



The Security Division of EMC

White paper

Five Key Considerations for Selecting a Data Loss Prevention Solution



What do you need to consider before selecting a data loss prevention solution?

There is a renewed awareness of the value and vulnerability of sensitive personal, financial and business information as a result of the increasing number of security breaches leading to data loss. According to the Identity Theft Resource Center, the

number of data breaches reported in 2008 rose almost 50% over those reported in 2007. In fact, since January 2005, over 260 million electronic records have been breached¹ – and that only accounts for those that have been reported.

Contents

The True Costs of Data Loss	page 1
Five Key Considerations for Selecting a DLP Solution	page 1
Consideration #1: Policy and Classification	page 2
Consideration #2: Identity-aware Policy and Response	page 3
Consideration #3: Incident Workflow	page 3
Consideration #4: Scalability	page 4
Consideration #5: Built-In Systems Approach to Information Security	page 4
How RSA Delivers	page 5
Consideration #1: Policy and Classification	page 5
Consideration #2: Identity-aware Policy and Response	page 6
Consideration #3: Incident Workflow	page 7
Consideration #4: Enterprise Scalability	page 8
Consideration #5: Built-In, Systems Approach to Information Security	page 9
Conclusion	page 10

The True Costs of Data Loss

Compliance is only one piece of the puzzle when it comes to protecting sensitive information. While civil penalties and fines may result from non-compliance, there are a multitude of other costs – both tangible and intangible – that make protecting sensitive data a critical component of any security strategy.

There are many tangible costs associated with a data breach such as the costs of customer notification, record recovery, investigation and legal fees. According to the Ponemon Institute, the average cost to an agency or business per compromised record is \$202 and the average total cost per breach is \$6.6 million.

However, the true costs are even more substantial when you consider the intangible costs – the effect on customer loyalty, brand and shareholder value. Many researchers have attempted to quantify the intangible costs that result from a data breach. The Ponemon Institute, for example, studied the effect of a data breach on customer churn. In their survey², nearly one-third of consumers notified of a security breach stated they have terminated their relationship with the breached company.

Even more damaging is the potential effect on brand and shareholder value. A 2008 study conducted by the University of Texas School of Management found that companies that experienced a data breach lost 2.1 percent of their market value within two days of the breach. This figure translated to an average of a \$1.65 billion loss in market capitalization per incident for the companies examined in the study.

¹ Privacy Rights Clearinghouse

² *Consumer's Report Card on Data Breach Notification*, Ponemon Institute, April 2008

Five Key Considerations for Selecting a Data Loss Prevention Solution

Data Loss Prevention (DLP) solutions are about reducing the risks of information loss by proactively locating and controlling sensitive data. As defined by leading analyst firm, Gartner, DLP technologies are “those that — as a core function — perform deep content inspection of data at rest or in motion and can perform some level of remedial action based on policy settings, which can range from simple notification to blocking.”

Organizations must consider three important questions as they start to explore the use of a DLP solution to protect their sensitive data:

- What types of data should I monitor and control?
- What actions can I take to reduce the risks to that data?
- How can I accomplish this in a cost-effective manner while minimizing the impact on my employees' ability to do their jobs?

By automating this process, the value of a DLP solution can be realized more quickly.

RSA, The Security Division of EMC, has been in the business of information security for over 25 years. RSA has numerous Data Loss Prevention deployments in use today across industries such as financial services, insurance, software, retail and telecommunications. These deployments range in size from a few hundred users to several hundred thousand users and are used to protect data at rest, data in motion and data in use.

Based on this extensive experience and insight, RSA has identified the following five key considerations that organizations should evaluate when selecting a DLP solution that is right for their business:

1. Policy and classification
2. Identity awareness
3. Incident response and workflow
4. Enterprise scalability
5. Built-in systems approach

The following sections describe these five key considerations in greater detail and their importance to selecting a DLP solution.

Consideration #1: Policy and Classification

The first consideration in evaluating a DLP solution is policy and classification. A robust and effective policy and classification library will save organizations time by enabling them to leverage more pre-built policies and reduce risk by applying effective policies to prevent data loss.

Robust Policy Library

The first step in the policy and classification process is to understand your information landscape and use policies that address the numerous types of sensitive data in your organization for all locations worldwide. This can be driven by the need to protect regulatory data or corporate intellectual property. Examples of regulatory data include Payment Card Industry (PCI) data such as credit card numbers or personally identifiable information (PII) such as Social Security numbers or international passport numbers. Examples of intellectual property include company financials, product roadmaps, blueprints, design documents, or M&A information.

