DLPX
DATA LOSS PREVENTION EXPERTS

The Evolution of Data Loss Prevention: Reducing Complexity

A DLP Experts White Paper

Published August, 2010

Sponsored By

BlueCoat

Author's Note

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

Sponsored by Blue Coat Systems

Blue Coat Systems is the technology leader in Application Delivery Networking. Blue Coat offers an Application Delivery Network Infrastructure that provides the visibility, acceleration and security required to optimize and secure the flow of information to any user, on any network, anywhere. This application intelligence enables enterprises to tightly align network investments with business requirements, speed decision making and secure business applications for long-term competitive advantage. For additional information, please visit www.bluecoat.com.

Copyright Notice

Introduction

In recent years, organizations have come to recognize the critical importance of safeguarding sensitive information. This importance has been driven home by numerous high-profile data breaches resulting in regulations that mandate the security of sensitive data and the notification of impacted parties if personally identifiable information (PII) is compromised. Data Loss Prevention (DLP) technologies fill an important role in maintaining the security of sensitive data.

The technologies we know today as DLP have evolved significantly from their initial conception. Today's traditional DLP solutions are characterized by a single overriding factor that has impeded adoption: they are overtly complex to acquire, install, manage, and scale. This white paper reviews the evolution of DLP and compares traditional architectures with a relatively new and innovative architectural approach, the multi-function DLP appliance. With this white paper, we will show that DLP implementations can be simplified in terms of architectural complexity and the overall cost of ownership.

The Evolution of DLP

The genesis of what would eventually become the data loss prevention marketplace started with technologies designed not for preventing data loss, but for passively monitoring network activity. These solutions identified incidents of network misuse, allowing an organization to intervene and reduce non-business Internet activity. One early vendor website typified these solutions in their advertising: "No more employee surfing, shopping, day trading, sexual material, inappropriate emails... effectively ends all non-business activity…!"[1]

A convergence of consumer need and technological capacity gradually came into focus and helped drive the evolution of the data loss prevention marketplace. Increasing identity theft fears (among many other concurrent events) brought new consumer protection legislation and forced many organizations into a mindset of sensitive data protection. At the same time, soon-to-be DLP vendors were looking for a home for their solutions and recognized the application of their technologies as a way to address sensitive data protection needs. What would eventually be known as the Data Loss Prevention marketplace, was born.

As this marketplace began to come into focus, first-to-market technologies targeted those organizations most at risk for data loss and with the lowest risk tolerance–the world's largest heath care and financial enterprises.

New technical challenges also developed as definitions for sensitive data were expanded and data loss vectors were discovered beyond the network. Vendors were now tasked with addressing the "vectors" (email, web, malware) for potential for data loss and with data of varying types. The DLP evolution was in full stride.

[1] from eSniff website (also known as Vericept and acquired by Trustwave) from May 10, 2000 as cached from archive.org

The Component Explosion

Since early DLP technologies were developed for the largest enterprises in the world, vendors found it made sense to break out individual components in order to support large user bases, huge amounts of bandwidth and data flow while still using standard PC components. It also made sense as vendors developed new components to address the expanding needs of the marketplace.

The first widely-adopted technologies were developed as network-based monitoring software designed to detect sensitive data leaving the network. This monitoring software was installed on standard server hardware or in the case of some DLP vendors, the software was paired with an appliance. The solution passively monitored all outbound traffic via a network tap or mirrored port on a switch. These early solutions proved effective to identify serious incidents of sensitive data leakage.

As early adopters of DLP came to recognize the ramifications of sensitive data loss, the next logical step was to try to *prevent* the movement of this sensitive data before it left the protected confines of the network. DLP vendors responded to this market need by developing new software components that included mail transfer agent integrations for blocking email and web proxy integrations for blocking web, SSL and FTP traffic. With these and other new components on the DLP product roadmap, vendors had to decide on the best way to implement them. The majority of early DLP vendors chose to employ a modular architecture, which seemed to provide a number of key benefits, especially considering their current target market of the large enterprise.

A modular architecture would allow development teams to keep the monitoring software code intact instead of having to re-engineer it to add new functionality, such as blocking. DLP monitoring solutions had already been publicly released—essentially as what amounted to data loss detection—and were functioning to specification. In many cases, data monitoring solutions were producing revenue streams critical to the continued viability of early vendors and the evolution of the DLP marketplace.

