clearswift
RUAG Cyber Security

Controlling Classified Information

A Clearswift Whitepaper

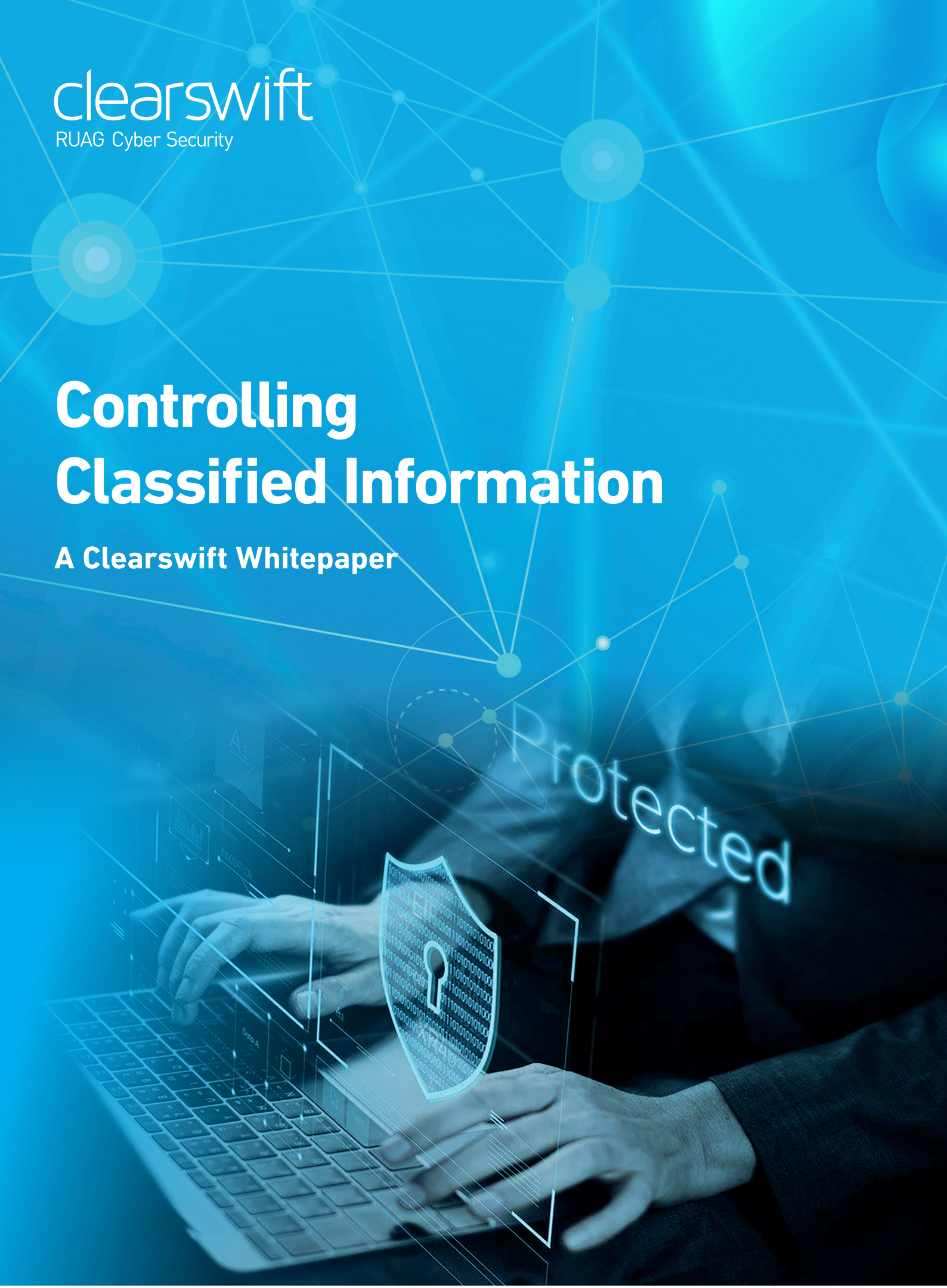


Table of Contents

Introduction 3

Deep Content Inspection & Protective Security Markings 3

Automated Policy Enforcement 4

Where Clearswift Fits (Infrastructure) 4

Data Classification 5

Advanced Information Security Features 6

Enhancing Information Security in Microsoft Office 365 & Gmail 7

Secure Managed File Transfers 7

Information Governance 7

Summary 7

Introduction

Clearswift is a provider of Adaptive Data Loss Prevention solutions that enable organisations to collaborate safely and securely through today's digital communication channels. Simple, flexible controls within Clearswift solutions have the specific objective of reducing data loss incidents and to assist with compliance obligations, including legislative requirements such as ITAR (International Traffic in Arms Regulations), to protect critical and classified information.

For Australian Federal Government agencies and commercial organisations required to comply with the Australian Signals Directorate (ASD) Information Security Manual (ISM), Clearswift addresses several controls around email, data protection and enforcement of the Protective Security Policy Framework (PSPF).

One of the mandatory requirements of PSPF states 'Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.'

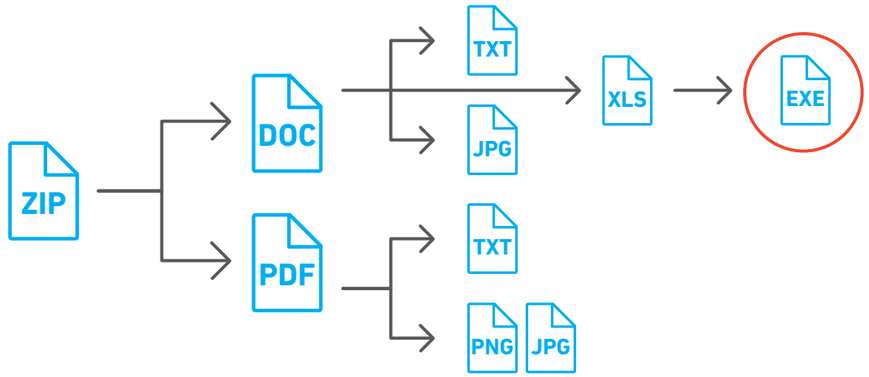
In October 2018, the federal government updated the PSPF and all Commonwealth agencies are required to adopt the new scheme by October 2020. Until then, agencies and organisations that are obligated to comply with the PSPF are required to accept and appropriately process both old and new email markings defined in the 2018 Email Protective Marking Standard (EPMS).

For the purpose of this document, email and web channels will be the focus of the Clearswift controls that address PSPF, covering:

- inbound and outbound email
- internal email
