail Safe ensure that your business will never lose an email by providing automatic email backup protection in the event of an unplanned server or network outage, or during planned maintenance. Furthermore, with MX Logic Message Continuity you'll be able to keep lines of communication open during an outage via Web-based email access, management and use.

### **Augment On-Premises Appliance Spam Blocking**

Businesses looking to lessen the load on their on-premises anti-spam appliances can turn to MX Perimeter Defense<sup>SM</sup>. This unique service package provides effective protection against inbound spam being distributed from known high-volume spam sources, which often accounts for more than 50% of all spam traffic.

After redirecting your mail exchange (MX) record to MX Logic, all inbound messages are compared against an extensive database of known spammer IP addresses. The Threat database is compiled and continually updated by the MX Logic® Threat Center, based on our 24x7 analysis of worldwide email traffic and third-party real-time blackhole lists (RBLs).

Messages are also filtered through our proprietary WormTraq® worm and virus detection engine, which rapidly identifies and intercepts zero-hour mass mailing worms and viruses before they can enter a corporate network. If a message includes a sending IP address found in the MX Logic Perimeter Block database or is found to contain a virus



or worm, delivery is denied and the connection is immediately dropped. The service also detects and blocks AR Bombs, which are messages that include heavily-nested or -compressed .zip files as attachments.

By reducing inbound email traffic by 50% or more, the threat posed by the deleted spam is eliminated, and customers can greatly reduce their bandwidth utilization. In addition, because MX Perimeter Defense is delivered as a managed service, there is no related hardware to purchase, install or maintain.

### Multiple of Filtering Technology

To ensure industry-leading filtering accuracy, our network perimeter-protection service is fortified using a multilayered strategy that combines over 20 forms of spam, virus, content, attachment, and email attack filtering technology.

	Stacked Classification Framework® spam detection system	Multiple allow and deny lists
<b>MX Logic's More Than 20 Layers of Protection</b>	<ul style="list-style-type: none"> <li>▪ IP Reputation Connection Manager</li> <li>▪ Deep Content Analysis<sup>SM</sup></li> <li>▪ Premium Anti-Spam Multi-Language Filter</li> <li>▪ Statistical Filtering</li> <li>▪ Sender Policy Framework (SPF)/Sender ID</li> <li>▪ Proprietary Heuristics</li> <li>▪ Reputation Analysis</li> <li>▪ URL filtering</li> <li>▪ Reputation-based RBL filtering</li> </ul>	<ul style="list-style-type: none"> <li>▪ Domain-level black and white lists</li> <li>▪ Distributed black list</li> <li>▪ User-level black and white lists</li> <li>▪ Recipient deny lists (Address)</li> </ul>
Email attack filtering	Content and attachment filtering	Sophisticated virus and worm scanning
<ul style="list-style-type: none"> <li>▪ Denial of Service (DoS) Attack Protection</li> <li>▪ Directory Harvest Attack (DHA) Protection</li> </ul>	<ul style="list-style-type: none"> <li>▪ Fraud Protection</li> <li>▪ Attachment Filtering</li> <li>▪ Archive and Compressed File Integrity Filtering</li> <li>▪ Spam Beacon and Web Bug Detection and Blocking</li> <li>▪ Multi-level HTML Content Protection</li> </ul>	<ul style="list-style-type: none"> <li>▪ Proprietary WormTraq® worm detection</li> <li>▪ Industry-leading Anti-virus engines</li> </ul>



	Stacked Classification Framework® spam detection system	Multiple allow and deny lists
	<ul style="list-style-type: none"> <li>▪ Keyword Filtering</li> </ul>	

## Spam Blocking

No longer viewed as merely a nuisance, spam has become a major problem for businesses across the globe. Accounting for over 80 percent of all email worldwide, spam is a costly drain on time and resources and, with its ability to stealthily transport worms and viruses, has become a significant threat to network security.

### **Advanced, layered technology to block spam**

As explained in the Technology Architecture section below, our network perimeter-protection service is fortified using a multilayered strategy with the MX Logic Stacked Classification Framework® spam detection system at the foundation of MX Logic® Spam Blocking. Powered by patented technology, the Framework combines the most effective spam-fighting filters and techniques in the industry. Within the Framework, the different spam filters separately assess and “vote” on the probability that a specific email is spam – a technique that results in highly-accurate threat protection with industry-leading low false positive rates (legitimate email misidentified as spam). Then, as new spam-detection techniques and filters are developed, (such as the Deep Content Analysis filter that effectively addresses attachment spam such as .pdf spam) these are quickly and seamlessly integrated into the flexible Framework.

### **Proactively control spam and protect your network**

By integrating MX Logic ClickProtect<sup>SM</sup>, businesses can find out more about how end-user email behavior could be impacting their network protection. ClickProtect is an industry-first technology that allows companies to monitor whether employees are clicking on websites that violate network security – sites that automatically add their addresses to spammer distribution lists or install spyware on their computers. In addition, ClickProtect increases user awareness by enabling customizable warning messages and gives administrators the ability to build and integrate lists of approved websites.

