Data Loss Prevention: simplified

Released: May 3, 2010
Author’s Note

The content of this white paper was developed independently of any vendor sponsors and is the sole work of DLP Experts.

Licensed by Code Green Networks

Code Green Networks, headquartered in the heart of Silicon Valley, was started in 2004 by the founders of SonicWALL. Code Green Networks’ TrueDLP provides comprehensive data loss prevention (DLP) in a simplified architecture that is easy-to-install, easy-to-manage and easy on the corporate pocketbook. Unlike other enterprise data loss prevention solutions, Code Green Networks enables the largest global organizations to cost effectively start solving their core data leakage problems in days not months.

http://www.codegreennetworks.com

Copyright Notice

The content of this publication is copyrighted by DLP Experts.
Introduction

Today’s traditional Data Loss Prevention (DLP) solutions are characterized by two overriding and generally unattractive factors: they are overly costly and overtly complex. This white paper compares traditional architectures with an innovative architectural approach to DLP as well as various DLP cost models. With this white paper, we will show that DLP can be simplified, both architecture and cost.

Data Loss Prevention (DLP) technologies have a well-deserved reputation for having a high level of technical complexity and for being very expensive to acquire and administer. Most of today’s DLP technologies employ a complex network architecture; a modular approach requiring multiple servers at each egress point.

MODULAR, MULTI-SERVER DLP ARCHITECTURE

Traditional DLP

A comprehensive DLP solution today typically runs each individual component on a separate server. Among many possible network devices, DLP solutions may require any number of the following separate servers:

- Network Monitor
- Email Blocking
- HTTP/S and FTP Blocking
- Network-Based Discovery
- Endpoint Management
- Incident Database
- Management Platform (to tie it all together)
In order to provide complete DLP coverage, this often results in three, four or even more servers physically installed at each egress point in a network. If high-availability is a critical component, an organization may need to further increase the number of devices at each egress point. The graphic below makes it easy to see how traditional DLP can become very complex, very quickly.

**TRADITIONAL MODULAR DLP ARCHITECTURE**

![TRADITIONAL MODULAR DLP ARCHITECTURE](image)

**Unified DLP Architecture – simplified.**

In contrast to the traditional, modular, multi-server DLP architecture, the ideal, simplified DLP solution integrates all components into a single appliance:
Compared to the complicated architecture of a modular DLP approach, a single appliance can present a refreshing alternative for companies concerned with managing the complexities of a DLP solution. The appliance approach has been well-accepted to address a host of network security concerns and DLP is no exception. An appliance to passively monitor all traffic, combined with email and web blocking integration, network-based discovery and endpoint management, provide a more simple and cost effective DLP solution.

Even in a multi-egress-point, high availability environment, this simplified DLP solution cuts the hardware overhead to a much more manageable architecture, as demonstrated below.

**DLP Appliance Advantage**

Consider the advantages of managing a single device for DLP compared to three, four or even five servers.

**Easy Installation.** Designed to be “plug and play,” a single DLP appliance and can be racked and ready in a matter of minutes.

**Reliability and High Performance.** DLP appliances use an optimized combination of DLP software, operating system and hardware designed for the solution’s express purpose of preventing data loss. This makes the appliance-based DLP solution more likely to perform at a higher level and less prone to the support issues of software solutions.

**Low Management Overhead.** A single appliance is much easier to manage than multiple instances of software-installed servers. DLP appliances don’t require regular maintenance updates and security patches and support is handled by the lone DLP vendor, instead of three: the hardware manufacturer, operating system vendor and DLP software vendor.

**License.** There are no license fees for a separate operating system, database or other installed software, just the DLP license itself.
Total Cost of Ownership (TCO). A single appliance-based DLP solution results in a lower TCO compared to a software solution.

Solution Scalability. The capacity of a single DLP appliance is based on a number of factors, including bandwidth and number of users being monitored. Appliance-based DLP solutions generally have capacities comparable to multiple servers running traditional DLP software with some vendor appliances supporting up to 20,000 users on a typical network.

Some may question how a vendor can so drastically simplify the architecture, while other vendor solutions seem to get increasingly more complex? This is the result of a comprehensive view of the DLP market that requires not only insightful vision for the future, but also learning from the deficiencies of first-generation DLP solutions.

Early DLP vendors responded to the changing needs of the marketplace as they arose and did not have the benefit of past experience when considering the complete architecture.

Complete Coverage in a Single Interface

Sensitive data can leak from any number of different vectors, including various network protocols and removable storage devices. Among vendors applying the moniker “data loss prevention” to their technologies, many provide only point solutions of either endpoint or network gateway coverage. Relatively few vendors actually provide coverage across major leakage vectors while also including discovery of sensitive data on endpoints and network.

