clearswift
RUAG Cyber Security

Adaptive Cyber Security & Data Loss Prevention

Clearswift Product & Solution Guide

www.clearswift.com

Table of Contents

Introduction

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to collaborate securely and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution that avoids the risk of business interruption and enables organizations to gain visibility and control of their critical information 100% of the time.

Our track record in innovation includes developing many of the features the security industry now considers standard, including:

- Deep Content Inspection (DCI)
- Policy-based encryption
- Inbound and outbound content scanning across multiple communication channels
- Internal content scanning for collaboration software
- SPF, DKIM/DMARC features

Clearswift continues to lead the IT security industry with the deployment of production-ready appliances, virtual gateways, hosted and managed Cloud deployments. Using powerful, effective and tested content-aware policies, these solutions protect our clients, employees and trusted third-parties from today's information borne threats.

With a strong focus on technology innovation, Clearswift is constantly developing our product portfolio with the latest features and functionality to combat information security threats as and when they evolve. Furthermore, our solutions adapt with business practice change driven largely by the increased adoption of Cloud collaboration applications and evolving data protection regulations.

An adaptive approach to securing your critical information

Securing business critical information from internal and external threats

With web and email traffic still being the primary point of exit for organizational information sharing, and the entry point to receive content from trusted 3rd parties, it makes sense to protect these key collaboration channels with consistent and complementary technologies. Whether you have an on-premise or cloud based security strategy, a Clearswift solution can be used in multiple deployment modes to replace or augment your existing technology.

Web and Email Gateways can be joined together so that they can share policy items such as compliance dictionaries, templates and rules, and have policy defined via a single console.

Many of today's security solutions can be difficult to use and manage. Clearswift solutions have been designed with the administrator and the user in mind; focused on masking the sophistication of the solution, making them both easy to use and easy to manage.

Easy to use, efficient to manage

Today, organizations have a cloud first attitude and Clearswift offers a variety of deployment options and combinations to meet the business requirements of our clients. Our products can be deployed in public cloud systems such as AWS or Azure, and for the organization who cannot or will not deploy in the public cloud, we can deploy on vSphere and Hyper-V as well as bare metal servers.

Customers can also choose Clearswift hosted or managed deployments to reduce day-to-day system maintenance chores.

Preconfigured and sample rulesets, including dictionaries for PCI and PII, coupled with an intuitive user interface is provided for each configuration of client-specific policies. With a consistent policy management framework and user interface style across products, system administrators can be easily cross-trained between products, reducing training overhead.

Administrators will save time thanks to automated downloads of updates, scheduled reporting, off-box backups, database optimization and application monitoring and alerting.

Common functionality and consistent policies

The Clearswift SECURE Gateways rely on shared core technology to make them easy to deploy and manage as well as ensuring consistency across the different communication protocols. Clearswift made its name with its innovative, world-class Deep Content Inspection Engine, and it is this same engine which lies at the heart of all the Gateways.

Deep Content Inspection

Deep Content Inspection identifies sensitive data and active code during filtering of information through the Gateways. The Deep Content Inspection engine is responsible for:

- True file type detection
- Text extraction
- Text scanning
- Image scanning
- Active code detection
- Data modification

Clearswift has developed its own innovative scanning and extraction engine, enabling it to determine additional important information. The ability to detect whether text is in a document's header, footer or main body, or in image files, for example, becomes important when designing detection policies. Without this additional intelligence, false positives can become unmanageable and the solution ineffective. Deep understanding of file types and the information they contain also enables the files to be modified and critical information that could cause a data leak or potentially dangerous code to be removed.

Once the inspection has been carried out, security and data loss prevention policies can be applied to meet both company and regulatory compliance requirements.

Data Loss Prevention

Data Loss Prevention (DLP) is built in as standard for the SECURE Gateways being passed from the Deep Content Inspection engine in order. DLP is direction agnostic, which is to say that it can be used to prevent information from entering an organization (unwanted data acquisition) as well as leaking out.

The evolution of cyber threats along with the continual increase in legislative requirements has seen DLP technology become essential for organizations of all sizes. Once thought to be only the preserve of global organizations, it can now be easily deployed by even the smallest.

Scanning for textual items within messages and attachments allows for the detection and redaction of sensitive information before it leaves your Gateway, including:

- Full Unicode support allowing keyword search of single and double-byte text
- Support for regular expressions based on POSIX standards
- Multiple pre-defined dictionaries supplied as standard (GLBA, SEC, GDPR, SOX, etc.)
- Search patterns constructed from words, phrases and tokens
- Predefined policies for PCI and PII (credit card, social security, passport numbers, identities, etc.)
- User definable policies which can be combined with existing expressions and tokens
- Boolean AND, OR, XOR and ANDNOT
- Positional operators NEAR, BEFORE, AFTER and FOLLOWEDBY
- Full and partial document fingerprinting using a centralized multi-protocol solution (Clearswift Information Governance Server)
- Exact Data Matching to look for sensitive content based on structured data exports
- Document properties such as document classification markers

The key to an effective DLP solution is ease of policy definition and flexibility in its use. A simple approach enables even the smallest IT department to put effective policies together quickly and efficiently.

While traditional DLP solutions operate with a 'stop and block' action on information which violates policy, Clearswift's Adaptive Redaction technology offers further flexibility, leading to an Adaptive Data Loss Prevention (A-DLP) approach; one that is better suited for today's digital landscape and collaborative organization.

Adaptive Redaction

The Clearswift SECURE Gateways and ARgon for Email have options for Adaptive Redaction to be included as part of the A-DLP actions. Standard DLP relies on detecting business critical information and blocking it at the Gateway. However, Adaptive Redaction provides the option to automatically remove the data that violates policy and allow the remaining information to continue to its destination. There are three common Adaptive Redaction options:

1. Data redaction

This is the policy-based removal of words, phrases and tokens. In order to maintain document integrity, these are replaced with an alternative character, for example '*'. For credit card tokens, there is an option to replace everything but the last four digits.

2. Document sanitization

Today's electronic documents contain information other than that which can be seen - there is hidden meta-data, such as document properties, i.e. name, subject, keywords, printers, windows version, etc. as well as revision history. This can all be automatically removed to prevent accidental data leaks.

3. Structural sanitization

With the ever increasing risk of malware in common file formats (e.g. Microsoft Office documents, Adobe pdf, etc.), the Gateways can detect and use Content Disarm and Reconstruction (CDR) techniques to remove Active Content from files. The sanitized document is delivered to the intended destination without the associated security risks present.

Adaptive Redaction, like DLP, is direction agnostic, so it works in both directions. As well as being used to prevent social security numbers from leaving the organization, for example, it can also prevent them from being received. Web pages which contain javascript can now be disabled from executing, ensuring a safe viewing experience. Organizations who use social media sites can often find employees unable to view a page due to offensive comments, Adaptive Redaction ensures that this problem does not occur.

In the case of business proposals, it is not uncommon to base them on an existing business proposal for a different client. This has caused embarrassment in the past with the client able to look at revision history or meta-data and see the original information. Document sanitization ensures that this won't happen.

