clearswift
A HelpSystems Company

Secure File Sharing for Defence

With a priority to responding to tasks and building for the future, Defence organisations demand enhanced capabilities for secure information sharing as part of a drive for digital by default, to harness the transformative power of technology whilst avoiding the burdens of non-standard, bespoke and 'locked-in' methods of exchanging data.

Products

- Clearswift SECURE ICAP Gateway (SIG)

Professional Services

Consultancy options are available to help with the deployment and configuration of this solution:

- Architecture Design
- Policy Design
- Solution Implementation

Support

Clearswift provides 24x7 global support as standard, with additional options for premium support.

Business Problem

Throughout the defence sector, there is a requirement for improved ways of secure working, whilst reducing cost and optimising performance for sharing nationally sensitive information. Email is commonly used as a suitable collaboration mechanism in many circumstances, however large files need an alternative solution for sucure transfer.

Clear guidance is provided by the MOD for the provision of ICT systems in support of national security commitments. These need to meet the associated system accreditation standards of the UK and its international partners. This includes managing policy, procedures and capabilities effectively to deliver appropriately configured systems that support the need to collaborate, communicate securely and share information effectively.

However, the risk remains high as with the need to share information comes the risk of exposing the wrong content to unauthorised individuals or organisations. Files that contain confidential information, either visible within the body of the file or hidden within its metadata, can be mistakenly shared. Equally, the reception of files from partners might open a door to embedded malware and external threats hidden within standard file transfers.

Highly secure digital file sharing with Clearswift

Organisations can gain full control of how and when information is shared both internally and externally. Managed data flows can be easily defined to exchange information through a portal to address the need to share large files securely and in a cost-effective manner.

By integrating a layer of Deep Content Inspection and document sanitisation through the ICAP protocol with a best-of-breed Managed File Transfer (MFT) solution, additional information controls can be set in place to enforce security and compliance policies for files being transferred.

The solution helps the MOD to meet accreditation requirements and the wider defence industry partners to meet the risk-based controls imposed by the Defence Cyber Protection Partnership (DCPP) and associated DefStan05-138 standard.

As all file transfer traffic can be directed to pass through this enhanced level of management and security, it overcomes the primary challenge that many consumer-oriented cloud collaboration tools suffer from, particularly as ICT systems migrate to shared or virtualised services.

How does Clearswift Secure File Sharing work?

The solution embraces the Clearswift SECURE ICAP Gateway, which is a market leading solution for enhancing cyber security infrastructure. It enables the balance to secure and protect sensitive information with the need to continuously collaborate.

The solution provides the ability to apply Deep Content Inspection, Adaptive Data Loss Prevention and Advanced Threat Protection technologies to align the flow of information to the organisation's information governance, risk and underpinning compliance policy requirements. It integrates with the market leading MFT solution, HelpSystems' GoAnywhere product, but can be integrated with an ICAP compliant device.

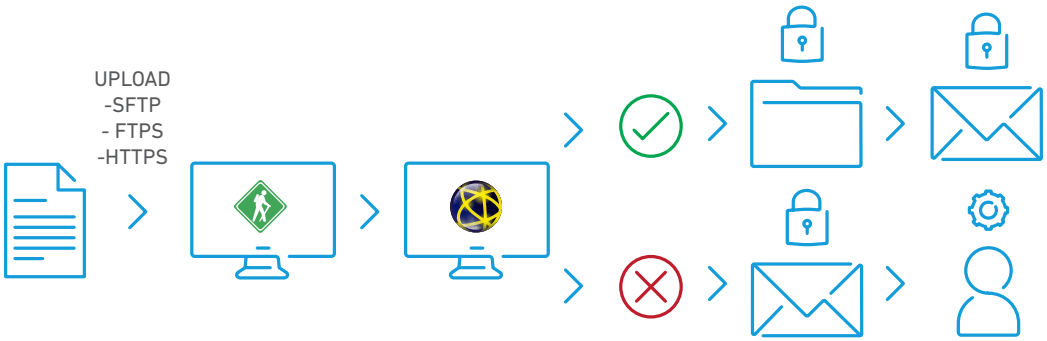

Diagram 1: File is sent through secure file sharing platform with integrated ICAP Gateway where it is deeply inspected for sensitive information that breaks security policy.

Clearswift's Deep Content Inspection (DCI) capability goes beyond the levels of what is traditionally offered in the market. It is not limited by zip/encryption, file size, analysis timing delays, virtual environment evasion techniques or multiple embedded document layers. As a result, it offers high detection rates and low impact to minimise false positive rates.

DCI coupled with document rewrite can remove both visible and invisible information as well as active content based on policy. 'Invisible' information, including that hidden in comments, document properties and revision history creates risk of unauthorised information sharing. While embedded active content in innocuous looking files can create risk from ransomware and other malware which is activated when the document is opened.

Adaptive Data Loss Prevention (A-DLP) is the non-disruptive removal or transformation of data according to policy (rules), to ensure that information shared complies with prevailing security policies before it is sent to, or received by, the recipient (person, application or system).

Intelligent policy enforcement is applied to only the information that breaks policy and compliance regulations, whilst allowing the rest of the document to continue without disruptive false positives. Adaptive DLP also sanitises documents by stripping out hidden metadata (author, username, server and software names, etc.) and other sensitive information that can be harvested and used for targeted attacks. Adaptive DLP modifies the information in real-time according to policies rather than a simple masking, to ensure only the acceptable level of information is shared and received, and that sensitive information always remains safe.