It is important to consider DLP enforcement technologies that include all key components of data-in-motion (network gateway), data-in-use (host or endpoint) and data-at-rest (discovery). Comprehensive DLP technologies are designed not only to provide more complete coverage than single-component point solutions, but also to simplify the administration between the different DLP components within a single management interface.

For example, an organization could configure a DLP enforcement policy that only allows U.S. social security numbers to be transmitted encrypted. The DLP technology will enforce that single policy throughout all components of data-in-motion, data-in-use and data-at-rest.

Even among vendors providing comprehensive coverage, few provide a single management interface through which to administer, set policy, run reports and manage incident workflow. Since many DLP solutions have been brought together under a single vendor via multiple acquisitions, some DLP offerings remain un-integrated, requiring administrators set policies through multiple interfaces. The result can be a very time-consuming process of manual policy duplication from one interface to another.

Still, some vendors claim integration in product marketing literature, even when this means simply that one interface makes a request of the other interface to display configuration settings or provide basic reporting. Actual DLP enforcement policy must still be done in separate interfaces, creating more costly administration overhead.
Cost Model

Cost is one of the most critical requirements for any organization considering new technologies and given the state of the world economy, cost is now an even greater consideration. If DLP solution costs do not match an organization’s reasonable budget parameters, there is little use in further considering technologies.

DLP enforcement technology cost structures can be as complex and varied as the underlying technologies themselves. Consider the following DLP sample pricing chart and the wide cost variance between sample Vendors A, B and C.

### DLP Sample Pricing

<table>
<thead>
<tr>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR A</td>
<td>$105,000</td>
<td>$16,000</td>
<td>$16,000</td>
<td>$16,000</td>
<td>$169,000</td>
</tr>
<tr>
<td>VENDOR B</td>
<td>$68,000</td>
<td>$55,000</td>
<td>$55,000</td>
<td>$55,000</td>
<td>$288,000</td>
</tr>
<tr>
<td>VENDOR C</td>
<td>$105,000</td>
<td>$65,000</td>
<td>$65,000</td>
<td>$65,000</td>
<td>$365,000</td>
</tr>
</tbody>
</table>

Sample pricing for 800 users is provided from three well-respected DLP vendors. Sample includes gateway, endpoint and discovery components. Hardware cost is estimated where appliances are not supplied. Sample supposes a single egress point for network coverage. Pricing is approximate and used for illustrative purposes. For an exact DLP vendor quotation, please contact DLP Experts.

A detailed breakdown of the pricing shows there to be three main reasons for cost variance: the number of components requiring separate license, licensing model and pure license cost.

### Number of Components Requiring Separate License

DLP vendors have differing approaches to licensing components within the solution. Some vendors employ an approach that adds significant license cost for each and every component. To see what kind of difference this can make, let’s refer to the following Licensed Components chart:
Vendor C charges a per-user license for no less than six separate components in our sample pricing: Network-Based Discovery, Endpoint Discovery, Endpoint Blocking, Network-Based Monitoring, Network-Based Blocking of Email and Network-Based Blocking of Web (Vendor C has even more licensed components that were not used in our pricing sample). Contrast this approach with Vendor A who charges for only three licenses: Network-Based Monitoring and Blocking, Endpoint Blocking and Discovery and Network-Based Discovery, which together provide the same coverage as Vendor C’s six licensed components.

Licensing Model

Most DLP solutions fall into one of two basic pricing models: perpetual license plus annual maintenance and annually-renewable subscription. DLP vendors typically use one license model; however, some vendors use both. (Vendor C allows buyers to choose the model they prefer. Our samples show Vendor C using their annually-renewable subscription model.)

The perpetual license model, as shown in our sample with Vendor A, typically carries a greater up-front cost, but provides long-term product ownership during the term of the license with an annual maintenance fee. Annually-renewable subscriptions, such as shown by Vendors B and C, may make for a more palatable initial purchase, but over the course of multiple contract years often result in a higher total cost of ownership.
PERPETUAL LICENSE VERSUS SUBSCRIPTION

<table>
<thead>
<tr>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR A</td>
<td>$105,000</td>
<td>$16,000</td>
<td>$16,000</td>
<td>$16,000</td>
<td>$169,000</td>
</tr>
<tr>
<td>VENDOR B</td>
<td>$68,000</td>
<td>$55,000</td>
<td>$55,000</td>
<td>$55,000</td>
<td>$288,000</td>
</tr>
<tr>
<td>VENDOR C</td>
<td>$105,000</td>
<td>$65,000</td>
<td>$65,000</td>
<td>$65,000</td>
<td>$365,000</td>
</tr>
</tbody>
</table>

