CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift SECURE Gateways

Securing business critical information from internal and external threats

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Table of Contents

Introduction

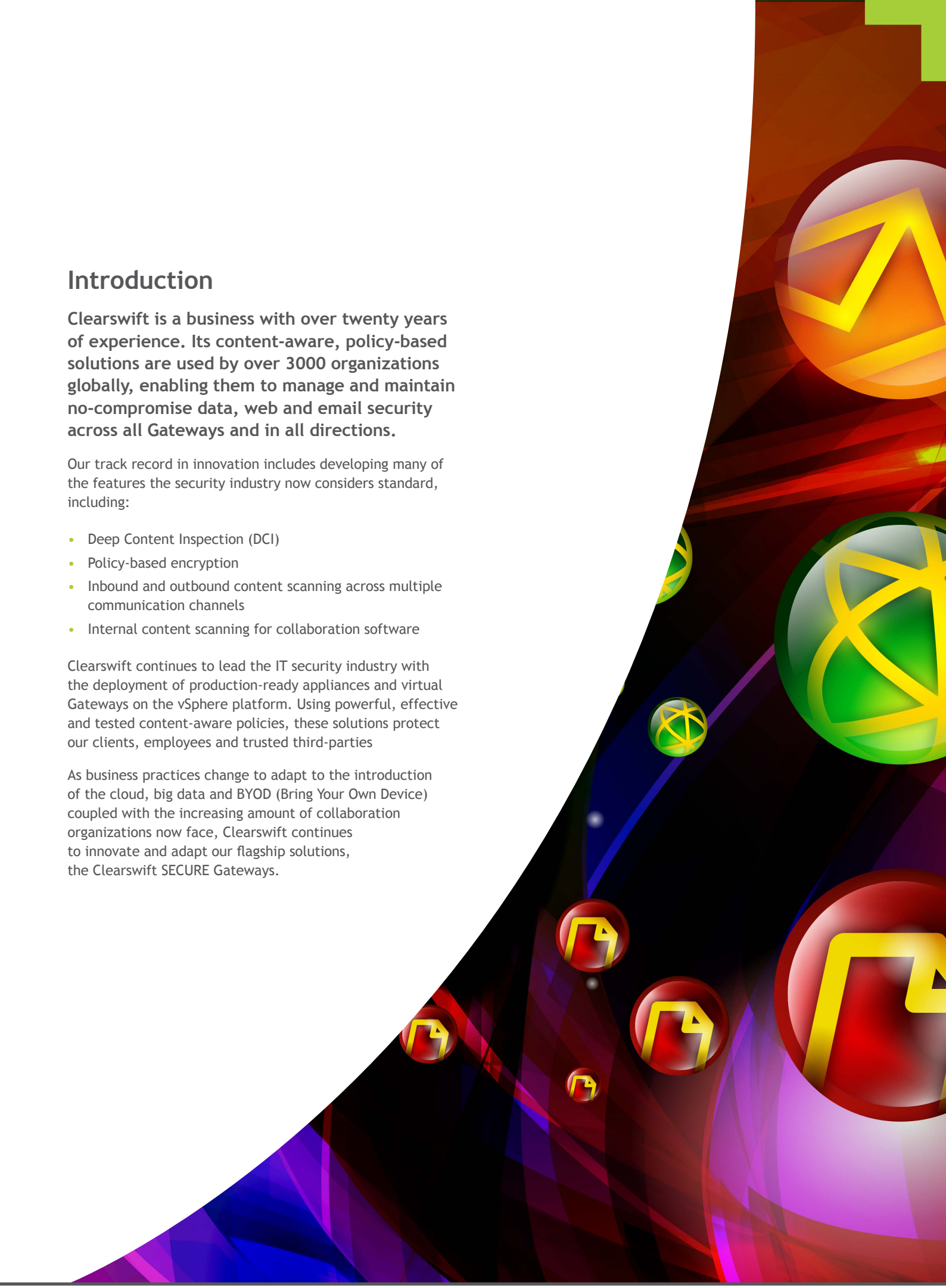
Clearswift is a business with over twenty years of experience. Its content-aware, policy-based solutions are used by over 3000 organizations globally, enabling them to manage and maintain no-compromise data, web and email security across all Gateways and in all directions.

