Data Loss Prevention Leading Vendor Review

A DLP Experts White Paper

Version 7.4 – Updated November 2016

Author's Note

The content of this white paper was developed independently of any vendor sponsors. The views and opinions in this paper represent the sole work of DLP Experts.

Copyright Notice

DLPX
DATA LOSS PREVENTION EXPERTS

Introduction

This work is the culmination of over eight years exclusive focus on Data Loss Prevention technologies and the DLP marketplace at large. The purpose of the DLP Vendor Review is to provide the reader with an overview of select Data Loss Prevention (DLP) vendor technologies. For the sake of expediency, this document does not attempt to examine all DLP vendors in the marketplace, rather a cross section of those vendors that represent leading enterprise DLP suites or that offer some unique approach to DLP. *This review covers only solutions that provide comprehensive DLP coverage.*

DLP Market Changes

For a number of years, the DLP marketplace remained very quiet with little movement – no significant emerging vendors, no major vendors leaving the space and no notable market consolidation. That has changed over the past 18 months and an explanation of these changes is important to understanding the content and approach of this review.

- **RSA quietly posted the End of Primary Support for their DLP solution.** While the company has issued no official statements on the future of its DLP offering, rumors abound and include the possibility of some DLP elements being rolled into RSA's Security Analytics platform. The fact remains, however, that the RSA DLP product as we know it is no longer being developed. RSA has confirmed the DLP solution is not being sold to new customers. Many current RSA DLP customers are now considering other DLP solutions.

- Long-standing DLP solution **Verdasys made significant changes** in order to become more relevant in the DLP space. The company named an information security veteran as its CEO, took on additional funding, changed the company name to Digital Guardian (its long-time product name), applied substantial funding to development, committed to the reseller channel and made a number of strategic acquisitions. In December, the company announced an additional $66 million in funding.

- In October, **Digital Guardian announced the acquisition of enterprise DLP vendor, Code Green Networks**. This acquisition brings network gateway and discovery capability, along with enhanced data detection methods that will enable Digital Guardian to compete outside its prior focus of intellectual property protection. While Code Green is now part of Digital Guardian, the products will continue to be marketed separately until there is some integration across the two solutions. For this reason, the product reviews will remain separate.

- **Raytheon completed its acquisition of Websense last May,** resulting in a Raytheon/Vista Equity Partners joint venture recently unveiled as **Forcepoint**. One of the most significant benefits to this joint venture has been access to Websense's commercial sales channels, which Raytheon saw as critical to competing in the commercial space. In addition to combining the Websense and Raytheon product lines, Forcepoint has also recently acquired the next-generation firewall products from McAfee. While this acquisition may not directly impact the data loss prevention marketplace, it puts Forcepoint in a stronger position as a security vendor.

DLP Vendors Included

As a result of recent changes in the data loss prevention market landscape, RSA has been dropped from this review, Digital Guardian has been added, a new section comparing DLP approaches has been included. The remaining DLP vendor solutions included in the review (in alphabetical order):

- Digital Guardian (reviewed separately as Code Green Networks and Digital Guardian)
- McAfee Total Protection for Data Loss Prevention
- Symantec Data Loss Prevention
- Forcepoint TRITON APX (newly-formed Websense/Raytheon joint venture)

What is DLP?

Data Loss Prevention means different things to different people. For purposes of this review, the terms "data loss prevention" and "DLP" refer to systems that detect and protect sensitive data – in motion, at rest and in use – using advanced content analysis techniques and from within a single management console.

It's not uncommon to find the term *data loss prevention* or *DLP* attached to products found in a neighborhood office supply store, such as power strips, privacy filters, remote data destruction, backup and recovery technologies and USB storage devices. In fact, at the 2015 RSA Conference, out of more than 500 exhibitors, roughly 140 used the term *data loss prevention* to describe their products or services in some way. Those companies included a password manager, a mobile phone manufacturer, a major telecommunications provider and the NSA. (By contrast, only 40 companies identified themselves using the term *anti-spam*.)

This demonstrates two things: 1) Basic data loss prevention capabilities have been added to many non-DLP technologies, and 2) Many companies simply want to align themselves with the term *data loss prevention*. It's not surprising that many vendors want to take advantage of the high visibility of recent data breaches as a means to attract attention to their products and services. The unfortunate result of all this, however, is that many organizations are misdirected away from more focused and DLP-specific technologies. Inadequate solutions are often considered to address the problem of data leakage, not realizing the solutions leave gaping holes through which data can be lost.

Generally speaking, there are two levels of DLP technologies: Full Suite (Enterprise) DLP and Channel DLP. Full Suite DLP technologies are focused exclusively on the task of preventing sensitive data loss and provide comprehensive coverage, while Channel DLP solutions provide a more limited DLP feature set amid a long list of non-DLP features.