A strong DLP solution will contain a rich policy library that can easily align with an organization's defined policies to detect sensitive data relevant to the full range of U.S. and international regulations and corporate intellectual property. Given that regulations are global and data loss prevention is a relevant issue for all organizations, it is necessary to have broad geographic policy support. A DLP solution that offers a comprehensive, pre-built policy library can help save valuable time and resources as security professionals are not required to develop policies from scratch.

Does the DLP solution address a complete range of global policies that meet my compliance and corporate security needs?

Effective Policies and Classification

The second step in the policy and classification process is to define effective policies. This involves specifying the usage and handling rules based on the sensitivity of the data. Usage and handling rules can vary, depending on industry regulations or corporate security policy and may include actions such as encryption, alerts, quarantine and blocking.

Policies are important for determining when a violation has occurred and how that violation should be handled. By defining a broad set of usage conditions and handling rules, organizations can ensure that the DLP system acts in accordance with their specific data protection needs.

Accuracy in detecting sensitive data, however, is most critical to finding the right data in order to avoid creating false positives. If a solution offers policy capabilities with a wide range of handling options, but does an inferior job of singling out data that must be protected, the level of remediation options available becomes unimportant. Organizations should consider a solution that uses the following content detection methods in order to achieve the highest levels of accuracy:

Described Content Detection encapsulates the logic and rules for detecting specific types of data such as Social Security numbers, proper names or corporate financials. Designed to be built once and reused many times, these classification modules can be leveraged across multiple policies that may require the identification of similar sets of data.

Fingerprinted Content Detection is the most accurate content detection technique for identifying whole or partial sections of documents. Fingerprinting is ideal for sensitive data that can be clearly identified ahead of time, such as structured data in databases, document-based content such as intellectual property and other kinds of digital content that maintains its integrity over time.

Effective policies require classification modules that are highly accurate. Product capabilities are one side of the equation; a robust engine that can define the rules and contextual evidence is essential. The other side of the equation is having a proven methodology to build the classification modules so they have the right balance of precision and recall. For pre-built out-of-the-box classification modules, it is necessary that the individuals

building them have the right background, specifically in areas such as library science, information science and/or linguistics. A dedicated team that is responsible for ensuring the accuracy of classification modules by staying abreast of the latest changes in global regulations and maintaining the policy library to reflect those changes is a key requirement.

Consideration #2: Identity-aware Policy and Response

Identity awareness is critical when preventing data loss. Organizations must be able to determine the individuals or groups that can access and use sensitive data and establish controls to make sure the right users are accessing the data. A DLP solution should offer strong identity awareness capabilities and controls to ensure that the right data is allowed into the hands of the right users and that the proper notifications and controls are in place to prevent data loss or misuse. Effective controls can minimize the impact on employee productivity and IT resources.

There are three specific areas that should be considered in evaluating the identity awareness capabilities of a DLP solution:

Identity-based policy. Establishing policies as to how sensitive data should be handled based on the user or group is important for increasing data security while also minimizing disruption. For example, in a healthcare setting, perhaps only a physician or nurse should be able to copy a patient's EHR data to a USB drive. A good DLP solution will offer policies that combine content and identity awareness.

Identity-based notification. When a policy is violated, it is important that a DLP solution have the capability to notify the necessary individuals and/or groups to take appropriate actions depending on the severity of the incident. For example, for critical incidents where highly sensitive data is moving outside the business, an organization may send a notification to both the sender and data owner that a policy has been violated. However, for less severe incidents, the organization may require just the sender to be notified and enable the document to be self-released by the sender.

Identity-based controls. Once sensitive data is identified, developing controls based on identity at the individual or group level is important to reducing the risk of exposure. Examples of identity based controls include enterprise rights management and access controls.

Making controls transparent to the user is important for safeguarding sensitive data while allowing employees to perform their daily job functions without disruption. Implementing a DLP solution provides a good opportunity to raise awareness among employees and other users within the organization about the potential impact their behavior could have in causing and preventing data loss. A DLP solution that offers self-remediation options can be an effective tool for educating employees on information risk as well as reducing the time spent by administrators investigating incidents that can be handled directly by the user.

Consideration #3: Incident Workflow

A DLP solution should have an effective process for alerting and remediating incidents in order to avoid unnecessary disruption and potential data loss from occurring. A smooth and consistent workflow, which ensures that the right alert is delivered to the right person/people with all pertinent information, will reduce the time spent in routing and analyzing incident reports.

