clearswift
A HelpSystems Company

# Supporting Cross Domain Solutions for Defense

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. Custom solutions are cost prohibitive in many cases and there is a drive to use commercially available solutions to reduce costs and speed up processes.

**Products**

- Clearswift SECURE Email Gateway
- Clearswift SECURE ICAP Gateway
- Clearswift SECURE Web Gateway

**Solution Guides**

- Improving Control of Regulated ITAR Information
- Secure File Sharing for Defense

**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

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 authorized 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 defenses to protect data
- Protect sensitive data with encryption
- Utilize Adaptive Data Loss Prevention functionality to ensure only authorized information sharing
- Regularly monitor networks
- Implement strong access control measures
- Track and monitor access to network resources and sensitive data

While 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 organization 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's SECURE Email, Web and ICAP Gateways can be set up to handle sophisticated policies and configured to filter the content in the traffic flow and prepare it to pass through a Cross Domain Solution.

## Key Features for Clearswift Solution

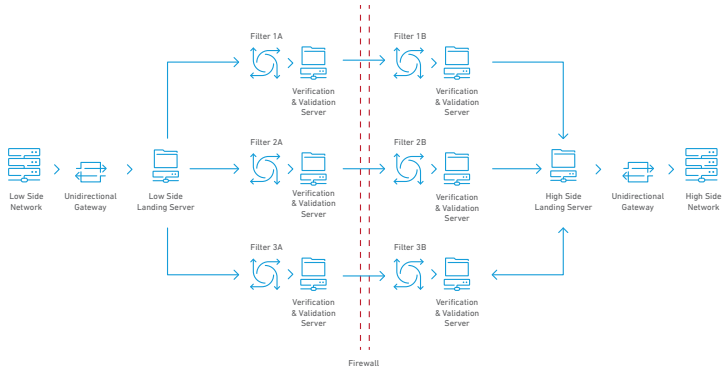
At the heart of every Clearswift solution is the Deep Content Inspection (DCI) engine. This enables the recursive disassembly of data into its constituent parts. Whether it is an attachment to an email, or a zip file to be uploaded to or downloaded from a website, Clearswift's DCI will perform over 50 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 content, Clearswift extends the approach to include data as well as active content. Providing protection not just weaponized documents, but also malicious insiders who wish to exfiltrate sensitive information in less common ways.

### Clearswift's filter configuration supporting Cross Domain Solutions




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

## Adaptive Redaction

Clearswift's award winning Adaptive Redaction is the ability to change content based on policy as it passes across 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.

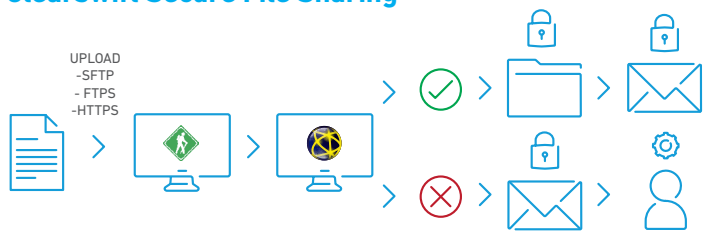
Redaction can also be applied to images. OCR is used to discover the text and the system can then 'black box' the text. Even inside a scanned image PDF, the image is black boxed, rather than being obscured, to ensure that the data cannot be recovered.

**2. Document Sanitization**

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

### Clearswift Secure File Sharing




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

**3. Structural Sanitization**

Structural sanitization detects and removes active content from documents. This ensures that weaponized documents are effectively neutralized before they are opened. Unlike sandbox technologies, structural sanitization 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.

## Content and Context Based Policy

While many solutions concentrate on the content, it is also 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 be blocked. Furthermore, the actions can depend on individual who is using the communication channel.

