

WHITE PAPER

Email Defense Services

Protecting Your Corporate Assets

- Increase control
- Reduce risk
- Minimize time

Executive Overview

The Internet has opened doors of opportunity for businesses around the globe – increasing commerce and trade, creating new markets, and allowing immediate access to volumes of data and information. Unfortunately, the Internet is also opening doors to some very dangerous email-borne threats. With about 564 million email users worldwide¹, electronic messaging is becoming a veritable breeding ground for computer viruses, unsolicited commercial or junk email (spam), and inappropriate content. These unwanted emails cause frustration and aggravation, but more importantly, have the power to jeopardize network security, employee productivity, and corporate integrity.

The risks of unwanted email are growing so quickly that in the second half of 2002, 52 percent of companies cited anti-spam solutions as their top IT priority². To protect their business assets, these professionals are turning to providers experienced in deploying email defense services. While each offers overall protection against spam and network threats, the architecture of the email defense varies – with solutions located at the desktop level, on the server level, and now at the network perimeter. Studies have shown, however, that protection at the desktop and server levels alone is inadequate since over 90 percent of worms and viruses and 100 percent of spam reach the internal network via external email. In order to fully identify and address these threats, the messaging security industry recommends that enterprises filter their email for viruses, spam, and unwanted content before it reaches the network.

Most progressive companies are already aware that malevolent email entering the network can be extremely costly – from a productivity and capital standpoint. In fact, companies spent about \$20.5 billion in 2003 to deploy additional servers due to the inflow of spam³. To stop this problem before it generates debilitating capacity issues, IT professionals and staff are incorporating an external, managed layer of email security at their network's perimeter.

This white paper, presented by MX Logic®, reviews the indisputable threats to the enterprise presented by increased email usage transferring dangerous spam, viruses, and worms. Specifically, this paper:

- Provides an overview of email and its inherent dangers
- Reviews the most effective ways to block email threats before they become detrimental
- Highlights MX Logic's technology and solutions designed specifically for the enterprise

By more fully understanding email trends, growing threats, and the pressure on the enterprise network, businesses can take proactive steps in the ongoing battle to keep email safe and productive.

¹The Radicati Group, January 21, 2004

²The Radicati Group, June 1, 2003

³The Radicati Group, Anti-Spam Market Trends, 2003-2007

Companies spent about \$20.5 billion in 2003 to deploy additional servers due to the inflow of spam.

52 percent of companies cited anti-spam as their top IT priority in 2002.

Studies have shown that protection at the desktop and server levels alone is inadequate since over 90 percent of worms and viruses and 100 percent of spam reach the internal network via external email.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

Email: Inherent Dangers

EMAIL IS UNIVERSAL

With 400 million corporate email boxes worldwide, no other business communications tool matches the popularity of email. Worldwide in 2002, Internet users sent about 14.9 billion emails per day and four trillion emails per year. By 2005, this number will more than triple – translating to a staggering 35 billion emails a day⁴. Currently, the average employee receives 30 emails per day. These statistics alone not only demonstrate the popularity of email, but also the power it yields.

EMAIL IS THE ON-RAMP TO THE NETWORK

As the saying goes, absolute power corrupts absolutely. Unfortunately, email users have more power than they may even know – power that can cause damage and lead to corruption. And because email is so easy and so instant, it can easily and instantly endanger an enterprise's network security and corporate integrity by transporting more than just business-critical communications. Email is today's superhighway being used by hackers and spammers to on-ramp destructive viruses and bandwidth-clogging spam. According to IBM's Global Business Security Index Report, 70 percent of all email traffic on the Internet is unsolicited commercial email. Furthermore, employees are also contributing to email abuse by intentionally spreading sexually- and racially-insensitive material – actions that are resulting in legal liability and corporate defamation.

VIRUSES CRIPPLE CORPORATIONS

As you probably know, email was the transportation culprit for the worldwide infestation of business by malicious code. The International Computer Security Association (ICSA) estimates that 99 percent of businesses suffered virus attacks in the last six months – many of which led to network contamination. According to Ferris Research, 90 percent of all computer viruses are spread by email and cost U.S. businesses \$6 billion in 2001.

- SoBig.F damage estimates range from \$500 million to more than \$1 billion in lost productivity, hours wasted, and lost sales.
- SQL Slammer worm cost between \$750 million and \$1 billion to clean up
- Code Red cost \$2.6 billion in productivity loss, LoveLetter cost \$8.8 billion and Klez virus cost \$9.0 billion.
- At the height of their outbreaks, one in 30 emails contained the SirCam virus, and one in 24 contained the Love Bug virus.
- New viruses, like the Klez variant, can be activated without user execution.

