clearswift
RUAG Cyber Security

Clearswift SECURE ICAP Gateway

The Clearswift SECURE ICAP Gateway (SIG) is the only fully automated critical information protection solution that enables you to take full control of information flowing through your users' browsing traffic. Maximize your existing web security infrastructure by using ICAP to easily integrate unique Clearswift technology, enabling the automatic application of the patented* Clearswift Adaptive Redaction technology to your critical information.

Through implementing the Clearswift SECURE ICAP Gateway (SIG) organizations are able apply deep content inspection, adaptive redaction and data loss prevention technologies to existing web security architectures, with no disruption to the current infrastructure, thereby having the ability to align the flow of information to the organization's information governance policies, mitigating risk and underpinning compliance requirements.

Data loss prevention

Implementation of data loss prevention (DLP) tools often fails due to the lack of accuracy, the complexity of the deployment and the operational overhead they require. Clearswift manages these operational concerns with advanced bi-directional features that restrict unauthorized information sharing, whilst minimizing the false positive occurrences that hinder business productivity.

Connection to existing data sources and flexible lexical analysis allow the ICAP Gateway to accurately identify real data loss possibilities before the breach occurs. Integration with the Clearswift Information Governance Server takes information protection to a new level, not only by detecting the content (fingerprints) of full or partial registered files, but also by tracking every piece of information navigating the Gateway.

Deployment is greatly simplified and integrated with your existing infrastructure through the use of ICAP.

Flexible actions allow for the triggering of workflows as a result of policy violations, or the modification of the content to allow continuous collaboration, in a compliant manner.

Deep content inspection

The Clearswift deep content inspection engine enables organizations to completely disassemble the communication flow to fully understand and protect the critical information being exchanged. This can be applied in web 2.0 applications and be set to adapt to the needs of individual users, roles and departments in the organization.

Context-aware scanning can detect and prevent users from uploading restricted information, while granular policies mean that (un)authorized users, can have a different policy applied, following inspection of the content they intended to share.

Many organizations are unaware of possible unauthorized exchange of critical information, so Clearswift allows these flexible policies to be applied in monitoring mode, to help identify and size the problem, whilst also fine tune policies before enforcement.

Adaptive Redaction

The Clearswift SECURE ICAP Gateway has been developed to extend the unique attributes of Adaptive Redaction** into an organizations existing web security infrastructure. This unparalleled technology allows the modification of content in real time, as it is being analyzed, ensuring that the information being exchanged meets organizational security policies.

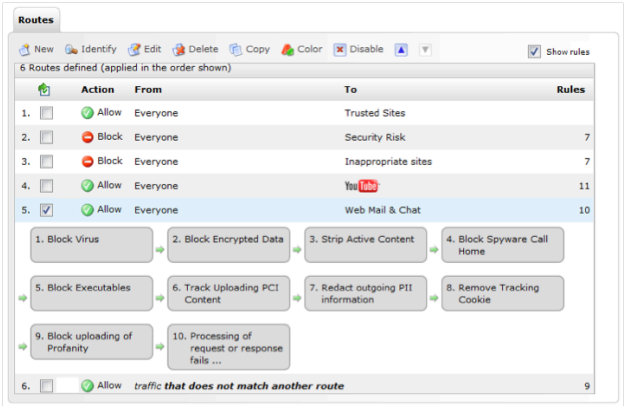
Meta-data, revision history, properties and other hidden and unchecked information such as executables can be seamlessly removed to protect your critical information.

* Patent Pending

** Adaptive Redaction has 3 distinct features. A minimum of one is required at implementation. The remaining 2 optional features are available as additional cost options

Active content in the form of embedded executables, scripts or macros can be detected and stripped to prevent unknown or Advanced Persistent Threats (APT) gain access to your organization's assets. Combined with information analysis rules, redaction allows removal and replacement of confidential or offensive content as it is being down/ up-loaded.

Fig1: Simplified rule enforcement definitions via the administration web interface.



