CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift SECURE Web Gateway

Remote Client Protection

Protect your critical information, everywhere.

The boundaries of organizations are blurring. Data needs to be accessed from everywhere. Remote users are becoming even more common and they need access to critical information. But this information needs to be protected. Clearswift SECURE Web Gateway Remote Client is a complete security solution enabling you to take full control of information flowing through your users' browsing traffic whether they are on-premise or remote.

In today's climate, organizations need to be prepared to manage users who work away from a primary base or static office environment, whether working from home, travelling on business, at hotels or using a public Wi-Fi. As users travel, their corporate information moves with them and so the same level (if not more stringent) of protection and security is required as though they were working on site.

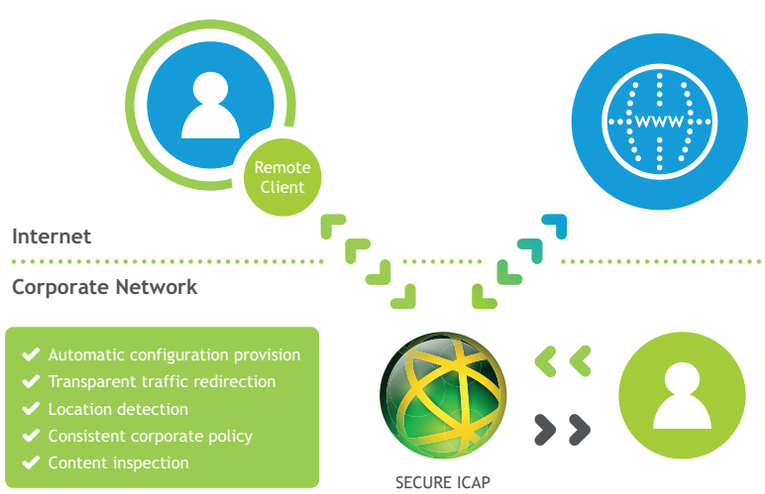
Clearswift SECURE Web Gateway with Remote Client allows organizations to take complete and granular control over the information that users access or share online, regardless of their location. Consistent policy is applied, which goes far beyond simply keeping your networks free of viruses, inappropriate content and harmful executables. It enables enforcing the corporate flexible content policy, whether it's limiting recreational browsing, or preventing critical information from leaving the network.

Deploying the Clearswift SECURE Web Gateway alongside the Clearswift Remote Client, enables technologies such as Clearswift Web 2.0, deep content inspection, unique adaptive redaction and data loss prevention technologies to be applied consistently to all of your users.

Easy deployment, easy configuration

The Remote Client is easy to deploy; a small agent footprint exists on the device and enables users to connect to the corporate network. It is as simple as that.

The entire configuration is automatically detected and applied. The next time your users connect remotely to the Internet, the agent will redirect their traffic to the corporate Gateway to enforce the content security policy as if they were in their corporate office.



Securely connected

The communication between the device and the SECURE Web Gateway is authenticated and secure. Information flows are therefore managed and the content security policy applied before the information goes unencrypted out to the Internet.

Policies are applied as if locally connected, so user authentication, departmental policies, time quotas and any other organizational policies are all in place.

Complete control

Remain in complete control of what users are allowed to do when using the Remote Client. A specific number of grace periods can even be enabled to allow your users to register with Wi-Fi services, both the number and duration of them can be defined.

For unsuccessful connections, you have the ability to decide whether to permit or block all connectivity to keep your organization's assets protected.

Adaptive Redaction

No organization wants critical information to be exposed. However, blocking policies are always a concern, as they hinder essential business collaboration, are prone to false positives that result in denying valid business processes. So the typical approach is to simply do nothing.

Clearswift, aware of these concerns, has released a world-first, unique Adaptive Redaction technology. 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. Breach of policy is actioned either via remediation, quarantine, management release approval amongst others and the data flows are not blocked, ensuring constant, secure collaboration.

Extended data loss prevention

Information is no longer static. Its value resides in the ability to be shared and communicated. This involves an inherent risk when critical information is somehow mistakenly shared. With the mobility of employees and information access from various smart media devices, this risk simply becomes ubiquitous, so today there is a need to keep protecting the information even outside the physical perimeter of the organization.

Clearswift SECURE Web Gateway manages the operational concerns of data loss prevention policies with advanced bi-directional features that restrict unauthorized information sharing, whilst minimizing the false positive occurrences that hinder business productivity.

