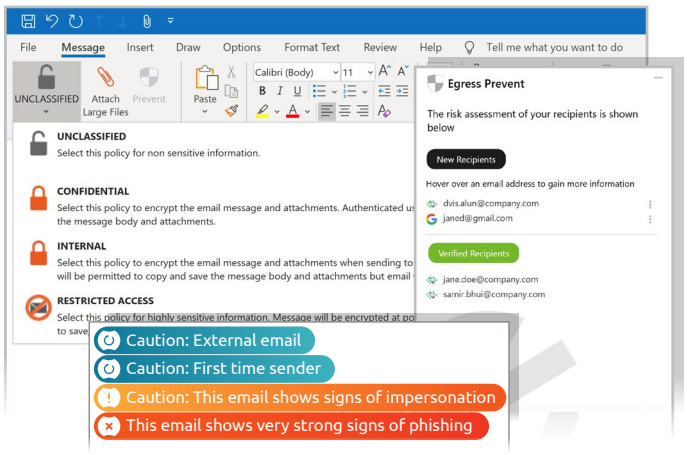
Augmenting Microsoft 365 with Egress Intelligent Email Security

Additional protection for Microsoft 365 that **mitigates human-activated risks on email**

Microsoft 365 (M365) is the go-to productivity tool for nearly 300 million employees worldwide, and has now significantly improved its native email security controls.

Organisations that had previously installed a secure email gateway (SEG) to plug the traditional security gaps in Exchange now see a lot of duplicate features, creating unwanted additional cost and complexity. And importantly, gaps remain in the architecture, especially in the face of complex and human-activated risks.

Egress augments your existing M365 or SEG architecture with sophisticated technologies that mitigate both inbound and outbound email security risks.



Mitigate email security risks

Reduce human-activated risk in M365.

Safeguard your reputation

Keep your customers happy.

Build a first line of defence

Empower people with real-time teachable moments.

Protect revenues

Avoid financial loss while making security a competitive weapon.

Detect and neutralise sophisticated email attacks

Legacy email security controls are resilient versus traditional email threats. However, the bad guys are smarter than ever, using complex techniques such as template-based attacks, supply chain compromise, and payloadless threats to evade existing email security defences.

Egress Defend augments your architecture to provide added protection. By combining zero-trust principles, linguistic analysis, and machine learning technology, you'll detect and neutralise even the most complex threats, such as compromised accounts and zero-day attacks.

Securing **7 million** users every day

Stop accidental and malicious data loss

Traditional email data loss prevention (DLP) tools allow organisations to configure policies that block data leaks to unauthorised sources. However, static rules cannot account for the complexities of human behaviour such as accidentally including the wrong recipient or attaching the wrong file. The lack of sophistication inevitably leads to false positives that frustrate people and extensive policy libraries that monopolise finite administrator resource.

Egress Prevent adds value with supervised machine learning that learns people's email profiles and establishes a baseline of normal behaviour. The technology then flags in real-time when employees are about to email a wrong recipient or attachment, or even maliciously steal company data. That way, you mitigate the risk of email data loss while gaining back significant bandwidth.

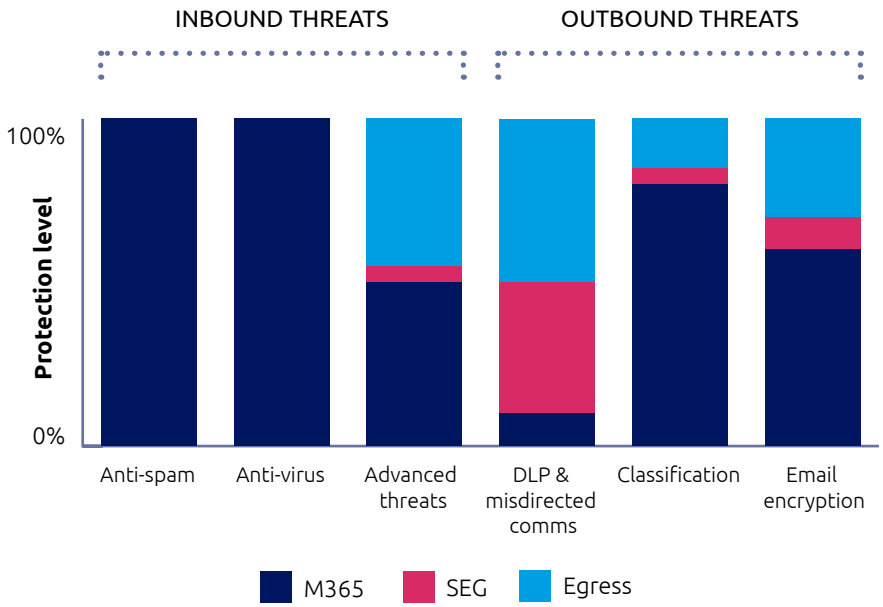
Top five features

1. Contextual machine learning
2. Zero trust models
3. Natural Language Processing
4. Social graphs
5. One-click access

Visit **www.egress.com** for more features.

Avoid recipient pushback on encryption

Microsoft 365 gives organisations an encryption toolkit for users to communicate securely. However, like many other encryption technologies, the layered authentication process risks creating friction that leaves third party recipients frustrated. Egress Protect takes a different approach. Depending on the chosen encryption label, users assign authentication either via a secure portal, a shared secret, or even one-click access, where recipients seamlessly access encrypted emails without needing to log in. That way, you enhance the experience for trusted customers and partners, and boost your brand in the process.



For more information please contact your account manager or call 0203 987 9666

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organisation faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

www.egress.com | info@egress.com | EgressSoftware