**egress**®

Egress **Discovery and Classification**

Helping organizations **identify, understand and control** their unstructured data to **manage risk and prevent data breaches**.

Organizations need to understand where confidential data is held across their network, especially when it is in unstructured format such as in the emails, files and folders created by users in vast quantities and on an ad-hoc basis. This insight is crucial to comply with data protection legislation and prevent breaches. Egress Discovery and Classification provides automated document and email classification using integrated, intelligent DLP policies, and can prompt or force encryption when classified data is shared.
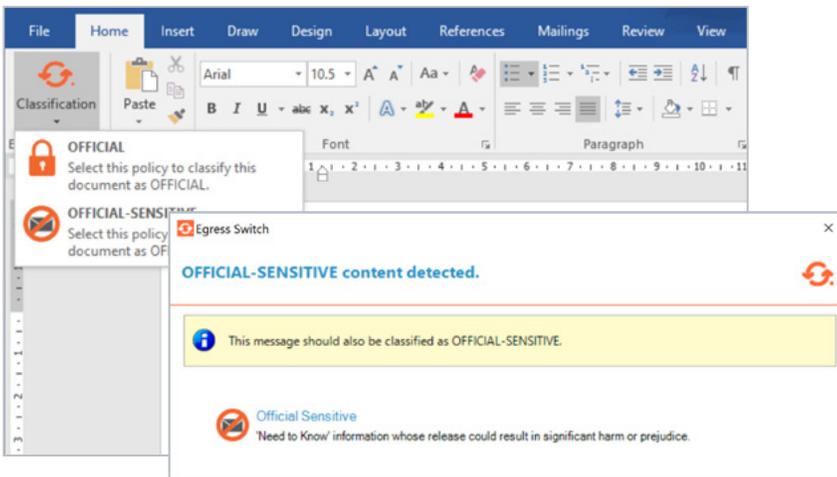

Improve organizational data security with document fingerprinting

Discovery and Classification adds metadata to documents. This document fingerprinting process helps users and organizations to audit content whenever it is shared, including when it is edited or the filename is changed. Additionally, integration with Egress Email and File Protection provides customizable policy-based encryption linked to document classification. For example, administrators can mandate the application of encryption if a user attempts to email an OFFICIAL-SENSITIVE document, or prevent the sending altogether if they are sharing internal documentation with an external domain.
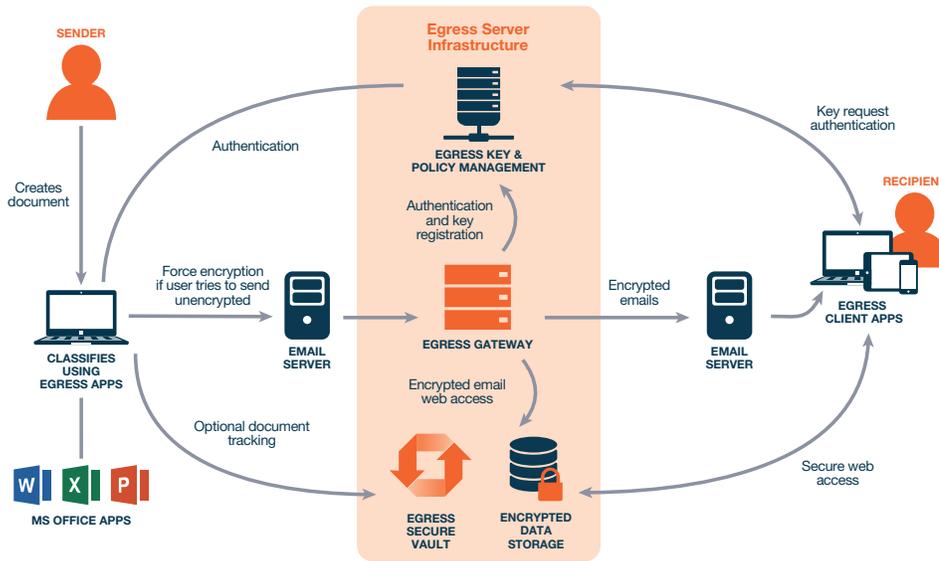
Benefits

- ✓ Understand and leverage organizational data, discovering how sensitive information is treated and promoting appropriate security processes

- ✓ Meet legislative and industry compliance requirements by keeping track of all data your organization holds

- ✓ Aid user education and promote data security awareness by encouraging the correct application of classification and encryption

- ✓ Make secure working more efficient with automated classification based on customizable keyword libraries

- ✓ Prevent data breaches by integrating classification with email encryption to reduce the risk of accidental send or data loss

