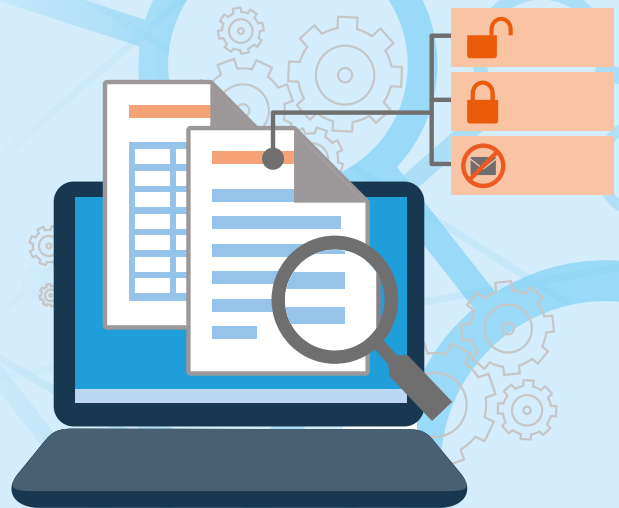


# Egress Switch Email and Document Classification

All organizations, irrespective of their business sector or type, hold and distribute sensitive information. One of the biggest challenges any organization faces when considering their data security strategy is understanding the types of sensitive data their employees handle and applying the correct levels of data protection.



## The benefits

- Integrated MS Office Add-in for Word, Excel and Powerpoint with dynamically configurable classification labels
- Classification policies can be closely integrated into Switch encryption policies to enforce and simplify the encryption process
- Fully configurable end-user experience including the ability to enforce selection of classification for any new or existing documents
- Header and footer classification information is fully customizable based on corporate requirements, including text and branding
- Perform classification of email and office documents at the desktop or at the email gateway
- Assign dynamic policies based on individual users or groups, or apply organization-wide
- Maintain detailed auditing and tracking of information as it enters and leaves your organization
- Integrate with existing DLP and content filtering tools

## Promote data security awareness

Many organizations perform detailed analysis of all data flowing internally and outside their network boundary to try to create an appropriate risk assessment. A key part of this is training and end-user education so that all employees take responsibility for the data they hold and share. Being able to visually identify and mark data with appropriate classification can greatly improve an organization's ability to control data flow and prevent data loss.

## Integrated data classification

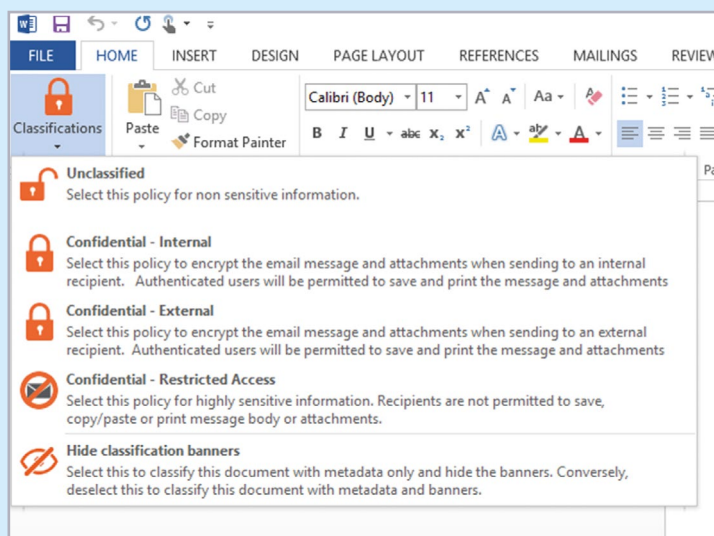
Egress Switch now includes functionality that enables users and systems to add visual and system identifiers to MS Office documents, assisting with the identification and protection of sensitive content. Policies to classify MS Office content can be centrally deployed and enforced, enabling greater protection and tracking of personally identifiable information (PII) and other sensitive content. This new functionality complements Switch's existing capabilities for marking and securing email.

## Automatically classify and encrypt data

The Switch Client and Gateway apps can automatically detect classified content and apply policy-driven encryption appropriate to the classification. This integration simplifies end-user encryption and provides higher levels of Data Loss Prevention (DLP).

Automatic classification and encryption policies can be applied using the following criteria:

- Detection of keywords and metadata embedded within email message body and attachments including: Word (.doc, .docx), Excel (.xls, .xlsx), PowerPoint (.ppt, .pptx) and PDF
- Automatically encrypt based on content, classification and recipient addresses to enforce security between trusted entities



### User education and behavior

Combined with Egress Switch Secure Email and File Transfer encryption technology, Switch classification functionality can educate employees, promote security awareness and change behavior. Users can be forced to classify content at the point of creation, when updating existing documents and when distributing it via email.

It is also possible to force compliance with information assurance standards such as ISO27001, and interact with users via customizable dialogs and prompts.

### Visual identifiers

Switch Email and Document Classification can apply visual identifiers (headers and footers) to Word, Excel and PowerPoint documents by default. The headers and footers are fully customizable, including content and branding to match your corporate policies and identity.

### Metadata

In addition to visual identifiers the Switch Email and Document Classification can add metadata tags and attributes to classified documents. This meta information can be used for tracking and be detected by DLP or other content inspection tools, as well as being used by the Switch Gateway for message-level encryption.

### Compliance

Switch Email and Document Classification helps organizations to meet data protection and compliance regulations, as well as increasing end-user awareness and education. However, if required, these identifiers can be removed, with content still classified via the underlying metadata. Advice on how and when to classify data can be displayed to the user upon any interaction with content, including when protective marking should be applied.

### About Egress Software Technologies Inc

Egress Software Technologies is the leading provider of information security services designed to secure shared data from start to finish and delivered to customers in the Public and Private Sectors using a single platform: Egress Switch.

Taking a holistic approach to information security, the Switch platform is made up of highly integrated and flexible service lines that enable users to securely share and collaborate on sensitive data. These award-winning services include email and document classification, the only email and file encryption product to be CPA certified by CESSG, secure managed file transfer, and secure online collaboration.

Using patented key management, the platform utilizes a unique community-based licensing model that consists of paying and free Switch subscribers, who are able share information securely with one another using a single global identity.

