A Websense® Brief

July 2011

SELECTING THE RIGHT DLP SOLUTION:

ENTERPRISE, LITE, OR CHANNEL?

With Websense, you can stay a step ahead of the threats. From our roots in web filtering, we've been analyzing and classifying content for more than 15 years, and we now offer must-have web, email, and DLP security that closes the gaping holes left by traditional security products.

websense®

ESSENTIAL INFORMATION PROTECTION™

The importance of DLP

Data loss and heavy fines due to regulatory noncompliance are all too common these days, pushing data loss prevention (DLP) solutions high on the security list. But "DLP" describes a wide range of solutions, from simple tools that identify file types to enterprise-level products that make intelligent decisions based on network traffic. The term is even used to enhance the perceived value of solutions that in actuality fall far short of robust DLP. Here, you can explore the different types of DLP solutions and evaluate their merit against your particular needs.

Definitions of DLP

Enterprise DLP: Some analysts have defined DLP as products that use deep content analysis to identify, monitor, and protect data in motion, at rest, and in use. While many products can perform some of these tasks, only an enterprise-class solution can perform all these tasks.

DLP Lite: A drawback to some enterprise solutions is that they are, in fact, too complex to deploy and manage. This has fueled the perception that all DLP solutions are too complex and difficult to implement. To counteract this perception, some vendors have introduced "DLP Lite" products. Such products perform some of the required DLP tasks, making the products easier to deploy and maintain – but at the expense of some key features.

Channel DLP: Other DLP solutions focus on specific channels of communication such as email or web. These channel DLP solutions provide comprehensive feature sets – but just for one specific channel that an organization has identified as its highest priority, such as web or email.

Key capabilities to consider

Organizations should consider two primary capabilities when selecting a DLP product:

1. **Channel:** What channels of communication does your company use to transmit data? Channels of communication can include web, email, FTP, instant messaging, printing, USB thumb drives, and others. After you've identified the channel(s), consider these capabilities:
    a. Discovery - scans for sensitive data stored throughout the organization's network
    b. Endpoint - usually refers to monitoring and enforcing data use on laptops.

2. **Detection:** This capability can range from simple keyword dictionaries and regular expressions to digital fingerprinting and heuristic analysis. A word of caution: Avoid products with detection capabilities that yield a large number of false positives. This makes it virtually impossible to wade through incident logs to identify a true data security incident – fueling the notion that DLP solutions are simply too complex and costly to implement.

Pros and cons of DLP types

To determine which DLP solution is ideal for your organization, it's important to assess the pros and cons of the three DLP types.

Enterprise DLP provides superior data security coverage in almost all areas.

- **Pros:** Supports common channels such as web and email, protocols such as FTP and IM, and endpoint and discovery capabilities. While the detection capabilities of Enterprise DLP solutions vary from one vendor to another, most provide a superior level of detection including higher accuracy compared to DLP Lite solutions.
- **Cons:** Usability depends heavily on individual vendors' implementations. For example, some Enterprise DLP solutions don't use a single-policy framework. This can result in the need to create multiple policies to secure each channel, increasing the complexity of deploying and managing the product.

Websense® Data Security Suite Enterprise DLP

The Websense eEnterprise DLP solution offers these and other features that set it apart as an industry leader:

- **PreciseID™ Natural Language Processing:** This approach combines several technologies – including statistical analysis, punctuation analysis, context, and data proximity to accurately identify sensitive data, with low false positives.
- **Data Classifiers:** Over 1,100 rules out-of-the-box for common data types and expressions are already defined so that, for example, administrators can easily define a policy for detecting SSNs and corresponding U.S. names.
- **File Types:** The product examines the file header rather than just the file name or extension, so organizations can accurately detect the file type and scan for sensitive data even if the file extensions have been changed.
- **Fingerprinting:** Digital fingerprints of files and databases let organizations identify the location and transmission of sensitive data, providing the highest accuracy in detecting whole or partial matches of sensitive data.

