WHITE PAPER

Stay ahead (of data leak) with Data Classification and Data Loss Prevention

RightsWATCH

Executive Summary

Information breaches resulting from the disclosure of sensitive data in email, documents, spreadsheets, PDF, etc. are widespread. The costs of such information losses are significant, while the risk mitigation difficult. Thus, organizations have turned to Data Loss Prevention (DLP) to thwart security breaches perpetrated by malice or even by user negligence.

Precisely configured, existing DLP offerings can deliver a comprehensive solution to the unauthorized disclosure problem. But precise configuration is often a daunting task when it comes to context-aware DLP tools, as these require heavy lifting upfront, namely data classification and discovery.

By classifying and labelling unstructured data at creation, RightsWATCH vets the unstructured data with the enterprise's document management policies. Thus the DLP can implement very precise, deeply content-aware decisions about the asset, to deliver more accurate outcomes with fewer false positives.

Classifying legacy data becomes even more straightforward when RightsWATCH is invoked to complement a DLP discovery and scanning capability, by applying visual and metadata markings to messages and documents.

You shouldn't be forced to compromise on corporate security policies, nor fight or rebuild your existing DLP. RightsWATCH enhances your DLP initiative, taking the guesswork out of identifying sensitive data.

Understanding the problem

The notion that an organization can be 100% secure is unrealistic in today's hyper-connected, borderless world. A more pragmatic question may not be if you are totally secure, but rather if the information that matters most to your organization is secure enough.

The fact that sensitive data seems to increasingly follow a pattern of being leaked, lost or stolen, has forced security professionals to rethink how their organizations can keep their most valuable assets safe.

According to Ernst & Young, one of the greatest challenges in managing data loss is the number of reasons and scenarios why it can occur. In order to address the risks resulting from data loss, a comprehensive solution that includes people, processes and technology needs to be implemented.

FIGURE 1 – DATA LOSS RISKS IN YOUR BUSINESS (IN "INSIGHTS ON GOVERNANCE, RISK AND COMPLIANCE", ERNST & YOUNG, OCTOBER 2011)

Facing DLP Challenges

Because organizations may not fully understand the limitations of DLP, they often end up with a system that is never fully rolled-out or widely used, or in some cases it is just shelved. DLP must be fully understood and enhanced to ensure that your data security risk is mitigated.

Enterprises looking at IP protection need to understand that any tool they bring in, DLP or others, is only going to look for data that has been identified and classified as sensitive or confidential by informed people.

Even with DLP controls in place, IP theft remains the elephant in the room for companies, dwarfing revenues lost by PII (Personally Identifiable Information), PHI (Protected Health Information), PCI and other data security incidents.

Five reasons why you should step up your DLP initiative

1. **1. The Struggle Is Real: DLP can be error prone**
   DLP struggles in identifying and applying policies to unknown data formats, unstructured data (anything outside of a database) and encrypted content. With DLP, the IT team needs to foresee what could happen before it does and set policies allowing DLP to recognize a threat situation. DLP is powerful, but it needs to be told what to do, with every policy defined before it occurs.
2. **False-Positive Results: DLP is imprecise**
   General rules are the strong suit for DLP - not specific data. DLP initiatives can be hampered by false positives and event overload. If an Admin needs to foresee every potential threat-scape before it occurs to make DLP effective, the input needs to be specific. If the setup for DLP is imprecise, when a policy is applied that should not be, false positives can occur.
3. **It's Complicated: DLP requires time**
   DLP initiatives can turn into long-term, never-ending projects, where specific policies have to be turned into automated rules for each identified threat. DLP initiatives require manual monitoring and regular policy updates to ensure that the security parameters are correct. Often, DLP initiatives are multi-year projects with policies that need to be fine-tuned on a regular basis.
4. **Limited by Tunnel Vision: DLP can have a narrow focus**
   DLP is not agile in enforcing access policies when data has crossed the perimeter and is outside the network defenses. DLP is like a security guard, protecting the doors. It will either stop or not stop elements from coming inside and breaching the perimeter. It will apply the policy on file and do as it instructs. This means that sometimes, threats can slip past the DLP protection in place.
5. **Some Assembly Required: DLP requires knowledgeable users to optimize its functionality**
   Unlike antivirus protection and firewalls, DLP is not a transparent security control. DLP applies the policies established for its function and applies as instructed. Users must recognize that for a DLP solution to be optimally effective, operators must understand the specific rules it requires to function. End users need to be educated and trained to ensure it is used properly.

