Enhance Microsoft 365 with Egress Intelligent Email Security
Introduction

The email security market has undergone a monumental shift in recent years, with the rapid migration to Microsoft 365 (M365) and adoption of the platform’s native email security, and subsequent diminishing reliance on secure email gateways (SEGs) for inbound and outbound threat prevention.

While many organizations are realizing a total duplication in features and functionality between M365 native security and SEGs, others will continue to rely on their SEGs to meet a small number of very specialist security and operational requirements, such as complex routing rules, content-based rules, and archiving. What all can agree on, however, is that the evolving threat landscape and continued anomalies in human behavior mean that, despite their current infrastructures, every organization remains vulnerable to advanced phishing attacks, data loss, and data exfiltration.

As a result, a new category of technology has emerged to complement and enhance the security offered by M365. Integrated cloud email security (ICES) solutions, such as Egress, are designed to provide core capabilities that Microsoft does not offer and to enhance protection as part of a multi-layered, defense-in-depth strategy. In addition to its ICES benefits for inbound threat detection, Egress also uses intelligent technology to prevent outbound data loss and exfiltration caused by human error and risky and malicious behavior, beyond the native security provided in M365.

Improving phishing detection with ICES

Gartner coined the term ‘integrated cloud email security’ or ‘ICES’ in their 2021 Market Guide for Email Security.1 The guide introduces ICES solutions as a new technology category and positions them as the best defense against the advanced phishing threats that evade traditional email security controls, such as those used by M365 and SEGs.

ICES solutions are cloud-based and detect anomalies in inbound emails by combining APIs with advanced AI techniques, including natural language understanding (NLU), natural language processing (NLP), and image recognition. Using inline analysis and/or API access to the cloud email provider, these solutions have much faster deployment and time to value and can analyze email content without needing to change the mail exchange (MX) record. ICES solutions also detect obfuscation techniques, behavioral anomalies through heuristic detection, and compromised internal accounts. Taking it one step further, ICES solutions can also augment security awareness and training (SA&T) programs through real-time risk alerts that form teachable moments.

In their 2021 report, Gartner reflected on the future of ICES solutions, suggesting that they would eventually render SEGs redundant:

---
1 Industry analyst Forrester refers to this category of technology as ‘cloud-native, API-enabled email security’ (CAPES). In this guide we’ll use ICES for consistency.
“Initially, these solutions are deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers’ native capabilities and an ICES is replacing the traditional SEG.”

**Get more from your M365 deployment with Egress Intelligent Email Security**

Egress Intelligent Email Security is designed to provide additional layers of security within M365 to defend organizations against the advanced inbound and outbound threats that get through the platform’s native controls and SEGs. In addition, Egress enables organizations to maximize the benefits of M365 and deliver extra functionality.

This guide explains the ways Egress enhances M365 and the benefits this can bring for your organization.
**Anti-phishing defenses**

Microsoft offers different anti-phishing capability depending on the license your organization has. This security is focused on detecting 'known bad' (previously identified payloads for which libraries of definitions exist) and end-user training.

All environments have Exchange Online Protection (EOP), providing traditional anti-virus engines to identify known-bad malicious payloads and leveraging techniques to check URLs in inbound emails against reputation lists. By default, EOP will send suspicious emails (and spam) to end users’ Junk folders, with only emails that it classifies as ‘High Confidence Phishing’ quarantined. By procuring enhanced licenses, organizations are given access to link rewriting for URLs identified as malicious to block users from visiting phishing websites; malware detonation within their sandbox environment; the ability to retrospectively purge phishing emails from users’ mailboxes once they are identified as malicious; user phish reporting; and phishing simulation training.

**Stopping more phishing threats in M365 with Egress Defend**

The native inbound email security in M365 is effective at addressing phishing threats containing a known payload.