- website uploads or downloads (including private email platforms or cloud storage applications)

Deep Content Inspection & Protective Security Markings

Clearswift's robust Deep Content Inspection (DCI) engine is built into all Clearswift solutions and enables the ability to recursively drill down into digital files to a level other competitive solutions can't inspect. This capability provides greater assurance that classified information is being treated correctly and malicious threats or sensitive data concealed within complex file structures are identified and can therefore be appropriately protected.



Janusseal is the security labelling and classification software application from Janusnet, providing government agencies and commercial organisations a simple to use and compliant EPMS 2018 solution for marking documents and emails with their relevant classification level.

The use of security protective markings is an effective means to maintain data confidentiality and prevent data leakage. It is a method for users and systems to determine how to treat sensitive information when it is communicated internally or to third party organisations.

It is now a mandatory requirement of the Australian Government Protective Security Policy Framework (PSPF) that agencies adopt a risk management approach to cover all areas of protective security activity across their organisations.

In addition, the Australian Government and Department of Defence now requires some of its supply chain to adhere to the standards of the ISM. For some businesses, this requires the application of protective marking controls, including the ability to block outbound or inbound emails with a protective marking higher than the sensitivity or classification that the receiving system is accredited for.

Irrespective of their requirement to adopt PSPF, it is good security practice to implement an information classification system to reduce the risk of inadvertent or intentional data loss.

