Data Sheet

Secure Messaging

Send and receive sensitive information securely over a user-friendly email channel

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.

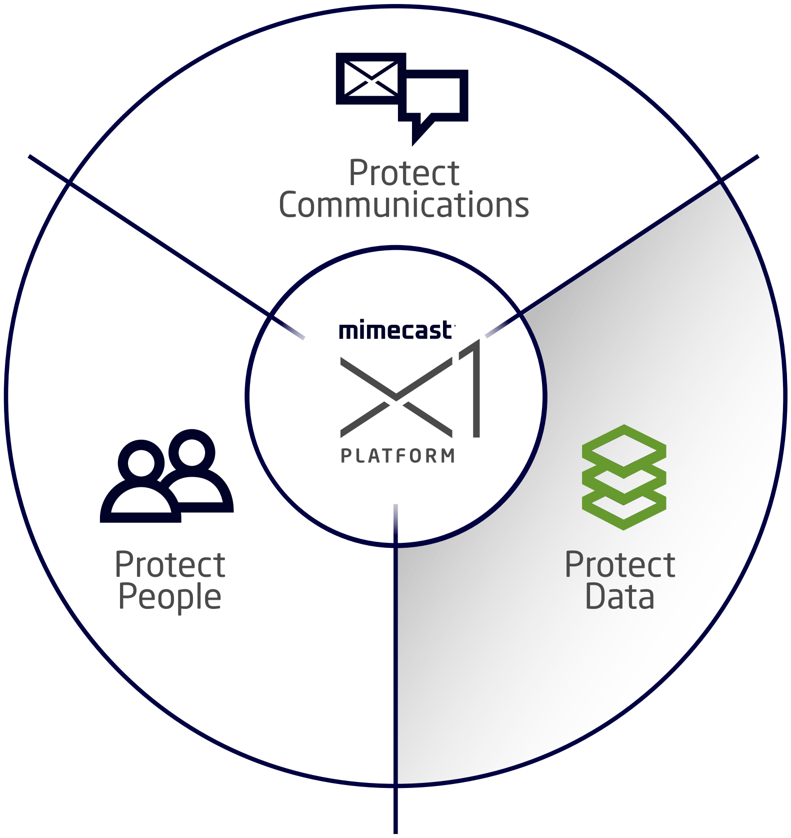
Secure, private email communications

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

Secure Messaging

- Secures email communication for sensitive information
- Provides intuitive and easy message access
- Ensures a familiar end user experience with fully customizable branding
- Enhances security with granular message controls
- Satisfies governance and compliance objectives



Seamless and secure communication for user and policy-initiated email delivery

Accessible from a browser, the Mimecast Secure Message Portal supports user and/or policy-initiated secure email delivery for sensitive information. The fully-featured, secure email web portal enables consistent access on any recipient device. No recipient software is needed, and no certificate or encryption key management is required.

Fully customizable branding

Customize notifications and your portal experience with your company's name, colors, and logo. This ensures brand recognition and recipient confidence when delivering emails via Secure Messaging.

Granular message controls

Secure Messaging gives organizations increased control over email with sender and policy-initiated actions to rapidly revoke message access, require read receipt, enforce message expiration dates, or prevent recipient actions like reply, reply all, forwarding, and printing.

Support governance and compliance objectives

Secure messages are subjected to anti-virus, Data Leak Protection (DLP), and compliance policies to help meet regulations including PCI-DSS, HIPAA, GLBA, and GDPR. Intellectual property and confidential information are protected to help meet regulations.