Data Loss Prevention

By:

Musab Haj-Hamed

Submitted to:
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

© Copyright Musab Haj-Hamed

The author grants to the School of Information Technology permission
To reproduce and distribute copies of this document in whole or in part.

Musab Haj-Hamed

Mark Stockman, Faculty Advisor

University of Cincinnati
College of Education, Criminal Justice, and Human Services
April 2014
# Table of Contents

Abstract .......................................................................................................................... 3

Introduction ................................................................................................................... 4

Current Situation .......................................................................................................... 4

User Profiles ................................................................................................................. 5
  Table 1 User Profile Form .......................................................................................... 6
  Figure 1. DLP’s Diagram ......................................................................................... 7

Technical elements ....................................................................................................... 7

Budget ............................................................................................................................ 8
  Figure 2. The University of Cincinnati’s e-mail demo ................................................. 8
  Figure 3 DLP’s Timeline .......................................................................................... 9

Quadrant Gartner ......................................................................................................... 9
  Figure 4. (Ouellet and Silva) .................................................................................. 10

McAfee vendor ............................................................................................................. 10
  Figure 5 – The Sources of Data Loss ....................................................................... 11

Symantec vendor ........................................................................................................ 11

Open Source OpenDLP ............................................................................................... 11
  Figure 6. Create a New Scan Profile .................................................................... 12
  Figure 7. Profile Submission ............................................................................... 13
  Figure 8. Start a New Scan ................................................................................... 14

Conclusion ................................................................................................................... 14

Works Cited ............................................................................................................... 16
Abstract

DLP solution is a system designed to detect potential data breach incidents in a timely manner and to prevent breaches by monitoring data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). The Information Technology environment within the University of Cincinnati is complex and decentralized. Sensitive electronic data resides and travels to and from individual user workstations, servers, databases and various applications without being properly restricted. The cost of the DLP solution depends on the number of users on the network. Given a number of business users at the university, the approximate initial cost would be around $200,000. Ongoing annual maintenance cost is estimated at $20,000.
Introduction

The University of Cincinnati wants to establish Data Loss Prevention (DLP) in the network and data center. DLP helps reduce the risk of losing data. The University of Cincinnati wants to research which vendors are best to purchase. Examples of vendors are HP, McAfee, and RSA. The objective is to research and assess a variety of DLP vendors and recommend one or two vendors best-suited for UC environments and infrastructure. A DLP solution is a system designed to detect potential data breach incidents in a timely manner and prevent them from happening. We want to monitor some of the specific data, which consists of the following: a driver’s license number, a social security number, and an ISO. The DLP solution scans data on the server, detects the sensitive data, and makes sure there is a good logical access control. It is localized in one place, and it starts scanning the servers and detects who has access to them.

Current Situation

The Information Technology environment within the university is complex and decentralized. The data center is not set up in the same place because the University’s infrastructures are set up in different ways. Some colleges do have a data center; some do not have a data center. Sensitive electronic data resides and travels to and from individual user workstations, servers, databases and various applications without being properly restricted. The University of Cincinnati has a problem with leaking data that is exported from the university and also importing data. The University of Cincinnati wants to reduce sensitive information and secure the data: “Unfortunately, companies constantly fall victim to massive data, loss and high-profile data leakages involving sensitive personal and corporate data continue to appear” (Simon and Rick), which means companies are losing a lot of sensitive and corporate data.
The University of Cincinnati has massive data loss; hackers steal sensitive data and hack databases to steal credit card numbers, ISO numbers, and customers’ first and last names. This is a common form of data loss, which is often due to the hacking of customer databases, making it the most common consequence identity theft. In the largest single attack of this type of date, hackers stole 130 million credit-card records from one of the US’s largest payment processors (Simon and Rick). This statistic illustrates that the most common consequence of hacking is identity theft. DLP is very important to avert hackers from stealing more information from corporations. The University of Cincinnati must accept the risk of business. The University of Cincinnati strives to establish a secure atmosphere to reduce data loss: “Today’s movement toward extensive use of electronic medical records can present a new class of risk for both the consumer and the organization” (Simon and Rick). The statement means customers and organizations have their own risk for their data. The customers and organizations have to accept the risk to continue their tasks or business. However, with this need for higher security, there is often a lack of user-friendly software. The security and user-friendly elements have to be in balance.