### **One quick click and spam is gone**

The technologists in the MX Logic® Threat Center continuously monitor the Internet for the latest spam attacks and then write spam-fighting rules to identify those threats in the future. We also analyze the unwanted email that our customers consider to be spam, and incorporate that information into additional spam-filtering rules so that similar messages are effectively filtered going forward. And, with Spam Control for Outlook®, end users can easily add a “Delete As Spam” button to their Microsoft®



Outlook® navigation bar to immediately delete suspect emails and simultaneously send the message directly to our Threat Center for analysis and action.

### **Stacked Classification Framework spam detection system**

In the fight against spam, MX Logic utilizes a patented method of identifying and controlling spam, which uses a voting algorithm based on a sophisticated form of intelligent reasoning, to achieve more than 99 percent accuracy. The MX Logic Stacked Classification Framework spam detection system successfully combines the most effective spam-fighting filters and techniques in the industry. These 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. Deep Content Analysis 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 each inbound message, the SPF classifier assesses whether the relationship between the DNS record and its list of authorized IP addresses is legitimate. Using this technology, MX Logic can more accurately filter fraudulent spoofed emails – those sent by spammers with forged "From" addresses.
- **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.



- **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:** MX Logic assigns a level of trust to key real-time blackhole lists (RBL), which rates the reputation of the RBL based on its accuracy at blocking spam. While most service providers use RBLs, MX Logic is the only one to provide a customer-configurable process for limiting false positives, which helps to ensure that our customers receive a high level of spam protection with minimum impact on their businesses. In addition, RBLs are uniquely deployed in two ways within the Email Defense Service:

- By opting in to RBL protection, mail coming from listed addresses will be automatically blocked prior to filtering by the Stacked Classification Framework® spam detection system.
- RBLs are also used within the Stacked Classification Framework as a voting filter. Should the RBL filter give a “high likelihood” score to a particular message while other voter filters score the message as “low likelihood,” the message will in most cases be allowed to pass through to the customer, reducing the instances of false positive messages being quarantined. All MX Logic customers receive protection from this voting filter.

#### **Additional filters such as allow and deny lists provide more protection**

MX Logic employs other filters to ensure your email is virtually free of spam including 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 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.
- **User-level black and white lists:** Through regularly-delivered MX Logic Spam Quarantine Reports, end users have the flexibility to develop their own, personal allow and deny lists.



### MX Logic® Earns Five Stars in VeriTest Independent Anti-Spam Test

The VeriTest Anti-Spam Benchmark Service is a technically rigorous subscription test service that measures the effectiveness of anti-spam technologies. VeriTest conducts these tests four times per year, in two configurations; an "out-of-the-box" configuration using a solution's default filtering settings, and a "tuned" configuration in which a solution's spam filtering parameters are optimized for the VeriTest testing scenario.

The MX Logic® Email Defense Service received five stars, the highest available rating, in the VeriTest Anti-Spam Benchmark Service™ Summer 2005 Report. The high rating was a result of the solution's performance in the vendor-tuned portion of the independent test, in which it posted a 99.76 percent Spam Capture Rate. MX Logic posted a Spam Capture Rate of 99.71 percent in the "out-of-the-box" configuration.

MX Logic also out-performed the industry average for false positives (legitimate email messages misidentified as spam), rating 25 percent better than average as an out-of-the-box solution and 75 percent better than average in the vendor-tuned portion of the test.

### VeriTest Anti-Spam Benchmark Service Testing Methodology

To conduct its Anti-Spam Benchmark Service, VeriTest sends a blended stream of spam and legitimate mail to each solution under test. The spam arrives at each solution directly from spammers and outside domains, with absolutely no involvement or mail header changes from VeriTest. VeriTest tests each solution by subjecting it to a live and unreflected stream of spam or legitimate mail, and ensures that it preserves the IP address of the last email hop.

To determine spam-blocking effectiveness, VeriTest measures the following:

- **Percentage of spam messages blocked** – calculated as the ratio of the number of spam messages correctly blocked to the total number of spam messages processed.
- **False-positive percentage** – calculated as the ratio of incorrectly blocked legitimate messages to the total number of legitimate mails sent.

### Virus and Worm Scanning

To help businesses increase network security and protect corporate integrity, MX Logic's comprehensive, network-perimeter email defense solutions include highly-effective, firm-wide virus and worm scanning.

### Multilayered protection to combat morphing threats

Because every virus and worm is unique, single desk-top anti-virus solutions have severe limitations. To combat these morphing threats, MX Logic® Virus and Worm Scanning



offers triple protection which includes our proprietary WormTraq® worm detection technology and leading anti-virus engines. This layered combination of protection provides the strongest defense for businesses of all sizes – even those already employing an on-premise virus software solution.

#### **Proprietary worm detection technology adds a critical layer of protection**

MX Logic's proprietary WormTraq zero-hour worm detection technology protects customers from the dangers of mass-mailing worms hours before anti-virus services can distribute signature updates to their customers. Through sophisticated content behavior analysis, the MX Logic® Threat Center is able to quickly identify the common characteristics found in sudden surges of suspicious email messages, which are then intercepted before they can reach customers' email networks.

#### **Addition of three leading anti-virus engines results in triple filtering**

Using a proactive defense strategy, the MX Logic Threat Center diligently tracks and blocks the latest waves of worm and virus attacks using sophisticated content behavior analysis, proprietary scanning and triple anti-virus engines. The tri-layered technology virtually eliminates the risk of malicious viruses and worms entering the enterprise network because the threats are automatically stripped from incoming email, or are quarantined for review. And, programming up-to-the-minute automated rules, MX Logic scans for anti-virus updates from these leading anti-virus services every five minutes.



