websense

PROTECTING IP DATA FROM LOSS AND THEFT:

THE SHORTEST PATH TO PREVENTION AND RISK REDUCTION

websense TRITON®

PROTECTING IP DATA FROM LOSS AND THEFT: **THE SHORTEST PATH TO PREVENTION AND RISK REDUCTION**

Executive Summary

Data loss prevention (DLP) has a poor reputation among information security professionals. DLP implementations are thought to be complex and costly, and many are left to languish in the data discovery, classification and monitoring phases, unable to ever produce the hoped-for benefits of active data loss prevention policies. High consulting fees often conspire to drive down return-on-investment (ROI) for DLP projects, and overly exhaustive efforts to discover every piece of potentially valuable data at rest across multiple business processes contribute to the gridlock. It's no wonder many newcomers to DLP fear it.

Despite these perceived drawbacks, DLP implementations are expected to surge in the year ahead. The theft of intellectual property (IP) is driving the need more than compliance requirements, as organizations are realizing that DLP can protect competitive advantages and prevent espionage by securing business plans, product roadmaps and other confidential information. So while most organizations are not looking forward to deploying DLP, they recognize that they must.

Organizations with the staying power to see a DLP implementation through to completion stand to derive significant value. Analysis consistently shows that DLP projects that reach the prevention phase show positive results, including fewer data loss incidents, lower risk and definable ROI. Research also shows that moving from monitoring to prevention greatly reduces data loss incidents as users learn the difference between acceptable and unacceptable use of confidential data. For example, one organization was able to reduce incidents by two-thirds after its prevention policies were in place for 60 days.[1]

In this paper we describe the shortest path to reaching the prevention stage of data loss and data theft incidents without bringing data flows to a grinding halt. We begin by presenting an expanded view of IP, including the rationale that it extends beyond an organization to encompass the IP of partners and suppliers. Next, recognizing that process, not technology, drives successful DLP implementation, we outline six steps an organization can take to deploy data security controls. Last, we introduce the Websense concept of "DLP as a defense," and demonstrate how our DLP technology offers robust and unique features, yet is easy to deploy and manage.

What You Must Protect—And Why

Proactive companies are protecting their IP and other confidential information through a combination of encryption services, digital rights management and DLP controls. However, they might not be protecting enough, narrowly defining IP as patents, trademarks and information that a legal team would protect. IP can also include operational information, plans, forecasts and working bids for future business. In fact, any information that provides competitive advantage can be considered IP. The following real-world DLP scenarios can help illustrate this fact:

- A gas company in Egypt wanting to protect its seabed exploration maps.
- An electronics manufacturer in the UK wanting to protect product designs.
- A health services agency in the United States wanting to protect health and research data.
- A retailer in Israel wanting to protect discount promotions before they are launched.
- A software developer in Hungary wanting to protect its source code.
- A bank in Saudi Arabia wanting to be meet PCI compliance requirements.
- An airline in Italy wanted to mitigate false procurement fraud.

[1] https://community.websense.com/blogs/websense-insights/archive/2013/04/05/six-steps-for-deploying-data-security-controls-part-ii.aspx.

IP can also extend to partner and other third-party information used in the creation of your company's goods and services. How your organization enables its IP to be used by outside organizations, and how you protect your partners' IP property, is a two-way street.

There are potentially high costs to insufficiently protecting your IP, and once a breach occurs it's usually too late to stop the damage: 69 percent of breaches are initially spotted by an external party, while only 9 percent are first detected by the organizations that were breached.[2] This external exposure can result in financial ruin, devastated reputations and other damages.