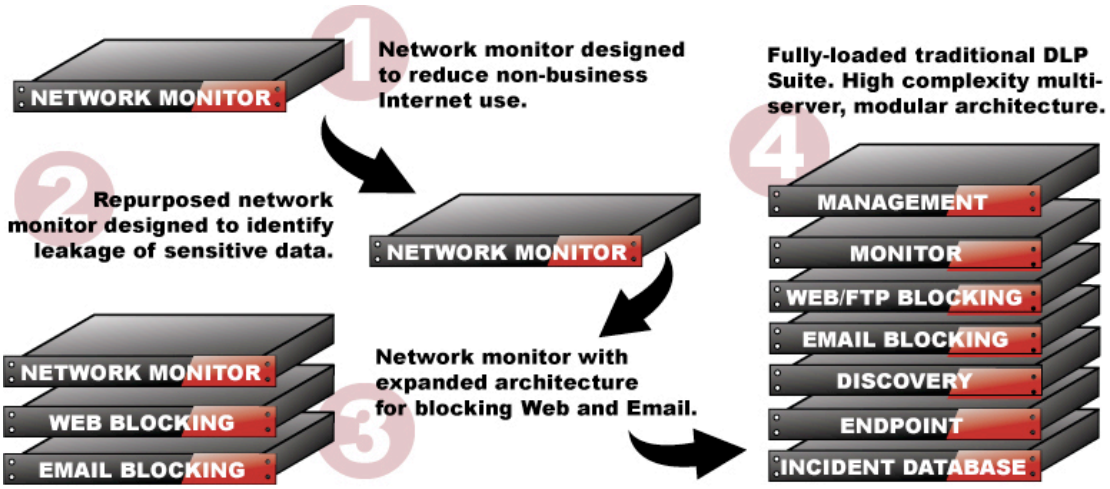
This modular architecture also allowed early adopters to test DLP cutting edge technologies one component at a time to suit their initial technical and budgetary requirements. And because early adopters also happened to be the world's largest enterprises, there was often a need to cover many separate egress points, which could be done at less expense with modular software.

One of the most important benefits to a modular architecture was that it kept the all-critical data detection component of passive monitoring unburdened by the processing requirements of other components. As with all passive monitoring devices, there is a danger of packets slipping by unseen on an overloaded server. In the case of protecting sensitive data, an overloaded server could allow that data to leak outside the protected network. Early DLP vendors quickly identified this limitation as critical to the overall success of their technologies—and their companies. A modular architecture allowed them to offload any additional processing requirements to servers running additional components, ensuring ongoing, effective detection of sensitive data.

DLP technologies continued to evolve with a modular, multi-server architecture at the core. One server/appliance each for separate components of the whole solution: management, monitoring, blocking email, blocking web, discovery, etc. Given the rapidly-changing DLP requirements and a customer base made up of the world's largest enterprises, it made sense for early DLP vendors to employ this modular, multi-server architecture.

With the significant financial outlays in legacy technologies and subsequent acquisitions by larger, public companies wanting to see quick returns, changing the architecture at this stage was out of the question for DLP vendors.

EVOLUTION OF DLP TECHNOLOGY



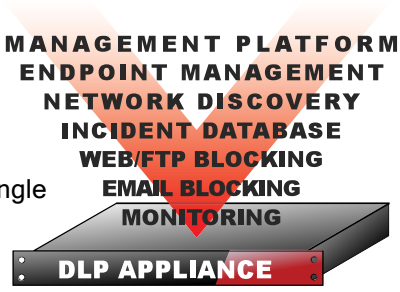
"Traditional" DLP

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.

Unified DLP Architecture – simplified.