Threat protection

While much is made in the press as to the effectiveness of threat protection measures such as Anti-Virus (AV) solutions in today's age of Advanced Persistent Threats (APTs) and other advanced threats, AV is still an efficient method of dealing with the millions of viruses and other malware which are present in email and on the Internet. Clearswift offers Cloud-assisted AV solutions from Sophos, Kaspersky and Avira that offer heuristics and behavioral scanning. AV definitions are updated automatically by the Gateways to ensure that the infrastructure is always protected. Many organizations prefer the additional layer of protection that running products from different AV vendors at the Gateway and endpoint offers.

The importance of people

Understanding the information that is being sent is only part of the story. Clearswift Gateways integrate with directory systems such as Active Directory to provide additional context, enabling policies which take both people and role based groups into account. This means that the CEO can have a different policy from an individual based in finance, for example, or a group of engineers. This added dimension of policy definition ensures that the system remains flexible, easy to deploy and simple to manage.

Reporting

Any security solution today needs to be intrinsic to an Information Governance or compliance programme.

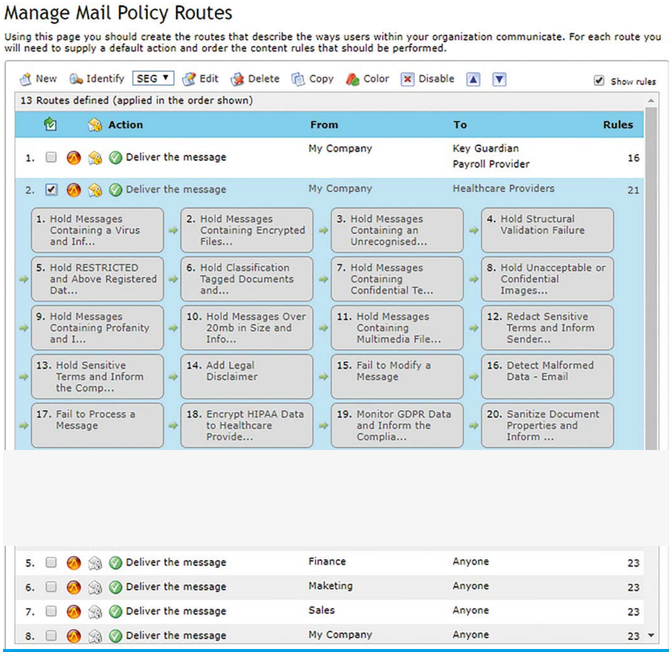
With more emphasis on information consolidation the growth of Security Information and Event Management (SIEM) solutions, the Clearswift SECURE Gateways are compatible with various platforms, including:

- RSA Envision
- HP ArcSight
- Splunk
- "ELK"

Gateways can be monitored using SNMP/SCOM management stations and they can also create SMTP and SNMP alarms to alert administrators to issues more quickly. When an issue is discovered, easy access to granular log files minimizes the time to resolution.

The Clearswift SECURE Gateways offer extensive reporting facilities in support of these requirements, enabling system administrators to rapidly create both management and real-time reports. As reports are often required to be shared, these can be created in different formats, whether that be HTML or PDF as a textual representation, or whether the data needs to be exported to CSV for import into a spreadsheet.

All changes to system configurations are audited, and with role based access control it is simple to delegate responsibilities and detect whether personnel are attempting to circumvent policy.



Manage Mail Policy Routes

Using this page you should create the routes that describe the ways users within your organization communicate. For each route you will need to supply a default action and order the content rules that should be performed.

13 Routes defined (applied in the order shown)

		Action	From	To	Rules
1.	□	Deliver the message	My Company	Key Guardian Payroll Provider	16
2.	☑	Deliver the message	My Company	Healthcare Providers	21

1. Hold Messages Containing a Virus and Inf...
2. Hold Messages Containing Encrypted Files...
3. Hold Messages Containing an Unrecognised...
4. Hold Structural Validation Failure
5. Hold RESTRICTED and Above Registered Dat...
6. Hold Classification Tagged Documents and...
7. Hold Messages Containing Confidential Te...
8. Hold Unacceptable or Confidential Images...
9. Hold Messages Containing Profanity and I...
10. Hold Messages Over 20mb in Size and Info...
11. Hold Messages Containing Multimedia File...
12. Redact Sensitive Terms and Inform Sender...
13. Hold Sensitive Terms and Inform the Comp...
14. Add Legal Disclaimer
15. Fail to Modify a Message
16. Detect Malformed Data - Email
17. Fail to Process a Message
18. Encrypt HIPAA Data to Healthcare Provide...
19. Monitor GDPR Data and Inform the Complia...
20. Sanitize Document Properties and Inform ...

		Action	From	To	Rules
5.	□	Deliver the message	Finance	Anyone	23
6.	□	Deliver the message	Maketing	Anyone	23
7.	□	Deliver the message	Sales	Anyone	23
8.	□	Deliver the message	My Company	Anyone	23

Easy to use policy definition:
where policies are being applied and what they are looking for

Clearswift SECURE Email Gateway

The Clearswift SECURE Email Gateway (SEG) is a multi-award winning, market leading solution for secure email collaboration. Used by thousands of organizations across the globe, the solution enables simultaneous protection from inbound cyber attacks and outbound data loss, without hindering communication flow.

With the most advanced security and data protection features built in, the Clearswift SEG offers the highest level of protection for secure collaboration across email - mitigating cyber threats and data leak risks, protecting critical information.

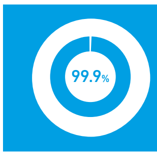
Threat protection

The Clearswift SECURE Email Gateway comes with multi-layer threat defenses, with a choice of multiple AV engines (Sophos, Kaspersky and Avira) and true file type detection coupled with Active Code detection/sanitization to identify unknown threats. The AV engines use heuristics and Cloud based signature pre-warnings of new malware exploits to reduce the chance of zero-day attacks.

A multi-layer spam defense consisting of network based reputation pre-detection followed by content based message analysis permits for a detection rate in excess of 99% with minimal false positives. Spam management can be managed by end users using portal, digests, Outlook plugins and iOS devices.

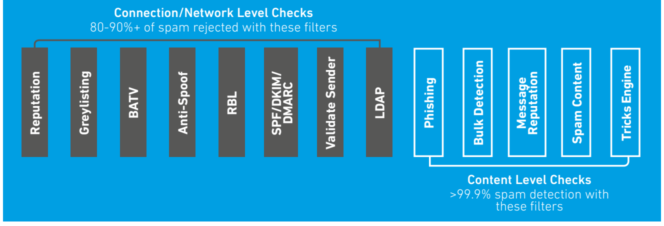
As with anti-virus, the definitions are constantly updated to ensure comprehensive up-to-the-minute protection against all the latest threats.

Message Sanitization permits URLs, Active Code and HTML to be removed from the message, preventing the risk of malware or Ransomware activating, or a link in a Phishing email being inadvertently clicked by a member of staff.