In 2001, companies spent a total of \$13.2 billion in recovery efforts⁵, with single attacks costing businesses an average of \$8,000 to \$100,000. Incidentally, 80 percent of those businesses required at least 20 working days to recover. By 2006, The Radicati Group expects the economic impact of computer viruses to approach \$60 billion worldwide. In a

12 billion spam messages are expected to be sent daily next year in North America alone, in addition to 13 billion person-to-person emails and 6 billion email alerts and notifications.

– IDC

Malicious code is expected to cause over 28 billion in economic losses in 2003, growing to over \$75 billion in economic losses by 2007.

– The Radicati Group

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

⁴ IDC, Channel One Internet Marketing Strategy Report, March 2003

⁵ International Computer Security Association

world increasingly dependent on Internet-based communication, viruses represent one of the most significant threats to the competitive enterprise.

SPAM CAUSES FAR MORE THAN FRUSTRATION

While spam creates tremendous administrative headaches for both email administrators and end users, it also contributes to serious productivity losses and administrative costs.

- In 2001, U.S. businesses spent \$12.3 billion to clean up damage caused by spam.
- In 2002, only five percent of U.S. businesses were able to block 90 percent of spam.
- By February 2003, it was estimated that 45 percent of all email traffic entering an enterprise was spam.
- The volume of spam messages worldwide will grow by 115 percent between 2003 and 2004, totaling 35 billion by the end of this year⁶.

With almost half of all email categorized as spam, and 80 percent annual growth since 2001, the costs are becoming increasingly evident. Osterman Research estimated that in 2002 a 5,000-person company lost \$344,000 in productivity costs because their employees wasted over 12,500 hours just deleting spam. Within the enterprise environment, spam can cost between \$600 and \$1,000 per year for every user⁷.

From an IT perspective, spam uses up bandwidth, slows mail servers, and diminishes productivity. A Radicati Group study found that spam costs corporations \$49 per person, per year in the form of additional messaging servers to handle the mail. Although spam is not intentionally malicious like viruses, it can be even more costly to deal with over time since industry experts believe that spam will account for 70 percent of all the email crossing the Internet by 2007.

UNWANTED CONTENT INCREASES LIABILITIES

In addition to the debilitating effects of spam and viruses, email has become an avenue for mass delivery of unwanted, non-business information. This unwanted content takes the form of profanity, pornography, off-color jokes, music, images, and video files – and puts businesses at substantial risk. In 1999, *USA Today* reported that at least 50 percent of employees received racist, sexist, pornographic, or other inappropriate email while at work.

INTERNAL EMAIL THREATS ADD TO CHALLENGE

Unfortunately, businesses don't have to look much further than their own internal operations to find email threats. With external threats on the rise, so is internal employee email abuse and the damage it can do. Whether employees intentionally spread offensive email, or inadvertently pass on sensitive company information, these activities expose companies to serious legal and financial risks. While establishing and publishing strict employee email and Internet use policies helps reduce some of the risk, email abuse still exists.

⁶The Radicati Group

⁷Jonathan Spira, Spam E-Mail and Its Impact on IT Spending and Productivity, 2003

Spam depletes
bandwidth, slows mail
servers, and
diminishes productivity

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

- In 1995, Chevron settled out of court with four female employees for \$2.2 million, when those employees were exposed to offensive emails sent by male co-workers.
- In July 2002, Hewlett Packard fired or suspended over 150 workers from its offices in the United Kingdom for viewing and sharing pornographic material.

Employees can unintentionally abuse email as well. In 1999, a well-meaning employee of Lockheed Martin sent an email about the National Day of Prayer to 60,000 fellow employees. The mass mailing crashed the company's email system – costing hours in repair and thousands of dollars in lost time and productivity.

Whether the issue is inappropriate content or company-sensitive information, companies risk legal and financial liability when they are unable to regulate the content of inbound and outbound email.

The corporate enterprise faces a multitude of email-based threats every day. These threats are technological, but they have a human element as well. In order to effectively deal with the human element, the enterprise should establish an epolicy – an email and Internet usage policy – to help protect itself and its employees from email abuse.

To address the technological aspects of email, an enterprise must meet increasingly sophisticated email-based threats with an equally-sophisticated and multi-faceted defense.

Email Security

PROTECTION AT ALL LEVELS

Considering the variety of email-borne threats, enterprise networks need a similarly comprehensive defense. Industry experts like MX Logic® recommend a layered approach as the most effective email security solution. A layered solution is one that combines multiple levels of defense for comprehensive email and network security, and is recommended by both the ICISA and Internet Security Alliance (ISA).

