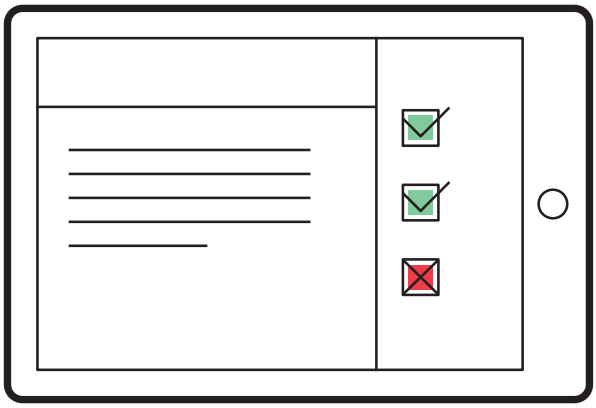
Secure Messaging

Technical Buyer Information

In this age of heightened awareness of information security issues...

Businesses of every size, in every industry – both regulated and non regulated – are recognizing the critical value of Secure Messaging's encryption and message control benefits.



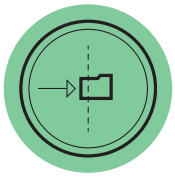
Secure Messaging **Highlights**

Secure Communications on Every Device

Secure Messaging enables users to simply and securely send, receive, track and control email communications on any device, including smart phones and tablets.

Data Loss Prevention

Secure Messaging works with any existing data leak prevention engine and can offer “intelligent keyword scanning” of message content based on an organization’s security policies. Plus, with the ability to fully revoke sent messages, data is always protected.

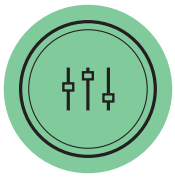


Secure Large File Transfer

Secure Messaging enables users to quickly and securely send and receive file attachments of up to 5GB in size through email without overloading inboxes.

Fully Customized Secure Environment

Secure Messaging provides businesses with a dedicated “slice” of the secure cloud that is fully customizable to match their security policies. The portal is also branded and encrypted for all customers and their existing email environment to create a seamless user experience.



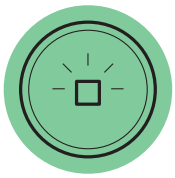
Controls communications

Secure Messaging’s patented “Delivery Slip” provides real-time activity notifications when an email is received and read and enables users to control whether it can be replied to or forwarded. Users can fully revoke a message after it has been sent and apply password protection for sensitive information.

Seamless Integration

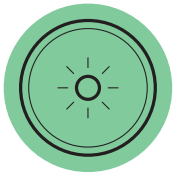
Secure Messaging quickly and easily integrates into existing email infrastructure including Outlook, Office365, Gmail Chrome and other standard email platforms using existing email addresses. Secure Messaging also seamlessly integrates with any proprietary or third-party billing and provisioning system.

Technical **Highlights**



- Data is secured in the cloud with AES-256 encryption.
- Deployed easily through an email plug-in with an optional multi-tenanted gateway that does not disrupt network architecture.
- Native secure email applications for iOS, Android, Blackberry 10 and Windows Phone 8.
- No gateway required for policy-based data loss prevention or encryption.
- Choice to have data hosted in regional data centers for any customer
- Secure Messaging supports the full spectrum of information privacy and security regulations for healthcare, financial services, legal and insurance organizations.

Secure Messaging **Cloud-Based Advantages**

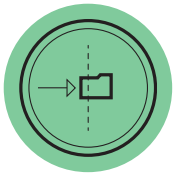


Easy-to-use encryption

Send, receive and track secure corporate messages and attachments using any existing email address or platform. Protect data, meet compliance requirements, and speed up workflow with innovative secure corporate messaging.

Powerfully simple data protection

Secure Messaging is the only DLP solution that can be deployed easily through an email plug-in with an optional multi-tenanted gateway that does not disrupt your network architecture. Additionally, Secure Messaging pairs content filtering with unique pre- and post-send controls such as “For Your Eyes Only” (F.Y.E.O.) password protection, forward- and reply-freeze and true message recall.



Securely send files up to 5GBs

Secure Messaging enables users to send, receive, track and control encrypted file attachments of up to 5GBs directly from any email program without the use of links, thereby eliminating the cost and risk of FTP, unsecured file sharing solutions and couriers. Asynchronous file transfer bypasses file size limitations set by organizations or by recipients so that multiple large file attachments can be sent without slowing down email systems.

Secure mobile device management

Secure Messaging’s native secure email apps for iOS, Android, Blackberry 10 and Windows Phone 8 enable users to send and receive encrypted email and large-file attachments with real-time tracking and enhanced security options from any device or location. No sensitive data is stored on the local device ensuring data remains confidential even if a device is lost. Data is secured in the cloud with AES-256 encryption.

No security keys

With no cumbersome “security keys” needed, Secure Messaging enables organizations to exchange confidential information with all stakeholders in a secure closed-loop environment that’s easy to deploy, manage and scale.

Simple to deploy

Secure Messaging takes minutes to deploy using the platform’s Cloud Command Center interface and rest-based API. A gateway is not required for policy-based data loss prevention or encryption.

Secure Messaging **Cloud-based Advantages**

Supports regulatory compliance and electronic discovery

Secure Messaging supports the full spectrum of information privacy and security regulations. For e-discovery purposes, Secure Messaging ensures messages are verified and intact, and provides real-time knowledge about whether messages were received and read, using date and time stamps.

Integrates with any existing archiving system

Using Secure Messaging's secure API delivery, encrypted messages can be automatically delivered via TLS in a readable format into any third-party archiving solution. This allows all secure messages to be indexed for audit and e-discovery purposes.

Single mail store

Decrypted messages can optionally be stored in the email server, creating a single mail store for e-discovery purposes and user convenience.

Flexible to data jurisdiction

Secure Messaging's cloud-based technology enables organizations to choose in which region their data is hosted to avoid privacy risks imposed by international laws.

Full localization support

Secure Messaging can be used anywhere and provides multilingual localization support for English, French, Spanish, German, Dutch and Japanese.

Secure Messaging **Technical Overview and System Security**

Secure Messaging complements the existing email infrastructure of an organization by adding security, data loss prevention, rapid large file transfer and powerful control features to business email.

Secure Messaging seamlessly adds functionality to existing capabilities without changing the way people send and receive messages. Every message is secure, tracked and auditable.

Secure Messaging also supports all standard third-party compliance archiving systems or document management systems through a powerful rest-based API.

- The optional plug-in for Microsoft Outlook® extends the functionality of the system and the patented Delivery Slip without requiring any mail server modifications for both the sender and recipient.
- No changes are required for the user's email address, email program or email server. Microsoft Hosted Exchange®, Office365® and Google Apps® are all supported.
- All communications with the browser or Microsoft Outlook® are secured via an HTTPS connection – no confidential information is delivered via SMTP.
- Secure Messaging cloud servers are hosted in world-class, tier-1 data centers based across the globe and data can be stored regionally in line with customer requirements.
- All data in transit is secured with a minimum of 128bit SSL and 256bit AES at-rest encryption using Microsoft's .NET Framework AES algorithm (AesCryptoServiceProvider class), a FIPS 140-2 compliant library.

Platform Support and Access

- Email: Microsoft Exchange®, Microsoft Hosted Exchange®, Office365®, IBM Domino® Google Apps®, Yahoo®, Zimbra®, Open-Xchange®
- Mobile O/S: iOS®, Android®, Windows Phone 8®, Blackberry 10®
- Other Web Apps: Google Chrome extension, Office 365 Web App