The nuisance of spam continues to be a burden for organizations and the SEG combines a number of filtering technologies to deliver 99.9%+ detection rates.

Multiple Technologies Provide Comprehensive Spam Protection



Deployment

The Gateway works on protocol SMTP and can deployed to protect on-premise systems such as Exchange, but it can also be used to protect Microsoft Office 365 environments for messages entering the Cloud environment, but also internal messages within Microsoft Office 365 to provide enterprise grade security.

Encryption

With the growing need to collaborate securely, organizations need methods of encrypting content that are easy to use from the senders' and recipients' perspective and also comply with organizational security and regulatory requirements.

The Clearswift SEG offers a wide range of channel and message level encryption to provide organizations with the security to ensure their privacy commitments are honored. These include:

- TLS
- S/MIME v3.2
- PGP
- Password protected PDFs or Zips
- Portal (On-premise or Cloud Hosted)

These methods can be used in conjunction with each other: for example, ad-hoc password protected files can be sent via the Portal.

With the PKI methods of S/MIME and PGP, key management gains importance - and the SEG has features to perform automatic key harvesting, Online Certificate Status Protocol (OCSP) and key server lookups to reduce the admin overhead even more.

Message management

System administrators can manage violations through a simple to use web console, but they can also allow users to manage "soft" violations using the Personal Message Management interfaces (Browser or App). These can allow users to release inbound or outbound violations securely and safely, such as Spam mail or profanity. The types of violations that they may have access to is controlled centrally based on corporate culture and policy.

When messages contain potential data breaches, it is unlikely that the IT function are the best people to judge whether the violation is malicious, accidental or just part of someone's role. In this case the line manager or supervisor can be provided with the means to release these violations in a controlled fashion that ensures that employee/manager collusion does not exist.

Clearswift SECURE Exchange Gateway

The Clearswift SECURE Exchange Gateway (SXG) enables organizations to apply data loss prevention policies to internal email communications. This solution can identify and prevent policy violations and can stop sensitive or inappropriate data from being shared internally and externally by monitoring incoming and outgoing email traffic.

Deployment

Ease of deployment enables organizations to be able to deploy the product quickly into their Exchange 2010, 2013 and 2016 environment. The Clearswift SXG can be deployed to filter traffic or in monitor mode to allow the product to identify policy violations without interrupting message flow.

Integration with the SECURE Email Gateway (SEG) permits policy, message management and reporting to be performed at a single management console.

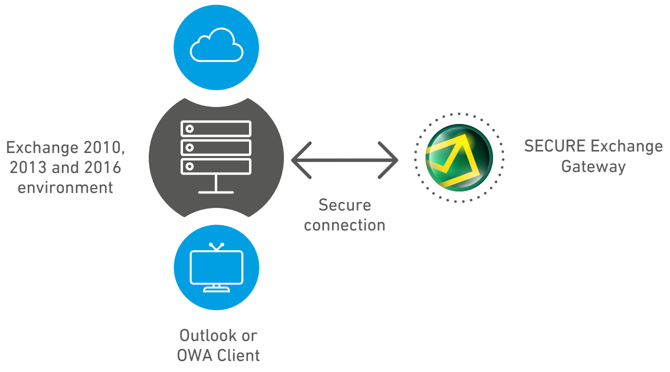
To mirror the resilient and high availability configurations implemented for Exchange Servers, the Clearswift SXG preferred deployment configuration is for 2 x SXG instances that execute in an Active-Active mode, balancing the workload automatically.

Internal scanning

With a growing need to ensure that internal communications are acceptable to the business and that confidential content is not sent to recipients who should not receive that content.

Rules can be created based on senders, recipients, file types, sizes and of course the content of the messages and their attachments.

This technology uses client-server architecture to ensure that although additional security is being applied there is no noticeable difference to the performance of the Exchange system.



Messaging policies

Email will continue to be the dominant communications medium for many years to come and every company is different so having flexibility to create policies that are appropriate to deal with business problems is essential.

Most organizations apply controls to messages to and from the Internet, but seldom consider risks of internal messaging. The SXG platform is designed to deal with the concerns of internal messages and focuses on Data Loss Prevention and the prevention of unacceptable messages and attachments inside the business.

Policies can be granular, created for individuals or user groups obtained from Active Directory, so policy rules can be created and applied to the appropriate senders and recipients.

Data Loss Prevention

With so much sensitive information available, organizations must enforce corporate confidentiality at every point in their infrastructure, not just at the egress points.

The Clearswift SECURE Exchange Gateway features all the standard content filtering and A-DLP functionality including integration with the Clearswift Information Governance server to provide full and partial document fingerprinting.

ARgon for Email

Argon for Email uses Clearswift Adaptive Redaction technology and tackles the problems caused by traditional Data Loss Prevention (DLP) solutions. It works to detect and remove only the content which breaks policy allowing the rest of the email and attachments to be delivered.

Data Loss Prevention (DLP) effectiveness is determined by the accuracy and the workflow of the product. Many DLP solutions are purchased and never deployed because they are too hard to configure or they generate too many false positives, resulting in increased operational overheads and decreased productivity through disrupted communications. ARgon removes this traditional barrier by enabling the mitigation of sensitive data leaks through email without hindering communication flow.

ARgon can be used in environments with no DLP solution or to augment an existing one. In both cases, ARgon removes next generation information threats from both inbound and outbound email. For those with an existing DLP solution, ARgon reduces the false positives by automatically removing the content which would cause the DLP solution to 'stop & block' the communication, whilst still delivering the legitimate content.

There are three key features within Adaptive Redaction that ARgon for Email utilizes:

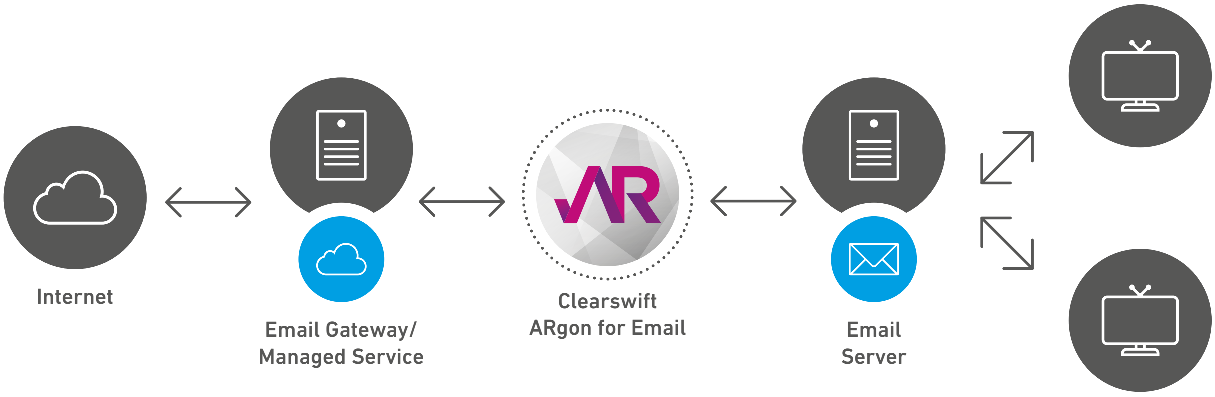
- Data Redaction
  Removes visible content that breaks policy from email and attachments, eg. PCI, PII and other sensitive data.
- Document Sanitization
  Removes document meta-data, revision history, etc.
- Structural Sanitization
  Removes active content embedded in inbound emails and documents.