Pure License Cost

Compounding the cost variances further are the straight per-user license costs. While it’s not possible to provide an apples-to-apples price comparison between vendors using different license models, we can still get an idea of actual annual license cost by averaging the total cost over a number of years. In the example below, note the license costs for endpoint coverage only (monitoring, blocking and discovery), and the dramatic annual per-user cost differential:

ANNUAL PER-USER LICENSE COST

<table>
<thead>
<tr>
<th>Year 1</th>
<th>Year 2</th>
<th>Year 3</th>
<th>Year 4</th>
<th>Year 5</th>
<th>Avg. Annual Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR A</td>
<td>$16</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
<td>$3</td>
</tr>
<tr>
<td>VENDOR B</td>
<td>$18</td>
<td>$18</td>
<td>$18</td>
<td>$18</td>
<td>$18</td>
</tr>
<tr>
<td>VENDOR C</td>
<td>$37</td>
<td>$37</td>
<td>$37</td>
<td>$37</td>
<td>$37</td>
</tr>
</tbody>
</table>

Average annual price per user over five years for a single user license of endpoint only coverage at 800-user price band. Pricing is approximate and used for illustrative purposes only. For an exact DLP vendor quotation, please contact DLP Experts.

This example of endpoint per-user license costs makes it abundantly clear just how widely pricing can vary from vendor to vendor. Similar variances can be found between vendors for other license costs; network-based monitoring and blocking, network-based discovery, etc.

Intangible Costs

A number of cost considerations exist in addition to license costs. As discussed previously, many traditional DLP solutions require multiple servers or appliances (i.e. one each for management, monitoring, blocking email, blocking web, etc.). This requirement is not always clear from reading vendor web sites, marketing literature— or even cost quotes. Still, intangible costs can be very significant.
• Personnel to manage and maintain multiple network devices
• Required Hardware
• Operating System or Database Licensing
• Operating System Maintenance and Updates

Many DLP vendors also may require expensive vendor-provided support in the form of professional services for installation, configuration and day-to-day DLP solution management. Conversely, a simplified architecture requires significantly less vendor support, saving on intangible costs.

When considering the total price of DLP technologies, be sure to get a complete overview of total costs. In particular, be sure to know both what components meet your requirements and exact costs for the following:

- **Licensing - Software Components**
  - Network-Based Discovery
  - Endpoint Discovery
  - Endpoint Blocking
  - Network-Based Monitoring
  - Network-Based Blocking of Email
  - Network-Based Blocking of Web
  - Network Protection

- **Licensing**
  - Pure License Cost

- **Hardware**
  - Appliances
  - Servers
  - Operating Systems
  - Maintenance Costs

- **Licensing Model**
  - Perpetual
  - Subscription

- **Vendor-Provided Support**
  - Professional Services
  - Installation/Configuration
  - Solution Management

**Conclusion**

Through a simplified, unified DLP architecture, a DLP enforcement solution can integrate all necessary components into a single, hardened appliance, thereby reducing the complexity and maintenance costs.

Using this unified DLP architecture results in a significant reduction in overall cost for hardware and accompanying maintenance. In addition to these cost savings, some vendors do not charge a license for each separate component, utilize a perpetual license model to provide a lower TCO and simply have lower license costs.

Data loss prevention enforcement solutions can be affordable and easy to install, configure and manage.
About the Author

Jared Thorkelson, Principal

Jared Thorkelson is a technology industry veteran and entrepreneur. Since cutting his teeth as a technical writer for IBM in the 80s, Jared has spent 18 years in executive-level roles with technology firms. Many of those years were spent as founder and president of a number of technology-related businesses, including, at the time, the largest facilities-based Internet service provider in San Diego.

His most recent experience includes over ten years in executive leadership roles with security firms, including an Internet security appliance manufacturer and a start-up DLP vendor, where he saw a business opportunity and developed a passion for the data loss prevention space.

Jared has a bachelor’s degree from Brigham Young University. He is a regular speaker, writer and contributor on the subject of Data Loss Prevention.

About DLP Experts

DLP Experts is a firm dedicated to providing unbiased assistance to companies considering the purchase and implementation of data loss prevention products. DLP Experts was founded by Jared Thorkelson after seeing firsthand the confusion of buyers of data loss prevention products. DLP Experts promotes the idea that data loss prevention is a process, not a singular product.

DLP Experts’ mission is to simplify the process of data protection for end users by providing the following services:

- Strategic consulting engagements for end users, including DLP enforcement technology selection, RFP management, DLP risk assessment, data protection planning and strategy, policy creation and internal promotion.

- Strategic consulting engagements for vendors, including product marketing and strategy, DLP competitive analysis and DLP technology review.

DLP Experts, LLC
DLPExperts.com
info@dlpexperts.com
+1 760.927.5000