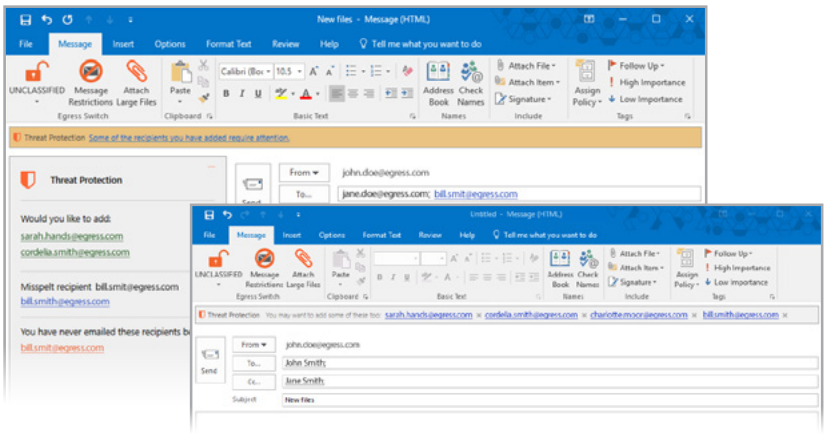
The Egress Threat Protection **Proof of Value**

A simple way to find out how many email mistakes and potential data breaches happen in your organisation.

What is Egress Threat Protection?

Email remains the single most important communication tool for all organisations as it is easy to use and enhances productivity. However, it also represents one of the largest data security risks with staff accidentally or intentionally sending sensitive data to the wrong person. Directly solving this problem, Egress Threat Protection safeguards against the mis-sending of email content and files.



What's involved in the Egress Threat Protection Proof of Value?

The Egress Threat Protection Proof of Value (POV) is a simple method for organisations to test drive the solution's capabilities to detect when emails are being sent to the wrong recipient. Egress applies its machine learning technology to an organisation's historic email to build a model of email communications and advise on future email sends, warning users about potential recipient errors before they hit send. This POV helps organisations:

- Quantify the risk of accidental email sends and gain insight into human error behaviour patterns
- Assess the benefits of Egress Threat Protection without any infrastructure or capital costs
- Build a business case for senior management to enhance policies, processes and potential technology investments to protect against the accidental send of emails

Benefits

- Prevent data breaches caused by staff sending sensitive emails and attachments to the wrong person
- Help employees make good decisions when using email and sharing sensitive data
- Meet compliance requirements, including under the EU GDPR
- Easy to use with no training required
- Prove diligence to stakeholders and regulatory bodies with complete email risk management
- Self-improving machine learning technology ensures low administrative overheads
- Total integration and simple interface ensure minimal disruption to staff
- Trial the solution to see the benefits and use data to build a business case

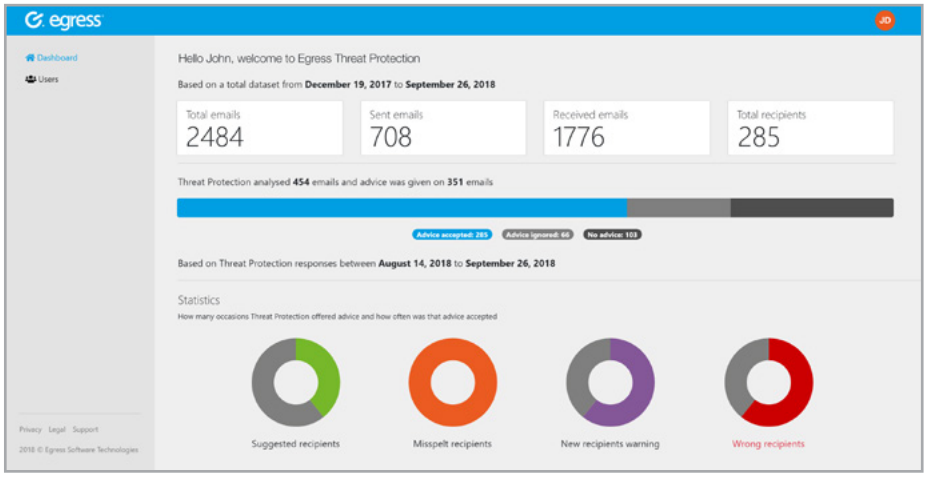
How can your organisation participate in the POV?

Participating in an Egress Threat Protection POV is a simple three-step process:

Step 1: The Egress Team provides participants in the POV with the Egress Endpoint Client for Microsoft Outlook. This software iterates through the end user's mailbox and sends information about historical user behaviour to the secure Egress Cloud. There are no requirements to route emails to Egress through an SMTP Gateway or through Exchange journaling. There are also no requirements to export Exchange logs or PST files.

Step 2: The Threat Protection machine learning engine hosted in the secure Egress Cloud applies social network and graph database technology to the end user's email information. It then works with the Egress Endpoint Client in real time to alert the user about any misaddressed emails or misspelt 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 the Egress system to end users versus the number of alerts accepted by end users. These statistics are available on the four types of alerts currently supported by the system, including: 'Suggested Recipients', 'Misspelt Recipients', 'New Recipient Warning' and 'Wrong Recipients'. The report also provides high-level information on the emails that were rated the highest by Egress Threat Protection.



Will the data provided for this POV be safe with Egress?

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 these POVs can only be accessed by authenticated and authorised employees with security clearance

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

Highlighted features

- Automatically alerts 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
- Avoid mistakes such as using To / Cc instead of Bcc in mass emails
- 'Send Validation' feature prompts user confirmation of recipients before sending
- Self-learn in discovery mode or ingest content via the Egress Desktop Client
- 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 into existing Egress apps enabling seamless adoption for existing customers
- Multiple layers of protection when used in conjunction with message / attachment-level encryption, including instantly revoking access

Visit www.egress.com for more features and information

About Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of privacy and risk management services designed to manage and protect unstructured data in a seamless user experience. The Egress platform leverages machine learning-led policy management, encryption and discovery to enable end-users to share and collaborate securely, while maintaining compliance and reducing the risk of loss.

CESG Certified Product
Foundation Grade
DGEE378428688-1104

Common Criteria

bsi. ISO/IEC 27001 Information Security Management

info@egress.com
0844 800 0172
@EgressSoftware
www.egress.com