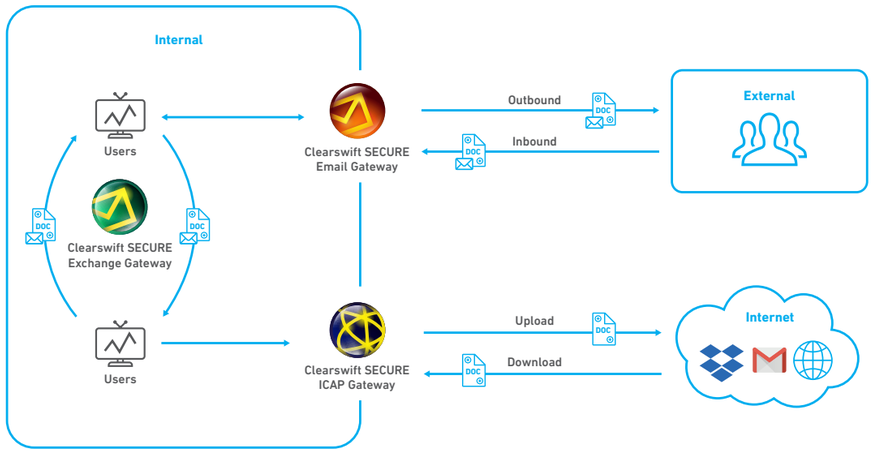
Enabling all people engaged in information handling within the organisation the ability to categorise sensitive information in emails, documents, and other files, helps to improve information security. If government contractors use the same classification schema as the contracting agency, they can ensure material is controlled and marked to the same degree of diligence that the government would apply to its own processes. This makes it easier for government and contractors to do business together, increasing efficiency across the supply chain.

This document demonstrates how Clearswift and document classification tools such as Janusnet work together to provide a combined document classification and Adaptive Data Loss Prevention solution that is **simple** and **secure**.

Automated Policy Enforcement

Clearswift solutions enable **automated** enforcement of policies based on the classification of the message or document, or, if either have not been classified. With the Clearswift SECURE Email Gateway[1] and SECURE ICAP Gateway[2], policies can be applied to **internal and external email or web uploads or downloads** (i.e. to OneDrive or Dropbox)..

Where Clearswift Fits (Infrastructure)

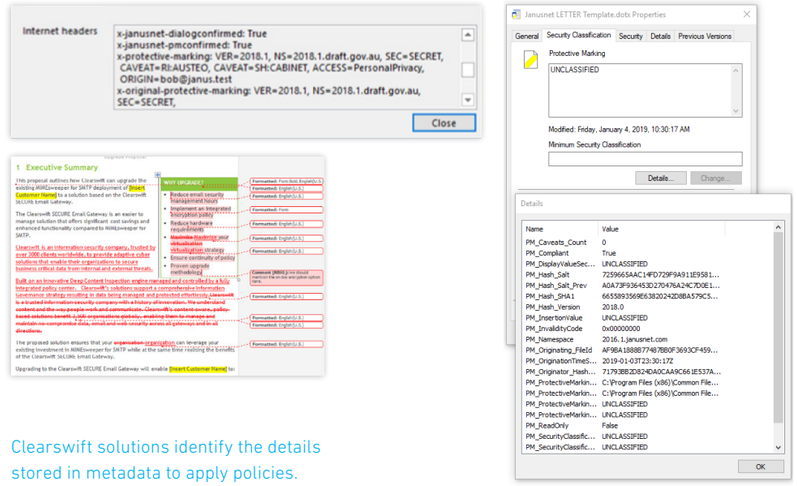


1 Clearswift's SECURE Exchange Gateway offers the same Adaptive Data Loss Protection for internal email.
2 Clearswift also provides a SECURE Web Gateway with full web proxy and hygiene capabilities.

Data Classification

Preventing information with a higher classification from being transferred to a lower classified system, is a critical requirement of the PSPF and ISM. Clearswift can enforce policies for emails and documents classified by the Janusnet solutions. Unmarked or inappropriately marked emails are covered in the ISM controls.

Not only is the classification marking in the body of the email or document checked, the Clearswift DCI also inspects metadata, such as document properties and revision history applying policy based on metadata tags, such as those inserted by Janusnet. Content based rules can be used to further inspect the document, looking for words and phrases which might indicate a mismarked document. Deep Content Inspection ensures hidden classified data is processed according to is correct classification (i.e. data classified at the highest level). For example, a zip file with a word document containing a spreadsheet which contains a hidden tab will have all information inspected and the appropriate policy applied.



