

Protect email messages

For most companies, email is used to communicate crucial and confidential information, from personal details to sensitive corporate data. Unfortunately, the vast majority of email content is sent as plain text and is therefore vulnerable to interception and tampering. Email encryption solutions designed to protect message content have been traditionally difficult to deploy and administer, and they typically require the bypassing of corporate gateway protection, such as anti-virus and content filtering controls.

IronMail Secure Delivery provides administrators with a manageable encryption solution. Available as a component of CipherTrust's IronMail appliance, IronMail Secure Delivery offers robust support for multiple encryption technologies. It eliminates end-user intervention and allows gateway anti-virus, anti-spam, content filtering and policy enforcement tools to review encrypted messages when entering and leaving the organization.

What makes IronMail Secure Delivery so effective?

Multiple Encryption Technologies

- TLS/SSL provides gateway-to-gateway and gateway-to-client encryption of SMTP, POP, and IMAP traffic.
- Server-side S/MIME and PGP support allows interoperability with legacy systems.
- Secure web delivery provides a secure link to a web-based mailbox, enabling encryption for any user with web access.
- Driven by Policy Manager and content filtering to ensure compliance with corporate policy.

Easy to Deploy and Administer

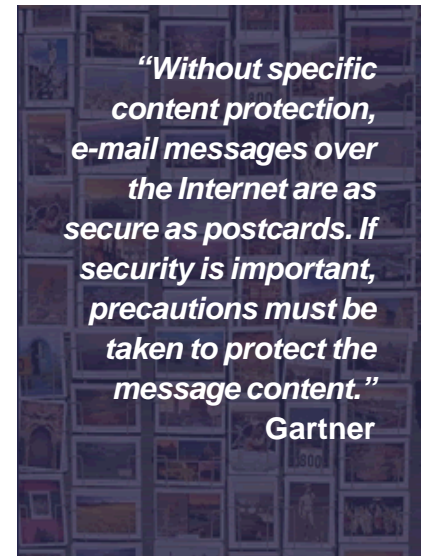
- Multiple encryption options ensure effectiveness regardless of recipient capabilities.
- Precise control and tracking of who, what and how messages are delivered securely.
- Rack-mounted appliance with a secure, browser-based interface.
- Policy enforcement of both incoming and outgoing messages.

Comprehensive

- Complete email gateway threat management, to address viruses, hackers, worms, intruders, spam, libelous content and secure delivery.
- Secure appliance platform provides a hard face to the Internet to protect the entire email system.

"The key to successful implementation of secure messaging is making it easy to use. Implementations will fail if they are seen as delaying message delivery, interfering with readability of messages or requiring too much work on the part of the sender or recipient."

Gartner



Benefits

- **Ensure secure delivery** of critical message content by encrypting based on sender, recipient, or message content.
- **Control message traffic** by monitoring and reporting on who, what, where and when secure messages are delivered.
- **Manage content** by filtering for confidential data and controlling which users are authorized to send encrypted messages.
- **Enforce corporate policy** with robust enforcement and monitoring capabilities, applied at the gateway.
- **Secure the gateway** by presenting a hard face to the Internet in front of your email systems, and controlling all incoming and outgoing mail.

IronMail Secure Delivery features include:

Encryption

- Multiple Technologies*
- Support for ALL major standards-based encryption methods
 - TLS/SSL for secure gateway-to-gateway SMTP, POP, and IMAP
 - Server-side S/MIME and PGP
 - Web delivery (HTTPS) via secure staging server
 - IronMail attempts delivery using any or all encryption methods

“On the Fly” Decisions

- Encryption based on keywords (“confidential”, “legal”, etc.)
- Encryption based on header information (recipient name, recipient domain, sender, attachment type)

- Management*
- Policy driven as well as user driven
 - Highly configurable
 - No client software required at the desktop
 - Interoperable with any email system
 - Message tracking at all stages of delivery



Administration & Reporting

- Secure, browser-based administration with optional Secure Client Authentication
- Comprehensive reporting across all functions of email throughput and policy compliance

Deployment & Scalability

- Standards compliant including HTTP, S/MIME, PGP, HTTPS, LDAP, TLS/SSL, SNMP to ensure integration with other security and mail tools
- High scalability with support for standard load balancers
- IronMail Centralized Management Console allows updates and status views 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



www.ciphertrust.com
877-448-8625