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 and virtual Gateways on the vSphere platform. 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 introduction of the 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 flagship solutions, the Clearswift SECURE Gateways.



CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift SECURE Gateways

Securing business critical information from internal and external threats

With Web and Email traffic being the primary point of exit for every organizations 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, the SECURE Gateways 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 SECURE Gateways have been designed with the administrator and the user in mind. They are focused on masking the sophistication of the solution, making them both easy to use and easy to manage.

This year Information Governance capabilities are being added to enable scanning of SMTP email, Internet traffic and Exchange based email, all managed through a central console.

Easy to use, efficient to manage

The Gateways have been designed to be easy to install, deploy and manage. With installations on preconfigured hardware, on a customer's preferred hardware supplier or with vSphere and Hyper-V, clients can be up and ready to configure a Gateway with their policies in less than 30 minutes.

Preconfigured and sample rulesets, including dictionaries tfor 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

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 Deep Content Inspection engine, 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 (or Leak) 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:

- Simple words, phrases and sensitive fragments from previously categorised documents
- Sophisticated token handling, such as banking codes, social security numbers, national insurance numbers and credit card details
- Personally Identifiable Information (PII) tokens
- User defined tokens
- User defined patterns and regular expressions
- Expressions based around Boolean (AND, OR, XOR, ANDNOT) and positional operators (NEAR, BEFORE, AFTER, and FOLLOWEDBY)
- Dictionaries containing expressions that can be created by clients
- Pre-defined compliance, including for GLBA, HIPAA, SOX, IBAN, NI, Tax File Number, German Identity and PCI
- Structured data search information which may be held in databases, e.g. client records
- Full and partial document fingerprinting using a centralised multi-protocol solution

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.

Adaptive Redaction

The latest generation of Gateways have options for Adaptive Redaction to be included as part of the 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 as well as revision history information. 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 are blocked due to offensive language can now have the offensive words removed, allowing the sanitized web page to be displayed. 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

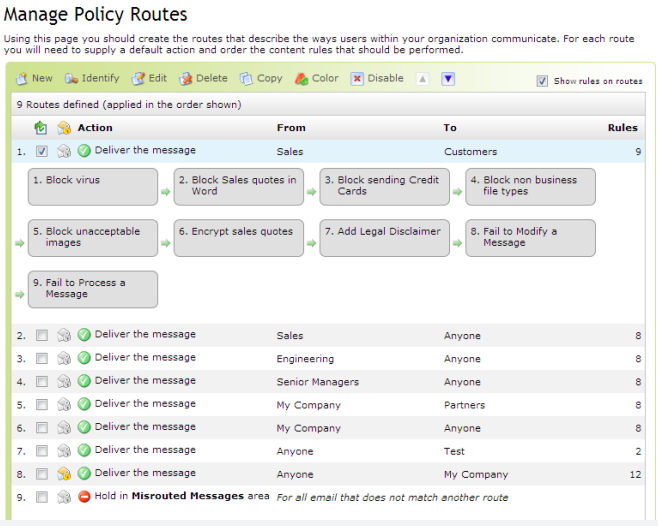
Any security solution today needs to be part of an Information Governance or compliance programme. The SECURE Gateways offer extensive reporting facilities in support of these requirements, enabling system administrators to rapidly create both management and real-time reports. As reports are often required to be shared, these can be created in different formats, whether that be HTML or PDF as a textual representation, or whether the data 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

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.