#### **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.

Phishing attacks use common spam techniques to distribute large volumes of official-looking fraudulent emails designed to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

With the MX Logic Email Defense Service and our layered anti-spam techniques, however, organization can protect their networks and employees from the risks of phishing. Using the same methods to detect spam, phishing emails and fraudulent content can be identified and filtered out of inbound email before they reach the network – ensuring that they never reach or dupe employees.



## Content and Attachment Filtering

Similar to the security threats posed by viruses and worms, businesses are now becoming more aware of the risk and liability associated with inappropriate content and attachments in email – liabilities that include licensing breaches, serious bandwidth overload, and sexual harassment law suits.

### **Email protection customized to support unique corporate policies**

While controlling spam with precise filtering accuracy is paramount, many organizations require that specific corporate filtering policies be established for both incoming and outgoing messages. For those organizations, MX Logic® Content and Attachment Filtering supports specific keyword filtering and attachment control. In addition to standard keyword “buckets” developed by MX Logic, businesses have the flexibility to program their filtering policies to meet their unique needs, whether it involves blocking the inbound and outbound transmission of private or proprietary corporate data, racially- and sexually-insensitive material, profanity, or any other content deemed inappropriate by the enterprise.

### **Attachment filtering keeps out large, malicious files**

MX Logic can protect the business network from the bandwidth-draining effects of dangerously-sized or malicious attachments. In combination with our spam blocking detection technology, which provides the first layer of email content control, Content and Attachment Filtering can be programmed to monitor email traffic and filter attachments according to business-specific configurations – filtering by size, by MIME media type (.exe, .vbs, .mp3, etc.), and by binary content. Using the same process, MX Logic can protect the network from archive files (e.g., .zip) that are capable of disabling messaging servers. When it detects suspicious compression ratios or suspected nested archives in attachments, the feature strips the file to prevent possible network outages. Additionally, MX Logic’s archive integrity filtering can intercept encrypted zip files or apply attachment policies to archive file contents.

### **HTML protection blocks the bugs and filters suspect text**

Because malware can now take many forms, MX Logic protects its business clients with multi-level HTML content protection. In fact, studies show that 50 percent of all spam messages contain beacons or Web bugs, which are intrusive, almost unperceivable tags embedded in HTML that give spammers the ability to monitor end-user activity and obtain certain information about them. MX Logic® Content and Attachment Filtering and HTML shield denies spammers the ability to know when and if their spam email is being read and keeps them from verifying the recipient’s email address. This feature also filters suspect HTML, JavaScript, ActiveX and applets based on defined policies.



### 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. Our proprietary Deep Content Analysis filter enables MX Logic to protect customers from increasing volume of PDF spam, or messages that carry infected .pdf attachments.
- **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.

### Email Attack Protection

Email has created tremendous opportunity, but has also made businesses vulnerable to billions of dollars in lost revenue and lost productivity because of its universal openness and accessibility. To protect businesses against spammer intrusion, MX Logic incorporates sophisticated email attack protection into its filtering layers using a unique mail exchange (MX) record masking technique.

### Shield the critical networking infrastructure

Spammers today are writing code and developing complex tools capable of easily bypassing typical email filtering mechanisms and capturing information about end users. MX Logic® Email Attack Protection provides real-time monitoring and analysis of incoming messaging traffic, conceals critical messaging gateways and shields groupware email servers from attack. By pointing your MX record to our SecureMX,



businesses can conceal their Internet-facing mail servers and remove the threat of anonymous connections. With MX Logic, malicious traffic is identified and quarantined at the network perimeter to ensure that the network is protected from directory harvest attacks, denial of service attacks, mail bombs, and channel flooding – attacks that can debilitate even the largest email systems.

### **Prevent Directory Harvest Attacks**

MX Logic Email Attack Protection defends business networks against directory harvest attacks (DHAs), which methodically bombard email servers with messages by using common name pairs or email address patterns, or uses “brute force” to run through possible alphanumeric combinations to identify valid addresses. Our solution blocks DHAs at the network perimeter to prevent spammers from gaining information about the validity of random email addresses used to target businesses for future attacks.

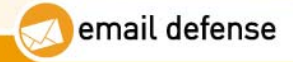
### **Blocking Denial of Service attacks**

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. DoS attacks are particularly stealthy because while they are designed to elude detection by masquerading as legitimate transactions, the intent is to launch them on a massive scale to overwhelm unprotected networks. When MX Logic detects the excessive SMTP “chatter” associated with DoS attacks, it limits the connections it will allow from the attacking IP address(es), throttling back the traffic and effectively stopping the DoS.

**Secure Message Delivery via Transport Layer Security (TLS):** The MX Logic® Email Defense Service supports SMTP over TLS, providing email delivery encryption allowing customers to easily send and receive email over a secure, end-to-end encrypted tunnel. MX Logic accepts and filters encrypted inbound and outbound messages and delivers them across a secure tunnel when recipients are TLS enabled. If a recipient is unable to receive a TLS encrypted tunnel, MX Logic will deliver the message via standard SMTP. Messages sent and received via an encrypted tunnel and are still automatically processed by the MX Logic® Threat Center, where they are scanned to block spam, viruses, worms, phishing attacks, unwanted content and attachments and other email threats.