Advanced Threat Protection is used to detect and automatically strip out active content in the form of embedded malware triggered executables, scripts or macros used to extract or hold sensitive data hostage. Clearswift's Advanced Threat Protection sanitises without delay in delivery, as only the malicious active content is removed, allowing the rest of the file transfer to continue unhindered.

The Clearswift Secure File Transfer solution streamlines the exchange of data between systems, employees, project teams and collaboration partners. It provides a single point of control with extensive security settings, detailed audit trails and reports. It is supported by an intuitive interface and comprehensive workflow features that help to eliminate the need for bespoke programs / scripts, single-function tools and manual processes that were traditionally required.

Features

Designed to scale to enterprise deployments, the system provides:

- business level information asset protection – focused on the asset value, risk profile and the associated impact of the data associated with it,
- secure handling of clearly identified sensitive information, managed according to the systems that support its communication,
- granular control required to meet the policy requirements,
- advanced options for dealing with scanned documents and image files (Optical Character Recognition and image-based text redaction),
- advanced Anti-steganography functionality to prevent infiltration of malicious code, or exfiltration of sensitive information in images,
- coherent sharing of information within and across teams both internal and externally to the organisation that are creating or managing the data
- supports the need for collaboration across multiple organisational and security domains,
- controls to enable visibility of the files flowing to support both audit and compliance under specific collaboration policy requirements for e.g. for DCPP,
- support for operational requirements for cyber security monitoring and incident response,
- support for multiple implementations of encryption that are common to the UK Defence community,
- compliance with policies and procedures that lay down how information is to be managed and secured within and across the defence community under DefStan 05-138.

Benefits

Designed for organisations of all sizes, the system provides:

- **Low friction:** Simple and frictionless deployment using an established, proven and assured security technology platform to minimise cost and maximise time to value;
- **Deep content validation:** Proven capability to meet the specific demands of the UK Defence community especially in the ability to implement controls requiring deep data checks, validation of content sensitivity and meeting the adaptive requirements for content modification for DLP policy;
- **Multiple domain support:** Support for architectures that will protect multiple operating domains and information exchange protocols to enable the benefits afforded by defence platform transformation in capability provision through industry-enabled services – cost, time, flexibility and diversity of supply;
- **User experience:** Innovation-led improvement to end user experience for secure sharing of information that reduces risk and the impacts of data loss or security breach;
- **Assurance:** Enhancing the baseline levels of cyber protection in the face of increasing state-level threat;
- **Reduced operational cost:** Specific features to deal with workflow, including policy violations to minimise operational costs;
- **Support:** Underpinned by a defence-aware organisational culture that is creative, passionate and built around a customer focused 'one-team' approach, aligned with the essence of the Team Defence community, to ensure the low-risk delivery of enhanced protection.

About Clearswift

Clearswift is trusted by organisations across the globe for advanced content threat protection and the highest level of defence against breaches through today's digital communication channels. Our technology supports a straightforward and 'adaptive' data loss prevention solution that gives teams the freedom to securely collaborate, whilst providing information security personnel with visibility and control of sensitive information flow.

Over 70% of Clearswift clients operate within critical national infrastructure, including defence conglomerates, government agencies and financial institutions, all of which demand the most advanced cyber threat prevention and information security solutions. Working closely with these clients over two decades has enabled Clearswift to gain a clear to understanding of the cyber challenges they face, keep abreast of their evolving threatscape, and support compliance with the complex regulatory environment within which they operate.

Our united approach to working with clients has ultimately driven the specialised development of the award winning Clearswift product portfolio which is backed up with a superior 24/7 customer and partner support service, and an extensive channel partner network across the globe.

To learn more about Clearswift, visit **www.clearswift.com**

Contact Us

Clearswift Ltd.
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire RG7 4SA
United Kingdom

E: info@clearswift.com

T: +44 118 903 8300

Deployment

The Clearswift SECURE ICAP Gateway is designed to be deployed stand-alone, or in conjunction with other Clearswift SECURE Gateway products to create the Clearswift Aneesya Platform. When deployed with other products, a consistent Deep Content Inspection and policy engine ensures consistent discovery of critical information, DLP policy and Adaptive Redaction functionality for information flow control. The products include:

Clearswift Information Governance Server (IGS): enables users to securely register and classify information with the IGS. Compliance Officers are given access to oversee who and what is being registered as well as the ability to track and trace information (not just files) passing across the organisation boundary, in real-time, including information provenance reporting.

Clearswift SECURE Web Gateway: offers granular control over what users can access or share online. Flexible, policy-based filtering and content aware inspection extends beyond limiting browsing, to view inside HTTP/S encrypted traffic to prevent phishing and malware attacks and the unauthorised exposure of sensitive information.

Clearswift ARgon for Email: augments existing email security gateway infrastructure to enable Adaptive Redaction functionality and the ability to track and control sensitive information contained in email crossing over the organisation's boundary (inbound/outbound).

Clearswift SECURE Exchange Gateway: enables data loss prevention policies to be applied to internal email communications, along with the ability to track and control internal information sharing and email segregation functionality without the need for separate infrastructures.

Clearswift SECURE ICAP Gateway: designed to co-exist with an existing web security solution, the Clearswift SIG enables Adaptive Redaction functionality, and the ability to track and control information passing through an ICAP compliant web gateway or solution, including Managed File Transfer (MFT), cloud storage and collaboration applications.

Cost

Flexible pricing options are available to suit differing implementation requirements across the varying scale of organisations that constitute the UK defence community. This ensures the solutions are commercially appropriate, affordable and sustainable whilst offering the ability for customers to consolidate their existing security solutions into an integrated platform for both on-premise and cloud delivered services.