DLP Lite solutions usually support a single channel such as web or email and are often bundled with related security solutions (e.g., email security solution).

- **Pro:** Can provide cost-effective base functionality
- **Con:** Not usually designed for expandability to cover additional features or channels for your company's future needs

Limitations of some DLP Lite solutions

DLP Lite products often omit key detection capabilities. For example:

- **Simple repository for keywords:** Detection of keywords contained in a simple repository often leads to a large number of false positives. For example, searching for the word "confidential" could identify genuine confidential information or a simple sentence using the word.
- **File types identified by file name extension only:** Detection of file types by analyzing the file name extension is often not specific enough. For example, a Word document or text file can contain either sensitive or benign data. Also, the file extensions can be renamed to bypass this capability.
- **Regular expressions:** Detection of specific data patterns is not flexible enough to articulate varying representations of data. For example, "XXX-XX-XXXX" may be identified as a Social Security number, but the same number written without hyphens, "XXX XX XXXX," could be missed.

Channel DLP solutions offer enterprise-level functionality and accuracy for a particular channel plus the simplicity and cost-effectiveness of DLP Lite solutions.

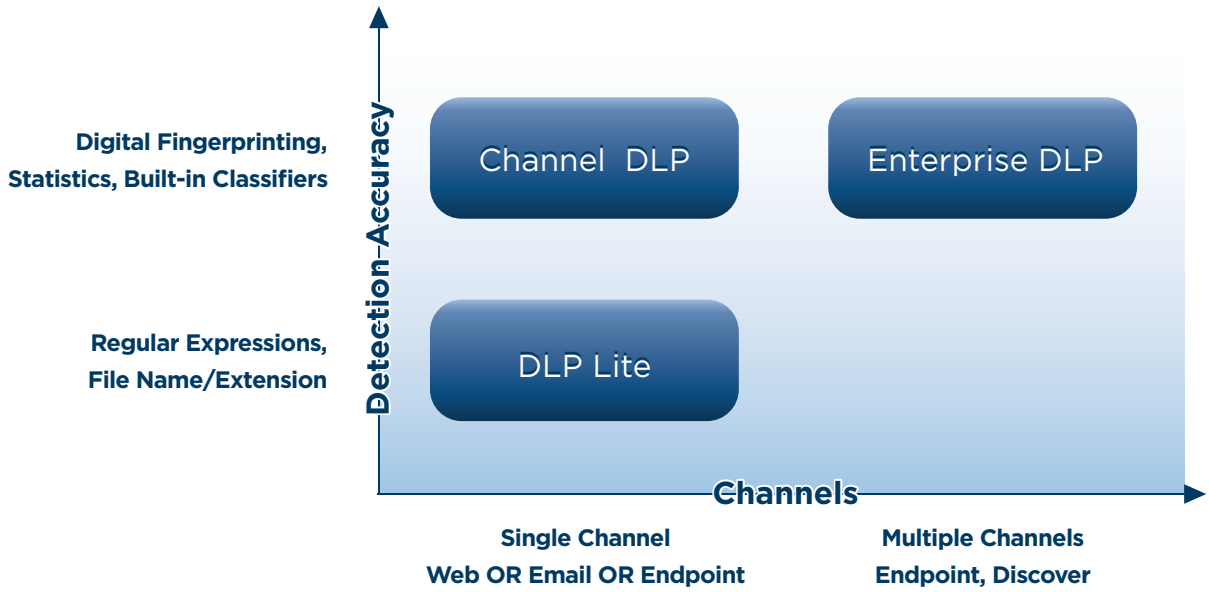
- **Pros:** Channel DLP is based on the same technology employed by Enterprise DLP solutions, so organizations do not sacrifice any detection or reporting capabilities. The configuration and management is also consistent with Enterprise DLP solutions, with the same tools available to the user. Since Channel DLP provides data security for a specific channel such as web or email, it offers tight integration with the corresponding security solutions (e.g., web security or email security gateways) and can be packaged on the same appliance, eliminating additional hardware and deployment costs.
- **Con:** Channel DLP solutions by design provide data loss protection over the most common channel of communication used by an organization. While this addresses the immediate concern, some Channel DLP solutions do not enable expansion to a full Enterprise DLP solution should additional channel coverage be needed. Therefore, it's particularly important to assess expandability of Channel DLP solutions.

