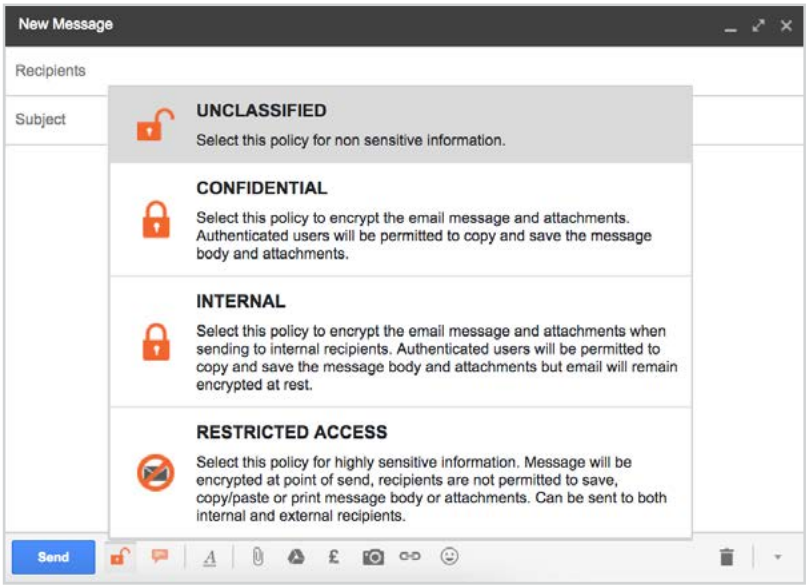
Egress and **G Suite**

The go-to security overlay for G Suite, **offering in-browser encryption** and **accidental send protection** for enhanced data privacy.

G Suite helps organizations increase efficiency and reduce costs, particularly as it enables users to access data and emails from various locations and across multiple devices. However, these working practices have led to an explosion of unstructured data, including information contained within emails, files and folders. Hosted environments can make it easier for this data to be shared across users and boundaries, which presents problems for organizations controlling and tracking sensitive information at a time of increased pressure from regulatory requirements. Egress addresses these concerns to help organizations manage risk and increase privacy in Google apps.



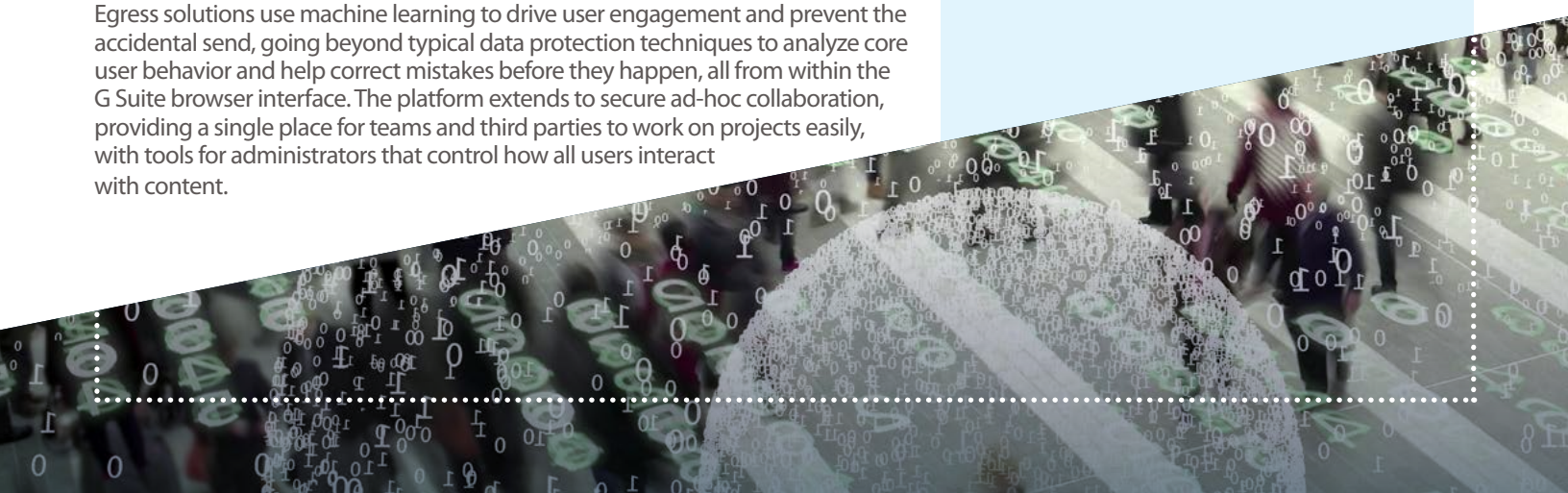
A data privacy and risk management platform

The Egress platform provides a comprehensive security overlay to G Suite, including message-level email encryption directly from the browser. In addition, configurable DLP policies can help users stay productive while working securely, reducing risk when sharing sensitive information.

