clearswift
A HelpSystems Company

ARgon: The Foundation of an Adaptive Data Loss Prevention Strategy

Dr. Guy Bunker

Table of Contents

Introduction

Clearswift has led the way in Deep Content Inspection for nearly two decades, and was one of the first companies to have an integrated Data Loss Prevention solution for email almost ten years ago. However, it has been the introduction of the award winning Adaptive Redaction technology which today offers a unique ability to reduce information risk to business which has driven the ARgon vision and can now be used by any organization as the foundation for an Adaptive Data Loss Prevention strategy.

The challenge for Clearswift has been to package Adaptive Redaction such that organizations that do not have a Clearswift SECURE Gateway are able to realize the benefits that over 2 million seat holders experience today; maximizing protection while minimizing the overhead and operational costs. This has now been achieved, and the first release to market is ARgon for Email, with the ARgon family being extended throughout 2015.

Business Risks and Needs

It wasn't that long ago that the need for Data Loss Prevention solutions was recognized. The initial use case was for inadvertent leaks of personal information which would result in reputational damage. Time passed and malicious attacks are being carried out with a view to stealing information, particularly financial information such as credit card numbers, and then monetizing it on the underground economy.

Technology solutions, coupled with process change and employee education becomes the order of the day and with it, changes in legislation become the impetus of putting a solution in place. Historically Data Loss Prevention was all about reducing business risk, by adequately protecting the information that the business is entrusted with. The same is true today, but the landscape of threats has continued to evolve, requiring technology innovation to reduce business risk whilst also striving to eliminate any loss of productivity and subsequent financial implications.

Collaboration and the Cloud

Over the past few years, the rise (and rise) of cloud collaboration and use of personal devices (or Bring Your Own Device, BYOD) has seen a change in requirements for a DLP solution. Understanding that change in business process is happening, whether the IT department likes it or not, is important when looking at how a solution can be deployed to help. While people are seen as the strongest component in any security solution, they are also the weakest – especially if they actively have to remember to do something different. The challenge is that individuals need to be flexible in their day-to-day activities and adapt to change on a regular basis. For example, laptops. While no-one plans to lose their laptop (unless it is a cunning ploy to get a new one?!), it wasn't front page news if you did – just an annoyance as you needed to get a new one and to restore the appropriate applications and data. However, that all changed at the end of the 2000's when legislation came in to protect critical information on (potentially) lost laptops by requiring that there should be encryption – and if you couldn't prove that encryption was deployed, you were fined. So encryption was added to the list of 'standard' security features that were required on an enterprise laptop. People still lose laptops, but the risk associated has been minimized. Security for the information was delivered through physical security of the box the information was stored on.

It's Not Just Financial Information

Unlike attacks such as those on Vodafone[1], South Korean Citizens[2] and Target Corp[3], recent cyber-attacks including Sony[4] and Community Health Systems[5] have shown that the cyber-criminal is no longer just after credit cards or bank details, but almost any information they can use which can then be monetized.

If you peel back the media coverage about the cancellation of screening 'The Interview' that dominated the Sony data breach attack, the really damaging and longer lasting effect was the specific targeting of information which was then used to damage the reputations of senior executives and the company itself. However other attacks have targeted Intellectual Property, for example the vacuum cleaner manufacturer Dyson and seemingly innocuous information, such as loyalty cards, which can then be used in phishing attacks.

There have been a number of breaches, such as the Australian Federal Police[6] and NMBS[7] whereby it was not the obvious information in a document which caused the breach, but rather the information that was 'invisible' or missed, such as that in the document properties, comments or the revision history. The need to collaborate more widely is pushing up the number of mistakes that employees make where they are unaware of what can, and what cannot be, shared. Furthermore, the primary delivery mechanism for Advanced Persistent Threats (APTs) and Ransomware is to embed malicious active content in innocent looking documents. Once again the need to collaborate with external organizations is driving up the infection rate as recipients are unaware of the threats that an innocuous looking document can pose.

The Downside of Traditional DLP

Implementing a DLP solution is not without its trials and tribulations. The theory is simple, put in place something that will reduce risk. However, traditional DLP solutions don't only reduce risk they also end up reducing collaboration as information gets stuck in quarantine areas due to a false positive action – stopping and blocking information that should have gone out. More often than not, the false positive could have been avoided if the information originator had removed it before it was sent. However, remembering to do this is not easy – for the vast majority of employees, security is not their primary job and so is not top of mind.

