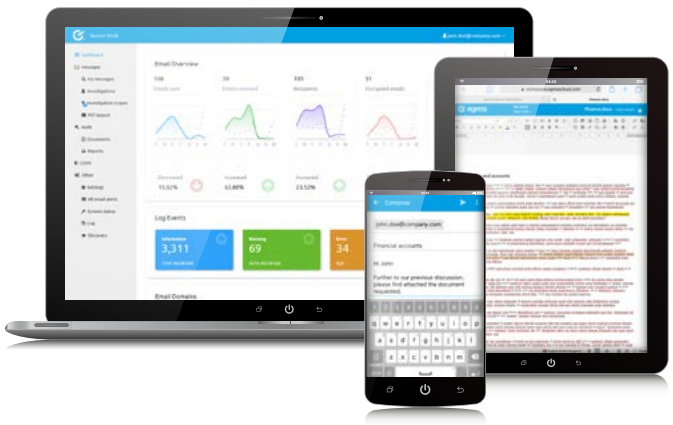
Egress in an **Office 365 world**

The **go-to security overlay** for Office 365, bringing compliance, user engagement and auditing to **hosted** environments.

Many enterprises are adopting Office 365 to reduce costs and increase productivity. While the cloud provides opportunities and efficiency gains, organizations still face many security threats, especially since emails and files remain the most common ways to store and share sensitive data. Many organizations have advanced use cases in terms of compliance, analytics, data loss prevention, user engagement and data residency that require a third-party data security solution that overlays O365.

This datasheet describes 10 benefits of overlaying Egress data security solutions on O365 deployments.



1. Avoid external recipient help desk support costs

Many organizations need to send encrypted messages to non-technical external users, but these recipients can generate a lot of help desk calls. Servicing these support calls is often a hidden cost of email encryption deployments.

While O365 does not provide help desk services to external recipients, Egress is one of the only vendors to offer first and second-line support to these users. This brings significant cost and efficiency savings to organizations looking to secure their external communications.

2. User engagement through machine learning

Misaddressed emails cause many data breaches, but most email encryption solutions only guarantee secure delivery, not whether the recipient is correct.

Egress solutions use machine learning to drive user engagement and prevent the accidental send, going beyond typical data protection techniques to analyze core user behavior and help correct mistakes before they happen.

3. Real-time message audit by users and administrators

Regulations such as the EU GDPR require detailed tracking of sensitive data as it flows inside and outside an organization. Knowing when an encrypted message was sent, understanding message content, and viewing access logs is crucial for compliance.

Egress provides easy-to-use auditing tools for admins and senders in order to quickly meet regulatory compliance requirements, both from within Outlook and through the browser.

4. Real-time revocation of messages by users and administrators

Many situations need instant revocation of encrypted messages. The speed of revocation is very important, and this functionality needs to be provided via intuitive interfaces for both senders and administrators.

Egress provides revocation tools for both admins and senders, including from within Outlook. Revocation is instantly applied, preventing the recipient from viewing the message in their Outlook client, browser and on mobile devices.

5. Fine-grained data analytics for GDPR compliance

Some articles of the GDPR can only be met by employing a fine-grained view of sensitive citizen data within an organization. Egress compliance and analytics tools allow organizations to perform specific searches in order to fulfil data requests as part of GDPR Article 15, including searching across Egress-encrypted content and easily exporting reports. Organizations can also delete data relating to a specific person at the click of a button, in compliance with GDPR Article 17, 'The right to erasure'.

6. Use of existing third-party DLP solutions

Organizations using third party content scanning and DLP tools in their O365 environment may run into problems since they cannot scan O365-encrypted messages. This loss of visibility into encrypted messages creates issues for auditing and compliance.

With Egress, even messages encrypted at the desktop can be decrypted at the network edge, scanned by third party DLP solutions, then re-encrypted for delivery outside an organization. This integration provides full visibility and control over the content of messages both entering and exiting an organization in encrypted form.

7. End-to-end encryption of messages

Regulations often require emails to be end-to-end encrypted, where the entire message and attachments are encrypted at the sender's Outlook environment and delivered in encrypted form. With Office 365 Message Encryption, the unencrypted message and attachments are first delivered via TLS to a central server where they are stored before the recipient uses a weblink to access them. Egress provides end-to-end encryption for Outlook and Outlook Web Access (OWA), as well as network edge encryption. It also supports the ability to scan, classify and protect emails within webmail environments, including OWA.

8. eDiscovery and search of encrypted messages

Regulations related to subject access requests and the Freedom of Information Act require organizations to quickly search through and retrieve content, even in encrypted messages. O365 does not currently provide the ability to retrieve O365-encrypted messages and perform content-related searches. Egress offers indexing and searching tools for both encrypted and plaintext email content, including within attachments. Encrypted messages can also be decrypted before being archived, and Egress supports the ability to bulk decrypt large message stores.

9. Ad-hoc and secure file collaboration

When working with third parties, teams need a single place to share, work on and store the latest file versions. SharePoint Online is more suited to internal groups, it is limited to Office file types and there are currently no tools for administrators to control how all users interact with content.

Egress provides a secure platform where all stakeholders can collaborate, including on PDFs. Users can access the platform from any web browser, while administrators use role-based permissions to manage user capabilities.

10. Data residency and security certifications

Data residency requirements may need data to be kept within geographical boundaries. Cloud services providers often store data in data centers across the globe, moving between data centers and potentially breaking data residency laws. Many customers also need solutions to have various security certifications.

Egress on-premise key management ensures that cleartext data never leaves borders and that data is encrypted before it is sent to the cloud. Certifications including Common Criteria, NCSC CPA and ISO27001:2013 ensure that the product is developed, deployed and managed to the highest security standards.

About Egress

Egress takes a people-centric approach to data security – helping users receive, manage and share sensitive data securely to meet compliance requirements and drive business productivity. Using machine learning, Egress ensures information is protected relative to the risk of a data breach and reduces user friction to ensure smooth adoption.

info@egress.com
1-800-732-0746
@EgressSoftware
www.egress.com