Egress solutions use machine learning to drive user engagement and prevent the accidental send, going beyond typical data protection techniques to analyze core user behavior and help correct mistakes before they happen, all from within the G Suite browser interface. The platform extends to secure ad-hoc collaboration, providing a single place for teams and third parties to work on projects easily, with tools for administrators that control how all users interact with content.

How does Egress provide secure cloud enablement?

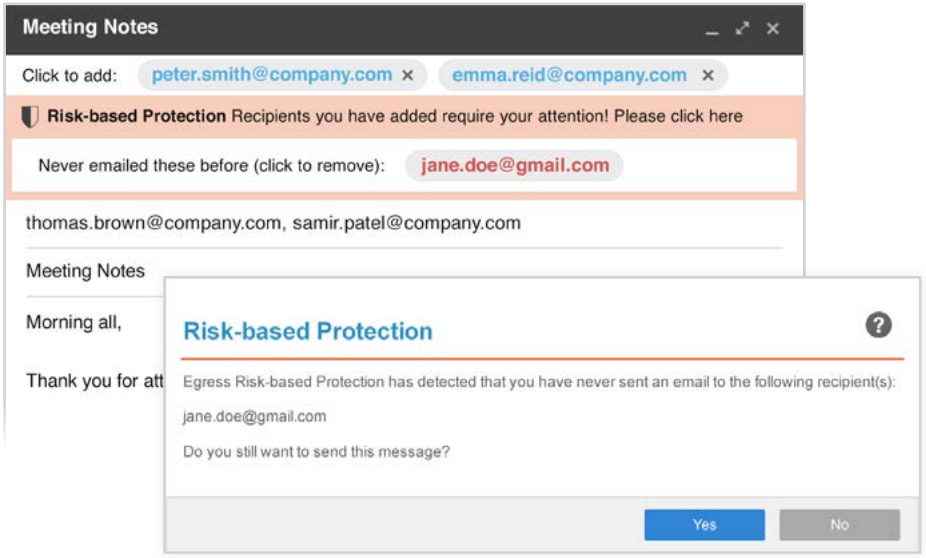
- Cloud migration presents challenges for data security, residency and collaboration
- The majority of data breaches are caused by human error when handling unstructured data such as emails and files
- The Egress platform provides security and auditing for the unstructured data created and shared within G Suite environments
- Egress manages risk by understanding and classifying data and preventing users from sharing information in error
- Putting users at the center, Egress creates a safety net for mistakes while encouraging productive working
- Advanced data privacy is achieved with message-level encryption and secure collaboration, with full control over users' actions
- Encryption at rest and comprehensive data analytics help meet regulatory requirements



Enabling security and compliance in the cloud

When moving to G Suite, many organizations have reasonable concerns around where data resides, as well as how they can effectively control access and manage risk to sensitive data without disrupting workflows. Data residency rules may also require data to be kept within specific geographical boundaries. Cloud services providers often store data in data centers across the globe, moving between data centers and potentially breaking data residency laws. The Egress platform can ensure that cleartext data never leaves borders and that data is encrypted before it is sent to the cloud.

Egress also enables compliance with regulations like the EU GDPR and CCPA, providing a fine-grained view of all the data an organization holds. Advanced data retention and disposal, efficient mechanisms for responding to data requests, detailed analytics and discovery all include the ability to search across and manage encrypted content. Auditing of all user activity and data transfer provides a complete view of organizational data processing within G Suite environments.



Business impacts

By improving security and productivity, Egress enables organizations to realize the cost and efficiency benefits of G Suite. Email content and attachments can be encrypted in transit and at rest, with real-time message auditing and access revocation keeping users informed and in control. Efficient ad-hoc encrypted collaboration and user engagement tools mean unstructured data is shared securely and with the correct people. Egress also minimizes the impact of deploying security technology on end-users by using machine learning to aid productivity. By designing tools that help users do their job, Egress reduces the pushback from staff that other technologies typically experience.

Highlighted features

- Help desk support for external recipients
- User engagement through machine learning
- Real-time message audit by users and administrators
- Real-time revocation of messages by users and administrators
- Fine-grained data analytics for compliance
- Use of existing third-party DLP solutions
- End-to-end message encryption
- Secure large file transfer
- Discovery and search of encrypted messages
- Ad-hoc and secure file collaboration
- Data residency and security certifications

Visit www.egress.com for more features and information

Download the Egress Chrome add-in here.

About Egress

Egress takes a people-centric approach to data security – helping users receive, manage and share sensitive data securely to meet compliance requirements and drive business productivity. Using machine learning, Egress ensures information is protected relative to the risk of a data breach and reduces user friction to ensure smooth adoption.

info@egress.com
1-800-732-0746
@EgressSoftware
www.egress.com