Motivations for Stealing IP

There are three primary motivations behind the theft of IP:

1. **Gaining security credentials for future attacks.** Unfortunately, the security credentials often used to protect an organization—such as one-time password token seeds or signing certificates on approved apps—also happen to be an attack vector, the theft of which enables future attacks to steal an organization's IP. Thus the key dependencies and trust relationships of such security credentials should not be assumed safe.
2. **Seeking trade secrets to gain competitive advantage.** Nearly two-thirds of IP theft attacks are against manufacturing, professional and transportation industries.[3] The motivation here is clear. IP theft can nullify the competitive advantage of the company it was stolen from, and reduce time-to-market for the company that benefits from the stolen information.
3. **Getting back at an employer.** The insider threat does exist. While 86 percent of attacks do not involve an employee or insider, the 14 percent that do are often attributed to lax security controls, and over 70 percent of these attacks happened within 30 days of an individual announcing resignation from the organization.[4]

Overall, financial gain drives most IP theft, and over 90 percent of data theft incidents are attributed to external actors most often using hacking or malware to pull it off.[5] The result is a faceless crime perpetrated over web communications that flow through our networks and past traditional defenses focused on securing infrastructure, not data.

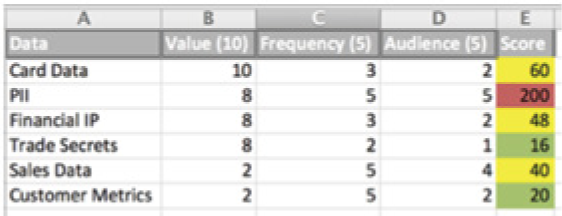
Six Steps for Deploying Data Security Controls

The best approach to implementing DLP is to start small and move methodically through all the steps to fully understand the project and results. IP is a good place to start before moving to larger datasets with more owners and business processes.

It's helpful to get advice from a peer or expert that has been through the process from beginning to end to know what to expect. The six steps below for deploying data security controls come from Neil Thacker, information security and strategy officer for the Websense Office of the CSO and former head of security operations for Camelot (UK National Lottery) and Deutsche Bank.[6]

1. **Calculate the value of your data.** Without a plan, this can be the most difficult part of the process. Data values can rise and fall as quickly as financial markets. The key to solving this problem is working with your executives and information owners. Determine a simple formula to estimate the value of your data.

   One of the best examples we've seen comes from the research group Securosis. Data value, frequency and audience is quantified within a table and allotted a score. Examples of data types include card data, personally identifiable information (PII), IP, sales data and any other specific data you are required to protect. An overall score is then defined based on the type of data. Below is an example of how this can work:



A	B	C	D	E
Data	Value (10)	Frequency (5)	Audience (5)	Score
Card Data	10	3	2	60
PII	8	5	5	200
Financial IP	8	3	2	48
Trade Secrets	8	2	1	16
Sales Data	2	5	4	40
Customer Metrics	2	5	2	20

   By scoring the data types, you can prioritize the importance of the data. Including frequency and audience also helps determine the likelihood of data loss, and again assists when prioritizing where and when to apply an action.

[2] Verizon "2013 Data Breach Investigations Report."
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Adapted from https://community.websense.com/blogs/websense-insights/archive/2013/04/05/six-steps-for-deploying-data-security-controls-part-ii.aspx.

2. **Make your ROI case.** To increase security spend and roll out new data security controls, you must demonstrate ROI. This means clearly quantifying the immense value that comes when you know where your data is, who is accessing it and how it's being used. It's critical to analyze, communicate and share the financial and organizational impact of stolen and lost data.

3. **Monitor and log your data.** Next, start monitoring who has access to data and observe how data moves around your network. Many organizations turn to a DLP solution for this. The best DLP solutions have the ability to monitor the perimeter entry/exit points for data in motion and thoroughly monitor endpoints for data in use.

   The initial monitoring phase should not last longer than a few weeks after deployment, even after tuning your policies to remove false positives. A good solution should quickly provide clarity into common data movement trends. Just remember to monitor every location where your data flows, including the often-overlooked printers, scanners, mobile devices and cloud services.

4. **Apply data security controls.** We often speak with organizations that are stuck in step three, in the monitoring and logging phase. They identify incidents as they happen, but lack confidence in applying controls to stop data leaving the organization. This is a mistake.

   Gartner Inc. demonstrated some time ago that passive security controls were dead. The same goes for DLP used exclusively in a monitor-only deployment. It doesn't demonstrate ROI to most businesses, especially if a significant loss or breach occurs while you are monitoring. We must apply controls.

