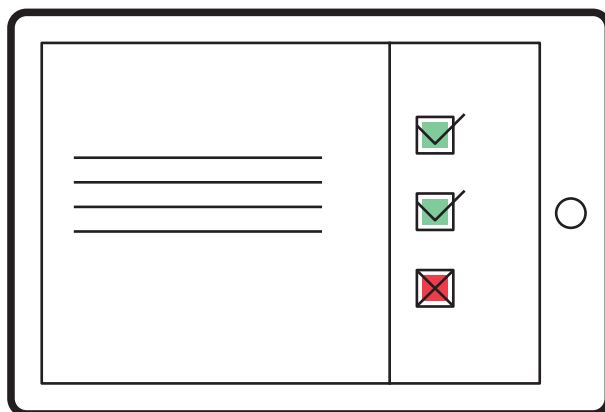
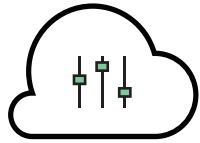


Secure Messaging Enterprise Dedicated Cloud

Secure messaging and message control that is flexible to data jurisdiction, integrates rapidly into Office 365 and Outlook, and supports regulatory compliance.

Enterprise organizations are recognizing the critical value of Secure Messaging Enterprise Dedicated Cloud to protect and enhance their existing email.





Secure Messaging Enterprise Dedicated Cloud

Secure Messaging Enterprise Dedicated Cloud provides a secure dedicated environment for organizations that want to protect, control, and manage how their information is exchanged, even after content has left the email outbox.

Secure Messaging Enterprise Dedicated Cloud (EDC) is far more than traditional encryption. It's a secure communications platform that empowers greater collaboration, productivity, and control, and provides broad support for security regulations and compliance.

Secure Messaging EDC makes it simple for your enterprise users to securely send, receive, track, and control email messages and attachments internally and externally on any device.

Your users can also easily and securely request and provide e-signatures as well as share large files within the email message without requiring additional complex deployments.

It integrates seamlessly with Office 365 and Outlook, letting your users do more work within the enterprise environment.

It also works with any data leak prevention set up (Microsoft DLP, Trend Micro DLP, etc.), as well as most archiving systems.



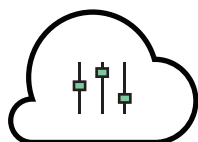
Business breach costs to jump to \$2.1 trillion by 2019.

Juniper Research



In 2015, 60% of enterprises discovered sensitive data breaches.

Forrester Research



Secure Messaging Enterprise Dedicated Cloud



Gives You Powerful Encryption and Tracking

Secure Messaging EDC provides powerful yet easy-to-use encryption and real-time activity tracking so users can securely send, receive, and track communications across devices.



Enhances Enterprise-Level Protection and Integration

Features such as message recall and forward freeze let users control and protect enterprise data. Plus, Secure Messaging EDC works with any existing data leak prevention (DLP) engine and includes “intelligent keyword scanning” of messages based on your organization’s security policies.



Supports Regulatory Compliance and E-Discovery

Secure Messaging EDC enhances compliance across major privacy and security regulations. For e-discovery, it ensures messages are verified and intact, and provides real-time records of whether messages were received and when they were read.



Integrates with Your SSO

Secure Messaging EDC seamlessly integrates with your existing SSO deployment (whether SAML2.0 or OAuth2.0) without requiring new identities for users. Plus, using your own federation service for authentication adds additional reputation to verifying the authenticity of every user.



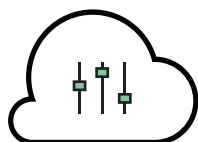
Scales to Match Your Needs

Secure Messaging EDC includes up to 1,000 PRO user licenses and unlimited GUEST user licenses to enable secure communications across the enterprise as well as externally with customers, partners, suppliers, and more.



Provides Advanced Message Control

Secure Messaging EDC lets users control if messages can be replied to or forwarded and can even let them add “for your eyes only” (FYEO) password protection for information meant to only be accessed by the intended recipient.



Secure Messaging Enterprise Dedicated Cloud



Deploys Rapidly and Seamlessly into Office 365 and Outlook

Secure Messaging EDC has no hardware to install, deploys in minutes, and requires no outside IT expertise. It integrates rapidly into existing systems, including Outlook, Office 365, Gmail, and other standard email solutions using existing email addresses.



Provides a Dedicated, Customizable, Secure Environment

With your Secure Messaging EDC portal, you get a dedicated “slice” of the secure cloud that can be easily adapted to your security policies. It’s also custom-branded, includes a dedicated URL, and is encrypted for a seamless user experience.



Provides Unlimited Secondary Domains

In addition to a dedicated URL, unlimited secondary domains can be configured to enable enterprise-wide secure messaging for all of your email addresses, from .com to .org and beyond.



Flexible to Data Jurisdiction

With servers located globally, you can choose where your enterprise data is hosted to comply with data jurisdiction requirements.



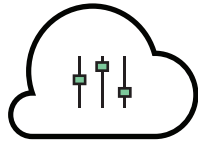
Integrates with Existing Archival Systems

Using a secure delivery method, encrypted messages can be automatically decrypted into any existing archival solution, allowing all secure messages to be indexed for audit and e-discovery purposes.



Enables Secure E-Signing

Secure Messaging EDC lets your users easily and securely request and provide e-signatures on sensitive documents (such as contracts, financial information, etc.). The process is simple and takes seconds at either end of the exchange without requiring additional complex workflows. It supports common document formats (PDF, DOC, PPT, etc.) as well as most image formats (JPG, GIF, PNG, etc.).



Secure Messaging Enterprise Dedicated Cloud



Enables Secure Large File Sharing

Secure Messaging EDC enables both senders and receivers to securely share large file attachments of up to 5GB in size without taxing the network or the mail server.



Enables Content Masking

Secure Messaging EDC lets users mask sender email addresses and subject lines to ensure maximum privacy and data security.



Provides Dedicated Cloud Control

Secure Messaging EDC gives you complete control over portal user groups, daily email-send restrictions (SPAM throttling), access permissions, and the ability to enable and disable Outlook and mobile apps, as well as:

- Leverage two/three-factor authentication for user registration;
- Customize your own SMTP relay for secure notification delivery (support for Sender Policy Framework [SPF] and Domain Message Authentication Reporting & Conformance [DMARC] records for anti-spoofing);
- Customize your own URL for branding purposes;
- Leverage your own SSL certificate to control the level of encryption in transit.