



MAILSHIELD

KEEP SPAM, VIRUSES, AND OFFENSIVE MATERIAL OUT OF YOUR COMPANY EMAIL

The one mission-critical application common to all businesses is email. Email is also the most vulnerable security point of any business network. Most viruses, trojans, and worms are delivered via e-mail. Include the prevalence of spam and inappropriate messaging, and email becomes a high security risk and impediment to productivity.

MailShield Email Security Service, powered by MX Logic®, protects against email based threats, by ensuring that the only mail that enters your network is safe and appropriate for business.

Spam now accounts for 75 percent of all email volume, and virus and worm attacks are costing corporations billions in clean-up efforts. MailShield E-mail Security, powered by MX Logic®, helps organizations eliminate unwanted email and benefit from:

- Increased employee productivity
- Decreased IT costs
- IT resource reductions
- Decreased network and storage costs
- Reduced corporate liability

With no upfront costs or integration lead time, MailShield allows you to protect your email environment with:

- Spam Blocking
- Fraud Protection
- Virus and Worm Scanning
- Content and Attachment Filtering
- Outbound Message Filtering
- Policy-based Management
- Secure Message Delivery via Transport Layer Security
- Sophisticated Quarantine Management

Ease of Administration through Web-Based Platform

From initial installation through final reporting, MailShield makes its services effortless. The service requires no integration or migration and can be activated within one business day. Using the MailShield Control Console, a secure, intuitive web-based email threat management platform, administrators can effortlessly fine-tune email protection, establish group filtering policies, customize corporate policies, and stay abreast of message traffic flow and trends.

KEY BENEFITS

- Simple, effortless activation
- Free up IT resources and reduce costs
- Integrate network perimeter email protection
- Safeguard the integrity of business communications
- Increase employee productivity and control
- Implement effortless email filtering policy-setting including group policies
- Benefit from MailShield Threat Center around-the-clock protection
- Protect against information loss and business disruption with our disaster recovery services

SOPHISTICATED QUARANTINE MANAGEMENT REDUCES TIME AND RISK

Once email is filtered, suspect messages are stored in a safe, external quarantine on the customers' behalf - an off-site queue accessible by corporate IT departments, employees or both. If the customer chooses to allow its employees to manage their own quarantine, MailShield sends a "Spam Quarantine Report" to the employees' email in-box. Our effortless quarantine management allows end users to determine how items captured by the filter should be handled in the future.

MAILSHIELD FEATURE	DESCRIPTION
Spam Blocking	<ul style="list-style-type: none">• MailShield E-mail Security blocks more than 99% of spam• Suspect messages are deposited into an external quarantine for future handling if desired
Content and Attachment Filtering	<ul style="list-style-type: none">• Automatic filtering identifies and blocks unwanted, inappropriate and malicious content in body copy and attachments before it enters or leaves your organization• HTML shield blocks intrusive spam beacons and web bugs
Virus and Worm Scanning	<ul style="list-style-type: none">• Proprietary worm detection technology, identifies and intercepts zero-hour mass mailing worms before they enter or leave a corporate network• MailShield leverages leading third-party anti-virus engines from Authentium®, McAfee® and Sophos®
Fraud Protection	<ul style="list-style-type: none">• Anti-spam rules automatically protect businesses from fraud and phishing scams• Around-the-clock monitoring provides proactive defense against the latest phishing attacks
Email Attack Protection	<ul style="list-style-type: none">• Unique MX record masking technique conceals email servers from the public Internet• Provides instant blocking of denial of service and other SMTP-based attacks
Outbound Message filtering	<ul style="list-style-type: none">• Protects corporate integrity by preventing distribution of sensitive or proprietary information• Option to add footer or disclaimer to all outbound messages
Disaster Recovery Protection	<ul style="list-style-type: none">• Fail Safe Service provides convenient email storage during outages• Optional Message Continuity provides storage as well as Web-based email access, management and use during outages

Advanced, Layered Technology to Block Spam

Unlike traditional on-premises appliance and software products, our feature-rich, highly-reliable service leverages a multilayered strategy to successfully keep more than 99% of destructive messages out of the business environment.

Primary to MailShield's effectiveness is the MX Logic® Stacked Classification Framework® spam detection system. This proprietary filtering system utilizes a patented method of identifying and controlling spam via a voting algorithm based on a sophisticated form of intelligent reasoning to achieve more than 99 percent accuracy. Within the Framework, different spam filters separately assess and "vote" on the probability 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).

Furthermore, as new spam-detection techniques and filters are developed, Mailshield can rapidly and seamlessly integrate them into the flexible Framework such as the Deep Content Analysis filter that addresses attachment spam such as PDF spam.

THE REAL NUMBERS

93% of organizations have had a virus, worm or Trojan Horse successfully infiltrate their network through email.

Osterman Research, Inc.