Combining Data Classification and Data Loss Prevention

By deploying Data Classification together with a DLP, organizations will enable the broad, effective application of protection and governance policies across the entire enterprise IT ecosystem, and throughout all the steps of the data life cycle.

Unstructured data is the most ubiquitous type of data, and according to Darin Stewart, Research Director for Gartner, 80% of the total information assets take this form.

A combined approach enables organizations to achieve:

A combined approach with a DLP system, where RightsWATCH automatically informs a DLP to take further preventative action, enables companies to achieve:

1. Dynamic classification of unstructured data assets, using content, context, and various metadata characteristics, so that unstructured data is granted some sort of structure.
2. Fewer false positives, by applying watermarks and tags to inform and help the DLP on the appropriate actions to take every time;
3. User transparency, by informing the user of how the data asset should be handled and why, thus mitigating security issues from inception;
4. Throughput, as it relieves the DLP of onerous content analysis, thus processes are dealt quicker, with more precision and more certitude.

RightsWATCH is Data Classification that works

RightsWATCH delivers user-friendly data classification and labelling, while automating a company's corporate policies and life-cycle document management:

- RightsWATCH digitizes your corporate classification policies, automating the process while simplifying the user experience.
- RightsWATCH helps to educate users by showing them why an asset is being classified or labeled, allowing them to modify the data before finalizing it if necessary.
- RightsWATCH works at the point of inception, so compliance is achieved with no extra work on the part of the end user.

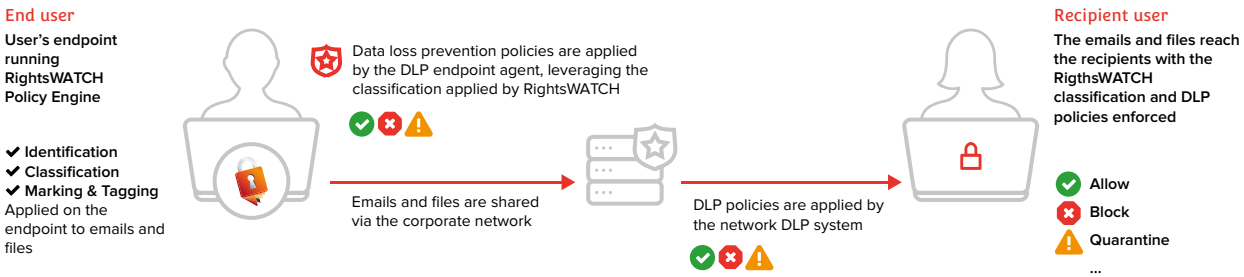

FIGURE 2 - RIGHTSWATCH AND DLP: A COMBINED APPROACH

Usage Scenarios with RightsWATCH and DLP

To illustrate the benefits of combining RightsWATCH with a DLP system more clearly, lets address a few common usage scenarios.

1. **Sending an e-mail to a wrong recipient**
   Sensitive data might be exposed when an email message is sent to a wrong recipient, intentionally or inadvertently. RightsWATCH prevents an email from being sent if sensitive content or attachments are being sent to unauthorized recipients. These blocking policies are triggered based on a central setting in RightsWATCH that defines if and in which conditions should the policy be enforced.

