



Key Elements of Data Loss Prevention
A white paper for executives making decisions
on information security, risk and compliance

Executive Summary

Every day, data is being removed from corporate networks, whether by accidental or malicious means. Once it is removed, the risk to the company can be substantial, and may result in industry sanctions, lawsuits, brand damage and the loss of consumer confidence.

Data Loss Prevention (DLP) solutions are specifically designed to avert such disasters. A DLP system has the ability to locate (Discover) confidential data within a corporate IT structure, determine how it is being used and how best to prevent its loss. DLP provides automatic protection of sensitive data across endpoints like laptops, USB devices, smart phones, network devices and storage systems. DLP also helps with incident response workflow to enable corrective action with employees.

There are many DLP solutions on the market. The best ones will identify broken business processes transmitting confidential data, monitor and protect communications of sensitive content, and deploy universal security policies across the enterprise.

Intended Audience

This document is intended for CEOs and executives responsible for information security.

Data drives business, and data loss can be catastrophic. However, despite a widespread and ongoing effort to improve security efforts, data breaches continue to occur, led by growing instances of identity theft.

Such incidents are not surprising given the universal and unlimited access to the Internet and the development of mobile storage and communication devices. Today, information can be instantaneously downloaded, shared and accessed. In a company, private data may be transmitted between employees, partners, consultants and outsourcing agencies. Workers can access information not only in the office but also from home, or on the road. The variability of platform versions on mobile devices has made localized DLP capabilities a challenge. Whether data is in motion or at rest, it is always at risk without the implementation of effective safeguards.

The federal government and industry organizations have passed a variety of regulations requiring companies to secure their data, from customer and employee social security numbers, to credit card numbers and Magstripe data, to internal documents on company pricing, products and marketing strategy. And yet, 81% of companies breached were not

compliant with PCI data security standards at the time of their data loss incident, according to a National Retail Foundation study.

Data is at risk from both internal and external threats, some of which may be unintentional. In fact, of the 76% of breaches caused by company insiders and partners, many of them are not the result of malicious intent, but merely a lapse in judgment. However, it is the external targeted attacks against high value data that cause the most significant damage – as much as \$6.7 million on average according to the Ponemon Institute.

Data Loss Prevention (DLP), also known as Data Leak Prevention, Information Leak Detection and Prevention (ILDLP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) and Information Protection and Control (IPC), offers the best defense against a variety of data threats.

Why is Data Loss Prevention Important?

The Night Dragon attacks illustrate the online dangers faced by companies, and the methods used by DLP to protect sensitive data.

Chinese computer hackers, dubbed Night Dragon, targeted U.S. oil, gas, and petrochemical companies. Proprietary and confidential information was stolen from executives through a combination of social engineering, Remote Access Trojans (RATs), and SQL injection attacks to gain access to external and internal hosts inside companies.

While Night Dragon was among the most highly publicized of breaches, recent attacks on other industries followed a similar pattern of accessing data through social engineering and publicly available RAT applications. Other common trojans used in these types of attacks include Gh0st RAT and Poison Ivy, all of which are readily available for download.

Unfortunately, remediation after a breach has occurred will always cost substantially more than implementing preventive measures. Preventing and blocking data leaks, whether the data is encrypted or not, and monitoring how data is accessed and transferred (email, smartphones, USB devices, etc.) provides the most effective means to thwart an attempted breach—and is the objective of a Data Loss Prevention system.

Traditional IT budgets focus more on preventing hackers by deploying peripheral security in the form of firewalls, IDS/IPS solutions, and Gateway Email and Web Security solutions. However, with a constantly evolving mobile work force and the ever-increasing use of mobile devices including smartphones, tablets, laptops, and USB devices, traditional peripheral security devices cannot protect against all threats, including insider threats. Furthermore, risk of sensitive data loss increases when transmitting data via alternate network capabilities, such as Bluetooth. With new attacks coming from social media avenues and endpoint devices, organizations are looking to proactively protect information assets no matter where the data is stored, travels, or used. We can no longer rely on peripheral security to prevent a breach.

What is DLP?

Data Loss Prevention (DLP) is a computer security term referring to systems that identify, monitor, and protect data-in-motion (network security), data-at-rest (storage security) and data-in-use (endpoint security). These systems achieve their goals through advanced content-aware inspection capabilities, contextual security analysis of transactions (attributes of originator, data object, medium, timing, recipient/destination etc.) and robust management consoles with a centralized framework. Cloud and software-as-a-service (SAAS) delivery models have now joined traditional delivery systems for DLP.

While other security tools are designed to detect any activity that can pose a threat to an organization, DLP is specifically designed to detect and prevent unauthorized use and transmission of confidential information. In the event of a breach, DLP can prevent data leakage, therefore reducing risk and consequences. There has also been an increase in the integration of identity awareness in traditional DLP products. And many prominent vendors are incorporating more DLP capabilities into such products as email boundary security, secure Web gateways and endpoint protection platforms.

In addition to protecting information, the most advanced DLP solutions also help identify risk, establish policies and processes, educate users, and integrate security technologies and controls.

The advent of content-aware DLP – a set of technologies and inspection techniques that enable the dynamic application of policy based on the classification of content – should also help companies to develop more secure business practices for the handling of sensitive data. Unlike transparent controls such as firewalls, the deployment of content-aware DLP is visible to the end user, and thus encourages more constructive user behavior. That explains why content-aware DLP deployments and sales have steadily increased from \$300 million in 2010 to \$425 in 2011, with projections for \$520 million in sales in 2012, according to a Gartner research study.

