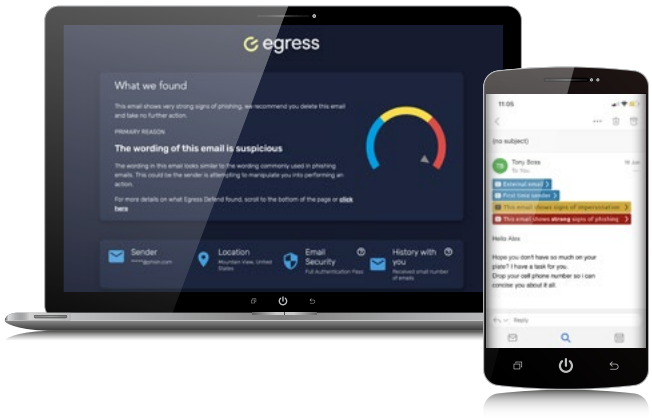
Egress Defend

Stop **inbound email attacks** and empower employees to become **security advocates**

Phishing is the entrance point in the kill chain that external agents use to gain access to your critical information. More attackers are now able to circumvent traditional email security solutions by exploiting our chief vulnerability: human behaviour.

Egress Defend has been shaped by GCHQ to provide advanced detection capabilities that stop phishing early. Armed with intelligent technologies that evaluate context and relationships, our solution prevents more inbound cyber threats, releases key resources to focus on other threats, and empowers your employees to become cyber advocates who can identify future breaches.



Stop phishing attacks

Stronger detection emulates a cyber expert when analysing a phishing email.

Reduce admin overheads

Free up administrator bandwidth to focus on other critical work.

Empower employees

Clear and intuitive banners offer in the moment user learning.

Avoid alert fatigue

Minimise the risk of users ignoring warnings altogether.

Emulate cyber expertise to strengthen your defence

Egress Defend reverse engineers phishing emails, breaking down and analysing all the sub-components for suspicious elements before delivering a final verdict. The technology investigates the email using zero trust models and evaluating content and context, looking at both positive and negative features in order to identify suspicious behaviour.

This allows the technology to detect the techniques used to deceive employees rather than the deceit itself, increasing the robustness and resilience of Egress Defend in the face of new and sophisticated attacks.

Securing **7 million** users every day

Empowering users to become security advocates

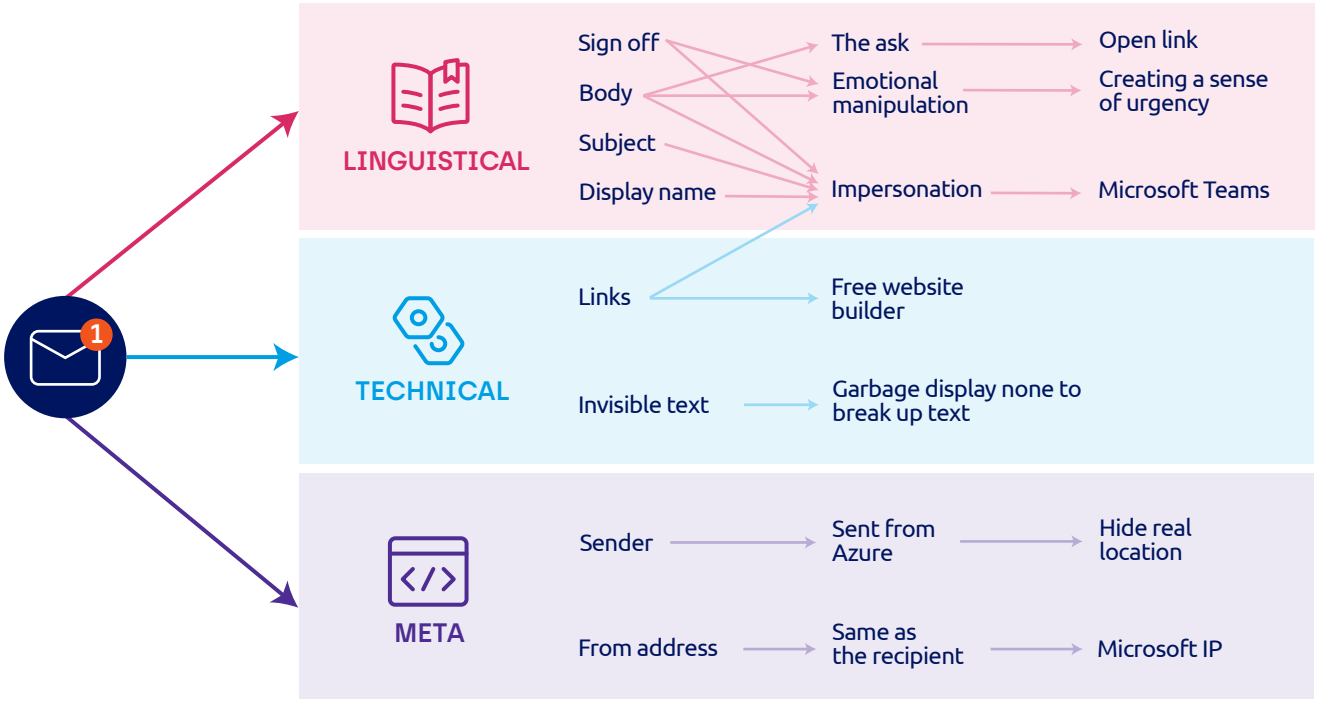
Egress Defend empowers users to become your first line of defence. An intuitive interface uses a clear and obvious heat-based warning system that immediately alerts them to a threat without distracting them from their workflow. The technology also explains why the phishing email is dangerous in plain human language, offering active learning for the user that reduces reliance on time-consuming and costly training programs.

