clearswift
by HelpSystems

GUIDE *(Cybersecurity)*

How to Enhance a Data Loss Prevention Strategy using ARgon for Email

Organizations need to secure sensitive data and prevent cyber-attacks, yet still communicate effectively with customers and suppliers. They need maximum protection for incoming and outgoing email, while also minimizing overheads and operational costs.

This guide introduces ARgon for Email – the solution from Clearswift that seamlessly integrates advanced data loss prevention functionality to existing infrastructures. ARgon for Email enhances the capability of existing email gateways, protecting the initial investment, while improving security and reducing risk.

Minimizing the Risk to Business

No organization wants to be on the receiving end of a costly and damaging fine for non-compliance with industry regulations, which is why Data Loss Prevention (DLP) solutions have a clear aim: to protect sensitive data.

They need to safeguard against inadvertent data leaks, where employees accidentally expose or share confidential information with unauthorized parties, and data exfiltration, where valuable data is stolen by malicious actors for monetary gain. Ideally, organizations need to manage these risks without impacting their ability to continuously collaborate and it's this particular requirement that's challenging to solve.

The Issue with Traditional DLP

Deploying an effective DLP strategy is not without its trials and tribulations. Traditional DLP solutions not only reduce risk, but they also end up reducing collaboration. This is because they operate by stopping and blocking every email that looks like it might break the organization's security policy. The emails that end up in quarantine then need to be managed and that burden usually falls to the IT team. Some of the emails are genuine and can be authorized for release or deleted, but in other cases the emails should not have been quarantined in the first place. These are known as false positives and they either occur when policies are imprecise or when the content looks like sensitive data (such as payment card information) but in fact isn't – either way the communication is prevented from reaching its destination, causing frustration. This frustration, coupled with the fact that managing large numbers of quarantined emails is time consuming and costly, often leads to the solution being toned down or switched off completely.

Clearswift has addressed the problems associated with traditional DLP solutions with a unique technology called Adaptive Redaction.

Game Changing Adaptive Redaction

The concept of Adaptive Redaction is simple; automatically remove the information that breaks policy and leave the rest of the communication to continue to its destination and do so without the need for manual intervention.

In practice, the solution is very sophisticated as it not only understands the content, but also the context in which it is being sent – i.e. who is sending what, to whom. The 'who' comes from inspecting the directory service which provides the organizational structure – either using Microsoft Active Directory or another LDAP compliant solution. Policies can be set so that certain individuals, teams or departments have more flexibility than others. By combining the content with the context, the solutions changes behavior. For example, the company CEO sends a specific document and the solution automatically encrypts it depending on the recipient.

Unparalleled Deep Content Inspection

It is Clearswift's unrivalled Deep Content Inspection (DCI) technology that enables Adaptive Redaction to occur. It takes emails and any attached documents apart, detecting and removing only the information that breaks policy, and rebuilds them before sending them on their way. This process removes the risk in real time and there's no delay to the communication.

The ARgon Solution

There are three key features within Adaptive Redaction, all of which are enabled in the ARgon solution:

- Data Redaction
- Document Sanitization
- Structural Sanitization

Data Redaction

ARgon for Email automatically redacts sensitive data from incoming and outgoing emails. This could be data such as payment card information (PCI) or personally identifiable information (PII) such as social security or national insurance numbers. Not only does this keep the communication secure, it also keeps it compliant.

