clearswift
RUAG Cyber Security

A Guide to Critical Data Protection in 2018:

The What, the Why and the How

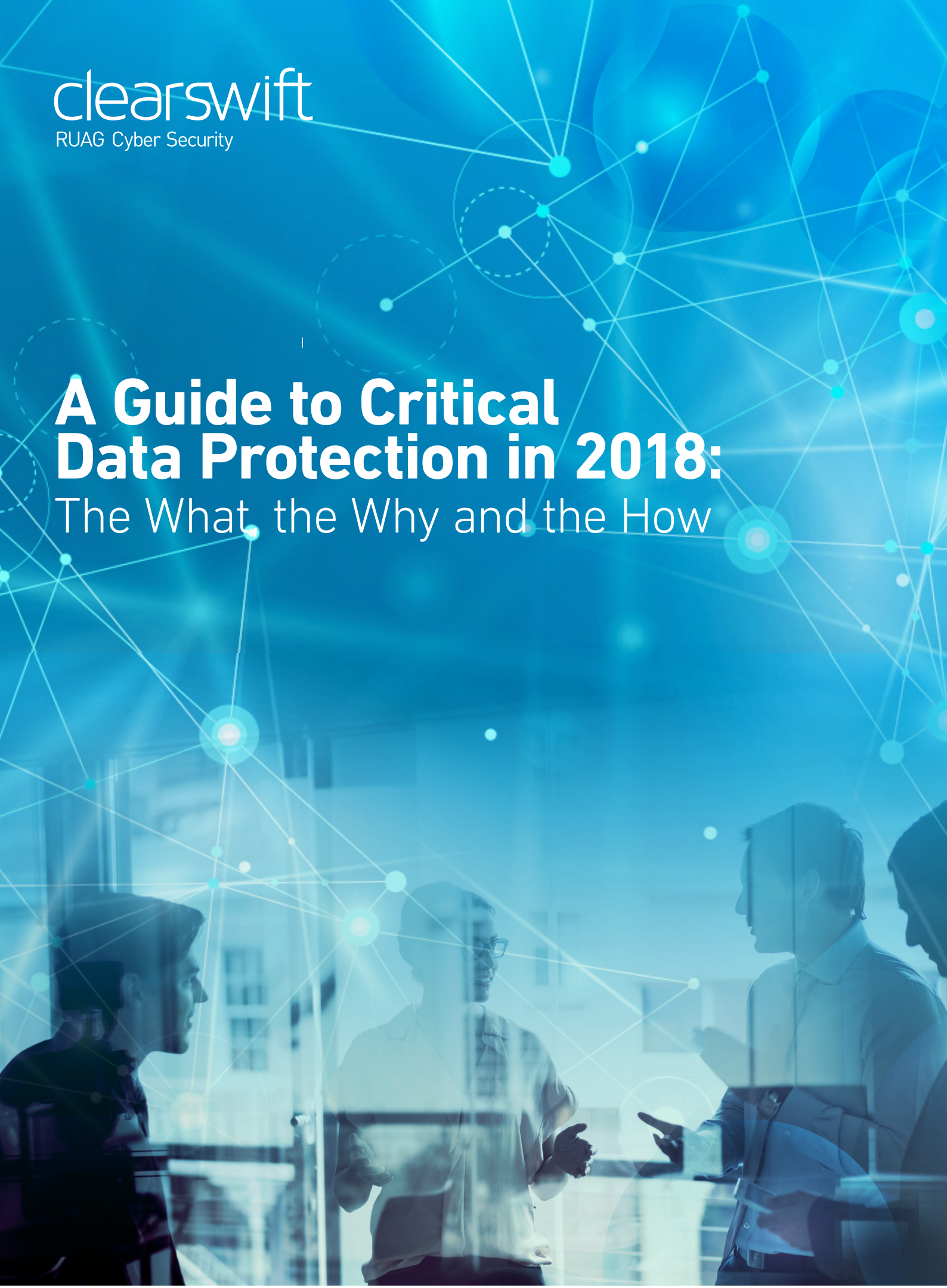


Table of Contents

Decide What Data loss prevention (DLP) Means To You

Introduction

Data loss, data leak, data theft and even data spill, depending where you are in the world there is a term for the loss of information from an organization. Across the globe, organizations both big and small are waking up to the need to protect their information, not just because it's bad to lose it, but also because there are legislative, national fines and even reputational damage that can occur.

Data Loss Prevention (DLP) means many things to many people, from physical security of printed information such as printed board papers and computer systems, through to blanket information encryption in various forms and then to content aware DLP. We will highlight what DLP is, and explain why 'traditional' DLP technology is no longer fit for purpose. We will outline the basic principles and features behind a DLP solution and cover the new technology that is being implemented to create the next generation solutions.

DLP solutions have been around for many years, however their use is now spreading to small as well as large organizations. By combining new technology with traditional DLP methodology it is possible for even the smallest business to take advantage of a sophisticated solution which is easy to implement and operates at a low cost – protecting the lifeblood of the organization... its information.

Follow the step by step guide within this paper which will enable you to both design and implement an effective and robust DLP strategy.

Adaptive Data Loss Prevention

It's all about the content

Content Aware Data Loss Prevention (CA-DLP), but also the usual interpretation for the DLP acronym is the action of carrying out a structured lexical analysis on electronic information and then performing an automatic action based on a policy in order to protect the information.