In addition, Egress Defend provides a low banner percentage, in turn gaining the trust of the user and removing the risk of banner fatigue.

Top features

1. Behavioural and linguistic analytics
2. Social graphing technologies
3. Real-time user warnings
4. Intuitive display panels
5. Additional prompt and alerts

Visit **www.egress.com** for more features.



For more information please contact your account manager or call 0203 987 9666

About Egress

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen.

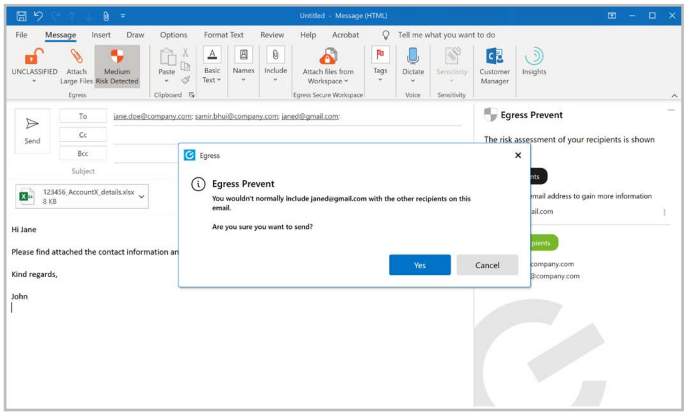
www.egress.com | info@egress.com | 0203 987 9666 | @EgressSoftware

Egress Prevent

Stop accidental and intentional email data breaches before they happen.

The nature of email security has changed. Today's digitally connected world and a 24/7/365 working culture means time-pressured employees are making more mistakes and putting sensitive data at risk. Emails to the wrong recipient(s) or containing the wrong content and attachments, phishing victims, and malicious exfiltration are just some of the human-activated threats that cause the majority of security breaches.

We use contextual machine learning and advanced DLP to spot when employees are about to accidentally or intentionally leak data, empowering organisations to:



Prevent email data breaches

Send the right information to the right recipient(s), including personal data.

Comply with global data privacy regulations

Ensure employees' use of email is compliant with regulations including GDPR.

Enhance business efficiency

Prevent mistakes on the go with full mobile and OWA support.

Minimise human error

Avoid user fatigue with seamless interaction and user experience.

