clearswift by HelpSystems

GO ANYWHERE® A HelpSystems Solution

DATASHEET *(Cybersecurity)*

Safely Share Information while keeping your Critical Information Protected

Advanced Threat Protection and Adaptive Data Loss Prevention for Managed File Transfers

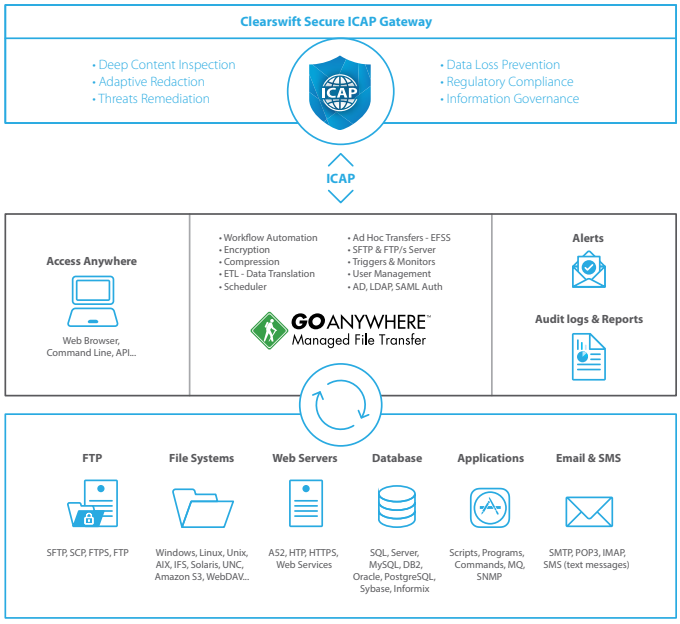
Online sharing of information between customers and trading partners has accelerated collaboration and transformed the digital fabric of today's businesses. However, with the need to share information comes the risk of exposing the wrong content. Files that contain confidential information, either visible within the body of the file or hidden within its metadata, can be mistakenly shared to unauthorized recipients. Equally, the receipt of files from suppliers or partners might open a door to embedded malware; external threats hidden within standard file transfers.

Clearswift and HelpSystems joined technology forces to enable the sharing of information with an unprecedented level of management and security, ensuring that the information transferred is only accessed by authorized parties and is sanitized of malicious threats.

One Collaboration Platform for Secure Information Sharing

Organizations can gain full control of what information is being shared internally, and in and out of the company network. Managed data flows can be easily defined to exchange information through a portal, transfer files through secure FTP or even move files in network shares. By integrating a deep layer of inspection and sanitization through the ICAP protocol, additional information controls can be put in place to enforce adaptive security and compliance policies for all files being transferred. As file sharing traffic passes through this enhanced level of management and security, it overcomes the primary challenge that consumer oriented cloud collaboration tools suffer from.

As all traffic passes through this enhanced level of management and security it overcomes the primary challenge that consumer oriented cloud collaboration tools suffer from.



Clearswift Secure ICAP Gateway

The Clearswift Secure ICAP Gateway is the market leading solution for enhancing your infrastructure. It enables the balance needed to secure and protect critical information with the need to continuously collaborate. Organizations are given the ability to apply deep content inspection, Adaptive Data Loss Prevention and Advanced Threat protection technologies to align the flow of information to the organization's information governance policies, mitigating risk and underpinning compliance requirements.

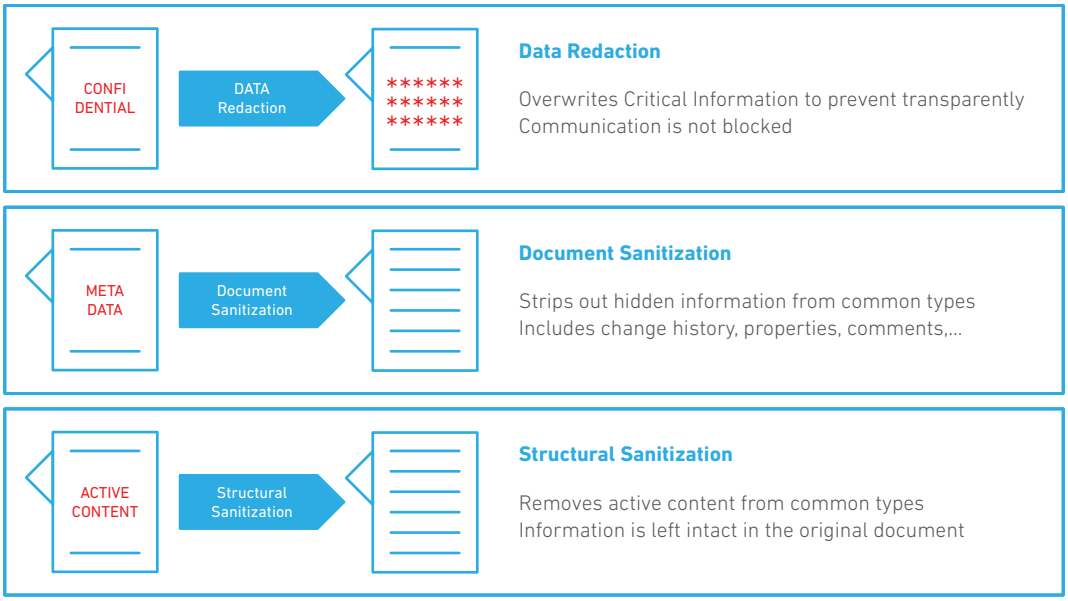
Deep Content Inspection

Clearswift's deep content inspection goes beyond any level of what is traditionally offered in the market. It is not limited by zip/encryption, file size, analysis timing delays, virtual environment evasion techniques or multiple embedded document layers. As a result, it offers amongst the highest detection rates and lowest impact (i.e. nearly eliminates false positives).

