

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


How Egress enhances email security, regulatory compliance and user engagement.


In their white paper, Osterman Research explain that while Office 365 (O365) offers a robust and feature-rich email platform, its scope and scale will never manage to be everything to every organisation. As a result, your business should seriously consider third-party solutions, either as replacements for the native capabilities that O365 offers, or as a complementary service that provides enhanced functionality to meet additional and specific needs.


Here we highlight aspects of O365 featured in the white paper and showcase how our Intelligent Email Security platform overlays O365 to help organisations improve data security and prevent breaches. Our human layer approach enhances the value you get from O365, wrapping contextual machine learning around people to simplify email security and deliver unobtrusive, real-time guidance that keeps data safe.



Securing  
**1,000+**  
large  
organisations

 **Prevent security breaches**  
Send the right sensitive information to the right recipient(s).

 **Keep sensitive data safe**  
Apply the appropriate level of security to sensitive email content.

 **Meet regulatory requirements**  
Protect data to stay on the right side of global data protection laws.

 **Boost business efficiency**  
Recipients without a full subscription can read and respond to Egress emails for free.

## The sender experience

Microsoft Office 365	Egress Intelligent Email Security
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 - including read-only, watermarking, and blocked print, forward and download.
<b>Misdirected emails</b>	
Office 365 does not analyse a user's normal sending patterns to warn of misdirected messages and lacks advanced anomaly detection capabilities to detect malicious intent in email sending behaviour.	<b>Egress Prevent</b> corrects wrong recipients and mistyped email addresses, spots wrong content, and flags potentially malicious email sends, with administrator auditing available.
<b>Message recall</b>	
Cannot recall access for a specific recipient or add new recipients after sending.	Can add or remove specific recipients, and recall access for individuals or all recipients at any point after sending.
IT administrators can recall messages on the behalf of a sender, but this requires a multi-step process to locate the message ID and use PowerShell to complete.	Message recall available for all end users at any point, with a simple one-click process to recall access to all / any recipients.
Message recall is not available in Outlook Web Access, or as an Office 365 service level option.	Message recall available in all Outlook, 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 recall 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 recalled messages not possible.

## The recipient experience

Microsoft Office 365	Egress Intelligent Email Security
No ability to request access.	Recipients can request access to secure messages across all <b>Egress apps</b> .
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	Egress Intelligent Email Security
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 organisations 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	Egress Intelligent Email Security
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 organisational needs, e.g. encryption keys stored on-premise while using cloud storage; highly sensitive email data is archived on-premise while non-sensitive data is 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.	<b>Egress Investigate</b> 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	Egress Intelligent Email Security
<b>Mailbox compromise</b>	
SSO with Gmail / Outlook credentials risks mailbox compromise. If a recipient's account is compromised, the hacker is 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.
<b>Data Loss Prevention (DLP)</b>	
It's 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 appropriate level of security, as well as providing advice to senders. We detect misaddressed emails and risky recipient domains, and recommend alternatives or block send depending on organisational risk profile.
The sender and sender organisation cannot demand additional identity verification to assure the message has been received by the correct recipient.	MFA can be applied as standard. Smart Authentication within <b>Egress Protect</b> can automatically mandate additional identity verification dependant on a recipient's 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.

## Security, encryption and classification (continued)

Microsoft Office 365	Egress Intelligent Email Security
<b>Phishing</b>	
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.	<b>Egress Prevent</b> 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.	We analyse the security profile of the recipient domain to understand the risk involved and take appropriate action.

## Compliance

Microsoft Office 365	Egress Intelligent Email Security
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. <b>Egress Investigate</b> provides advanced analytics and reporting functionality for a detailed view of all organisational 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 Subject Access Request completion and deletion in line with the right to be forgotten.

**For more information please contact your account manager or call 0844 800 0172**

### About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen.



[www.egress.com](http://www.egress.com) | [info@egress.com](mailto:info@egress.com) | 0844 800 0172 | [@EgressSoftware](https://twitter.com/EgressSoftware)