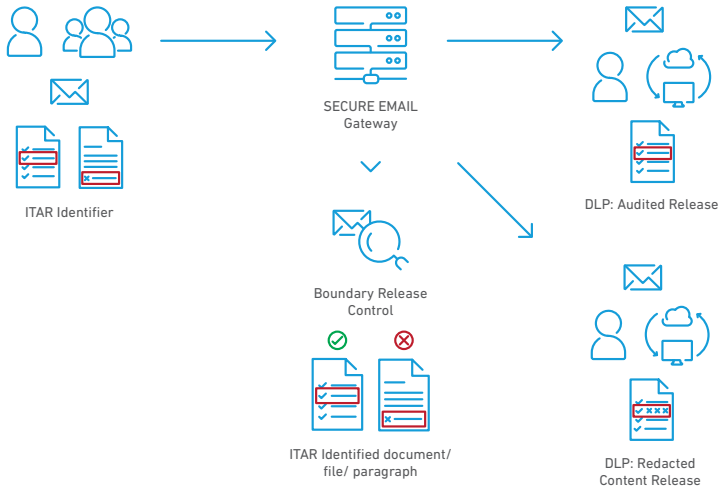
## Adaptive Data Loss Prevention (A-DLP)

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

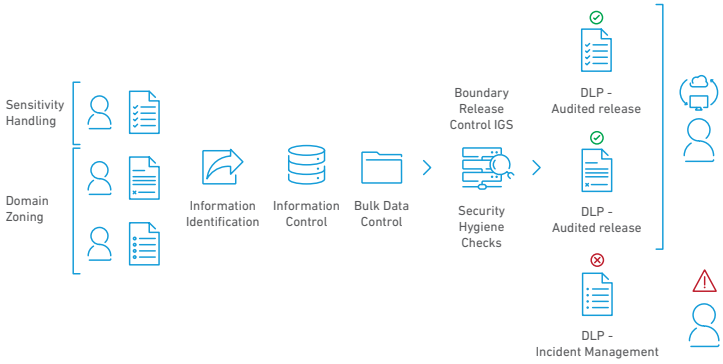
Often the hidden cost for any security solution is operational overhead. Clearswift, with its deep integration into LDAP or Active Directory systems can proactively policy violations to the sender's manager – as well as to a specific individual or group. The outcome of the policy violation is usually 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 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.

### Improving Control of Regulated ITAR Information




- Boundary controlled release.
- Fully audited information control.

### Protecting Information Across The Information Supply Chain




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

## Integration with SIEM Solutions

For many organizations, 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 are designed for use with SIEM solutions, forwarding events accordingly. For those smaller installations without a SIEM solution, comprehensive reporting and event alert mechanisms are built in.

## Benefits

Designed for organizations and deployments of all sizes, Clearswift 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 internal and externally to the organization that are holding or creating the data in support of the need for collaboration across multiple organizational and security domains
- **Low friction:** Simple and frictionless deployment using an established, proven and assured security technology platform to minimize cost and maximize time to value

## About Clearswift

Clearswift is trusted by organizations across the globe for advanced content threat protection and the highest level of defense 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, while providing information security personnel with visibility and control of sensitive information flow.

Over 70% of Clearswift clients operate within critical national infrastructure, including defense 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 specialized 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 Corporation**
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
UNITED STATES

**E:** info@clearswift.com

**T:** +1 856-359-2360

- **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 minimize 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 defense-aware organizational culture that is creative, passionate and built around a customer focused 'one-team' approach, aligned with the essence of the Team Defense community, to ensure the low-risk delivery of enhanced protection
- **Low risk:** Aligned with the essence of the Team Defense 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 SECURE Email Gateway:** Track, trace and control information as it flows through email.

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

**Clearswift Information Governance Server:** Track, trace and control information (not just files) passing across the organization boundary, including information provenance reporting

**Clearswift SECURE Web Gateway:** Track, trace and control information as it travels to and from the Internet

**Clearswift ARgon for Email:** Augment existing email security gateway infrastructure to track, trace and control information contained in email across the organization boundary.

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

## Cost

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