clearswift
RUAG Cyber Security

Clearswift Adaptive Redaction

For Critical Information Protection

Copyright

Published by Clearswift Ltd.

Information in this document may contain references to fictional persons, companies, products and events for illustrative purposes. Any similarities to real persons, companies, products and events are coincidental and Clearswift shall not be liable for any loss suffered as a result of such similarities.

Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

Table of Contents

- Introduction 4
- Defence against attack 5
- Compliance 6
- Ease of Use 7
- Centralized Management 9
- Total Cost of Ownership / Return on Investment 10
- Sharing of Knowledge 10
- Summary 10

The Wider demands of the Chief Information Security Officer

The Chief Information Security Officer (CISO) is the custodian of information security for organizations who must have intricate knowledge of both the internal and external threats that organizations faced in order to effectively protect their organization against data breaches. At the other end of the scale, the CISO also needs to ensure the right solutions are in place to make information more widely available to the organization in order to operate effectively and drive business growth.

Information today is a core component of business differentiation; the value and control of the information now has a direct impact on financial and reputational elements of a business. The increased adoption of Cloud collaboration platforms including social networking tools now complement traditional communication channels such as email. Combined with accessibility of information from a wider range of smart media devices (SMDs) and connectivity via increased bandwidths, the Information Supply Chain (ISC) now reaches every corner of the world at the touch of a button.

Furthermore, the attacks on organisations are becoming increasingly sophisticated, with innocuous looking documents and images becoming the carriers of targeted Advanced Persistent Threats (APTs) on the way in, and tools for concealing critical information on the way out.

Fortunately, security technology has evolved alongside the threatscape to help combat new age cyber risks, but a traditional 'stop and block' data loss prevention (DLP) approach is not viable given our reliance on technology for business operation as it hinders communication flow and organizational agility.

The protection and security of information is not the sole responsibility of the CISO alone. The CISO maybe the custodian of information protection, but the information owners are the CISO's peers; HR, Operations, Sales, Marketing, amongst others. Each of these individuals needs to take equal responsibility to ensure that malicious and negligent access in the sharing of critical information is minimized as part of their own and their team's activities.

Defence against attack

In the early years of digital collaboration, the primary security focus was on cyber-attacks which were identified as external actors such as hackers, script kiddies and cyber criminals, each using their skills to intentionally interrupt, damage and extract information or systems of a target organization. Since then, a major shift and re-focus has occurred. The 'insider' threat is now more prevalent and makes up almost 60% of today's information loss, so the information security shift is now on protecting information loss from the inside out. Whereas most external attacks are generally managed reactively, internal data breach risks can be more proactively mitigated, significantly reducing the amount of negligent and inadvertent unauthorized information sharing that happens to cause the breach incident.

Clearswift's **Adaptive Redaction** approaches the challenge of the 'insider' threat from two interlinked perspectives:

1. The technology builds on Clearswift's Data Loss Prevention (DLP) functionality and automatically redacts (removes) content that breaks policy, i.e. the sender should not be communicating or the recipient receiving specific information, immediately - reducing the risk of an internal policy breach. However, the rest of the content is sent – rather than being blocked.
2. Upon redaction, the sender is sent an email to inform them that the communication has been redacted. If the redaction is deemed unnecessary, the sender can immediately request the content to be communicated in its original format, or a change request made to the policy to ensure the content will not be blocked in the future. As well as protecting critical information, the automated feedback provides education on policy around not sharing unauthorized information in the future.

Specifically relevant to point 2 above, most DLP technologies may inform the sender that their content has been quarantined, and in most cases no further interaction happens, unless disciplinary action is involved, penalizing the sender in most cases for something they had not been educated 'not to do'. This 'stop and block' approach is unproductive as it hinders communication flow and ultimately business operation.

Clearswift offers a proactive approach to data loss prevention that protects individual and the business from unauthorized information sharing, significantly reducing the number of outbound information breaches that the organization could experience. This allows the CISO and information security teams to focus their efforts on information security strategy and high level projects, rather than spending their days dealing with 'false positives' and system administration.

Compliance

A major component of Clearswift's Information Governance strategy is the ability to enable organizations to adhere to industry, governmental and internal governance, regulation and compliance (GRC) requirements. There are ever increasing government and vertical industry bodies requiring regulations to protect data that businesses manipulate every day. It has been widely accepted that non-adherence to these new regulations can harm an organization financially as well as reputationally, damaging both business confidence and growth.

