# Egress Intelligent Email Security for law firms
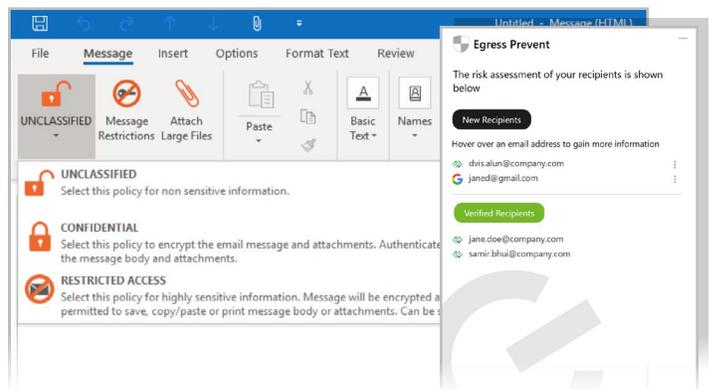
Human layer security that preserves **client confidentiality** , stops **sophisticated phishing attack**s and protects **privileged information**.

Law firms are under ever-increasing pressure from clients to protect confidential email communications with both internal and external recipients. On top of that, phishing attacks are becoming more sophisticated, with bad actors compromising legitimate supply chain partners in order to infiltrate your firm and steal money or data.

Firms need to act now to implement security technology that removes the risk of a breach. Our Intelligent Email Security platform combines linguistic analysis, supervised machine learning, and state-of-the-art encryption so that busy legal professionals can keep email data safe.

### ✓ Preserve client confidentiality
Send the right sensitive information to the right internal and external recipient(s).

### ✓ Keep sensitive data safe
Protect privileged email contents with accredited encryption.

### ✓ Stop phishing attacks
Stay safe from targeted and sophisticated email threats.

### ✓ Avoid reputational harm
Satisfy client requirements and make security a competitive advantage.

## Delivering end-to-end email security

Our Intelligent Email Security platform uses a combination of linguistic analysis, machine learning, and government-accredited encryption to detect sophisticated phishing attacks, prevent accidental or malicious data loss, and secure email communications. Our platform has three key modules:

- **Egress Defend** for stopping sophisticated phishing attacks
- **Egress Prevent** for sending the right email content to the right people
- **Egress Protect** for effectively securing sensitive emails and large files

Securing
**1,000+**
large organizations

## Stop accidental and malicious email data loss

Legal professionals are busy, often working long hours, which elevates the risk of a security incident. Our technology works by establishing a baseline of normal user email behavior, and then detects anomalous recipients and attachments in real-time. That way, you can avoid embarrassing and potentially costly email errors, and stop employees maliciously or negligently exfiltrating company data.

On top of that, we combine zero trust models with linguistic analysis to detect sophisticated phishing attacks that slip through traditional email security solutions and Secure Email Gateways.

### "We selected Egress so we could assure our clients their confidentiality wouldn't be breached by unauthorized access to privileged information."

HEAD OF INFORMATION GOVERNANCE AND SECURITY, GLOBAL LAW FIRM

## Top five features

| 1 | Contextual machine learning |
| 2 | Automated email protection |
| 3 | Full mobile support |
| 4 | TLS verification for recipient domains |
| 5 | Smart Authentication to reduce recipient friction |

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

## Security technology that's easy for lawyers and customers to use
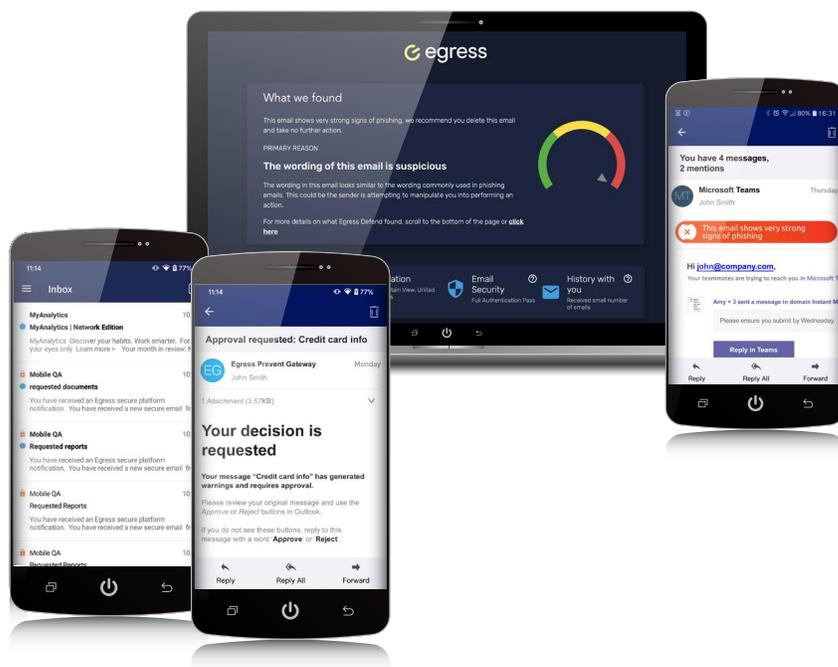
With machine learning algorithms that learn user behaviour, employees can spot wrong recipients and attachments in real-time without changing the way they work, while automated encryption seamlessly comes into effect with the presence of unique identifiers such as Case IDs.

One-click access then removes barriers by giving recipients instant access to encrypted emails without logging into a secure portal. In addition, our technology works on mobile, meaning busy employees can stay safe from phishing attacks, avoid data leaks, and keep data secure wherever they are.

## For more information please contact your account manager or call 1-800-732-0746

## 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 | 1-800-732-0746 | @EgressSoftware