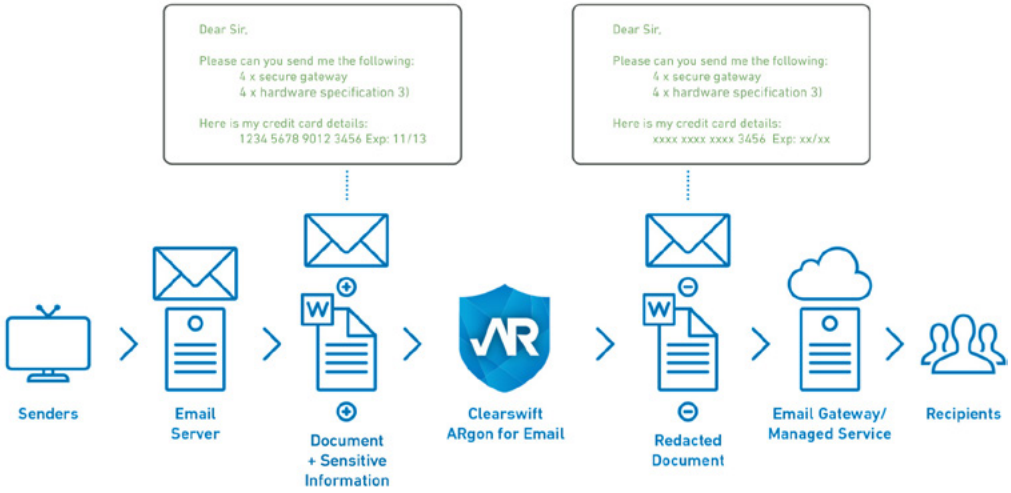

Figure 1: Data Redaction

When a communication is changed, both the sender and recipient are informed that an action has been taken. A security event is also raised so the IT team can take further action if required.

Document Sanitization

Hidden data also carries risk. Document properties, such as usernames, comments, and revision histories, often contain sensitive information that could be used as the basis of a cyber-attack. To prevent this information from being exfiltrated, documents can be sanitized (wiped clean) before they leave the organization.

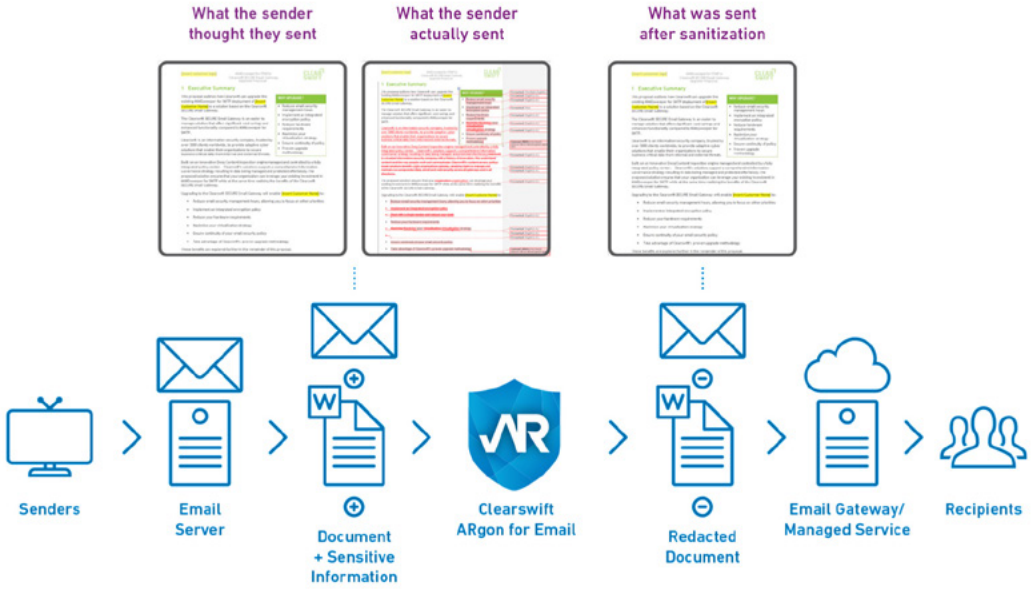

Figure 2: Document Sanitization

For many organizations, the policy would apply to all documents. Some however will want to leave certain properties such as protective markings or document classifications in place. Thanks to the fine level of granularity provided by Clearswift's DCI technology, these can be left alone while the other properties are removed, ensuring that confidential information remains protected.

Structural Sanitization

Today, email is a common method of delivery for Advanced Persistent Threats (APTs). Active content, such as macros from Office document, scripts and ActiveX, is embedded in documents that, when opened, releases malware into the network. Detecting APTs is a challenge because they've been designed to evade traditional email security defenses such as anti-virus solutions. Automating the removal of all active content is therefore an effective way to protect the organization and ARgon for Email achieves this through the Structural Sanitization feature.

