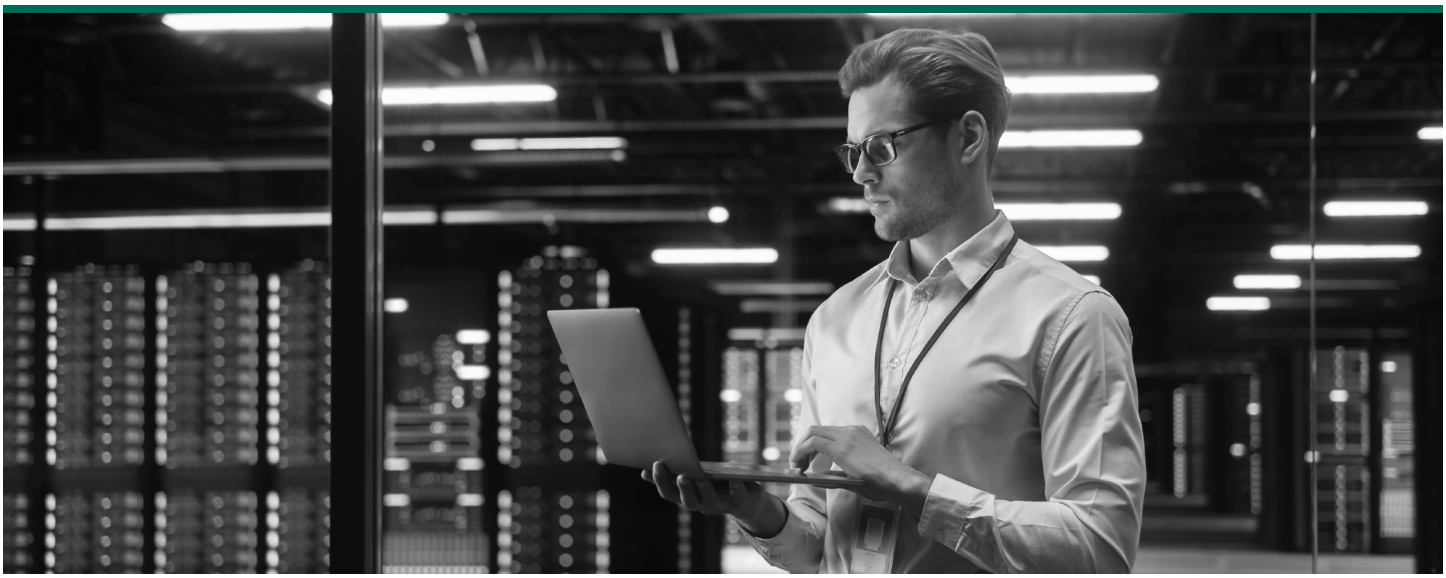
FORTRA

GUIDE (EMAIL SECURITY)

# Fortra Email Security Solutions for Critical Information Protection



Information today is a core component of business differentiation; the value and control of the information both have a direct impact on financial and reputational elements of a business. Our dependence on technology for business operation means that a traditional 'stop and block' data loss prevention (DLP) approach is not viable anymore. The communication flow must remain unhindered. Yet, with increasingly sophisticated cyber attacks designed to go undetected, our need for security is at its greatest!

The Clearswift Adaptive Redaction solution covers a multitude of vulnerabilities in an organization, from the neutralizing the insider threat to protecting critical information and ensuring compliance with data protection laws and regulations. Read on to find out about how our Structural Sanitization and Document Sanitization technology can ensure compliance and protect your organization against active content and Advance Persistent Threats (APTs).

## 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.

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.

With the attacks on organizations are becoming more 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 may be 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.