Optical Character Recognition (OCR)

In addition to the above features, ARgon for Email also incorporates another crucial DLP feature - Optical Character Recognition (OCR). OCR is the process of detecting and extracting text from an image file, an image embedded within an electronic document, or a scan of a document. All Clearswift email security products have OCR functionality built-in to mitigate the risk of data loss through images shared through email. The OCR feature supports multiple languages, enabling it to be easily used by global organizations who operate using more than one language.

Deployment

ARgon is deployed between the email hygiene (and/or DLP) service and the internal email server.



- ARgon for Email uses standard SMTP messaging technology to enable compatibility with any email gateway solution
- The email gateway service can be provided by any vendor and located on-premise or hosted
- The email server can be Exchange, Lotus Notes, or Groupwise
- Proof of Value trials can use either 'Side Car' or 'In Series' deployments

Quarantine

The separation of hygiene services and Argon content inspection/remediation, allows policy breach events to be sent to:

- IT personnel - to focus on harmful viruses and malware;
- Business/audit personnel to focus on sensitive content violations

SECURE Web Gateway

With more and more companies adopting cloud based services such as Salesforce, Office365 and Dropbox, the Internet can now be considered an extension of your IT infrastructure. Going beyond advanced filtering and hygiene the Clearswift SECURE Web Gateway provides an unprecedented layer of threat detection and data loss prevention features for secure collaboration through the Internet and cloud collaboration applications.

The Clearswift SECURE Web Gateway (SWG) enables organizations to take complete and granular control over what users access or share online. Flexible, policy-based filtering and content aware inspection extends beyond limiting recreational browsing, to view inside encrypted traffic, preventing phishing and malware attacks, and sensitive data leaks.

Deployment

The Clearswift SWG is easy to deploy and can be set up in either a forward (explicit) proxy, Transparent (WCCP) proxy or in conjunction with Firewalls that support policy based routing.

HTTP/S scanning

HTTP/S is now more prevalent than HTTP as it allows organizations to prevent eavesdropping on browser sessions. This technology can render some content scanning solutions unusable, but the Clearswift SWG has an integrated SSL decryption engine so that these sessions are automatically decrypted and passed to the content scanning engine to ensure no policy violation can take place.

Flexible policies

With such diverse business requirements, it's necessary to provide security profiles to ensure that users both in the office and working remotely are presented with policies that enable them to work effectively and securely.

As well as required access to business sites, a number of organizations will permit their staff to use social networking sites in a controlled manner.

Organizations need to be able to define who is using these services based upon their authenticated ID or Organization Grouping, when they are using the sites and also for how long.

This enables rules to be created, such as:

- HR department can use LinkedIn and Facebook all day
- All other users can view LinkedIn between 12:00 and 14:00 for 1 hour maximum
- All other users can view Facebook between 12:00 and 14:00 for 1 hour maximum and can update their status, but not perform any file uploads

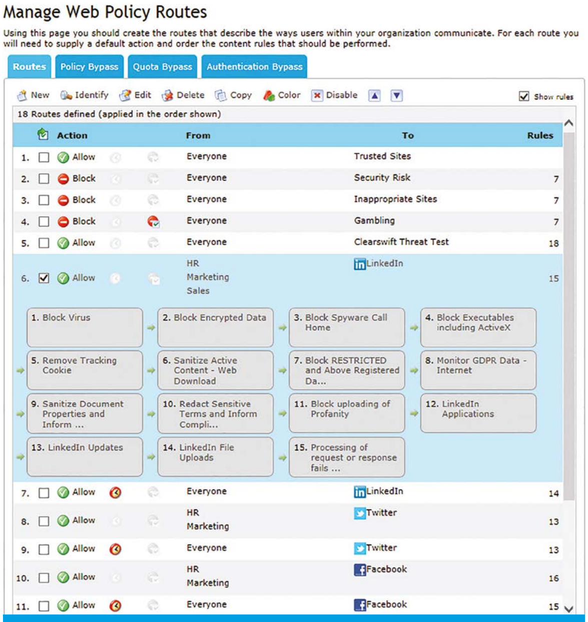
Of course any content posted will still be subject to the corporate security policies for that individual.

Website categorization

Embedded into the Clearswift SWG is a URL filtering engine with over 50 million URLs which are updated daily and sorted into more than 80 different categories, including Phishing, Malware and Security Risk. Malware definitions are refreshed hourly to supplement the integrated anti-virus scanning of any downloads.

Along with the URL database, there is a real time categorizer which detects page content as it is being downloaded. This allows the Clearswift SWG to determine whether pages contain content that might be pornographic, use remote proxies or include hate or violence, amongst other content.

With the increase in the amount of personalized content delivered through social networking pages, this feature ensures that employees are kept safe from pages which are on reputable sites but have been hijacked or abused.



Manage Web Policy Routes

Using this page you should create the routes that describe the ways users within your organization communicate. For each route you will need to supply a default action and order the content rules that should be performed.

18 Routes defined (applied in the order shown)

		Action	From	To	Rules
1.	□	Allow	Everyone	Trusted Sites	
2.	□	Block	Everyone	Security Risk	7
3.	□	Block	Everyone	Inappropriate Sites	7
4.	□	Block	Everyone	Gambling	7
5.	□	Allow	Everyone	Clearswift Threat Test	18
6.	☑	Allow	HR Marketing Sales	LinkedIn	15

1. Block Virus
2. Block Encrypted Data
3. Block Spyware Call Home
4. Block Executables including ActiveX
5. Remove Tracking Cookie
6. Sanitize Active Content - Web Download
7. Block RESTRICTED and Above Registered Da...
8. Monitor GDPR Data - Internet
9. Sanitize Document Properties and Inform ...
10. Redact Sensitive Terms and Inform Compli...
11. Block uploading of Profanity
12. LinkedIn Applications
13. LinkedIn Updates
14. LinkedIn File Uploads
15. Processing of request or response fails ...

		Action	From	To	Rules
7.	□	Allow	Everyone	LinkedIn	14
8.	□	Allow	HR Marketing	Twitter	13
9.	□	Allow	Everyone	Twitter	13
10.	□	Allow	HR Marketing	Facebook	16
11.	□	Allow	Everyone	Facebook	15

Easy to use policies:
how granular policies can be applied to categorized website as well as social networks

Clearswift SECURE ICAP Gateway

The Clearswift SECURE ICAP Gateway (SIG) is designed to co-exist with your existing web security provider using industry standard ICAP functionality delivered by suppliers such as F5 Networks, Blue Coat, IBM, Cisco and Barracuda Networks.