The result of blocked communication is not only to slow business, but to also create frustration. Frustration from the sender that the information hasn't been sent. Frustration from the recipient that the information hasn't been received. And frustration from IT and/or the compliance department as they now have people on the phone asking for a release of an email that was innocent and should have been sent. All too often, the business risks associated with the DLP solution are higher than the benefits, so the solution is either switched off or toned down to a point of not providing any valid protection.

For most communications that are blocked, had a specific piece of information been removed, the information would have travelled unhindered and without frustration. Clearswift has addressed the problems with traditional DLP and the issues with false positives with a unique technology, Adaptive Redaction.

[1] http://www.ft.com/cms/s/0/d0f7608c-1bae-11e3-94a3-00144feab7de.html#axzz3QbJ9GCBo
[2] http://www.securityweek.com/20-million-people-fall-victim-south-korea-data-leak
[3] http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219
[4] http://www.bbc.co.uk/news/technology-30692105
[5] http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818
[6] http://www.theguardian.com/world/2014/aug/28/federal-police-mistakenly-publish-metadata-from-criminal-investigations
[7] http://www.flanderstoday.eu/business/nmbs-data-leak-was-breach-privacy

Adaptive Redaction

Adaptive Redaction (AR) is conceptually simple; automatically remove the information that breaks policy and leave the rest to continue unhindered to its destination. In practice the solution is very sophisticated as it not only needs to understand the content but also the context in which it is being communicated.

Content

From a content perspective Clearswift differs from other DLP solution vendors in that it utilizes its own Deep Content Inspection (DCI) technology which enables Adaptive Redaction to occur. This means not only taking an email and any attached archives or documents apart, but also being able to re-build them, omitting the information that breaks policy. With this understanding there are three key features within AR, all of which are enabled in the ARgon solution.

- **Data Redaction**
- **Document Sanitization**
- **Structural Sanitization**

Data Redaction

The simplest way to explain data redaction is by way of an example. A customer places an order with an organization and includes their credit card number (might sound daft to us as security aware professionals, unfortunately it happens all too often!) The customer support organization hits 'reply' to acknowledge receipt and the email is blocked – as it contains a credit card number. With ARgon, the Data Redaction feature just removes the credit card information – but sends the 'new' version on, see Figure 1.

When a communication is changed, both the sender and the recipient are informed of the action, as well as a security event being raised to enable the IT department to take action if required. For 95% of all events, an innocent error was made by the individual and so no further investigation is required.

ARgon enables fast release of the original message if required, by simply clicking on a URL in a inform email. The policy can be set such that it can be done by an authorized individual, the sender's manager, or another named individual or department.

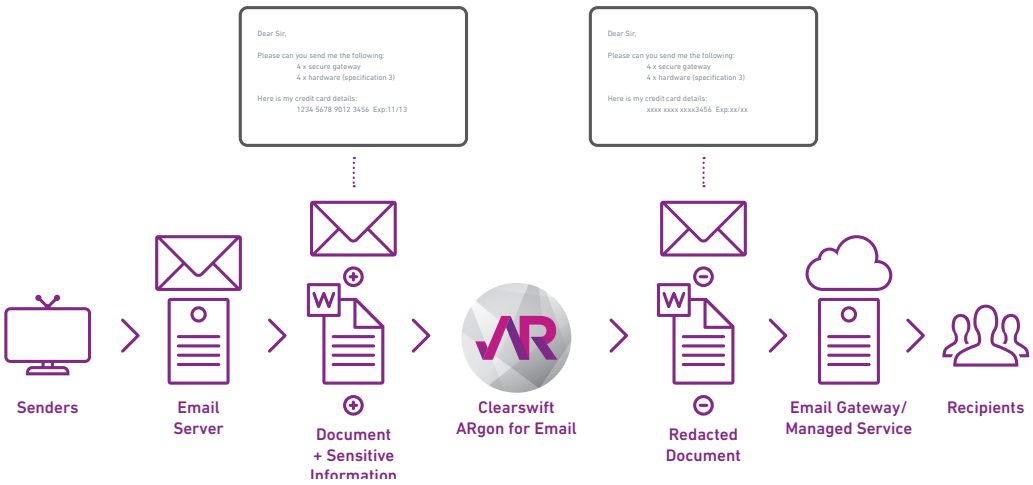

Figure 1: Data Redaction

Document Sanitization

Document Sanitization enables organizations to readily set a policy regarding document properties and revision history. For many, the policy is simple and applies to all documents leaving the organization – document properties which could contain sensitive information, such as usernames, must be removed, as should all revision information, see Figure 2.

Clearswift's expertise over the last 20 years in DCI provides a fine level of granularity on removing things such as document properties, so if there is protective marking or classification in place, these can be left alone while the others are removed. Along with document revision history, fast save information can also be removed to ensure that what the sender thought they were sending out, was indeed what was sent out.

