

McAfee Email Encryption

Policy-based protection for outbound messages



“McAfee Email Encryption has helped us secure our patient information and transmit critical messages without worrying about whether we are violating a policy or regulation.”

– Jim Donaldson, Baptist Health Care Corporation

McAfee Email Gateway Encryption Benefits

- Enables secure email communication in any environment, regardless of a recipient’s encryption capabilities
- Policy-driven encryption protects sensitive information without end-user action
- Easy to install and compatible with any messaging server, including Exchange, Notes, and Domino
- Robust reporting and analysis tools provide instant insight into email traffic across the enterprise gateway
- Multiple encryption options for business-to-business or business-to-user communication assure compatibility with any recipient
- Either select an encryption mechanism or let the intelligent encryption process choose the most transparent encryption mechanism for end users

To safeguard against the loss of sensitive data and to maintain compliance with regulations requiring the encryption of sensitive data, email bearing sensitive and confidential information should be encrypted during transmission. But the difficulty of installing and managing existing solutions has prevented many organizations from fully securing their messaging environments. McAfee® Email Encryption, Gateway Edition provides enterprises with an integrated solution for policy-based email encryption. McAfee Email Encryption, Gateway Edition is available as an optional module on McAfee Email Gateway appliances. Customers may choose to deploy it on their Email Gateway appliances or use it as a standalone encryption appliance. McAfee Email Encryption, Gateway Edition provides these capabilities:

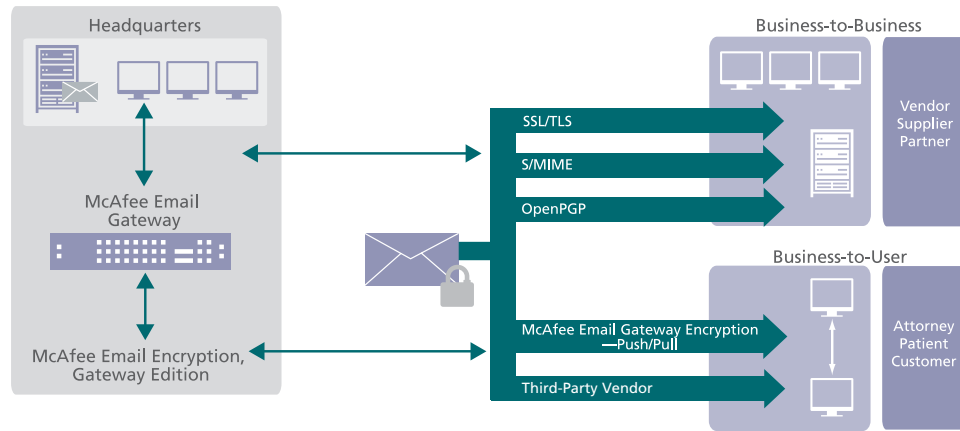
- *Business-to-business encryption*—Default options for secure gateway-to-gateway delivery include TLS/SSL, server-side S/MIME, and OpenPGP for legacy system interoperability
- *Business-to-user encryption*—McAfee Email Encryption, Gateway Edition provides easy-to-use data protection and requires no cumbersome key management. It’s the perfect solution for sending secure messages to any end user. The ability to ensure encryption, regardless of the recipient’s decryption capabilities, opens up the email channel to communications that are protected by government privacy regulations, as well as sharing of sensitive information among business partners.
- *Policy-driven encryption*—Effective encryption depends as much on defining which messages to encrypt as on selecting the right technique. The robust McAfee policy engine leverages lightweight directory access protocol (LDAP) groups, policies, and message characteristics to provide granular policy definition for all types of messages, content, attachments, and recipients.
- *Precise, accurate policy enforcement*—This solution uses today’s most precise and complete detection and enforcement capabilities, employing multiple layers of detection technology to determine a compliance score, select encryption policies, and enforce execution
- *Intelligent encryption process*—It automatically chooses the encryption mechanism that is most transparent to end users. Administrators can also choose the appropriate encryption mechanism.
- *Ease of administration*—Automated key management through a central console simplifies updates, eliminates end-user training, and reduces administrative workloads. McAfee Email Encryption integrates seamlessly with existing infrastructure through LDAP to work in any messaging environment.
- *In-depth reporting and analysis*—Automated logging and reporting allows administrators to instantly see who is sending what type of emails to what recipients, how many are encrypted, and when messages and attachments are opened. The gateway dashboard provides a comprehensive view of traffic flows throughout the entire messaging infrastructure.
- *Scalable and enterprise ready*—McAfee Email Gateway and McAfee Email Encryption are specifically designed for enterprise environments and can efficiently accommodate environments from 25 users to millions of users
- *User customization*—Customers can customize the encryption portal seen by recipients with company branding
- *Handheld support*—Encrypted messages are formatted for viewing on handheld devices

“McAfee Email Gateway (formerly IronMail) is one of the most full-featured email security solutions on the market, providing organizations with protection against spam, viruses, Trojans and phishing, and from outbound policy and compliance violations (including regulatory compliance) related to sensitive data leaks.”

– SC Magazine



“Best Email Security Solution”



Supports six different types of encryption, including both B2B and B2C communications.

Business-to-Business Encryption

McAfee Email Gateway supports multiple protocols for securing communication among businesses, including:

- *SSL/TLS*—Secure sockets layer (SSL) is a protocol for encryption and authentication of Internet connections. Transport layer security (TLS) is the standardized version of SSL. McAfee Email Encryption uses SSL/TLS to create a secure tunnel to the recipient server or client.
- *S/MIME*—McAfee supports secure multipurpose Internet mail extensions (S/MIME) and automatically manages S/MIME key exchange between sender and recipient servers
- *OpenPGP*—McAfee customers can also select OpenPGP technology to send encrypted messages. This solution combines market-leading McAfee message scanning and policy enforcement technology with OpenPGP’s encryption capabilities.

Business-to-User Encryption

Organizations often need to communicate with recipients who have no encryption capabilities. For these situations, McAfee offers several methods to secure messages:

- *McAfee Email Encryption, Gateway Edition—Push*: the push encryption module sends recipients a secure message as an attachment to an otherwise standard email. The recipient can view and respond to the message using any web browser.
- *McAfee Email Encryption, Gateway Edition—Pull*: McAfee offers a secure staging server as a pull encryption option. With this method, an email notifies the recipient that a message is waiting in a secure web-based mailbox. The recipient logs into a secure web page to retrieve, view, and reply to any encrypted messages.
- *Third-party encryption servers*—McAfee Email Gateway supports many third-party encryption servers

Conclusion

McAfee Email Gateway combined with McAfee Email Encryption, Gateway Edition provides a comprehensive solution for email security. For maximum enforcement, it allows granular policies to be set on individuals, groups, and domains; uses advanced techniques to detect message contents; and offers the widest possible range of actions to secure them. For maximum flexibility, it offers six different encryption options with B2B technologies for partner communications and B2C technologies for end users. For maximum return on investment (ROI), the entire solution is delivered via high-throughput, easily scalable appliances that are easy to deploy, implement, and manage.