In order to immediately safeguard businesses' compliance needs and also ease of deployment, Clearswift's DLP, specifically **Adaptive Redaction** technology, is provided with 'out of the box' policies and dictionaries that provide immediate coverage for: Sarbanes Oxley (SOX), Personal Identifiable Information (PII), Payment Card Industry (PCI), Protected Health Information (PHI), amongst other sensitive data types whilst also ensuring that organizations can meet compliance for data protection laws and regulations, for example:

- General Data Protection Regulation 2018 (Europe)
- Federal Data Protection Act 2018 (Germany)
- Data Protection Act 2018 (France)
- Notifiable Data Breaches Scheme 2018 (Australia)
- Consumer Privacy Act 2018 (California, USA)
- Personal Information Protection and Electronic Documents Act (PIPEDA) 2018 (Canada)

Most organizational compliance policies cover areas of profanity, inappropriate content and unauthorized sharing of confidential information, such as salary details, performance review information, company strategy, etc. Internal policy compliance breaches happen through a number of collaboration tools such as email, social networks and the web, each is distinct and not (in most cases) integrated with each other.

Clearswift's Adaptive Redaction technology reviews all content being shared through email, the web and collaboration applications to ensure compliance across all these communication channels, mitigating the need for 'no use' collaboration tool policies.

Ease of Use

Adaptive Redaction technology resides within the Content Aware – Data Loss Prevention (DLP) category. Commercially available DLP solutions have not changed architecturally for the past 10 years. Their intent is to stop information being leaked out of an organization, via policy-based policing, that quarantines the content for review by a security analyst after policy violation. Unfortunately, traditional DLP is known for its 'False Positives' which have meant inappropriate delays through the 'stop and block' approach which in turn effects business collaboration and the timeliness of business operations. Anything that stops business fluidity is bad, so all too often DLP solutions become shelf-ware, never being deployed or realizing the true business value it creates.

Adaptive Redaction is the bi-directional intelligent removal or amendment of information within a document or image file, email message or web posting as part of a critical information asset protection strategy. The technology ensures that the communicated content meets organization policies for information security. The automatic removal of hidden content (sanitization) and the removal of sensitive content (redaction) combine to provide an advanced Data Loss Prevention and Information Governance solution, utilizing existing (where applicable) DLP policies, minimizing the time to implement and creating a timely return on investment. In essence, Adaptive Redaction strips out those specific pieces of information that would break policy, but leaves the rest to continue to the recipient unhindered. For example, redacting credit card numbers but leaving the rest of an order untouched when it is sent onward to a third party for fulfilment.

The award winning, patented, **Adaptive Redaction** functionality is integrated into the Clearswift Email and Web Gateway products, with solutions available to address:

- **Enhancing Existing Web Security Infrastructure:** Integrated with the Blue Coat ICAP solution (ProxySG) and the F5 ICAP proxy, the Adaptive Redaction functionality is provided within the Clearswift SECURE ICAP Gateway that enhances existing web proxies and their clients with advanced critical information protection.

- **Internal Email Security:** Integrated alongside the Microsoft Exchange Server, the new Clearswift SECURE Exchange Gateway provides advanced DLP and Adaptive Redaction capability for internal email collaboration, identifying and redacting critical information assets before unauthorised communication can occur.

- **Enhancing an Existing Email Security Solution:** Clearswift's ARgon for Email is available for use with any third party email security solution. This not only protects against advanced information threats but can also be used in conjunction with an existing DLP solution to remove the effects of 'stop and block' created by false positives.

All Clearswift solutions are capable of bi-directional Adaptive Redaction (on inbound and outbound traffic), based on policies created by the administrator and performed automatically without any manual intervention. Only a fully-automated solution can be trusted to provide consistent and effective protection. Commercially sensitive information (intellectual property or business plans), national security concerns (such as planned projects or operations), and/or legally restricted assets (NIN, Tax Information, etc.) can all be protected from being uploaded and/or sent outside the organization through redaction. As only the policy identified critical information is removed, the rest continues unhindered, enhancing business continuity through sharing information without breaking corporate, legislative or regulatory requirements. For example, if an email is sent with personal or financial information, the Clearswift SECURE Email Gateway or ARgon for Email solution will remove/redact the information asset and replace it with asterisks (*) then send the new 'redacted' communication, allowing the business to continue interactions while safeguarding critical information. The Sanitization and Redaction functionality occurs in real time with no quarantine required.