Does the DLP solution offer the superior accuracy needed to secure my business? Is it backed up by a team of experts dedicated to keeping the policy library up-to-date?

Issues such as receiving multiple alerts for the same incident or not being able to retrieve the necessary information in the alert to effectively respond could inhibit administrators from quickly resolving the problem and expose the organization to potential data loss incidents as action may be delayed. An effective incident workflow can also reduce the resources required to manage incidents.

A DLP solution that can integrate with a security information and event management (SIEM) solution is also important to prioritizing how incidents are handled. By using server logs created by a SIEM solution to identify which files are accessed, a DLP solution can determine which of those files were sensitive and how they were used.

A DLP and SIEM integration enables organizations to detect security threats earlier and prioritize incidents based upon the sensitivity of the information potentially compromised. This can help reduce the impact of security incidents and allow for quicker remediation.

Consideration #4: Scalability

Scalability is an important factor when considering a DLP solution. Large organizations have many locations and large data stores accessed by thousands of users and applications. Will you have to buy lots of additional hardware servers at all of your locations to deploy a DLP solution to scan your data repositories or can you leverage existing hardware resources?

Scanning speed is also a key scalability feature that should be considered. Organizations with large data stores need to be able to scan large amounts of data – and fast. A DLP solution should be able to make the best use of IT resources to process DLP scans as fast as possible. The scanning infrastructure should also offer load balancing across multiple scan servers to scan data more quickly without requiring a lot of manual tuning from the IT team to optimize the process.

Besides the cost of hardware, there are the IT personnel costs associated with setting up and managing the scanning process. Assume an organization wants to scan an environment with 12 databases, 100 SharePoint sites and 500 file servers. Will the IT staff have to spend a lot of time determining how to segment the infrastructure by scan server or does the DLP solution offer the flexibility to allocate scan server resources based on the amount of data to be scanned? What are the additional IT resources that will be required if the organization decides to scan more of the environment or add more scanning servers to the infrastructure? A solution that is not capable of adapting to changes in the IT infrastructure will add complexity, increase ongoing management costs and add to the total cost of ownership.

It is also critical to be able to conduct a scan for sensitive data as quick as possible without hampering the performance of the IT infrastructure. This is especially important when performing a new scan after a policy has been changed or added. A DLP solution should have an architecture that minimizes the amount of data sent over the network and scans the environment with minimal impact on production applications.

Consideration #5: Built-In Systems Approach to Information Security

Securing information is an end-to-end problem. It requires visibility and control of information throughout the infrastructure for data at rest, data in motion and data in use. Many solutions today only address one element in the infrastructure. For example, to protect lost or stolen laptops, a vendor might offer full disk encryption. Another vendor

Does the DLP solution combine identity and content awareness to protect my sensitive data based on who is accessing it?

might offer access controls to protect a file server from unauthorized access. Each of these point solutions come with their own management console and set of policies, and are often applied without content or identity awareness.

To effectively address the end-to-end problem of securing data, organizations should be able to centrally define a set of policies and apply them across the infrastructure to identify sensitive data, apply the right controls to that sensitive data based on identity and context, and collect incident and event data for auditing and reporting. To accomplish this, there is a need to embed a common DLP policy and classification framework into common infrastructure elements such as those provided by Microsoft and Cisco and to integrate the controls that customers use today such as enterprise rights management to enforce DLP policies.

Finally, the ability to send incidents and control data to a security information event management (SIEM) solution ties content-based incidents with infrastructure-based incidents, providing a single pane of glass to manage security incidents.

Organizations should ask several questions when evaluating the built-in approach being taken by a DLP solution provider:

- Does the provider partner with infrastructure vendors to embed DLP classification technology and policies across all elements of the infrastructure?
- Does the provider use a common policy and classification framework to push policies down into the infrastructure and to push incidents up to a common management console?
- Does the provider integrate with third party controls for enforcement and with SIEM vendors to provide a single pane of glass for incident management?

How RSA Delivers

The RSA® Data Loss Prevention Suite offers a comprehensive data loss prevention solution that discovers, monitors and protects sensitive data whether at rest in a data center, in motion over the network, or in use on a laptop or desktop. The RSA DLP Suite provides a policy-based approach to securing sensitive data, enabling organizations to discover where it resides, enforce appropriate controls, and report and audit as mandated.