Full Suite DLP

Coverage

Most Full Suite DLP solutions were purpose-built with the idea of data loss prevention in mind and include comprehensive coverage for maximum effectiveness. These solutions provide coverage across the complete spectrum of leakage vectors: data moving through the network gateway or *data in motion*, stored data on servers and workstations or *data at rest*, and data at the workstation/endpoint level or *data in use*. Equally as important, Full Suite DLP solutions address the full range of network protocols, including email, HTTP, HTTPS, FTP and other TCP traffic.

Detection Methodologies

Another critical distinction of most Full Suite DLP solutions is in the depth and breadth of sensitive data detection methodologies. The earliest DLP technologies relied exclusively on pattern matching of text strings – looking for patterns that matched account numbers, certain phrases or a dictionary of related words. These early detection methodologies detect very specific patterns, but are often false positive prone. Over time, enterprise DLP solutions have introduced a number of new detection methodologies, providing meaningful increases to DLP effectiveness.

One critical detection methodology, data fingerprinting, is now common across many leading Full Suite DLP vendors. The fingerprinting process can be used on databases (structured data) and documents (unstructured data) by initially creating and storing a one-way hash on the DLP system. The DLP solution then analyzes content, compares it with the stored hashes and returns an incident if there is a match. The result is highly accurate identification of sensitive database content, such as a last name and account number as well as exact or partial matches of documents.

Central Management Console

Another unique and critical feature of Full Suite DLP solutions is a central management console for configuring coverage across data in motion, data at rest and data in use, creating and managing policies, reporting and incident workflow. This eliminates the need for multiple management interfaces and significantly reduces the management overhead of a comprehensive DLP initiative.

Channel DLP

By definition, Channel DLP solutions were designed for some function other than DLP but were modified in order to add some DLP functionality. Common Channel DLP offerings include email security solutions, device control software and secure web gateways.

In each case, Channel DLP solutions are limited both in their coverage and detection methodologies. For example, many email security vendors – both on-premise and cloud-based – have the ability to scan email content for sensitive data. In most cases, however, detection methodologies are limited to pattern matching across email, while content in other widely-used network protocols leaves the network without any inspection whatsoever.

Technological Approaches to DLP

The recent addition of vendors to this document necessitates an explanation of core differences between various DLP approaches. For our purposes and for simplicity's sake, we have separated vendors into two groups: Traditional DLP (TDLP) and Non-Traditional DLP.

The vendors that comprise the TDLP solution group include Code Green Networks, McAfee, Symantec and Websense. While certainly not identical, each of these TDLP vendors supports what has become the generally accepted and market leading, three-pronged DLP approach: coverage at the network gateway, in storage and at the endpoint. This three-pronged approach was the first to garner significant market share and has helped shape today's DLP market. For these reasons we have chosen to group these vendors together under the TDLP label.

Only one vendor is represented in the Non-Traditional DLP group: Digital Guardian (DG). While DG's recent acquisition of Code Green Networks (CGN) could be seen as bringing DG into the TDLP fold, the reality is that the solutions are still sold separately for the foreseeable future. Currently, DG is the only viable DLP solution that does *not* support the traditional three-pronged DLP approach as described above. DG comes at the problem of data loss prevention in its own unique way. Over many years and by design, the company has avoided more conventional DLP technological approaches, effectively separating itself from TDLP products. In this respect the company has chosen to challenge the entire marketplace.

Because DG stands alone in the Non-Traditional group, we will reference that group simply as *DG*. Noting the main differences between Traditional and Non-Traditional DLP at this point will provide a foundation to better understand the capabilities of each of the vendors included in this review.

Context vs. Content

One major difference between DG and TDLP solutions is its emphasis on ***context over content***. Generally speaking, TDLP solutions do the converse: they put ***content over context***. One important note: all DLP vendors included in this review use both content and context in detecting and protecting sensitive data. The difference is in which element – content or context – is given more weight in the detection process.

A TDLP ***content-based*** approach might focus on the elements of sensitive data (the content) – such as a social security number and last name – and then use context – such as source and destination – to help improve accuracy.

By contrast, the DG ***context-based*** approach might focus on a combination of many contextual elements – such as a computer and user, a file accessed from a particular network share, an application and a network operation – and then add the element of content – such as a social security number – to help improve accuracy.

As might be expected, DG provides many more contextual data points than do TDLP solutions. Conversely, the TDLP vendors' *content over context* approach offers more content detection methods than does DG. The question that remains unanswered is whether the different approaches are able to achieve comparable levels of accuracy.

While each vendor will certainly contend that their approach is more accurate, only comprehensive vendor testing – in a customer environment with the customer's actual data – is likely to prove out vendor claims. Such testing will likely find one DLP approach better than others for an organization's unique requirements and data types.

