FORTRA™

SOLUTION BRIEF (CLEARSWIFT)

Cross Domain Security Solutions For Defence

There remains an ongoing challenge with Cross Domain information sharing, as increasing cyber risk further exposes the danger of the wrong information being sent to the wrong place and the transferred material containing malicious content which can harm critical information systems. This challenge is increasing with the priority now given for effective information interoperability and the ongoing demand for collaboration between governments, their agencies and their supply chains. Bespoke solutions are cost-prohibitive in many cases and there is a drive to use commercially available solutions to reduce costs and speed up processes.

Business Problem

The need to share information continues to grow with increasing interaction between governments, their agencies and their supply chains. Wherever information flows it needs to do so with the assurance that it has been inspected and authorised for sharing. Information is time-critical, so communication and sharing must be carried out in a timely manner, but with the assurance that only the right information is being shared. While email is still the primary communication method, the need to share large files which are unsuitable for email continues to grow exponentially between machines, systems, and applications. Operational costs remain key when considering the solution to ensure that an additional burden is not required for the successful deployment, running and administration of the system.

Highly Secure Information Sharing with Clearswift

Cross domain requirements for each project will be different, but there are some common ones which should be considered:

- Understand the appropriate risks associated with sharing critical information
- Define and maintain an effective information security and security operations policy
- Build and maintain a secure network by installing and maintaining network defences to protect data
- Protect sensitive data with encryption
- Utilise Adaptive Data Loss Prevention functionality to ensure only authorised information sharing
- Regularly monitor networks
- Implement strong access control measures
- Track and monitor access to network resources and sensitive data

PRODUCT SUMMARY

Products

- Clearswift Information Governance Server (IGS)
- Clearswift Secure Email Gateway (SEG)
- Clearswift Secure Exchange Gateway (SXG)
- Clearswift Secure ICAP Gateway (SIG)
- Clearswift Secure Web Gateway (SWG)

Solution Guides

- Improving Control of Regulated ITAR Information
- Protecting Information Across the Defence Supply Chain
- Secure File Sharing for Defence
- Cross Domain Gateway Filters

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.

Whilst this list is not exhaustive, it does highlight the need for securing sensitive data through the identification of information using both content and context for analysis.

Information needs to be protected as it flows both internally between teams within the organisation and across the external boundary to the sharing partner. The protection will vary according to the differing risks associated with the direction of the flow and this needs to be reflected in the policies and controls managing the various flows.

Clearswift offers several Cross Domain solutions to address the different system requirements, however there are key features that are common to them all.

Key Features for Cross Domain Solutions

At the heart of every Clearswift solution is the Deep Content Inspection (DCI) engine. This enables the recursive disassembly of data into its constituent parts. Whether it is an attachment to an email, or a zip file to be uploaded to or downloaded from a website, Clearswift's DCI will perform over 50 levels of recursion, so an image in a document, embedded in another document, inside a zip file attached to an email creates no issues. Even images are processed with Optical Character Recognition (OCR) technology to ensure that text is identified for further processing.

At each level throughout the recursion, analysis is carried out and the appropriate policy-based mitigation applied. This is a key attribute to the Clearswift approach which underpins the flexibility to meet a range of system and project requirements through the following collection of features

Content Disarm and Reconstruction (CDR)

While traditional CDR solutions look at malicious embedded active content, Clearswift extends the approach to include data as well as active content. Providing protection not just from weaponised documents, but also malicious insiders who wish to exfiltrate sensitive information in less common ways.

Adaptive Redaction

Clearswift's award winning Adaptive Redaction is the ability to change content based on policy as it passes across the SECURE Gateway. There are three principle components:

1. Data Redaction

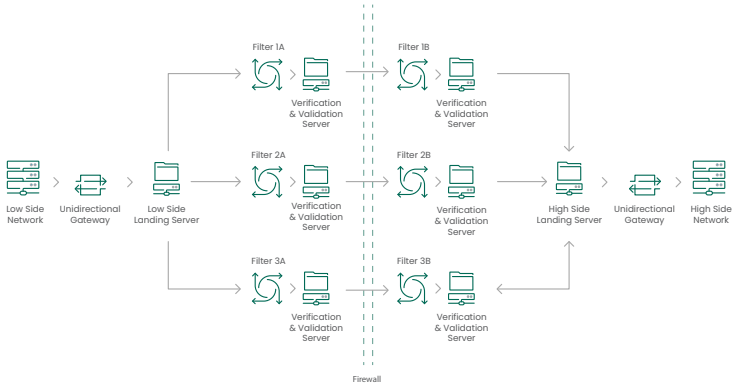
Data redaction is the removal of 'visible' data in documents based on policy, replacing the content with asterisks.