### **Outbound Message Filtering**

Worldwide, 31 billion emails are sent each day. With each email sent, there are risks involving confidential information getting into the wrong hands, files so large they can bring down servers, and content so sensitive it can cause costly legal ramifications.



### Outbound Message Filtering helps maintain your corporate image

MX Logic® Outbound Message Filtering enables businesses to proactively integrate email policy enforcement for all messages *leaving* the corporate network en route to valued customers or business partners. With this added protection, organizations can reduce liability and corporate risk by preventing the distribution of company-sensitive information and blocking the transmission of harmful viruses and worms to important business partners and clients. To further strengthen your security, you can also add a disclaimer or footer to all outgoing messages.

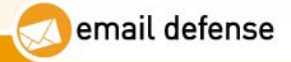
### Ensuring messages are safe, appropriate and in compliance

While the MX Logic Email Defense Service is protecting the network from malevolent *incoming* email messages, Outbound Message Filtering enables businesses to protect intellectual property by preventing accidental or intentional distribution of sensitive or proprietary internal information. The service also helps safeguard corporate integrity by stripping viruses and worms from outgoing messages and ensuring that inappropriate content does not get distributed. Finally, integrating outbound message filtering allows businesses to enforce policies that help comply with legislative, privacy and security regulations.

Outbound Message Filtering Features	Outbound Message Filtering Benefits
Content Filtering	Prevents inappropriate, malicious or confidential content from leaving the corporate email system – allowing organizations to monitor and enforce the appropriateness of outbound corporate messages
Attachment Filtering	Automatically filters attachments by size, by media type or by binary content.
Virus and Worm Scanning	Employs triple filtering to stop viruses and worms from leaving the corporate email system and infecting recipients. The level of outbound virus and worm scanning protection businesses receive is the same as the inbound filtering protection they select – combining our zero-hour proprietary worm scanning with signature-based engines.

### Convenient Administrative and Reporting Tools

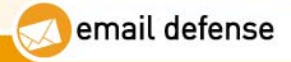
MX Logic email defense solutions can be easily configured to fight spam, viruses and worms, and other threats based on the unique needs of each organization. Our MX Control Console<sup>SM</sup> is a centralized email threat management policy platform that provides you with one interface for managing all corporate-wide email threats,



protection and security. This easy-to-use administration and reporting tool enables organizations to:

- Establish policies that direct how viruses, spam, unwanted attachments, unwanted content and unwanted HTML in messages are handled.
- Create customized group policies filtering that meets the unique needs of specific user groups, including functional groups like accounts payable, sales or engineering, or even individual users.
- Synchronize account information through MX Logic® Directory Integration, including primary and alias email addresses and distribution lists, thereby eliminating the need to manually make changes in both the corporate Active Directory and the MX Logic system.
- Reduce spam-management burden on your IT staff by determining whether the quarantine process for email threats will be managed by IT, your end users, or both.
- A backscatter abatement feature helps customers to eliminate the growing number of bounce messages or Non-Delivery Reports (NDR) that result whenever a spammer forges or spoofs a legitimate sending address, and that spam message is rejected by the recipient mail server.
- Automatically quarantine suspect messages by safely isolating unwanted messages outside of your network, where they can be reviewed and deleted or released according to the policies you set. All stand-alone Email Defense Service packages include a seven-day quarantine, with an available 14-day quarantine option that is included as part of all MX Logic Service Bundles.
- Create customized message rules lists, including "Allow" and "Deny" lists (for message senders), as well as an "Exempt Users" list (for users and recipients).
- Organizations with multiple locations can configure MX Logic® Intelligent Routing to seamlessly route email coming into a main public-facing domain (johndoe@company.com) to the appropriate local domain of the user (johndoe@company-uk.com). Intelligent Routing also accommodates delivery of emails sent directly to the local domain, if the local domain has a public mail exchange (MX) record. Intelligent Routing fulfills the role of an internal routing solution, eliminating the need to manage and maintain separate routing equipment.

The MX Control Console<sup>SM</sup> also provides a wide range of real-time daily, weekly, monthly and on-demand reports, which enable staff members to quickly analyze and track email traffic and trends. This reporting can help you to improve overall performance and isolate issues before they can escalate. All MX Control Console reports are available for downloading in CSV or text file formats. The reports include:



- Traffic and bandwidth reports
- Spam and virus volume reports
- Content and Attachment policy violations reports
- Quarantine reports
- User activity
- Event logs
- Audit trail
- MX Logic® Disaster Recovery overview and events

MX Logic® Performance Reports provide customers with greater insight into the on-going performance of their email and Web security services. These reports will allow not only the easy manipulation and comparison of data but also the ability to send these reports automatically to a distribution list. Administrators can opt for weekly and/or monthly delivery of Performance Reports, which cover more than 20 vital areas within the Email Defense Service and the MX Logic® Web Defense Service.

In addition, organizations that subscribe to ConnectWise can configure the delivery of customer-specific, domain-level email traffic and threat data directly to their managed services platform dashboard through the MX Logic® MSP Connector.

