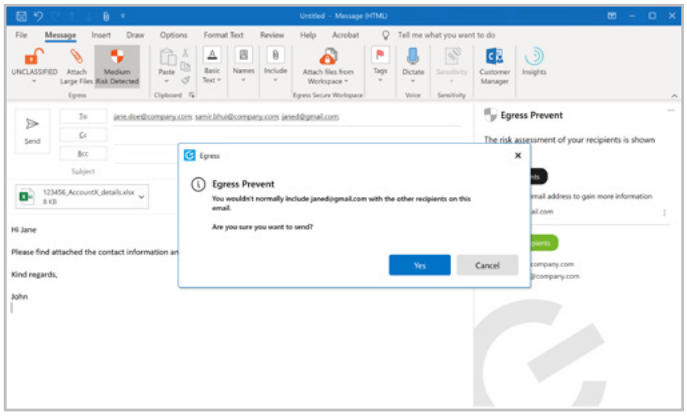
egress

Contextual machine learning in action

Removing **human activated threats** to email security

Digital connectivity has unleashed a 24/7/365 culture where employees not only face constant time pressures but also find themselves working around the clock. Rushed or simply fatigued, workers are accidentally sending emails to the wrong people or with the wrong content, or even clicking on links in harmful phishing attacks. And it's leading to very expensive security breaches.

Standard Data Loss Prevention (DLP) technologies can no longer keep pace with these human activated threats, with maintenance of static rules not only stealing multiple hours away from more productive workflows, but also paying no attention to user context or relationships.



Prevent security breaches

Spot and prevent human activated threats to security.

Gain time back

Eliminate multiple hours spent on maintaining DLP rules.

Avoid financial loss

Comply with global regulations and stay clear of heavy fines.

Boost business productivity

Keep employees working with minimal interruptions to workflows.

Using contextual machine learning to prevent security breaches

We combine DLP rules with contextual machine learning that interrogates and continuously learns an email profile to create context around a user's working patterns. This means we can then spot abnormal behaviour and prevent a security breach.

The technology ingests and then continuously analyses who users are emailing and when, message content (including the data inside an attachment), and their role within the business. We can then detect any deviation from the norm and instantaneously alert users in order to avoid a costly error.

Securing **1,000+** large organisations

The data science behind contextual machine learning

Underpinning our contextual machine learning is a series of algorithms that truly learn and empower users to prevent mistakes before they can happen. Bayesian inference models update statistical probabilities by continuously ingesting more user information as it becomes available, while graph databases map out and interrogate the strength of a user's relationships and how they interact. Working together, the tool allows you to more effectively minimise the risk of emails going to the wrong person or with the wrong content.

Top four features

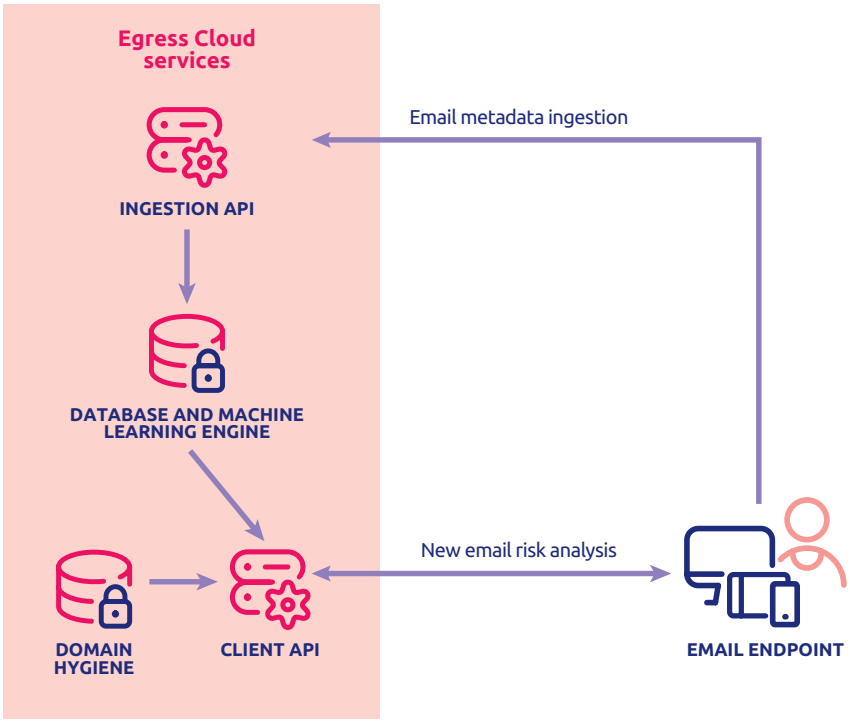
1. Statistical probability updates
2. Analysis of relationship cliques
3. Access time patterns
4. Detection of mis-spellings

"Egress is very transparent and straightforward to use, especially when compared with other solutions we evaluated."

DIRECTOR, INFORMATION SECURITY, MARTIN'S POINT HEALTH CARE

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

Furthermore, Gaussian mixture models allow the system to continuously learn a user's access time patterns, meaning the tool can spot unusual sending times for given recipients or message content that might ultimately lead to an accidental send. In addition, by deploying the Levenshtein Distance algorithm, we can detect words, email aliases and names that are within a degree of similarity but ultimately incorrect in order to detect a potential error and stop a breach of security.



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 | info@egress.com | 0844 800 0172 | @EgressSoftware