Full Featured Encryption System for Office 365 Message Encryption

A full-featured encryption system that allows users to exchange information securely via email. This system gives organisations the tools to adhere to state and federal privacy regulations. This ensures end-to-end encryption so that sensitive data remains entirely confidential and secure between the sender and recipient.

The need to secure email communications containing sensitive data has never been greater. Fines for non-compliance, negative publicity, legal ramifications, and loss of customer trust are potential consequences for organizations that lose confidential or customer information.

Why Do Organisations Using Microsoft 365 Need Email Encryption?

Microsoft's email encryption service, Office Message Encryption (OME), works with Microsoft 365 to help protect sensitive emails. Recipients of encrypted messages using Microsoft 365 can read those messages in Outlook using their M365 credentials. Other secure message recipients can view the message in the OME portal after logging in through a one-time code or social media login credentials.

Organizations need a 3rd party solution for email encryption, as Microsoft 365 message encryption does not guarantee complete protection against threats. This full featured encryption system integrates with Microsoft 365 and has a seamless integration with Outlook. It has an available Outlook plugin that gives users access to powerful options, including setting the number of days a secure message is accessible to the recipient.

Full Featured Encryption System Vs. Office 365 Message Encryption Feature Comparison

Features Comparison	Full Featured Encryption System	Office Message Encryption (OME)
Target Users	Users are looking for a full-featured encryption service and message that offers multiple delivery methods and is recipient-friendly.	Microsoft 365 customers looking for easy-to-use email encryption without using a third-party solution.
Sending Mail with Encryption	This full featured encryption system can be used as a Secure Message Centre, allowing a customer to self-register, login, and "compose" a secure message to send to anyone within your domain, all without first receiving a secure message.	Allows encrypted emails to be sent both internally and externally. For M365 customers, it's a seamless process. However, recipients are redirected to a portal page if they use another email service.
Configuration Controls	Configuration notifications, including read receipts, a message recall function, and complete auditing of a message such as read, print, save, delete, and reply.	OME users have control options that include the ability to restrict the forwarding and printing of encrypted messages.
Notifications	Secure email recipient reminder notifications so that secure messages are not dismissed. Configuration notifications, including read receipts.	Not available. OME does not provide a notification or confirmation that an email was sent out as encrypted.
Setup and Migration support	Dedicated concierge setup and easy Microsoft 365 and Google G-Suite integration. Full support during POS and after-sales technical support.	Not available. There is no support for migration and setup for M365.
Integrations with Microsoft 365 & Google Workplace	Yes	Microsoft 365 only.
Automatic Policy Based Encryption	Yes	Yes

Multi-tenant	Yes	No
Branded Portal	Yes	No
Cloud-based	Yes	Yes
Excellent Analysing & Reporting Capabilities	Yes	No
TLS with Host Verification	Yes	No
DLP and Keyword Filtering Encryption	Yes	Yes
Email Auditing & Recall	Yes	No

Deployment Options

Keyword Policy-based Encryption

Organizations can select a keyword that employees can add to an email's subject line to force the mail to be encrypted.

Encrypted emails will be sent over TLS 1.2 or higher (HIPAA compliant) or through our secure portal. This can be selected at the onboarding stage.

Outlook Plug-in

The outlook plug-in can be used with our keyword encryption deployment, where the user can select which emails to encrypt for the add-in.

Provides a user with access to powerful options, including the ability to set the number of days a secure message is accessible to the recipient.

DLP-Based Encryption

DLP-based encryption is where all outbound mail must be sent through our EncryptTitan servers.

It has pre-built DLP policies and settings that will look for regulated content in the message body or attachment to encrypt messages automatically.

Why Are Customers Choosing Full Featured Encryption System Over OME?

Microsoft 365 is a great email service provider. However, it lacks in the areas of email spam filtering, email encryption, and email archiving. Hence, additional 3rd party solutions are critical for organizations to create a strong email defense barrier from cyber threats, phishing, ransomware, and data protection.

Another reason Microsoft 365 customers are choosing Full Featured Encryption System over OME is that Microsoft 365 end-users can only use OME if they are using Microsoft 365 Plan E3, Plan E5 or have an Azure Information Protection license.

In addition to this, to view an encrypted message, the M365 users receive an access code to the same email address. Many users feel that this process splits the encrypted message into two emails.

Protect your information and safeguard your organization with Full Featured Encryption System.

Book a Free Full Featured Encryption System Demo