FORTRA

DATASHEET *(Cybersecurity)*

Clearswift Secure Web Gateway

The internet is now considered an extension of an enterprise's own infrastructure. With the ever growing adoption of cloud-based services such as Salesforce.com and Office365, alongside employee use of the internet whilst at work, organizations need to ensure that the content and information that exists and is viewed online is both appropriate and permitted. Protecting themselves from any critical information data breaches resulting in serious financial penalties or loss of business reputation is paramount. The Clearswift Secure Web Gateway (SWG) offers a proactive, policy-controlled web gateway solution transforming the web from a high-risk environment to a secure resource, tailored exactly to your organization's needs.

Clearswift's award-winning deep content inspection capabilities facilitate the competitive advantages inherent in open and safe communications. SWG goes beyond simply keeping your network free of viruses, inappropriate content and harmful executables. It enables complete granular control over the information that is accessed or shared online, whether it's limiting or monitoring recreational browsing or preventing the inappropriate leak of critical information. The Clearswift Secure web gateway enables an organization to reap all the benefits that collaborative web 2.0 technologies have to offer, safe in the knowledge that Clearswift's unique Adaptive Redaction functionality allows for content to be dynamically modified to make the content 'safe' rather than have to 'stop and block' the collaboration ensuring a proactive approach to critical information protection.

Data Leak Prevention

By using the lexical analysis capabilities of the Secure Web Gateway, accidental data leaks can be detected and prevented– one of the scourges of modern corporations. Even hidden information in metadata can be removed from documents while being uploaded. Images can also be scanned using Optical Character Recognition (OCR) to prevent sensitive information from being exfiltrated. Either by searching file uploads for key watermarks within the documents that indicate sensitive data or by understanding the content, the leak can be identified, stopped and proper repercussive actions taken.

To ensure regulatory compliance is maintained and to prevent the leak of critical information, SWG has the ability to receive feeds from existing databases, as well as standard templates and dictionaries of common terms that may be indicative of a communication containing sensitive data.

Depending on the content, the use of Adaptive Redaction enables the sensitive data to be monitored, and if required, automatically redacted therefore allowing the communication to continue but with the information contravening policy removed. This process can be applied both to document properties and to any change history that potentially houses sensitive data.

Deep Content Inspection

Intelligent, deep content inspection enables risk-free social media communications – Clearswift's sophisticated deep content inspection engine can recognize the difference between an innocent Tweet and a potentially damaging one. Context-aware scanning can detect and prevent users from uploading restricted information and images. The combination of 'Content' and 'Context' aware policies dramatically reduces the opportunity for false positives, providing less resources to manage an efficient data loss prevention strategy.

Policy-based Web Security

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

Flexible Web 2.0 PolicyControls

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; in turn this means that employees are free to use the social web to innovate and grow your business. High quality reporting and auditing features give actionable insight into the way information is used on your networks, driving inbound threat protection, preventing data leakage and maintaining productive use of company network resources.

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

Predefined Regular Expressions for PII Personally Identifiable Information) and PCI (Payment Card Industry)

- National insurance and ID number
- Credit card numbers
- Social security number
- International Bank Account Number (IBAN)

Editable Compliance Dictionaries

- Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Securities and Equities Commission (SEC) and Sarbanes Oxley (SOX)

Contextual Policy Rules for Facebook and Other Web 2.0 Sites

- Inbound threat protection
- Outbound data leakage
- Specific Facebook rules

This intuitive and powerful user interface means that administration tasks are simplified, reducing errors and operational costs.

Inbound Threat Protection

The Secure Web Gateway features integrated Cloud-assisted Avira or Sophos anti-virus, anti-malware and antispyware protection, with automatic updates to provide the latest protection. The AV engines also support heuristic and behavioural scanning is available.

These technologies are further enhanced by the MIMEsweeper content inspection engine, which prevents suspicious script and other high-risk content such as executables from being downloaded. Even more, active content can be detected in documents and HTML to be optionally sanitized.

Text in web content can be searched, using both context and direction, and a policy applied.

- **URL:** Prevent inappropriate searches or allow them but inform HR
- **Documents:** Prevent sensitive data being uploaded to Web 2.0 sites or via webmail
- **Web Page:** block pages with profanity that might offend
- **HTTP headers:** Block old un-patched browser versions

Advanced URL Filtering

The Clearswift URL database contains 84 categories and is updated daily. It covers millions of sites, and represents billions of web pages. Also operates an additional database covering malicious malware and phishing categories, which is updated hourly.

Real-time Categorization

This functionality detects new inappropriate sites, remote proxies, pornography and hacking, that can appear or occur on a daily basis. SWG's real-time categorization engine is trained to recognize the characteristics of these sites and prevent access.

Browse Time and Quota Policy

Sophisticated policies enable both definition of 'time of day' and 'total amount of time per day' any user can browse selected categories of a given site.

Flexible Deployment Options

You decide how you want to buy and deploy the Clearswift Secure Web 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 and public Clouds such as AWS and Azure or alternatively virtualized in a VMware environment.

Feature	Benefit
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.
Time and quota user web access rights	Define time-of-day and time-quota policies for selected websites to limit access.
Policy direction to provide additional context	Prevent certain file types e.g. spreadsheets, being uploaded but allow downloading.
Acceptable usage 'inform' pages	'Inform pages' highlight individual web usage is being monitored and is subject to company policy.
Hygiene	
Cloud assisted anti-virus with heuristics and behavioural 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 and infected machines.
URL filtering database with 84 categories	Prevents access to inappropriate sites and provides context for web usage 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 which contain inappropriate content.
Content aware inspection to 50 levels	Stops executables including ActiveX being downloaded even when embedded in other file types or compressed containers.
Structural sanitization*	Detect and remove active content like macros and scripting inside documents or HTML content.
Content inspection	
Optical Character Recognition (OCR)	Extracts text from attached images and images in documents, allowing them to be scanned for policy violations and subsequently redacted.
MIMEsweeper 'binary file-type' identification	Accurate signature based identification with the ability to define own file signatures.
Full HTTPS inspection and analysis	See inside encrypted traffic to prevent malware and outbound sensitive data leaks.
Lexical analysis and regular expression rules	Search communication content for keywords and phrases using simple expressions or more complex pattern matching, with regular expressions, Boolean and locational searches to identify sensitive data patterns. Create custom tokens to enable more refined search profiles to reduce false positives and also check against Structured Data sources.
Adaptive Redaction	Automatically redact text from commonly used applications based on predefined keywords or tokens. Remove unwanted or sensitive file history information including custom and even "unexpected" (or rogue) properties. Detect active content and remove any traces of it.
Pre-defined sensitive data templates	Identify credit card, bank account, social security, personal IDs and national security numbers.
Compliance policies	Multi-language profanity and editable compliance dictionaries including GLBA, HIPAA, SEC, SOX, PCI, PII and GDPR to minimize reputational and terminology risks.
Management and reporting	
Intuitive web-based interface	Ease of use and no requirement to learn complex syntax or Linux commands. Roles Based Access Control with AD authentication for administrative roles.
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.
Active Directory (AD) and LDAP integration	Full user-based policy control for flexible policy and audit reporting by group or individual.
Scheduled spyware reporting	Better control of spyware and the identification of user devices requiring remediation.
SNMP, SMTP and SYSLOG Alerting	SNMP or SMTP management alerts facilitates 'lights out' data center deployment and log files can be automatically consolidated using SYSLOG.
Secure HTTP caching proxy	Supplied either as a pre-installed hardware appliance, as a software image that can be loaded on a choice of platforms, or alternatively virtualized in a VMware environment.

* Cost option

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.