

Adaptive Redaction: Data Redaction

A component of Clearswift's unique, award winning Adaptive Redaction technology.

What is Redaction?

Redaction is the removal of sensitive content or details from a document. That content could be commercially sensitive (intellectual property or business plans), a national security concern (such as planned projects or operations), or legally restricted (wide-ranging Personally Identifiable Information – PII). On hard copy, redaction is usually achieved by blacking out the problematic terms. Clearswift's data redaction option achieves the same effect within digital copy by replacing sensitive words, phrases or numbers with a series of Xs.

The data redaction option is available on the Clearswift Secure gateways and within ARgon for Email.

The Need for Redaction

Protecting critical information is no longer an option, but a commercial and legal necessity. Without redaction, such protection can be achieved through straightforward blocking; meaning files containing sensitive data are inspected, recognized and blocked at the gateway. It is an all-or-nothing process, and is the usual (and frustrating) behavior in traditional Data Loss Prevention (DLP) solutions. The problem is that documents containing 99% important and time-sensitive data could potentially be blocked because of one sensitive word or phrase. Adaptive Redaction removes only the sensitive content, allowing the redacted file to continue to its destination without delay.

A more recent use case for this technology is to protect a company from receiving unwanted content. Some online merchants do not want to have to certify their email systems for PCI compliance so redacting Credit Card details eliminates risk of customer credit card being exposed.

The Need for Automated Redaction

Critical information or sensitive data content can be included and left in files either by accident, staff naivety, or – in the worst possible case – malicious intent. The traditional method for finding and removing such content is either by manual inspection or with the help of third-party software; but both cases require user intervention that is easily omitted or content that is overlooked; this process is unreliable and manually time intensive.

Only fully automated data redaction, as provided by Clearswift, can offer an alternative to traditional DLP and support the Secure, continuous collaboration required by organizations today.

Clearswift's redaction option is provided through customer-specified phrases and tokens together with a configurable detection threshold. If lexical analysis of the content reaches the phrase detection threshold, the specified content is automatically redacted.

Redaction Tokens and Supported Document Types

Tokens are slightly different, and can be thought of as templates. For example, if the template for a standard bank card number is detected within a file, all the numbers except the last four are automatically replaced by Xs – and this happens automatically for all bank cards. The redaction option works with multiple document types, including: text, HTML, PDF, RTF and Office 2007+, Open Office, Word, Excel and PowerPoint files.

Bi-directional Redaction

Clearswift's data redaction applies to both outgoing and incoming data. For incoming files it can be used to prevent offensive and possibly illegal information getting onto the organization network

via staff web browsing or received emails. For outgoing files, attachments posted to web based email, on social networking sites or attached to messages being sent through a corporate email system can be checked for sensitive data and cleaned as appropriate.

Adaptive Redaction

Adaptive Redaction is a unique and award winning technology for the proactive approach to critical information protection, preventing sensitive data inadvertently being shared outside or within an organization as well as mitigating inbound targeted attacks. The cornerstone of an Adaptive Data Loss Prevention solution, Adaptive Redaction provides a mechanism whereby the traditional 'stop and block' nature of traditional Data Loss Prevention solutions can be overcome with the automatic removal of only the exact content which breaks policy – leaving the rest of the communication to continue unhindered. Adaptive Redaction can also remove potentially harmful active content from documents before they are opened by the user, enabling the Secure flow of business. For many, the challenge of receiving documents with embedded APTs (Advanced Persistent Threats) can be easily overcome by removing active content from all received documents. The required information gets through unhindered, the malware is blocked.

Data redaction can be used across the Clearswift Secure gateway and ARgon families, and protects the organization's business interests; ensures data protection compliance; and supports the business process.

- **Business interests:** redaction prevents the accidental (or otherwise) export of confidential business critical information
- **Business compliance:** redaction maintains regulatory compliance by preventing the leakage of PII, especially in the use of tokens
- **Business processes:** redaction removes only the sensitive data, without preventing or delaying the delivery of the remaining data



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.