mimecast®

Mimecast Secure Messaging

A user-friendly, secure channel for sending and receiving sensitive information via email.

Email, containing sensitive or confidential information, requires appropriate security and control.

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 burden or end user client installation requirements.

Mimecast Secure Messaging helps solve these challenges by providing a user-friendly, cloud-based secure channel for sending and receiving sensitive information via email. Sensitive information never leaves the Mimecast Secure Messaging portal.

BENEFITS AT A GLANCE

- Send emails containing sensitive information easily and securely - user-initiated or policy-driven secure email delivery from the Mimecast Cloud

- **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 company name, colors and logo – helping 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 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 and GLBA

WHY USE SECURE MESSAGING?

EXAMPLE USES INCLUDE:

- Publicly listed organizations may need to share information about financial results or mergers and acquisitions via secure communications to avoid potential compliance and regulatory breaches

- In healthcare it is crucial to keep individually identifiable health information private. Data leaks could damage reputation and customer or patient privacy and confidence

- Manufacturers should safeguard blueprints from competitors. Exposure of valuable intellectual property could destroy competitive advantage built from years of development and research

How it works

Employee initiated secure message

- Employees create a new email in Outlook. They click on the Mimecast tab within Mimecast for Outlook and select Send Secure. Alternatively, secure messages can be initiated in Mimecast for Mac or using the Secure Messaging webportal

- From the menu they can select administrator-defined secure options: for example; read receipt, expiration and restricted - no print, no reply. Then click Send, as normal

Policy initiated secure message

Secure Messaging can be triggered when email meets certain gateway policy criteria configured in the Mimecast Administration Console. For example:

- When sent to a particular domain or recipient

- As a fallback option to enforced Transport Layer Security (TLS)

- The sender puts a keyword (e.g. Confidential) in the subject line
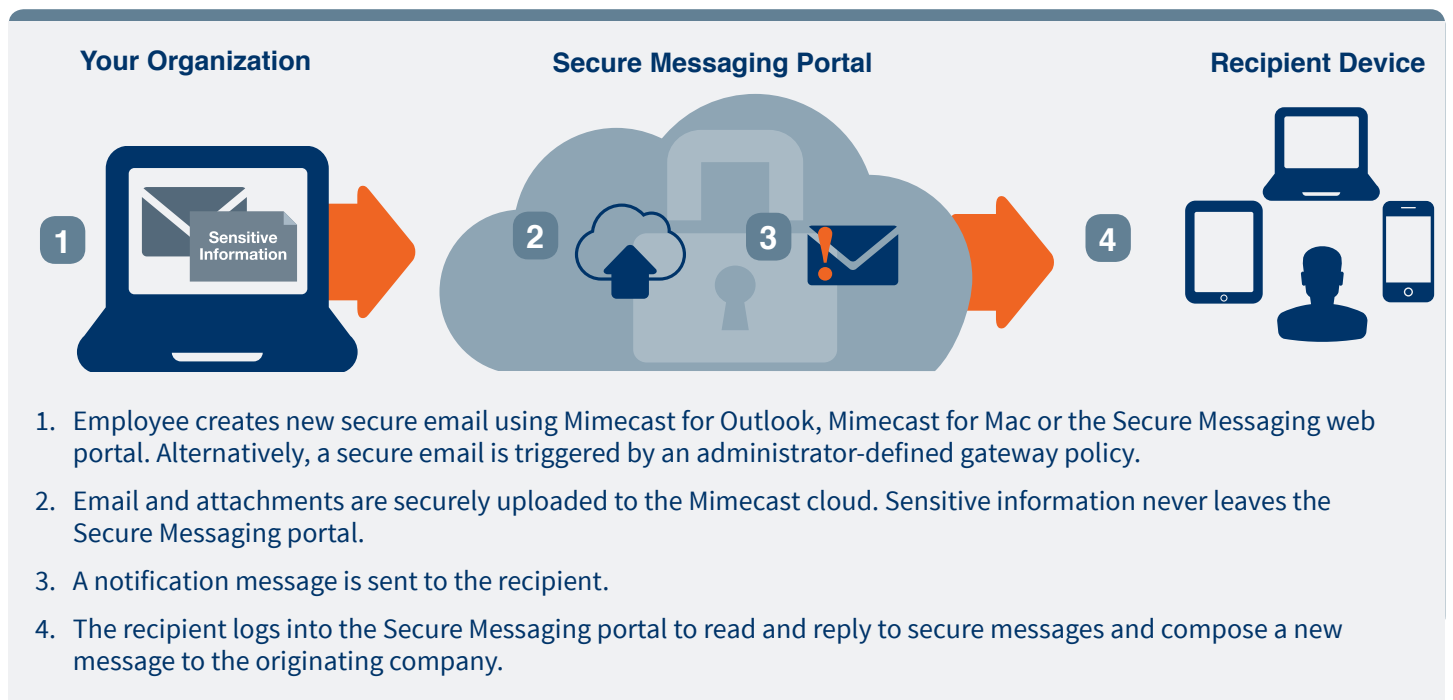
Encrypted cloud archive

- 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

- A notification message is sent to the recipient

Recipient experience

- The recipient receives a notification to collect the email from the Secure Messaging 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 portal, they can read and reply to secure messages and compose a new message to the originating company

- Any message options that were set by the sender are reflected in the recipient web portal

*optional add-on

Your Organization **Secure Messaging Portal** **Recipient Device**

1. Employee creates new secure email using Mimecast for Outlook, Mimecast for Mac or the Secure Messaging web portal. 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 is sent to the recipient.

4. The recipient logs into the Secure Messaging portal to read and reply to secure messages and compose a new message to the originating company.

Mimecast's security, archiving and continuity cloud services make business email safer. The Company protects the email of over 13,000 customers and millions of employees worldwide.

SCHEDULE A MEETING ›
Let us demonstrate how to make email safer in your organization.
www.mimecast.com/request-demo

CHAT WITH SALES ›
Got a question? Get it answered by a Mimecast expert.
www.mimecast.com/contact-sales

GET A QUOTE ›
Tell us what you need and we'll craft a customized quote.
www.mimecast.com/quote