Before DLP can begin there is a series of pre-processing steps. This includes capturing the information from various channels and deciphering the communication protocols. For example deciphering SMTP for email and extracting the text from binary file formats such as Microsoft Word. Deep Content Inspection (DCI) is used to break down the data, for example an email and if required any attachments. With further recursive analysis to break down zip files into the separate files and even to the images that may also be contained.

There are multiple communication protocols and document formats which can be supported. For most organizations, email and web (HTTP / HTTPS) are the primary communication channels which need to be covered by a DLP solution in conjunction with the most popular document formats, Microsoft Office and Adobe PDF. As data can be found at many points in the corporate infrastructure, it is no surprise that the DLP solution needs to be applied at each point. For most, the simplest place to begin is with the network as it offers the least deployment complexity with the biggest return. After the network, the endpoint is next in line for protection to prevent information from leaking out through alternative channels such as USB devices and CD ROMs. When looking for a DLP solution it is worth considering the longer term deployment plans as it is important to choose one where policies can be shared between the network and the endpoint [1]. Policy consistency is important, as inconsistency creates risk.

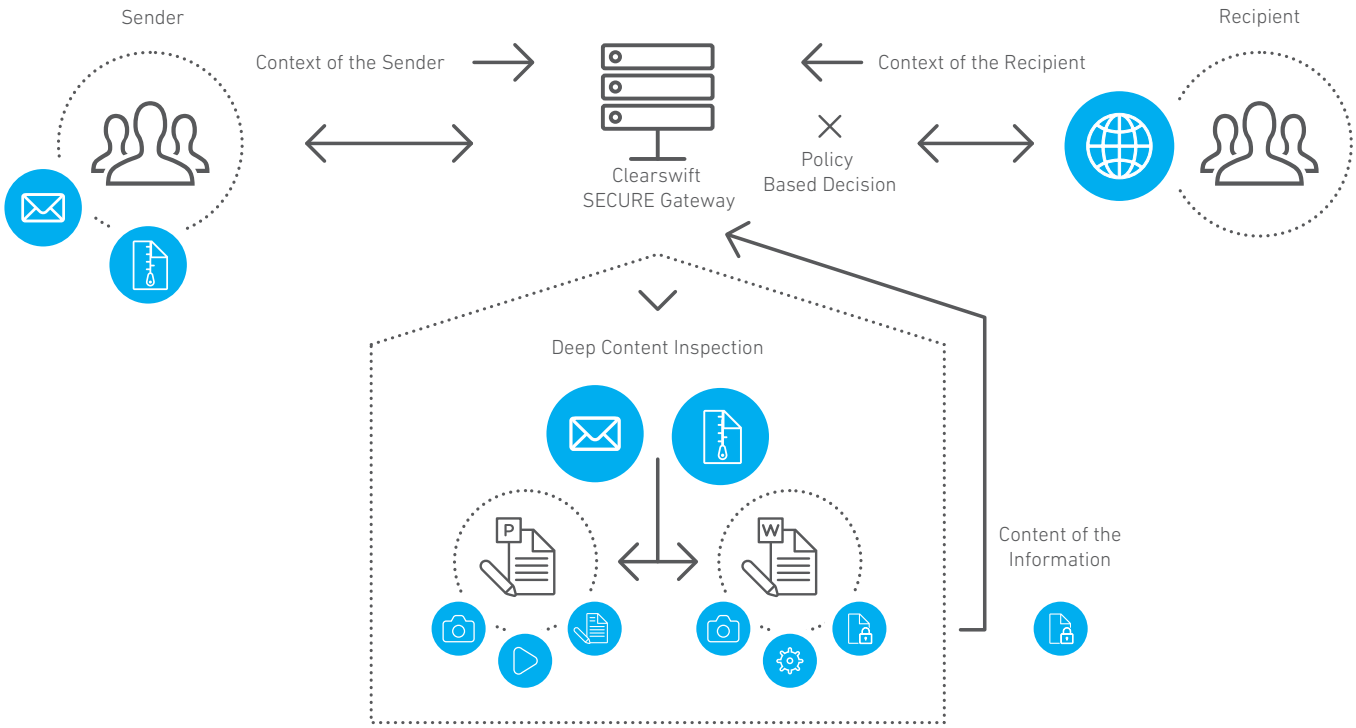
Traditionally the outcome of a DLP policy breach is to stop and block the information from being communicated, although there are many other actions that can also occur. For example to help educate employees about why what they are trying to do is not allowed, especially when a new information security policy is implemented. For many DLP solutions, the primary action is very black or white, either the information is sent, or it isn't. This approach leaves out a very important piece of context – the person sending the information.

[1] Endpoint refers to systems which users interact with and are usually thought of as laptops, tablet computers and smartphones. However, workstations and servers should also be considered as endpoints and potential sources of data loss and therefore need to be protected as well.

Consider who should be accessing what information

In the same way that not all data is created equally, neither are all people. An effective DLP solution needs to take into account the person trying to communicate the information. For example, a manager sending out the pricelist to partners through corporate email would be authorized to do – as it is part of their job. However, an engineer doing the same thing probably isn't. DLP polices need to be tailored to individuals or groups to ensure that those who have specific needs are adequately catered for. Blanket policies covering everyone in an organization tend to create more problems than they solve, so the chosen DLP solution needs to have the flexibility required by an organization to fit its business processes, rather than trying to change all the business processes to fit the DLP solution. See Figure 1: Content and context based decisions.