Content Detection: Fingerprinting vs. Regular Expressions

The next major point of differentiation between TDLP and DG is in content detection methodologies. TDLP solutions provide many methods for identifying sensitive content. These methods can be layered and combined with contextual data points to improve detection accuracy. General categories of content detection methods include:

- **Regular Expression Pattern Matching.** The most basic of all content detection methods and widely used across technologies for protecting data. Regular expressions (or regex) can be written to identify common patterns for words, numbers or phrases.

- **Statistical Analysis.** Uses a number of statistical techniques (machine learning, Bayesian analysis) to analyze textual content.

- **Fingerprinting.** The process of creating a one-way hash of known sensitive content – individual database fields, complete or partial documents – which the DLP solution uses to monitor data for matches.

TDLP solutions leverage all available methods of content detection, whereas DG makes use of only regular expressions.

Regardless of methodologies, each technological approach has merit. The question of which approach will be more effective in detecting sensitive data in an organization's unique environment will need to be tested and confirmed.

Research Recommendations

DLP Experts is an organization focused exclusively on data loss prevention technologies. As such, our preference is almost always for the comprehensive protection offered only by enterprise DLP suites and including coverage for network, endpoint and discovery.

In more than eight years dedicated exclusively to the DLP space, we have not encountered a single instance where an organization was best served by limiting DLP coverage to one area. Comprehensive coverage in a layered approach to data protection is always better than less coverage. Key areas of protection may need to be addressed first and budgets may limit options, but as long as data needs to be protected, the need for comprehensive coverage will remain.

No One-Size-Fits-All Approach to DLP

It is important to note that as much as vendors promote their products as being the best solution for every data loss prevention need, there is no one-size-fits-all approach. Requirements differ from organization to organization based on many factors: number of users, number of endpoints, number of egress points, network architecture, technology budget, personnel resources, sensitive data types, etc.

In most every call for DLP, there will be DLP vendors that are better suited to specific requirements than others. It pays to research the DLP marketplace for a solution that best meets your organization's specific requirements.

The Vendor-Agnostic Approach of DLP Experts

This is precisely the reason DLP Experts is in business. As a vendor-agnostic reseller of leading DLP solutions, we face each customer DLP project as unique and bring no pre-conceived ideas with us. We bring only eight years of exclusive DLP experience. Our approach is to first understand specific requirements, unique environments and data types, and then match vendor capabilities to those requirements. We are able to bring any or all vendors to the table.

What sets DLP Experts apart from other resellers is the fact that we go one step further: Unlike the vendors and their traditional resellers, DLP Experts discloses all relevant vendor information – ***the good, the bad, and the ugly*** – giving organizations a truly unbiased view of the DLP market landscape.

DLP Experts' unique approach enables buyers of DLP technologies to go into the purchasing process with their eyes wide open and aware of not just the upside, but also the downside of every DLP technology under consideration.

Vendor Reviews

In the remaining pages, we will discuss the individual vendors and their DLP solutions.

Code Green Networks

Company Overview

Digital Guardian acquired Code Green Networks (CGN) in September 2015, bringing together the last two independent providers of comprehensive data loss prevention solutions. CGN was started in 2004 by the founders of SonicWALL (SNWL) to bring a new, streamlined architectural approach to the data loss prevention marketplace. The company's product offering has been focused exclusively on preventing the loss of sensitive data.

Product Overview – Code Green Networks TrueDLP

The CGN TrueDLP solution is designed to reduce the complexity traditionally associated with data loss prevention technologies by employing a single appliance approach. A single appliance – either virtual or hard – supports all DLP software components, including the following:

- Web-based management console
- Incident database
- Passive monitoring for data in motion (email, web and generic TCP)
- Blocking for email
- Blocking for HTTP, FTP and HTTPS
- Network-based discovery
- Endpoint-based discovery
- Endpoint monitoring and blocking

A single appliance is deployed at each Internet egress point and additional appliances can be added for high availability. The solution requires no additional software components.

Like the other TDLP solutions in this review, the CGN DLP solution integrates with an ICAP-capable proxy for blocking of HTTP, HTTPS and FTP, and existing email infrastructure to provide quarantine and blocking for email. Other common integrations provide for routing sensitive email through encryption solutions as well as an organization's Active Directory structure.

Pros and Cons – Code Green Networks TrueDLP

Simplicity is one major benefit of the CGN DLP solution. The solution meets the most common and core DLP requirements, especially in organizations with heavy structured data requirements, such as consumer personally-identifiable information (PII) or protected health information (PHI). The CGN single appliance approach has been very well received, especially across the small to medium enterprise marketplace. Although CGN would argue that the company's successful implementation across enterprises with as many as 80,000 users proves the product in the large enterprise.