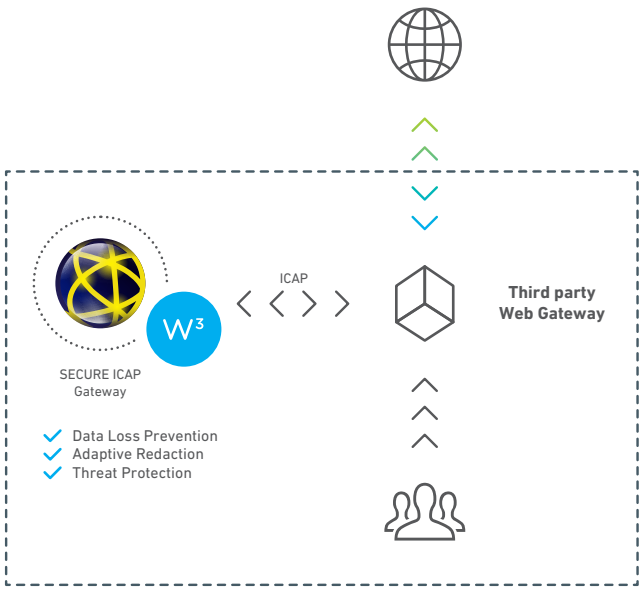
Policy-based web security

The intuitive and powerful user interface means that administration tasks are simplified, reducing errors and minimizing post implementation operational costs. The Gateway's flexible and easy to configure policy comes with comprehensive reporting and auditing functionality.

To ensure you maintain compliance with current and future regulations and to make data loss prevention easier, the Clearswift SECURE ICAP Gateway includes standard templates and dictionaries for common terms that may indicate a potential loss of regulated information and / or sensitive corporate intellectual property (IP).

ICAP interface

Why change your infrastructure when you can complement it to completely satisfy your information security needs? By providing an ICAP interface, the full power of Clearswift's technology can be integrated with supported ICAP gateways. Thus, you can focus on protecting critical information through content inspection with the Clearswift SECURE ICAP Gateway and leave other network related tasks to your existing platform.



Flexible web 2.0 policy controls

Clearswift has made setting policies for the most popular social media sites easy, with specific social networking policy routes for sites such as Facebook, LinkedIn, Twitter and YouTube. This capability allows different departmental policies to be set, and each route comes with pre-populated content rules allowing policies to be defined according to the website's capabilities.

If you're concerned about data leaks via Facebook, webmail or similar sites – you can still allow access but control the outbound data flow. YouTube may contain inappropriate content – you can allow access, but only to authorized videos. The Clearswift SECURE ICAP Gateway's granular policies help you mitigate data loss, legal and reputational risks, and maintain regulatory compliance.

Inbound threat protection

The SECURE ICAP Gateway can be optionally licensed for either Kaspersky or Sophos anti-virus, anti-malware and anti-spyware protection, with automatic updates to provide the latest protection.

These technologies are further enhanced by the Clearswift content inspection engine and Adaptive Redaction, which prevents suspicious scripts and other high-risk content such as executables from being downloaded. Additionally, active content can be removed from files or web pages in real time without delaying the communication.

Advanced URL filtering

The Clearswift SECURE ICAP Gateway includes a complete URL database that contains 84 categories. It covers millions of sites, and represents billions of web pages.

The database includes security risks categories, covering malicious malware and phishing categories, which are continuously updated to provide additional security protection.

Real-time categorization

With more than 50 million new websites per year, the possibility exists that one of your users will visit a site that hasn't yet been categorized. Even though these sites are automatically submitted for categorization, instant action is required and that's when the real-time categorization engine is able to recognize the characteristics of inappropriate sites and prevent access.

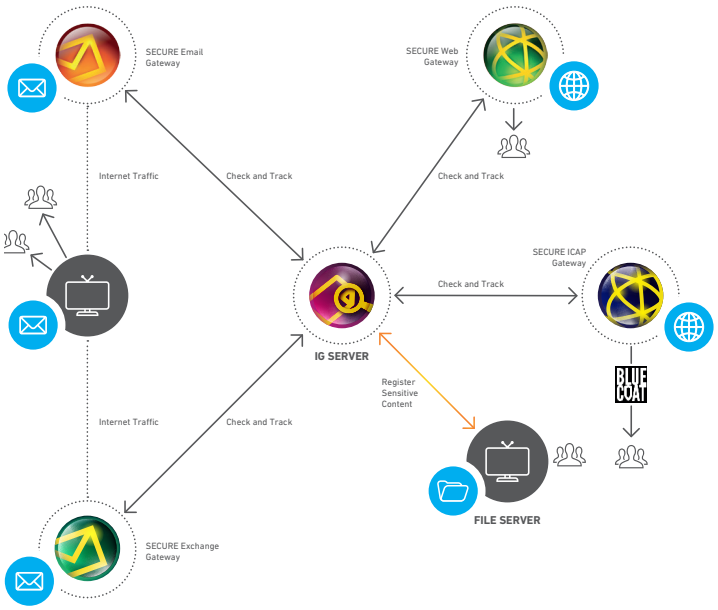
Flexible deployment options

You decide how you want to buy and deploy the Clearswift SECURE ICAP Gateway. It's supplied either as a pre-installed hardware appliance, as a software image that can be loaded on a choice of hardware platforms, or alternatively virtualized in a VMware environment.