The RSA Data Loss Prevention Suite is offered in three distinct modules:

- RSA® Data Loss Prevention Datacenter identifies and controls sensitive data stored across file shares, SAN/NAS, databases and other data repositories such as content management systems.
- RSA® Data Loss Prevention Network identifies and controls sensitive data as it travels throughout the network and enables policies to be enforced across areas such as corporate e-mail systems, web-based e-mail systems, instant messaging and web-based protocols.
- RSA® Data Loss Prevention Endpoint identifies and controls the usage and movement of sensitive data on laptops and desktops

The RSA DLP Suite offers many distinct features to address each of these five key considerations.

Consideration #1: Policy and Classification

The RSA DLP Suite takes a policy-based approach to securing sensitive data – combining data discovery and classification and policy creation into a single process. Once sensitive data is discovered and classified, policies enable data controls to be enforced, determines who gets notified and how incidents are handled.

The RSA DLP Suite offers a robust policy library containing more than 150 “out-of-the-box” policies. RSA boasts the broadest set of U.S. and international policies covering a wide range of regulations including HIPAA for health care, ITAR for export compliance and FERPA for education. It also offers wide coverage for PII policies such as International Bank Account Numbers (IBAN) in France, Germany, Italy, Netherlands, Sweden and the UK.

The content library is continually being developed and updated by RSA’s Information Policy and Classification Research team, a group of researchers dedicated to studying the U.S. and international regulatory environment and applying that knowledge to develop relevant policy templates that can be applied across multiple industries and regulations. By eliminating the need to set up and tune new policies, the RSA DLP Suite enables organizations to realize the value of their DLP deployment more quickly while also reducing the overall total cost of ownership.

The RSA DLP Suite also provides superior data detection accuracy by leveraging both fingerprinting and described content capabilities, depending on the type of sensitive data and where it resides. With industry-leading accuracy (see sidebar), it can limit an organization's exposure and save valuable administration time and resources.

Consideration #2: Identity-aware Policy and Response

The RSA DLP Suite is an identity-aware solution that offers identity and content awareness. It leverages Microsoft Active Directory® Groups on the network and at the end point to identify which files users are accessing, who gets notified in the event a policy is violated and how incidents are handled. The RSA DLP Suite provides identity awareness in several ways:

Identity-based policy. The RSA DLP Suite uses AD Groups to set granular policies for individuals or groups. For example, in the RSA DLP Network module, a policy can be set up to only allow the finance department to send corporate financials outside of the network.

Identity-based controls. The RSA DLP Suite leverages controls such as encryption or blocking based on individual or group identities for data in use or data in motion. RSA's integration with Microsoft Rights Management Service (RMS) also provides identity specific controls for data at rest.

Identity-based notification. Policies in the RSA DLP Suite can be designed to notify specific users once a policy violation has occurred. For example, if an employee violates a policy by copying a sensitive document to a USB stick, that employee's manager can be notified.

The RSA DLP Suite also offers a self-remediation option so the user is personally notified when a policy is violated and allowed to make a decision about what action to take. This option is good for raising education among employees concerning how their actions can put data at risk. But more importantly, it can save administrative time and resources having to investigate incidents that do not have a high severity impact.

The RSA DLP Suite is also tightly coupled with Microsoft SharePoint® through RSA SecureView so that a SharePoint administrator can have visibility into which user groups have access to sensitive data in the SharePoint resource hierarchy. SecureView for Microsoft SharePoint communicates with the RSA DLP Suite and SharePoint to enable SharePoint administrators to centrally view the

entire resource hierarchy for a single SharePoint farm and determine the user access policies along that hierarchy. It enables administrators to select specific branches of the hierarchy to see if sensitive information, as discovered by RSA Data Loss Prevention Datacenter, resides there. As a result, SharePoint administrators can easily discover who has access to sensitive information across the entire farm from a single console.

The RSA Data Loss Prevention Suite Demonstrates Superior Accuracy Capabilities – an Independent Study by WIPRO

Recently, the RSA Data Loss Prevention Suite was evaluated on a number of levels next to a leading competitor. As part of the assessment, both solutions were rated for accuracy in identifying policy violations of sensitive data. High accuracy means the solution can detect a high percentage of sensitive documents, thereby protecting an organization from a security breach and limiting its exposure. In addition, it can reduce total cost of ownership by reducing the time and resources spent by administrators having to investigate low-priority incidents.