Cybercriminals, however, continue to evolve their attacks to bypass this detection, leaving organizations exposed to zero-day attacks, emerging attacks to cover the time lag while Microsoft’s definitions libraries become available, and ‘payloadless’ attacks that leverage social engineering and written content within the message body to achieve their aims, including those originating from compromised accounts on trusted external domains.

Egress Defend provides an additional layer of security to detect the threats that get through M365 native controls, with particular focus on identifying threats that traditional definitions lists cannot cater for, including zero-day events, supply chain compromise and business email compromise (BEC), spear phishing, impersonation, and CEO fraud. As Defend integrates directly with Exchange Online, rather than sitting in front of it like a SEG, messages analyzed by Defend have already been filtered by EOP, classified as legitimate emails, and delivered to the inbox. As a result, Defend delivers a valuable layer of security by detecting and neutralizing the phishing threats missed by Microsoft.

**Augmenting anti-phishing defenses in M365 with Egress**

Organizations benefit from M365’s effective detection of known phishing threats, which utilizes definitions libraries to determine whether a payload is malicious or not. With Egress Defend, organizations increase their detection capabilities to cover zero-day attacks (‘unknown’ threats) and advanced social engineering attacks, including BEC and attacks originating from compromised trusted domains.
Intelligent phishing detection with Egress Defend

Egress platform data shows that on average, up to 45% of phishing attacks evade Microsoft’s signature-based detection. Egress Defend uses AI to detect and neutralize these advanced phishing attacks, and real-time teachable moments to improve employee awareness. All Defend’s detection techniques are used to build a holistic understanding of an inbound email, providing more granular and reliable threat detection compared to solutions that implement their techniques in isolation of one another.

**Linguistic and contextual analysis**

Using natural language processing (NLP) and natural language understanding (NLU), Defend detects the linguistic indicators of phishing emails, including attention-grabbing subject lines, credibility statements, requests, pressure tactics and emotive language, and consequences of inaction. This enables the solution to identify social engineering attacks that don’t contain a malicious payload but rely on the recipient to perform an action, including BEC attacks such as impersonation and CEO fraud, spear phishing, and invoice and payment fraud. Additionally, this linguistic analysis enables the solution to detect the anomalies present in phishing emails sent from compromised trusted domains.

**One-to-many detection**

Defend proactively detects attackers’ underlying techniques so it can stop the most sophisticated zero-day phishing attacks, as well as emerging threats before definition libraries are available for them.

**Zero trust approach for all inbound emails**

Defend implements a zero-trust approach to all inbound emails, which are analyzed pre-delivery to ensure malicious content is sanitized before it enters a user’s mailbox. The solution doesn’t apply social graph or trust-based analysis until the technology understands the context and content of the email, enabling Defend to detect advanced threats including supply chain compromise (attacks sent from compromised trusted domains) and spoof attacks.

**Robust remediation**

Robust remediation capabilities also allow any Exchange Online customers to enjoy simple-to-use phishing remediation workflows, without requiring additional licensing.

**How Egress Defend proactively protects users from all phishing threats**

Best-practice anti-phishing guidelines consistently call out people as an unreliable mechanism for detection and reporting. People can’t be expected to detect every phishing email, particularly advanced threats such as BEC. At the same time, removing any exposure to cyber threats works against SA&T programs, making people even more unreliable. Additionally, non-cyber experts are unable to consistently differentiate between phishing and spam emails, which can poison some AI models.

By sanitizing emails within the inbox, Defend bridges the gap between neutralizing threats and improving employee education and awareness, while the user-based reporting built into the software has no negative impact on the technology’s detection capabilities.
Dynamic banners that deliver real-time teachable moments

Defend adds banners to every external email but unlike generic warnings that stay the same, the banners vary based on the threat level detected within each email. Using a heat-based warning system, Defend shows amber and red banners depending on the severity of the threat detected, with concise explanations of risk. Users can also click on the banners to visit a webpage that explains how each email has been analyzed by Defend, with a clear explanation of the risks detected.

These visually rich and dynamic banners provide real-time teachable moments at the point of risk, transforming threats into training opportunities and are proven to tangibly reduce risk in customer environments.