Deployment

The likes of F5 Networks and BlueCoat proxy servers are well known to network administrators to provide both proxy and network bandwidth management capabilities. They also provide an interface to allow 3rd party solutions such as Anti-Virus and Data Loss Prevention solutions to connect via the ICAP. Connecting the Clearswift SECURE ICAP Gateway to the third party devices allows the network security features of the device to be complimented by the Clearswift Adaptive Data Loss Prevention functionality.

Enabling policies

Clearswift actively increases, rather than hampers, employee productivity by facilitating employee engagement with collaborative online technologies through our flexible web 2.0 policy rules.

User identities are authenticated by the ICAP proxy and passed to the Clearswift SECURE ICAP Gateway so that granular user policies can be applied to the content coming in and out of the organization.

The Clearswift SECURE ICAP Gateway goes beyond simply keeping your networks free of viruses, inappropriate content and harmful executables. It enables complete, granular control over the information that you access or share online, whether it's limiting recreational browsing, or preventing sensitive data from leaking into status updates using the Clearswift Adaptive Redaction technology.

The Clearswift SIG enables organizations to reap all the benefits that collaborative web 2.0 technologies have to offer, safe in the knowledge that your sensitive data, IP and brand reputations are protected.

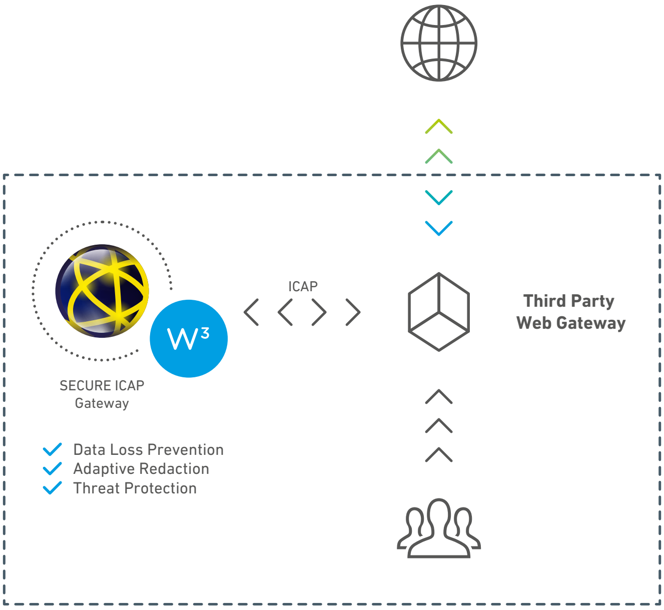
Managing data securely

The Clearswift SIG provides all the standard content filtering and A-DLP functionality such as Data Redaction, Structural and Document Sanitization to ICAP clients that permit data modification by the ICAP server.

The Clearswift SIG can also support integration with the Clearswift Information Governance Server to provide full and partial document fingerprinting.

Managing data securely

It's not just web proxies that use ICAP as a means to check content. This interface can be found in other security devices such as Firewalls and Managed File Transfer products. These devices can also benefit from the deep content scanning provided by the Clearswift SIG.



Clearswift Endpoint DLP

By controlling where sensitive data resides and how it is used on endpoint devices, organizations can manage information security, governance and compliance risks and identify control priorities.

The Clearswift Endpoint DLP (CED) solution supports a combination of security features – including device control, deep content inspection, remediation actions, encryption and comprehensive auditing.

Deep content inspection

Clearswift Endpoint DLP (CED) is a fully content-aware endpoint data loss prevention solution that provides complete visibility of data stored on the endpoint, as well as granular control over what data can be transferred to and from devices. The transfer of critical information can be logged, blocked or encrypted and the solution provides automated policy-based remediation. The Clearswift Endpoint DLP Agent scans files for sensitive content and based on a granular organizational policy it provides the necessary flexibility to permit multiple behaviors, depending on the user and destination of file operations.

Device control

Today's organizations need to have the ability to control users connecting personal USBs or smart devices to the corporate network. In fact, this has become a critical security requirement. Sensitive data can be lost and malicious applications can be introduced to networks due to the uncontrolled use of removable media. The Clearswift Endpoint DLP integrated device control provides granular management of removable media, permitting the legitimate productivity-enhancing use of these devices whilst reducing network risks and support costs – resulting in increased data security.

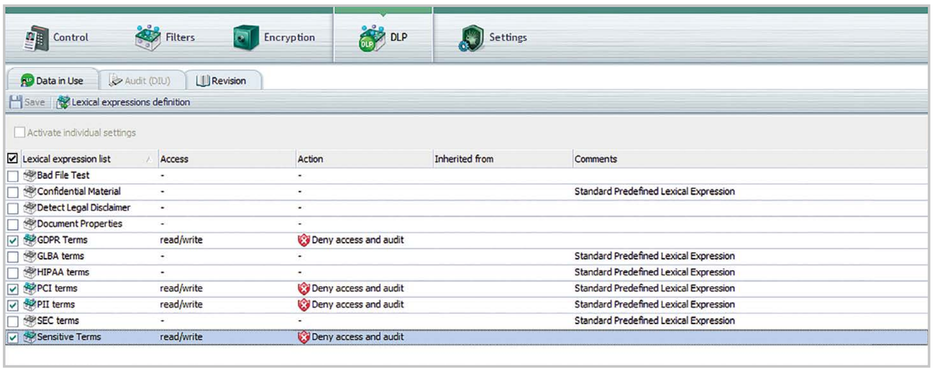
Context-aware Data in Use (DIU) policies

Flexible policies and context-aware content inspection means that you no longer have to choose between the productive use of removable media and unacceptable risk. Rules can be created that block all spreadsheets containing particular keyword terms from being copied to external devices. Alternatively, these files can be encrypted when transferred – which ensures that the contents of a USB cannot be read if it was to be left behind in a taxi or in another public place.

Discovering Data at Rest (DAR)

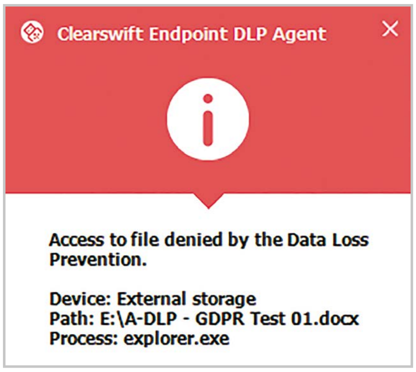
By using the Clearswift Deep Content Inspection Engine, critical data can be discovered wherever it is stored on desktops, notebooks, servers, shared networks or cloud collaboration apps (e.g. Dropbox). This enables organizations to audit and manage critical information cleanup within data at rest. As with 'data in use' policies, built-in and customizable lexical expressions are included, which enables discovery of required critical information as detailed in the likes of Data Protection Acts of the Länder, Privacy Act, PCI, HIPAA, GLBA and GDPR.

Running in the background, utilizing advanced throttling techniques, the agent silently discovers critical information without interrupting end user activity. This provides unprecedented insight into potential data protection vulnerabilities that exist on your networks and systems.