#### **Sophisticated, safe external quarantine**

The MX Logic sophisticated quarantine further reduces false positives (legitimate email misidentified as spam) and IT administrator burden by allowing end users to customize their filtering policies and manage their own quarantine. For organizations that support employee quarantine management, MX Logic emails a Spam Quarantine Report to their employees who can then simply and quickly delete, forward, white list and black list quarantined email via our intuitive, Web-based MX Control Console<sup>SM</sup>. Spam Quarantine Reports can also be accessed on-demand at any time.

#### **Quarantine saves time and helps eliminate false positives**

MX Logic consistently achieves industry-leading low false positive rates using 'intelligent,' customizable spam filtering technology. MX Logic believes that leveraging this unique technology is the most effective way to minimize false positives, especially given the growing complexity of spam and the subjectivity of what users define as legitimate email. As an enterprise-class solution, simply blocking or always allowing email according to MX Logic rules is not a foolproof method for optimizing email communications. With built-in features that allow customers to effortlessly condition the quarantine, MX Logic email defense solutions offer the industry's most effective protection against spam and false positives.

#### **MX Logic quarantine process**

MX Logic blocks spam and filters content and other email threats according to corporate guidelines businesses establish and configure when they begin using the



service. Once the email is filtered, the suspect messages are held safely in an offsite quarantine on the customers' behalf. This email quarantine can be managed by the corporate IT department, employees or both.

### **Setting rules around legitimate messages**

Most MX Logic customers opt for IT- and end-user management of the quarantine. Allowing control for both IT staff and end-users helps reduce the amount of time IT managers spend dealing with spam, and also further ensures that the messages end-users view as legitimate are quarantined.

### **Sophisticated end-user conditioning**

When businesses opt for end-user management, which offers employees the ability to condition their own quarantine, MX Logic sends a Spam Quarantine Report to their employees' email in-box based upon pre-established parameters. This allows employees to review the messages that MX Logic has identified as spam – based in part on corporate-defined parameters – and further fine-tune the quarantine rules to meet their specific needs. Employees can simply and quickly delete, forward, always allow, or always deny the messages contained in the report.

### **Keeping spam sensitivity rates high, false positives low**

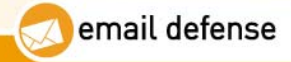
The ability to set highly-specific rules for the quarantine enables businesses to keep spam sensitivity rates high, while keeping false positives extremely low – a tricky combination for businesses who rely on specific e-newsletters, online advertising, and emailed promotions to do business. By spending a few minutes during the first week of service having end-users review and condition their own quarantines, organization can be confident that their corporate policies are enforced, but that email communication remains optimized on an end-user level.

### **Extended quarantine period available to meet your organization's needs**

MX Logic offers a seven-day spam quarantine as part of all Email Defense Service packages (except MX Perimeter Defense<sup>SM</sup>). Businesses can also choose an optional 14-day quarantine period, which is a standard feature within all MX Logic Service Bundles.

## **MX Logic® Disaster Recovery Services**

Unexpected events like natural disasters and malicious email threats can bring down a business network within seconds – derailing communications, jeopardizing business opportunity and resulting in lost revenue. To help businesses take the next step toward end-to-end email security, MX Logic provides valuable email backup protection with our robust disaster recovery services – MX Logic<sup>SM</sup> Message Continuity and the MX Logic® Fail Safe Service.



### **Avoid business disruption with constant communication**

MX Logic Message Continuity provides a wealth of features designed to keep communications flowing during outages, including Web-based email access, management and use. The service provides full email functionality – including Read, Compose, Reply, Forward and Delete – and while both inbound and outbound email is protected from threats by the MX Logic Email Defense Service. Once connectivity is restored, Message Continuity delivers intelligent post-outage email activity synchronization with your mail servers, including all email forensic information (time and date stamps, CC and BCC recipients, and read or unread status).

### **Never lose another email**

Both MX Logic disaster recovery services ensure a company will never lose an email by providing automatic email backup in the event your business is struck by an unforeseeable outage or malfunction, or during planned maintenance. These valuable features are part of the complete line of email defense solutions from MX Logic – features not commonly available with appliance and software solutions.

### **Proactive monitoring, automatic detection, immediate back-up**

With MX Logic<sup>SM</sup> Message Continuity or the MX Logic Fail Safe Service, organizations no longer risk email delays, interception, damage or loss. The services are designed to instantaneously begin email spooling to the MX Logic<sup>®</sup> Threat Center when a loss in connectivity is detected between MX Logic and one or more of a business' Message Transfer Agent (MTA) servers. Once the connection with the email server(s) is restored, current and spooled email is delivered to the business.

### **Flexible platform enables manual operation**

The automatic, proactive features of the disaster recovery services can also be manually activated. While the services are designed to proactively discover disturbances or identify server malfunctions, administrators can manually program Message Continuity or MX Logic Fail Safe spooling for use during planned email server maintenance.