The RSA Data Loss Prevention Suite clearly outperformed the competing solution for accuracy in preventing false positives or "false alarms" and in scanning speed. Scanning for Payment Card Industry (PCI) data, the RSA DLP Suite consistently demonstrated 100% accuracy in avoiding false positives. In contrast, the competitor's solution recorded only 73% accuracy in avoiding false positives – that is, 27% of the documents identified as violating the policies were not sensitive.

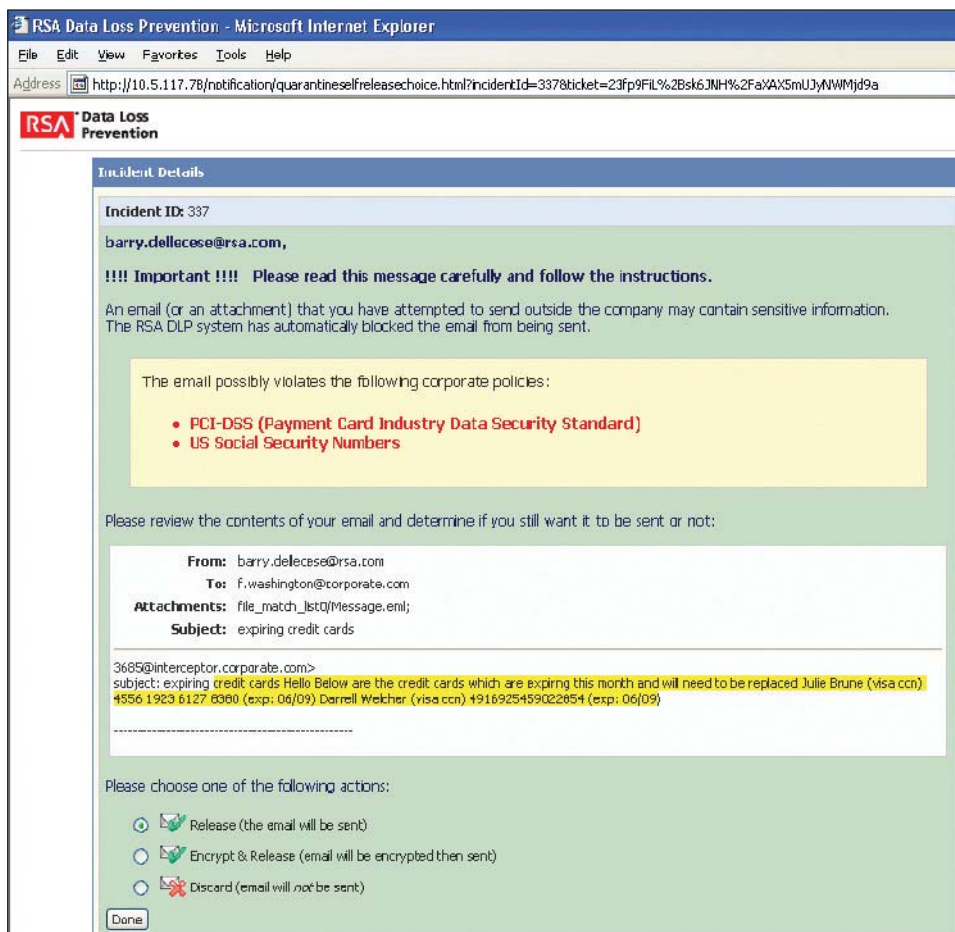
Finally, the RSA DLP Suite has been integrated into the Microsoft Rights Management Service (RMS) platform to discover and automatically protect sensitive data at rest. This reduces the risk of data owners not applying policies properly and it protects the most important data by applying RMS controls based on data sensitivity. This results in protection based on content and identity awareness which further reduces the risk of data loss.

Consideration #3: Incident Workflow

The RSA DLP Suite is known in the industry for its simple and highly actionable incident workflow. It gets the right information to the right user at the right time, avoiding the issues of receiving multiple alerts for the same incident or not being able to retrieve the necessary information in the alert to effectively respond. This saves organizations valuable time and resources in the incident workflow process.

The RSA Data Loss Prevention Suite offers the following incident workflow capabilities:

- Integration with the RSA enVision® platform, a leading log management solution, to enable effective prioritization of incident handling based on data sensitivity
- Built-in notifications and alerts workflow, using the Microsoft Active Directory hierarchy, to inform data owners as individuals or groups about affected files
- Correlates all related findings into a single alert along with all information that caused the alert in the first place. This allows incidents to be remediated quickly, thereby minimizing risk.
- The ability to customize alerts and notifications based on a number of factors so that incidents are prioritized for review



Self Remediation Option for DLP Policy Violation