□ Activate individual settings

☑ Lexical expression list	Access	Action	Inherited from	Comments
□ Bad File Test	-	-		
□ Confidential Material	-	-		Standard Predefined Lexical Expression
□ Detect Legal Disclaimer	-	-		
□ Document Properties	-	-		
☑ GDPR Terms	read/write	Deny access and audit		
□ GLBA terms	-	-		Standard Predefined Lexical Expression
□ HIPAA terms	-	-		Standard Predefined Lexical Expression
☑ PCI terms	read/write	Deny access and audit		Standard Predefined Lexical Expression
☑ PII terms	read/write	Deny access and audit		Standard Predefined Lexical Expression
□ SEC terms	-	-		Standard Predefined Lexical Expression
☑ Sensitive Terms	read/write	Deny access and audit		

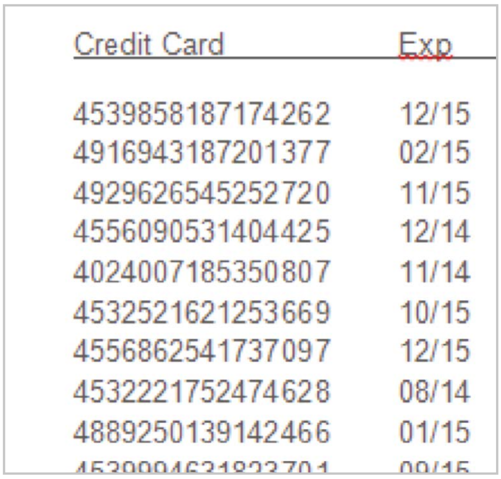


Access to file denied by the Data Loss Prevention.

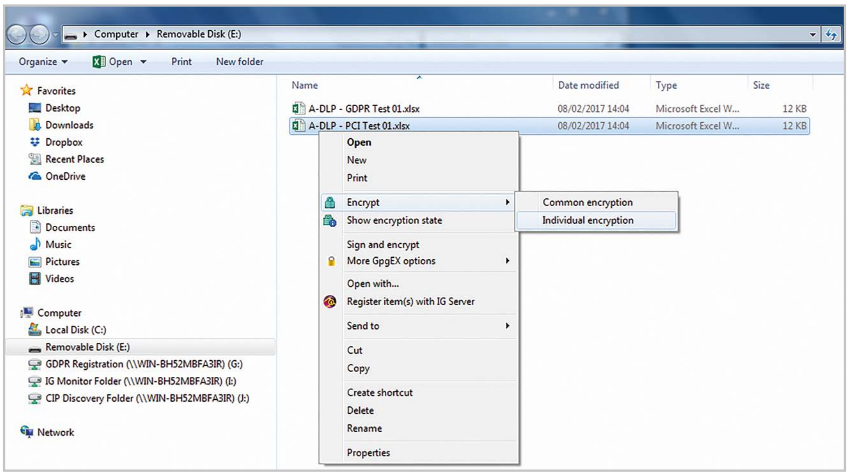
Device: External storage
Path: E:\A-DLP - GDPR Test 01.docx
Process: explorer.exe

Protect critical information to comply with regulations

Staying within the bounds of a regulatory framework is paramount. By encrypting files, organizations can ensure that they comply with regulation, while facilitating the legitimate and productive use of removable media. Flexible policies can be built to enable the transfer of non-sensitive data such as sales brochures, whilst encrypting and protecting files that do contain critical information.



Credit Card	Exp
4539858187174262	12/15
4916943187201377	02/15
4929626545252720	11/15
4556090531404425	12/14
4024007185350807	11/14
4532521621253669	10/15
4556862541737097	12/15
4532221752474628	08/14
4889250139142466	01/15
4539094631823701	09/15



Name	Date modified	Type	Size
A-DLP - GDPR Test 01.xlsx	08/02/2017 14:04	Microsoft Excel W...	12 KB
A-DLP - PCI Test 01.xlsx	08/02/2017 14:04	Microsoft Excel W...	12 KB

Integrated policy management

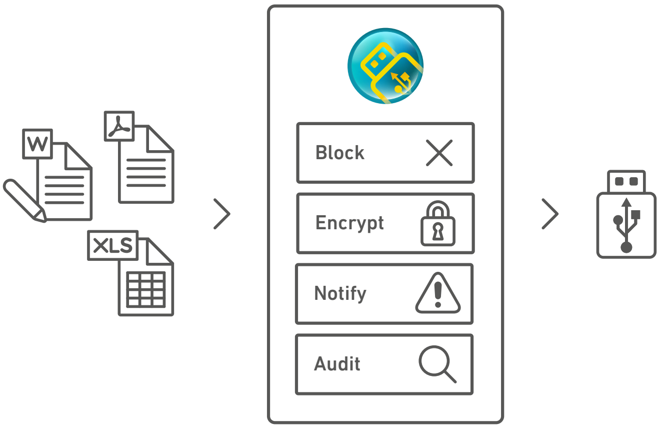
The interface of the Clearswift Endpoint DLP product is simple to use. With pre-defined lexical expressions, file name lists and media types, it's easy to build policies, manage violations and report on trends and behavior. Valuable insight is provided without consuming valuable admin resource.

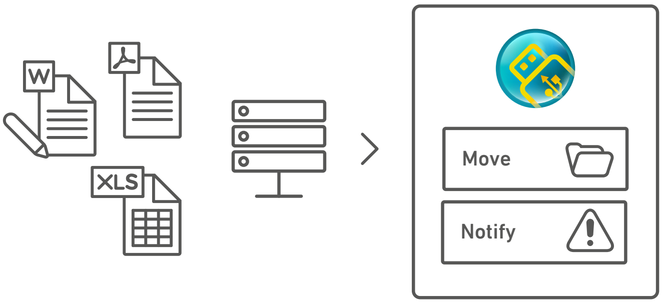
The Clearswift Endpoint DLP Agent enforces flexible, content-aware policies and can carry out different actions depending on the content policy from group level or for individual team members.

The results are provided by Clearswift's reporting function, which shows where critical information resides, who is using endpoint devices and what information is being transferred to insecured devices. Reports will generate a detailed audit of discovered data, devices connecting, and the information transferred to and from the device by each user.

Reporting and Monitor Mode

Clearswift is able to provide a useful proof-of-value exercise by running the Clearswift Endpoint DLP Agent in 'Monitor Mode', which enables organizations to see the results of their policies without the operation executing in 'Active' mode.



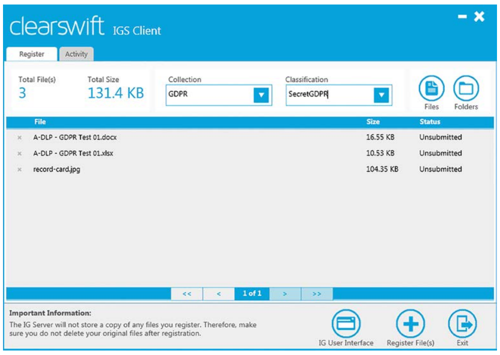


Clearswift Information Governance Server

With the ability to track hundreds of thousands of documents and monitor billions of communication transactions, the Clearswift Information Governance Server (IGS) integrates with your own environment and the Clearswift SECURE Gateways. Document owners can access the system using their existing Windows credentials to securely register and classify data with the Clearswift IGS Server. Compliance Officers are given access to oversee who and what is being registered.