Redaction can also be applied to images. OCR is used to discover the text and the system can then 'black box' the text. Even inside a scanned image PDF, the image is black boxed, rather than being obscured, to ensure that the data cannot be recovered.

2. Document Sanitisation

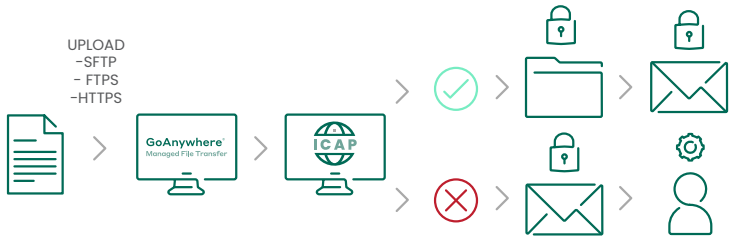
Document sanitisation is the removal of 'hidden' information found in electronic files. This includes items like document properties, revision history, comments and

Solution 1: Clearswift Cross Domain Gateway Filters



- Scalability for performance and availability
- Information flow segregation with content and destination aware policy

Solution 2: Clearswift Secure File Sharing



- Granular control over asset sharing both inter and intra organisation
- Full Deep Content Inspection with Adaptive Data Loss Prevention

fast save data. Policy granularity ensures that those items which are required, for example embedded classification tags, remain, while the others are removed. Missing classification tags can be detected and the document routed back to the sender for enforcement.

Document sanitisation can also be applied to images, not just for property removal, but also for anti-steganography functionality. This disrupts any information concealed in an image so that the hidden information cannot be recovered. It is used to prevent data exfiltration (outbound traffic) as well as stopping inbound malware payloads or 'command and control' activities by botnets.

3. Structural Sanitisation

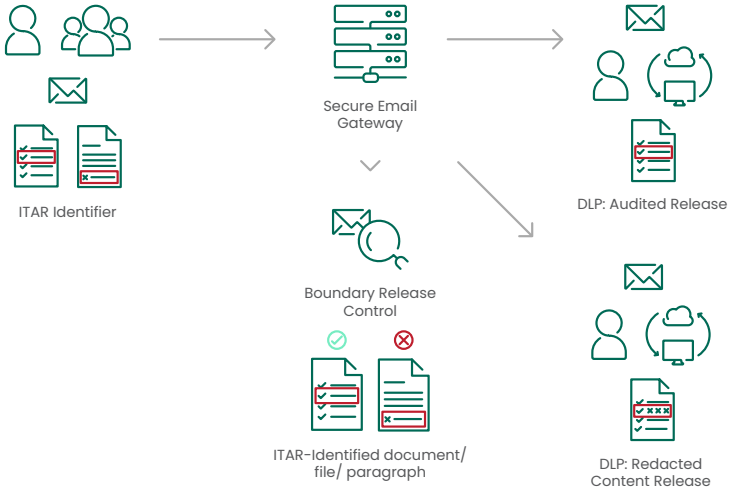
Structural sanitisation detects and removes active content from documents. This ensures that weaponised documents are effectively neutralised before they are opened. Unlike sandbox technologies, structural sanitisation happens in milliseconds ensuring the secure continuous flow of information across the domains.

While this is most frequently used for Advanced Threat Protection, it can also be used to protect intellectual property held, for example, in macros in spreadsheets.

Direction-Agnostic

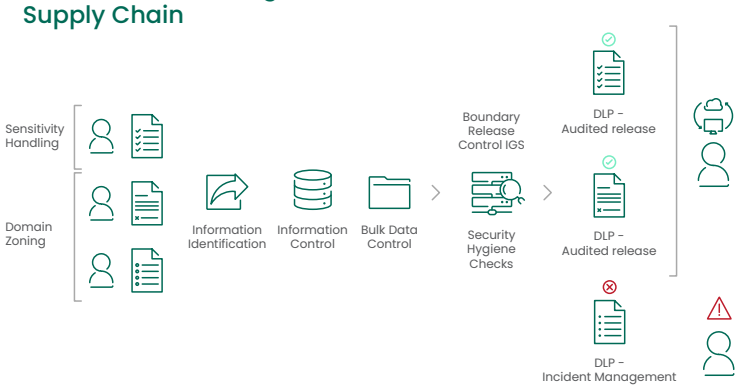
Clearswift's DCI and policy engine is direction-agnostic enabling polices to be set on information travelling in either direction. There are examples of where both inbound and outbound use provide risk reduction. For example, data redaction can be used to mitigate the risk of unwanted data acquisition as well as data loss prevention.