Integration with the IG Server

Data Loss Prevention is typically controlled using known keywords or phrases. However, how does an organization deal with sensitive information that is not easy to categorize? Whilst a document may have "Top Secret" in the headers, what happens if someone uses cut-and-paste to copy key sensitive sections into a new uncategorized document? This is where advanced fingerprint algorithms can help to find sensitive documents or even just fragments of them. The Information Governance (IG) Server allows users in the organization to register sensitive data with the IG Server, which stores a digital representation of the whole document as well as the constituent elements, such as paragraphs, images and other embedded content. When connected to the IG Server, the SECURE ICAP Gateway can be used to detect sensitive content traversing the Gateway and take the proper actions if they contravene the security policy.

The IG Server also provides a data tracking service which permits the Administrator to find who may have seen a particular file or document fragment, permitting appropriate remediation as required.



About Clearswift

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.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

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

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
Australia

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1210
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0)221 828 29 888
Technical Support: +49 (0)800 1800556
Email: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

United States
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

clearswift
RUAG Cyber Security

Feature	Benefit
Platform	
ICAP server	Connect to existing ICAP clients within your infrastructure. Supported ICAP client: Blue Coat Proxy SG
Flexible deployment options: Hardware, Software image, VMware vSphere	Provides full flexibility to adapt to your organization's IT strategy.
Active Directory (AD) / LDAP integration	Full user-based policy control for flexible policy and audit reporting by group or individual.
Policy	
Flexible and granular policy controls	Easily define policies to enable and allow Web 2.0 usage while minimizing risk.
Facebook, LinkedIn, Twitter and YouTube policy	Allow access to Web 2.0 sites, but only to content and features allowed by your policy.
Policy direction to provide additional context	Prevent certain file types, e.g. spreadsheets, from being uploaded but allow them to be downloaded.
Customizable block pages	Educate users by providing personalized feedback on their actions.
Data Loss Prevention	
Adaptive Redaction: Data Redaction *	Modify content in real time to avoid delaying business processes while protecting sensitive information.
Adaptive Redaction: Document Sanitization*	Prevent hidden information within documents (e.g. metadata, properties, or quick save data) from being leaked.
Adaptive Redaction: Structural Sanitization*	Detect and strip active content from documents and HTML pages to protect from APT's and unknown threats.
Clearswift Information Governance Server integration**	Detect full or partial files being uploaded or downloaded. Allow tracking of any information traversing the SECURE ICAP Gateway.
External data source connection	Accurately identify data from your databases that is found in transit.
Lexical analysis and regular expression rules	Search file content for key words and phrases using simple or more complex pattern matching to identify sensitive data in over 200 character encodings.
Pre-defined sensitive data templates	Identify credit card, bank account, social security and national security numbers.
Compliance dictionaries	Multi-language editable compliance dictionaries including GLBA, HIPAA, SEC, SOX, PCI and PII to minimize risks.
Predefined Tokens	Multiple, including: Credit Card, Social Security, IBAN, National Insurance, Tax file number, German Identity, Business Identifier Code
MIMEsweeper true 'binary file-type' identification	Accurate binary based identification with the ability to define own file signatures.
Hygiene	
Bi-directional virus and anti-malware scanning**	Stops known and unknown malware infection entering or leaving the network.
Bi-directional anti-spyware scanning	Stops spyware, adware, key loggers and spyware call homes from infected machines.
URL filtering database with 84 categories	Prevents access to inappropriate sites and provides context for web reports.
Malware, Phishing and Spyware categories	Prevents access to known high risk URLs and sites with hourly updates.
Real-time categorization engine	Prevents access to new or uncategorized sites with inappropriate content.
Content aware recursive inspection	Decomposes the requests and responses to provide true detection of content like executables even when embedded in other file types or compressed containers.
Management and Reporting	
Intuitive web-based interface	Ease of use and no requirement to learn complex syntax or operating system commands.
Pre-defined customizable reports	Easy to modify, run and share graphical reports with intuitive drill down.
Scheduled reporting	Allows create once, run and distribute many times with circulation via email.
Multi-Gateway consolidated reporting	Consolidated reporting view of user's activities for easier analysis and sharing of management data.
SNMP, SMTP Alerting	Facilitates 'lights out' data center deployment using SNMP or SMTP management alerts.

* A minimum of one option is required at initial implementation. The remaining 2 optional features are available as additional cost options

** Cost option