Data Sheet

mimecast

Secure Messaging

A User-Friendly, Secure Channel for Sending and Receiving Sensitive Information via Email

Organizations need a method to communicate with external contacts that helps stop inadvertent or deliberate data leaks and protects information in transit. It needs to be simple and intuitive for the sender and recipient and have minimal IT overhead. Traditional approaches, such as Public Key Infrastructure or enforced server-to-server Transport Layer Security, create administrative burdens or client installation requirements.

Secure, private email communications

Mimecast Secure Messaging is a pull encryption service that helps solve these challenges by providing a user-friendly, cloud-based secure channel for sending and receiving sensitive information via email. Sensitive information remains fully protected inside the Mimecast Cloud, with simple, secure access from a browser by following an email notification.

Key Benefits

- **Send emails containing sensitive information easily and securely** - User-initiated or policy-driven secure email delivery via the Mimecast Secure Message Portal with access from a browser.
- **Secure and intuitive message access -** A secure email web portal provides a consistent experience on any recipient device. No recipient software needed. No certificate or encryption key management required.
- **Fully customizable branding -** Tailor notifications and the portal with your company name, colors and logo – helps ensure brand recognition and recipient confidence.
- **Granular message controls -** Sender or policy-driven options to rapidly revoke message access, require read receipt, enforce message expiration dates, prevent reply, reply all, forwarding and printing.
- **Support governance and compliance objectives -** Secure messages are subjected to anti-virus, data leak prevention (DLP) and compliance policies to help meet regulations including PCI-DSS, HIPAA, GLBA, and GDPR.

Secure messaging use cases

- **Send emails containing sensitive information easily and securely**
  User-initiated or policy-driven secure email delivery via the Mimecast Secure Message Portal with access from a browser.
- **Secure and intuitive message access**
  A secure email web portal provides a consistent experience on any recipient device. No recipient software needed. No certificate or encryption key management required.
- **Fully customizable branding**
  Tailor notifications and the portal with your company name, colors and logo – helps ensure brand recognition and recipient confidence.
- **Granular message controls**
  Sender or policy-driven options to rapidly revoke message access, require read receipt, enforce message expiration dates, prevent reply, reply all, forwarding and printing.
- **Support governance and compliance objectives**
  Secure messages are subjected to anti-virus, data leak prevention (DLP) and compliance policies to help meet regulations including PCI-DSS, HIPAA, GLBA, and GDPR.

How it works

Use case 1: user initiated secure message

Users are provided with the flexibility to send a secure message in a number of ways:

- Mimecast for Outlook plugin
- Mimecast for Mac
- Mimecast Personal Portal
- Mimecast Mobile application
- Mimecast Secure Messaging Portal

Users can select a number of options, including request a read receipt, message expiry and restrict printing and replies. Once composed, the message is sent, parked in the Secure Messaging Portal and a notification email containing a link is sent to the recipient.

Use case 2: policy initiated secure message

Secure Messaging can be triggered when emails meet certain policy criteria configured in the Mimecast Administration Console. For example:

- When sent to a particular domain or recipient.
- As a fallback option for enforced Transport Layer Security (TLS).
- The sender puts a keyword (e.g. Confidential) in the subject line.

Encrypted cloud archive

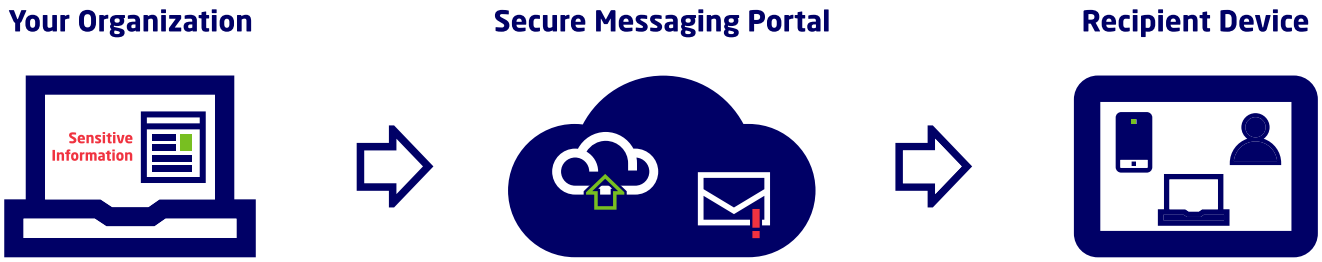
Email and attachments are securely uploaded to the Mimecast cloud, scanned for malware and checked against content and DLP policies before being stored in a secure AES encrypted archive.

Recipient experience

The recipient receives a notification with a link to collect the email from the Secure Messaging Service portal.

The notification email and portal are customized with the originating organization's name, colors and logo. Once the recipient has logged into the Secure Messaging Service portal, they can read and reply to secure messages and compose a new message back to the originating company.

Any message options that were set by the sender are reflected in the recipient's view of the web portal.



1. Employee creates new secure email using Mimecast for Outlook, a Web portal, Mimecast for Mac, or the Mimecast Mobile application. Alternatively, a secure email is triggered by an administrator-defined gateway policy.
2. Email and attachments are securely uploaded to the Mimecast cloud. Sensitive information never leaves the Secure Messaging portal.
3. A notification message with a link is sent to the recipient.