Solution 3: Improving Control of Regulated ITAR Information



- Boundary controlled release
- Fully audited information control

Solution 4: Protecting Information Across The Information Supply Chain



- Security hygiene checks and Advanced Threat Protection
- Information identification and bulk data control

Content- and Context-Based Policy

While many solutions concentrate on the content, it is also the context which is equally important. Clearswift's DCI is consistent across all communication methods, but the actions can depend on the context used. For example, a document sent by email could be encrypted, while a document sent via a managed file transfer (MFT) solution could be redacted, and a document copied to a USB stick could be blocked. Furthermore, the actions can depend on the individual who is using the communication channel

Adaptive Data Loss Prevention (A-DLP)

Clearswift supports traditional Data Loss Prevention (DLP) functionality, including keyword search, lexical expressions, regular expressions, and lexical expression qualifiers. It supports multiple tokens, for example credit cards, social security and driving license numbers as well as the ability to define custom tokens. Policies can be extended with reserved works, such as 'NEAR' or 'AFTER', to help ensure that the policy is only triggered at the appropriate moment. When used in conjunction with the Adaptive Redaction features a comprehensive solution is created for use in the most demanding of cross domain scenarios.

Distributed Operations

Often the hidden cost for any security solution is the operational overhead. Clearswift, with its deep integration into LDAP or Active Directory systems can proactively route policy violations to the sender's manager, as well as to a specific individual or group. The outcome of the policy violation is usually to hold the offending message for review. The manager will have more context around the event his report has created and so should be able to act more quickly to resolve the issue. Should the event have been created by a False Positive, then it is a simple matter of clicking on a link to release the original content. Use of Adaptive Redaction can ensure that content will be delivered, albeit with some information removed – however, this does ensure that collaboration continues.

Integration with SIEM Solutions

For many organisations, the ability to use an event aggregator such as a Security Information Event Management (SIEM) solution, is key to enabling cross product correlation. Clearswift Gateways and designed for use with SIEM solutions, forwarding events accordingly. For smaller installations without a SIEM solution, comprehensive reporting and event alert mechanisms are built in.

Benefits

Designed for organisations and deployments of all sizes, Clearswift Cross Domain solutions offer:

- **Business-level information asset protection:** focused on the asset value, risk profile and the associated impact of the data associated with it;
- **Coherent and consistent:** ensures appropriate sharing of information within and across teams both internally and externally to the organisation that are holding or creating the data in support of the need for collaboration across multiple organisational and security domains;
- **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 content detection, including ITAR, especially in the ability to implement controls requiring deep data checks, validation of information sensitivity and the adaptive requirements for content modification for an effective policy
- **User experience:** innovation-led improvement to end user experience for secure sharing of information that reduces risk and the associated impact of a compliance breach;
- **Reduced operational cost:** specific features to deal with policy violations to minimise operational costs;
- **Data flow visibility:** necessary controls and visibility of the data flowing to support both audit and compliance under the specific collaboration policy requirements for ITAR;
- **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;
- **Low risk:** aligned with the essence of the Team Defence community, to ensure the low-risk delivery of enhanced cyber protection

Deployment

Clearswift solutions are 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): Track, trace, and control information (not just files) passing across the organisation boundary, including information provenance reporting

Clearswift Secure Email Gateway (SEG): Track, trace, and control information as it flows through email

Clearswift Secure Exchange Gateway (SXG): Track, trace, and control information as it travels in internal email providing internal DLP and email segregation functionality without the need for separate infrastructures

Clearswift Secure ICAP Gateway (SIG): Track, trace, and control information which passes through an ICAP-compliant web gateway or solution, including Managed File Transfer (MFT) applications

Clearswift Secure Web Gateway (SWG): Track, trace, and control information as it travels to and from the Internet

Clearswift solutions are fully compatible with Microsoft 365, and can augment security policies provided by M365.

Cost

Flexible pricing options are available to suit differing implementation requirements across the varying scale of organisations that constitute the Australian 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.

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.