



# A data privacy and risk management platform

Put people at the centre to **reduce risk when sharing unstructured data.**

Factors such as modern working practices, digital transformation and migration to the cloud have resulted in over 80% of enterprise data being considered 'unstructured', including information within emails, folders and files. To date, organisations have struggled to classify, control and track this data as it is stored and shared across users and boundaries, often leading to breaches caused by human error at a time of increased pressure from regulatory requirements. To solve the problem, the Egress platform thinks differently, putting the user in the centre of a suite of privacy and risk management tools driven by intelligent, self-learning software.

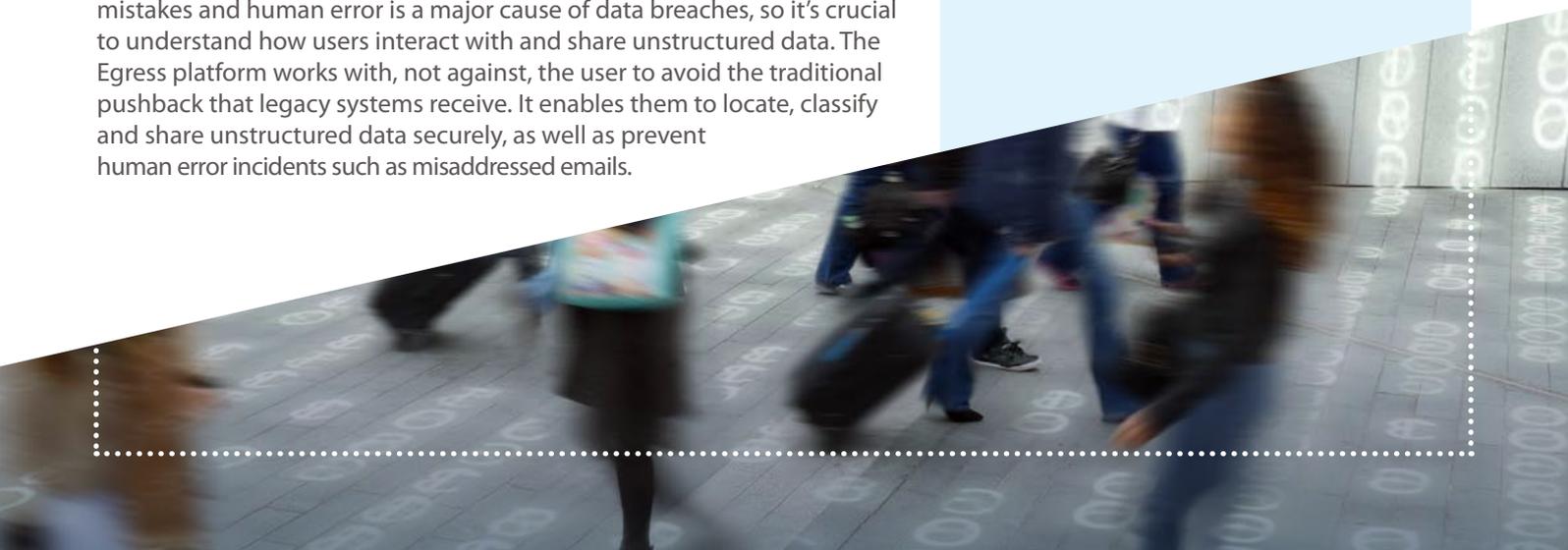


## Put the user at the centre

Technologies and the ways we consume them are always evolving. Even so, users are the constant across all information systems and technology, so comprehensive data security needs to surround the user with the tools they need to protect sensitive information. People are prone to mistakes and human error is a major cause of data breaches, so it's crucial to understand how users interact with and share unstructured data. The Egress platform works with, not against, the user to avoid the traditional pushback that legacy systems receive. It enables them to locate, classify and share unstructured data securely, as well as prevent human error incidents such as misaddressed emails.

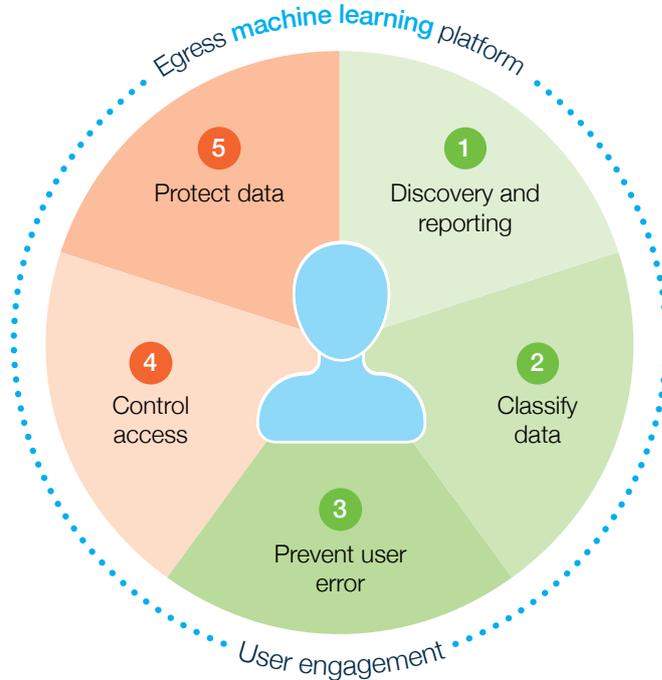
## What is the unstructured data problem?

- ✓ The unstructured data in files, emails and networks is difficult to secure and control
- ✓ The majority of data breaches are caused by human error when handling unstructured data
- ✓ Putting users at the centre, the Egress platform creates a safety net for these mistakes while encouraging productive working habits
- ✓ Risk is managed by understanding and classifying data and preventing users from sharing information in error
- ✓ Advanced data privacy is achieved with message-level encryption and secure collaboration, with full control over users' actions
- ✓ Comprehensive data analytics help meet regulatory requirements
- ✓ Cloud enablement is achieved by securing and auditing data in hosted environments



## A data privacy and risk management platform

Egress helps users and organisations manage risk by helping them understand the sensitive data they store and process, and then applying suitable classification to ensure it is always handled correctly. Where this information needs to be shared, the Egress platform makes sure it is only sent to the right people, and that necessary privacy measures are applied, including email and file protection, and by providing secure collaboration environments. User engagement and machine learning also drive usage and efficiency, offering bespoke advice and ensuring security is applied effectively, every time.



## Business impacts

As well as improving security, the Egress platform enables organisations to achieve cost and operational efficiency. Significant benefits can be seen from digitising processes such as postal and courier services, while machine learning and intelligence can help users make educated choices over who to include in their communications.

Egress also helps organisations to securely take advantage of the increased flexibility and reduced costs provided by cloud environments, including Office 365. 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 enables compliance with regulations like the EU GDPR, providing a fine-grained view of all the data an organisation 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, while auditing of all user activity and data transfer provides a complete view of organisational data processing.

## Highlighted features

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

Visit [www.egress.com](http://www.egress.com) for more features and information

## 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

0844 800 0172

@EgressSoftware

[www.egress.com](http://www.egress.com)