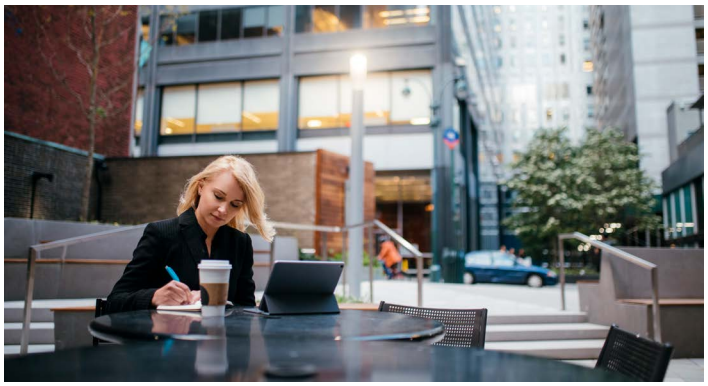
egress

Staying compliant with the SHIELD Act

Using Egress to **stay compliant**, **avoid financial penalties** and **steer clear of litigation**.

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act is the latest in an ongoing wave of new US data privacy regulations. It requires any organization owning or licensing private information of a New York resident to put in place technical and physical safeguards in order to protect that data.

With violations potentially costing hundreds of thousands of dollars in fines and associated legal costs, Egress provides the safeguards that your organization needs in order to remain compliant and stay clear of financial and reputational damage.



Keep sensitive data safe

Remove the risk of a costly security breach.

Safeguard ROI

Drive user adoption by making security easy.

Avoid financial loss

Stay clear of penalties, litigation, and reputational damage.

Boost business productivity

Avoid disruption to user workflows.

Removing the risk of email data loss

While inadvertent disclosure might not require notification of a breach in very specific, limited circumstances under the SHIELD Act, emails sent in error to the wrong person or with the wrong content have recently become the #1 cause of security breaches. **Egress Prevent** spots and fixes a potentially costly email data breach before it can happen by using contextual machine learning that deeply understand a user's role and working patterns so that we can spot abnormal behaviour and flag risk to the user in real-time.

Securing **1,000+** large organizations

Applying the appropriate level of protection as a critical safeguard

Egress Protect allows users to apply the appropriate level of encryption to email content, with different permissions and controls available depending on the level of sensitivity. With a seamless Outlook plug-in and dedicated mobile app, users can easily encrypt confidential information, edit classifications, and even revoke messages altogether in order to keep data safe.

Egress Prevent makes encryption even easier for users by analyzing content, including data inside attachments, and providing automated prompts that recommend or even enforce encryption when sensitivity is particularly high.

Top five features

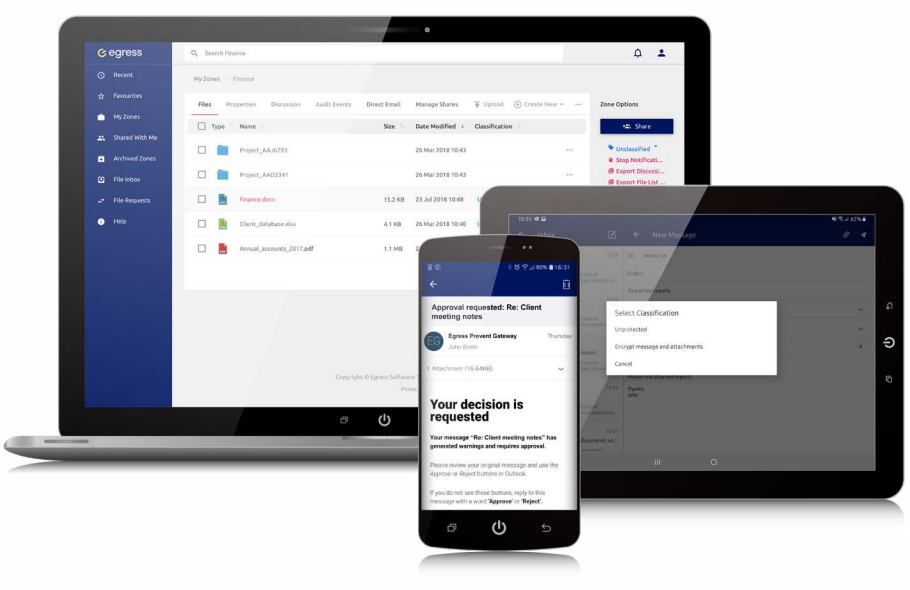
1. Contextual machine learning
2. In-depth attachment analysis
3. Easy-to-use, automated encryption
4. Granular user controls
5. Secure, segregated zones

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

Secure file sharing that keeps information safe from unauthorized users

The SHIELD Act obligates organizations to protect against unauthorized access to, or use of, private information. **Egress Secure Workspace** offers a government-certified, encrypted environment for teams to securely share sensitive files and collaborate on confidential content either internally or with external parties.

Enterprise-grade controls remove the risk of unauthorized access with restrictions on location, time of access, editing, downloading, and sharing keeping sensitive information locked within secure zones. In addition, detailed audit logs allow organizations to demonstrate compliance and avoid litigation costs, fines, and reputational damage.



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.

CESG Certified Product
Foundation Grade
DGEE37842868-1104

bsi. ISO/IEC 27001 Information Security Management

Common Criteria

NATO OTAN

www.egress.com | info@egress.com | 1-800-732-0746 | @EgressSoftware