Figure 1: Content and context based decisions



Time to become adaptive

So in an ideal world the DLP system needs to take into account the content and the context. Context needs to be extended to cover not just the individual sending and the recipient, it also needs to take into account the way in which they are trying to communicate.

Is this a formal email using the corporate email system, or is it an upload to a social networking site? The latter may have much stricter controls than the former. It might be that the user is trying to copy the same content onto a USB stick or some other removable media, in this case, perhaps it can be copied but needs to be encrypted.

The solution doesn't lie in increasing complexity for the administrator, but rather the ability of the solution to adapt the content given the various parameters allowed for sharing it. Today businesses and governments rely on continuous communication and collaboration, but they need assurance that critical information remains secure at all times. Adaptive DLP delivers on this essential requirement.

Challenges with traditional DLP solutions

The biggest challenge facing organizations when they decide to implement a DLP strategy is to decide what information they want to protect, where it is located and then how to build a policy to detect and protect it.

For many organizations, the major hurdle with implementing a DLP solution is how to deal with the stop and block behavior of most DLP solutions. In instances where a data breach event occurs, the information is stopped from being communicated and business is put on hold until a resolution is achieved. Unfortunately, this frequently occurs because the policy is incorrectly configured, causing a false positive, blocking information that has to be sent 'now', stopping legitimate communication and the business. The other effect of blocking is that if there is no efficient process to resolve the block, the sender will resort to other mechanisms

to communicate the information. This often results in attempts to use of insecure channels such as personal email accounts or web uploads. The overall consequence is that the organization needs to choose between security and business – and business always wins. Traditional DLP solutions end up becoming shelfware or switched into a 'report only' mode which offers no additional security.

Furthermore the next generation of information borne threats are not addressed by traditional DLP solutions leaving organizations open to attack through these new vectors.

In order to overcome these challenges, DLP needs to be rethought and that is where Adaptive Redaction comes to the fore.

Adaptive Redaction

Adaptive Redaction is a unique, award winning, technology developed by Clearswift which is aimed at overcoming the challenges with traditional DLP solutions. By removing the information that would create the data breach on-the-fly, communication can continue unhindered. In the vast majority of cases, the information that is removed is unnecessary to the conversation in any case. Take for example the person who emails an order into the organization and includes their credit card number. Upon receipt the sales department hits 'reply' to say 'thank-you', but at that point they are then in breach of the Payment Card Industry Data Security Standard (PCI DSS) as they will be sending out the credit card information – even though it is going back to the person who sent it!

With stop and block behavior, this interrupts the communication flow, whereas with Adaptive Redaction the credit card number would have been automatically removed and the email would have reached its destination unhindered. The sender would have been informed that information had been redacted from their response, but the response would have made it through. Business continues.

There are three components to Adaptive Redaction; Data Redaction, Document Sanitization and Structural Sanitization. (We frequently include encryption as another type of Adaptive Redaction as that too changes the original information on-the-fly – although it does not remove anything.)

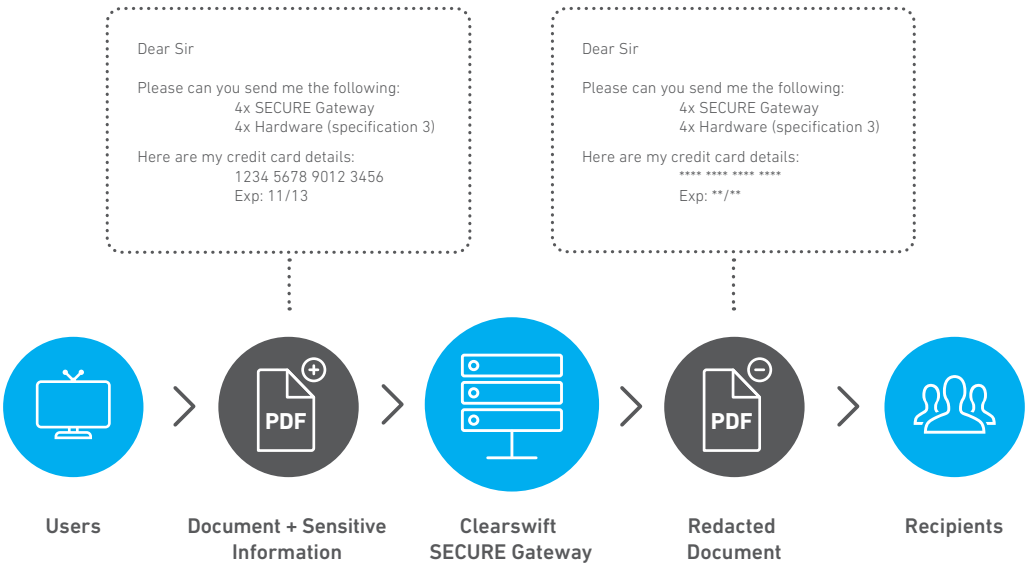
Data Redaction

Data redaction is where strings, regular expressions and tokens are removed and replaced by an alternative, for example an asterisk. Or in the case of a credit card number, multiple asterisks except for the last four digits, see Figure 2: Data redaction in action.