### **Ample storage and immediate notification**

Regardless of whether a business requires backup protection due to scheduled maintenance or in the event of an unplanned outage, Message Continuity and MX Logic Fail Safe automatically engage email spooling when they detect a loss of connectivity to your email server(s). To accommodate prolonged outages, Message Continuity provides 60 rolling days of unlimited storage, while MX Logic Fail Safe provides five rolling days of unlimited storage. Additionally, the services are programmed to automatically provide email notifications – sent to an alternate email address located at another domain – that alert the network administrator when either service has been automatically activated following repeated unsuccessful attempts to connect to the specific email server. Several updates are provided throughout the service activation period including alerts regarding storage capacity and a



confirmation when the service has reestablished a connection to the email server and is releasing spooled and current email.

### Ease of administration through Web-based platform

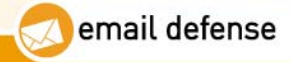
With the MX Control Console<sup>SM</sup>, a secure, intuitive Web-based administration and reporting tool, businesses are given maximum flexibility to customize email protection policies including Message Continuity and MX Logic Fail Safe specifications, notifications and additional storage capacity. Using the MX Control Console, businesses can quickly monitor disaster recovery service activity and spooling levels and easily configure the following:

- Preferences regarding email spooling priority
- Customized disaster recovery notifications
- A schedule for outages
- Ability to suspend incoming mail flow

### Technology Architecture

Fighting spam and other email threats is a constant battle. While companies struggle to stay ahead of the latest threats with new techniques and technologies, spammers and worm authors are developing more and more ways to bypass those defenses. That's why the technology behind MX Logic advanced email defense is the key to defending the entire business network from the entire range of email threats.

- **Network-perimeter protection:** At the core of our advanced technology is our network-perimeter defense – a defense proven to be the most effective way to protect the entire enterprise email system. Because the Internet is a breeding ground for threats, our solution acts as the border patrol between the Internet and the business network to identify, quarantine, block and strip email threats before they can cause damage and disruption.
- **Intelligent Message Processing:** MX Logic Intelligent Message Processing leverages a proxy-based filtering approach that filters email in real time which, unlike the store-and-forward method used by other providers, does not write and store email messages to disk before forwarding them onto the recipient. This method virtually eliminates risk of loss associated with systems outages, message interception or corruption from an infected email base. The process acknowledges the inbound email traffic, immediately opens a connection to the destination recipient email server and filters the message as it flows through the network stream environment and into your messaging system.



- **Multilayered protection framework:** The MX Logic technology framework was designed with a plug-and-play foundation to rapidly and seamlessly integrate the latest filtering layers and techniques available. At the core of our multiple layers is the MX Logic Stacked Classification Framework® spam detection system. Aggregating the most effective spam filters and techniques in the industry, each of the filters in the Framework dynamically calculates the spam probability of every message.
- **Proprietary worm detection technology:** MX Logic's proprietary WormTraQ®, worm detection technology protects against the dangers of mass-mailing worms hours before anti-virus services can distribute signature updates to their customers. Through sophisticated content behavior analysis, the MX Logic® Threat Center is able to quickly identify the common characteristics found in sudden surges of suspicious email messages, which are then intercepted before they can reach customers' email networks.
- **Three leading anti-virus engines equals triple filtering:** In addition to its proprietary worm detection technology, MX Logic incorporates virus protection from three leading engines. The triple protection virtually eliminates the risk of malicious viruses and worms entering the enterprise network because the threats are automatically stripped from incoming email, or are quarantined for review. And, programming up-to-the-minute automated rules, MX Logic scans for anti-virus updates from its anti-virus service providers every five minutes.
- **Threat Center monitors global state of email:** Powering our email defense solutions is the MX Logic® Threat Center, a sophisticated streaming data environment that monitors the global state of email for spam, viruses, worms and other email threats 24 hours a day, seven days a week. The MX Logic Threat Center employs a dynamic defense by continuously incorporating information from its sensor network into its database and writing and updating its filtering rules to protect against the latest threats. And, the centralized nature of the service allows MX Logic's experts to update its systems more rapidly than other types of solutions in order to react to new forms of email threats and, in turn, provide immediate protection to its thousands of customers.
- **Guaranteed around-the-clock availability:** Our data center production environment provides immediate disaster recovery and high availability, and the MX Logic Network Operations Center (NOC) provides 24x7x365 operational support and automated monitoring of all service components. Our production facilities provide for carrier-grade infrastructure and our architecture design lends itself to a low-cost and highly distributed "pod"



environment. Network and application monitoring provides remote operations personnel visibility into suspect or trouble alerts and alarms.

- **Scalable and robust:** Filtering billions of messages each month for organizations around the globe, MX Logic supports email networks of any size, in any location. MX Logic's distributed design provides for geographic system deployment and its decoupled components allow for independent scaling or grouping. Organizations can feel confident that MX Logic's scalable systems architecture supports increased volume and growth, its fault-tolerant, multiple data centers will handle excess capacity, and individual elements of the architecture can be scaled in response to traffic requirements. Effortless integration with all business networks is possible through the solutions' native Internet standards support for SMTP, LDAP, MIME, XML-RPC Web services API, LDAP/POP3 authentication, LDAP subscriber queries, and SQL interfaces.

#### **A Closer Look at the MX Logic® Threat Center**

MX Logic believes in the power of technology made possible by human innovation. With the experience and expertise of the MX Logic Threat Management team, the MX Logic® Email Defense Service is successful in blocking over 99 percent of unwanted email from entering business networks, and in delivering a proactive defense against harmful worms and viruses and other malicious threats.