Clearswift solutions identify the details stored in metadata to apply policies.

New documents, spreadsheets, presentations or PDFs are usually created from an existing file. This creates a risk of a file with a higher classification being modified and reclassified at a lower level without the original information being removed from the document's history.

Clearswift's DCI and Adaptive DLP technology will inspect the hidden metadata and either apply the appropriate classification policy, or redact the document history, removing the previously classified information and ensuring compliance.

In addition to classification-based policies, the Clearswift SECURE Gateways provide content policies based on user specified rules to look for predetermined words, phrases and expressions that may indicate that the file contains Payment Card Industry (PCI) data, Personally Identifiable Information (PII) and user specified structured data. DCI provides full text searching of common file formats like Office, PDF, Libre Office and HTML ensuring the whole document or email and attachment is inspected, including the metadata, revision history and embedded objects such as images or other files, such as spreadsheets. If the DCI engine finds content that is not appropriate for the final destination, then the file can be appropriately handled by one of the many Policy Actions based on both the content and the context of the communication, for example:

Data Loss Prevention Channels

- Inbound and outbound email
- Internal email
- Recipient and receiver
- Web uploads or downloads (including private email or cloud storage applications)

Classification Based Policy Actions

- Block
- Strip file
- Request manager approval
- Encrypt
- Redact

In addition to Adaptive DLP, the Clearswift Gateways include standard hygiene protection including:

- Anti-spam controls
- Multiple Anti-Virus options (including real-time look ups and heuristics)
- File type controls (e.g. executable file types, script files embedded within compressed file formats, etc.)

Advanced Information Security Features

Clearswift solutions offer advanced information security features including Optical Character Recognition (OCR), Anti-Steganography[3] and Adaptive Redaction technology that enable the highest level of threat prevention and data protection for secure digital collaboration.

Adaptive Redaction (3 components)

Adaptive Redaction is the ability to modify content in real-time when crossing the organisation boundary to remove only those pieces which break policy, while leaving the rest to travel to its destination. The functionality can be applied automatically and consistently to both inbound and outbound traffic flows to reduce organisational risk. There are three primary components:

Data Redaction: Clearswift can detect and redact sensitive data such as (PII, PCI, ITAR's, Medical IDs, ATN's, Passport numbers, DOB and more) from email attachments as well as documents being uploaded to the web. When used in conjunction with OCR, redaction of text in images can also be achieved. For example black boxing information on a screenshot.

Structural Sanitisation: Structural sanitisation mitigates the risk of ransomware and advanced persistent threats (APTs) by automatically removing active code embedded in documents protecting against advanced threats that traditional AV or sandbox technology cannot detect.

Document Sanitisation: Clearswift's Document sanitisation is built into all email and web products and removes 'hidden' information such as metadata data and revision history information to prevent sensitive data loss and mitigate data harvesting risks. Metadata includes critical information such as, author names, software version, GPS coordinates and dates which cybercriminals can use to create a targeted attack. Removal of such information is essential for public-facing documents, such as those published on websites, but is also good practice for all documents leaving the organisation through email or being uploaded to Cloud collaboration and storage applications.

Lexical Expression Qualifiers (LEQs)

Built into core Clearswift email and web products, LEQ's can be used as a method to validate 'true' information found against an external data source such as a database. By strengthening the ability to match critical information, LEQs enable organisations to further mitigate false positives, ensuring that the data seen is really the data that is being monitored for.

Encryption

Clearswift solutions offer a variety of Email Encryption options including TLS, PGP and S/MIME. The products also seamlessly integrate with popular Encryption Portals such as Echoworx and Ciphermail. The Clearswift Endpoint DLP solution has encryption options to secure information transfers to removable media, for example a USB stick. This ensures that should a USB stick be lost or stolen, critical information cannot be accessed by unauthorised users.