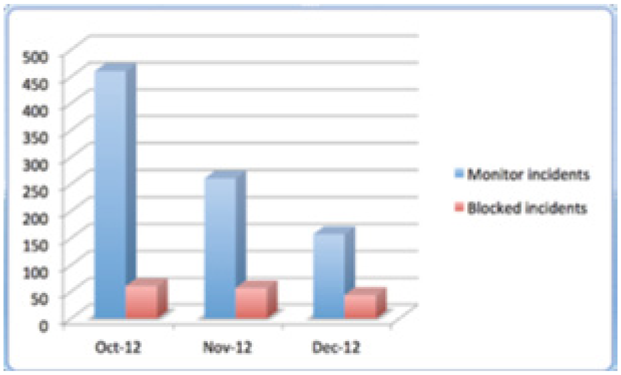
   First, revisit your most valuable data. Start amending the rules and policies to begin active protection of those crown jewels. We don't recommend enabling all block rules immediately. Our experience indicates that a phased approach is the most efficient way of applying data security controls.

5. **Find your data.** Once you have a score associated with each data type and the funding to proceed, the next stage is to locate the sensitive data on your network. Based on the scoring exercise explained above, it's always advisable to begin this process with the most valuable data. Focusing on your crown jewels minimizes the negative impact to your network. Unfortunately, stand-alone discovery and data mining services are usually expensive and take a considerable time to run.

   Another option is relying on DLP solutions. Most leading DLP solutions offer a mechanism to discover, identify and fingerprint data in periodic sweeps. These sweeps can be scheduled daily, weekly or monthly. This process provides a marked increase in visibility and improved efficiency by identifying duplicate data and flagging it. (Many organizations waste large amounts of money backing up and storing duplicated data; to a security officer, reducing the cost of this process is great additional justification for the purchase of a DLP solution.

6. **Implement proactive protection and increase employee education.** As user awareness becomes more prominent, the number of blocked incidents will stabilize and the number of monitored incidents will go down. Why? A typical user is much more aware prior to clicking on a link or sending an email if they understand that these actions will result in a block and notification. As a result, information owners and security teams gain tremendous value through proactive protection, as well as a beneficial reduction in the IT team's workload.

Below is a graph showing proactive protection in action. The number of incidents steadily decreased when a 2,500 user enterprise activated blocked actions in October 2012.



We may have made the previous steps sound easy to implement, and they should be. A data security control strategy can add more value than any technical solution deployed within an organization.

DLP as a Defense

There are two sides to the concept of DLP as a defense. The first is blocking external actors from using hacking and malware to steal IP and confidential data, and the second is using DLP to reduce the rate of occurrence of data loss incidents through prevention policies.

The first side of DLP as a defense requires technology as advanced as the threats facing organizations today. A web gateway with traditional (i.e., outdated) defenses—such as anti-virus and URL filtering—is ineffective against targeted attacks and modern malware; having such technology in place would defeat any DLP project. And when you consider that 95 percent of nation-state affiliated espionage relied on email phishing in some way, it becomes clear that both web and email gateways are avenues for data theft, and few today have containment defenses or data security controls.[7]

The unified Websense® TRITON® architecture changes the data-protection playing field in a number of ways. By embedding DLP directly into web and email gateways, it requires no integration steps or custom connection protocols, and because the triton architecture unifies data security controls for web and email gateways the same console can be used to manage the entire security solution. Further, it provides continuous threat protection by relying upon key Websense technologies: the Websense ThreatSeeker® Intelligence Cloud, which refers to security ratings before a request is allowed to pass; Websense ACE (Advanced Classification Engine), with real-time inline defenses and DLP controls implemented during a request process; and Websense ThreatScope™ malware analysis sandboxing, which can be employed after a request to uncover hidden unknown threats and communications.

There are additional ways the unified TRITON architecture enables DLP as a defense that other solutions can't provide. It can detect password file theft, or the use of custom encryption, and provide geo-location destination awareness. More specific to DLP controls is the ability to detect slow data leaks (e.g., one record every hour); the ability to use optical character recognition (OCR) of text within images to detect data theft or loss; plus when possible it offers the forensic capture of data on security incidents. Threat dashboards and forensic reporting details are also exportable to SIEM solutions.