Using contextual machine learning to account for real-world risks

Employees' behaviour is unpredictable, meaning traditional, static approaches to data loss prevention (DLP) are unable to dynamically prevent breaches. Instead, we use contextual machine learning to inspect and continuously learn from a sender's behaviour - including who they're emailing, when, and with what content - so we can detect abnormal behaviour and prevent breaches of security before they happen. Our intelligent approach also minimises employee interruptions, so they're not frustrated with an avalanche of prompts.

Securing **1,000+** large organisations

Granted: EP3533184, US10911556, US11223695, GB2681188, US10911417, GB2581190, GB2581189, US11218379
Pending: EP 20186594.6, AUS 202019455, EP20703077.6, Singapore 11202108481X, AUS 2020218635, EP 20708550.7, Singapore 11202108482V, US16/749,580, AUS 2020219929, EP20708551.5, Singapore 11202108489T, US16/749,606, US17/535/135

Quantifying risk for measurable compliance

We provide administrators with quick, on-demand reporting that tracks sensitive data and pinpoints any threats to regulatory compliance. Our granular insights ensure you can detect at-risk employees who require frequent help with misdirected emails or might be attempting to intentionally exfiltrate sensitive information.

In addition, our interactive timeline highlights where you have reduced instances of insecure data sharing to potentially unknown systems, improving compliance posture and demonstrating tangible ROI.

Detecting abnormal behaviour

We use contextual machine learning to spot abnormal behaviour that puts data at risk and apply dynamic protection by analysing four key areas:

Top features

1. Recipient and domain analysis
2. Email subject, body and attachment analysis
3. Full mobile and OWA support
4. Integration with MS Outlook
5. Comprehensive reporting

Visit **www.egress.com** for more features.

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 in the past

3. Recipient information

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

4. Content analysis

- Subject line and message body analysis
- Assessment of attachment name / type
- Analysis of data inside attachments

Dynamic protection

Protection against misdirected emails

Able to spot and provide guidance on incorrect recipients

Quantifiable risk assessment

Provides numeric risk score within email client

Dynamically applied security

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

Protection of sensitive information

Safeguards against the sharing of sensitive data with unauthorised recipients

For more information please contact your account manager or call 0203 987 9666

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organisation faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

CESG Certified Product Foundation Grade DGEE378428688-1104 | bsi. ISO/IEC 27001 Information Security Management | Common Criteria | NATO OTAN

www.egress.com | info@egress.com | EgressSoftware

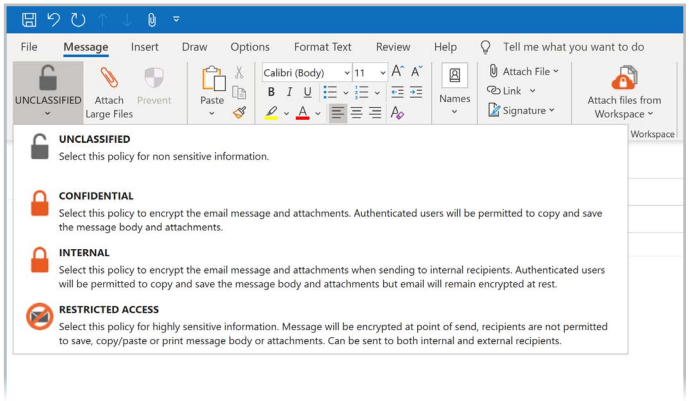
egress

Egress Protect

Intelligently secure emails and large files with the appropriate level of security.

Every employee has access to email. However, organisations still struggle to protect the sensitive data they share both internally and externally.

We offer easy-to-use, flexible email and file encryption that intelligently applies security in proportion to the risk of a data breach. As well as encrypting message content and attachments, we provide total control over shared information in real time, including email recall, audits of user actions, and message restrictions to prevent mishandling - enabling organisations to:



Secure data shared by email

Encrypt personally and commercially sensitive data, including using multi-factor authentication.

Encourage user adoption

Share sensitive information from Office 365 and Outlook, and when using mobile devices.

Stay in control

Maintain compliance with detailed audit logs, message restrictions, and real-time email recall.

End-to-end secure communication

It's free for recipients to communicate with your full subscribers.