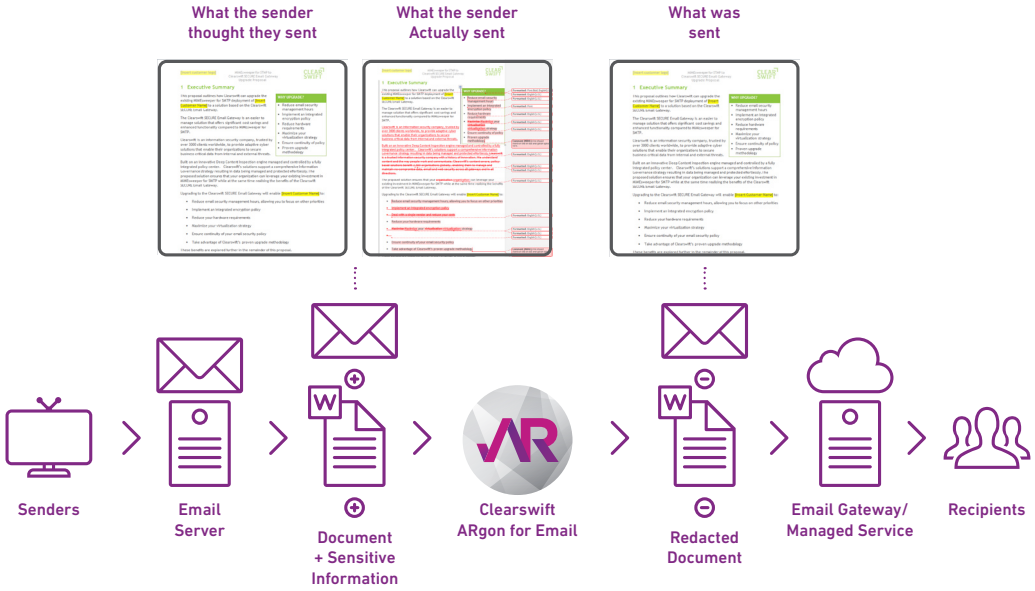

Figure 2: Document Sanitization

Structural Sanitization

Today, it is embedded active content which is the largest cause of Advanced Persistent Threats (APTs). However, since this is targeted at specific individuals or organizations it is frequently not picked up by traditional Anti-Virus solutions, however detecting APTs is a challenge and for many organizations the simple removal of all active content is all that is required to protect against these most insidious of threats, see Figure 3. Of course if it is removed in error, a false positive, then a rapid release mechanism is provided which can be enacted by an authorized individual or the sender's manager, or another named individual or department.

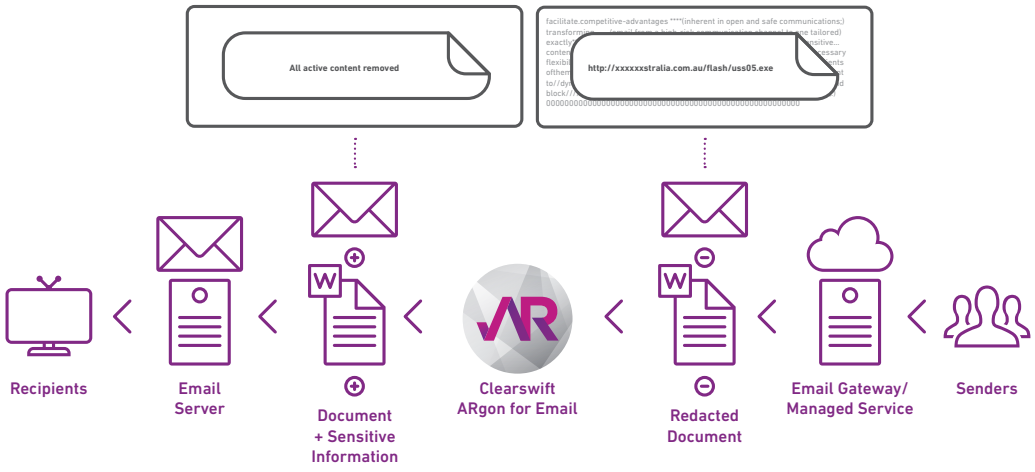

Figure 3: Structural Sanitization

Context

Context depends on a number of different factors. In essence, who is sending the information, who is receiving it and how is it being communicated. In this case the 'who' is provided by inspecting the directory service which provides organizational structure – either using Microsoft Active Directory or another LDAP compliant solution. Policies can be set so that the CEO can potentially have more flexibility than someone working in finance.

