TOLL

Secure Digital Exchange
Powered by egress

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 to understand the flow of sensitive data leaving an organisation, 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 organisations struggle to identify what types and classification of sensitive information are 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 organisation 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.

Contact:

Justin Cybul
National Business Development Manager

T: +61 3 9676 1250
M: +61 413 018 409
E: SDX@tollgroup.com
W: www.tollgroup.com/secure-digital-exchange

Our approach

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

Egress Software Technologies has developed Email Discovery to help organisations 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 organisation

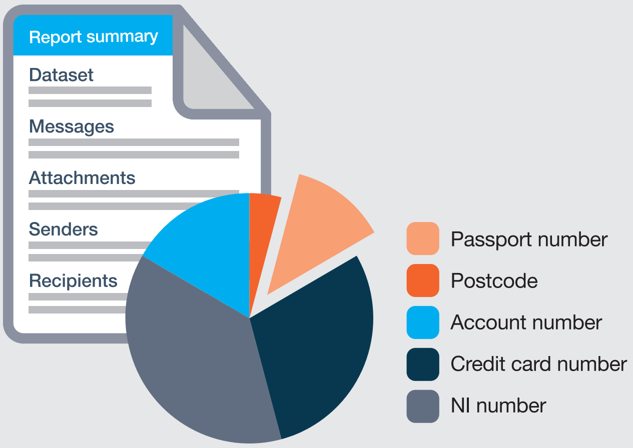
Email Discovery can be quickly and easily deployed within an organisation's existing email infrastructure to silently monitor all inbound and outbound email, providing detailed reports on the confidential information being shared.

Specific rules can be created to scan for relevant and targeted content based on an organisation's information sharing requirements. These can include, for example, key words or phrases, case reference numbers, document trends or types and unstructured content.

Reporting functionality

Once the monitoring process is complete, detailed analysis is provided demonstrating the security of critical information flowing throughout the organisation. 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 Secure Digital Exchange

The findings from these reports can subsequently be used to implement email security policies that suit an organisation's newly identified data protection requirements. When deployed via the Secure Digital Exchange gateway, Secure Email and Secure 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.

The Secure Digital Exchange 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 Secure Digital Exchange Gateway server. As the Secure Digital Exchange 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

About Secure Digital Exchange

Toll is already renowned as a world-class integrated logistics provider and is pleased to be enhancing its offerings in the digital space with its Secure Digital Exchange for email, documents, web forms, digital workspaces and mailrooms – for both internal and external communications in a completely secure environment.

Our new product suite is powered by Egress©, the world leader in encryption platforms, which today enables over 1,000 global organisations and is certified by the UK Government and NATO.

Taking a holistic approach to information security, the solution enables users to securely share and collaborate on sensitive data. Using patented key management, the platform utilises a unique community-based licensing model that consists of paying subscribers and designated recipients, who are able to share information securely with one another using a single global identity.

Toll is delighted to present Secure Digital Exchange – powered by Egress© – to our clients in Australia and New Zealand.

Egress© Certifications

UK Government

NATO IACD