Optical Character Recognition (OCR)

OCR is the process of detecting, extracting and analysing text from an image file, an image embedded within an electronic document, or a scan of a document to determine if there is sensitive information displayed in the image. If found, then Data Loss Prevention (DLP) actions can be taken. For organisations that use multi-function printers to scan documents to PDF or companies that don't prevent "Print Screen", this functionality is essential to manage the data loss risk of scanned critical information.

Text Redaction in Images

Clearswift inspects and detects sensitive information in images using OCR and then automatically redacts it out, allowing the redacted image to be delivered. If your organisation uses multi-purpose printers for scanning sensitive documents to PDF's, regularly collaborates using images, or files containing images, this feature offers the benefit of preventing sensitive data loss through image files.

Anti-Steganography

The evolution of digital collaboration has also seen an evolution in cyber threats and new ways of sneaking data in and out of an organisation. This includes steganography - hiding sensitive data within images - which can then be emailed out or uploaded to the web. Clearswift's Anti-steganography functionality sanitises the image file, disrupting any hidden information or malicious code which may have been hidden inside of it, protecting your organisation from this newest of threats.

3 Removal of information maliciously embedded in innocuous looking images through image disruption, preventing exfiltration of the data.

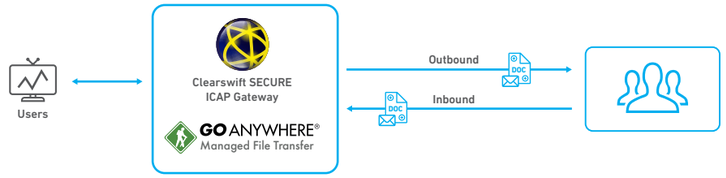
Enhancing Information Security in Microsoft Office 365 & Google's G Suite

Clearswift can seamlessly augment Cloud email solutions with the advanced security and data protection features outlined above. Enterprise strength advanced threat prevention and sensitive data protection features can be seamlessly added to Microsoft Office 365 and Google G Suite platforms, including internal data loss prevention functionality.

Secure Managed File Transfers

Deep Content Inspection can also be added to file transfer Cross Domain Solutions (CDS). The Clearswift and HelpSystems **Managed File Transfer** (MFT) solution provides a method of automating the transfer of files with maximum security, ensuring the sender remains in complete control of both the file and the system the transfer is shared from/to.

The combined Clearswift and HelpSystems (GoAnywhere) solution offers increased security as all file transfers are subject to Clearswift's DCI, enabling the application of data protection and classification policies. Inspection on the outbound files ensures only the appropriate information is shared, while on the inbound both anti-malware as well as security level checks on content can be readily carried out.



File Transfer Control to Removable Devices

Clearswift Endpoint DLP offers organisations the ability to control information transfers to removable devices, discovering classified data stored on endpoints or enforcing policies of documents being saved to external storage devices or cloud drives[4] (OneDrive, Dropbox etc).

Information Governance

An additional layer of security enforcement and information tracking can be achieved with the use of the Clearswift Information Governance Server (IGS). Users can register documents with an appropriate classification which are then monitored for if they try to traverse the organisational boundary. Monitoring is carried out on the information rather than at the file level, ensuring that even if a paragraph is cut and pasted into another document, the system will detect it and apply the appropriate policy, for example blocking the email. An audit and reporting system enables an information provenance report to be created to show who sent or received the information, when and how.

Compliance Officers can be given access to oversee who and what is being registered, and to monitor in real-time for leaks and compliance violations.

Summary

The Clearswift Deep Content Inspection engine is the content inspection engine of choice for the most sensitive defence and intelligence organisations in the Five Eyes community. Why? "because Clearswift can detect information that other vendors can't".

The combination of Clearswift and Janusnet provide organisations:

1. Simple and powerful enforcement of classification policies,
2. Control sensitive and classified information communicated internally, to trusted partners or leaving the organisation through multiple channels,
3. Ensure compliance with the ISM, EPMS and PSPF.

Irrespective of an organisation's compliance obligations, it is good security practice to implement and enforce an information classification system to reduce the risk of inadvertent or intentional data loss.

4 Additional support being added in 2019.

clearswift
RUAG Cyber Security

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.**

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

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
AUSTRALIA