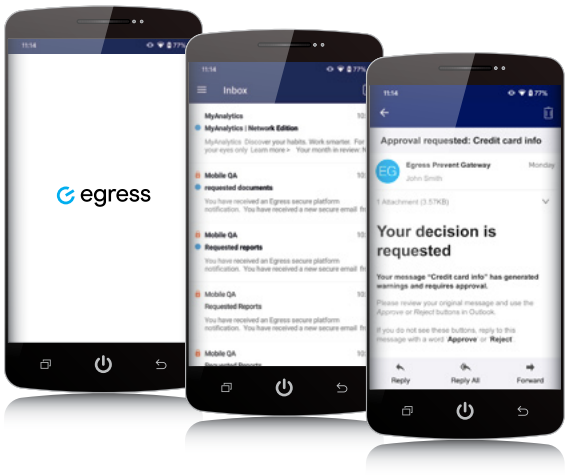
Prevent security breaches on the go

Intelligent email security **out of the office.**

Forty-nine per cent of business emails are now opened on a mobile device, while a further 33% are accessed via webmail (source: IBM). Although today's workforce has become increasingly remote, it is more connected than ever as employees respond to emails outside of business hours in a bid to get things done and meet tight deadlines.

While this offers great opportunities for businesses to be even more productive and achieve objectives faster, the risk of a security breach surges as fatigued employees working around the clock fail to spot a potentially expensive error.



Minimise human error

Send the right information to the right recipients from your mobile device.

Boost business efficiency

Keep productivity moving with with full mobile and OWA support.

Prevent email security breaches

Apply sophisticated approval mechanisms to keep data safe.

Avoid financial loss

Comply with global regulations and stay clear of heavy fines.

Using contextual machine learning to prevent security breaches on the go

Sending emails to the wrong recipient, sharing the wrong content and attachments, and falling prey to phishing emails are just some of the human-activated threats resulting in security breaches today. We provide contextual machine learning at your fingertips to inspect and continuously learn 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, wherever you are.

Securing **1,000+** large organisations

Eliminating the threat of disruption to productivity

Other solutions require emails sent on a mobile to be routed to their own cloud which, in the event of an outage, would completely cease all mobile email usage for employees. On top of that, there's also the risk of a malicious hacker accessing all sensitive emails should they end up infiltrating the cloud. Either would spell disaster for productivity.

Our cutting-edge solution deploys an arbitration mailbox at the Exchange level in order to keep sensitive data away from hacking attempts, minimise disruption to user workflows, and allow employees to send emails safely from OWA or their mobile device.

"Egress provided quick, great customer service and provided everything needed to get up and running"

EGRESS CUSTOMER REVIEW VIA G2 CROWD

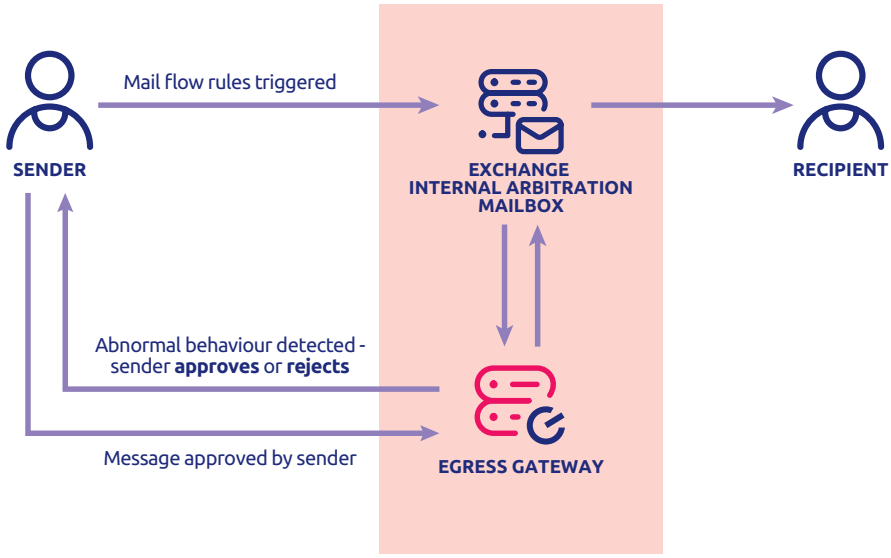
Top five features

1. Contextual machine learning
2. OWA and mobile support
3. Non-disruptive arbitration mailbox
4. Easy approve/reject functionality
5. iOS and Android-enabled

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

Simplicity and ease to avoid user fatigue

An intuitive mobile experience means that your business can keep pace with today's digital demands without ever worrying about employees sending emails to the wrong person or with the wrong content. If our contextual machine learning picks up abnormal behaviour, you receive a notification explaining why there might be a risk. You can then quickly approve or reject any potentially misdirected email or content on the spot, keeping the business moving and, importantly, removing the threat of a security breach.



For more information please contact your account manager or call 0844 800 0172

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 | 0844 800 0172 | @EgressSoftware