Implementation is greatly simplified by the CGN single appliance approach, with average deployment times much shorter than other products that require 100- to 200-hour professional services engagements. Because implementations require no additional servers/software, Windows software or virtual machines, implementations can often be completed in a single day, with only minimal policy tuning required thereafter.

Organizations heavily invested in the virtual appliance approach will be glad to know that CGN can provide a fully-virtualized implementation. For monitoring and DLP at the network gateway, most vendors require at least one server or appliance per egress point to address the unique challenges related to effective packet sniffing. CGN allows a virtual appliance with a physical NIC to be used for Network DLP.

To simplify the phased implementations common with many DLP projects, the CGN solution is upgraded simply via the management console. No additional servers, software, VMs or complex configurations are required. This significantly reduces future professional service requirements.

From a feature standpoint, while CGN meets most core requirements for network and discovery DLP, organizations with very specific endpoint DLP needs should review CGN features to confirm capabilities. Historically the CGN Endpoint DLP agent has lacked OS X and Linux support as well as features such as network monitoring for email and web, and blocking of print and copy/paste functions. However, with the CGN acquisition and DG's own highly regarded endpoint agent, it's possible that full-featured endpoint agents covering Windows, OS X and Linux could be added to the near-term roadmap.

Pricing – Code Green Networks TrueDLP

The Code Green DLP solution has long been the most aggressively priced of major DLP solutions, however, cost models may change with the recent acquisition. CGN solution costs include only three licenses required for full suite implementation, plus any appliance costs (no cost in the case of the virtual appliance option). In most situations, the total cost has been far less than the rest of the marketplace. The company uses a perpetual license model requiring annual support and maintenance of 18% of the cost of licenses and any hardware.

Professional deployment service costs are charged by the day, with expenses not included. Given CGN's simple architectural approach, deployment costs are generally counted in hours, rather than weeks, making it a fraction of the cost of more complex DLP solutions.

Final Word – Code Green Networks TrueDLP

There's no two ways about it; DLP solutions are complex and expensive. However, CGN is the vendor that has done the most to effectively address that complexity and high cost. The unique CGN single-appliance architecture is a good fit for organizations with tight DLP budgets, with limited personnel resources that can't support solutions with high management overhead. Companies that need to protect consumer personally-identifiable information (PII), such as financial information or protected health information (PHI) to support HIPAA compliance, will find the CGN solution meets core requirements.

For organizations with an endpoint DLP focus, the current CGN offering is not as full-featured as many of its competitors. On the flipside, the CGN endpoint agent is much lighter and unobtrusive to the end user than other, more feature-rich endpoint DLP solutions.

Digital Guardian

Company Overview

Digital Guardian (DG), formerly known as Verdasys, is a venture-funded software vendor of data loss prevention solutions. The company was founded in 2003 and until its recent acquisition of Code Green Networks, was one of only two remaining independent providers of comprehensive data loss prevention. The company also stands alone as the only product in this review to be included in the *Non-Traditional DLP* category.

Product Overview – Digital Guardian

The DG DLP solution is an endpoint agent residing at the kernel level. This allows for deep visibility into system events but must balance that benefit without compromising the OS. From a purely technical standpoint, DG represents a radical shift from the major DLP vendors, even considering the CGN acquisition and the expected addition of network and discovery DLP coverage. Architecturally, the solution is very simple: endpoint agents covering Windows, OS X and Linux, which communicate with a central management server.

Unique Product Capabilities

User and System Events. One of the unique benefits of the Digital Guardian solution comes from it residing at the kernel level. The solution automatically monitors and logs all endpoint activity, even without defined policies. That means even without any policy configuration, many instances of sensitive data misuse can be identified. Based on findings in monitor only mode, policies can be enacted to enforce data protection.

Network DLP Coverage. Unlike TDLP, DG's network coverage is achieved by monitoring all network communication *before it leaves the endpoint*. This approach is not inconsistent with other leading TDLP solutions, many of which can also monitor some network activity at the endpoint. However, the current DG approach does not employ network DLP coverage at the gateway. (This may change with the CGN acquisition.)

DG's endpoint-based network coverage does have its distinct advantages, including the ability to block across *all protocols*. TDLP network DLP coverage is limited to proxiable protocols supported by secure web gateways via ICAP. This generally includes HTTP, HTTPS, FTP and some instant messaging platforms.

Discovery (Stored Data) DLP Coverage. Like Traditional DLP solutions, the DG endpoint agent has the ability to scan local file systems for sensitive data. However, when it comes to network-based storage, DG's capabilities are limited to servers upon which the agent can be deployed. If an agent *can* be installed on a server, then that local data *can* be scanned. If an agent *cannot* be installed, then that local data *cannot* be scanned.