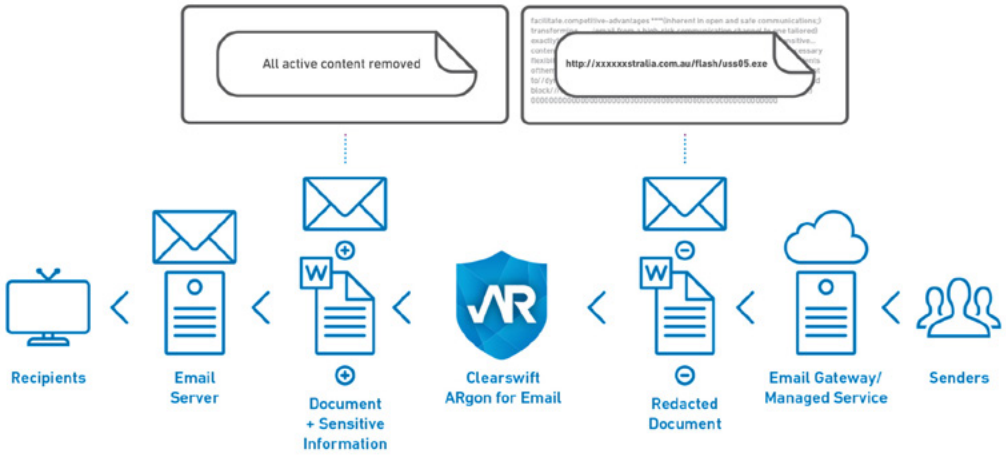

Figure 3: Structural Sanitization

Easy and Rapid Deployment

ARgon for Email can be deployed inline, or in parallel with any email gateway – protecting the existing investment, while enhancing security and reducing risk.

To ensure it can be deployed rapidly, ARgon for Email is shipped with several default policies, policy actions and reports. Additional customization can be applied when required. By default, it protects all emails and attachments leaving and entering the organization by:

- Redacting all credit and payment card details
- Sanitizing all meta-data, revision history and fast save information
- Removing all embedded active content.

All notifications of a breach in policy are sent to the IT Department, but Manager Notifications can also be readily enabled. It can also be integrated with a SIEM solution for further analysis. Other policies can be easily applied, for example it can also redact other standard tokens such as National Insurance and Social Security numbers.

Figure 4: ARgon for Email deployment

Building a Business Case for ARgon

As with any investment in IT today, there is a need to build a business case to justify its purchase. This can be challenging, especially for security solutions as they provide insurance against potential cyber-attacks and data breaches and this can be hard to quantify. When it comes to managing risk, most organizations take probability and consequence into consideration. In building a busines case for ARgon, it is easier to start with the potential consequences, and these include (but are not limited to):

- Non-compliance with industry regulations for example Financial Conduct Authority (FCA) or HIPAA, resulting in a fine and loss of reputation
- The exfiltration of product designs, intellectual property, contract bids, and other valuable assets that could reduce market competitiveness
- Hackers gaining access to internal systems causing disruption and loss of data.

Next comes probability, and in today's digitally connected world the probability of an organization suffering a data breach or cyber-attack is very high. Unfortunately, it's no longer a question of 'if, but 'when' it occurs. The probability of an action being inadvertent rather than malicious is also very high. Human error is one of the most common causes of a data breach, and an employee accidentally emailing sensitive data to the wrong person is a good example.

Although often used as a scaremonger tactic, it is worth taking the average cost of a data breach into consideration when putting a business case together. This varies year on year, but the latest research suggests it has risen by 10% over a five-year period to $3.86M in 2020.

Finally, as ARgon for Email is not designed to 'rip and replace' existing solutions but to augment their functionality, it provides a cost-effective alternative to a replacement strategy. It offers everyday protection from data loss and next generation threats and can be added easily at any time. It is also capable of processing many thousands of messages per hour on a regular server or virtual platform, allowing organizations to reduce capital outlay.

ARgon: Flexibility and Security Combined

Today's organizations, whether a global multi-national or local enterprise, require security solutions that are flexible in the way they work and adaptive to evolving needs – both from a business and a regulatory perspective.

With ARgon for Email, all organizations – no matter which email security solution they have deployed – can benefit from the advantages brought by Clearswift's award-winning Adaptive Redaction technology. It enhances productivity by reducing the number of false positives typically associated with 'stop and block' DLP solutions, as well as removing one of the biggest external threats to organizations today, the APT.

Next Steps

To find out more about the ARgon for Email solution, download the datasheet or request a demo online.

Additional resources are available at www.clearswift.com

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.