

Dramatically reduce unwanted messages at the gateway with an array of integrated anti-spam and content control technologies managed through a single, unified interface.

The problem of unwanted and offensive email has graduated from being a nuisance to seriously threatening corporate productivity and uptime. The sheer volume of spam, combined with the ingenuity of professional spammers has rendered traditional anti-spam tools practically ineffective.

IronMail, the leading solution for enterprise spam control, provides exceptionally high detection rates with unparalleled accuracy and excellent manageability, making IronMail the solution of choice for large organizations.

What makes IronMail Anti-spam so effective?

Key Technologies

- Enterprise Spam Profiler (ESP) is the first enterprise spam tool to aggregate the results of multiple spam detection techniques and evaluate spam messages based on an overall profile. ESP allows IronMail to achieve the highest detection rates in the industry.
- User Quarantine provides the highest possible accuracy by allowing users to review their personal quarantine queue, ensuring that no legitimate mail has been captured. Administration is automated, including investigating false positives and constructing rules and policies in response to user feedback. User
- Quarantine allows IronMail to achieve zero false positives with no administrator intervention.
- IronMail's unique gateway appliance form factor ensures that IronMail is in the right place in the network to address all email threats and enforce email policy.
- Unwanted email is stopped at the gateway, before it enters the network, saving bandwidth, storage, and resources.

Multifaceted Detection Tools

- Statistical Lookup Service applies signatures to identify bulk email via collaborative filtering.
- Header Analysis to identify forged headers by applying heuristics.
- Heuristic traffic scanning to identify new threats and spam outbreaks.
- Whitelists, blacklists, content filtering and automated list updating.
- Other tools including Reverse DNS lookup, Realtime Blackhole List support.

Flexible Message Management

- Block, copy, quarantine, forward, subject rewrite or strip headers from messages.
- Create targeted rules for individuals, groups (from LDAP or custom lists) or domains.
- Test rules without interfering with actual mail flow.
- Updates, available as often as hourly, can be automatically applied.

Comprehensive

- Unified policy enforcement at the gateway addresses all email threats, including viruses, hackers, worms, intruders, spam, libelous content and secure delivery.
- Secure appliance provides a hard face to the Internet and protects the entire email system.

Customer experience

"IronMail has succeeded in blocking spam that amounts to about 15% of the total e-mail traffic into Norfolk Southern Corp." according to Tony Samms, director of security information technology at the freight and natural resources company in Norfolk, VA. "Only 1% to 2% of traffic getting through IronMail to users is spam," said Samms."

Computer World



Benefits

- **Increase productivity** by reducing unwanted, unsolicited, non-work related email.
- **Limit liability** by filtering inappropriate email that may offend employees.
- **Reduce load** on your email system by blocking spam and other unwanted email at the gateway before it reaches mail servers.
- **Secure the gateway** by controlling all incoming and outgoing mail and presenting a hard face to the Internet in front of your email systems.
- **Control message traffic** by monitoring and reporting on message volume, size, content, attachments, senders and recipients.
- **Enforce corporate policy** by setting rules based on all major message header and body characteristics including size, attachment type, encryption type, sender, and recipient and provide policy compliance feedback.

IronMail's Anti-spam and Content Filtering features include:

Key Technologies

- Enterprise Spam Profiler (ESP) compiles combined probability and determines actions using multiple anti-spam tool thresholds to detect and block spam
- User Quarantine generates reports for users on quarantined mail and allows them to release messages individually, to ensure no false positives and eliminate administration



Detection Tools

- Rules, policies and signatures developed from CipherTrust's distributed network of customer and Internet detection points
- IP-based blacklist lookup including MAPS, RBL, RSS, DUL and ORBS, as well as a local deny list of suspect IP's
- Anomaly Detection Engine identifies spam based on uncharacteristic IP address, Subject, From, and other key message patterns.
- Automated Spam Management generates new anti-spam rules and policies automatically.
- Weighted analysis tools examine message headers and content
- Pre-installed "dictionaries"
- Message header, body, and attachment filtering of over 200 file types

Management

- Ability to quarantine, forward, drop, "subject rewrite", copy, log or strip headers
- Support for LDAP group-based rules
- Local customizable whitelists to override any or all anti-spam technologies

Administration & Reporting

- Secure, browser-based administrator access
- IP-based access control lists
- Optional Secure Client Authentication
- Comprehensive real-time reporting across all functions of email throughput, intrusion detection, and policy

Deployment & Scalability

- Standards compliant including SMTP, ESMTP, POP3, IMAP4, HTTPS, LDAP, TLS/SSL, SNMP
- Support for standard load balancers allows easy scalability
- Standards-based design compliance ensures integration with other security and mail tools
- Management of multiple IronMail units from a single console

Technical Specifications

- Rack-mounted Intel-based server appliance with redundant components, RAID storage, integrated hardware and software, secure, browser-based interface

Support & Maintenance

- Platinum maintenance program with full upgrades and 24/7 support
- Easy to use and administer through a secure browser-based interface

The IronMail Difference

Secure Platform > IronMail is designed from the ground up to comprehensively secure enterprise email systems at the gateway. It offers the most secure platform available. Built on an extremely hardened operating system, combined with our secure application software, the IronMail appliance eliminates vulnerabilities and unyieldingly protects the entire email infrastructure. With IronMail deployed in your network, the entire email application is hardened against spam, unwanted content, viruses, worms, attacks, and intruders.

Unified Policy Enforcement > While other solutions provide a fragmented approach to policy management, the IronMail unified policy manager enforces policy across the entire email system. It applies comprehensive content filtering, monitoring and reporting capabilities and proactively manages policies across the whole mail system. IronMail improves productivity, reduces liabilities and saves valuable network resources.

IronMail Solutions:

- Anti-spam
- Web mail protection
- Anti-virus
- Secure delivery
- Application protection
- Policy enforcement