**User Profiles**

The University of Cincinnati has different infrastructures because almost each building has Information Technology. Some buildings have Information Technology but not all. University of Cincinnati wants to focus on small networking; for example, CECH’s networking, instead of entire University’s networking. There is no Information Technology center or headquarters for the entire university. The software and interface vendors are McAfee, Symantec, and RSA. The Quadrant Gartner helps us understand which vendors are best to procure. Microsoft Outlook is used mostly for college, but the College of Medicine does not
have it. The University of Cincinnati medical school uses paper instead of e-mail. If the data were encrypted, it would be more secure. If it is not encrypted, then the security and monitoring of the data must improve. The data center will use DLP software for everyday use while the system is up consistently. The system will set up monitors 24/7 to perceive sensitive information in an e-mail, web application, and data in motion.

Table 1 User Profile Form

<table>
<thead>
<tr>
<th>User Profile Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application:</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Potential Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. University of Cincinnati Students</td>
</tr>
<tr>
<td>2. University of Cincinnati Facility</td>
</tr>
<tr>
<td>3. Exterior user an E-mail</td>
</tr>
<tr>
<td>4. Students</td>
</tr>
<tr>
<td>5. Faculty</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software and Interface Experience:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user should have experience loss data by an e-mail and network traffic. The user set up filter an email to help reduce loss sensitive data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience with Similar Applications:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Vircom software</td>
</tr>
<tr>
<td>2. OpenDLP</td>
</tr>
<tr>
<td>3. McAfee DLP Endpoint</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task Experience:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Managing a Network.</td>
</tr>
<tr>
<td>2. Managing a E-mail</td>
</tr>
<tr>
<td>3. Managing a Data Center</td>
</tr>
<tr>
<td>4. Managing a DLP server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Frequency of Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The data loss prevention should open seven days a week. The data loss prevention software will running by 24/7 and never shut down or disable.</td>
</tr>
</tbody>
</table>
The data server set up in the data center and the DLP’s listener is between DLP servers to application. The DLP’s listener monitors packet and decides to approve or reject going through each application. There are different application examples in the diagram.

**Technical elements**

The technical elements inspect projects with different vendors and software to capture sensitive data. The software’s names are McAfee, RSA, HP, and Symantec. The research concerns different software to decide which the best procurement is. Wireshark is able to capture the packet and perform analysis. The University of Cincinnati prefers to purchase software instead of open source because of the license and technology support. The technical elements are Microsoft Exchange 2013, Microsoft Server 2008 R2. The Microsoft software is from the University of Cincinnati MSDN academic alliance software center. The University of Cincinnati offers Sandbox for virtual to test DLP.
Budget

The cost of the DLP solution depends on the number of users on the network. Given a number of business users at the university, the approximate initial cost would be around $200,000. Ongoing annual maintenance cost is estimated at $20,000 to $40,000. DLP implementation is fairly straightforward and does not require assistance of external resources. One to three network appliances would need to be deployed on UC’s network. The DLP solution, an OIS resource should be assigned to monitor daily potential violations. This requires an additional ongoing personnel expense of $85,000 (including benefits) (University of Cincinnati/Information Security). The Open Source OpenDLP is free software, and there is no budget really needed for it.

Figure 2. The University of Cincinnati’s e-mail demo
Figure 3 DLP’s Timeline

Quadrant Gartner

By employing the quadrant, one can learn which vendor is best. The Quadrant Granter has four different locations with different vendors. How can the Quadrant be used to choose the best vendors? The four types of area in vendors are Leaders, Visionaries, Players, and Challengers. They are characterized in the following fashion. Leaders- run well against their current vision and are well positioned for the future. Visionaries- Understand where the market is going. Niche Players- focus successfully on a small segment. Challengers- May dominate a large segment. The University of Cincinnati is in the categories Leaders category because of their size. The Quadrant Gartner showed four different areas, but they only looked at the Leaders. Compare Quadrant Gartner from 2012 to 2013 and see which vendors have grown.
McAfee vendor