Like home security, there are different levels in email security. A home with standard locks on its doors and windows offers some security, while adding an alarm system, motion detectors, and outside video cameras greatly increases protection and limits the risk of intrusion. But the highest level of security would come from an additional layer of protection well beyond the house itself – a guard gate that monitors traffic entering at the perimeter of the community. This solution keeps unwanted visitors away from the house and its on-premise security system.

Enterprise email systems should be protected in the same way. In order to provide optimal protection, email security should be three layers deep: security at the desktop, server, and network perimeter.

Email security should be three layers deep: security at the desktop, server, and network perimeter.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

DESKTOP PROTECTION IS ONE LAYER

The most common form of email security is desktop anti-virus software. This is a sensible client-side solution, but has several limitations.

Desktop anti-virus software must be continuously updated to protect against the latest viruses – requiring hours of systematic and diligent intervention. While an Internet-based subscription service can relieve some of the administrative pressures, they only update every few hours, sometimes even days, which leaves large windows of opportunity for new viruses.

Another shortcoming is that desktop anti-virus software must be properly configured to be effective. This is a challenge, and a risk to the network, since individual users are often not sufficiently trained to properly configure a desktop solution, or can simply neglect to handle the responsibility.

Adding to these dangers, some recent viruses can even disable properly-configured desktop anti-virus security without user intervention.

Desk-top anti-virus solutions are also limited by capability – missing approximately five percent of all viruses. Unfortunately, because different anti-virus engines often cannot work together on the same computer, users cannot strengthen their anti-virus protection to decrease this percentage.

From an anti-spam perspective, free and subscription-based software exists for desktops. These services, however, require constant configuration and may not work at all on an enterprise's network. Effective desktop-based anti-spam subscription services can cost as much as \$10-\$30 per month, but must reside on the email server.

SERVER-SIDE SOLUTIONS MAY BE LIMITED

For most enterprises, the email server is the logical place to install anti-virus and anti-spam software. According to the Gartner Group, about 90 percent of viruses (and, of course, 100 percent of spam) enter a network via email – making the email server the first stop in the route to desktops, operating systems, and applications.

There are a wide variety of email security products available at the server level, and most organizations employ them. But even server-level protection has its limits. As on the desktop, anti-virus and anti-spam software must be installed. With many server-level anti-virus and anti-spam solutions, this can also require the installation of additional hardware. From an administration standpoint, integrating additional software and hardware means increased IT resources to handle configuration, updating, and maintenance.

Nevertheless, because most enterprise email is routed through the email server, protection at the server level is a requirement. In spite of all the available security measures, the server is equally susceptible to many of the same problems that the desktop solution faces: improper configuration resulting in diminished or ineffective protection, and the probability of five percent of viruses getting into the network. Clearly, email protection at the server level alone does not offer comprehensive protection for the enterprise network.

Desk-top anti-virus applications miss five percent of viruses.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

To thoroughly protect the enterprise, viruses, spam, and other forms of dangerous or unwanted email need to be stopped before they can affect the network – at the perimeter.

THE PERIMETER ACTS AS GATE-KEEPER

Like the home security example where the house is protected by a gated community, perimeter email protection implies scanning email for viruses, spam, and unwanted content as it enters the enterprise network from the Internet. This type of protection has been recognized by the messaging security industry as a crucial, though underutilized, layer of corporate network protection.

The ICSA, which studies virus traffic and its resulting damage, has strongly recommended perimeter protection in the past. In fact, after its annual survey of virus prevalence, the ICSA claimed that an external email security service, one that can be configured to filter email as it crosses the enterprise network's perimeter, is "arguably one of the most important assets in the corporate security strategy." This industry group also believes that although perimeter protection is not a replacement for desktop and server protection, it is another layer of protection and a key component necessary for a complete corporate virus protection strategy.

A perimeter email security service provides an enterprise with two significant benefits. First, it filters email outside the enterprise network, removing or blocking viruses, spam, and unwanted content before it can pass through the enterprise firewall. Second, it is significantly less expensive than maintaining a similar set of security services on premise. Finally, perimeter email defense provides more email security options at a lower cost than an in-house solution.

Perimeter email security services briefly route messages intended for the enterprise through a series of filters. By directing the enterprise's mail exchange (MX) record to the filtering service first, incoming email is channeled through the filters prior to entering the enterprise network.