File Tagging

While still actively used by only one other TDLP vendor, file tagging is often seen as an antiquated and ineffective approach because it requires input from fallible end users to apply document classifications. Digital Guardian relies heavily on file classification and "tagging," however, the process is automated and does not require user input. The classification process, which adds metadata tags to files, provides a good starting point for policies. Tags can be applied based on any number of criteria, including automatic classification depending on where a file came from. For example, a CSV extract from a database containing sensitive data can automatically and permanently be tagged as "confidential."

Pros and Cons – Digital Guardian

The Digital Guardian solution brings a high level of visibility to user actions and data handling. This increased *context awareness* can help companies find ways to improve data protection that otherwise may have gone unnoticed. This context awareness can also call attention to other problems within a protected network. Anomalous user behavior can be identified and may indicate a more serious cyber security problem, such as malicious outsiders living within an otherwise protected network.

DG employs a simple architecture, covering Windows, OS X and Linux, with no network integrations required. The solution can actively see and block sensitive data within SMTP, HTTP, HTTPS, FTP and other network protocols without an ICAP-compatible proxy or email integration. This is especially helpful for companies that do not have budget to add a proxy or simply prefer a proxy-free environment. The architecture reduces the need for a network monitoring device at each egress point, which can drive up hardware costs, increase architectural complexity and ongoing management.

DG's limited content detection methods and current lack of fingerprinting capability could significantly reduce its appeal for organizations with compliance requirements to protect consumer or patient confidential information. Limited discovery coverage may also be a concern for DLP buyers. That said, with the recent acquisition of Code Green Networks, these deficiencies are likely to be addressed over the next 12-24 months.

Pricing – Digital Guardian

DG licenses three main solutions. The base offering is Data Visibility and Control (DV&C), providing out-of-the-box visibility into all system and user activity with no policy configuration. Two additional solutions can be added on top of DV&C: DLP and ATP (Advanced Threat Protection). A number of add-on modules are also available offering capabilities such as encryption and enhanced forensics.

The DG solution is available as an on-premise perpetual license, as a managed service or as a hybrid of the two. First year on-premise, perpetual license costs are priced per endpoint, with added cost for the management console, initial setup (currently performed only by DG) and required training. There are also annual support charges for each endpoint license and management console.

The DG managed service has been well received as a cost-effective alternative for organizations that want to leave on-going solution management to DG's experts. The managed service is based on a monthly, per-endpoint cost, plus initial setup and required training. There are three flavors of managed service with the lowest providing user visibility but no DLP content scanning. The next step up includes DLP and the high-end managed service provides higher service levels.

Final Word – Digital Guardian

The DG solution is a solid option especially in its proven marketplace of protecting intellectual property or for organizations that have specific endpoint DLP needs. DG's visibility into all system and user events is a key feature that separates them from the pack. TDLP solutions only find what specific policies call for – if there is no policy looking for *xyz*, then *xyz* will not be found. DG is able to uncover incidents that otherwise would be impossible to find.

Organizations with specific compliance requirements to protect personally-identifiable information (PII), such as banking and healthcare, may find a traditional fingerprinting approach more precise. However DG's automated classification and tagging capability may provide benefits in different areas.

Future roadmap plans for integrating DG and Code Green Networks will have a significant impact on DG's near term success. However, once integrations are largely complete, we expect DG to be even more competitive than it is now.

McAfee

Company Overview

Intel completed the acquisition of security leader, McAfee, in 2011, becoming part of Intel Security. McAfee has revenue of over $2 billion and over 7,000 employees. McAfee entered the DLP space in 2006 with its acquisition of endpoint DLP player Onigma, but didn't gain full momentum until its 2008 acquisition of Reconnex, then a leader in the area of Network DLP. The company has now integrated significant portions of its DLP offering into its highly-regarded management platform, ePolicy Orchestrator (ePO).

Product Overview – McAfee Total Protection for Data Loss Prevention

Smaller companies considering McAfee DLP should note that there are two McAfee offerings marketed under the Data Protection category: 1) *McAfee Total Protection for Data* and 2) *McAfee Total Protection for Data Loss Prevention*. It is important to note that the *Total Protection for Data* offering includes only an endpoint agent and does not represent the full DLP functionality of the *McAfee Total Protection for Data Loss Prevention*. It's not uncommon for smaller organizations to be directed by McAfee to the lower cost endpoint-only offering.

McAfee Total Protection for Data Loss Prevention ("McAfee DLP" for our purposes) employs an appliance (or virtual appliance) approach, with four components. At the core, DLP Monitor watches and captures network traffic. DLP Discover scans network systems and databases, while DLP Prevent provides for the network blocking capability of the solution. The fourth component, DLP Manager, brings it all together by accepting all input from the appliances, providing the management interface and communicating with ePO.