The TRITON architecture is the foundation of Websense Data Security Suite, which can help manage the risk of data theft from malicious insiders or advanced threats, the accidental misuse of data, and provide regulatory compliance while securing your organization against a wide range of data theft and loss scenarios. Data Security Suite contains three DLP modules—Data Security Gateway, Data Discover and Data Endpoint—that can be licensed separately if you plan to start with one capability and later expand to others.

Importantly, Data Security Suite is in a class of its own when it comes to reducing the cost and complexity commonly associated with the deployment of a DLP solution. (And after evaluating Data Security Suite, Gartner Inc. positioned Websense as a leader in its "Magic Quadrant for Data Loss Prevention" for the 6th consecutive year.[8])

Websense Data Security Suite provides:

- Easy integration with existing network infrastructure.
- One console to centrally manage web, email, mobile and endpoint DLP security policies.
- ActiveSync agent to apply mobile email DLP policies to all compatible mobile devices.
- Off-network protection of remote devices, including MAC OS X and Windows systems.
- Over 1700 predefined policies and templates easily selected by region and industry.
- Advanced data classifiers and natural language processing to protect IP.
- OCR of text within images for data-in-motion and data-at-rest (an industry first and only).
- Enable user self-remediation with administrator auditing to keep data-in-motion.
- Email notifications to accelerate incident management process flows.
- Portable decryption included for USB and media devices.

[7] Verizon "2013 Data Breach Investigations Report."

[8] 2007 and 2008 reports were titled Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Reduce the Pain of DLP Deployments

To move from the monitoring stage to the prevention stage with minimal impact on data flows, Data Security Suite enables users to provide remediation input with administrator auditing. This capability keeps data flowing while educating users on what actions should be prevented or allowed, providing a valid reason for auditors. In addition, email notifications enable faster remediation process workflows, all in an effort to keep data-in-motion and business processes moving forward while an organization adapts to new data security controls.

New to regulatory controls, the Data Security Suite solution comes with over 1,700 policies and templates that are easily selected by region and industry type within a start-up wizard. Websense data security researchers keep the database updated with the latest new policies and templates required around the globe.

The same DLP policy engine is used within all locations of the TRITON architecture, combining rich classifiers with real-time contextual awareness of user, data and destination to provide high accuracy and consistent data loss prevention. This also enables context aware alerts providing user identification, manager within AD structures, and the web category of the destination making remediation steps easier and faster for helpdesk administrators.

A single policy framework enables a DLP policy to be applied to one or multiple channels, and provides granular response options based on severity of incident. Getting started comes down to selecting an identification method, channels to monitor, scheduling a discovery task, and setting severity and responses followed up by incident investigation.

For endpoints, the Data Endpoint module of Data Security Suite is unique in providing off-network protection for registered (or fingerprinted) data that is likely to include IP, whereas competitive solutions often require a network connection to a central database. Data Endpoint also includes portable encryption for mobile media and USB devices at no extra charge. For stricter controls, Data Endpoint supports agent-to-agent encryption in which another Data Endpoint enabled system is required to open the encrypted file.

Summary

2013 is the year DLP becomes more than a means to comply with regulations. The theft of IP by companies and nation-states—by spies, criminals and activists—is changing the future of industries, economies and entire countries, and as a result DLP is increasingly necessary to protect against the loss or theft of IP—that belonging not only to an organization, but its supply chain and partners as well.

DLP as a technology is now at an advanced state within the TRITON architecture. Such a unified architecture enables contextual security with real-time awareness to user, destination and data that is not possible with standalone solutions and basic integration. This strengthens policy controls, improves accuracy and consistency and reduces overall cost of operations.

DLP need not be painful, costly or drawn out for years. Start small with a focused dataset and work though the six steps outlined above. Getting to DLP prevention policies shows the best return and reduces risk; you just have to get started—understanding that your organization has either been attacked, is being attacked right now, or is about to be attacked. It's just a matter of time.

Learn More at **www.websense.com**

+1 800.723.1166 | info@websense.com

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense
TRITON®