Deployment

The Clearswift Information Governance Server (IGS) is deployed centrally in an organization. Running on a Linux platform, the Clearswift IGS integrates with your own environment for enterprise single sign on and support for current Clearswift SECURE Email, Web, Exchange, ARgon for Email and ICAP Gateways. Our architectural strategy provides for future integration with additional Clearswift solutions.



Total File(s): 3
Total Size: 131.4 KB
Collection: GDPR
Classification: SecretGDPR

File	Size	Status
A-DLP - GDPR Test 01.docx	16.55 KB	Unsubmitted
A-DLP - GDPR Test 01.xlsx	10.53 KB	Unsubmitted
record-card.jpg	104.35 KB	Unsubmitted

Important Information:
The IG Server will not store a copy of any files you register. Therefore, make sure you do not delete your original files after registration.

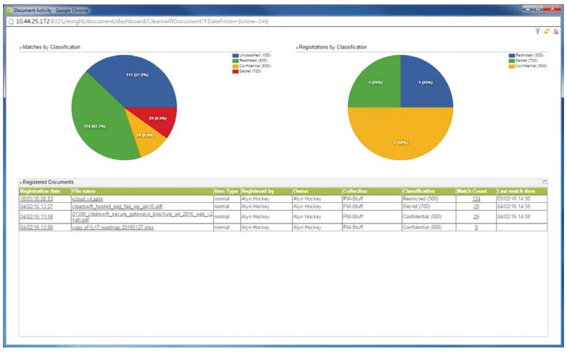
Document management

Businesses today have to be more dynamic when it comes to information security. The Clearswift IGS permits users to register sensitive documents, or pieces of information within documents, through a simple-to-use web interface or a Windows client.

Registered Document Owners are notified of any violations if that document, or even a fragment of it, is uploaded to a website, sent internally or emailed to an external recipient, depending on your deployed policy.

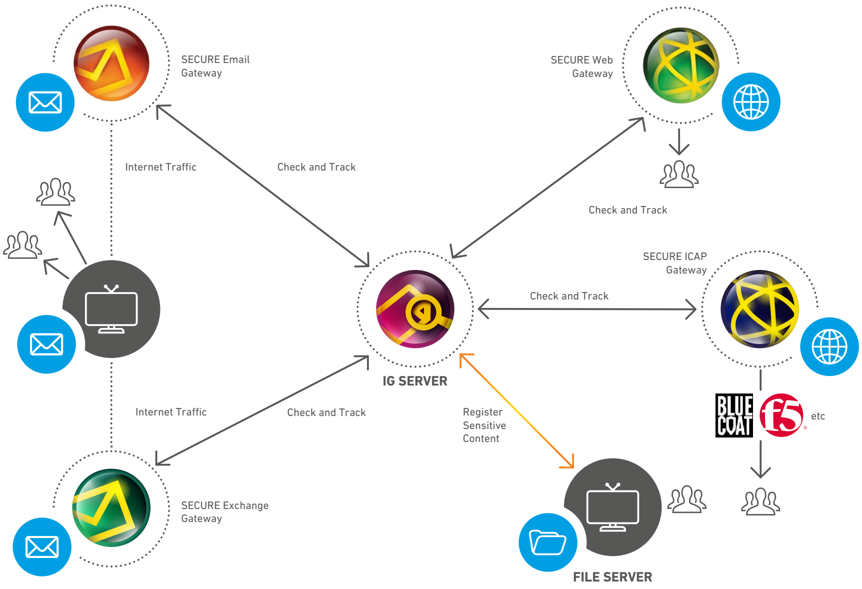
Document track 'n' trace

The Clearswift IGS is not a repository of documents, but of their fingerprints. It is also used to store transactions from all of the connected Gateways. This data store can then be mined to show information flows and relationships. The information analytics provided will allow the ability to follow a piece of data across multiple protocols providing the CISO with unique insights into how and where their information is going.


Document Activity - Google Chrome
10.44.25.172:8321/insight/document/dashboard/ClearswiftDocument?f:DateFrom={s:now-1m}
Matches by Classification
111 (37.9%)
124 (42.3%)
29 (9.9%)
29 (9.9%)
Unclassified (100)
Restricted (300)
Confidential (500)
Secret (700)
Registrations by Classification
1 (25%)
1 (25%)
2 (50%)
Restricted (300)
Secret (700)
Confidential (500)

Registered Documents

Registration date	File name	Item Type	Registered by	Owner	Collection	Classification	Match Count	Last match time
18/01/16 08:53	icloud v4.pptx	normal	Alyn Hockey	Alyn Hockey	PM-Stuff	Restricted (300)	124	03/02/16 14:30
04/02/16 13:57	clearswift_hosted_seg_faq_wp_jan16.pdf	normal	Alyn Hockey	Alyn Hockey	PM-Stuff	Secret (700)	29	04/02/16 14:58
04/02/16 13:58	01390_clearswift_secure_gateways_brochure_a4_2016_web_v2+ah.pdf	normal	Alyn Hockey	Alyn Hockey	PM-Stuff	Confidential (500)	29	04/02/16 14:58
04/02/16 13:58	copy of fy17 roadmap 20160127.xlsx	normal	Alyn Hockey	Alyn Hockey	PM-Stuff	Confidential (500)	0	



Clearswift deployment options

Clearswift security solutions are available with a range of deployment options to fit your existing IT infrastructure, to meet your business requirements and to reduce the time and costs associated with deployment and maintenance.

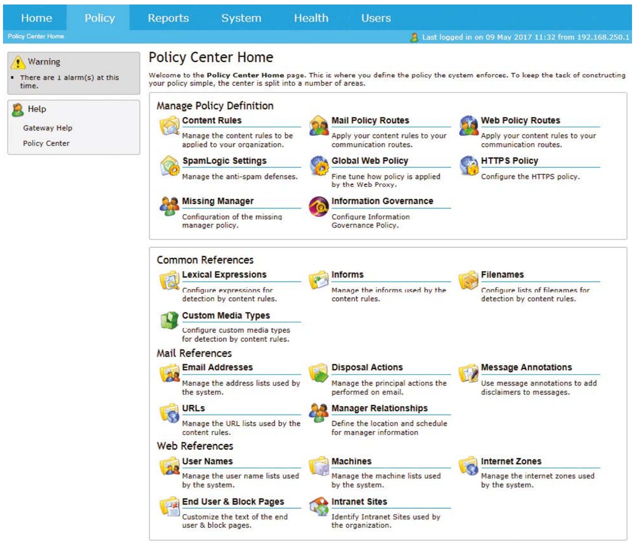
For the quickest return on investment, and to reap efficiency savings, simple deployment is essential. Clearswift offers email, web and endpoint security solutions that work how you do.