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

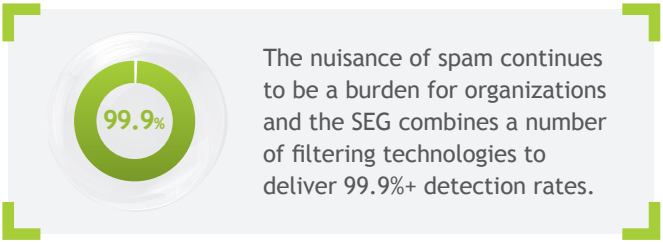
Clearswift SECURE Email Gateway

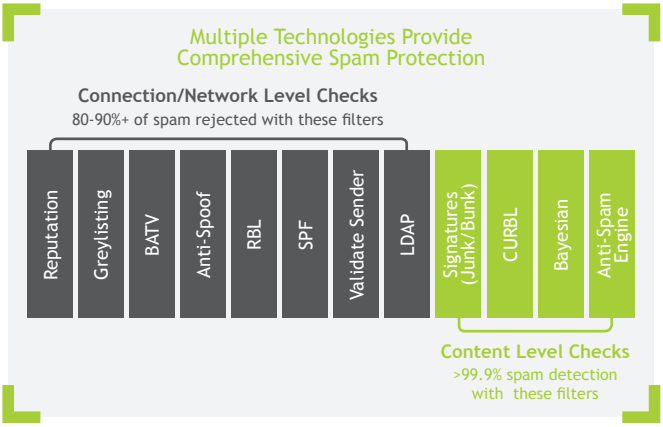
The SECURE Email Gateway (SEG) has its heritage in the Clearswift MIMEsweeper product. Along with the shared functionality, it is designed to offer secure email-based communications closely aligned to an organization's business requirements.

Spam protection

The multi-layer spam defense includes both connection and network level checks coupled with monitoring of content. It incorporates the TRUSTmanager IP reputation system, which uses community feedback on good and bad senders, to effectively block spammers and malware at the IP connection, in conjunction with SpamLogic and a Bayesian filter. A cloud-assisted spam detection system recognizes new spam runs as they are emerging.

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 end-users. 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 Web Gateway

The SECURE Web Gateway (SWG) contains the common functionality, but is designed specifically for dealing with web based communication through HTTP and HTTP/S.

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 and 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

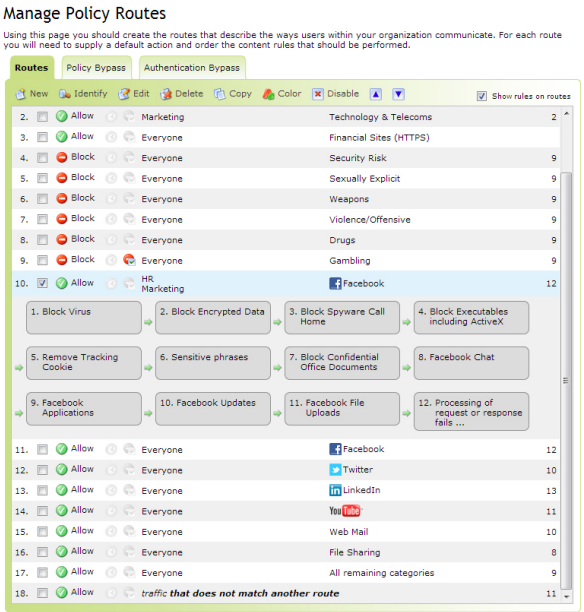
The SWG supports remote clients, meaning that even if the user is not connected to the organization's network, the device will be subject to corporate security policies. This option can also be deployed on BYOD platforms ensuring that corporate information is kept safe no matter where it is being accessed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



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

Clearswift SECURE Exchange Gateway

The SECURE Exchange Gateway (SXG) is designed specifically for securing internal communication in a Microsoft Exchange environment

Deployment

Ease of deployment enables organizations to be able to deploy the product quickly into their Exchange 2007/2010 or 2013 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.

