# clearswift

# Clearswift SECURE Email Gateway

**With email still being the primary business collaboration tool, organizations need to ensure that the content and information they send and receive is both appropriate and permitted to enter or leave the organization. The Clearswift SECURE Email Gateway (SEG) helps to secure against critical information data loss; protecting the intellectual property and brand reputation of your organization and ensuring compliance with current regulations and standards.**

Clearswift's award-winning deep-content inspection capabilities facilitate the competitive advantages inherent in open and safe communications; transforming email from a high-risk communication channel to one tailored exactly to your organization's needs. The Gateway scans emails for sensitive content, and based on a granular organizational policy it provides the necessary flexibility to permit multiple behaviours, depending on the senders and recipients of the message. The Clearswift Adaptive Redaction functionality allows for content to be dynamically modified to make the content safe rather than having to stop and block and force a remediation.

### Inbound threat protection
Featuring integrated Kaspersky and / or Sophos anti-virus, with automatic updates every fifteen minutes to provide the latest protection. These technologies are supplemented with zero-hour anti-malware and active code detection to ensure that no malware comes in, or goes out, via email. Targeted attacks typically use email with commonly used Office and PDF files as a means to deliver a payload. If these exploits manage to reach the desktop they will be run with the user privileges of the recipient, which could be provide access to sensitive data. So as an addition to standard anti-malware features the Structural Sanitization feature permits macro's, scripts and Active/X to be removed from messages, PDF and Office file formats significantly reducing the risk of targeted attacks being successful.

### Best-of-Breed spam detection
The NEW Clearswift SECURE Email Gateway comes with a completely redesigned anti-spam engine incorporating the best-of-breed Mailshell component. This reduces the amount of spam reaching the end-user and the number of false positives. DKIM support enables yet further spam reduction and with a new Outlook Spam Reporter included, spam can be monitored, registered and eliminated. Featuring a new multi-layer spam defence mechanism using IP reputations, greylisting, signatures, SPF, RBL, recipient authentication and machine learning (Bayesian) engines to provide > than 99.9% detection rates, the SEG is able to drastically reduce the amount of time users spend managing their inboxes and significantly reduces the effect of malware contained in spam.

### Context-aware content inspection policies
Flexible policies and context-aware content inspection mean you no longer have to choose between free-flowing communications and unacceptable risk. Flexible policy is the key to any real-world deployment. If the policy is too restrictive then people either cannot work effectively, or they find ways to get around their security policy.
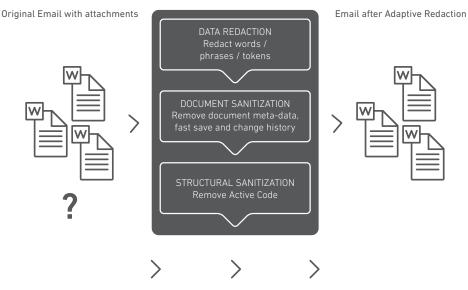
### Adaptive Redaction
Clearswift's unique Adaptive Redaction features permits the content of messages and attachments to be modified dynamically based on policy. The Data Redaction feature allows information to flow when before it would have been blocked. Customers can create policies to change specific words and phrases in messages and documents with "*" characters to make the content safe. This can apply to Credit Card numbers, Social Security details, Project codes, individual names or any custom value.

**Figure 1. Clearswift Adaptive Redaction: Data Redaction**



The Document Sanitization feature can remove outstanding revision changes, clearing history and fast-save data that can also hold embarrassing critical information being accidentally disclosed. Document properties, such as "Author", "Organization" and "Status" can be completely removed or bespoke properties can be preserved.

### Adaptive Redaction



## Adaptive Data Loss Prevention

Data loss is one of today's biggest organizational concerns. Be it the latest designs, customer details or private employee information, the loss of intellectual property can ruin a company, both from a financial and reputational perspective.

To reduce the chances of accidental data loss, the SECURE Email Gateway is able to control messages based on their content and their context. Context is provided through integration with Active Directory or LDAP, so policy can be applied to a specific individual or group (or the whole organization). The content of the message is checked through looking for text in the message body, subject line and also attachments, against pre-defined search patterns and tokens.

Search patterns consist of standard words, phrases or regular expressions, which can be used to look for complex alphanumeric patterns. These patterns could be used to identify an organization's assets, such as credit cards, IBAN numbers, social security numbers, and many more.

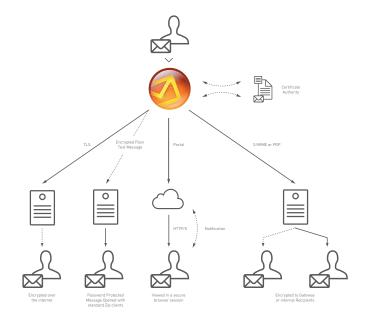These phrases can be combined using Boolean and positional operators to create examples such as:

- Credit .FOLLOWEDBY=1. Card
- Confidential .AND. (Project .OR. Material)

## Compliance

Staying within the bounds of a regulatory framework is very important. To help you maintain compliance, the SECURE Email Gateway includes standard templates and dictionaries for common terms that may indicate a data breach.