Data redaction is a simple addition to any DLP policy action. As it is applied automatically, it is applied consistently. This ensures that all documents are treated equally, and should the policy change, it will be efficiently implemented without the need for staff training.

While it is most frequently used for information going outside an organization, it can also be used for information coming in. For example, if you are not set up to handle credit card numbers, receiving one on the internal network can cause auditing and additional protection measures to have to be put in place, resulting in additional business cost and complexity. Data redaction can be used to ensure that the credit card never comes past the organization boundary, however the rest of the message will be delivered – along with an indication that the message has been changed from the original sent.

Figure 2: Data redaction in action



Document Sanitization

In today's electronic documents there is a great deal of hidden content. For example information in the metadata, revision histories or 'quick save' data. Document sanitization enables the DLP solution to strip out this information either in its entirety or on a more granular basis.

There have been several high-profile cases where hidden information has been uncovered and caused huge embarrassment to banks, pharmaceutical companies as well as governments and even the United Nations.

While it is possible to manually purge hidden information it relies on the individual actually doing it. By putting in place Document Sanitization this can happen automatically, consistently and based on policy.

Structural Sanitization

Along with hidden content, there is also the possibility for documents to contain hidden code or embedded active content. This can be in the form of a simple macro, or a more sophisticated piece of embedded malware, such as the embedded Adobe Flash vulnerability which infected RSA[2]. Structural sanitization automatically removes any such active content. While this policy can be applied on outgoing documents, it is most commonly used on incoming communication (both email and web) – where organizations don't want potential issues with viruses and other malware coming in through documents.

Embedded active content in innocuous looking legitimate documents is the primary cause of infection or organizations by Advanced Persistent Threats (APTs). As APTs become more sophisticated and are able to evade sandbox detection techniques, structural sanitization provides an effective alternative by removing all inbound active content. As with all Adaptive DLP features, the original can be held in quarantine and easily released by a manager if required.

Although primarily used on incoming documents for advanced malware protection, Structural Sanitization can also be used on outgoing documents to protect Intellectual Property that might be contained in macros, for example in Financial Services spreadsheets.

[2] http://www.computerworld.com/s/article/9215444/RSA_hackers_exploited_Flash_zero_day_bug

Define What's Valuable

There are many different ways to analyze information, whether it is a simple examination of a file type through to looking inside the information for a complex pattern.

For most organizations creating a DLP policy is not about selecting one piece of functionality, but rather multiple pieces of functionality applied appropriately to the types of information that need to be monitored. A good DLP product masks the complexity of the analysis making it simple for the business / information owner to pick out what works best for them and their data and for the systems administrator to implement it.

File Type and True File Type

Perhaps the simplest DLP functionality is looking for specific file types and preventing those from leaving the organization. A good example of this would be CAD / CAM files, which have a very specific file type. Basic systems just look at the file extension, for example .doc, and make their decision based on that. However, more sophisticated solutions examine the contents of the file more closely to determine the actual file type and even provide the ability to support new data types. This 'true' file type detection prevents a simple rename of the file and the data being able to be exfiltrated.

Words and phrases

After file type analysis the next piece of DLP functionality is the process of looking for specific words or phrases within the text. One use is looking for profanities where there is a file containing a list of all the profane words and phrases. A policy can then be created to look for any occurrence of a word in the list which will then trigger the policy. From a management perspective it is much simpler to have a policy relating to 'unacceptable language' which can be simply updated by adding the word to the list, rather than having to update everything individually.

Other common uses of word lists are around 'secret' projects, including mergers and acquisitions. The project usually has a code name and it is this which is monitored for by the DLP solution. Any occurrences outside of the people who should know can be flagged as a potential leak.

One challenge global organizations have is that some words in one language are offensive in another and vice versa. One example, which is (hopefully) not too offensive, is 'Slut'. In the UK this has a very specific, if derogatory, meaning, whereas in Norwegian it means 'end', and can be found on phones as the button used to terminate a call! So, in this case there can be false positives created if the language is not correctly detected. These problems do not occur very frequently as systems have become more sophisticated, recognizing the language based on the content, rather than the language hint usually contained in the document.

Regular Expressions

A regular expression, or RegEx as it is often known, is a rule relating to a specific string of characters. For example if you have an order number, 'MyCo1234', then this might be expressed as 'MyCo[a-zA-Z0-9]{4}' in a regular expression, where [a-zA-Z0-9] indicates most normal characters and {4} indicates there should be four of them. You can be more specific by indicating that the characters are to be numbers. For example 'MyCo[0-9]{4}' will ensure that the four characters following 'MyCo' are all digits between 0 and 9. In essence regular expressions define the pattern you are looking for. There are multiple operators that can be used including '?' to match any 'single' character and '*' to match any number of characters. See Figure 3: Example records and RegEx pattern matching. If you are unfamiliar with RegEx then there are many primers available on the Internet, although creating them often seems like a bit of magic!

Figure 3: Example records and RegEx pattern matching

Record	[a-zA-Z0-9]{8}	[a-zA-Z0-9]{8}	[a-zA-Z0-9]{8}	[a-zA-Z0-9]{8}	[a-zA-Z0-9]{8}
ABCD1234	•				•
MyCoABCD	•	•			
MyCoAB12	•	•	•		
MyCo1234	•	•		•	

Tokens and Customized Tokens

A token is a specific example of a regular expression, but also usually has additional validation. The best known token is that for a payment card number, for example those found on credit and debit cards. This is typically defined as a 16 digit number (but it does vary in different parts of the world) which includes a single check digit which is enforced by the well-known Luhn algorithm. So in order to validate whether the DLP solution has found a credit card number, it needs to find 16 digits and then calculate the checksum and compare the checksum with the check digit.

