Egress Prevent

Defend against **human error and data exfiltration** with intelligent email DLP.

Organizations lose data every day through human error, people breaking processes, and malicious behavior. Egress Prevent uses supervised and unsupervised machine learning to proactively stop email data loss incidents before they happen.

Part of the Intelligent Email Security platform, Egress Prevent leverages an adaptive security architecture, automatically adjusting its security controls based on real-time risk assessments.

---

**Key benefits**

- Detects and prevents data loss incidents caused by outbound email
- Uses an adaptive secure architecture to automatically adjust outbound security controls based on risk
- Lowers administration overhead with intelligent self-learning outbound detection
- Engages users with an unobtrusive real-time risk assessment as they compose an email
- Easy to deploy and maintain cloud service
- Provides visibility and quantifies risk based on user behaviours

---

**Protect against accidental and intentional data loss**

Static DLP is unable to prevent breaches caused by unpredictable human behavior. Egress Prevent uses a combination of intelligent technologies, including machine learning, social graph, and contextual content analysis to detect anomalies that are indicative of human error or malicious intent.

Contextual prompts engage users at the point of risk, enabling them to work efficiently and securely, and reinforcing training with real-time teachable moments.

---

"From a governance point of view, Egress Prevent helps maintain the integrity of client data and demonstrates that we’ve taken the necessary steps to reduce human error when emailing."

Andrew Black, Director of IT at Muckle LLP
Quantify risk while lowering admin overheads

The Egress Security Center provides on-demand visibility of each individual user’s risk level, including insight into employees who receive frequent prompts and monitoring of intentional exfiltration. When a user’s risk score reaches a high risk threshold, Egress Prevent will dynamically adapt its controls to prepare customers for threats before they materialize.

Cloud-based, fully mobile device supported, and easy to deploy, Prevent integrates seamlessly into Microsoft 365, augmenting its native security and that offered by secure email gateways (SEGs). In addition, its self-learning detection technologies require minimal configuration and ongoing maintenance from admins.

Key features

- Automatically detects misaddressed emails and incorrectly attached files
- Adaptive security architecture provides automatic security controls
- DLP policies block malicious exfiltration of sensitive information
- Contextual content analysis of all email parts and attachments to detect anomalous content
- Social graph and machine learning discover relationship strengths to detect anomalous recipients
- Senders are immediately prompted when anomalous behaviours are detected
- Integrates with Azure Information Protection to enforce DLP policies

Integrations

Unlock more value from your existing technology ecosystem investment through native Egress integration with Microsoft 365, SIEM/SOAR, Security Awareness & Training and more.

Book a demo

www.egress.com/book-a-demo

About Egress

Egress is the only cloud email security platform to continuously assess human risk and dynamically adapt policy controls, preparing customers to defend against advanced phishing attacks and outbound data breaches before they happen. Trusted by the world’s biggest brands, Egress is private equity backed with offices in London, New York, and Boston.

www.egress.com

© Egress Software Technologies Inc 2023. 1742-0723

Patents