Adaptive is the key word in Adaptive Redaction. By combining the content with the context, the solution changes behavior. So, even with the CEO sending a specific document, the solution may secure it in different ways depending on the recipient and the communication method. For example, for email it might be encrypted, whereas an upload to the web may be redacted, while a copy to a USB stick could be blocked.

Direction Agnostic

Traditionally DLP has been thought of protecting critical information from leaving the organization. Today's increasing information supply chains requires more flexibility and there is a need to protect the organization against information coming in – as well as going out. This is not just about removing malware through removing the embedded active content, but also using data redaction in specific cases as well.

For example, for one customer, their network was not PCI DSS (Payment Card Industry Data Security Standard) compliant; the challenge came when a third party processor sent an email with credit card details in an attachment (this only occurred in exceptional circumstances, which in practice was several times a month.) As the receiving network segment was not certified compliant, a process needed to be enacted to purge the information from the network in order to keep the auditors at bay – data redaction was deployed to remove the offending information before it arrived on the uncertified network, but kept the rest of the communication intact so it could be acted upon.

Likewise, the removal of active content can be deployed on outbound communications, for example in removing Intellectual Property in the form of macros within spreadsheets from an investment broker.

The ARgon Solution

Adaptive Redaction is rapidly becoming a standard within all Clearswift clients as the immediate benefits around information risk reduction are realised. When speaking with our partners and prospective clients it became apparent that this unique functionality should be available in conjunction with other email and web security solutions. The ARgon appliance was created for just this purpose.

The initial appliance is ARgon for Email, with further appliances being released throughout 2015 to incorporate further communication channels.

ARgon for Email can be deployed inline, or in parallel with any existing email gateway – protecting the existing investment, but enhancing the security and reducing risk with Adaptive Redaction, see Figure 4.

Figure 4: ARgon for Email deployment

ARgon ships with a number of default policies, policy actions and reports to ensure a rapid deployment and deliver instant risk reduction. Further customization can then be applied when and if required.

The default policies for ARgon for Email are:

- All credit card numbers redacted from all email and attachments leaving the organization.
- All meta-data, revision history and fast save information to be removed from all email and attachments leaving the organization.
- All embedded active content to be removed from all email and attachments entering the organization.

As a default, all notifications of a breach in policy are sent to the IT Department. Manager notification can also be readily enabled, as well as integration with a SIEM solution.

Other policies can be easily enabled, for example redacting out other standard tokens such as National Insurance and Social Security numbers.

Building a Business Case for ARgon for Email

As with any investment in IT today, there is a need to build a business case to justify the purchase. This can be challenging, especially for security solutions.

Many security solutions are about insurance, insurance from hackers gaining access to internal systems and then creating havoc. Data Loss Prevention solutions are really designed to keep the organization safe from the regulatory authorities and legislator who would jump into action should a breach occur. Solutions driven on FUD (Fear, Uncertainty and Doubt) are not what the modern organization needs. Today's organization, whether a global multi-national or a local enterprise, requires solutions which can be flexible in the way they work and adaptive to the changing needs – both from a business and a regulatory perspective. They need to be able to provide 'everyday value', not just be useful in a time of threat. And, most importantly, they must not hinder business or individual productivity.

Risk in a business comes down to probability and consequence. In building a business case for ARgon we need to look at the same, however it is easier to start with the consequences, these include (but are not limited to):

- Are you regulated, for example by the Financial Conduct Authority (FCA) or HIPAA?
- Do you have product designs or other Intellectual Property that you need to protect from competitors?
- Do you have sales information, for example bid for new contracts or purchase of goods which would be damaging if it fell into the wrong hands?
- Are you PCI compliant; would the arrival of credit card information on your network cause a headache for your CIO, CISO, compliance or audit office?
- Do you manage data that underpins critical national infrastructure?
- Do you hold personal customer or employee data?

The next piece is to look at probability. Actually, when it comes to probability, the chances of having a breach are around 100%, it is no longer a question of 'if', but rather 'when'. So, it is therefore better to look at likelihood of a particular action, including:

- Have you ever had a data breach? When was the last time?
- Have you ever sent an email containing critical information to the wrong person?
- Have you ever received email containing critical information in error?
- Have you ever had a malware outbreak on your network caused by embedded active content in a document?
- Have you ever suffered embarrassment from revision history being left in a document and accessed by someone who shouldn't have seen it? (The most common case here is in sales; where an old proposal is taken and modified for a new client – but then the old information is not removed from the document, so the new recipient can still read it.)
- Do you have people working in your organization?