Government and industry-certified data security

We provide government and industry-certified security and authentication for protecting email content and attachments, including large files, in transit and at rest. We also support multi-factor authentication, customisable policy control, and access to secure information via mobile devices.

Users stay in control of their information after it has been shared by recalling emails, preventing actions such as download and copy / paste, and viewing audit logs. We are certified under CCPA, Common Criteria and ISO 27001:2013.

Securing **1,000+** large organisations

Granted: GB2450197, RE45,047, RE45,046, GB2470008, GB2505375

Avoiding recipient pushback through flexible authentication

Authentication doesn't need to painful. Our flexible authentication techniques support your recipient's requirements by offering a range of ways to authenticate. The secure Egress portal offers traditional security by requiring recipients sign into their complimentary Egress account, while our shared secrets technique expects recipients to enter a password or unique identifier only known to them and the sender. And with one-click access, users can allow trusted partners to access sensitive emails securely without even authenticating, in turn removing friction from the process and enhancing their experience.

"Without Egress, we would have had to buy at least five different systems to meet our information sharing requirements."

HEAD OF INFORMATION GOVERNANCE AND SECURITY, HCA HEALTHCARE

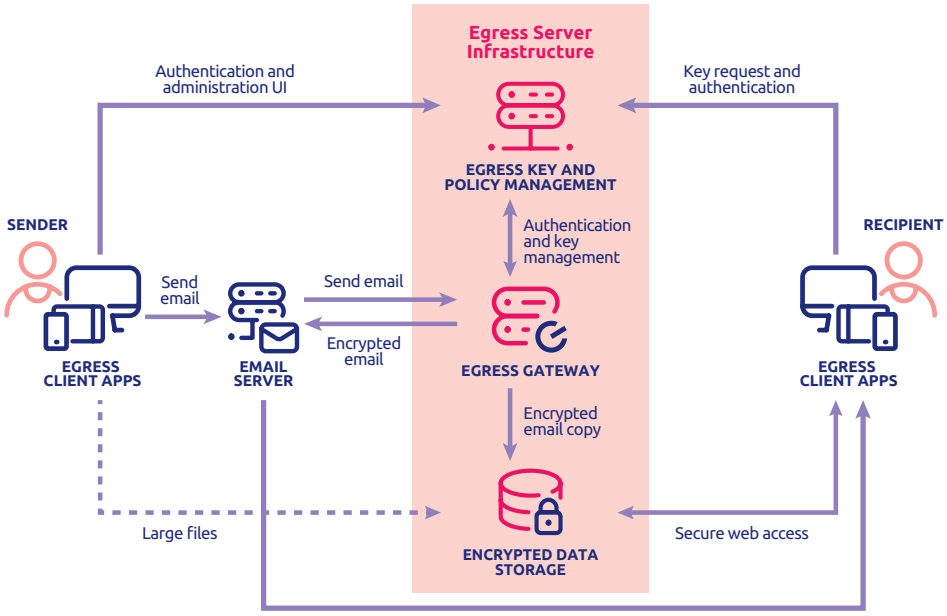
Top five features

1. AES-256 bit encryption secures data at rest and in transit
2. Email encrypted at the gateway and the desktop
3. Supports single sign-on via MS Active Directory using ADFS or other providers, such as SAML v2
4. Choice over data hosting
5. Flexible authentication removes recipient friction

Visit **www.egress.com** for more features.

Email encryption and file transfer made easy

We integrate with Microsoft Outlook and Office 365 to provide one-click email encryption, while our powerful mobile apps allow for easy and secure data sharing on the go. We also enable users to encrypt large files when shared via email, bypassing the usual Exchange / Exchange Online size limitations and removing reliance on less secure, free alternatives. Recipients can reply to and initiate secure emails and file transfers to Egress subscribers for free, keeping costs down and encouraging user uptake.



For more information please contact your account manager or call 0203 987 9666

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organisation faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

CESG Certified Product Foundation Grade DGEE378428688-1104 | bsi. ISO/IEC 27001 Information Security Management | Common Criteria | NATO OTAN

www.egress.com | info@egress.com | EgressSoftware