Securing your critical information with Clearswift
Product & Solution Overview
# Table of Contents

- Introduction: 3
- Clearswift SECURE Gateways: 4
- Clearswift SECURE Email Gateway (SEG): 8
- Clearswift SECURE Exchange Gateway (SXG): 9
- Clearswift ARgon for Email: 10
- Clearswift SECURE Web Gateway (SWG): 11
- Clearswift SECURE ICAP Gateway (SIG): 12
- Clearswift Critical Information Protection Server: 13
- Clearswift IG server (IGS): 15
- Gateway Deployment Options: 16
- Support and Professional Services: 17
- Summary: 18
- About Clearswift: 19
Introduction

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.

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

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.

As business practices change to adapt to the continued growth of Cloud, big data and BYOD (Bring Your Own Device) coupled with the increasing amount of collaboration organizations now face, Clearswift continues to innovate and adapt our solutions.
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 every organization’s information, and the entry point for collaborative content from trusted 3rd parties, it makes sense to protect them 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 dictionaries, templates and rules, and have policy defined via a single console.

While security solutions can be notoriously difficult to use and manage, the Clearswift solution has 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

With installations on preconfigured hardware, on a customer’s preferred hardware supplier or with vSphere, Hyper-V or Cloud deployments, clients can be up and ready to configure a Gateway with their policies in less than 30 minutes.

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 & 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, and it is this engine which lies at the heart of all the Gateways.

Deep Content Inspection

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

• True file type detection
• Text extraction
• Text scanning

Clearswift has developed its own innovative extraction and scanning engine, enabling it to determine additional important information. The ability to detect whether text is in a document’s header, footer or main body, for example, becomes important when designing detection policies. Without this additional intelligence, false positives can become unmanageable and the solution ineffective. Deep understanding of document types and the information they contain has also enabled the development of a new technology, Adaptive Redaction, which allows documents to be modified and critical information that could cause a data leak to be removed.

Once the inspection has been carried out, policies can be applied. The most common policies are those around Data Loss Prevention.
Data Loss Prevention

Data Loss Prevention (DLP) is built in as standard for the SECURE Gateways and relies upon the information being passed from the Deep Content Inspection engine in order to make decisions. DLP is direction agnostic, which is to say that it can be used to prevent information from entering an organization as well as leaking out. With the increase in legislative requirements, DLP is becoming 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, SOX etc)
- Search patterns constructed from words, phrases and tokens
- Predefined tokens for PCI & PII (credit card, social security, passport numbers, identities etc)
- User definable tokens 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 centralised multi-protocol solution
- Structured data search to look for database content

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, the new 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 ‘X’. 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 the common file formats (e.g. Microsoft Office documents, Adobe pdf, etc.), the Gateways can detect and 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 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 different AV solutions from Sophos or Kaspersky as well as the ability to use multiple AV engines at the same time. 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. The SECURE Gateways offer extensive reporting facilities in support of these requirements, enabling system administrators to rapidly create both management and realtime 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 be exported to CSV for import into a spreadsheet.

For organizations with a Security Information and Event Management (SIEM) solution, the Gateways are compatible with various platforms, including:

- RSA Envision
- HP ArcSight
- Splunk

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.

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.
Clearswift SECURE Email Gateway

The Clearswift SECURE Email Gateway (SEG) is the award winning, market leading solution for securing your email communications, enabling your organization to balance the need to protect critical information with the ability to continuously collaborate; on premise, in the Cloud or bringing requisite Enterprise security to an Office365 environment. Offering the latest in inbound threat protection, the SEG prevents sensitive data being leaked via both incoming and outgoing email - reducing the risk of threat to your organization.

**Threat protection**

The Clearswift SECURE Email Gateway comes with multi-layer threat defences, with a choice of a single or dual AV engine (Sophos, Kaspersky) 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 defence 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 plugin’s 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.

**ImageLogic**

In the past, it was just pornographic images which needed to be blocked. While the same is true today, the Email Gateway ImageLogic functionality can also be used to protect intellectual property contained in images from leaving the organization.

**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 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
- PGP
- Ad-Hoc password protected
- Portal (pull and push)

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.