The primary strength of McAfee’s policy orchestrator is that it remains one of the better management platforms in these advanced features. McAfee is a great company and they have good technical support. Another crucial strength is that McAfee “helps you build DLP policies faster and better by giving you visibility into how your sensitive information is used across your enterprise” (Karwoski). The features capture technology, data classification, location, application tagging, virtualization support, and security connected platforms. McAfee offers many different features and security. Lou Karwoski from McAfee Company said, “While other DLP vendors support VDI, they only have a single policy enforced on these terminals – meaning that one policy must apply to all users, regardless of role or business requirements. Only McAfee offers the per-user policy” (Karwoski). This is the reason why the University of Cincinnati should purchase McAfee. The University of Cincinnati is entitled to DLP Endpoint and everything will be centrally managed through current ePO infrastructure.
As for weaknesses McAfee’s personal firewall or ePO policies, which may require the creation of duplicate policies for different subsystems.

*Figure 5 – The Sources of Data Loss*

The figure 5 is about the sources of data loss that happen in three different data types. The three different data types are data in motion, data at rest, and data in use.

**Symantec vendor**

The strength is full range of endpoint and servers, mobile management. Symantec offers the best for mobile management.

The weakness of the Symantec is very expensive, but they offer many different features and options for DLP. This software is unaffordable for University of Cincinnati. The University of Cincinnati’s budget is fairly limited to purchase Symantec.

**Open Source OpenDLP**

The OpenDLP is open source and is also free to download the software. The open source has both strengths and weaknesses regarding software. The benefits with OpenDLP are that it is free and more secure software. The problem with software is that there is no support with
software, update, and limited resources. The software can work with agentless-based, centrally-managed, and with an agent. The OpenDLP has minimum requirements to install. The minimum requirement is Windows 2000 or higher, written in C with no .NET Framework, and virtual box. The OpenDLP scans the network to find sensitive data. The OpenDLP has discovery tools with components for agent and Web applications. The software is useful for compliance personnel, network, system administrators, and penetration testers. The tools have a reusable policy to help you scan with whitelist, blacklist files, and directories. It also more pushes finding files securely.

The University of Cincinnati decided not to purchase OpenDLP because there is no technical support software, update, and license.

*Figure 6. Create a New Scan Profile*

The open source has a profile to set up where you want to scan, which has a location in the
directories. The examples of the location in the directories are `c:\windows`, `c:\wint`, and `c:\system volume information`. The profile submission sets up what kind scan you prefer and set up and which extensions you want OpenDLP to scan. The profile offers which types of the credit card for scan, for example, Discover, MasterCard, and Visa. There are numerous options available for selection.

*Figure 7. Profile Submission.*
Figure 8: Explains the start of a new scan. For the system to scan, it needs an IP address. When you set up an IP address, the system will scan to that IP address only. There is no limit to the number of IP addresses to add on scan part. One can add Ubuntu Virtual box’s IP address or Windows’s IP address to scan.

Conclusion

My proposed solution for my project is about researching different vendors and figuring out which procedure is best. The University of Cincinnati decided to use two different vendors, but cannot effectively utilize two at the same time because of potential issues. The University of Cincinnati must test each vendor individually to access actual cost of ownership. The University of Cincinnati decided McAfee is the best vendor to choose because of the price and McAfee offers the best features for DLP. The capture technology is key for capturing data. The University of Cincinnati benefits because McAfee “helps you build DLP policies faster and better by giving you visibility into how your sensitive information is used across your enterprise” (Karwoski). The University of Cincinnati can be confident in its choice of McAfee because it
“provides a historical record of all data leaving the enterprise without impacting performance of business data and traffic” (Karwoski). I highly recommend University of Cincinnati to purchase McAfee.

Lawhorn, Brian. Kroger. Personal Interview, 1 Nov. 2013


doi: http://dx.doi.org/10.1109/MITP.2010.52

Karwoski. Lou. Personal Interview, 7 Nov. 2013


