FORTRA

DATASHEET *(Clearswift)*

Adaptive Redaction: Structural & Document Sanitization

Key components of Clearswift's unique, award winning Adaptive Redaction technology.

What is Sanitization?

Sanitization involves cleansing or purging files of dangerous hidden content. That content can be either active (for example, malware), or informational (such as hidden properties). An example of harmful code could be an invisible and malicious script on an otherwise legitimate web page or embedded into a document. Remediation for this requires structural sanitization. An example of hidden sensitive text could be that contained in document properties, which frequently contains user and system names as well as revision information. Whether hidden code or information, both need to be sanitized in order to protect the organization from potential harm. Sanitization is one of the options in the Clearswift Adaptive Data Loss Prevention toolkit.

Structural and Document Sanitization options are available on the Clearswift Secure gateways as well as in ARgon for Email.

The Need for Sanitization

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, insert their own active content into either purpose-built or compromised documents – for example in HTML to be downloaded or PDF documents distributed as email attachments. This needs to be detected. Since the active code will rarely affect the information content, it is a good idea to simply remove it.

Document Sanitization: many office documents contain hidden data that could be sensitive. This could be the document properties, which can disclose both the author and the true date of the document; or 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 Need for Automated Sanitization

The traditional method for file sanitization is either manual inspection, or deletion via the application's own facilities for data; and the possible use of third party software for both. In all cases, however, success is dependent on user or IT department intervention and can be easily omitted.

Only fully-automated sanitization – can be trusted to provide blanket, consistent and effective Structural and Document Sanitization.

Sanitization is an option built into the Secure Gateways and ARgon families. Because the facility is an automatic server-side option it is applied consistently across the whole network, and requires neither user training nor intervention.

Document sanitization, can be used to detect and remove both document properties and revision history for multiple document types, including: PDF, Open Office and Office 2007+ Word, Excel and PowerPoint files. It is a key component in any Adaptive Data Loss Prevention (DLP) solution, protecting hidden data from leaking outside the organization.

Structural sanitization utilizes the Active Content Detection rule and automatically removes active content, such as VBA macros from Office documents, JavaScript, VBScript and ActiveX from

HTML message bodies and HTML attachments; and JavaScript and ActiveX from PDF documents.

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.

Sanitization involves cleansing files of any dangerous content. Where that dangerous content includes hidden or obfuscated code, it can lead to a system compromise by external actors – and will involve all of the loss of reputation and intellectual property, potential regulatory action and cost of remedial action involved in a system breach. Clearswift sanitization will prevent all of this automatically, centrally, without user involvement, and without impinging on organizational processes.

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.