Link rewriting

Defend neutralizes all payloads, including malicious URLs. Every link contained within an inbound email is automatically rewritten and analyzed when it is clicked. Safe URLs take users directly to the legitimate website, while users are held at an Egress information page if they click on a phishing link despite the warning banners. This page provides a clear explanation of why the link is considered malicious and users can be blocked from visiting the phishing website itself.

Neutralized phishing email with Egress Defend banners clearly and concisely explaining the threat.

Egress information pages block users from visiting phishing websites, while providing clear and detailed explanations of the risk.
Defend’s detection capabilities for malicious URLs are focused on identifying anomalous redirects, brand and identity impersonation, and common link-based threats like credential harvesting. These techniques do not rely on existing definitions of ‘known bad’ URLs, enabling Defend to augment Microsoft’s SafeLink’s capabilities by detecting zero-day and emerging threats, as well as URLs that are weaponized with post-delivery redirects to phishing websites.

**User phish reporting**

Defend empowers users to provide feedback on emails they believe have been miscategorized. The most common application for this is when Defend detects a low level of risk from an inbound email and the user detects no risk. For example, an email sent from a new external contact, which triggers a first-time sender banner in Defend.

Unlike other solutions, however, Defend is not reliant on this feedback to identify zero-day and emerging attacks. Additionally, this feedback is not used to inform Defend’s AI detection models, meaning they are preserved from misinformation, for example spam reported as phishing, which can reduce detection capabilities in other solutions.

---

**Customer value delivered by Egress Defend in M365**

- **24,012** total number of inbound threats
- **2,789** compromised accounts
- **1,852** impersonation attacks
- **8,802** advanced threats missed by MS
- **15,210** threats detected by MS and sent to junk
- **71%** reduction in user interactions with phishing emails

Data taken from 15,000 employees over a 30-day period.
**Summary: Enhancing M365 anti-phishing capabilities with Egress Defend**

M365’s native anti-phishing controls enable organizations to detect phishing emails containing payloads (phishing links and malware attachments) that are identified in their definition lists, with some link rewriting, and end-user reporting and training capabilities, depending on their M365 licenses.

Defend enhances these controls by using intelligent technology to detect zero-day and emerging attacks that aren’t available on Microsoft’s definition list, and ‘payloadless’ attacks that leverage social engineering, including those sent from compromised trusted domains. Additionally, Defend delivers real-time teachable moments to improve employee education and awareness.

**Summary of a defense-in-depth approach combining MS and Egress**

Augmenting M365 native security with Egress Defend enables organizations to stop more phishing attacks using Microsoft’s protection for known bad attacks and Egress’ AI-driven and behavioral-based security for zero-day, emerging, and social engineering attacks.

<table>
<thead>
<tr>
<th>Inbound hygiene</th>
<th>General phishing</th>
<th>Threat intelligence</th>
<th>Linguistical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware protection</td>
<td>Full attachment/link protection</td>
<td>Threat intelligence</td>
<td>Behavioral, Anti-deception</td>
</tr>
<tr>
<td>Phishing protection</td>
<td>External phishing</td>
<td>Threat intelligence</td>
<td>Behavioral, AI-driven, Deception-driven, Linguistical</td>
</tr>
<tr>
<td></td>
<td>Spear-phishing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social engineering protection</td>
<td>BEC and impersonation fraud</td>
<td>Rule-based</td>
<td>Behavioral</td>
</tr>
<tr>
<td></td>
<td>BEC and invoice fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account compromise protection</td>
<td>Vendor account compromise</td>
<td>NO</td>
<td>Behavioral, Linguistical</td>
</tr>
<tr>
<td>Modern end user experience</td>
<td>Works on any device</td>
<td>YES</td>
<td>Behavioral</td>
</tr>
<tr>
<td></td>
<td>Automated safe listing</td>
<td>Threat intelligence</td>
<td></td>
</tr>
<tr>
<td>Simplified visibility and operations</td>
<td>Single pane of glass</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>Fine grain detection and remediation</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>
**Outbound email defense**

Outbound email threats are behavior-based and caused by both human error and deliberate actions.