**Personal message management**

Administrators can also delegate message release to the endusers. It’s common for users to be given access to manage spam messages that ‘might’ be legitimate and allow them to be whitelisted so that they won’t be blocked again. The SEG extends this capability so that end users can be responsible for releasing other message violations coming in and leaving the organization based upon corporate culture and policy.

The SEG also provides a number of methods which allow the end-user to manage their mail via an email digest, web portal or via an app for Apple iPhone and iPad devices.

For example, lawyers working on cases where profanities appear in court documents could trigger policy violations and be blocked; Personal Message Management allows them to be granted permission to release the messages without administrator intervention, using a simple hyperlink.

Of course every transaction is also audited for compliance purposes.
Clearswift SECURE Exchange Gateway

The Clearswift SECURE Exchange Gateway 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 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 permits policy, message management reporting to be performed at a single management console.

To mirror the resilient and high availability configurations implemented for Exchange Servers, the 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 take the risks of corporate confidentiality at every point in their infrastructure, not just at the egress points.

The SECURE Exchange Gateway features all the standard content filtering and A-DLP functionality including integration with the Clearswift IG server to provide full and partial document fingerprinting.
ARgon uses unique Adaptive Redaction technology from Clearswift and tackles the problems caused by traditional Data Loss Prevention (DLP) solutions by automatically removing only the content which breaks policy and then sending the rest of the email and attachments onwards. This enables continuous collaboration, safe in the knowledge that critical information is protected.

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 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 utilises are:

- **Data Redaction**
  Removes visible content that breaks policy from email and attachments.

- **Document Sanitization**
  Removes document meta-data, revision history, etc.

- **Structural Sanitization**
  Removes active content embedded in inbound emails and documents.

**Deployment**

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

**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

**Deployment**

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

**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
The Internet can now be considered an extension of your own infrastructure with more companies adopting cloud based services such as Salesforce, Office365 and Dropbox.

Deployment
Ease of deployment enables organizations to be able to deploy the product quickly into their infrastructure. The SWG can be deployed either as a forward (explicit) proxy, Transparent (WCCP) proxy or in conjunction with Firewalls that support policy based routing.

HTTP/S scanning
More and more organizations are now securing their sites using HTTP/S to prevent eavesdropping on browser sessions. This technology can render some content scanning solutions unusable, but the 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
The Internet can now be considered an extension of your own infrastructure with more companies adopting cloud based services such as Salesforce for CRM, Office365 for messaging structure and sites like Dropbox for file sharing. 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.

Remote client option
The SWG supports remote clients, meaning that even if the user is not connected to the organization’s network, the device will be subject to corporate security policies. This option can also be deployed on BYOD platforms ensuring that corporate information is kept safe no matter where it is being accessed from.

Website categorization
Embedded into the 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 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.
The SECURE ICAP Gateway is designed to co-exist with your existing web security provider using industry standard ICAP functionality including F5 Networks, Blue Coat 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 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
We actively increase, rather than hamper, 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 SECURE ICAP Gateway so that granular user policies can be applied to the content coming in and out of the organization.

The 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 functionality.

The Clearswift SECURE ICAP Gateway 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 SECURE ICAP Gateway provides all the standard content filtering and A-DLP functionality such as Adaptive Data Redaction, Structural and Document Sanitization. The SIG can also support integration with the Clearswift IG server to provide full and partial document fingerprinting.
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 Critical Information Protection (CIP) Management Server and Agent supports a combination of security features – including device control, deep content inspection, remediation actions, encryption and comprehensive auditing.

**Deep content inspection**
Clearswift CIP is a fully content-aware endpoint data loss prevention solution that provides complete visibility and control of data transferred from the endpoint and stored on it. The transfer of critical information can be logged, blocked or encrypted and the solution provides automated policy-based remediation. The Critical Information Protection 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**
The ability to control users connecting personal USBs or smart devices to the corporate network 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 CIP 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 mean that you no longer have to choose between the productive use of removable media and unacceptable risk. A policy which is too restrictive means that people either cannot work effectively, or they will find ways to bypass their security policy. 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 and GLBA. 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.