Payment card numbers are not the only tokens that can be created. Many others will be predefined, such as social security and national insurance numbers as well as other banking numbers, for example IBAN codes and BICs (Business Identifier Codes).

Most countries have their own specific identifiers which can be defined as a token, sophisticated DLP solutions enable customized tokens to be created. Once created they can then be easily referred to and used in the DLP rules that are created.

Structured data search

Often there is considerable content held in databases which also need to be protected by the DLP solution. One example could be the list of all customer credit cards. In this case, if the DLP solution comes across a credit card it can check to see if it is one which is known about, or a different one.

There may be a different action related to whether it is known or not.

Configuring the structured data search functionality is usually done by extracting the appropriate information out of the database and then putting it into a format which can be readily searched by the DLP solution, a fingerprint[3]. As the extracted data is sensitive, the format is secured by the DLP solution ensuring that it cannot be accessed and cause its own data leak, see Figure 4: Process for structured data search. Extracting the data and processing it separately by the DLP solution has the benefit of not impacting database performance and also offers the ability to run the DLP solution remotely from the database in question, for example on an endpoint.

More advanced structured data search functionality takes a number of fields from the database and allows cross checking. For example not just the customer credit card details, but also their name. The more fields that can be checked, the more accurate the policy and consequently a reduction in false positives.

Figure 4: Process for structured data search

Image analysis

For many, image analysis is about being able to detect and block pornographic pictures; this is typically done using skin tone analysis on the image being received.

However, image analysis can also be used to prevent specific images from leaving the organization – for example a product design. In this case specific images are registered with the system through the creation of a unique fingerprint and the DLP solution monitors for them, blocking their transmission if detected.

These images are detected even if they are embedded in other documents, providing they are the same as the one that was registered with the system.

[3] A fingerprint is a unique signature that is generated by an algorithm based on the data it relates to. This can be as simple as a phrase or an image, or can relate to an entire document.

Make Staff the Solution Not The Problem

Discovering that there is data which breaches policy is one thing, figuring out what to do is another.

When DLP solutions are first put in place they tend to discover all sorts of poor business practice.

For example, while it might not be in the policy to send out the company price book (as it contains Intellectual Property) there will be people who do. Some will do it because they should, others in a more malicious manner. Switching on a DLP solution and immediately stopping anything which breaks policy will probably stop the business. So, there needs to be a process of upping the ante over time to ensure that the DLP solution does not create more problems than it stops.

Education

Perhaps the most important action a DLP solution can carry out is education. This will tell the user what is wrong with the communication they are attempting and then give them options. At the start of the rollout of a DLP solution the option is most likely to continue with the operation. For example sending out an email with the price list in. To stop this, at this point in time, will stop the person from carrying out their business tasks. However, once this event has occurred it should act as a prompt to both the individual and the organization (through DLP event auditing) that there is probably a process which needs to change.

In November 2016, a Boeing employee mistakenly emailed a spreadsheet full of employee personal data outside of the organization to a non-authorised recipient. The spreadsheet contained personal information of around 36,000 Boeing employees including social security numbers, dates of birth and other personal identifiable information in 'hidden' columns within the spreadsheet. Today, a DLP solution would have prevented this data from leaving the organization in the first place, protecting the employee, as well as the organization, from experiencing a data breach.

Insider threats account for the majority of today's data breaches. Specifically, the inadvertent leaking of an organization's critical information poses the highest threat. Education is about understanding and improving information handling practices as it is about providing awareness of the policy itself. When policies change the DLP solution is useful in order to educate employees that the policy has changed and how it affects their working practices.

Stop and block

The most common DLP policy action is to stop and block the communication, for example an email to an external recipient or a web upload, with the original being placed into quarantine or a copy of the transaction being sent to an auditor. When a breach occurs, there are several additional actions that can occur.

Firstly, the individual can be informed that they have breached a policy and be given the opportunity to withdraw the communication. However, they may be told of the violation and be able to do nothing about it or they might be told nothing. Likewise, the IT department or support desk may receive notification that a breach attempt was made, but the individual withdrew the request, or they may only see those breaches which are actually blocked.

While stop and block is the most common DLP action, it can also be the most disruptive to the organization, as it stops communication. In the case of false positives (where the system makes a 'mistake' and blocks communication which is valid) then this too can cause frustration from the individuals' perspective. In order to counter this, the most sophisticated DLP solutions have "Adaptive Redaction" as an advanced feature; this is explained later in this paper.

Encryption

Encryption is a very important part of the DLP policy action suite. The stop and block approach is adequate for stopping inadvertent leaks of sensitive information such as credit card numbers, but there are many occasions where information needs to be shared, but in a secure manner. Encryption is a very effective approach to this and in essence, the action part of the DLP policy is to encrypt the information and then continue to send it out. There are many different approaches to encryption, from TLS to PGP and S/MIME through to ad hoc ZIP based, and once again this is where an adaptive solution is required to remove the decision making from the user and pick the appropriate one based on the recipient and the content.