Incidents caused by human error are completely unintentional and most commonly the result of:

- Misdirected emails, where one or more incorrect recipients are added to an email, often due to Outlook autocomplete

- Misdirected files, where one or more incorrect attachments are added to an email or attachments contain hidden sensitive data (like in a spreadsheet)

- Replying to spear phishing emails

- Failure to use the Bcc function

- Breach of internal information barriers

- Failure to protect confidential data to an appropriate level

- Replying to newly created or insecure domains

Data exfiltration, meanwhile, falls into two broad categories: well-intentioned but risky actions and malicious behavior. Well-intentioned but risky actions happen when employees knowingly break security policy while completing their work. Examples include sending company data to personal email addresses so they can work from personal devices or print at home, or not protecting sensitive data when shared externally due to complexity for sender and recipient.

People who exfiltrate data maliciously are also aware that their actions contravene security policies, however their behaviors are motivated purely by personal advantage or gain – whether that’s getting ahead at a new job by taking data with them, receiving financial payments for insider trading, receiving compensation from competitors, or the satisfaction of harming the company.

Microsoft’s Azure Information Protection (AIP) provides static, rules-based data loss prevention (DLP) that can be used to detect some human error and deliberate data exfiltration events across the organization. This detection is based on Microsoft’s out-of-the-box gateway policies that can be augmented by administrators’ own rules. These policies integrate with Microsoft’s classification system and work well for standardized data loss incidents, for example preventing certain classifications or types of data from being shared externally. The specific functionality provided depends on the license type an organization holds. Basic features come standard for E3 users and above, while AIP Premium P1, has more features centered on classifying documents that can then enforce DLP policies when shared via email. In addition, Microsoft provides 'Outlook Message Encryption (OME) for organizations with E3 licenses and above. OME provides basic levels of protection without end user features for tracking and revoking messages.
Stopping more outbound email threats with Egress Prevent and Egress Protect

The simple ethos of Egress’ outbound email security is to protect an organization’s most sensitive assets by ensuring only the right data is sent to the right person and with the appropriate level of security.

Egress Prevent and Egress Protect layer security on top of the standard Microsoft policies and tools, enabling organizations to address the most prevalent advanced outbound email threats caused by human error and intentional data exfiltration.

Using machine learning and other advanced techniques, Egress detects incidents that are driven by an individual’s behavior at the specific time that they happen in a way that cannot be detected by static technology alone, primarily due to the unpredictable nature of this threat and scale involved to implement rules department or organization-wide.

When Egress detects that an accidental data breach is about to happen, it delivers prompts directly to the user within their mailbox (in the compose email panel), so mistakes can be corrected in real time. Additionally, email encryption can be automated without relying on end-user input, and specific risky actions can be blocked entirely.

Intelligent email data loss prevention and email encryption with Egress

Egress’ solutions leverage intelligent technology that makes them more scalable and flexible than static solutions, meaning organizations can prevent more security incidents.

Machine learning that dynamically prevents data loss and data exfiltration

Prevent uses machine leaning models to understand each individual user’s behavior when using email, including the recipients and groups of recipients they contact, the regularity with which they email them, and the types of content shared.

The algorithms used include:

- **Supervised and unsupervised machine learning**: Egress’ machine learning is supervised by our policy engine and organizational rules set by administrators to meet a broader set of outbound email security use cases than unsupervised machine learning can alone. As well as enhanced detection and tailoring based on organizational inputs, this supervision also mitigates the chance that Prevent will learn wrong behaviors when incorrectly informed by users.

  Our self-learning technology is layered onto this and is informed by context and user behavior to provide real-time detection of the accidental and intentional behaviors that lead to data breaches.