**Educate users**
The key to an effective information security management policy is educated end users. The CIP can notify users of the risks involved when transferring critical information to unprotected devices, allowing them to specify a reason for the activity before the file is allowed to be transferred.
Integrated policy management

The interface of the Critical Information Protection Management Server is powerful, yet 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. In this way, valuable insight is provided without consuming valuable admin resource.

Integration with the award-winning Clearswift SECURE Email and Web gateways enables teams to share policy elements, which ensure the consistent application of content rules and compliance with regulations.

The Critical Information Protection Agent enforces flexible, content-aware policies and can carry out different actions depending on the content policy.

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 unsecured devices. Reports will generate a detailed audit of discovered date, devices connecting, and the information transferred to and from the device by each user. The audit is unnoticeable to the end user, so that data and device details can be collected without the user changing their behavior. This helps organizations to understand the usage patterns and business requirements for removable media.

Flexible deployment options

You decide how you want to buy and deploy the Critical Information Protection Management Server. 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 virtualized in a VMware environment.

Discover critical information at rest on endpoint devices and take appropriate remediation actions according to policy, reducing the risk of breaching data protection regulations.

Reporting and Monitor Mode

Clearswift is able to provide a useful proof-of-value exercise by running the CIP Agent in ‘Monitor Mode’, where organizations can see the results of their policies without the operation executing in ‘Active’ mode.
Clearswift Information Governance Server

**Deployment**
The Clearswift Information Governance Server (IGS) is deployed centrally in an organisation. Running on a Linux platform, this integrates with your own environment for enterprise single sign on and support for current SECURE Email, Web, Exchange and ICAP gateways; our architectural strategy provides future Gateway integration.

**Document management**
Businesses have to be more dynamic when it comes to security. The IG server permits users to register sensitive documents through a simple-to-use web interface or a windows client. Document owners are also 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 IG server is not just a repository of document 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 to how and where their information is going.
Gateway deployment options

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

For the quickest return on investment, and to reap efficiency savings, simple deployment is essential. Clearswift’s options give you total web and email security that works how you do.

Hardware deployment options

The Clearswift SECURE Web and Email 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 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 SECURE Gateways operate on a hardened Linux distribution, offering ultimate flexibility for your own hardware deployment choices.

Hosting & Cloud options

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.

Customers who embrace public cloud deployments such as AWS will be pleased to know that the Clearswift Gateways are also supported within this environment.

Virtualization deployment options

The Clearswift SECURE solutions also support virtualization using VMware and Hyper-V for email filtering, allowing the creation of private cloud security systems for greater network management flexibility. Your deployments can then be assembled from a combination of physical and virtualization servers according to your specific business needs and environment.

Peered Gateways

If more than one Clearswift Gateway is deployed, or more than one type of Gateway (e.g. Web and Email) is deployed, then integration occurs at all points. Peered Gateways share common policy and system settings, ensuring that, should one Gateway fail, the remaining Gateway 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.

Peered Email and Web Gateways permit policy changes from a single console.
Support and Professional Services

The development of world class products is complemented with a 24/7 support and professional services organization.

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
The Professional Services organization offers our clients help in all aspects of securing their infrastructure. It can offer Gateway infrastructure design, installation and configuration services. Clearswift Professional Services also offers policy design services and system upgrade and system health check support.
Summary

Clearswift offers a straightforward, manageable approach to adaptive data loss prevention, suitable for organizations of all sizes, bringing award winning technology to secure and support your organization today. And tomorrow.

Offering protection from both inbound and outbound threats, Clearswift takes a proactive approach to data loss negating today’s threats such as the insider threat, and malicious cyber attacker activity. With a Clearswift solution in place, you can be rest assured that your organization remains secure at the same time as business activity and collaboration remains consistent and agile.

Clearswift SECURE Gateway functionality summary table:

<table>
<thead>
<tr>
<th>Key Feature</th>
<th>SECURE Email Gateway</th>
<th>SECURE Web Gateway</th>
<th>SECURE Exchange Gateway</th>
<th>SECURE ICAP Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Content Inspection</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Anti-virus</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Encryption*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Remote Client Support*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Text Redaction*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Document Sanitization*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Structural Sanitization*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Standard / Advanced* / Premium* Support</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Professional Services*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

*Additional cost option
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.

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.