Hardware deployment options

The Clearswift SECURE Gateways are available as pre-configured appliances ready for immediate hardware deployment at your network perimeter. A range of hardware performance profiles allow you to select the correct unit for your filtering needs and provide scope for future growth. Hardware deployment options from Clearswift are also backed by 'Next Business Day' or 'Four-hour' onsite service options.

Software deployment options

The Clearswift SECURE Gateway solutions are also available for deployment on your own server hardware, allowing you to maintain consistency in your environment using systems from your preferred vendor. The Clearswift SECURE Gateways operate on a hardened Linux distribution, offering ultimate flexibility for your own hardware deployment choices.



- There are 1 alarm(s) at this time.

Policy Center Home

Welcome to the **Policy Center Home** page. This is where you define the policy the system enforces. To keep the task of constructing your policy simple, the center is split into a number of areas.

Manage Policy Definition

Content Rules Manage the content rules to be applied to your organization.

Mail Policy Routes Apply your content rules to your communication routes.

Web Policy Routes Apply your content rules to your communication routes.

SpamLogic Settings Manage the anti-spam defenses.

Global Web Policy Fine tune how policy is applied by the Web Proxy.

HTTPS Policy Configure the HTTPS policy.

Missing Manager Configuration of the missing manager policy.

Information Governance Configure Information Governance Policy.

Common References

Lexical Expressions Configure expressions for detection by content rules.

Informs Manage the informs used by the content rules.

Filenames Configure lists of filenames for detection by content rules.

Custom Media Types Configure custom media types for detection by content rules.

Mail References

Email Addresses Manage the address lists used by the system.

Disposal Actions Manage the principal actions the performed on email.

Message Annotations Use message annotations to add disclaimers to messages.

URLs Manage the URL lists used by the content rules.

Manager Relationships Define the location and schedule for manager information

Web References

User Names Manage the user name lists used by the system.

Machines Manage the machine lists used by the system.

Internet Zones Manage the internet zones used by the system.

End User & Block Pages Customize the text of the end user & block pages.

Intranet Sites Identify Intranet Sites used by the organization.

Peered Email and Web Gateways permit policy changes from a single console

Hosting & Cloud options

Customers who embrace public cloud deployments such as AWS and Azure will be pleased to know that the Clearswift SECURE Gateways are also supported within these environments.

Clearswift offers a straightforward, secure and cost-effective hosted solution to protect your organization; allowing organizations to have complete control over a dedicated system whilst reducing their on-site footprint; including hardware, power, rack space and maintenance costs.

Our hosted solution supports today's collaboration model, whilst bringing award winning security to critical information allowing organizations to achieve their desired operational efficiencies safe in the knowledge that communications remain safe and compliant in the Cloud.

Managed Email Security Service

Clearswift offers an affordable and effective managed email security service that enables the highest level of protection, a reduction in day to day management overhead, but keeps you in control.

The service offered includes:

- 100% Email Delivery
- Single anti-virus (multiple anti-virus available for additional cost providing protection from infection by 100% of known malware)
- Anti-spam protection will provide 99% or greater detection
- Two instances in geographically diverse data centers
- File type control
- Up to two updates and two patches per year
- Access to Personal Message Manager (PMM)

Virtualization deployment options

The Clearswift SECURE Gateway solutions also support virtualization using VMware and private cloud security systems for greater network management flexibility. Your deployments can then be assembled from a combination of physical and virtualized servers according to your specific business needs and environment.

Peered Gateways

Peered Clearswift Gateways share common policy and system settings, ensuring that, should one Gateway fail, the remaining Gateway(s) will be able to pick up the load. With more than one Gateway deployed, administrators can use a single interface to enforce a consistent policy across multiple communication protocols.

> “World class products, 24/7 technical support and professional services”

Clearswift Support and Professional Services

Clearswift's Support Services organization is dedicated to protecting our customer's investment. Our team of experts ensure ongoing and consistent operational capabilities, attaining the highest levels of satisfaction through the delivery of professional and highly responsive services. We offer a variation of Support Options and Professional Services to best meet your business needs and requirements.

Standard Support

The Standard Support offering gives a highly reactive and responsive 24/7 service, enabling Clearswift to take immediate ownership of reported issues, providing full visibility of progress and status through the end-to-end management of incidents.

Advanced Support

An Advanced Support offering is available, recognizing the business critical nature of Clearswift solutions. It delivers enhanced support capabilities, including automated service monitoring and reporting and regular service reviews to further secure consistent operational availability through a more proactive level of support.

Premium Support

The Premium Support offering is a highly personalized service, delivering additional services through a dedicated Support Account Manager, inclusive of best practice consultation, on-site support days and regular on-premise service reviews in true partnership with our clients.

Professional Services

At Clearswift, we recognize that there will be times when you require expert knowledge to help with a product deployment, upgrade, or migration over to our products. Accordingly, we offer an array of Professional Services that vary from consultation for business process change to periodic health checks to deployment plans, content security policy configuration and compliance requirements. The range of professional service packages we offer have been designed to ensure that you get the maximum value from your Clearswift investment.

Summary

Clearswift offers a straightforward, manageable approach to mitigating cyber threats and preventing data loss across digital collaboration channels. Our technology is suitable for organizations of all sizes, bringing a Gartner Magic Quadrant recognized solution to support your organization today, and tomorrow.

Offering simultaneous protection from inbound and outbound threats, Clearswift takes a proactive approach to data loss, mitigating data leak risks from within the network and preventing malicious cyber attacks from outside. With a Clearswift solution in place, you can rest assured that your organization remains secure and protected at the same time as business activity and collaboration remains consistent and agile.

Clearswift solution functionality summary table

Key Feature	SECURE Email Gateway	SECURE Web Gateway	SECURE Exchange Gateway	SECURE ICAP Gateway	Clearswift Endpoint DLP
Deep Content Inspection	●	●	●	●	●
Data Loss Prevention	●	●	●	●	●
Anti-virus	●	●	●	* ●	○
Encryption*	●	○	○	○	●
Remote Client Support*	○	●	○	○	○
Text Redaction*	●	●	●	●	** ●
Document Sanitization*	●	●	●	●	** ●
Structural Sanitization*	●	●	●	●	** ●
Optical Character Recognition (OCR)*	●	○	●	○	○
Standard / Advanced* / Premium* Support	●	●	●	●	●
Message Sanitization	●	○	○	○	○
Professional Services*	●	●	●	●	●

*Additional cost option

** Due in 2019 release

Notes

clearswift
RUAG Cyber Security

Clearswift is trusted by organizations globally to protect critical information, giving teams the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution that avoids the risk of business interruption and enables organizations to gain visibility and control of their critical information 100% of the time.

As a global organization, Clearswift has headquarters in the United States, Europe, Australia and Japan, with an extensive partner network of more than 900 resellers across the globe.

UK
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA
Tel : +44 (0) 118 903 8903
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1200
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
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
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
Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com