clearswift
RUAG Cyber Security

SECURITY+
for Email, Web and Cloud

Clearswift's SECURITY+ empowers organizations with the ability to augment their existing IT security infrastructure to increase inbound threat protection and enable adaptive data loss prevention across their key business collaboration channels.

Adaptive Redaction (ARgon)

Unique to any other technology on the market, Adaptive Redaction comprises 3 components which are available with all the Clearswift SECURE Gateways and can be added-on to non-Clearswift email and web infrastructure. The technology was developed to overcome advanced information borne threats and to conquer the fundamental challenge which most traditional Data Loss Prevention (DLP) solutions have; the 'false positive'.

Adaptive Redaction works in conjunction with Clearswift's robust Deep Content Inspection Engine to detect and modify the content of documents, including email, MS Office documents, Open Office documents, HTML, web pages and PDF, to ensure that policy is not breached, but the communication still occurs. *This modification occurs automatically at the organization's perimeter, on inbound and outbound traffic, without hindering communication flow*.

Importantly, Adaptive Redaction can help organizations to automate many of today's best practice information security processes for added protection against inadvertent data leaks, phishing attempts, cyber-attacks and to support GDPR compliance.

STRUCTURAL SANITIZATION

Remove the code, prevent the risk

Zero-hour phishing, malware and ransomware protection. Automatically removes active code (macros, scripts etc) embedded in incoming email attachments and web downloads in real-time, to **prevent the risk of attacks** being triggered inside an organization without hindering communication flow.

At the same time, Structural Sanitization can protect active content embedded in Intellectual Property to **prevent inadvertent exposure** via email, websites or cloud collaboration tools.

DOCUMENT SANITIZATION

Data harvesting protection, sensitive data and hidden metadata leak prevention.

Automatically removes sensitive 'invisible' information from documents and attachments, such as the author name in document properties or any other 'hidden' properties which could create a potential data leak across email or the web. It can also remove revision history, fast save and comments left in documents **from inbound and outbound traffic**.

DATA REDACTION

Critical information protection, supports GDPR Compliance.

Automatically replaces sensitive 'visible' information from a document or email with *** before it's shared via email or published on the web unauthorized. For example, Personally Identifiable Information (PII) such as birth dates, National/Social Security Numbers and other identities left inadvertently in documents, or Credit Card data (PCI) left in an email. Data Redaction can protect this data from **either entering or leaving an organization** through email, being published on the web, or uploaded to web applications.

SECURITY+
for Email, Web and Cloud

Augmenting existing security infrastructure for advanced protection against today's information borne threats. Request a Demo or Evaluation of Clearswift SECURITY+ solutions today.

SECURITY+ for Email

ARgon for Email **complements existing non-Clearswift email gateways** by adding-on the 3 components of Adaptive Redaction. ARgon will enhance inbound threat protection and enable adaptive data loss prevention across an organization's busiest communication channel. Quick to deploy, easy to manage. Can be deployed in 'Monitor Mode' for an Evaluation.

SECURITY+ for Exchange

The Clearswift SECURE Exchange Gateway **ensures that internal email correspondence on Exchange deployments matches the confidentiality and compliance policies** of an organization. Messages that contain certain violations can be quarantined for manual inspection, or the offending content can be removed through the use of Adaptive Redaction features. With critical information protection starting within the organization, malicious and or accidental data leakage is further mitigated.

SECURITY+ for Web

This Clearswift solution is **designed to co-exist with an existing web security provider** using industry standard ICAP functionality including F5 Networks and Blue Coat. Through implementing the SECURE ICAP Gateway, organizations are able to apply Clearswift's deep content inspection, Adaptive Redaction components and data loss prevention policies to existing web security infrastructure with no disruption, enhancing threat protection and aligning to information governance policies and compliance requirements.

Clearswift SECURE Email Gateway

The Clearswift SECURE Email Gateway (SEG) offers an unparalleled level of cyber-attack protection and outbound data loss prevention for secure email collaboration. With its legacy in the MIMEsweeper for SMTP technology, the Clearswift SEG incorporates dual AV (Sophos and Kaspersky), a multi-layer spam defence mechanism, multiple encryption options, deep content inspection control on size and types of attachments, and all 3 Adaptive Redaction features. **Secures cloud email platforms such as Office 365 and Gmail**. **On-premise or Hosted deployment options available**.

Clearswift SECURE Web Gateway

Going beyond advanced filtering and hygiene the Clearswift SECURE Web Gateway provides an unprecedented layer of threat detection and sanitization for **secure web**, **social and cloud collaboration**. Enables complete and granular control over what users access or share online. Flexible, policy-based filtering and content aware inspection extends beyond limiting recreational browsing, to view inside encrypted traffic preventing phishing and malware attacks, and sensitive data leaks. **Secures cloud collaboration tools and services such as Salesforce**, **Dropbox**, **Google Drive**, **Office 365 etc**.