Egress Switch
Email Discovery

Regulatory laws and compliance are increasingly driving the need for more comprehensive and integrated security procedures and practices across all industries. One of the biggest challenges faced is understanding the flow of sensitive data leaving an organization, in particular via email – which remains the most popular mechanism for sharing information with external third parties.

However, when implementing email security and data loss prevention measures, many organizations struggle to identify what types and classification of sensitive information is being shared by specific individuals and departments, as well as the quantities and regularity with which this is done.

The benefits

- **Understand the flow of sensitive information**
  Monitor all inbound and outbound emails to gain oversight into how sensitive information is shared by individuals and the organization as a whole

- **Flexible monitoring**
  Scan for sensitive data shared via email based on industry-specific data protection regulations, individual business function and universal policies

- **Detailed reporting functionality**
  Receive comprehensive analysis of information sharing trends to identify key areas in need of data loss prevention measures

- **Implement data security measures based on specific policies**
  Use the information gathered to develop and deploy robust information security measures tailored to the specific requirements identified

The Egress approach

Without access to a comprehensive analysis of the sensitive information leaving an organization, it is difficult to put in place all necessary measures to protect against data breaches and losses. This can lead to fines of up to £500,000 from the ICO, and cause untold harm to the individuals and businesses involved, including reputational damage.

Egress Switch Email Discovery has been developed to help organizations evaluate the types and quantities of confidential data being shared by specific departments and employees, to ensure the appropriate remedial action can be taken to protect this content.

Monitor the data released by your organization

Switch Email Discovery can be quickly and easily deployed within an organization's existing email infrastructure to silently monitor all inbound and outbound email, providing detailed reports on the confidential information being shared.

Specific rules can be created to scan for relevant and targeted content based on an individual organization's information sharing requirements. These can include, for example, key words or phrases, case reference numbers, document trends or types, and unstructured content. In addition, Switch Email Discovery is also supplied with a list of default universal policies to scan for, including:

- Credit card and financial information
- UK National Insurance / Social Security numbers
- UK driving license number
- UK and international passport numbers
- Data protection-related content
- Child protection and adult social services content
- Personally identifiable information

info@egress.com www.egress.com 1-800-732-0746 @EgressSwitch

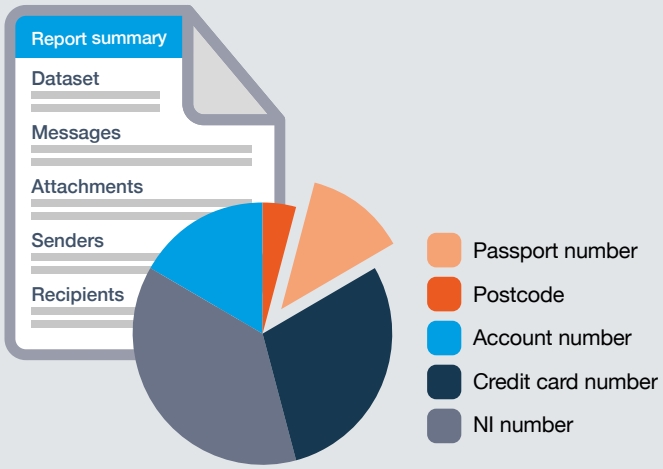
egress

switch
secure data exchange

Reporting functionality

Once the monitoring process is complete, detailed analysis is provided demonstrating the security critical information flowing throughout the organization. These reports highlight key data sharing trends and any specific areas of vulnerability, such as:

- Summary of emails processed and associated data characteristics
- Summary of message types
- Details of attachments, including size and type
- Demographic of senders and recipients
- Data loss prevention message triggers
- The email domains that sensitive content is sent to
- The individuals sending sensitive content
- Message trends by volume and date / time



Putting policies in place with Egress Switch

The findings from these reports can subsequently be used to implement email security policies that suit an organization's newly identified data protection requirements. When deployed via Egress Switch Gateway, Egress Switch Secure Email and File Transfer can enforce flexible policies at both the desktop and the gateway to help protect all sensitive information shared both internally and externally.

For example, where user acknowledgment and involvement is required, policies can integrate at the desktop to trigger alerts and messaging to prompt users to apply security measures. Automatic encryption, meanwhile, can be enforced based on content, destination or source of attachments. Switch Gateway is designed to integrate seamlessly into existing email flow, either by routing all email through the server or by enabling a journal in Microsoft Exchange and sending a copy of all emails to the Switch Gateway server. As Switch Gateway sits on the SMTP protocol, it is possible to integrate it to any email platform or topology.

System requirements

- Microsoft Windows Server 2008R2 / 2012R2 (32 / 64 bit)
- Microsoft .NET framework 4.0 + Microsoft SQL Compact Edition 3.5+ / SQL Express / SQL Standard
- Connection to https://switch.egress.com (443)

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 CESG, 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.

CESG Certified Product
Foundation Grade
35512043DGEE

Common Criteria

FIPS VALIDATED 140-2
FIPS 140-2 Inside

bsi. ISO/IEC 27001 Information Security Management

CYBER ESSENTIALS PLUS