FORTRA™

Clearswift and Echoworx Encryption Portal

There are a variety of email encryption options available on the market today, but a number of these solutions can be too complicated for people to use and adoption of encryption technology is often hindered for this reason. Fortra's Clearswift, in conjunction with Echoworx, provides an intelligent, automated encryption solution to ensure that email messages are delivered securely, and critical information is protected from today's cyber threats — within or outside the network.

Business Problem

Encryption offers the most advanced level of protection for secure information sharing through email, but many organizations are unsure of the best encryption method to adopt, including how to deploy it, configure it, and get staff and external email recipients to use it correctly.

The key issue with email encryption is the need for key exchange of public keys to email to be encrypted. PGP and S/MIME encryption is "industry standard" and works fine for businesses communicating with other businesses (B2B). However, these options are not ideal when a business needs to communicate with small organizations or members of the public (B2C).

This is largely due to the practical issue of educating the users, both internally and externally, as to how to use the encryption functionality within Microsoft Outlook (email client), Microsoft 365, or Gmail (in Google Workspace) effectively. Examples of this include a chartered accountant needing to send sensitive data to the client, a doctor needing to email a medical report to a patient, or a hotel needing to email a reservation confirmation to a guest. The accountant, doctor, and hotel representative are experts in their associated fields, but they are not an expert in email encryption.

Furthermore, some organizations may have relationships with third-parties where they need to use a particular encryption method such as PGP, but where the messaging platform that they operate on, such as Microsoft 365, does not natively support PGP encryption.

Clearswift, in conjunction with Echoworx, offers an encryption solution that resolves the above uncertainties and business challenges.

PRODUCT SUMMARY

Professional Services
A number of additional consulting options are available to help with the deployment and configuration of this solution:

- Architecture Design
- Policy Design
- Solution Implementation

Products
On-Premises Portal Encryption is an optional, priced module for the following product:

- Clearswift Secure Email Gateway (SEG) appliance

Support
Clearswift provides 24/7 global support as standard, with additional options for premium support.

The Solution

The benefit of using Clearswift's Secure Email Gateway (SEG) appliance in conjunction with Echoworx's OneWorld Encryption Portal is that the email encryption process can be entirely automated for a more streamlined and user-friendly encryption option deployed for those who want to control what information is encrypted and when.

The Clearswift products provide TLS email encryption which encrypts "the pipe" in which email travels through. Echoworx encrypts "the data" — the email that is traveling through the pipe. Effectively, Echoworx is the mechanism/tool used for automating encryption and the Clearswift products provide the intelligent decision making as to what email should be encrypted.

The combined solution offers organizations three types of Encryption options:

1. **Client-initiated.** This is where the user has made the decision that the email communication needs to be encrypted. The user very simply either clicks on an "Encrypt" button (add an x-header to the email) within the Outlook OR the user adds a token into the subject of the email – e.g., [ENCRYPT]. Once the user sends the email, the on-premises Clearswift Secure Email Gateway will identify the button has been selected by looking for the x-header OR detects the [ENCRYPT] within the email subject line. The Clearswift SEG appliance will then securely send the communication to Echoworx for encryption.

2. **Content-initiated.** This is where the client has not made any decisions on whether the email should be encrypted or not, and when the Clearswift SEG steps in. Using deep content inspection engine and granular security policy, the on-premises SEG appliance can identify the context of the email and whether it needs to be encrypted. The polices can be set up to detect in text format or within images (using optical character recognition):

   - PCI – credit card information
   - PII – personal information
   - Data formats, for example Excel files with sensitive data/IP

3. **Route-initiated.** This is where client is not aware of the sensitivity of the recipient and the business decision has been made that all email communication to the recipient must be encrypted, regardless of the content of the data. This means the Clearswift SEG appliance can determine the email will be encrypted by recognizing the email domain (for example, @clearswift.com).

Once the Clearswift SEG appliance has made intelligent decisions when to encrypt messages (based on numerous criteria), the email message is then relayed securely over TLS to the OneWorld Web Portal where messages are automatically encrypted using OneWorld's cloud-based X.509 Certificate Authority.

The three different decision capabilities of the combined Clearswift and Echoworx solution mean that regardless of the users understanding of encryption, email will always be securely transmitted through the business communication processes. This underpins organizational security policies, as well as legislative requirements such as PCI DSS, GDPR, and other statutory regulations.

More Information

For more information or pricing, contact the Clearswift team at www.clearswift.com/about/contact.

FORTRA™

Fortra.com