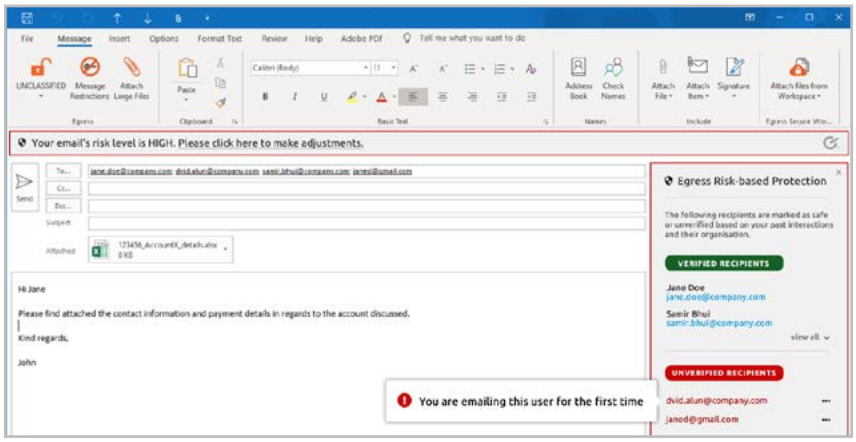
Egress **Risk-based Protection**

Empowering people to share sensitive data **with confidence**.

Despite improvements in usability and key management security, outbound email protection solutions typically still take a one-size-fits-all approach to securing data, through static DLP rules or end-user actions like encrypting emails at the desktop. However, these methods often don't take into consideration real-world risks to data as it travels over untrusted networks to potentially untrusted recipients, nor do they consider human error and malicious behavior. Ultimately, this makes it difficult to avoid data breaches and demonstrate compliance with rigorous data protection regulations, such as GDPR, HIPAA, and the NYDFS Cybersecurity Regulation.

Using AI and machine learning, Egress Risk-based Protection analyzes the sensitivity of data and applies protection proportional to the risk of sharing it.



Intelligent email security for real-world risks

Most email protection systems rely on senders to either manually apply protection based on their best judgment or rely on static rule-based DLP systems. However, Risk-based Protection uses machine learning and AI to answer the following questions and determine the actual risk of a data breach:

- Is the content being sent to the right person?
- What is the security profile of the recipient's domain and is there a previous history of interaction to establish 'normal' behavior patterns?
- Has the sender communicated this type of content with recipients before and what risks do their normal systems of access present?

Risk-based Protection then couples these risk factors with the sensitivity of the data being shared to ensure the appropriate type and level of protection is applied.

Benefits

- Ensure the right level of protection is applied to sensitive data to reduce the risk of a data breach
- Reduce the risk of accidental disclosure of sensitive information via email by correcting wrong recipients and mistyped email addresses
- Improve compliance with complex data privacy and protection regulations by ensuring appropriate protection of sensitive data
- Achieve a balance between security and usability to reduce friction in secure communications
- Improve security awareness and user engagement to reduce the risk of users bypassing security controls
- Enhance the utilization of existing third-party email protection solutions, including Microsoft O365 OME, Voltage, Zix, Virtru, etc.
- Auto-encrypt emails to other Egress customers to increase security without compromising on usability
- Quantifiably prove increased compliance with data privacy regulations through analytics and reporting tools

Quantifying risk for measurable compliance

Risk-based Protection provides administrators with insight reports into organizational risk, complete with information about the types of sensitive data being shared internally and externally, and how effectively they are meeting relevant compliance requirements, such as GDPR and HIPAA. An interactive timeline also demonstrates how Risk-based Protection has reduced instances of insecure data sharing to potentially unknown systems. This information cumulatively results in an improved compliance posture, data breach mitigation and demonstrable ROI for email security investments.

Automated risk-based assessments

Egress applies its machine learning and graph database technology to analyze risk factors and apply dynamic protection based on risk assessments in three areas

Automated risk assessment

1. Recipient domain

- Domain authenticity
- DKIM / SPF
- Historical analysis of secure communications with domain

2. Sender history

- History of communications with sender, including all recipients emailed previously

3. Recipient information

- History of communications with recipient
- Geographic and system information about data access

Dynamic protection

Protection against email misdelivery

Able to spot and provide guidance on wrong recipients

Quantifiable risk assessment

Provides numeric risk score within email client

Dynamically applied security

Based on computed risk scores, solution dynamically applies appropriate protection, including Egress, TLS, Microsoft O365 OME, Voltage, Zix, Cisco, Virtru, etc.

Analytics and reporting for compliance

- Statistics on number of incorrect recipients added to emails
- Information about the types of sensitive data shared with internal and external domains
- Detailed reporting on compliance with regulations such as HIPAA and NYDFS
- Timeline showing reduction of insecure sharing of sensitive data, especially with external domains

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