Recognizing that perimeter email security is the key layer for protecting enterprise networks, MX Logic developed its Email Defense Service, a perimeter-based email threat management solution. This additional layer of protection does not replace desktop and server protection, but instead acts as the first line of email defense in a network security strategy – identifying, quarantining or blocking viruses, spam, and malicious content and attachments at the perimeter before they enter the network.

MX Logic's perimeter-based protection reduces risk to desktops and servers, minimizes the time spent on security maintenance, and allows the enterprise to increase control over its own network.

Perimeter protection is another layer of protection and a key component necessary for a complete corporate virus protection strategy. –

Internet Security
Alliance

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

MX Logic: Perimeter Email Security

CUSTOMIZABLE WITH ZERO-INTEGRATION

The MX Logic® Email Defense Service features include Email Attack Protection, Spam Blocking, Fraud Protection, Virus and Worm Scanning, Content and Attachment Filtering and Outbound Message Filtering. As the primary layer in the corporate email security strategy, these intelligent, perimeter-based email filtering solutions successfully identify, quarantine or block suspect messages at the perimeter before they enter the network. Because it is a managed service, it requires no additional hardware or software to install, integrate, or maintain, and zero integration means fast and easy deployment.

Enhancements and new features are continuously developed and automatically implemented, removing technology management burdens from the enterprise. The MX Logic® Email Defense Service is also policy-based which means that an enterprise's IT administrator can customize email filters to suit the unique requirements of the company. In fact, the MX Control ConsoleSM, MX Logic's web-based administration and reporting portal, allows the enterprise to maintain complete control over its email security. With the MX Logic Email Defense Service, the enterprise experiences a dramatic decrease in network damage, downtime, storage utilization, bandwidth congestion, and IT resources. Employees regain time and productivity, enabling them to focus on their core competencies.

NO-RISK ARCHITECTURE

The MX Logic Email Defense Service resides outside of the enterprise network, monitoring incoming traffic from the Internet. The service neither stores nor acknowledges receipt of an email message, so there is no risk of message loss. Instead, the service acts as a proxy, recognizing inbound email traffic with the Simple Mail Transport Protocol (SMTP), and immediately establishes a connection to the destination recipient (enterprise) email server.

Messages are then passed through multiple filtering layers as they are streamed to the enterprise's email server. Email messages filtered by MX Logic experience virtually undetectable latency – usually passing through the filters in a matter of milliseconds. With mirrored, geographically-distinct data centers and 24x7x365 network operation monitoring, MX Logic's services are redundant, diverse, and secure.

EASY, WEB-BASED ADMINISTRATION

The MX Logic Email Defense Service is easy to manage. Administrators can access the MX Control Console to configure their enterprises' unique policies for email filtering. A graphical user interface enables administrators to configure policies according to the enterprise's requirements, including:

- Spam tolerance levels
- Virus quarantine
- Allowable attachments
- Allowable message sizes
- Allowed/denied senders lists
- Unwanted content keywords

MX Logic's Email Defense Service protects the network against spam, viruses, unwanted contact, and blended attacks.

Using proxy-based technology, MX Logic neither stores nor acknowledges receipt of messages.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

Administrators can also view and resolve quarantined email, generate reports, and view real-time email traffic information. Easy to use but with a high degree of detail, the MX Control Console allows for complete control of the service.

ATTACK AND THREAT BLOCKING

MX Logic's email attack protection feature scans incoming email for SMTP compliance or abuse, and blocks any protocol aberrations. The service also protects the enterprise from denial of service (DoS) and other email-based attacks by analyzing and responding to hostile email traffic patterns.

In addition to DoS attacks, protection against other threats include dictionary attacks, mail bombs, traffic flooding, and any other types of attack designed to interrupt service or harvest corporate email addresses. These increasingly common attacks are easy to propagate, but are difficult to defeat – once they reach the enterprise servers the damage is done. The email attack protection feature prevents these attacks from ever reaching the enterprise network with no action necessary on the part of the enterprise business.

With around-the-clock monitoring and virus scanning, MX Logic's experienced staff watches the radar screen – immediately updating and re-programming the service to capture these new attacks. The service protects your business, while removing some of the burden of email quarantine management from the business leader and IT manager.

SOPHISTICATED SPAM DETECTION

MX Logic's Stacked Classification Framework® for spam, a multi-layered approach to identifying unsolicited junk email, halts delivery of spam before it reaches the enterprise network. Using a combination of proprietary, as well as known spam filtering techniques, collaborative anti-spam networks, hundreds of heuristic tests and rules, and a statistical classification engine, MX Logic's anti-spam engines successfully eliminate junk email.

