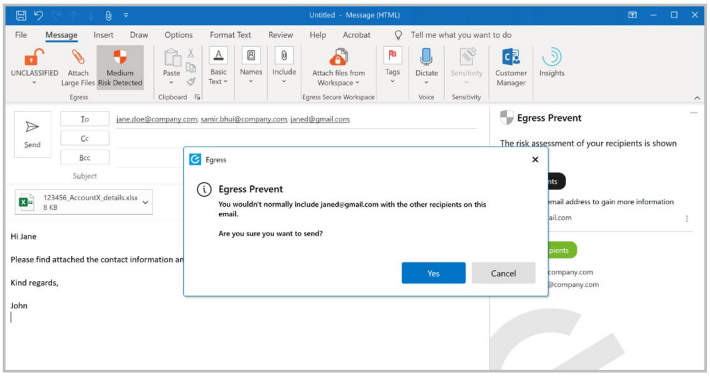
Egress Prevent

Stop **accidental and intentional** email data breaches before they happen.

The nature of email security has changed. Today's digitally connected world and a 24/7/365 working culture means time-pressured employees are making more mistakes and putting sensitive data at risk. Emails to the wrong recipient(s) or containing the wrong content and attachments, phishing victims, and malicious exfiltration are just some of the human-activated threats that cause the majority of security breaches.

We use contextual machine learning and advanced DLP to spot when employees are about to accidentally or intentionally leak data, empowering organizations to:



Prevent email data breaches

Send the right information to the right recipient(s), including personal data.

Comply with global data privacy regulations

Ensure employees' use of email is compliant with regulations like CCPA, GDPR, and PDPA.

Enhance business efficiency

Prevent mistakes on the go with full mobile and OWA support.

Minimize human error

Avoid user fatigue with seamless interaction and user experience.

Using contextual machine learning to account for real-world risks

Employees' behavior is unpredictable, meaning traditional, static approaches to data loss prevention (DLP) are unable to dynamically prevent breaches. Instead, we use contextual machine learning to inspect and continuously learn from a sender's behavior - including who they're emailing, when, and with what content - so we can detect abnormal behavior and prevent breaches of security before they happen. Our intelligent approach also minimizes employee interruptions, so they're not frustrated with an avalanche of prompts.

Securing **1,000+** large organizations

Granted patents: US10911417, US11218379, US11223695
Pending patents: US16/749,580, US16/749,606, US17/036,029

Quantifying risk for measurable compliance

We provide administrators with quick, on-demand reporting that tracks sensitive data and pinpoints any threats to regulatory compliance. Our granular insights ensure you can detect at-risk employees who require frequent help with misdirected emails or might be attempting to intentionally exfiltrate sensitive information.

In addition, our interactive timeline highlights where you have reduced instances of insecure data sharing to potentially unknown systems, improving compliance posture and demonstrating tangible ROI.

Top five features

1. Recipient and domain analysis
2. Email subject, body and attachment analysis
3. Full mobile and OWA support
4. Integration with MS Outlook
5. Comprehensive reporting

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

Detecting abnormal behavior

We use contextual machine learning to spot abnormal behaviour that puts data at risk and apply dynamic protection by analyzing four key areas:

Automated risk assessment

1. Recipient domain
- Domain authenticity
- DKIM / SPF
- Historical analysis of secure communications with domain

2. Sender history
- History of communications with sender, including all recipients emailed in the past

3. Recipient information
- History of communications with recipient
- Geographic and system information about data access

4. Content analysis
- Subject line and message body analysis
- Assessment of attachment name / type
- Analysis of data inside attachments

Dynamic protection

Protection against misdirected emails
Able to spot and provide guidance on incorrect recipients

Quantifiable risk assessment
Provides numeric risk score within email client

Dynamically applied security
Based on computed risk scores, dynamically applies appropriate protection, including Egress, TLS, Microsoft O365 OME, Voltage, Zix, Cisco, Virtru, etc.

Protection of sensitive information
Safeguards against the sharing of sensitive data with unauthorized recipients

For more information please contact your account manager or call 1-800-732-0746

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization 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.

CESG Certified Product Foundation Grade DGEE378428688-1104

bsi. ISO/IEC 27001 Information Security Management

Common Criteria

NATO OTAN

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