Traditional DLP solutions merely "stop and block" the communication, preventing a policy breach but also creating a barrier to the business process flow and possible 'False Positive' situations.

Clearswift's Adaptive Redaction currently includes support for hundreds of different file formats so no matter what digital collaboration channel sensitive information is being shared through, or what file type is being shared in (eg. email messages, documents, images or HTML), Clearswift will inspect all information flow and automatically redact sensitive data to prevent unauthorized exposure.

In addition to data redaction, Clearswift's Adaptive Redaction is also capable of two other operations that remove the risks found in hidden content; Document Sanitization and Structural Sanitization. The traditional method for sanitization of information in communications, including files, is either a manual inspection, or deletion via the application's own facilities, for example the "Inspect Document" option in Microsoft Word. However, success is dependent on the user remembering to carry out the task, which can be easily forgotten or even maliciously bypassed. Adaptive Redaction's Sanitization functionality automatically ensures the consistent application of this functionality to remove hidden sensitive metadata such as Author Names, track changes and other sensitive information attached to documents and files, as well as active content often used to deliver malware into a corporate network.

Structural Sanitization

Active content exists everywhere. Its purpose is to provide the user with a more interactive experience, either on the internet or within a document. Hackers, however, embed their own active content into either purpose-built or compromised documents and files – for example in HTML and Office documents to be downloaded or PDF and images files distributed as email attachments. Since the active code rarely affects the content, it is good practice to simply remove it. Infection of the corporate network by Advanced Persistent Threats (APT) is a CISO's nightmare and embedded active content is the most common way to deliver them. Removing the active content, removes the threat.

Structural sanitization policies are most frequently used on incoming content – so documents and files that are downloaded from the web, or sent through email, can be secured against embedded malware. Deploying Structural Sanitization policies will automatically reduce the risk of targeted attacks such as Phishing or Ransomware campaigns, being successful by automatically removing the delivery mechanism – the active content.

Outgoing documents can also have Structural Sanitisation applied, for example in stripping macros from financial spreadsheets, where the macros are the Intellectual Property or 'secret sauce' for the organization.

Document Sanitization

Most documents and files contain hidden data that is often sensitive. This could be in the document properties, which can disclose both the author and the true date of the document; or in tracked change histories, which can leak sensitive data that the author or authors believe they have removed – such as project details, new product names and prices.

The Australian Federal Police Department experienced a data breach because a document containing 'hidden' metadata information about the subjects of criminal investigations was made public and the critical information was subsequently found. Other examples of sensitive information being exposed in metadata that could have been mitigated by Clearswift's Adaptive Redaction technology have been experienced by some of the largest global companies such as Merck, Microsoft and the British government.

Merck: Metadata revealed that the company deleted vital information concerning the arthritis drug Vioxx, resulting in users having false information on heart attack risk associated with taking the drug.

