

An ILLUMANT White Paper



Efficiently Choosing a Data Loss Prevention Solution

WRITTEN BY

ROGER SMITH

DATE

OCTOBER 2008

Efficiently Choosing a Data Loss Prevention Solution

Selecting a cost effective DLP solution can be a daunting task unless one takes into consideration several key issues. How daunting? Illumant currently tracks and maintains a spreadsheet of approximately 50 vendors who claim offerings within the three major areas of the DLP product suite. The remainder of this document describes these key issues to help simplify the selection process.

DLP Product Suite Areas of Functionality

There are three primary components to a full-suite DLP package. When selecting DLP vendors to evaluate, it is helpful to be aware of the product distinctions to help narrow the field. The three primary areas are:

1. Discovery and Classification Tools
2. Monitoring Tools
 - a. Monitor Data in Motion
 - b. Monitor Data at Rest
 - c. Monitor Data in Use
3. Reporting Tools

These components contribute to the three main areas of functionality most usually associated with a full suite DLP solution:

- Define Sensitive Data
- Identify Sensitive Data
- Enforce Control and Compliance

Most enterprises shopping for a DLP solution are looking for a vendor that offers a full suite solution – that is one that provides major functionality in all three product suite areas. This is useful to know as about half of the known vendors specialize in only one or two of the three functionality areas.


Clearly Identify Goals and Objectives

Many companies and enterprises are reluctant to approach DLP solutions because they see them as “big brother” monitoring of individuals for compliance violations. Attempting to deploy DLP with this preconception will almost certainly meet with considerable resistance from key stakeholders. Instead, DLP should, at least initially, be approached from the perspective of detection of broken business processes and controls. For example, at one client we recently discovered that a future quarter’s 10Q was being sent to a public auditor for review. This is not only an egregious violation of SEC rules, but it was also done unencrypted which further exacerbated the problem. The accounting department staff that was responsible for this thought it was part of the accepted business process of preparing the 10Q and therefore considered it OK to obtain an auditor opinion. They were not aware it was a violation of SEC rules. Therefore this broken business process was brought to light by DLP and controls were put into place to prevent future compliance violations.

“At one client we recently discovered that a future quarter’s 10Q was being sent to a public auditor for review. This is not only an egregious violation of SEC rules, but it was also done unencrypted which further exacerbated the problem. The accounting department staff that was responsible for this thought it was part of the accepted business process of preparing the 10Q and therefore considered it OK to obtain an auditor opinion. They were not aware it was a violation of SEC rules. Therefore this broken business process was brought to light by DLP and controls were put into place to prevent future violations.”

Data Loss Challenges

- ▶ To identify sensitive data
 - For data in motion in network
 - For data at rest in data center
 - For data in use in end points
- ▶ To identify violations in usage of sensitive data
 - Violation against compliance
 - Violation against corporate policy
- ▶ Take actions
 - Take remediation actions
 - Enforce controls
 - Manage remediation through a work flow process



Identify the network Perimeters

Clearly identifying the perimeters that are to be protected must be done early and concisely in order to determine the range of tools needed. Each of the three monitoring tools addresses a specific portion of the network perimeter.

Data-in-Motion Monitoring

Data-in-Motion addresses data crossing the enterprises (or departmental) primary portal. This is usually the transition from an internal network to a public Internet and would normally be defined by a firewall or router. However, it can also be a departmental boundary isolating a departmental LAN from a larger enterprise WAN/LAN.

Data-at-Rest Monitoring

Data-at-Rest tools sit on a network's backbone. They periodically search all known disks, disk farms, and file stores for the currently identified set of fingerprints. This form of monitoring can catch broken business processes that allow users to remove files or documents from databases and other protected archives and store them in unsecured areas.

Data-in-Use Monitoring

Data-in-Use tools address user activities at the endpoints. Endpoints are usually defined as the laptops and desktops throughout the enterprise. Data-in-Use monitors for activities involving file and document movement to memory sticks, removable disks, PDSs, and so forth. Mobile and removable devices serve to extend the network perimeter under protection – sometime drastically so.