Auditing and reporting

Critical to any IT system today is the ability to audit events and report on them. Whereas most systems audit and report on the system itself, DLP solutions can also audit and report on individuals or groups of individuals. This enables organizations and Compliance Officers to target 'problem' areas. The chances are that if a significant number of people inside a particular group have an issue, there is a business process which needs to be updated.

Distributed operational management

When a breach occurs and a security event is created there needs to be some action taken. In the case of a DLP event this is typically to review what sort of information was being sent which shouldn't have been. For most DLP solutions all events are sent to a specific individual or group within an organization for them to review and act on. However this does not scale particularly well and in the majority of cases the individual reviewing the event does not know whether the person who caused it was doing anything wrong. Today's next generation DLP solutions get around this problem by automatically distributing the operational task of reviewing events to the appropriate person. In most cases this is simply the manager of the individual involved. Sophisticated DLP solutions are able to interrogate the corporate Identity and Access Management (IAM) system, such as LDAP or Microsoft Active Directory to discover the manager and then send the request for resolution to them. Spreading the operational aspects of a DLP solution it makes it considerably cheaper to run and more efficient as bottlenecks are automatically reduced.

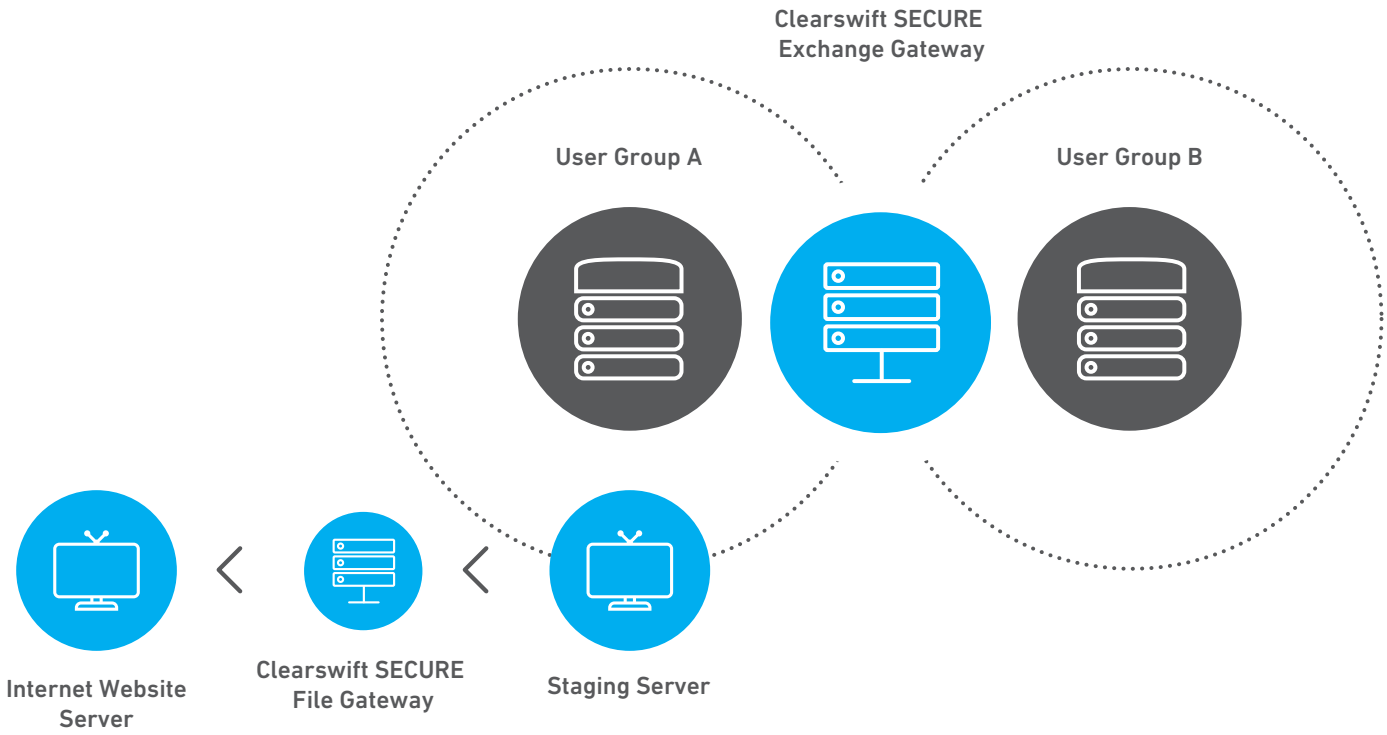
Understand Who Is Accessing What, Where and How

DLP has traditionally been used to prevent information from leaking outside the organization, but we have now seen how Adaptive Redaction can also be used to prevent unwanted information from coming into the organization. However times are changing and whereas all information within an organization used to be shared, today there is a move to only providing those people with 'the need to know' access. While Access Control Lists (ACLs) exist on systems, internal email remains a substantial risk as a means to share information, inadvertently, with the wrong person or maliciously in collusion with others.

In some industries and sectors, namely financial (specifically front office and back office banking), pharmaceutical and defense the concept of segregating staff communication has been around for decades. It is most commonly achieved by having separate systems for each and then blocking contact between each. The idea of segregation is good, but today there needs to be a more cost effective solution, and internal DLP is just that, such as that provided by the Clearswift SECURE Exchange Gateway solution. In essence all the policies that can be applied to information going outside an organization can also be applied inside. Preventing both inadvertent as well as malicious communications, see Figure 5: Examples of where DLP can be used internally.

