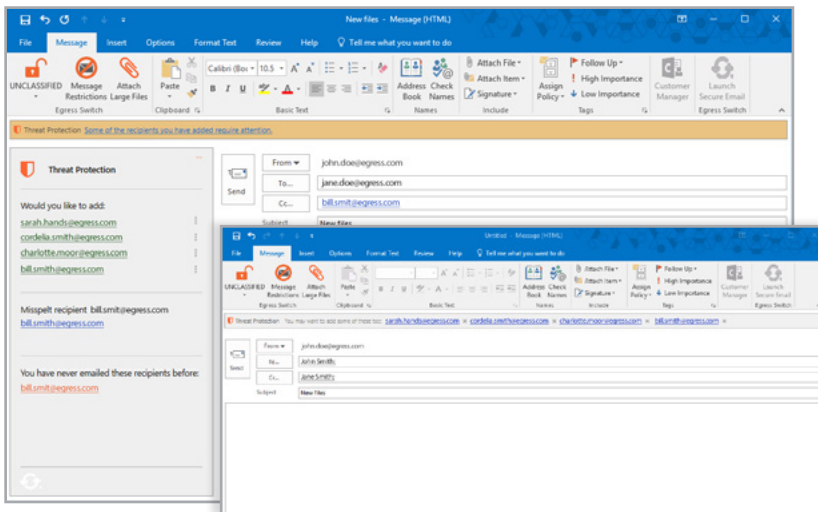




# Egress Switch Threat Protection

Stop users **accidentally sending** emails to the **wrong people and prevent a data breach** before it happens.

Email remains the single most important communication tool for all organisations. It is easy to use, immediately effective and makes staff highly efficient in what they do. Yet it also represents one of the largest data security risks: staff accidentally or intentionally sending sensitive content via email to the wrong person. Directly solving this problem, Egress Switch Threat Protection safeguards against the mis-sending of email content and files.



## Stop emails being sent to the wrong people

Everyone has experienced the sinking feeling that comes with accidentally sending an email to the wrong person. Regularly caused by similarities in recipient names or relying on autocomplete, it is especially common with emails to multiple recipients. A data breach of this kind can be devastating to any organisation. Switch Threat Protection uses trends and historic email conversations combined with contextual awareness to build patterns and relationships that can predict a potential breach. In addition, by learning from users' sharing patterns it can help by suggesting additional recipients that you normally share with, as well as reminding staff to use Bcc instead of To / Cc in mass emails.

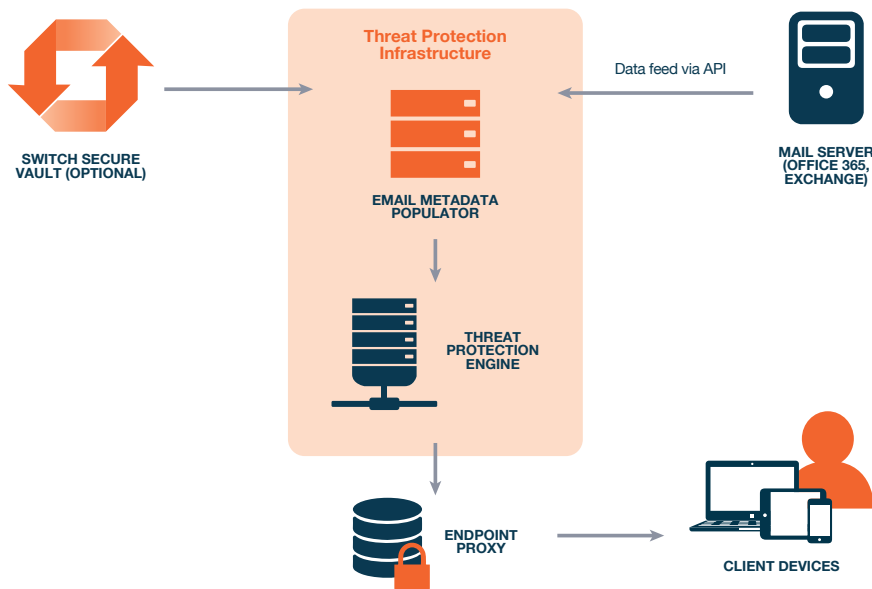
## Benefits

- ✓ 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 and the Data Protection Act
- ✓ Easy to use with no training required
- ✓ Integrates into existing infrastructure, including Exchange and Office 365 environments
- ✓ Understand in detail how employees share data, and tailor security policy to fit
- ✓ Prove diligence to stakeholders and regulatory bodies with complete email risk management
- ✓ Self-improving machine learning technology means low administrative overheads
- ✓ Total integration and simple interface ensures minimal disruption to staff



## Pre-empt data breaches and maintain compliance

With stringent data protection rules and significantly large fines under the EU General Data Protection Regulation (GDPR), no organisation can risk the legal issues, financial penalties and reputational damage caused by a data breach. Employees at all levels and in all departments can access email, and a large proportion will also handle personally or commercially sensitive information, which can lead to a compliance issue under the GDPR if this information is shared in error. Switch Threat Protection solves this by helping users make correct decisions about data security, alerting them to accidental data breaches, and encouraging them to use email encryption and classification to protect sensitive content.



## Prevent mistakes in O365, with integrated email encryption and classification

Alongside Switch Secure Email and File Transfer, Switch Threat Protection works with any email platform, including MS Office 365, meaning organisations can benefit from cloud email services without compromising data security. Additionally, as data owners, organisations will need to protect and control personally and commercially sensitive information, even when it's sent to the right person. Switch Threat Protection works alongside Switch DLP and message-level encryption technology to provide integrated email encryption, protecting content in transit and at rest based on sensitive keywords, filetypes, recipients and data classification. This includes full auditing of completed and attempted email sends, and the ability to revoke access to emails at any time, even after opening.

## Highlighted features

- ✓ Automatically alerts users to mistakes when sending emails and warns administrators about potentially malicious intent
- ✓ Detect mistyped addresses similar to previous recipients or existing contacts
- ✓ Suggest additional recipients in the context of historical interactions
- ✓ Avoid accidental send such as To/Cc instead of Bcc in mass emails
- ✓ Self-learn in discovery mode or feed historical email through processing engine for instant protection
- ✓ Integrates with any existing email platform, including MS Exchange and Office 365
- ✓ Works alongside classification and message-level encryption to recommend or force email encryption
- ✓ Integrates into existing Switch 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](http://www.egress.com) for more features and information

## About Egress Software Technologies Ltd

Egress Software Technologies is the leading provider of data security services designed to protect shared data using a single platform: Egress Switch. The Switch platform is made up of highly integrated and flexible service lines. These award-winning solutions include email and document classification, software to prevent emails being sent in error, NCSC-certified email and file encryption, secure managed file transfer, secure online collaboration, and secure archiving.



info@egress.com

0844 800 0172

@EgressSwitch

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