- **Bayesian inference models**: Once deployed, Prevent is continuously learning and updating each users’ behavior model to improve detection capabilities. User information is ingested as it becomes available and Bayesian inference is used to continuously update the statistical probability that a user is acting as expected.

- **Social graph database**: This technology is used to analyze each user’s relationships, establishing their strength and how they interact, and enabling identification of new or atypical email recipients.
• **Gaussian mixture models:** As part of understanding whether a user is behaving as expected, Gaussian mixture models analyze their typical access patterns to highlight when they are working at unusual times or locations, which might indicate greater potential for error or intentionally malicious activity.

• **Levenshtein Distance model:** This is a metric used to measure the similarity or difference between two strings. Prevent uses this model to analyze words, email aliases and names that are similar but not identical to detect instances of mistyped email addresses, or potential phishing attempts.

Working in real time as an email is composed, these machine learning models determine whether the correct content is being sent to the correct recipient(s). When an anomaly is discovered, Prevent will prompt users to correct mistakes and can block intentionally risky or malicious actions.

**Domain analysis**

Prevent analyzes the domain(s) of every recipient as they’re added to an email. As well as determining whether it’s appropriate to share the content included in the email body and attachments, domain analysis can also be used to increase email security and reduce several additional risks.

This analysis includes:

• Domain age – highlighting newly created domains

• Block-listed domains

• TLS hygiene/status

**Stopping responses to phishing emails, including impersonation attacks**

When a user replies to an email they have received, Prevent conducts its advanced domain analysis. Domain age and block-listing can be used to detect responses to phishing attacks, including scenarios where a spoofed email address has been used and masked from the end user or was difficult for them to detect.
Content analysis

Prevent analyzes the content contained in the email body (including earlier messages within email threads) and any attachments. Leveraging its machine learning models, Prevent compares the content with the recipients and the senders’ previous behavior patterns to detect misdirected emails and files, as well as data exfiltration.

Egress Prevent uses intelligent technology to analyze email recipient(s) and content to prompt users when they inadvertently include incorrect email address(es) or attach incorrect file(s).

Monitoring company leavers

As Prevent is continuously analyzing each user’s behavior, it can alert administrators to unusual behavioral patterns that have been detected (while also blocking risky actions and those that contravene security policy). This includes detecting key indicators that an employee is about to resign from their position, for example sending certain data to their personal email address to be used in a new job.

Once a user has formally resigned, they can be placed on a ‘watch list’ until their contract ends, with greater policy controls to stop leaver exfiltration.

Automating email encryption

Prevent performs content inspection for sensitive data in the message body and attachments for every email. Customizable policies scan the subject line, message body, and attachments for sensitive data, such as social security numbers, financial details, or other specified keywords and expressions. Prevent can also detect Microsoft AIP meta data and apply policy based on these identifiers.

Egress uses this data to perform a risk assessment of the message and the recipient(s) it is being sent to and will prompt the user if it identifies sensitive content or a potential security problem. Users can be notified to encrypt emails where the risk is high or encryption can be automated using Protect, with the message body and attachments seamlessly encrypted with 256-bit AES encryption to keep all data secure and accessible to the intended recipients only.
Transport Layer Security (TLS)

Where sender organizations have configured for opportunistic TLS to fail open, senders are not notified that the message will be sent unprotected if TLS is not correctly configured by the recipient organization(s).

When analyzing recipient domains, Prevent determines whether the correct configuration is in place to allow emails to be sent via TLS. Where it is not in place Prevent can notify the sender that their email will be sent unprotected and prompt them to use email encryption (such as Protect) to secure sensitive content. Additionally, where risk to sensitive data is high, Prevent can notify the user to apply more protection even when TLS is available or can automate encryption via Protect.

Dynamic prompts within the mailbox for real-time tangible risk reduction

Prevent delivers real-time notifications to users at the point when risk occurs. These prompts differ significantly to static DLP solutions, which are formulaic in format and frequency – for example, notifying the sender every time they send an email to an external domain or asking them to approve every recipient and attachment before an email is sent. These static solutions lead to click fatigue, where the sender no longer reads or checks the prompts.