#### **Integrating human intelligence with technology**

The MX Logic Threat Center combines advanced, accurate and up-to-the-minute automated technology with the intelligence and hands-on monitoring of seasoned messaging security experts. Within our sophisticated streaming data environment, our technologists and our technology monitor the global state of email for spam, viruses, worms and other email threats 24 hours a day, seven days a week. Monitoring tens of millions of messages a day for organizations around the world, the MX Logic Threat Center evaluates messaging trends and uses analytics to fine-tune filtering techniques in order to proactively defend against constantly shifting spammer, virus and worm tactics.

#### **A dynamic email defense keeps the network threat-free**

Using around-the-clock email traffic monitoring, our Threat Center veterans proactively identify suspicious patterns and volume anomalies, and then head-off potential infection and attack by quickly implementing updated filters and patches. Because the Threat Center team includes Internet and email experts who live and breathe complex messaging security, we are able develop solutions immediately and block threats in near real-time.



### **Rewriting the filtering rules to address shifting threats**

The MX Logic Threat Center monitors streaming data and completes up-to-the-minute research, while incorporating the latest virus, worm and spam attack information into its database and rewriting filtering rules to capture the new threats. For example, using an automated, real-time threat update program, the Threat Center captures data, like spam fingerprints that contain the URLs of suspected spammers, and then blocks the suspicious URLs. The Threat Center also updates the heuristics – or rules – and loads them into the system to enable it to more effectively separate legitimate email from spam. Anti-virus and anti-worm updates distributed by third-party anti-virus engines are also collected in real-time and systematically loaded.

### **Threat Center monitoring thwarts global attacks**

The advanced technology of MX Logic and its experienced staff successfully detected and integrated protection against the global damage subsequently caused by MyDoom and SoBig.F. Our proprietary WormTraq® worm detection system is uniquely capable of defending against zero-hour threats, which was evident by the rapid response that prevented the MyDoom.A worm from entering our customers' networks within 23 minutes of its outbreak in January 2004 – over five hours before other leading anti-virus companies developed and implemented their own patches.

### **Armed with knowledge**

In addition to staying on top of the latest threats, the team at MX Logic works hard to provide early notification of destructive email to the business community. Using a standard threat communication process, the MX Logic Threat Center is positioned to quickly warn its customers of current viruses, worms, and directory attacks and raise awareness of their characteristics.

### [More about MX Logic Intelligent Message Processing](#)

Email protection and security service companies traditionally leverage one of two methods for filtering email: the 'proxy-based' method and the 'store-and-forward' method. Unlike other email service providers, MX Logic almost exclusively filters messages by proxy, as this method offers greater security and eliminates the risks inherent in store-and-forward filtering.

### **The flow of email makes the difference**

While both methods utilize the domain's mail exchange (MX) record for filtering, the proxy-based method is clearly superior in its email delivery performance – removing domain-level vulnerabilities and increasing overall network security. In general, the difference in the methods comes down to how the email flows through the filtering process: the proxy-based method does not disturb the normal flow of email, while the flow is significantly altered with the store-and-forward method.



### **Email vulnerability risks are virtually eliminated**

The store-and-forward method presents risks of message loss and interception. Unlike the proxy-based method, store-and-forward filtering writes and stores all email messages to disk outside the corporate firewall, filters them in succession, and then forwards them to their intended recipients. The vulnerability with the store-and-forward method exists within the message queue. Because messages are stored, filtered and then forwarded, email messages are subject to loss through system outages, message interception, or corruption from an infected email base. Using Intelligent Message Processing technology, MX Logic proxy-based filtering virtually eliminates message delivery risks.

### **Removing the risk of delivery failure**

The proxy-based filtering approach also removes the risk of delivery failure that results from 'network islanding.' Network islanding occurs when the destination server identifies a message as undeliverable and the message becomes stranded between the originating server and its destination. Proxy-based filtering removes this risk by never accepting responsibility for the delivery of legitimate message traffic. If disaster strikes at the destination message server, the email will bounce back to the sender normally as mandated by the Simple Mail Transport Protocol (SMTP).

Both MX Logic<sup>SM</sup> Message Continuity and the MX Logic<sup>®</sup> Fail Safe Service are available to ensure that your business never loses an email by providing automatic email backup protection in the event of an unplanned server or network outage, or during planned maintenance. Both of our disaster recovery services automatically engage email spooling when we detects a loss of connectivity to your email server(s). Once the connection with your email server(s) is restored, current and spooled email is delivered to your business.

### **Real-time message filtering reduces latency**

The MX Logic proxy-based method delivers sub-second message latency as it does not accept and store the messages in order to filter them. Generally, MX Logic acts as a conduit between the email sender and recipient – filtering the message in-stream, real-time as it passes from the sender to the recipient. Because messages are never stored during the in-line filtering process, emails filtered by MX Logic experience sub-second delivery – avoiding the latency issues from high-traffic and overburdened queues commonly experienced with the pure store-and-forward method employed by other providers.



## MX Logic Email Defense Service Packages

The MX Logic Email Defense Service is packaged and priced in five solution bundles.

