FORTRA™

DATASHEET (CYBERSECURITY)

Encryption in Fortra's Clearswift Secure Email Gateway

A Component of Fortra's Technology for: TLS • S/MIME & PGP • Password-protected ZIP Files • Portal

What is Encryption?

Encryption, the bi-directional conversion of meaningful content to unintelligible content, is the single most powerful information security tool the email security admin's armory. On its own, it fulfills two of the three fundamental tenets of security — "CIA" — and facilitates the third.

Encryption guarantees:

- **Confidentiality** of organizational data
- **Integrity** of organizational data
- **Availability** of organizational data

Deployed correctly, encryption ensures there is no way sensitive information can be exposed to an unauthorized recipient. Encryption also ensures there is no way for an attacker to intercept sensitive data transfers across email. Encryption is today's essential option in the Adaptive Data Loss Prevention (A-DLP) toolkit.

The Need for Encryption

Encryption underwrites the security of corporate data even if a system is breached or data is stolen.

Encryption is also necessary for compliance with the increasing number of legal and regulatory requirements that are designed to protect personal information. Many of these regulations accept that lost data simply isn't lost — regardless of who has possession of it — if it is encrypted.

Thus, encryption provides corporate security and regulatory compliance.

The Need for Automation

Encryption can be driven by the sender but if they forget that the data is sensitive, you can rely on Fortra's Clearswift Secure Email Gateway appliance to make a policy-based decision to ensure data is fully secured to the recipient.

The On-Premises Clearswift Secure Email Gateway Encryption Options

The intelligent encryption policy can be based on sender, recipient, subject content, message body, attachment types, attachment content, message header, or document metadata.

Pre-configured dictionaries for the detection of PCI, PII, GDPR, HIPAA, and other regulations are included to ensure compliance. Dictionaries can be extended by customers through the use of expressions, Regexp, and database export.

Encryption Options

The Clearswift Secure Email Gateway appliance supports a number of different encryption regimes to allow companies to select the most appropriate methods for their different user communities.

Understanding how your internal users and systems communicate with external parties will allow you to determine which encryption methods to use.

- TLS is standard where encryption is required simply between the organization and other organizations. TLS can operate in both "Opportunistic" or "Mandatory" mode; clearly "Mandatory" mode is required for when messages can only be sent over an encrypted tunnel.

TLS just protects the message over a public network; if encryption is required to the desktop/recipient, then it would be necessary to encrypt the messages themselves. There are a number of different methods for doing this, including:

  - PKI (S/MIME or PGP)
  - Password-protected Zip files
  - Password-protected PDFs
  - Web Pickup

- PGP and S/MIME are examples of public key infrastructure (PKI) encryption systems. These technologies are for business communication between recipients using standard email clients such as Microsoft 365 (Outlook), Exchange (Outlook), and Domino (Notes), rather than webmail systems such as Hotmail and Gmail. This technology relies on the concept of a user having a keypair, where one part is made public to allow people to encrypt mail to you, and the other part must be kept private to allow you (and only you) to be able to read the message.
- Password-protected files rely on a passphrase being used to "lock" the file so that only the people with the passphrase can do so. The security of these files was previously quite low, but recent changes to Microsoft and Zip-file security now provide strong levels of encryption. However, the strength of the key is still important, much like a user's password.
- Web Pickup allows messages to be sent securely to recipients without the need for keys or special mail clients, and requires the recipient to have a browser to send and receive messages.

  As this is browser-based, this method also supports mobile devices. The message recipients would receive a branded email notifying them that a message was available to read on the message portal. They would connect securely over HTTPS, authenticate, and then be able to read and reply to the message.

Adaptive Redaction

Adaptive Redaction is the intelligent removal or change of information within a document to ensure that the content meets organization policies for information security. Encryption can also be applied after the data has been sanitized. See the other Clearswift Adaptive Redaction datasheet for further details.

Encryption Summary

Encryption is a powerful tool for both organizational security and regulatory compliance. Clearswift's on-premises Secure Email Gateway offers a range of options to meet all levels of encryption requirements. It provides automatic, policy-driven, transparent encryption across the whole organization.

The New FIPS Support

The Secure Email Gateway appliance now provides an option for it to be installed in FIPS (Federal Information Processing Standards) mode. When enabled, FIPS mode ensures that all encryption used is compatible with U.S. government agency standards. For this to occur, the options around ad hoc and PGP encryption are disabled and removed from the user interface.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.