clearswift
by HelpSystems

GUIDE *(Cybersecurity)*

Augmenting existing security infrastructure to mitigate information borne risks

Today, all organizations have information security technology in place, but much of it is centered on 'traditional' security applications. For example, anti-virus as part of an endpoint security solution, firewalls and intrusion detection / prevention systems on the network. Often there is additional security around email, in the form of an email gateway offering additional anti-virus and anti-spam detection, while another gateway on the web will also offer anti-virus scanning and URL filtering.

However, times have changed. Threats have evolved as has data protection legislation and organizations are being forced to reassess their information security strategy. Ransomware and advanced persistent threats are becoming increasingly commonplace. Threats are now cleverly 'hidden' in innocuous documents which are then targeted at individuals in organizations – and when opened, the malware is activated and the infection begins. Furthermore, the existing Payment Card Industry Data Security Standard (PCI DSS) and the introduction of the EU's General Data Protection Regulation (GDPR) are creating the need for increased information governance for organizations of all sizes and across all verticals. The scope of the legislation reaches further than the EU, with global organizations who deal with EU citizen data being required to comply or face significant fines.

While new technology exists to mitigate against this next generation of threats and aid compliance, many organizations have investment in existing security solutions, so a 'rip-and-replace' strategy is not an option. Clearswift enables organizations to augment existing security infrastructure rather than replacing it, which effectively 'enhances' infrastructure already in place with additional threat protection and data loss prevention features.

Advanced Information Borne Threats

Cyber-attacks today are not easy to spot as they are embedded into innocuous documents which can be distributed through many different communication channels, see Figure 1: Advanced threats lead to data loss and business risk. This might be malware which is targeted at specific individuals in a business, for example, it might be a CV sent to the HR department, or an invoice sent to the Finance department. Other information loss risks could be a simple 'cut and paste' error from one document to another which results in confidential information being shared with unauthorized individuals. Or sensitive information in the form of document metadata and revision history inadvertently leaked outside an organization.
This data can be harvested by cyber-criminals and used to create targeted phishing attacks.

Figure 1: Advanced threats lead to data loss and business risk

Deep Content Inspection and Consistency

Clearswift has spent more than twenty years developing its Deep Content Inspection (DCI) technology which takes documents and breaks them into their constituent parts. For example this might be an email with a zip file attachment. Inside the zip, see Figure 2: Deep Content Inspection in action, may be a number of documents, and the documents may have further embedded documents. DCI, continuously decomposes the items until there are only single items left. The DCI engine can then continue its inspection at the information level, for example to find a credit card number or other confidential information.

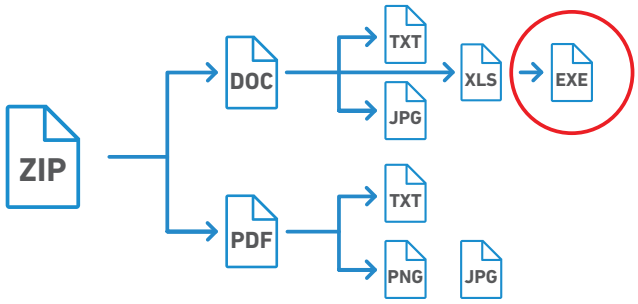

Figure 2: Deep Content Inspection in action

Clearswift uses the same DCI in all its products which also share the same policy engine to ensure consistency, because when it comes to security, consistency is imperative. If there is a weak link in the IT environment, then this will be used by attackers to mount their attack. While the policy engine may be the same, the actions taken can be different – and based on the context of the communication.

Context consists of the originator, the recipient and the method of communication, for example email, through the web or copying to a USB stick. So, the same document being emailed could be encrypted, an upload to a website could result in redaction, while copying to a USB stick could be blocked. However, these actions can also vary based on the individual, so the CEO may be allowed more (or less) flexibility compared to someone working in Finance.

Adaptive Redaction

Adaptive Redaction (AR) was developed to overcome advanced information borne threats and to solve the fundamental challenge which most traditional Data Loss Prevention (DLP) solutions have; the 'false positive'.
AR works in conjunction with the DCI engine to modify the content of documents, including email, MS Office documents, Open Office documents, HTML, web pages and PDF, to ensure that policy is not breached, but the communication still occurs.

There are three components to AR:

- **Data Redaction**
  Replaces sensitive 'visible' information from a document with ***, for example Personally Identifiable Information (PII), or Credit Card data (PCI) which has been cut and pasted in error, or inadvertently left in a document or email.
- **Document Sanitization**
  Removes sensitive 'invisible' information from a document, such as the author name in document properties or any other properties which could create a potential data leak. It can also remove revision history, fast save and comments.
- **Structural Sanitization**
  Removes active content, such as macros and embedded executables from a document or attachment.