2. **Data classification and protection from inception**
   RightsWATCH can be used to label and tag unstructured data (emails, Office files, PDFs, image files, etc.), from the moment these are produced in a distributed fashion, by an organization's user population. A DLP working downstream in the process, can then leverage the classification labels and file attributes added to the email and file from RightsWATCH, to apply and enforce corporate Role-based Access Control (RBAC) policies to control and prevent the mishandling of sensitive data and users from performing inappropriate actions with it.

3. **Legacy data classification and enforcement of policies**
   RightsWATCH's Data Classification engine can be dynamically invoked by a DLP to automatically classify and label legacy files that are stored in corporate repositories. Via several integration scenario options available, RightsWATCH makes it straightforward to seamless integrate a DLP's Data Discovery and Content-aware scanning capabilities with automatic Data Classification.

4. **Sharing sensitive data via cloud drives**
   The use of cloud drives, and other removable drives, exposes businesses to a significant risk of sensitive data being leaked or lost. Additionally, many organizations use network shared drives for collaboration purposes, which might have limited access controls. RightsWATCH and a DLP system can work together to prevent the copying of sensitive material to an unprotected network share, cloud drive or removable drive:

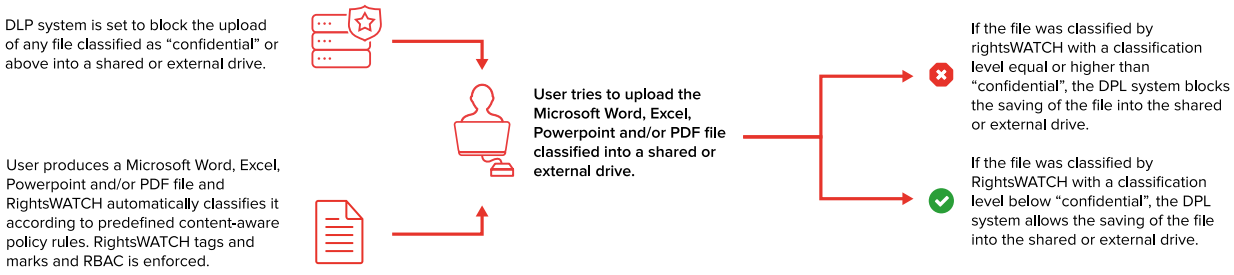

FIGURE 3 – SAVING FILES INTO A SHARED OR EXTERNAL DRIVE WITH RIGHTSWATCH AND DLP

5. **Enforcing policies on emails being produced on Mobile Devices**
   Because of limitations in OS APIs, the variability of OS configurations, different computing capabilities, DLP vendors have not been capable of deploying native content-aware DLP software onto tablets or smartphones. RightsWATCH enables organizations to embrace a BYOD initiative as it classifies and tags emails being sent on iOS and Android devices, so that the network DLP can leverage those to better understand and reason with which policies to enforce to each email.

The emergence of mobile devices and smartphones has turned the concept of a "secure network perimeter" upside down. Now, some of the most vital and sensitive corporate information travels the globe on the same device as social networking, games and kids' homework.

Summary

A combined approach, where RightsWATCH automatically informs a DLP to take further preventative action, enables enterprises to have mechanisms to discover information, monitor its flow and protect it to prevent exfiltration (intentional or inadvertent), to ensure compliance with information security and access policies, and to maintain an audit trail for control and compliance.

Combining RightsWATCH classification with a Data Loss Prevention system allows enterprises to:

1. **Remind users of information management policies as the information is created;**
2. **Enforce policies before the data leaves the endpoint;**
3. **Track where what type of unstructured data is being created, and by whom;**
4. **Streamline information classification and labelling across the extended enterprise (BYOD).**

In a nutshell, you shouldn't be forced to compromise on corporate security policies, nor fight or rebuild your existing DLP. RightsWATCH enhances your DLP initiative, taking the guesswork out of identifying sensitive data.

RightsWATCH

More info at: www.watchfulsoftware.com
and info@watchfulsoftware.com