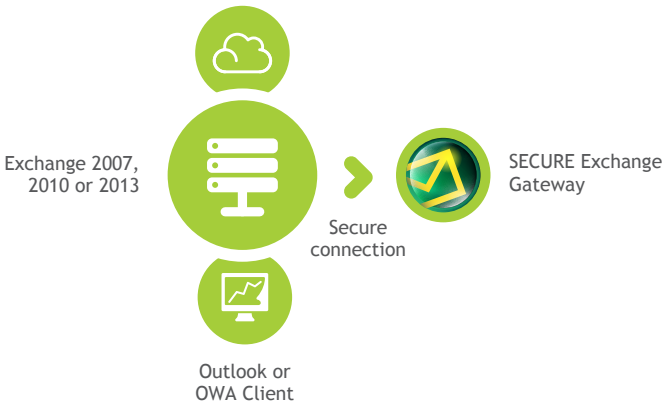
To mirror the resilient and high availability configurations implemented for Exchange Servers, the SXG preferred deployment configuration is for 2 x SXG instances that execute in an Active-Active mode, balancing the workload automatically.

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, 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 Data Leakage prevention including integration with the Clearswift IG server to provide full and partial document fingerprinting.

Clearswift SECURE ICAP Gateway

The Clearswift SECURE ICAP Gateway works with BlueCoat Proxy SG series products to provide information security of the browser traffic using an off-proxy scanning engine.

Deployment

The 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 Proxy SG devices allows the network security features of the BlueCoat device to be complimented by the Clearswift information protection functionality.

For organizations who already have a ICAP AV solution for their BlueCoat system they can consolidate devices and use the SECURE ICAP Gateway to provide both Anti-malware and Clearswifts' Advanced Data Loss Prevention in a single system.

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.

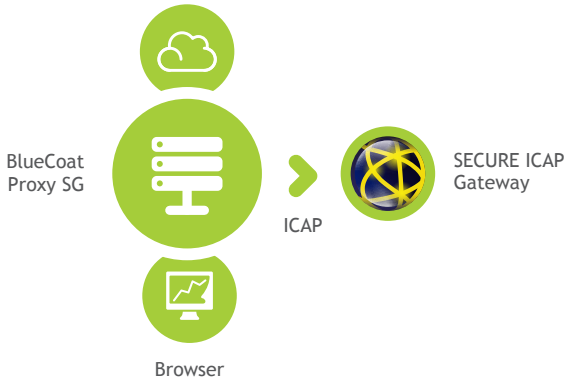
User identities are authenticated by the BlueCoat proxy and passed to the SECURE ICAP Gateway so that granular user policies can be applied to the content coming in and out of the organization.

The SECURE ICAP Gateway goes beyond simply keeping your networks free of viruses, inappropriate content and harmful executable. 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 Data Loss prevention features 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.



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 for current SECURE Email, Web, Exchange and ICAP gateways; our architectural strategy provides future Gateway integration.