Compliance Issues Are Commoditized Among Most Providers

The entire suite of compliance issues has matured to the point where most vendors offer “canned” libraries that define all known instances. This applies to PCI, HIPAA, and FERPA, to name but a few. Vendors who are not up to this level should be given lower priority consideration. Prospective DLP users should consider the issue as binary; i.e., the vendor either provides a library with definitions for all combinations and permutations of violations for compliance areas or they do not. Vendors will want selection panels to evaluate their product as providing superior service for compliance. Panels would be much better advised to spend their time evaluating other areas of differentiation.

Primary Areas of Differentiation

There are several areas emerging among the major vendors that do help distinguish one from another and that are worthy of consideration for any selection panel.

Unstructured Data

There are significant differences between the approaches taken by each of the principal vendors for the handling of unstructured data. This is the term usually used to describe intellectual property and can include items like source code, engineering drawings or documents, process descriptions, chemical or biological formulae, etc. Look for a vendor with a discovery tool that does not require everything to be pre-defined, i.e., a tool that can be “pointed” at a file to establish a fingerprint to use in future searches for similar files.

Forensics

Many vendors are very strong on forensics and can literally replay an entire incident, while others do not maintain any form of playback data store. The ability to playback an incident helps with analysis and can also contribute to evidence accumulation. Panels must decide if the collection of evidence of violations is important in their search and narrow the parameters accordingly.

Discovery and Classification

This is the class of tools that can be a real key differentiator in a selection process. Many of the vendors are surprisingly weak in this area. However, the ability to discover and classify all forms of sensitive data early in a DLP project (according to the definitions set in your data classification standard) will definitely make a big difference in the magnitude, complexity, and possibly even success, of the implementation phase.

Sampling Design

Some of the vendors only sample the data stream, especially during periods of high traffic. This quite obviously results in (possibly high) false negatives, i.e., missed violations. Make sure you fully understand the vendor’s sampling strategy and their scheme for handling periods of high traffic volume.

Network Coverage

Most DLP vendors will try to convince you that you have to buy a seat for every staff member, including those who do not handle sensitive data in any form, e.g., maintenance, warehouse, shipping & receiving, etc. Illumant believes that, for many clients, a more cost-efficient approach would be to isolate the sensitive data to a dedicated portion of the network and then place the DLP tools at those network borders. Of course, prudent access controls and rights management within the dedicated networks are equally essential components of a robust security program.

About the Author



Roger Smith spent 15 years as a consultant at NASA's Ames Research center. Upon leaving NASA he went into senior IT management working for such notables as the original Napster. Right after Napster he opened a security and compliance practice and has been specializing in those two areas ever since. He is now with Illumant, LLC, a security and compliance practice where he leads the DLP efforts for the firm.

Illumant has spent months and hundreds of staff-hours assessing the capabilities and limitations of almost 50 vendors in this market space. Give us a call today and let us share this expertise with you as you explore DLP capabilities for your enterprise. Our experienced consultants can save you hundreds of hours in selecting a vendor, tens of thousands of dollars over a typical DLP installation, and potentially save you even more money on post-implementation administration and support.

Illumant Proudly Represents



Our most recent study matrix of almost 50 active DLP Vendors can be found at:
http://www.illumant.com/Illumant_DLP_Vendors.php



ILLUMANT

2672 Bayshore Parkway
Suite 505
Mountain View, CA 94043
Phone: +1 650.961.5911
Fax: +1 650.961.5912

www.illumant.com

ABOUT ILLUMANT

Illumant is a trusted strategic and tactical risk management advisor to Fortune 500 companies, higher education institutions, and other public and pre-public enterprises.

Leveraging best practices and deep knowledge of governance, risk management, compliance, and information technology, we partner with our clients to assess and solve critical business problems. Whether the focus is on initiatives driven by regulatory compliance, corporate mergers and acquisitions, or operational pain points, Illumant plays a major role in helping clients consistently meet their objectives.