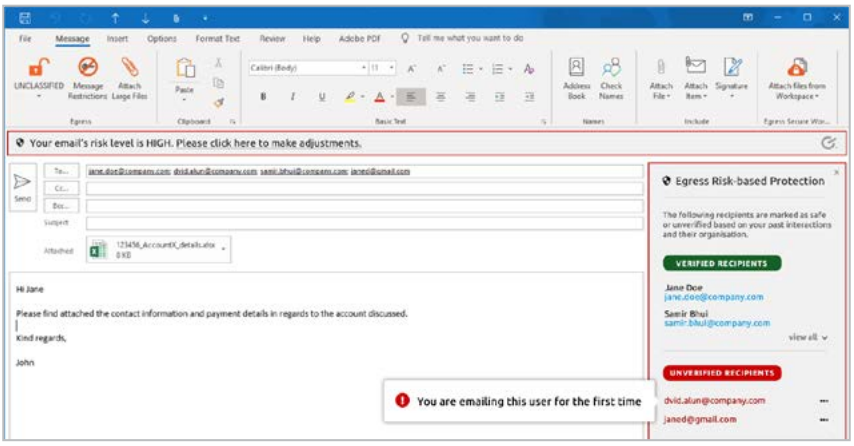
Egress Risk-based Protection **Proof of Value**

A simple way to assess how many **email sending mistakes** and potential **data breaches** happen across your organization.

What is Egress Risk-based Protection?

Email remains the single most important communication tool for all organizations. However, it's also one of the greatest data security risks—with staff accidentally or intentionally sending sensitive data to the wrong person. Egress Risk-based Protection solves this problem— safeguarding against the mis-sending of emails and including their attachments.



What's involved in the Egress Risk-based Protection Proof of Value?

The Egress Risk-based Protection Proof of Value (POV) enables organizations to test drive the solution's capabilities to proactively detect mistakes before emails are sent to the wrong recipient. Egress applies its proprietary machine learning technology to users' inboxes to build a model of email communications. It then advises on email sends— warning end-users about potential recipient errors.

The Egress Risk-based Protection POV helps organizations:

- Assess the benefits of Egress Threat Protection without any infrastructure or capital investment
- Quantify the risk of accidental email sends and gain insight into human error behavior patterns
- Build a business case for management to protect against the accidental sends of email through enhanced policies, processes and technology investments

Key benefits

- Prevent data breaches caused by staff sending sensitive emails, including their attachments, to the wrong person
- Help employees make good decisions when using email and sharing sensitive data
- Meet regulatory compliance requirements
- Easy to use with no training required
- Intelligent security with low management costs through machine learning
- Minimal disruption to staff through seamless integration with desktop and mobile clients

Trial the solution to see the benefits and use reports to build a business case for investing in Egress Risk-based Protection.

The POV is a simple three-step process:

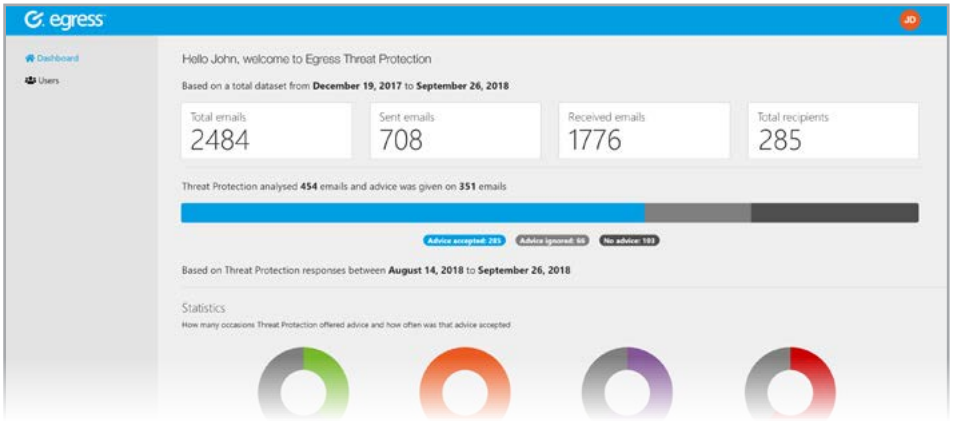
Step 1: The Egress Team provides end-users with the Egress Endpoint Client for Microsoft Outlook. This software observes the end-user's mailbox and sends information about historical end-user behavior to the secure Egress Cloud. There is no need to route emails to Egress through an SMTP Gateway or through Exchange journaling. Egress Risk-based Protection does not export Exchange logs or PST files.

Step 2: Egress Risk-based Protection applies social network and graph database technology to the end- user's emailing patterns. It then works with the Egress Endpoint Client in real time to alert the end-user about any misaddressed emails or misspelled email addresses.

Step 3: Business administrators as well as end-users can access a web interface to view detailed reports comparing the number of alerts provided by Egress Risk-based Protection to end-users, versus the number of alerts acted upon by end-users. Statistics are available on four types of alerts:

- Suggested additional recipients
- New recipient warning
- Misspelled recipients
- Wrong recipients

The report also provides high-level information on the emails that were ranked the highest security risk by Egress Risk-based Protection.



How Egress protects your data

Egress takes the utmost care while handling and processing customer information:

- Data collected to build networks of email sharing patterns is stored and processed in ISO 27001 accredited environments
- Customer data is encrypted at rest as well as in transit when it is supplied to Egress
- All environments set up as part of the POVs can only be accessed by authenticated and authorized employees with security clearance

Please reach out to the Egress Team with any additional questions.

Highlighted features

- Automatically alerts end-users to mistakes when sending emails, and warns administrators about potentially malicious intent
- Detects mistyped addresses similar to previous recipients or existing contacts
- Suggests additional recipients in the context of historical interactions
- Prevents mistakes such as using To/Cc instead of Bcc in mass emails
- Prompts end-users to confirm recipients before sending
- Integrates with any existing email platform, including MS Exchange, Office 365 and G Suite
- Works alongside classification and message-level encryption to recommend or force email encryption
- Integrates with the Egress platform, enabling seamless adoption for existing customers
- Multiple layers of protection when used in conjunction with message/attachment-level encryption, including instantly revoking access

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