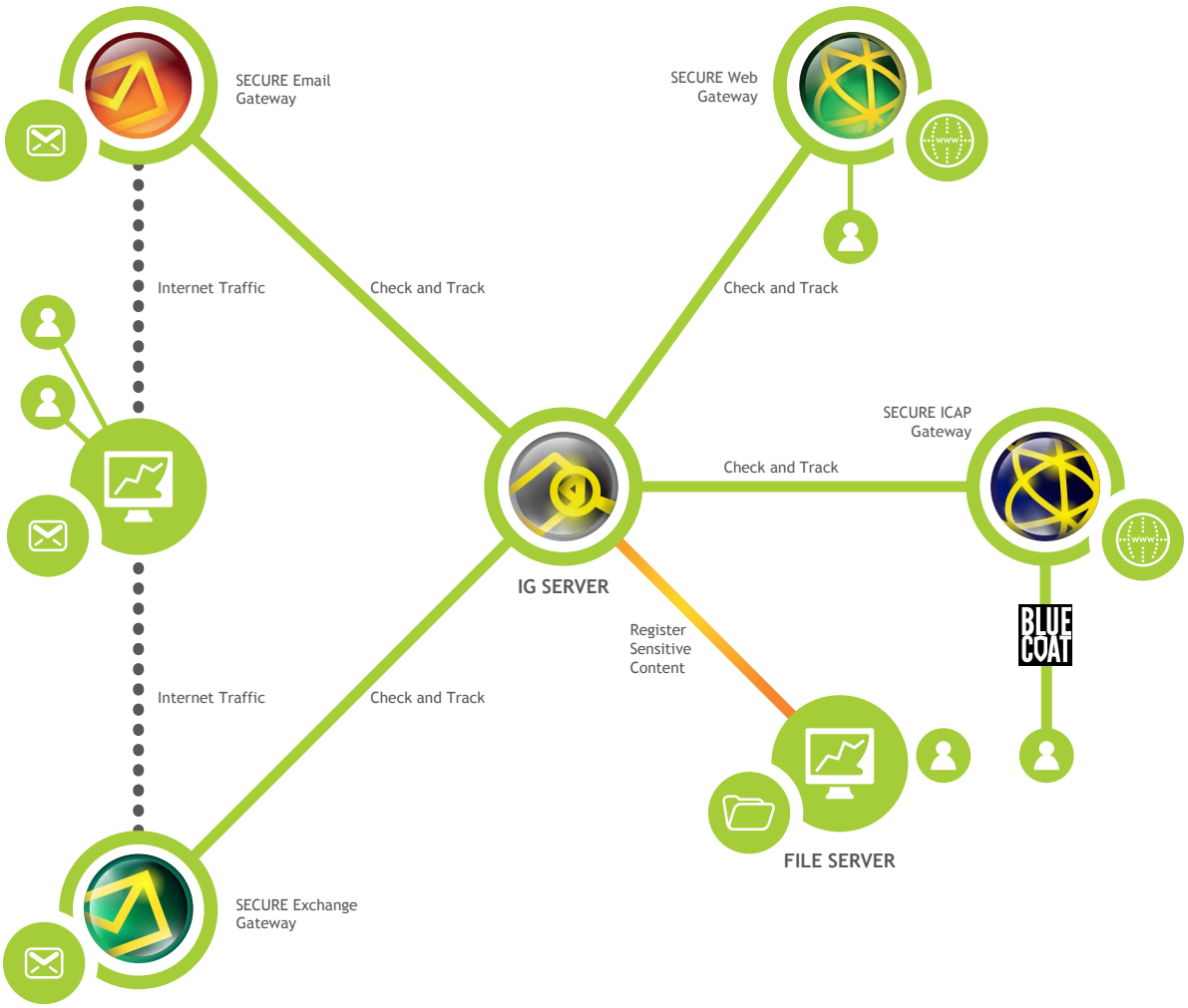
Document management

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. Users can manage the registration of content as well as deregistration when the information's sensitivity status has changed.

They are also notified of any violations if that document or even a fragment of that document is uploaded to a website, sent internally or emailed to an external recipient.

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.



Clearswift SECURE File Gateway

More than just email

Your business may already understand email as a potential risk, but what about files that are too large to attach to a message? The Clearswift SECURE File Gateway can scan large files of up to 16GB as they are transferred internally between departments or externally to partners through FTP or other non-email transfer protocols, ensuring total data security.

Content recognition

The File Gateway's content inspection engine recognizes over 150 different file or format types, using strong signature and data parsing techniques that ignore unreliable external indicators like file extensions. The engine performs recursive decomposition and systematically opens and searches within archive files like ZIP and TAR to locate all embedded objects such as images or active content within Office documents. Inspection continues until there is nothing left to process.

By recognizing particular file types it is possible to set a policy to decide which file types are acceptable and which should be blocked. The inspection also extends to textual content, covering the words and phrases contained within the files.

Two person integrity

As this content can be extremely sensitive the SFG supports a more military style of two-person integrity on policy modifications. Any changes can only be applied once a second administrator has approved the first administrator's changes.