The McAfee DLP Endpoint solution is managed via ePO, however some aspects of the DLP suite remain under the control of the DLP Manager appliance, resulting in two touch points to manage the complete solution.

The McAfee DLP Monitor component is unique among DLP offerings, allowing the capture of not only data from incidents triggered by policy violations, but potentially *all* network traffic. This allows review of data that does not meet existing rule sets, uncovering incidents or violations that otherwise may have gone unnoticed. Policies can also be edited or fine-tuned and then run against this captured data, providing a historical view of how policy changes would have impacted incident results.

McAfee DLP integrates via its Prevent appliance with an existing ICAP-capable proxy for blocking of HTTP, HTTPS and FTP, and existing email infrastructure to provide for email remediation. The solution can also be integrated with email encryption solutions and Active Directory.

Pros and Cons – McAfee DLP

The McAfee DLP solution is most often acquired based on two major strengths: the unique DLP Monitor approach and the integration with ePO, which is used by nearly all McAfee enterprise customers. For current customers, the McAfee DLP solution is often a good choice, especially when McAfee sees the ability to bolster its position within its user base. The McAfee DLP Endpoint solution provides stand-alone functionality as an entry-level DLP offering for smaller companies or those looking to grow into DLP.

McAfee DLP Manager is currently required to support certain management functions, in addition to ePO for DLP Endpoint. Having these two touch points is not ideal and adds more management overhead to some administrative tasks. Internal McAfee sources have recently reiterated the product roadmap includes moving full management of the DLP suite to ePO, thus doing away with the DLP Manager. But, this has been discussed since the Reconnex acquisition in 2008 and to-date remains unconfirmed.

Since the Intel acquisition, McAfee DLP has seen very few product updates. The most recent full release (version 9.0) was made available in late 2010, with the most recent point release (9.4) coming four-and-a-half years later.

Pricing – McAfee DLP

Like all DLP solutions, McAfee DLP can be a costly proposition. However, this is especially true when appliances are required and even more so with multiple egress points that may need more than a single DLP appliance. Virtual appliances can lessen that cost, but, at a minimum, the DLP Manager appliance will always be required if deploying all DLP components.

The pricing model is based on a perpetual license with a 20% annual cost for Gold Software Support. Professional Services are required for all new DLP purchases and vary based on the DLP components selected. Generally, most organizations should expect to incur a minimum of 100 professional services hours to as many as 200 for full DLP deployment.

Final Word – McAfee DLP

The McAfee DLP solution is most likely to be selected by existing McAfee customers firmly entrenched in and committed to ePolicy Orchestrator. McAfee is known to promote the DLP solution to its existing customer base very aggressively with hard-to-resist, competitive pricing packages. Like some other DLP vendors, McAfee has a very lucrative installed base of other products that it must protect from replacement – and McAfee DLP is often used as an incentive to remain committed to these other products. Current McAfee customers should attempt to leverage this to the extent possible for increased savings.

From a purely technological standpoint, the unique data-capture approach of the McAfee DLP Monitor component certainly represents the single biggest technological differentiator among leading DLP solutions. However, this unique component may not be enough to sway buyers from other DLP solutions, as evidenced by the continued growth of McAfee's DLP competitors.

While McAfee was one of the first major vendors to jump into the DLP space by acquisition in 2006, it took the company a number of years to acquire and integrate the different parts of its enterprise DLP offering. Other vendors took advantage of that downtime, stealing critical momentum that McAfee has been unable to regain in the last few years. More recently, with the acquisition of McAfee by Intel, the momentum of the DLP offering has slowed further, causing many in the space to question Intel's commitment to the product.

Symantec

Company Overview

Symantec has grown to become the leading provider of DLP in the market. In 2007, Symantec acquired Vontu, the then-current DLP market leader for $350 million. Symantec did not rest on its Vontu laurels, however, and continued to transform the DLP marketplace, bringing to light many of the major innovations in the space. Today the Symantec DLP offering continues to be the undisputed leader.

Product Overview – Symantec DLP

Symantec DLP is the proverbial 800-pound gorilla of the DLP space. Symantec boasts the largest DLP install base and ongoing revenue of any DLP vendors. Most estimates put the Symantec DLP market share anywhere from two- to three-times the next closest competitor. The product is considered to be the most feature rich of any DLP offering and often is the bar against which all other DLP products are measured.