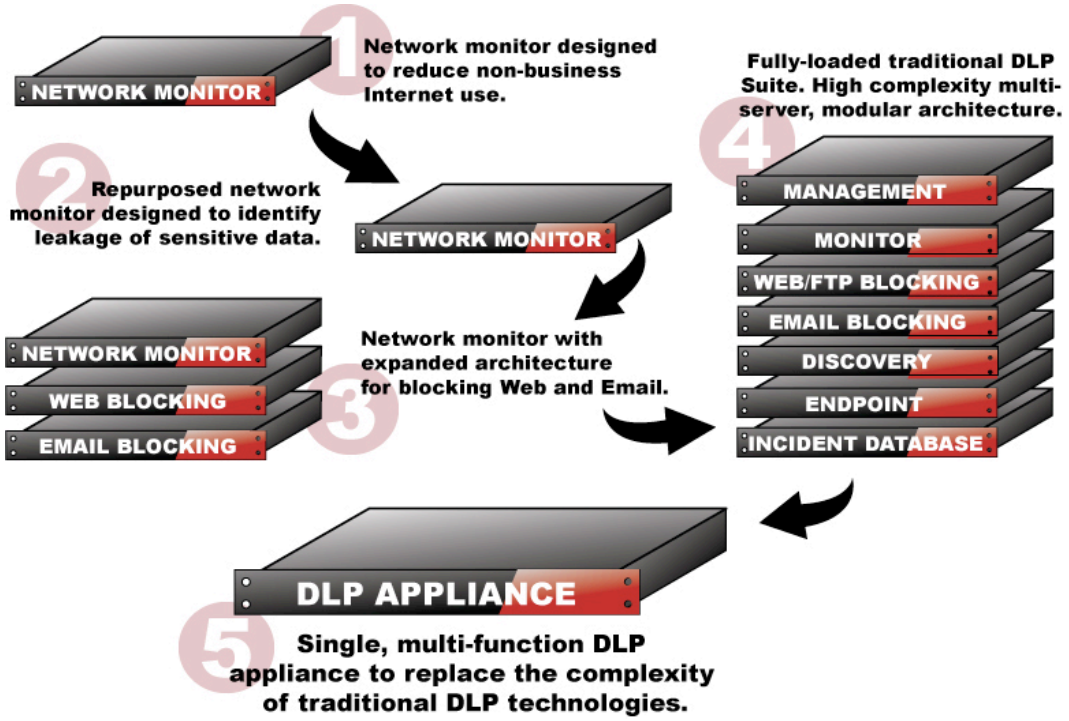


In contrast to the traditional, modular, multi-function DLP architecture, the ideal, simplified DLP solution combines all components into a single appliance, integrating with existing infrastructure such as mail and proxy solutions. Compared to the complicated architecture of a modular DLP approach, a single multi-function appliance can present a refreshing alternative for companies of all sizes, concerned with managing the complexities of a DLP solution.

The appliance approach has been well-accepted to address a host of network security concerns. Its application in the DLP world is no exception. An appliance to passively monitor all traffic, combined with email and web blocking integration, network-based discovery and endpoint management, provides a more simple and cost effective DLP solution in terms of deployment, operations, scalability and management. For smaller companies a single multi-function DLP appliance can handle all functions. For larger companies multi-function appliances can be flexibly specialized and distributed to remote offices at the flip of a software switch. Growing companies can benefit as well, quickly repurposing their appliances for email, web or data discovery at will.

The final evolution toward a simplified DLP solution cuts the complexity and architectural overhead to a much more manageable structure:

SIMPLIFIED DLP ARCHITECTURE



DLP Multi-Function Appliance Advantage

Multi-function DLP appliances provide significant advantages over modular, multi-server DLP architectures. Acquiring, installing, managing and scaling a single, multi-function appliance for DLP is simpler than the multi-server approach of most DLP vendors. Consider the following additional advantages:

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.

Lower Total Cost of Ownership (TCO). A single appliance-based DLP solution results in a lower TCO compared to a software solution which can require building multiple servers, installing operating systems and databases and acquiring licenses for each. Professional services associated with simplified appliance deployment and implementation can also be reduced significantly.

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. Centralized management of multiple appliances enables easy expansion to hundreds of thousands of users without additional operations overhead.

Ease of Acquisition. Acquiring appliance-based DLP technologies can be much easier than traditional solutions in that unified DLP architectures seldom require the purchase and deployment of additional hardware and often offer all-inclusive licensing.

Ease of Installation. Designed to be "plug and play," a single DLP appliance and can be racked and ready in a matter of minutes and easily integrate with existing infrastructure such as proxies for blocking. By combining the multiple components found in traditional DLP (management console, network monitors, incident database, etc.), there are fewer servers to integrate, leading to reduced deployment times and operational costs.

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.

Deployment Flexibility: A multi-function DLP appliance can be deployed more flexibly than a single-function system. This enables the security architect to utilize a single appliance in a small business environment and instantly re-purpose and specialize appliance use as the organization grows.

License. There are no license fees for a separate operating system, database or other installed software, just the DLP license itself. And as mentioned above, DLP appliance vendors often offer all-inclusive licensing.

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.