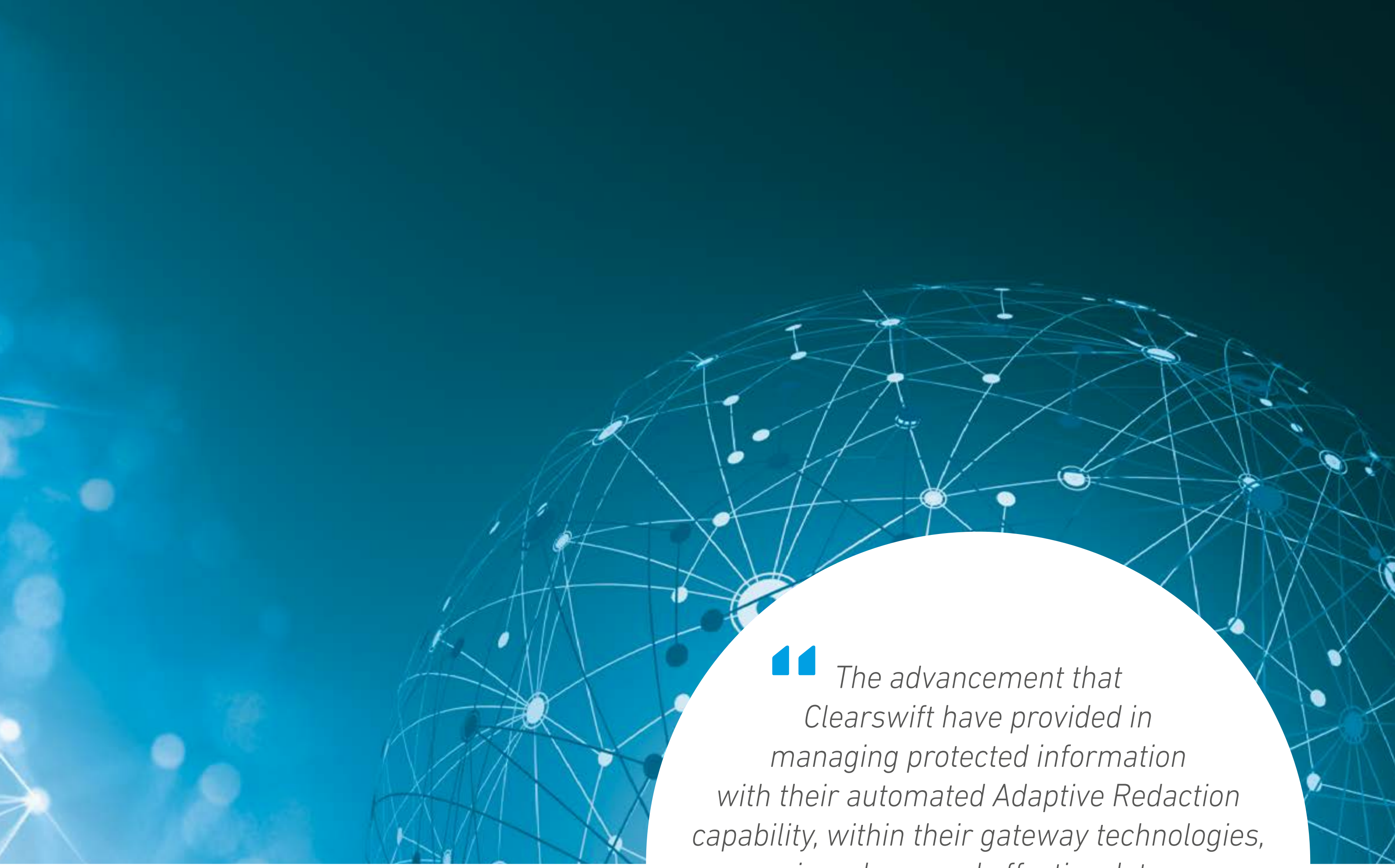
Microsoft: Hidden data in Microsoft Office documents was discovered by the Associated Press and showed that Microsoft's advertising campaign highlighting a customer that switched from Apple to Microsoft was actually a member of their PR firm.

British Government: Released a dossier titled "Iraq: Its Infrastructure of Concealment, Deception, and Intimidation." The government says the dossier is based on high-level intelligence and diplomatic sources and was produced with the approval of Prime Minister Tony Blair. Unfortunately, the dossier still held the original properties from a September 2002 article by university student Ibrahim al-Marashi.

Document sanitization is frequently applied as a policy for documents leaving an organization to ensure that there is no hidden information that might be found and come back to bite the sender in the form of a data, or an embrassing situation.

Many industries have differing requirements for the movement and collaboration of critical information assets. If the policy of the organization is not to utilize the Clearswift Adaptive Redaction technology (i.e. not to block or redact sensitive/private information or IP), there is an option to create a policy within the SECURE Gateways to encrypt the message and/or attachments as an alternative action when the email or attachment is scanned and found to have critical information.

Some DLP solutions have encryption built-in, however not all governments and organizations use the same encryption standards. Clearswift supports all of today's common industry standard encryption technologies, including TLS, S/MIME, PGP, password protected zips and Portal-based encryption. The choice of the type of encryption is policy based on the recipient, making it transparent for the sender and removing operational overhead. This removes any concerns around interoperability and gives clients the assurance that their critical information asset can be securely shared with other organizations without the risk of data breaches occurring.



