egress

Osterman Research:
Why your company needs third-party solutions for Office 365

A summary of how Egress can provide **enhanced security**, **user engagement** and **regulatory compliance**.

In their white paper, Osterman Research explain that while Office 365 (O365) is robust and capable, a platform of its scope and scale will never manage to be everything to every organization. As a result, third-party solutions should seriously be considered for deployment, either as replacements for the native capabilities available from Microsoft, or as supplements that provide enhanced functionality to meet specific organizational requirements.

This guide highlights aspects of O365 featured in the white paper and describes how the Egress Platform complements O365 deployments to help organizations improve data security, minimize risk and enable effective secure sharing. Egress enhances the value users and teams get from O365 by taking a people-centric approach. It makes email security and compliance easier for internal users and third-parties, by combining intelligently-applied security with unobtrusive, effective guidance within existing workflows.

The sender experience

Microsoft Office 365	The Egress platform
No local audit information for end users and cannot see if the message has been opened by the recipient.	Full auditing for end users, including message opens, forwarding attempts (forwarding blocked as standard) and date and time of access.
Cannot change encryption status or rights after sending.	Increase or decrease classification levels and add or remove any recipients at any point after sending.
There is no read-only mode for multiple attachments.	Multiple attachments can be given restricted-access permissions simultaneously - read-only, watermarking, blocked print, forward or download.
Misaddressed emails	
Office 365 does not analyze a user's normal sending patterns to warn of misaddressed messages and lacks advanced anomaly detection capabilities to detect malicious intent in email sending behavior.	**Egress Risk-based Protection** corrects wrong recipients and mistyped email addresses, and flags potentially malicious email sends, with administrator auditing available.

The sender experience (continued)

Microsoft Office 365	The Egress platform
Message recall	
Cannot revoke access for a specific recipient or add new recipients after sending.	Can add or remove specific recipients, and revoke access for individuals or all recipients at any point after sending.
IT administrators can revoke messages on the behalf of a sender, but this requires a multistep process to locate the message ID and use PowerShell to complete.	Message recall available for all end-users at any point, with simple one-click process to revoke access to all recipients.
Message recall is not available in Outlook Web Access, or as an Office 365 service level option.	Message recall available in all Outlook, Gmail, Web and Mobile apps as standard.
Message recall has the following limitations: • It fails if the message has already been read • It fails if the recipient is in another Office 365 tenant, is not using Outlook, or has moved the message into another folder	Egress message revocation works at any point after sending, regardless of the message being read, moved or accessed on a non-Outlook client.
Recalled messages can be recovered by the recipient through the recovery of deleted items.	Recovery of revoked messages not possible.

The recipient experience

Microsoft Office 365	The Egress platform
No ability to request access.	Recipients can request access to secure messages across all Egress apps.
OME doesn't give third parties the ability to initiate secure communications.	Third-party recipients without a full Egress subscription can read, reply to and initiate secure communications to paying users for free, forever.

Support for third parties

Microsoft Office 365	The Egress platform
Difficulty managing secure email usage of members of the public.	Egress is one of the only vendors to offer first and second-line support to all users. This brings significant cost and efficiency savings to organizations looking to secure their external communications.
Support requests will be redirected back to the customer. Support desk costs are likely to increase.	

Infrastructure

Microsoft Office 365	The Egress platform
Support for hybrid architectures: Microsoft's Advanced Threat Protection lacks hybrid capabilities, meaning that customers with Exchange or SharePoint on-premises, for example, must have a second and separate threat protection offering.	Egress solutions are available in a range of cloud-hosted, on-premise and hybrid configurations. Implementations can be as complex as required for organizational needs, e.g. encryption keys on-premise while using cloud storage, highly sensitive email data archived on premise while non-sensitive data automatically stored in cloud. Gateway implementations allow continued usage of third-party mail scanning platforms.
eDiscovery in the Security & Compliance Center does not work with on-premises Exchange, SharePoint and OneDrive for Business environments.	Egress eDiscovery and Analytics can be implemented across cloud-hosted, on-premise and hybrid infrastructures, and is mail provider and platform-agnostic.

Security, encryption and classification

Microsoft Office 365	The Egress platform
Mailbox compromise	
SSO with Gmail / Outlook credentials risks mailbox compromise. If a recipient's account is compromised, the hacker can able to send encrypted replies to the original sender and other recipients.	Can enforce use of additional authentication measures e.g. MFA to avoid mailbox compromise. Message encryption at rest means even if mailbox is compromised, encrypted content remains protected.
Data Loss Prevention (DLP)	
Not possible in Exchange Online to automatically encrypt when required. Human intervention by the original sender or an administrator is required. In Office 365 Security & Compliance Center, DLP policies cannot proactively flag email sending mistakes.	DLP engine can detect sensitive content in email body and attachments and automatically apply correct level of security, as well as providing advice. **Risk-based Protection** detects misaddressed emails and risky recipient domains, and can recommend alternatives or block send depending on organizational risk profile.
The sender and sender organization cannot demand additional identity verification to assure the message has been received by the correct recipient.	MFA can be applied as standard. Smart Authentication feature in **Egress Secure Email and File Transfer** can automatically mandate additional identity verification dependant on recipient risk profile, e.g. history of communications, domain trustworthiness, location, device.
OMEv2 offers encryption for Microsoft Office file types and PDF documents only.	All filetypes can be encrypted in transit and at rest, with no file size limitations.
Phishing	
Protecting users from being impersonated by others requires manual action by an administrator to create an anti-phishing policy and list each specific sender to protect.	**Risk-based Protection** can detect phished domains and warn or block users from replying.
Common email authentication mechanisms that are not effective at identifying brand-spoofing where look-alike or soundalike domain names with their own strong email authentication are used.	**Risk-based Protection** analyzes the security profile of the recipient domain to understand the risk involved and take appropriate action.

Compliance

Microsoft Office 365	The Egress platform
No long-term storage of audit logs for compliance (Office 365 E3 Audit Log retains for 90 days, for Exchange Online an administrator can change the default from 90 days, for Exchange logs only. Office 365 E5, audit log entries can be retained for a maximum of one year).	Long term storage of immutable audit logs as standard, and logs update in real time. **eDiscovery and Analytics** provides advanced analytics and reporting functionality for a detailed view of all organizational mail flow, enabling intelligent responses and improvement in information security policy. Also enables fast response to regulatory requests, with assurance that all data is encrypted and untampered with.
Events are not logged in real-time nor available for real-time analysis.	
Exports are CSV files saved locally so exported file does not guarantee authenticity.	
Basic functionality to support subject access requests and the right to be forgotten requirements, but the burden is on IT to fulfil them.	Comprehensive support for the relevant GDPR articles, including advanced, efficient support for SAR completion and deletion in line with the right to be forgotten.

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