Instead, Prevent only prompts users when a risk is detected, drawing attention to it in real time in the email ribbon and via an expandable side panel. Prevent’s prompts are also customizable and will change based on the warning being given. As a result, Prevent provides value to the user at the point of risk, without overloading them with unhelpful or irrelevant checks. As part of Egress’ philosophy of real-time teachable moments, Prevent transforms threats into training opportunities and tangibly reduces risk.

Preserving rules for the transmission of classified data and information barriers

One of the biggest advantages of M365 E3 and E5 licences is the additional security capabilities available. Egress can integrate with these capabilities, like AIP, to deliver targeted use cases such as advanced DLP, information barrier protection, or specific rules aligned to the transmission of classified data.

As part of the Egress Outlook Add-in and combined with Egress’ gateway infrastructure, Prevent enforces information barriers and ethical walls within an organization based on the system administrators’
customizable parameters. Using GraphAPI to access metadata, as well as other data sources within the organization, Egress can dynamically manage and synchronize keywords, terms, and policies to preserve information barriers on email.

**Certified email encryption with enhanced rights management controls**

Protect provides certified 256-bit AES encryption to protect sensitive files and content shared by email. Through integration with Prevent, encryption can be automated based on organizational policies and real-time risk to confidential data as it is shared by email.

Encryption can also be applied by the user. A user-friendly Outlook add-in makes it easy for to encrypt email content by selecting the appropriate option. This menu and related encryption policies are fully customizable by an organization.

**Revoking access to sent emails and additional access controls**

As Protect provides message-level encryption, both users and administrators can revoke access to encrypted emails after they have been sent to prevent unauthorized access to sensitive data.

Additionally, each encryption label applies varying levels of permissions and control, including read-only access, disabled attachment downloads, and restricted forwarding. The different options also assign their own recipient authentication.

**Authentication**

Egress offers multiple authentication measures to reduce recipient friction. Trusted recipients enjoy seamless authentication without needing to log into the Egress web portal. However, portal-based access, multi-factor authentication, SSO via OpenID, and access using a shared secret remain options for when the risk to sensitive data is higher.

---

**Customer value delivered by Egress Prevent in M365**

<table>
<thead>
<tr>
<th>Type</th>
<th>Prevent Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental data breaches prevented</td>
<td>223</td>
</tr>
<tr>
<td>Total number of incidents detected</td>
<td>566</td>
</tr>
<tr>
<td>Previously identified</td>
<td>11%</td>
</tr>
<tr>
<td>Previously unidentified</td>
<td>89%</td>
</tr>
<tr>
<td>Human error</td>
<td>223</td>
</tr>
<tr>
<td>Data exfiltration</td>
<td>203</td>
</tr>
</tbody>
</table>

**Types of outbound threats**

- Misdirected emails
- DLP violations
- Misspell addresses
- Unprotected information
- Failure to use BCC
- Malicious exfiltration
- Excess recipients

Data taken from a legal firm with 3,000 employees over a 60-day period.
Summary: Enhancing M365 DLP and encryption capabilities with Prevent and Protect

M365’s native DLP controls enable organizations to prevent some human error and data exfiltration security use cases using static rules and email encryption.

Prevent and Protect enhance these controls by using intelligent technology to detect the abnormal behavior that leads to data loss and data exfiltration to dynamically prevent risks and automate protection for sensitive content. In addition to ensuring the right content is sent to the right recipient with appropriate protection, Prevent delivers real-time teachable moments that improve employee education and engagement.