Selecting the right DLP solution

Enterprise DLP, with its advanced capabilities and security coverage across multiple channels is almost always a superior solution to deploy. But when security budgets are tight or the primary business requirement is to secure a specific channel, DLP Lite or Channel DLP solutions can be good alternatives.

DLP Lite capabilities are often bundled with other security solutions at no extra cost. It's not uncommon for email security solutions, for example, to tout integrated email DLP. While DLP Lite capabilities are inferior to Enterprise or Channel DLP, the cost savings can be a compelling reason to purchase this solution. DLP Lite gives you a high-level, passive view of the types of data traversing the network. But take extreme caution in deploying these solutions to actively enforce data security policies or define regulatory compliance policies because of the high rate of false positives.

Channel DLP, with enterprise-class DLP capabilities and tight integration with security appliances, is a sound approach to data security. Unlike DLP Lite solutions, robust Channel DLP solutions support future expansion to cover additional channels and capabilities. Organizations can easily upgrade to support additional channels (e.g., from web channel DLP to web and email channel DLP) as well as other Enterprise DLP capabilities, including Discover and Endpoint. This flexibility enables organizations to deploy a robust DLP solution to address their immediate needs today and then easily expand the solution to secure other channels as their business needs grow.



Websense® DLP Solutions

Websense offers the following DLP solutions:

- **Websense® Web Security Gateway Anywhere:** Based on our proven Websense Web Security product, this solution integrates all the capabilities of the Websense Enterprise DLP solution for the web. As a Channel DLP solution, it includes all the Enterprise DLP capabilities such as Precise ID Natural Language Processing, digital fingerprinting, and built-in classifiers. The tight integration between web security and TruWeb DLP™ capability also offers organizations clear and informative details on the web destination. Websense Web Security Gateway Anywhere is available on the Websense V5000™ or Websense V10000™ appliances.
- **Websense® Email Security Gateway Anywhere:** Integrating the Websense Email Security solution with TruEmail DLP™ capability (our enterprise-class DLP solution for the email channel), this product provides comprehensive security for email. This Channel DLP solution includes all the Enterprise DLP capabilities as well as the ability to expand to additional channels with a simple click of a mouse. Websense Email Security Gateway Anywhere is available on the V5000 and V10000 appliances. Both Email Security Gateway Anywhere and Web Security Gateway Anywhere can run concurrently on a single V10000 appliance.
- **Websense® Data Security Suite:** As the Websense Enterprise DLP solution, this suite provides data security coverage for all channels as well as the advanced capabilities needed for comprehensive data security. In addition to securing common channels such as web and email, it offers coverage for IM, FTP, and other protocols. The solution also offers the capability to discover sensitive data stored throughout your network and, if necessary, take remediation action. It extends the data security coverage to laptops

and can be used to restrict copying of sensitive data to removable media as well as disable print-screen or copy-paste features. Organizations with TruWeb™ DLP or TruEmail™ DLP solutions as part of Websense Security Gateway Anywhere and Websense Email Gateway Anywhere can easily upgrade to Data Security Suite with a simple license upgrade. Data Security Suite, TruWeb DLP and TruEmail DLP all share the same management server and UI.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in unified Web security, email security, and data loss prevention (DLP) solutions, delivers the best content security for modern threats at the lowest total cost of ownership to tens of thousands of enterprise, mid-market and small organizations around the world. Distributed through a global network of channel partners and delivered as software, appliance and Security-as-a-Service (SaaS), Websense content security solutions help organizations leverage mobile devices, Web 2.0 and cloud-based platforms while protecting against targeted threats, preventing the loss of confidential information and enforcing Internet use and security policies. Websense is headquartered in San Diego, California with offices around the world.

For more information, visit: www.websense.com.