The solution is unlike any of the offerings previously reviewed. The Symantec DLP approach is decidedly software; no true appliance option is available, although some Symantec DLP resellers will package and deliver hardware and software together. A different software – and license – is required for most Symantec DLP components, however the DLP suite can be purchased at a single, discounted price:

- Enforce Platform (management platform – separate license not required)
- Network Monitor
- Network Prevent for Email
- Network Prevent for Web
- Network Discover
- Network Protect
- Endpoint Prevent
- Endpoint Discover
- Data Insight (included in DLP Suite)
- Data Insight Self-Service Portal (add-on)
- Oracle Standard Edition One

Most every software component can be installed on Windows, Red Hat Enterprise Linux or as a virtual machine – and it's okay to mix and match.

Like the other solutions, the passive Network Monitor is connected via a SPAN port or network tap. In order to block web or email, Network Prevent works with existing email infrastructure and ICAP-capable proxies. Symantec DLP supports integration with various other technologies, including email encryption and Active Directory.

Pros and Cons – Symantec DLP

Because of its extensive feature lists, Symantec DLP almost always makes the cut when considered for DLP project requirements and matching vendor capabilities. Its features are not limited to any single component of DLP; they are universally strong, making it a solid choice across Network, Discovery and Endpoint.

One unique advantage of the Symantec DLP solution is the inclusion of Data Insight in the DLP suite. Data Insight provides visibility into unstructured data usage, ownership and access permissions. This product competes directly with solutions outside the DLP space and can represent a good value for organizations looking for this additional capability. No other DLP vendor provides this type of solution.

On the downside, Symantec DLP is generally considered to be the most complex of the available DLP solutions, with more individual software components that must be installed and configured. This limits the appeal among many smaller sized organizations that do not have the resources of larger enterprises. Symantec's DLP solution also requires the use of a separate instance of Oracle Standard Edition One. For non-Oracle shops, this can prove to be intimidating and become a management headache.

The company has made attempts to streamline the separate components by leveraging virtual machine environments. This has helped somewhat to position Symantec DLP for smaller organizations. In some cases, multiple components may be installed on a single server, making for a more streamlined approach. But this ability is dependent on the size of the organization and hardware configuration, among other things. It's important to keep in mind that there are limitations to running certain components as virtual machines – not all components are suited to such virtual environments. In the end, each component, whether VM or server/software, still represents another moving part in the overall solution.

Pricing – Symantec DLP

Symantec DLP cost is based upon a per-user, perpetual license model, although an annually-renewable subscription is sometimes available upon request. In addition to the perpetual license, there is an annual maintenance cost of 23%. The complete Symantec DLP solution is offered as a suite and at significantly reduced pricing. While individual components can be selected from the many offered, the DLP Suite represents the best value for Symantec DLP.

Symantec DLP has the dubious distinction of being the most expensive solution in the market, from a pure license cost standpoint. Of course, there are other costs besides software licensing and these must be considered, as well. Since Symantec DLP is a software solution, no hardware costs are priced directly by Symantec. Any such costs will depend on the hardware requirements for the specific implementation plan. A handful of Symantec VARs provide bundled DLP hardware offerings to simplify the process.

Like other DLP solutions, professional installation services are required and can represent a significant overall cost to the DLP project. Buyers of Symantec DLP should expect a minimum of 100 hours for more basic deployment services, and upward of 200 hours for larger, more complex implementations. Phased deployments may require additional professional services for each new DLP component added.

Final Word – Symantec DLP

Organizations that find comfort in numbers, often feel most comfortable with the market share leading Symantec DLP offering. As we have heard more than one DLP buyer say, "No one was ever fired for buying Symantec DLP." It certainly stands out as the safe choice for DLP. However, just like any other DLP solution, Symantec DLP is not a one-size-fits-all solution and thus not an automatic fit for all organizations.

Because of Symantec's architectural complexity, small and medium enterprises under 1000 users will likely find it very difficult to take on the cost and personnel resources required to acquire, deploy and manage the Symantec DLP solution. On the other hand, organizations with complex network architectures or distributed environments may find Symantec's software/virtual machine approach to be very flexible, forgiving – and even cost effective.

Forcepoint (formerly Websense)

Company Overview

Although Websense is now Forcepoint, we will use the Websense name. Websense was first named a DLP Leader in Gartner's 2007 *Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention*, so the offering is one of the longest standing in the DLP marketplace. The DLP leader distinction came just a few months after Websense acquired early DLP vendor PortAuthority Technologies. This was the first DLP acquisition of consequence, giving Websense first crack at the space they had been eyeing and that could help establish them as more than just a web filtering company.

Product Overview – Websense TRITON APX

Websense's TRITON APX approach is unique among DLP vendors in that it is part of a comprehensive security approach that includes 1) web security, 2) email security and 3) data security (hence the name *TRITON*). Our review here, speaks only to the DLP components of TRITON APX.