Summary of a protection-in-depth approach combining MS and Egress

<table>
<thead>
<tr>
<th>Feature</th>
<th>Microsoft 365</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent and Protect</td>
<td>Static rules Static rules ML AI-based detection</td>
<td>Static rules synchronized with OU/group membership ML AI-based detection</td>
</tr>
<tr>
<td>Email data loss prevention</td>
<td>Advanced DLP detection for sensitive content</td>
<td>Gateway-based, standard libraries Client-based, custom libraries</td>
</tr>
<tr>
<td>Information barriers</td>
<td>Prevent cross-boundary communication for sensitive or restricted content</td>
<td>Azure AIP provides classification markings Static rules synchronized with OU/group membership ML AI-based detection</td>
</tr>
<tr>
<td>Misdirected email protection</td>
<td>Prevent emails being sent to the wrong person</td>
<td>Not supported ML AI-based detection</td>
</tr>
<tr>
<td>Mis-attached file protection</td>
<td>Prevent mis-attached files/data being sent to the wrong person</td>
<td>Not supported ML AI-based detection</td>
</tr>
<tr>
<td>Data exfiltration detection</td>
<td>Prevent and alert on data exfiltration events</td>
<td>Not supported ML AI-based detection</td>
</tr>
<tr>
<td>Enforced email security</td>
<td>Automatically apply appropriate message security</td>
<td>Azure AIP feeds into classification status TLS Message-level encryption applied based on classification and destination</td>
</tr>
<tr>
<td>Track sensitive content</td>
<td>Automatically classify encrypted content and track delivery</td>
<td>Azure AIP Egress Classification feeds into message-level encryption</td>
</tr>
<tr>
<td>Revoke or expire encrypted emails</td>
<td>Stay in control of encrypted content at all times</td>
<td>Office Addin Message-level encryption</td>
</tr>
<tr>
<td>Realtime Domain Analysis</td>
<td>Perform domain hygiene analysis for email addresses</td>
<td>Basic domain verification only Authentication, reputational analysis including lookalike/ anomaly detection</td>
</tr>
</tbody>
</table>

Microsoft 365 uses static rules and ML AI-based detection for various security features. Egress, on the other hand, offers a range of advanced capabilities such as Azure AIP for classification and TLS encryption. This comprehensive approach ensures a high level of security and control over email communications.
Conclusion: Combining Egress and Microsoft email security to stop more inbound and outbound threats

Combining Egress and Microsoft is an effective defense-in-depth email security strategy. Egress has purpose-built its Intelligent Email Security platform to be highly complementary to M365, using technologies not provided by Microsoft or SEGs to provide enhanced security and to support an increased number of use cases.

When customer organizations layer Egress' advanced technology into their M365 environment, they benefit from intelligent threat detection and prevention capabilities to stop more inbound and outbound threats, without a costly and cumbersome duplication of features.

By enhancing M365 with Intelligent Email Security, organizations are proven to detect the advanced phishing attacks (including BEC, impersonation attacks and CEO fraud, invoice and payment fraud, etc.) that are engineered to circumvent Microsoft’s detection capabilities. At the same time, organizations enhance their outbound security and controls with Egress’ machine learning-based DLP and certified email encryption to stop security incidents caused by human error and data exfiltration, as well as ensure confidential data has the correct level of protection applied.

Integrated seamlessly into M365, Egress Intelligent Email Security is fast to deploy and provides immediate value. With Egress deployed directly into Microsoft Outlook for Windows and Mac, Outlook Web Access (OWA) and all mobile platforms, users require minimal or no training and no changes to working practice. Users also benefit from real-time teachable moments, delivered through banners and prompts directly in the inbox, tangibly reducing risk and augmenting SA&T programs.

The improvements to email security delivered by combining Egress and Microsoft enables organizations to increase their resilience in today’s evolving threat landscape, operate with greater efficiency, and protect themselves from the reputational damage, financial impacts, and customer churn associated with breaches of email security.

To learn more about Egress’ innovation in the ICES space and how it can help you protect your organization, request your personalized demo today.

About Egress

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognize that people get hacked, make mistakes, and break the rules. Egress’s Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats that protect against data loss, resulting in the reduction of human activated risk. Used by the world’s biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.