If you answer yes to one or more of these questions, then it is worth looking at some of the costs associated with data breaches. These vary year on year, and while they are often used as a scaremongering tactic to justify a solution, they are really a very useful tool in putting some numbers behind a business case.

When looking at the likely actions that can lead to a data breach it is also worth considering how many are inadvertent rather than malicious. Recent studies show that breaches are far more likely to come from within the Enterprise rather than outside – that's not to say that the outside ones have diminished, just that more care needs to be take around the insider threat.

The final piece of the puzzle is to look at existing security investments. ARgon is not designed to be 'rip and replace', but to augment existing solutions and protect against the next generation of threats. Providing a cost effective business efficient alternative to a replacement strategy that can be added at any time.

[8] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Clearswift and ARgon Futures

Clearswift has been the leader in Deep Content Inspection for many years and sells Adaptive DLP solutions across email, web and the endpoint. ARgon for Email is the first Adaptive Redaction appliance that Clearswift has brought to market, starting with Email since it's still the primary communication and collaboration application, however times are changing and the need for Adaptive Redaction functionality extends beyond this medium.

All Clearswift products are built on the same core technology enabling single polices across multiple communication channels and ARgon is no different. Additional ARgon appliances will be released in the forthcoming months to address the new risks posed to information. As with ARgon for Email, these are designed to be complimentary to existing security and email solutions. The result will be a set of ARgon solutions which can be peered together, see Figure 5.

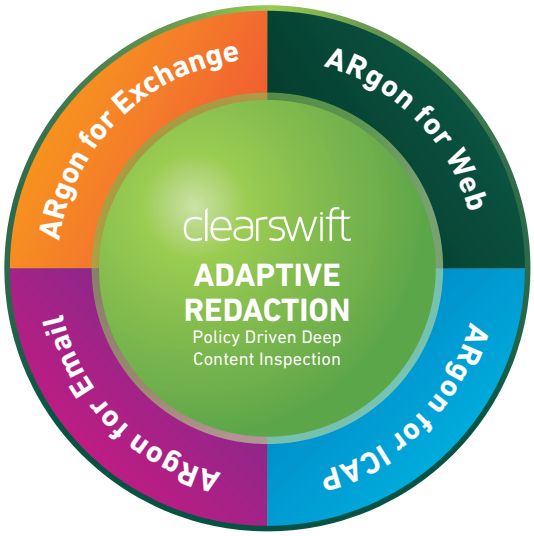

Figure 5: The ARgon Product Suite

The ARgon for Web appliance is designed to deliver the same functionality as ARgon for Email, but in the web environment. This can be used in conjunction both HTTP and HTTP/S traffic. For those who have ICAP based web proxies, there will be ARgon for ICAP in order to deliver the Adaptive Redaction functionality. ARgon for Exchange has been designed to help reduce the internal threat, enabling Adaptive Redaction to be used on internal email.

Summary

Heraclitus said "The only thing that is constant is change", and today's business is undergoing constant change. When it comes to security, it is all change there as well, with new threats combining with new legislation to create new imperatives around securing critical information.

An ARgon appliance from Clearswift has been designed to address some of the new threats that organizations face, both the malicious and the inadvertent ones. As a solution it is designed to work in conjunction with the existing security solutions that an organization has in place and remove most of the challenges organization have with a traditional DLP solution. With Adaptive Redaction removing only the information that breaks policy while leaving the rest to continue unhindered, ARgon enhances productivity by removing the most common false positives. It also removes the biggest external threat to organizations today, the APT, by removing embedded active content from incoming documents.

Clearswift set out to enable Adaptive Redaction to be implemented for all organizations, no matter which secure email or web gateway they had previously purchased, ARgon is the realization of that vision.

[9] http://www.clearswift.com/solutions/insider-threat

About Clearswift

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.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific 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**

clearswift
A HelpSystems Company

UK - International HQ

Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support:
+44 (0) 118 903 8200
Email: info@clearswift.com

Australia

Clearswift (Asia/Pacific) Pty Ltd
Hub Hyde Park
223 Liverpool Street
Darlinghurst
Sydney NSW 2010
Australia

Tel: +61 2 9424 1200
Technical Support:
+61 2 9424 1210
Email: info@clearswift.com.au

Germany

Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0)221 828 29 888
Technical Support:
+49 (0)800 1800556
Email: info@clearswift.de

Japan

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

Tel: +81 (3)5326 3470
Technical Support:
0800 100 0006
Email: info.jp@clearswift.com

United States

Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support:
+1 856 359 2170
Email: info@us.clearswift.com