IT administrators and individual users can also configure customizable 'allow and deny' sender lists to further ensure control over incoming email. With MX Logic, enterprise networks regain storage and bandwidth resources, while relieving taxed IT personnel. Network administrators can also configure the spam blocking feature so that any message that appears to be spam is tagged or quarantined for review instead.

MAXIMUM VIRUS AND WORM PROTECTION

MX Logic's virus and worm protection feature filters email using a combination of MX Logic's proprietary worm scanning engine and industry-leading engines from Authentium®, McAfee® and Sophos®. By leveraging three engines instead of one, MX Logic's virus and worm protection virtually eliminates the risk of known viruses entering the enterprise network undetected. Virus patterns and signatures are actively updated every five minutes, making it one of the most up-to-the-minute anti-virus solutions available. Viruses are either stripped from incoming email, or the message is quarantined for review and handling by the network administrator. Additionally, MX Logic uses sophisticated content behavior analysis to detect and block new viruses.

In addition to DoS attacks, protection against other threats include dictionary attacks, mail bombs, and traffic flooding.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

ATTACHMENT AND CONTENT FILTERING

MX Logic's content and attachment feature filters and blocks unwanted attachments before they enter or exit the corporate network. Attachments are filtered three ways: according to filters configured by the enterprise IT administrator, by MIME media type, and by binary content (making sure the attachment's content matches the indicated file type).

Additionally, the content and attachment feature filters messages for content, allowing the enterprise to protect itself by disallowing the transmission of private or proprietary corporate data, racially- and sexually-insensitive material, profanity, and other content considered inappropriate by the enterprise. Both incoming and outgoing messages can be filtered for content and attachments. In conjunction with an epolicy, which is recommended for all enterprises by legal experts on electronic messaging, MX Logic's solutions can help promote and maintain a secure and "hostile-free" workplace.

OUTBOUND MESSAGE FILTERING

One way corporations are proactively addressing the concerns around sent mail is by integrating automated email policy enforcement and email protection for all messages leaving the corporate network. Recognizing the need, MX Logic offers Outbound Filtering service as a standard feature in the MX Ultimate Defense package.

The feature reviews outbound email based on corporate specifications and rules, and filters the messages to prevent accidental or intentional distribution of sensitive or proprietary internal information, guard against the transmission of viruses and inappropriate or offensive content, and ensure regulatory compliance.

Integrated with Content and Attachment Filtering, and Virus and Worm Scanning, MX Logic Outbound Message Filtering is one of the most advanced and proactive ways to ensure mail leaving a corporate network is not sending the wrong message to customers and business partners.

Conclusion

Spam is more than a nuisance. It comprises more than half of all incoming email for corporations today and is growing exponentially – with a 600-700 percent increase in spam growth year over year. Spam clogs end-user email boxes, takes up valuable server space, and impacts network speed. End-user productivity is seriously affected, and IT management is required to handle the increased volume of calls and issues resulting from the increased volume.

Viruses and malicious code pose another set of problems – equally serious although often much more crippling to an enterprise. With billions of dollars each year spent on recovery efforts from virus attacks, today's business leaders are ready to fight and win the battle to make email safe.

The ISA has recognized in several published documents that maintaining a layered security architecture is one of the ten most important information security practices an enterprise can

MX Logic's content and attachment feature filters and blocks unwanted attachments before they enter or exit the corporate network.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com

implement. While a layered approach offers the most complete email security solution for the corporate enter-prise, the strategy is incomplete without a perimeter-level solution.

MX Logic's Email Defense Service is a perimeter-based email security solution that acts as the first and most substantial line of defense. The service enables IT administrators to successfully identify, quarantine, block or strip suspect messages at the perimeter before they enter the network – ultimately increasing control, reducing risk, minimizing wasted productivity, and allowing business professionals to focus on their core competencies.

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. With over 20 layers of defense that are automatically and continually updated, the company's feature-rich solution suite is the industry's most comprehensive, flexible and easy to use.

MX Logic processes billions of messages each month for over 6,000 organizations worldwide, including EnCana, Hyundai Motor America, Internet Initiative Japan, ServiceMaster, The Sports Authority, Verio Inc., and YMCA. 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.

For more information, visit www.mxlogic.com.

MX Logic processes billions of messages each month for over 6,000 organizations worldwide, including EnCana, Hyundai Motor America, Internet Initiative Japan, ServiceMaster, The Sports Authority, Verio Inc., and YMCA.

More Information:

MX Logic Sales Team
9781 S. Meridian Blvd.
Suite 400
Denver, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com