FORTRA™

DATASHEET (CLEARSWIFT)

Protecting Information Across the Defence Supply Chain

Clearswift supports organisations to comply with the Defence Cyber Protection Partnership cyber risk control requirements that seek to protect UK military capability throughout the MOD supply chain.

Business Problem

In the face of cyberattacks being recognised as a Tier 1 threat within the National Security Strategy, the UK seeks to secure a truly competitive, sustainable, and globally successful Defence sector that provides affordable, leading-edge capability and through-life support for the Armed Forces and international customers.

The Defence Cyber Protection Partnership (DCPP) imposes risk-based controls in order to protect UK military capability by improving cyber defence throughout the MOD's entire supply chain. Whilst aiming to preserve existing investment in cybersecurity measures, the DCPP mandates specific requirements for boundary flow control relating to contractual information, information identification, data loss prevention policies, and zoning between information domains.

In a complex collaborative environment, this can be a challenge for organisations of all sizes.

Supporting DCPP Compliance with Clearswift

At the heart of DCPP compliance, there is a need to stringently secure information and ensure it remains protected across the entire information supply chain. The risk-based approach of DCPP means that rather than trying to protect everything, critical information needs to be singled out for maximum protection.

In order to protect this information, there is a need to be able to track it to and from users and across the organisational boundary, as well as to and from the supply chain. Only with this understanding can the appropriate protection be applied.

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)

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 vpremium support.

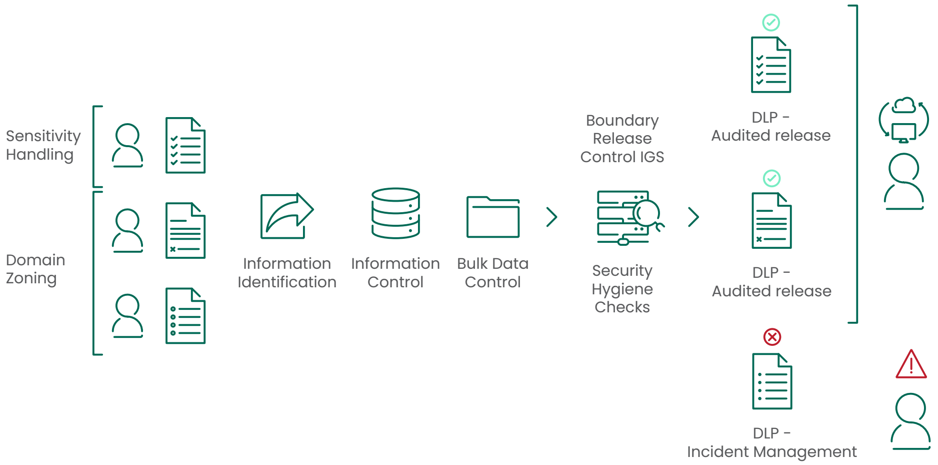

Diagram 1: Security hygiene checks and Advanced Threat Protection. Information Identification and bulk data control.

Clearswift provides a cybersecurity platform, Aneesya, that addresses the need to identify, track, trace and protect sensitive information to enable it to be securely shared with collaboration partners across the supply chain. The platform, based on a set of optionally deployed components, can seamlessly integrate with existing information systems to enable improved ways of working and secure information management.

At the heart of the Aneesya platform is the Clearswift Information Governance Server (IGS) which will:

- simplify end-user handling of sensitive information through automatic detection of classification tags and content;
- enable tracking of information at both the file and sub-file information level;
- enhance DLP solutions by blocking registered content when it is attempted to be communicated to unauthorised recipients;
- enable tracing of information in ‘after-the-fact’ analysis of communication flows;
- enable the creation of information provenance and user interaction reports to support monitoring, audit and incident management

How does the Clearswift Information Governance Server work?

The Clearswift Information Governance Server (IGS) sits in the heart of the network and provides a central repository for critical information. This information is not just complete files, but also partial file information. Files are registered by the end user, document owners, and then the information is fingerprinted to enable monitoring as it flows through email or across the organisation boundary. The IGS database contains both the full fingerprint values, as well as the partial information fingerprints. The fingerprints created use a one-way hashing algorithm to ensure that no critical information can be reverse engineered into its original values.

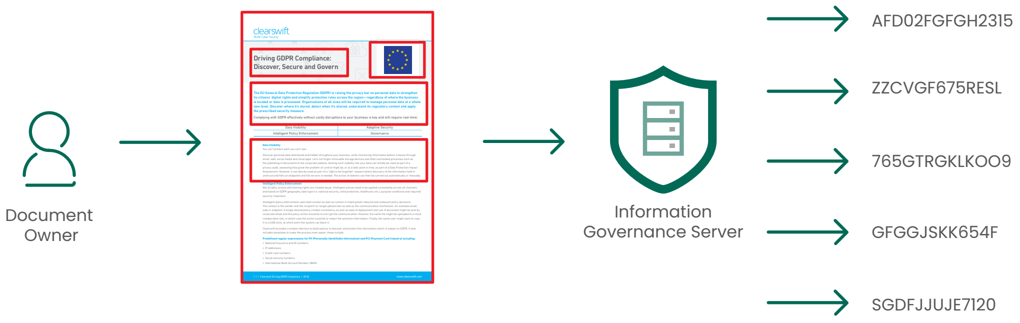

Diagram 2: User registers file with Clearswift IGS. The file and information within the file is fingerprinted for tracking and monitoring when shared.

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 and management:** according to the systems that support the communication of clearly identified sensitive information–such as email, web, and endpoint–and granular control based on both content and context required to meet policy requirements;
- **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;
- **Data flow visibility:** necessary controls, visibility, and reporting of the data flowing to support both audit and compliance under the specific policy requirements; for example, DCPP;
- **Support for operational requirements:** for cybersecurity monitoring and incident response, including integration with SIEM solutions, as well as multiple implementations of encryption common to the UK and international Defence communities, including PGP, S/MIME, and portal-based;
- **Optical Character Recognition (OCR) and image redaction:** to support secure sharing of images and scanned documents;
- **Adaptive Redaction options:** to enable real-time modification of in-flight content to ensure adherence to policy;
- **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:** seamless 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 content inspection checks, validation of content sensitivity and the adaptive requirements for content modification for effective 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 breaches;
- **Assurance:** enhancing the baseline levels of cyber protection in the face of increasing state-level threats;
- **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

Deployment

The Clearswift Information Governance Server is designed to be deployed in conjunction with the Clearswift Secure Gateway products for boundary control that enables enhanced DLP policy, to include Adaptive Redaction functionality (the ability to modify content based on policy), for full information flow control. The products include:

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

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

Clearswift Secure Web Gateway (SWG): 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.

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.

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.