Deep Content Inspection can occur at all levels of embedded documents ensuring that critical information is protected at all times.
The false positive is a problem which occurs in traditional Data Loss Prevention solutions whereby an overzealous (or inaccurate) policy stops communication from flowing when it is in fact legitimate.

The result is, while the information may have been protected, the blocked communication stops business. This causes frustration across the organization; the sender who thinks their communication has gone but it hasn't, the IT or other department who needs to deal with the blocked communication and re-write the policy, and for the recipient who was expecting something which hasn't been delivered.

Adaptive Redaction, specifically the Data Redaction component, will remove that piece of the document but leave the rest to continue on. Furthermore, if there is a need for the original document to be sent on, then a very simple mechanism is used whereby the sender's manager (and/or a specific department or group) can authorize the release and sending of the original. This adaptive approach to DLP reduces the operational overheads which would otherwise occur. Distributed operations and ease of use are key to Clearswift solutions.

Augmenting an Existing Email Security System

Email remains the most used business tool for organizations of all sizes and across all verticals, vital for both internal and external collaboration. However, it has also become the most significant threat vector for social engineering and the delivery of ransomware.

Most organizations have an email security gateway where anti-virus and anti-spam technology is deployed to protect users. While these technologies are still relevant, there is now a need for further protection to be deployed.

Clearswift enables existing IT security to deploy the latest state of the art email security technology to augment any existing solutions - see Figure 3.

Clearswift's ARgon for Email enables businesses to mitigate risk through the Adaptive Redaction functionality.
A set of default polices are provided to protect against the most common threats at your perimeter:

1. Remove active content from email and documents. Protects against malware and ransomware.
2. Remove document properties, revision history and fast save data. Protects against information harvesting that can be used for targeted phishing.
3. Removal of credit card details. This example of data redaction will mitigate the risk of PCI DSS non-compliance.

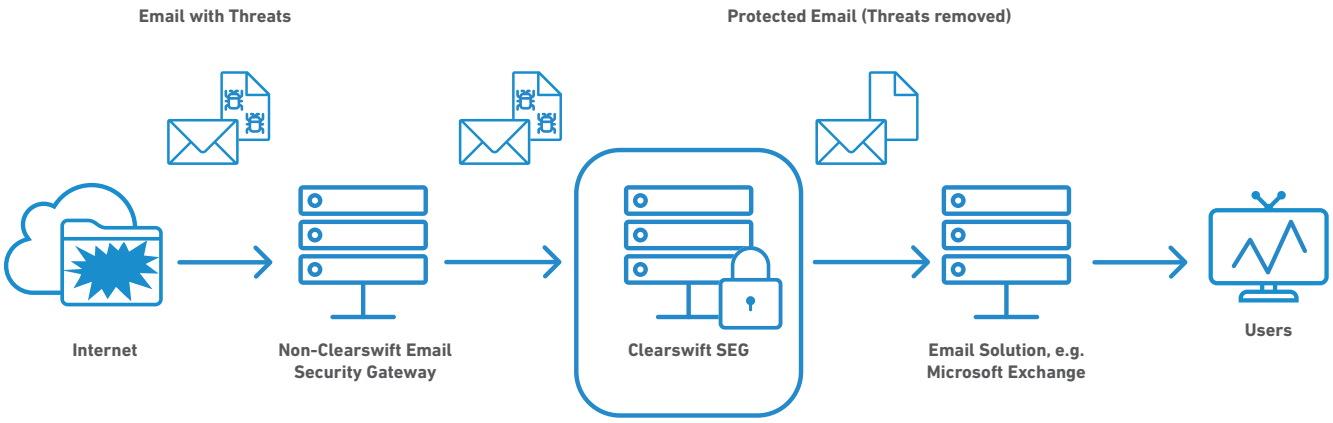

Figure 3: Clearswift augments existing email security infrastructure

The default policies can be customized to cover organization specifics. Clearswift policies are direction agnostic, so can be applied in either direction. For example, data redaction can be used to remove credit card information to prevent it entering an organization as well as preventing it from leaking out. This is useful if the email system is not PCI DSS compliant. Similarly, structural sanitization can be used to remove active content as it leaves the organization. One example of this is with financial institutions where macros in spreadsheets are part of their Intellectual Property (IP) – and so shouldn't be shared. Automating the removal protects the IP and doesn't rely on users needing to remember to do it manually.

Augmenting Infrastructure to enable Internal Email Security

While many organizations are improving their security around collaboration solutions by restricting access, internal email still remains a risk – as anybody can send anything to anyone internally. While all employees should be deemed as trustworthy, experience would indicate that this isn't always the case. The likes of Bradley Manning and Edward Snowden are high profile instances of malicious insiders, while the lower profile breach at Sage in 2016 is another more regular occurrence.