- ✓ Change user behavior when creating, sharing and using sensitive content
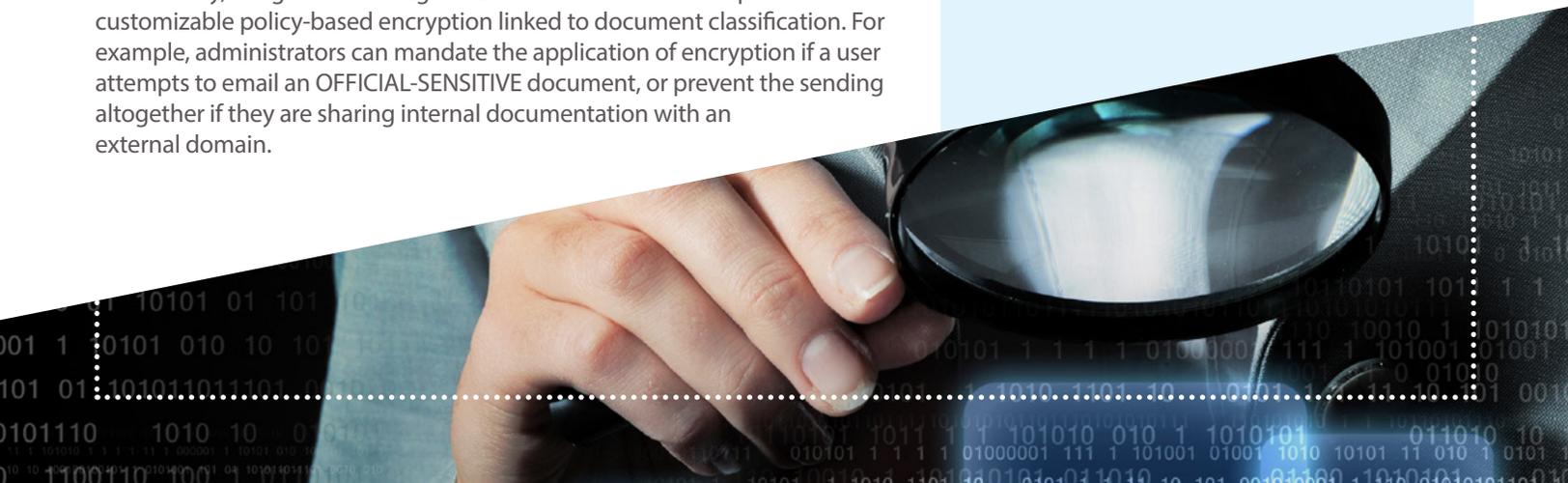
Customizable classification with integrated, policy-based management and DLP

The headers, footers and watermarks added to documents during classification are fully customizable, while the DLP triggers and keyword libraries can also be tailored to organizational requirements. Further, the dynamic, policy-based management of Discovery and Classification allows administrators to fine-tune the classification and encryption of data as users throughout the organization create, store and share this content.

SENDER

Creates document

Authentication

CLASSIFIES USING EGRESS APPS

Force encryption if user tries to send unencrypted

EMAIL SERVER

Optional document tracking

MS OFFICE APPS

Egress Server Infrastructure

EGRESS KEY & POLICY MANAGEMENT

Authentication and key registration

EGRESS GATEWAY

Encrypted email web access

EGRESS SECURE VAULT

ENCRYPTED DATA STORAGE

Encrypted emails

EMAIL SERVER

Key request authentication

RECIPIENT

EGRESS CLIENT APPS

Secure web access

Automation and effective user interaction for sensible data security

Discovery and Classification seamlessly integrates into Microsoft Office and Outlook to provide easy document classification within existing workflows. Automated prompts to apply classification and encryption also improve user education, aiding in-depth understanding of how to treat data of varying sensitivities. Administrators can easily manage the policies that dictate how users should classify different document types and then set up the prompts for appropriate security. Administrators can also view audit logs to get a detailed overview of user activity and identify how to improve their organizational data security strategy.

Complementary products

- Egress Email and File Protection
- Egress Secure Vault
- Egress Secure Workspace

Highlighted features

- ✔ Integrated MS Office add-in for Word, Excel and PowerPoint with dynamically configurable classification labels
- ✔ Customizable headers, footers and watermarks for Office documents
- ✔ Classification policies integrate with secure email policies to recommend or enforce encryption
- ✔ Document fingerprinting provides comprehensive tracking, including after edits and filename changes
- ✔ Full auditing and reporting for keeping track of data as it is shared and stored
- ✔ Integrates with existing DLP and content filtering policies
- ✔ Fully configurable end-user experience

Visit www.egress.com for more features and information

About Egress Software Technologies Inc

Egress Software Technologies is the leading provider of privacy and risk management services designed to manage and protect unstructured data in a seamless user experience. The Egress platform leverages machine learning-led policy management, encryption and discovery to enable end-users to share and collaborate securely, while maintaining compliance and reducing the risk of loss.

Common Criteria

bsi. ISO/IEC 27001 Information Security Management

CESG Certified Product
Foundation Grade
DGEE378428688-1104

egress®

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

www.egress.com