Adaptive Data Loss Prevention

Adaptive Data Loss Prevention (A-DLP) is the non-disruptive removal or transformation of data according to policy (rules), to ensure that information shared complies with corporate security policies before it is sent to or received by the recipient (person, application or system). Intelligent policy enforcement is applied to only the information that breaks policy and compliance regulations, while allowing the rest of the business activity to continue without disruptive false positives. Adaptive DLP also sanitizes MFT documents by stripping out hidden metadata (author, username, server names, etc.) and personal information that can be harvested and used for targeted phishing attacks.

Traditional data loss prevention solutions offer a basic 'yes' or 'no' response to attempts to share information, as they lack the architectural design to disassemble, inspect, amend and re-assemble the content 'in its original format'. Adaptive Data Loss Prevention removes this barrier completely by modifying (redacting, blocking or encrypting) the information in real-time according to policies, so as to ensure only the acceptable level of information is shared and received, and that critical information remains safe at all times.



Advanced Threat Protection

Detect and automatically strip out active content in the form of embedded malware triggered executables, scripts or macros used to extract or hold sensitive data hostage, while potentially creating havoc within critical business systems. Clearswift's Advanced Threat Protection sanitizes without delay in delivery, as only the malicious active content is removed, allowing the file transfer to continue unhindered. This morph-free protection against today's leading malware and ransomware (i.e. CryptoLocker, CryptoWall, TorrentLocker, Dridex, Dyre, Black-Energy, etc.) and tomorrow's even more sophisticated variants.

GoAnywhere Managed File Transfer

GoAnywhere MFT™ is a managed file transfer solution which streamlines the exchange of data between your systems, employees, customers and trading partners. It provides a single point of control with extensive security settings, detailed audit trails and reports.

GoAnywhere's intuitive interface and comprehensive workflow features will help to eliminate the need for custom programs/scripts, single-function tools and manual processes that were traditionally needed. This innovative solution will reduce costs, improve the quality of your file transfers, and help your organization comply with data security policies and regulations.

Business Benefits

Secure collaboration

- Information is continuously exchanged. GoAnywhere provides a solution to exchanging information within the organization or with third parties with complete access control.
- The Clearswift Secure ICAP Gateway augments HelpSystems' GoAnywhere ability to control information by applying deep content inspection and Adaptive Data Loss Prevention to enforce more thorough information security policies to prevent data loss, ensure compliance, and prevent advanced malware threats from infecting the organization.
- The combined solution provides a response to an organization's need to exchange information that would otherwise be fulfilled by users with external uncontrolled tools, like online storage websites.

Protection against cyber threats

Any incoming communication can pose a threat to an organization and file exchange is not immune to it. Files received from third parties can include a malicious payload embedded in an innocuous document. Cyber criminals are continuously trying to find the easiest way to attack organizations and using less well protected partners is becoming a common route for attack. Clearswift and HelpSystems offer a combined solution that will stop those threats while allowing business information exchange to continue.

- Malware, and specifically spyware and ransomware, is frequently distributed as active content hidden in common document formats, like Microsoft Office files or PDF documents. Clearswift's Advanced Threat Protection can decompose the files, identify the active content and neutralize it to remove these risks.
- With the flexibility provided by HelpSystems' GoAnywhere workflows, organizations can completely automate their file transfers. By integrating with Clearswift Secure ICAP Gateway, those processes can be checked to identify and neutralize threats that otherwise could easily get to your internal users.

Get complete information control back

- Data privacy regulations such as the EU GDPR require organizations to take full control of what information is being shared and with whom. HelpSystems' GoAnywhere combined with Clearswift's Secure ICAP Gateway provides a means to identify users accessing or sharing information and apply the appropriate policy. By automating the detection and cleansing of information subject to regulations, organizations are able to deal with the increasingly high amount of information exchanged, keeping information under control and allowing business communications to continue.
- Documents are typically reviewed by different team members before being published. But the history of changes along with comments and properties are stored as metadata in the files. This hidden information is also subject to regulatory compliance, in addition to posing a high risk of data loss. HelpSystems' GoAnywhere uses the Clearswift Secure ICAP Gateway to inspect, detect and clean metadata and revision history in files being transferred.

Clearswift and HelpSystems

Share critical information inside and outside your organization with an unprecedented level of management control and security. Together, Clearswift and HelpSystems introduce the world's first integrated Advanced Threat Protection and Adaptive Data Loss Prevention solution for Managed File Transfer (MFT). It's unique automated data redaction and sanitization layer ensures that information shared is only accessed by authorized parties and safe from malicious threats.

For more information, please visit clearswift.com.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.