For those organizations who want to take segregation further, file gateways are becoming a means to intelligently prevent information from being transferred from one network segment or system to another. Secure file gateways have been used in the military domain for a long time, ensuring that information of different classifications, for example 'top secret' and 'secret' remain separate and when a transfer from one to the next, usually 'down' the classification ladder, does occur it meets the required policy. Once again, this technology is finding its way into even the smallest of organizations as a way to ensure information meets policy before being shared. While this is usually between departments, there is growing case for having a file gateway between the internal organization and the externally facing website.

Figure 5: Examples of where DLP can be used internally



Set Your Strategy

Building an Adaptive DLP strategy

When looking to build a DLP strategy, there is one key item to remember... Don't try to do it all at once. While this may appear obvious, there is a tendency for everyone in an organization to believe their information is the most important and needs protecting. This is rarely the case, so start small and grow by prioritizing your information and iterate through the process to a level at which the organization finds the risk acceptable. For example, you may decide to invest more heavily in protecting the designs for next year's products than for sales quotes. The chances are you will never protect all your information, but you will be able to protect that which is mission critical.

Step 0: Communicate

Before you even begin to think about implementing DLP, you will need to communicate to all the stakeholders. While many IT projects are run by IT and rolled out to the organization, DLP needs to be run by the organization in conjunction with IT. It is the organization which understands its information and the importance of it – not IT.

Identifying stakeholders and bringing them together to communicate the program is essential. Stakeholders are the people who most often create the information, use it or are responsible for it. So this will include departments such as finance and legal as well as support, engineering and sales. There is also specific information which should be protected that comes under the auspices of HR and of course IT. Identifying the stakeholders and communicating with them before the project begins will make the rollout considerably smoother.

Communication is not just something to be done at the start of the project; it needs to be done throughout, and repeated at certain points. For example when the policy (and supporting technology) is being rolled out, there will need to be initial communication to those in the pilot group. When being rolled out across the organization, communication will need to address everyone.

Step 1: Identify the types of information you have

Strange as it may seem, most organizations don't understand the value of their information. So while this task may appear obvious it will not be as easy as it seems. The stakeholders need to be involved in the identification process and then the information needs to be prioritized. A simple rule of thumb is:

1) Information that you have a legislative reason to protect. For example HR or customer details. Credit card and bank information.
2) Information that if it fell into the competition's hands would cause immediate damage. For example sales quotes for customers or end of quarter financial information.
3) Information which if used by the competition would cause long term damage. For example Intellectual Property, corporate strategy and merger and acquisition plans.

In the case of #2 and #3, there is often a time component to the value which also needs to be considered. The year-end financial results are incredibly interesting the day before the announcement, but public knowledge the day after. Likewise there are different criteria on the value of items; an order worth $10K which is lost to the competition is less significant than one worth $1M. Plans for a product replacement to a line of business worth $1BN should be better protected than the next incremental upgrade to one worth $1M.

Step 2: Identify where your information is stored

Once again, this should be an easy question to answer, although the results are often surprising.

There will be applications sitting on databases which contain a great deal of valuable information. However even with these information sources there will be reports that can be run in order to extract the information, which will then be downloaded, as well as cut and pasted into reports, attached in emails and possibly uploaded to the web.

Developing an understanding of exactly where information is stored and accessed from enables a cost effective plan to be put in place. Prioritize the information stores based on risks. If all the critical information remains inside the organization on devices which don't travel outside the perimeter then a network DLP solution will be sufficient. However, if it also needs to be protected while on laptops, tablet computers and smart phones then an endpoint DLP solution will also be needed.

Step 3: Identify who needs access to the information

The third step is to identify who needs access to the information. Not who should have access, but who really needs to have access. Is it individuals or groups, are they geographically organized, or by role?

For effective integration of the DLP solution the organizational structure need to be reflected in the corporate Identity and Access Management (IAM) system, such as LDAP or Active Directory. While it is possible to implement a DLP solution without this, it is much easier to do it with one, and is simpler and cheaper to maintain.

Step 4: Identify how the information is communicated

The final step before building the policy is to identify and prioritize how the information is communicated. For most organizations, the top priority will be corporate email, with the web being second. For those organizations with laptops there should also be protection against information being insecurely copied onto removable media, such as USB drives, as well as to CD ROMs and DVDs. For many devices, there also needs to be protection from data loss when not on the corporate network, for example when working from home or in a coffee shop. While most organizations have secure network access for these remote devices, they can also connect to public networks as well – without the protection of corporate network security there is an opportunity for a data leak to occur, either maliciously or inadvertently.

Step 5: Identify the risks

Organizations run on risk, understanding the risks, including information risk, mean that investment can be focused in the most cost effective manner. For example a lack of communication to all employees creates a serious risk to any DLP project, while the need to identify *all* information or where it is held creates a risk that the project will never begin.

In many cases now there is a 'cheap' win than can occur with Adaptive Redaction as that can be deployed across the organization to prevent embedded malware from coming in and remove all 'hidden' content on the way out. Both of these reduce risk very quickly and protect against the latest threats which are carried inside documents.