## Defense Against Attacks

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 cybercriminals, 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 Email 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

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 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:

- HIPAA (Health Insurance Portability and Accountability Act) 1996 (United States)
- Sarbanes-Oxley Act 2002 (USA)
- PCI DSS (Payment Card Industry Data Security Standard) 2004 (worldwide)*
- GDPR (General Data Protection Regulation) 2018 (Europe)
- Federal Data Protection Act 2018 (Germany)
- Data Protection Act 2018 (France)
- NDB (Notifiable Data Breaches Scheme) 2018 (Australia)
- CCPA (California Consumer Privacy Act) 2018 (USA)
- PIPEDA (Personal Information Protection and Electronic Documents Act) 2018 (Canada)
- DORA (Digital Operational Resilience Act) 2023 (European Union)

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 of which is distinct and not (in most cases) integrated with one other. *Any such organizations that deal with or possess credit card information (PII) must be compliant by **March 31, 2025**!

## Caveat: PCI DSS 4.0 DEADLINE IS JUST AROUND THE CORNER!

PCI DSS, released in 2004, was created to ensure any organization that processes or stores credit card information, can do so securely. *However, the new version (4.0) set to roll out by **March 31st, 2025** is even more stringent, requiring organizations to ensure that the PCI standard meets the security needs of the payments industry, including the promotion of security as a continuous process, and the enhancement of validation methods and procedures.


This is where the DMARC email authentication protocol can help satisfy the requirement to set up anti-phishing mechanisms to defend against attacks (as expressly stated in Section 5.4.1 of the guidelines). And you can trust Fortra's Agari to help you achieve this, as we were one of the founders of the DMARC protocol!

## DMARC Email Authentication

A challenge that organizations continue to face involves the complexity of today's email channel. Driven by the addition of new cloud-based email services, the acquisition of new companies, or the set-up of unauthorized email servers by shadow IT, an organization's "email identity" is constantly changing. This creates both a security risk when unauthorized email is sent on behalf of that organization's brand, as well as a potential business problem if legitimate email is blocked from getting to customers.

Luckily, Agari DMARC Protection can automate DMARC email authentication and enforcement for organizations to prevent brand abuse and protect customers from costly phishing attacks by:

- **Improving customer trust** by protecting your brand from being used in phishing attacks;
- **Accelerating DMARC enforcement** and decrease time to reject by automating implementation;
- **Maximizing marketing efficacy** and improve email engagement with trusted communications;
- **Reducing operational costs** associated with email channel management.

Besides helping to ensure seamless delivery of business email as well as inbound enforcement, DMARC helps keep your organization compliant. Most recently, Google and Yahoo changed their requirements to have DMARC authentication set up for those organizations that are bulk senders.

## Ease of Use

Resides within the content-aware Data Loss Prevention 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, affects 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.

Addressing the bi-directional 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, this 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 strategy and Information Governance barrier, utilizing existing (where applicable) DLP policies, minimizing the time to implement and creating a timely return on investment. In essence, while stripping out sensitive data that could break policy, it leaves the rest to continue to the recipient.

The award-winning, patented, **Adaptive Redaction** functionality is integrated into the Clearswift on-premise Email and Web Gateway solutions, 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 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.

All of these 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 appliance 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 in real time with no quarantine required.

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 (e.g., email messages, documents, images or HTML), Clearswift will inspect all information flow and automatically redact sensitive data to prevent unauthorized exposure.

It 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 (APTs) 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 Sanitization 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.

For example, 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 and agencies, such as Merck 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.
- **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 embarrassing 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 blocking or redaction of sensitive data or IP, there is an option to create a policy within the Secure Gateways to encrypt the message and/or attachments after being 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.

## Centralized Management

Adaptive Redaction technology resides on each of the Clearswift Secure Email and Web Gateway 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, userfriendly 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 on-premise Secure Email Gateways, two Secure Exchange Gateways and three Secure Web Gateways servicing up to 5,000 clients. Policy across the entire solution ensures consistency.

## 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 that result in quarantined data are reported on by automatically routing through LDAP/MS Active Directory, rather than any brash 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.

**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, identifying the financial penalty savings and associated reputational damage.

## 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.

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.