Software Developer Kit (SDK)

The technology at the heart of every Clearswift product, a high-performance deep content inspection engine that provides comprehensive data recognition and thorough content processing is also available for System Integrators as a Software Developer Kit (SDK). The SDK gives access to all key functionality including:

- Data recognition using true-file typing, not simply extension-based recognition
- Recognition of over 150 common formats
- Data integrity checking and verification
- Data decomposition of nested and compressed files (including large files up to 16GB) and the subsequent analysis of extracted files
- Text extraction from standard office files (including MS Office, OpenOffice, PDF and HTML) with pattern matching, programmatic operators and more
- Active content detection recognizing macros and scripts in Office and PDF formats
- Malware detection including interfaces to 3rd party AV engines

The SDK is used by companies who have clients across all vertical markets operating around the world to ensure regulatory compliance, prevent leakage of sensitive or classified information and detect inappropriate communication.

Packaging

With interfaces, documentation and sample code in C, C++ and Java, deployable on x32 and x64 Windows 2003/2008 and RHEL 5/6 platforms, this SDK allows software developers to build client/server applications that can be more 'content aware'.

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

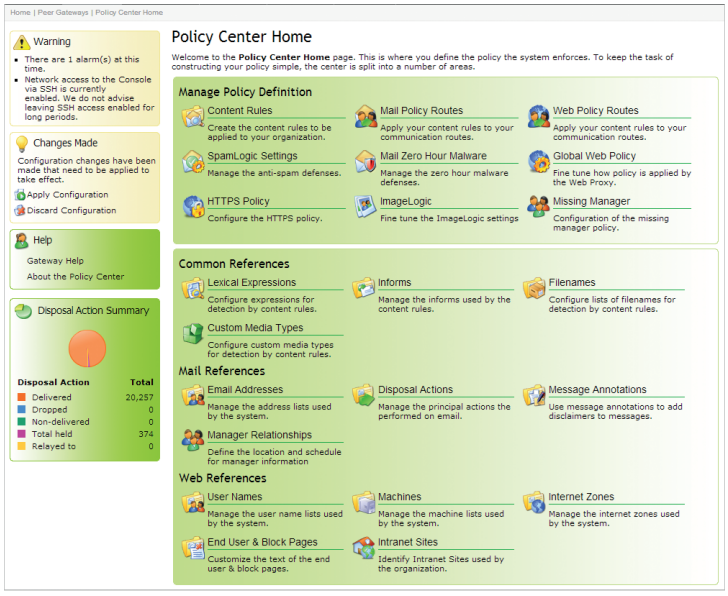
The Clearswift SECURE solutions are also available for deployment on your own server hardware, allowing you to maintain consistency in your environment using systems from your preferred vendor. The SECURE Gateways operate on a hardened Linux distribution, offering ultimate flexibility for your own hardware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

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

> *"World class products, 24/7 support and professional services organization"*

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

The Clearswift SECURE Gateways offer the ability for organizations of all sizes to deploy a sophisticated web and email security solution.

With Clearswifts Advanced Data Loss Prevention (DLP) capabilities built in, they offer protection from inbound threats as well as protecting against data leaks. New technology DLP options are available to make DLP even more cost effective to deploy and to support new ways of working.

Key Feature	SECURE Email Gateway	SECURE Web Gateway	SECURE Exchange Gateway	SECURE ICAP Gateway
Deep Content Inspection	✓	✓	✓	✓
Data Loss Prevention	✓	✓	✓	✓
Anti-virus	✓	✓	✓*	✓*
Encryption*	✓			
Remote Client Support*		✓		
Text Redaction*	✓	✓	✓	✓
Document Sanitization*	✓	✓	✓	✓
Structural Sanitization*	✓	✓	✓	✓
Standard / Advanced* / Premium* Support	✓	✓	✓	✓
Professional Services*	✓	✓	✓	✓

*Additional cost option

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

About Clearswift

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

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

As a global organization, Clearswift operates out of offices in Europe, Australia, Japan and the United States.

Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at www.clearswift.com

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading, RG7 4SA
UK

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

United States
Clearswift Corporation
161 Gaither Drive
Centerpointe
Suite 101
Mt. Laurel, NJ 08054
UNITED STATES

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

Australia
Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street
North Sydney
New South Wales, 2060
AUSTRALIA