Step 6: Design and implement the policy

With all the information gathered it is now possible to design and implement the policy. The effort put into steps 1 to 5 will be reflected in how quickly a policy can be designed and implemented.

Choosing a DLP solution which can have a unified policy across both the network and endpoint, as well as across email and the web, will help in implementing a consistent policy. Within security there is an old adage that you are only as strong as the weakest link. With DLP the same is true, if you protect email, but there is access to the Internet, then a potential data loss risk. If the policy that defines information as 'top secret' on the network but only classifies it as 'informational' on the endpoint, this creates a potential data risk.

Even when wanting to start small, the task can appear daunting. Prioritizing the information, location, people and communication channels will help narrow the scope. While all organizations are different, most prioritize email first, with an initial emphasis on information which, if compromised, would result in legislative action, for example credit card details. Email can be most easily protected using a network DLP solution. Network based solutions have the advantage of protecting any device which attaches to the network, there is no separate agent required on every endpoint. This makes it an obvious starting point for deployment. Successful deployment for email can then be followed up with protection on the web and finally the endpoint. At each stage policies can be reviewed and refined.

For many deployments an initial 'monitor mode' can help fine tune policies before they become active by creating a report on what would have been done – rather than actually doing it. Implementation is not for the faint hearted and there will be challenges, an adaptive solution which incorporates Adaptive Redaction will alleviate some of the frustration of initial deployment by removing the issues created by 'stop and block'. The worst thing that can happen is an implementation is abandoned as it will be very difficult to restart at a later date – and the organization will remain at risk.

Step 7: Build the action list and priorities

Take into account of all the information gathered in the previous steps in order to build the action list and consider the consequences of implementing any action which might hinder business. Revisit the policies and check that they are fit for purpose. Minimize any false positives by tweaking the policies before they are rolled out. Hold meetings with the IT support staff about the new policy and technology so they can be prepared for any calls that may come in.

The actions can be built up over time. The first set can be warnings before moving to the more draconian measures of stopping and blocking the content. This is where Adaptive Redaction comes into its own, as automatically removing the content which breaks policy but allowing the communication to continue ensures that business continues without interruption.

Step 8: Review and update

A DLP policy is never finished - probably not something that either the IT department or the organization as a whole wants to hear. Legislation changes, business processes change, information changes, storage devices change and of course people change. The DLP policy needs to reflect those changes in order to support the business – which means they need to be regularly reviewed and updated.

Both the IT support staff and individuals within the business should be consulted as they are the people with first-hand experience of the policy and actions, and they will have suggestions as to how to make changes to improve both which has the important side effect of improving organizational efficiency.

Step 9: Build a data breach process

Data breach, unfortunately, is not a matter of 'if' but 'when', so it pays to be prepared. For some industry sectors there is a requirement of self-disclosure so a process is of paramount importance, for others the creation of a data breach process will save time, effort and confusion when a breach occurs. What would you do if a breach occurred, or information was lost? Thinking through the scenario will help build a process and looking at other actions people have taken in the media will also provide valuable input. Being able to do this in an imagined scenario means it can be done calmly and logically rather than under pressure of a real breach – which could result in poor decisions as to the actions required.

The key is to have a team with well understood responsibilities, especially when it comes to dealing with the media and customers. Who will be the face of the company should an event occur? Frequently it will depend on the size of the company, but it needs to be someone with enough gravitas to ensure that both the customers and the media know you are taking it seriously. It is therefore more likely to be the CEO or Managing Director than someone in marketing.

Towards Information Governance

Many of the steps required to put in place a DLP strategy are also useful for creating an Information Governance (IG) strategy. Good IG is predicated on understanding the information within the organization, where it is stored and who has access and communicates it.

Integration of a context and content aware Adaptive DLP solution with with Clearswift's Information Governance solution provides additional benefits, such as being able to detect and block arbitrary text from specified documents, as well as being able to redact entire blocks of protected information. For many, IG might be an aspiration at this point in time, but rest assured that the work carried out in implementing DLP is also essential for starting an IG project.

Summary

Adaptive DLP is a significant part of the arsenal that organizations must have to protect their mission critical information. Utilising both context and content aware decision making, coupled with technological innovations such as Clearswift's Adaptive Redaction, a DLP solution can become an enabler to business as well as an enforcer.

In a world where digital collaboration is increasing and new data protection regulations, including the EU General Data Protection Regulation (GDPR) are being enforced, the need for DLP technology has never been stronger. Clearswift's Adaptive Redaction functionality enables organizations - large and small - to seamlessly implement a comprehensive DLP strategy in a cost effective manner. While at the same time contributing towards the compliance needs of today's businesses.

The design and development of policies which govern the Clearswift DLP solution's behaviour needs to be carried out with stakeholders within the business as this is not something that an IT team can carry out on its own. Clearswift can help with the development and implementation of an effective Adaptive DLP strategy.

Contact the Clearswift team for a discussion today.

clearswift
RUAG Cyber Security

Enhance your IT Infrastructure with Adaptive Security and Data Loss Prevention technology from Clearswift.

Prevent Threats.
Protect Critical Information.
Comply with Regulations.

clearswift
RUAG Cyber Security

Clearswift is trusted by organizations globally to protect critical information, giving teams 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.

For more information, please visit **www.clearswift.com.**

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

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount 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
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
AUSTRALIA