> *The advancement that Clearswift have provided in managing protected information with their automated Adaptive Redaction capability, within their gateway technologies, is a clever and effective data loss prevention technique to facilitate continuous collaboration while mitigating the effect of potential false positives that inhibit business communication.*

Frank Dickson, Industry Principal Network Security, Frost & Sullivan

Centralized Management

Adaptive Redaction technology resides on each of the Clearswift solution email and web security instances to ensure both availability and scalability. All solution instances can be peered, creating resilient processing groups and their centralized management is provided by a modern, user-friendly web-based user interface (UI). A granular authorization architecture, which is integrated with LDAP or Microsoft Active Directory, enable system administrators with different privileges to perform different system tasks such as policy definition, message management (quarantine), reporting and system monitoring.

All Clearswift solutions can be peered to share policies from a single UI. For example, a customer might have two SECURE Email Gateways, two SECURE Exchange Gateways and three SECURE Web Gateways servicing 5,000 clients. Policy across the entire solution ensures consistency of

Total Cost of Ownership/ Return on Investment

The Clearswift Adaptive Redaction technology provides two levels of Total Cost of Ownership or Return on Investment:

1. **Immediacy:** Organizations can install the standard system with pre-defined policies which include standard dictionaries and tokens within 30 minutes, immediately redacting content that breaches these policies. This level of immediacy can also be implemented in 'Watch mode', where potential breaches are reported on, rather than any actions taken. This provides a level of visibility into potential policy breaches enabling fine-tuning of policies before they are enforced. A pre or post implementation engagement can create more sophisticated policy definitions which can be applied to protect unique critical information, such as intellectual property, as well as minimize 'false positives'.

   A level of automated education will be received by users who are unknowingly or inadvertently breaching policies through the system feedback mechanisms, negating the need to provide specialist data loss education away from their main role.

   Breach events which result in quarantined data can be automatically routed, through LDAP / MS Active Directory, to the senders' manager rather than to a central point, reducing the workload for IT or security analysts who would otherwise be required to resolve the events. Distributed workflow reduces the overall operational costs and enables managers to make decisions on breach severity, rather than relying on someone who may not understand the full intricacies of the business. Managers also have the ability to release original content if required. This is easily carried out by simple clicking a link in the breach event notification.

2. **Risk Mitigation:** A breach of policy that causes critical information assets to be accessed or shared by an unauthorized individual can result in financial and reputational penalties. As an example, when Stoke-on-Trent City Council were fined £120,000 by the Information Commissioners Office (ICO) for sending 'Care Order' information about a juvenile to the wrong person, the Clearswift Adaptive Redaction technology would have stopped this sensitive information being sent to unauthorized recipients, mitigating the breach from happening and subsequently saving the council its £120,000 fine, plus the costs incurred to manage the incident. Subsequent possible breaches would also be negated.

   Organizations can further determine the 'Risk Mitigation' TCO/ROI by using the policy breach reporting facility and applying those breaches to examples that are freely available[4], identifying the financial penalty savings and associated reputational damage.

Sharing of Knowledge

The Clearswift Information Governance strategy, which incorporates the world's first automated Adaptive Redaction technology, encourages the authorized sharing of intelligence, knowledge, information and data with the assurance that unauthorized information is secure – as it will be removed before the recipient receive it. This technology enables continuous collaboration as it overcomes the traditional 'stop and block' inadequacies in existing DLP solutions. It also reduces the effect of false positives as it allows authorized business content to reach the recipient – so even if not all information is received (due to the policy), at least some is, and the recipient is not left wondering what happened to the communication.

Summary

In today's ever-changing business environment, it is essential for automated technologies such as Adaptive Redaction to be implemented as a strategic tool to manage the growth in authorized information sharing and control the information supply chain. While the risks were once perceived as being external only, it is now the internal threat and threats carried unseen in documents which also need to be addressed. Adaptive Redaction is designed to enable secure continuous collaboration across all communication channels.

[4] Privacy Rights Clearinghouse Chronology of Data Breaches 2005 to Present http://www.privacyrights.org/data-breach

clearswift
RUAG Cyber Security

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

As a global organization, Clearswift has headquarters in the United States, Europe, Australia and Japan, with an extensive partner network of more than 900 resellers across the globe.

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading
RG7 4SA
UNITED KINGDOM

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

www.clearswift.com