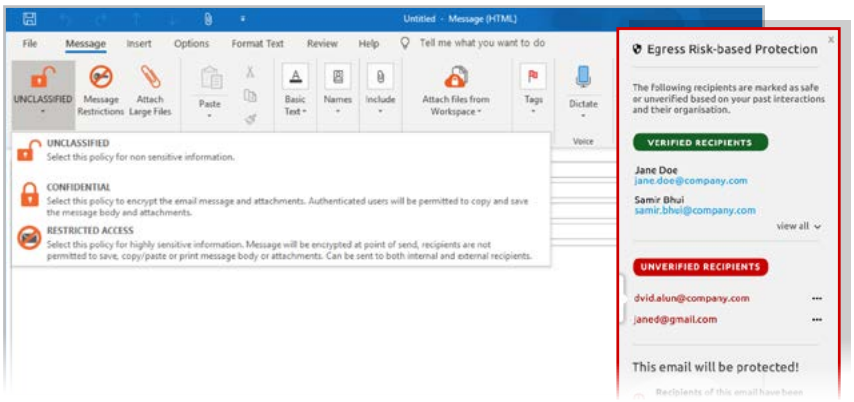
# Egress **Email Protection**

## The complete solution for **securing shared data** and managing modern risks

Many email protection solutions still rely on a one-size-fits-all approach to protecting content that doesn't consider the real-world risks of a data breach as information travels over untrusted networks to potentially untrusted recipients.

Egress helps organizations protect unstructured data to meet compliance requirements and drive business productivity by mitigating human error and malicious behavior. Using AI and machine learning, the Egress Email Protection platform empowers users to easily control and secure the data they share via email, with measurable benefits in data protection and end-user satisfaction. Using Email Protection, organizations can secure cloud email environments and enhance compliance with data protection regulations, as well as demonstrate measurable return on investment.



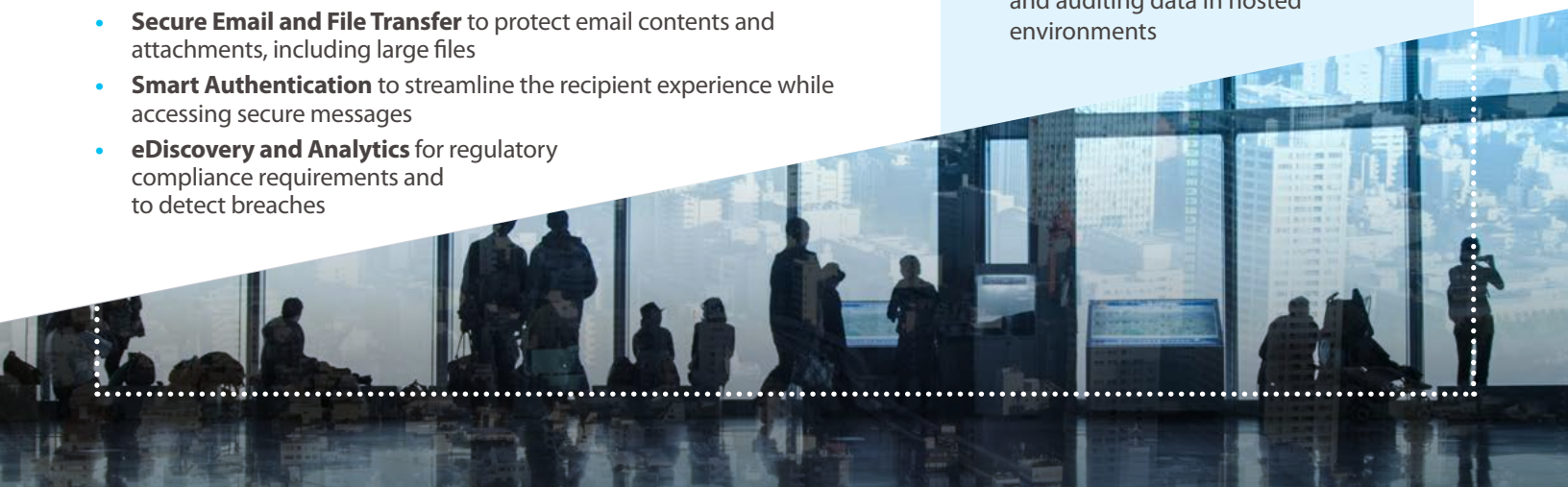

### The right level of protection for every email

The Email Protection platform uses AI and machine learning to automatically apply security to data that is proportional to the actual risk of a data breach. To create a holistic view of real-world risk, the platform analyzes multiple factors, including the sensitivity of the data and the recipient's profile. The Email Protection platform has five primary capabilities:

- **Email Classification** and automated DLP to prevent accidental or malicious release
- **Risk-based Protection** for preventing misaddressed emails and applying security in proportion to the risk
- **Secure Email and File Transfer** to protect email contents and attachments, including large files
- **Smart Authentication** to streamline the recipient experience while accessing secure messages
- **eDiscovery and Analytics** for regulatory compliance requirements and to detect breaches

### Business benefits

- Measurable decrease in the risk of a data breach by applying appropriate protection to an email and its attachments
- Proven improvement in compliance with data privacy and protection regulations
- Reduce the risk of accidental disclosure of sensitive information via email
- Reduce friction and increase user satisfaction in reading and replying to protected messages
- Improve security awareness and engagement to reduce the risk of end-users bypassing controls
- Enhanced utilization of existing third-party email protection solutions, including Microsoft O365 OME
- Create a safety net for mistakes while encouraging productive working habits
- Achieve advanced data privacy with message-level encryption and secure collaboration, with full control over users' actions
- Comprehensive data analytics to help meet regulatory requirements
- Achieve cloud enablement by securing and auditing data in hosted environments

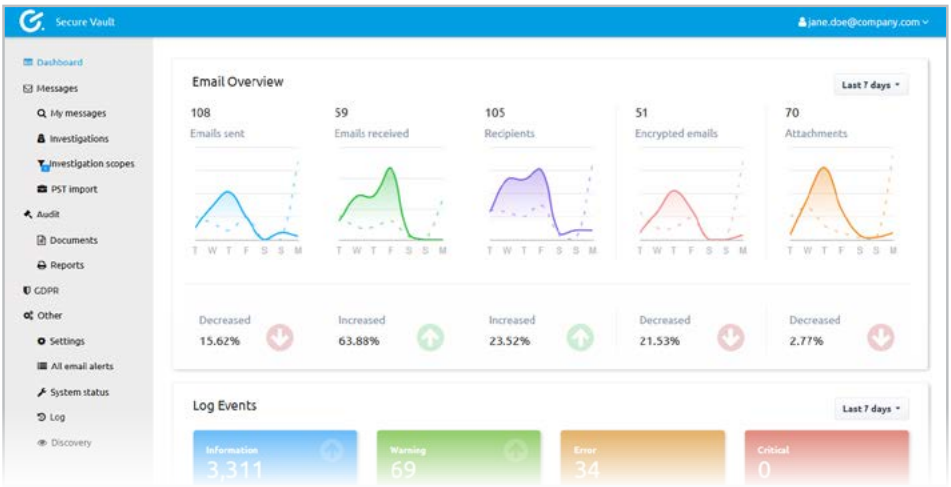


## Balancing security and usability to empower users and manage risk

Egress' commitment to people-centric data security starts with automated document classification and DLP tools that prevent accidental or malicious release of sensitive content.

Risk-based Protection then ensures that the right people receive sensitive data and calculates the risk of a breach to understand the right level of security to apply. This includes Egress message-level encryption, as well as third-party encryption solutions, including Microsoft OME.

Egress Smart Authentication then secures and streamlines the recipient experience, automatically configuring an appropriate level of authentication. Overcoming legacy authentication approaches for ad-hoc recipients that often result in user dissatisfaction and customer support issues, Smart Authentication balances risk with ease of use. A recipient accessing highly sensitive content from a high-risk domain, location or device may need to use MFA, while trusted internal users could achieve read-only access seamlessly.




## Intelligent analytics for improved security and compliance

eDiscovery and Analytics completes the holistic email protection package by leveraging fine-grained reporting to build an organization-wide risk profile and enable delivery of targeted, effective security policies.

Many organizations have advanced use cases for compliance and data residency that require detailed reporting on user behaviour. At the same time, organizations often struggle to prove reductions in risk and improvements in compliance. By providing a fine-grained view of all the email data an organization holds, Egress enables compliance with regulations like GDPR, HIPAA, and the NYDFS Cybersecurity Regulation, etc. Admins can search and manage all emails, including Egress-encrypted content, to efficiently respond to data requests.

## Highlighted features

- End-to-end encryption of messages
- User engagement through machine learning
- Helpdesk support for external recipients
- Real-time message auditing for users and administrators
- Instant revocation of messages by users and administrators
- Fine-grained data analytics for compliance
- Use alongside existing third-party DLP solutions
- 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**

## 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**