The Gateways are supplied with customisable dictionaries for GLBA, HIPAA, SEC and SOX to save deployment time. Organizations that must adhere to PCI and PII regulations can use a custom dictionary and the special 'credit card' and 'social security' tokens. Customers can augment the standard dictionaries with ones that may be more applicable.

Some information will always need to be shared and email encryption is another important capability of the Gateway, ensuring that regulations relating to sensitive data sent over the internet are protected using strong encryption. The HITECH Act in the US and the UK's Data Protection Act make it clear that sensitive data must be encrypted when sent via email;
the SECURE Email Gateway supports a number of different encryption mechanisms to provide flexibility as required.



## Email encryption

With TLS as standard, and cost options to provide either S/MIME, PGP and password protected files or Web portal-based encryption, the Email Gateway offers a variety of options to cater for customer requirements. Whichever you choose, the Gateway allows sensitive data to be delivered securely, in seconds, using the optimal format for the recipient.

## Management and reporting

The user interface of the Gateway is powerful, yet simple to use. With roles based administration, automation and policy re-use, it's quick and easy to build policy, manage violations, track messages and report on trends and behaviour. In this way, valuable insight is provided without consuming valuable admin resource.

## Deep content inspection

True file-type detection that recognizes files by signature and not by extension allows the Clearswift SECURE Email Gateway to understand files accurately. Compressed file archives are opened and the contents examined in real-time; embedded documents are discovered, and content is scanned in depth, to ensure data leakage is kept at bay.

## Flexible deployment options

You decide how you want to buy and deploy the Clearswift SECURE Email Gateway, either as a pre-installed hardware appliance, as a software image that can be loaded on a choice of hardware platforms, or alternatively virtualized in a VMWare / HyperV environment. The Clearswift SECURE Email Gateway is also available as a Cloud solution using providers such as AWS or from Clearswift (regional offerings) as hosted virtual servers where you maintain control of the platform, but with the convenience and benefits of a Cloud delivery model.

| Feature | Benefit |
|---|---|
| **Flexible Policy** | |
| Granular policy controls | Easily to define with self-documenting policies to allow usage while minimising risk. |
| Directory integration | Gather email addresses for senders and recipients from centralized directories on a regular basis and organization hierarchy details. |
| Flexible Policy | Create workflow for email messages permitting manager review & release allowing better context to be applied to message management. |
| **Inbound Threats** | |
| Bi-directional virus and anti-malware* scanning | Stops known and unknown malware infection entering or leaving the network with up to 2 AV engines (Sophos and / or Kaspersky). |
| Zero-hour anti-malware | Detect and block new outbreaks before virus signatures are available reduces the risks from new malware strains. |
| Multi-layer anti-spam | Multiple spam engines provide a holistic approach to spam detection delivering a genuine > 99.9% detection with a 1 in 300,000 fp rate. |
| Structural Sanitization | Rather than simply detecting active code, such as(macro's, scripts and Active/X in messages and attachments, these documents can have the active code removed from Microsoft Office, Open Office and PDF files so that they can be delivered safely. |
| Pornographic image scanning | Images that contain pornographic material can be analysed and quarantined reducing the risk of offending the recipients. |
| **Data Loss Protection** | |
| Binary file-type identification | Accurate signature based identification with the ability to define own file signatures. |
| Adaptive Redaction* | Data Redaction can be used to remove sensitive words and phrases in messages and attachments. Document Sanitization is used to remove document properties, tracking changes and fast-save data. |
| Lexical analysis and regular expression rules | Search file content for key words and phrases using simple expression or more complex pattern matching with regular expressions to identify sensitive data. |
| Pre-defined sensitive data templates | Easily identify and detect standard information tokens, including credit cards, bank account, social security and national security numbers. User tokens can easily be created and used. |
| Work flow rules | Methods to enforce outbound messages to be copied to a manager; Messages violations can be managed by line managers; Messages can be delayed by a custom time to allow for messages to be deleted before it leaves the organization. |
| **Compliance** | |
| Compliance dictionaries | Multi-language profanity and editable compliance dictionaries including GLBA, HIPAA, SEC, SOX, PCI and PII to minimize reputational and terminology risks. |
| Integrated Encryption | TLS provided as standard with optional S/MIME, PGP and Password* protection methods to allow messages to be sent securely. |
| Portal based encryption* | Web based portal email encryption permits encrypted messages to be sent to non-technical user. |
| Support for offbox archiving | Relay-to and BCC to divert copies of all or some of the message to on-premise or Cloud based archiving solution. |
| **Management** | |
| Intuitive web-based interface | Ease of use and no requirement to learn complex syntax or Linux commands. |
| Multi-gateway consolidated reporting | Consolidated reporting view of user's activities for easier analysis and sharing of management data. |
| Multi-gateway message tracking | Enables a view of where messages came from, how they were processed and where they went across multi-gateways, complete with manual or scheduled export capability. |
| Centralised SYSLOG, SNMP, SMTP Alerting | Consolidate to a central SIEM, or use SNMP or SMTP management alerts for a 'lights out' data centre deployment. |

\* Cost Option

**clearswift**