As with many markets early DLP vendors responded tactically to the evolving needs of the marketplace without the benefit of past experience or an architectural framework. To complicate matters further, many traditional DLP solutions grew through the acquisition of multiple, disparate DLP components that prevented effective cross-functional integration. This new generation of DLP technologies developed from the ground up, result in a more scalable and integrated approach to protecting data that are now more simple, effective and scalable.

Complete DLP Coverage in a Single Management 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.

While comprehensive coverage is important, many companies choose to deploy DLP technologies in a phased approach, often starting with network coverage. Network DLP casts a wide net to cover the major data leakage vectors of email and web. For compliance purposes a network DLP-led deployment can also show significant compliance progress with the most minimal cost and management overhead. Even more, with a multi-function appliance-based architecture, upgrading to discovery and endpoint within the unified DLP architecture is often done without adding any hardware.

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 loosely or 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. Again, the multi-function appliance architecture more often provides a single view integrated console that simplifies system and compliance management.

"New Generation" vendors, with their multi-function appliance capabilities and single management interfaces:

- Simplify policy creation and distribution through all communication channels (web, email)
- Similarly consolidate policy for data at rest, in motion and in use.
- Consolidate all of these components in an integrated management interface, greatly reducing operational costs.

License Models

DLP licensing structures can be as varied as the underlying technologies themselves, adding unnecessary confusion to an already complex purchase. These licensing variances can often lead to difficulty in comparing "apples to apples" between different DLP offerings.

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.

LICENSED COMPONENTS

<table>
<tr><th>VENDOR A</th><th>VENDOR B</th><th>VENDOR C</th></tr>
<tr><td>Network-Based Discovery</td><td>Network-Based Discovery</td><td>Network-Based Discovery</td></tr>
<tr><td rowspan="2">Endpoint Blocking and Discovery</td><td rowspan="2">Endpoint Blocking and Discovery</td><td>Endpoint Discovery</td></tr>
<tr><td>Endpoint Blocking</td></tr>
<tr><td rowspan="3">Network-Based Monitoring and Blocking</td><td>Network-Based Monitoring</td><td>Network-Based Monitoring</td></tr>
<tr><td rowspan="2">Network-Based Blocking</td><td>Network-Based Blocking of Email</td></tr>
<tr><td>Network-Based Blocking of Web</td></tr>
</table>

Vendor C charges a per-user license for no less than six separate components in our sample: 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 this 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.

Multi-purpose DLP appliances utilize a unified architecture that can provide a more simple licensing structure, as shown with Vendor A. Instead of licensing each available DLP component, a multi-purpose appliance often requires fewer licensed components. Also beneficial is the fact that each component can be implemented via the user interface without having to deploy additional servers.

Total Cost of Ownership

There are various Total Cost of Ownership (TCO) issues to be considered with DLP technologies. 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, it's important to consider all relevant components that make up total cost:

- Personnel to manage and maintain multiple network devices
- Required Hardware
- Professional Services

- Operating System or Database Licensing
- Operating System Maintenance and Updates

Special attention should be paid to those DLP solutions that require expensive vendor-provided support in the form of professional services for installation, configuration and ongoing system management. The simplified multi-functional appliance architecture requires significantly less vendor support, saving ongoing costs that can double or even triple actual costs.

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

- **Licensing - Software Components**
  - Network-Based Monitoring
  - Network-Based Blocking of Email (encrypted and non-encrypted)
  - Network-Based Protection
  - Network-Based Blocking of Web (unencrypted and SSL)
  - Network-Based Discovery
  - Endpoint Discovery
  - Endpoint Blocking
- **Licensing Model**
  - Perpetual
  - Subscription
- **Hardware**
  - Appliances
  - Servers
  - Operating System Licensing
  - Database Licensing
  - Maintenance Costs
- **Vendor-Provided Support**
  - Professional Services
  - Installation/Configuration
  - Solution Management

Conclusion

The evolution of DLP technologies has come full circle from simple, low-value data loss detection to highly-complex, multi-server architectures and finally evolving to multi-function appliances within a unified DLP architecture that provide comprehensive data loss prevention.

Leveraging a simplified, unified architecture, prospective buyers can integrate all necessary DLP components into a single, hardened multi-function appliance, thereby reducing complexity and cost of the overall solution. 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 vendor offerings provide a lower TCO by using a more reasonable license model and reducing the cost impacts of professional services.

Solutions utilizing a unified DLP architecture have broken the mold of traditional DLP and represent technologies that are not only affordable but also easy enough to acquire, install, configure and manage for almost any organization complying with regulations or protecting their valuable data.

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