- **MX Ultimate Access<sup>SM</sup>**: Our most comprehensive package includes powerful email security plus MX Logic<sup>®</sup> Message Continuity, which provides email storage, access and use during planned or unplanned outages.
- **MX Ultimate Defense<sup>SM</sup>**: A robust package of email threat services and the MX Logic<sup>®</sup> Fail Safe Service, our storage-only disaster recovery service.
- **MX Critical Defense<sup>SM</sup>**: An ideal package for businesses that require advanced protection against inbound threats.
- **MX Enterprise Defense Plus<sup>SM</sup>**: This package allows organizations of all sizes to customize the Email Defense Service to meet their unique email threat and disaster recovery needs.
- **MX Perimeter Defense<sup>SM</sup>**: The ideal low cost service perfect for businesses needing to reduce the load on their existing on-premises anti-spam solution.

	MX Ultimate Access <sup>SM</sup>	MX Ultimate Defense <sup>SM</sup>	MX Critical Defense <sup>SM</sup>	MX Enterprise Defense Plus <sup>SM</sup>	MX Perimeter Defense <sup>SM</sup>
Perimeter IP Filtering	✓	✓	✓	✓	✓
Advanced Spam Blocking	✓	✓	✓	✓	
Premium Anti-Spam Multi-Language Filter	✓	✓	✓	✓	
Triple Virus & Worm Scanning	✓	✓	✓	Add-on	
Double Virus & Worm Scanning				Add-on	
Zero-hour Worm Protection	✓	✓	✓	✓	✓
Content & Attachment Filtering	✓	✓	✓	✓	
Email Attack Protection	✓	✓	✓	✓	✓
Fraud Protection	✓	✓	✓	✓	
Advanced Administrative & Reporting Portal	✓	✓	✓	✓	
Sophisticated Quarantine Management	✓	✓	✓	✓	
24x7 Monitoring	✓	✓	✓	✓	✓
24x7 Customer Support	✓	✓	✓	✓	✓
Outbound Message Filtering	✓	✓		Add-on	
MX Logic <sup>®</sup> Message Continuity	✓			Add-on	
MX Logic <sup>®</sup> Fail Safe Service		✓		Add-on	
Extended Spam Quarantine	Add-on	Add-on	Add-on	Add-on	
Intelligent Routing	Add-on	Add-on	Add-on	Add-on	



### MX Logic Service Bundles

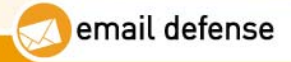
MX Logic service bundles combine the power and protection of our industry-leading email security, Web security and email archiving managed services – all backed by live 24x7 support, innovative technology and our experienced team of threat experts. You can choose from five service bundles to meet the unique needs of your organization:

- **Complete Security<sup>SM</sup>** - A comprehensive bundle that protects your business from spam, viruses and worms, email attacks, fraud and spyware, while enabling you to efficiently store and retrieve all inbound, outbound and internal emails. In addition to the MX Logic® Email Defense Service, Complete Security includes MX Logic® Message Archiving and MX Logic® Web Defense Service Total Control.
- **Email Security & Archiving<sup>SM</sup>** – This bundle combines our award-winning Email Defense Service threat and disaster recovery services with MX Logic® Message Archiving for organizations looking to protect their vital email communications.
- **Email & Web Security<sup>SM</sup>** – The services included in this bundle effectively keep a wide range of email and Web threats from ever entering or leaving your corporate network, by combining our award-winning Email Defense Service with Web Defense Service Total Control.

### Service Bundle Packages and Features

Below are the major features that you can put to work for your business through one of our unique service bundles.

Email Security	Web Security (WDS Total Control <sup>SM</sup> )	Message Archiving
<ul style="list-style-type: none"> <li>• Advanced spam blocking</li> <li>• Triple virus and worm scanning</li> <li>• Content and attachment filtering</li> <li>• Email attack protection</li> <li>• Fraud protection</li> <li>• MX Logic® Message Continuity</li> <li>• MX Control Console<sup>SM</sup></li> <li>• Sophisticated, 14-day spam quarantine</li> <li>• Group policies management</li> <li>• 24x7 threat monitoring and protection</li> <li>• (Optional) Outbound message filtering</li> <li>• (Optional) MX Logic® Intelligent Routing</li> </ul>	<ul style="list-style-type: none"> <li>• Anti-spyware scanning</li> <li>• Anti-virus scanning</li> <li>• Anti-phishing protection</li> <li>• URL filtering</li> <li>• Safe Search protection</li> <li>• Peer-to-peer site blocking</li> <li>• Streaming media site blocking</li> <li>• Group policies management</li> <li>• IP and user-level authentication</li> <li>• MX Control Console<sup>SM</sup></li> <li>• 24x7 threat monitoring and protection</li> </ul>	<ul style="list-style-type: none"> <li>• Unlimited storage</li> <li>• Advanced search options</li> <li>• Definable retention for 3, 5 or 7 years</li> <li>• Secure data transport and storage</li> <li>• Transactional data acquisition</li> <li>• Parallel Search Technology</li> <li>• Saved searches capabilities</li> <li>• Mail source health monitoring</li> <li>• MX Control Console<sup>SM</sup></li> <li>• 24x7 online or phone Customer Support Services</li> <li>• (Optional) Additional historical data storage (25GB increments)</li> </ul>



### 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).

#### **MX Logic Sales Team**

9781 South 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)