The Remote Client moves this protection with the user. Whether they connect to an open guest network, airport Wi-Fi or through mobile networks, information stays protected.

Connection to existing data sources and flexible lexical analysis allows the SECURE Web Gateway to accurately identify real data loss possibilities before the breach occurs. Integration with the Clearswift Information Governance Server allows the detection of content (fingerprints) of full or partial registered files, and tracking every piece of information crossing the Gateway.

Deep content inspection

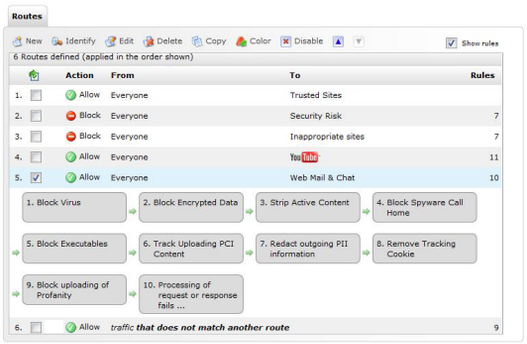
The Clearswift deep content inspection engine enables the ability to completely disassemble the communication flow to fully understand and protect the critical information being exchanged. This can be applied in web 2.0 applications and be set to adapt to the needs of individual users, roles and departments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

Policy-based web security

The intuitive and powerful user interface means that administration tasks are simplified, reducing errors and minimizing costs. The Gateway's flexible and easy to configure policy comes with comprehensive reporting and auditing. Policies are defined on a per user/department/corporate basis, regardless of whether the user is locally or remotely connected.

To ensure you maintain compliance with current and future regulations and to make data loss prevention easier, standard templates and dictionaries for common terms to prevent data losses or regulations violations are included.



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 collaboration tools – 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.

Inbound threat protection

Inbound threats become an even bigger risk when users connect remotely. Internet access through free open WI-FI networks is protected by encrypting the traffic and redirecting it for inspection. The SECURE Web Gateway comes with 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 functionality, 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 Web 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 websites, 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.

Integration with the Clearswift 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? 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 Web Gateway can be used to detect sensitive content traversing the Gateway and take the proper actions if it contravenes the security policy. With the Remote Client, this protection is extended to users connecting remotely.

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.

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

About Clearswift

Clearswift is an information security company, trusted by thousands of clients worldwide, to provide adaptive cyber solutions that enable their organizations to secure business critical data from internal and external threats.

Built on an innovative Deep Content Inspection engine managed and controlled by a fully integrated policy center, Clearswift's solutions support a comprehensive Information Governance strategy resulting in data being managed and protected effortlessly.

As a global organization, Clearswift operates out of offices in Europe, Australia,Japan 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
5th Floor
165 Walker Street, North Sydney
New South Wales, 2060
Australia

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

Germany
Clearswift GmbH
Landsberger Straße 302
D-80 687 Munich
Germany

Tel: +49 (0)89 904 05 206
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: 0066 33 812 501
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

Feature	Benefit
Remote Client	
Encrypted connection	Communication is encrypted from the user to the corporate Web Gateway.
Automatic configuration	Deployment and configuration is highly simplified as it is automatically applied when first connected on premises.
Active Directory (AD)/LDAP integration	Full user-based policy control for flexible policy and audit reporting by group or individual.
Automatic detection of connected network	Automatically detects when users connect to the corporate network or remotely, to only redirect traffic when needed.
Customizable grace period	Number and duration of grace periods can be configured through the web interface on the SECURE Web Gateway.
Optional lock-down if connection is not possible	In case the connection to the corporate Web Gateway is not possible, network accesses can optionally be blocked.
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	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 Protection	
Adaptive Redaction: Data Redaction (Optional)	Modify content in real time to avoid delaying business processes while protecting sensitive information.
Adaptive Redaction: Document Sanitization (Optional)	Prevent hidden information within documents (e.g. metadata, properties, or quick save data) from being leaked.
Adaptive Redaction: Structural Sanitization (Optional)	Detect and strip active content from documents and HTML pages to protect from APT's and unknown threats.
Clearswift Information Governance Server integration (Optional)	Detect full or partial files being uploaded or downloaded. Allow tracking of any information traversing the SECURE Web 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.
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.