clearswift
by HelpSystems

DATASHEET *(Email Security)*

ARgon for Email

Add Advanced DLP Capabilities to Any Email Gateway

ARgon for Email is the add-on security solution that instantly improves your organization's Data Loss Prevention (DLP) capability. It enhances the functionality of existing email gateways, protecting the initial investment, while improving security and reducing risk.

ARgon for Email allows organizations to benefit from the advantages brought by Clearswift's award-winning Adaptive Redaction technology. It Secures sensitive data and helps prevent cyber-attacks, yet still allows the organization to communicate effectively with customers and suppliers. It provides maximum protection for inbound and outbound emails, helping to keep the organization compliant with industry regulations.

Balancing Security with the Need to Continuously Collaborate

No organization wants to be on the receiving end of a costly and damaging fine for non-compliance with industry regulations. To reduce risk, organizations deploy DLP solutions to safeguard against inadvertent data leaks and data exfiltration.

Many DLP solutions are purchased and never successfully deployed because they are difficult to configure and generate too many false positives. Typically, they stop and block any email that looks like it may break the organization's security policy, causing large numbers to end up in quarantine. The burden of managing quarantined emails falls to the IT or messaging team. Some emails are authorized for release or deleted, but others should not have been quarantined in the first place. False positives occur when policies are imprecise or when content looks like sensitive data (such as payment card information) but in fact isn't. Either way the email 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.

The ARgon Solution

Clearswift addresses the issue of false positives with a unique technology called **Adaptive Redaction.** Adaptive Redaction automatically removes the content that would cause the DLP solution to stop and block the email in the first place. In real time, a **Deep Content Inspection** engine detects and removes only the information

PRODUCT SUMMARY

KEY FEATURES

- Standard SMTP messaging technology makes it hygiene service agnostic
- Integrates with products from Cisco, Symantec, Sophos, and Microsoft
- High performance: capable of processing many thousands of messages per hour
- Bi-directional data redaction in document and images ensures compliance
- Threat protection and sanitization to combat malware and phishing
- Easy configuration with built in compliance dictionaries
- Lexical Expression Qualifiers to minimize false positives
- Supports TLS encryption

SYSTEM MANAGEMENT

- Flexible and granular policy control
- Active directory or LDAP integration
- Easy to use web-based management interface with role-based access control
- Comprehensive workflow options
- SMTP management alerts
- Monitor mode enables policies to be fine-tuned before enforcement
- Detailed reporting and SIEM integration

DEPLOYMENT OPTIONS

- Public cloud deployment on Microsoft Azure or Amazon Web Services
- Virtual VMware environment
- Software image on own or packaged hardware

that breaks policy, leaving the rest of the communication to continue without delay. Built in compliance dictionaries and over 200 pre-defined PCI and PII tokens simplify policy definition and deployment. ARgon for Email also detects, protects, and audits data using Lexical Expression Qualifiers to validate sensitive information.

Game Changing Adaptive Redaction

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

1. Data Redaction

ARgon for Email automatically redacts sensitive data from incoming and outgoing emails in real time. This could be sensitive data such as social security or national insurance numbers, or payment card information. Not only does this keep the communication Secure, it also keeps it compliant. 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.

2. 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.

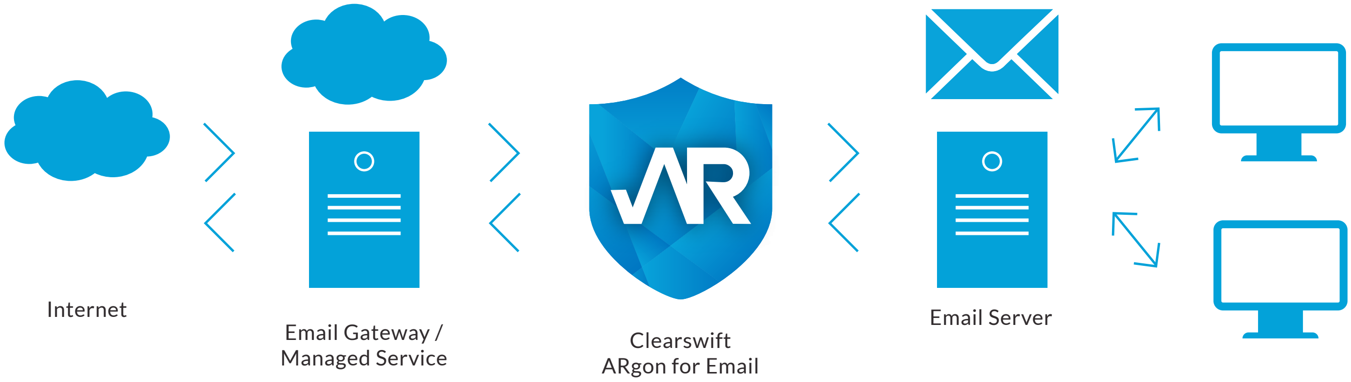
For many organizations, the policy would apply to all documents. Some however will want to leave certain properties such as protective markings or document classifications in place. Thanks to the fine level of granularity provided, these can be left while the other properties are removed, ensuring that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

3. 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.

Ease of Deployment

ARgon for Email is deployed very easily, without the need for weeks of intrusive service implementation. It sits between the email hygiene solution and the internal exchange server.



ARgon for Email uses standard SMTP messaging technology to enable compatibility with any email gateway solution, located on-premise or in the cloud. It supports Exchange, GroupWise, Lotus Notes, SMTP and POP exchange servers.

Cost Effective DLP

Today's organizations require security solutions that are flexible in the way they work and adaptive to evolving needs. As ARgon for Email is not designed to 'rip and replace' existing infrastructures but to augment their functionality, it provides a cost-effective alternative to a full replacement strategy. It is integrated into existing infrastructures easily and offers effective protection from data loss and Advanced Persistent Threats.

Let's Get Started

To see it in action, visit www.clearswift.com to arrange a demo.

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.