In 2015, Websense decided to keep the buying public on its toes by rearranging and renaming the DLP product offering. Confusingly, the Websense TRITON APX DLP offering is not actually called "TRITION APX DLP." In fact, the well-established "DLP" moniker is nowhere to be found in Websense marketing collateral (except in reference to the add-on DLP Module offered with the separately offered email and web security solutions). With the introduction of the Forcepoint brand, we would have expected changes to the product names to more closely match the DLP marketplace. That did not happen.

The DLP components of Websense TRITON APX are made up of ***two*** separate components that curiously cover the ***three*** areas of DLP: Network, Discovery and Endpoint. The two components that encompass the three areas of DLP include:

- **TRITON AP-DATA**, which includes *TRITON AP-DATA Gateway* – known to the rest of the DLP world as Network DLP (or *data in motion*) – and *TRITON AP-DATA Discover* – known to the rest of the DLP world as Discovery DLP (or *data at rest*).
- **TRITON AP-ENDPOINT,** known to the rest of the DLP world as Endpoint DLP (or *data in use*).

This report refers to the full suite Websense DLP solution inclusively as "Websense DLP."

The architecture for Websense DLP is very simple:

- **TRITON Management Server.** The TRITON Management Server is the Windows machine that hosts the TRITON Manager, the management and reporting console for Forcepoint web, data, and email protection solutions.
- **TRITION AP-DATA.** TRITON AP-DATA can be installed on the same server as the TRITON manager and includes the policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.
- **Protector.** The protector works in tandem with the TRITON AP-DATA server. The TRITON AP-DATA server provides advanced analysis capabilities, while the protector sits on the network, intercepts traffic and can either monitor or block the traffic, as needed. The protector supports analysis of SMTP, HTTP, FTP, plain text, IM traffic (e.g., Yahoo, MSN, chat, and file transfer). The protector is also an integration point for third-party solutions that support ICAP.

Pros and Cons – Websense DLP

The Websense DLP offering will easily meet the core DLP requirements of most organizations and is considered to be a very full-featured DLP solution. We find the TRITON approach to be an advantage, especially for current customers of other Websense solutions. The architecture is, in fact, much more streamlined than some of the other leading DLP solutions and the product scores high in ease of use.

Websense's hybrid platform approach allows organizations to choose from appliances, server/software, virtual machines and cloud (in some components). Virtual machine support for many of its components allows buyers to take advantage of the move toward and investments in virtual machine environments. However, many organizations would rather be able to choose something other than Windows Server for the management console.

Perhaps the biggest caution we would give for buyers of Websense DLP is to consider the cost of the subscription over a multi-year term compared to the perpetual license offerings of every other vendor. Over the course of five or more years, Websense DLP can be much more costly than its DLP counterparts.

Pricing – Websense DLP

Websense DLP cost is based upon a per-user, *subscription license model*. Consequently, the license and support costs for subsequent years will be the same as they were in year one. This pricing model makes the Websense DLP solution look downright cheap when compared to the front-loaded perpetual license models of the competition. However, shortsighted buyers may have sticker shock when they see the first of the annual renewals.

As noted above, there are three components to the Websense DLP license: Gateway, Discover (both part of TRITON AP-DATA) and Endpoint (TRITON AP-ENDPOINT). Each of the three components carries a separate license cost, however, multi-product discounts are available. Also available are multi-year discounts for two or three year subscriptions (paid up front). Premium support is required for DLP at a cost of 15% of the total product price with a minimum annual support fee of $5000.

As with other DLP solutions, professional installation services will be required and can add significant cost to a Websense DLP implementation. While Websense DLP deployment costs are not typically as high as some of the other vendors considered in this review, buyers should request very detailed implementation plans and costs prior to any purchase agreement.

Final Word – Websense DLP

Websense DLP is a high quality product, but can have a high quality price tag to go with it. For existing customers of Websense web filtering, DLP can be a good choice, especially for those customers who have already bought into the concept of the TRITON architecture with the Web Security Gateway. Like all of the products considered here, the product works.

For cost-conscious organizations, there are probably solutions that will cost less over the long haul, even among some of the leaders.

About This Review

The DLP Vendor Review represents the sole work, views and opinion of DLP Experts. Every effort has been made to verify the content included for each vendor is current, accurate and best represents the vendor and its DLP offering. As with any document of this sort, we acknowledge that much of the content represents opinion. Where personal judgment is called for, we reserve the right to share our personal experience and acquired knowledge. Of course, we appreciate feedback from vendors and the DLP-using public to ensure the content is accurate and up to date.

About DLP Experts

DLP Experts is a vendor-agnostic reseller and integrator focused exclusively on Data Loss Prevention technologies. The company's mission is to provide organizations with a complete, unbiased view of the DLP marketplace, available technologies and a vendor-agnostic approach to finding solutions that match technical and budgetary requirements. This is accomplished using a unique methodology that views data protection as a process, not a technology silver bullet.