Another future growth area for DLP technology is in identifying non-text data in content analysis (audio, video, images).

Data-In-Motion

Data-in-motion refers to data transmitted across a network. Protection through DLP typically features a software or hardware solution that is installed at network egress points near the perimeter. It analyzes network traffic to detect sensitive data that is being sent in violation of information security policies.

This data can be regarded as secure if both hosts are capable of protecting the data and a third party cannot eavesdrop on the communication. With DLP technology in place on the network, these organizations are able to immediately reduce the risk of losing data in transit.

While data-in-motion solutions block transmissions, they do not provide root cause remediation capabilities. They cannot offer notification of new instances of unsecured sensitive data. Thus, organizations using data-in-motion technology alone do not have information that allows them to proactively take action and minimize exposure risk. This risk can be mitigated through a combination of implementing device and port control policies in conjunction with EndPoint DLP.

Data-At-Rest

Data-at-rest refers to data stored on computers, stored on storage devices, or being used by the data owner. Examples include files, databases, or e-mails saved on a hard drive or server. A DLP system provides a software solution that is installed in data centers to discover confidential data stored in inappropriate and/or unsecured depositories.

Data-at-rest solutions should be both corrective and proactive. They should provide a company with the means to address the root cause of most data loss scenarios by securing data at the source. When such data at rest is found, it can be automatically moved to a secure location or encrypted based on policy.

A comprehensive data-at-rest solution will also provide centralized reporting on aggregate risk exposure. By analyzing trends over time, a company can determine if their security policies are sufficient and effective.

Data-In-Use

As with data-in-motion, endpoint-based security, or data-in-use, can address both internal and external communications, and help to secure information flow between employees, organizations or types of users. It can also control email and Instant Messaging communications before they are stored in the corporate archive.

Endpoint DLP enables organizations to identify sensitive information on laptops and desktops and stop it from being copied to USB drives and iPods, or burned to CDs or DVDs. With DLP capabilities at the endpoint, organizations are now able to reduce the risk of losing data in use.

A data-in-use system is an agent-based solution that runs on end-user workstations, laptops and servers. By monitoring data that leaves via removable devices, it also provides auditing and protection against users who print classified data.

With a unified DLP solution across endpoint, network, and storage systems, organizations can better understand where their sensitive information is, how it is used, and how best to prevent its loss.

The Human Element

In addition to monitoring technology, DLP also reduces the risk of a data breach by focusing on employees as well. Virtually all data breaches are a result of people not following proper security policies. Whether the employee was unaware of the policy, or chooses to ignore it, the result is the same.

Either way, DLP protects data and helps to prevent its loss. It will also notify the employee of his or her error in real time and suggest corrective action. This can provide a tremendous boost to best practices in the security realm, by not just correcting one employee's mistakes but by influencing the behavior of others with whom that employee interacts. One Fortune 100 company noted a 90 percent drop in data loss incidents just 10 days after turning on the automated user notification capabilities within DLP, according to an article by Joseph Ansanelli, Vice-President of Data Loss Prevention Solutions at Symantec.

Choosing a DLP System Provider

The choice of a DLP system should begin with a basic question: What do we need to achieve through a DLP deployment? All decisions made regarding the planning and operation of DLP should be made with the input of both IT and non-IT security stakeholders.

An effective DLP system should use sophisticated detection techniques to find confidential data wherever it is stored, or in any combination of network traffic, data at rest or endpoint operations. These techniques may include partial and exact document matching, structured data fingerprinting, statistical analysis, extended regular expression matching, and conceptual and lexicon analysis.

The solution should create an inventory of sensitive data, and automatically manage data cleanup. It should understand how a company uses confidential data, and whether an individual user is on or off a corporate network. It should work in conjunction with the company's security policies to prevent confidential data from leaving an organization, as well as help to define universal policies across the enterprise. Any incidents that do occur should be remediated and reported.

The solution should also address social media policies – for example, which social media sites are allowed as part of corporate marketing, and what type of content is approved for posting onto social media sites from the company network or systems.

When choosing a DLP provider, it helps to find out as much as possible about the quality of their products and their reputation within the industry. Several questions can help to make an informed decision, such as:

- What protocols (email, Web, file transfers, Instant Messaging) can be blocked or analyzed?
- Does the system control which applications can or cannot be run on endpoints?
- Can the system review encrypted data streams?
- Can the system search for data without any endpoint agents installed?

- How fast will data pass through the DLP system?
- What types of reports will the system generate? Are reports generated in real time?
- Has the DLP product been certified by the Federal Information Processing Standard (FIPS)?

Aurora has assisted many clients to implement DLP solutions, and while we recommend utilizing all components of enterprise DLP to safeguard high-risk data on servers, databases, endpoints, and throughout the network, we also advocate a phased approach so as not to overwhelm a company's resources.

Conclusion

Enterprise DLP solutions can significantly reduce the risk of data loss due to inadvertent employee behavior and broken business processes, the causes of 95 percent of data loss incidents.

Companies can no longer rely on traditional perimeter security solutions to guard high-risk data, and must consider DLP strategies to include data-at-rest, data-in-use, and data-in-motion.

About Aurora

Aurora is a security consulting firm providing security services to help clients gain visibility to vulnerabilities and increase their security posture. Services include Gap Analysis, Penetration Testing, Vulnerability Assessment, Employee Best Practice Training, and more. In addition to these services, Aurora provides implementation planning, and deployment services for enterprise DLP and Encryption projects.