

## Encryption in the SECURE Email Gateway



A component of Clearswift's Adaptive Redaction technology for:  
TLS • S/MIME / PGP • Password Protected ZIP • Portal

### What is encryption?

Encryption, the bi-directional conversion of meaningful content to unintelligible content, is the single most powerful security tool in the admin's armory. On its own it fulfills two of the three fundamental tenets of security, 'CIA' – and facilitates the third. It guarantees the **C**onfidentiality of organizational data; it ensures the **I**ntegrity of organizational data; and, by allowing secure remote storage, it facilitates the **A**vailability of organizational data. If done correctly, there is no way for an attacker to break modern encryption. Encryption is an 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 and even if 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.

Encryption thus provides corporate security and regulatory compliance.

### The need for automated encryption

Encryption suffers one major drawback – all too often it is too difficult to implement and too confusing to use.

Only fully-automated encryption – such as that provided by the SECURE Email Gateway option – can be trusted to provide blanket, consistent and cost-effective data encryption.



## The Clearswift gateway encryption option

SECURE Email Gateway secures data at the point of exit in accordance with pre-defined policy. All sensitive data can be encrypted automatically whenever it is sent outside the corporate system, whether this is an email or the content of an attachment.

The intelligent encryption policy can be based on sender, recipient, subject content, message body, attachment types, attachment content or message header attributes. Dictionaries of PII data – such as bank card numbers, social security numbers, IBAN code templates and so on – are included to ensure regulatory compliance. If a template is recognized, the content is encrypted.

## Encryption options

SECURE Email Gateway supports a number of different encryption regimes to allow users to select the most appropriate method for themselves. TLS is standard, and is useful where encryption is required simply between the organization and other known organizations.

Portal-based encryption is an option where more generalized secure communication is required with organizations that have either different or no encryption regimes. This employs a hosted encryption portal to serve as a separate 'pick-up' center. Encrypted content is sent to and received from the portal using HTTPS in a push/pull manner.

Another option uses PGP and S/MIME public key encryption where greater crypto strength is required. This can be used for communication between recipients who use standard email clients such as Outlook, Outlook Express and Notes; and can be used to create policy-based secure connections between Gateways or from Gateways to Recipients.

## The new FIPS support

When the Email Gateway is installed there is 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 US government agency standards. For this to occur, the options around ad hoc and PGP encryption options are disabled and removed from the user interface.

## Adaptive Redaction

Encryption is one of Clearswift's Adaptive Redaction options. Adaptive Redaction is the intelligent removal or change of information within a document to ensure that the content meets organization policies for information security. The automatic removal of hidden content (sanitization) and the removal of sensitive content (redaction) combine to provide next generation Data Loss Prevention and Information Governance solutions.

Where there is no need for full encryption but some content nevertheless needs to be hidden, one of Clearswift's other Adaptive Redaction options can be used as an alternative. This does not encrypt the entire document, but removes the sensitive information before it is sent outside the organization.

See the other Clearswift Adaptive Redaction datasheets for further details.

## Encryption summary

Encryption is a powerful tool for both organizational security and regulatory compliance. 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.

### UK - International HQ

Clearswift Ltd  
1310 Waterside  
Arlington Business Park  
Theale  
Reading  
Berkshire  
RG7 4SA

Tel : +44 (0) 118 903 8903  
Fax : +44 (0) 118 903 9000  
Sales: +44 (0) 118 903 8700  
Technical Support:  
+44 (0) 118 903 8200  
Email: info@clearswift.com

### Australia

Clearswift (Asia/Pacific) Pty  
Ltd  
5th Floor  
165 Walker Street  
North Sydney  
New South Wales, 2060  
AUSTRALIA

Tel: +61 2 9424 1200  
Technical Support:  
+61 2 9424 1210  
Email: info@clearswift.com.au

### Germany

Clearswift GmbH  
Landsberger Straße 302  
D-80 687 Munich  
Germany

Tel: +49 (0)89 904 05 206  
Technical Support:  
+49 (0)800 1800556  
Email: info@clearswift.de

### Japan

Clearswift K.K.  
Shinjuku Park Tower  
N30th Floor  
3-7-1 Nishi-Shinjuku  
Tokyo 163-1030  
Japan

Tel: +81 (3)5326 3470  
Technical Support:  
0800 100 0006  
Email: info.jp@clearswift.com

### United States

Clearswift Corporation  
309 Fellowship Road, Suite  
200  
Mount Laurel, NJ 08054  
United States

Tel: +1 856-359-2360  
Technical Support:  
+1 856 359 2170  
Email: info@us.clearswift.com