Traditional Data Loss Prevention tackles information leaving an organization, but the Clearswift Secure Exchange Gateway enables organizations to augment their Microsoft Exchange environment with internal DLP and Adaptive Redaction. As the solution is 'off-box' and direction agnostic, the impact to the Exchange server performance is minimal and all email can be monitored and action taken if required, see Figure 4 below.

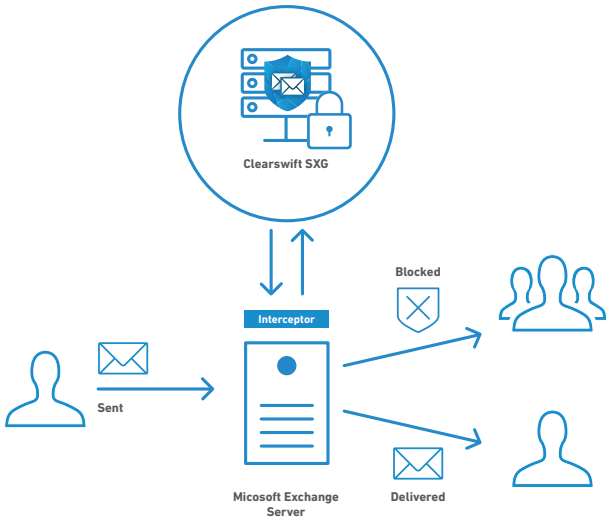

Figure 4: Augmenting infrastructure to enable internal security

As with all Clearswift products, the same Deep Content Inspection engine is used, so the policies can remain consistent with other deployed solutions. As this is about internal email, most deployments are around detection rather than blocking or redaction. Default redaction policies are available to prevent propagation of Credit Card numbers through the organization, but its primary use is to segregate

business units from unauthorized sharing of critical information without the need for a complete segregated Exchange solution.

Augmenting an Existing Web Security System

In the same way that most organizations have some email security, they also have some level of web security. Usually this is through a proxy which can carry out URL filtering and anti-virus scanning on downloaded files. Proxies, such as those from Blue Coat or F5 have the ability to add additional functionality through a standardized interface, ICAP. The Clearswift Secure ICAP Gateway can be used in conjunction with any proxy to add another level of security to prevent information borne threats - see Figure 5 below.

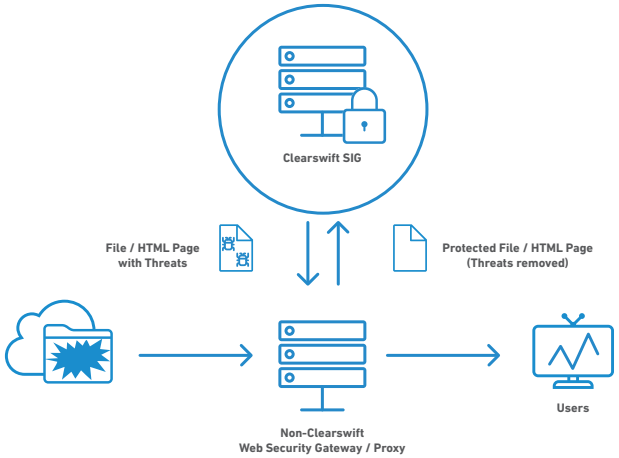

Figure 5: Augmenting existing internet security with Clearswift

The Clearswift Secure ICAP Gateway can also be used in a reverse proxy configuration, whereby corporate websites can be protected both from the upload of documents with malware and ensure that document properties and other information which is frequently harvested to aid in phishing attacks is automatically removed from any documents which are downloaded.

There are default policies which can be deployed to ensure consistent protection across both email and the web. Customized polices can be used to add additional controls, over specific web sites including social media and cloud collaboration sites. More than seventy percent of ransomware attacks are delivered through the web. The most popular documents are CVs and job offers. These can be delivered as an attachment to an email, but are often a URL from which the document can be downloaded. In many cases these are also accessed through an employee's personal web based email.

Augmenting Existing Cloud Security

Many organizations are moving their applications into the cloud. While some cloud application vendors offer rudimentary security around their solutions it is generally accepted that more is required, especially to address compliance needs and mitigate advanced threats. Clearswift can be deployed on premise, or in the cloud, offering flexibility to support the organizations working practices and strategic direction.

Summary

Today's security threats are constantly evolving and the CIO needs to protect the organization from both attacks and data loss risks. However, changing IT infrastructure is not something which can be done quickly and simply, which leaves the organization at risk from the new threats. Clearswift enables protection against the new threats by augmenting the existing IT security infrastructure rather than requiring it all to be replaced.

Clearswift solutions can augment existing email and web infrastructure to enable the highest level of security and data protection for safe collaboration across an organization's digital collaboration channels.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.