



# SENTINEL RIDGE CONSULTING GROUP INC.

**“YOUR COMPUTER SECURITY EXPERT”**

## **Data Loss Prevention**

Ian Parker, GCUX, GCFW, CCSA, CSSE  
President  
Sentinel Ridge Consulting Group, Inc.

# 1 Introduction

The corporate Information Security Officer was visibly proud as he provided his visitors a tour of the company's data centre and explained how the various security technologies employed on the network made a network intrusion extremely unlikely. "We employ only best of breed firewalls, intrusion prevention systems and virus scanning", he exclaimed. As he spoke, a gentleman dressed in janitorial clothing passed the group. He smiled and nodded his head as he passed. While the manager did not recognize the man, he was gratified that the cleaning staff were so friendly.

As he left the room, the man felt in his pocket and fondled the USB flash drive that now contained the entire contents of the company's R&D server.

While the above story is fictitious, it is entirely plausible and similar catastrophes have befallen many companies. Fortunately, industry is now waking up to the fact that the best perimeter protection in the world is rendered useless if somebody with physical and logical access to a host containing confidential information, whether that person be a disgruntled employee or an intruder masquerading as the janitor, can simply insert a removable device and walk off with the company's most critical information assets.

For this reason, a new technology to detect and prevent unauthorized use and transmission of confidential information has become the new frontier of information security. This technology goes by many different names and acronyms, such as Data Leak Prevention (DLP), Information Leak Detection and Prevention (ILDLP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) and Extrusion Prevention.<sup>1</sup> This article uses the term Data Loss Prevention and acronym DLP.

## 2 Why We Need DLP

As described in the introduction, DLP technology can detect and prevent an unauthorized individual from obtaining confidential information and then passing that information to external parties. However, the technology can equally well prevent authorized individuals from inadvertently performing a similar action. An example would be an employee who intends to send an e-mail with a sensitive attachment to John Smith, the company president but instead sends it to another individual with the same name. A more common example may be somebody who clicks "Reply All" in their e-mail client and sends sensitive information to unintended recipients. Finally, who hasn't heard of or actually experienced the horror of sending a sensitive document to the wrong printer located in a public area in a different building?

## 3 Types of DLP Solutions

As is the case with most security technologies, different vendors are addressing the DLP challenge in different ways. Today's DLP solutions address sensitive data from three

---

<sup>1</sup> Hopefully, once the technology matures and gains widespread acceptance, a generally accepted term will emerge.

perspectives, namely, data-in-motion, data-in use and data-at-rest.

Let's take a look at each type of solution.

### 3.1 Data-in-Motion DLP

This type of DLP solution, otherwise known as network-based DLP, attempts to detect and act on (e.g. block, quarantine or encrypt) sensitive information as it travels across the network.

This type of DLP solution tends to be relatively simple and inexpensive to implement, as it normally consists of a single hardware appliance placed at an appropriate point on the network, usually on the path between the internal environment and the Internet.

Diagram 1 shows how such an appliance, placed inside the Internet firewall, could potentially analyze and act on all outbound traffic.

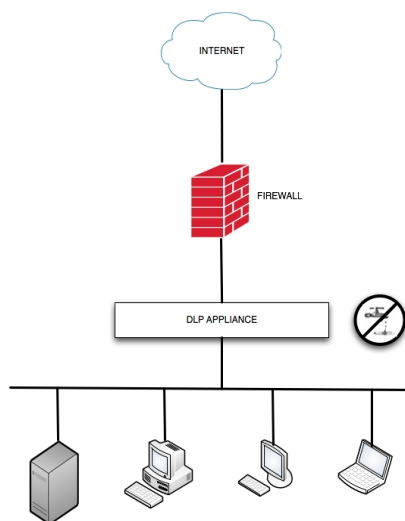


Diagram 1. Data-in-Motion DLP Solution Example

Depending on the capabilities of the appliance, a network-based DLP solution can prevent the leakage of sensitive information that is part of Web, FTP, e-mail or instant messaging traffic.

Note, however, that this type of solution would not prevent the scenario presented in the introduction to this article i.e. the transfer of data to a removable device. How significant a drawback this might be depends in part on why a DLP solution is being implemented, as I will discuss shortly.

### 3.2 Data-in-Use DLP

This type of DLP solution, otherwise known as host-based DLP or endpoint DLP, attempts to address the apparent shortcomings of network-based DLP by analyzing all data as it is accessed, whether it remains on the original host, travels across the network, is copied to a removable device or is printed.

Diagram 2 shows the same simple network as earlier but this time, instead of a single DLP

appliance, a DLP software agent is installed on each internal host. This agent can effectively detect and act upon sensitive data wherever and whenever it is used, hence the term “data-in-use”.

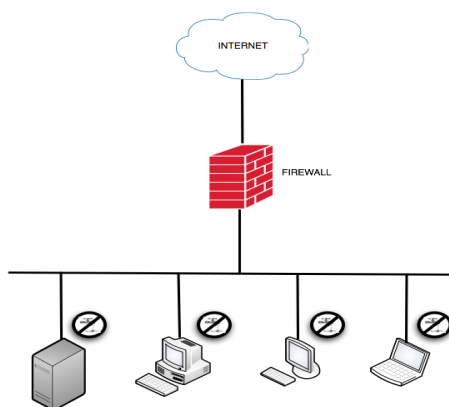


Diagram 2. Data-in-Use DLP Solution Example

In order for this solution to work, DLP software must be present on every device in the organization that might conceivably contain sensitive data. As is the case with other security applications that rely on such agents, this presents a problem for many organizations. There are many possible reasons why it may be impractical to install and maintain a DLP agent on every device connected to an organization's network, including application and operating system incompatibilities, insufficient computing resources to run the agent, devices that are offline and third party devices e.g. contractor laptops, external devices used for remote access etc.

### **3.3 Data-at-Rest DLP**

Often a company may not even be aware of which devices on the network contain sensitive data. A data-at-rest DLP solution, which may be integrated into either of the preceding solutions, attempts to reach across the network and discover sensitive data wherever it may reside, whether or not it is currently being accessed. Depending on how the solution is implemented, it may simply report on what it finds or may actually perform some kind of remediation. If, for example, sensitive data is found in an inappropriate location, it may be automatically encrypted or moved to a more secure location.

## **4 Which DLP Solution is Best?**

As you may suspect and as is so often the case, the answer to the question of which solution is best is “It depends”.

As I stated earlier, DLP can prevent the leakage of sensitive information either by malicious intent or by user error. The kind of scenario presented in the introduction fortunately constitutes the minority of data leakage incidents. The reason it is not more common is that

companies typically have other kinds of both logical and physical security controls in place to prevent random individuals from stealing data. For example, strong access control mechanisms and enforcement of password-protected screen savers would go a long way towards preventing unauthorized individuals from walking up to an unattended workstation, inserting a USB flash drive and walking away with confidential information.

Far more common are the instances of user error and the most common type of error is undoubtedly inappropriate information that is mistakenly sent by e-mail. Proponents of network-based DLP, therefore, argue that their solutions effectively deal with e-mail leaks, while avoiding the cost and complexity of a host-based DLP solution.

The best advice I can offer to companies contemplating a DLP solution is to perform a thorough risk assessment to determine the most likely means by which data leakage could occur and then deploy a solution that will integrate well with their existing security infrastructure. The following suggestions are far from all inclusive but do provide a starting point for a discussion on what kind of DLP solution to deploy.

#### ***4.1 What Security Technologies Already Exist?***

Other security technologies that the company employs may already possess some “DLP-like” functionality that is not currently being utilized. For example, some e-mail content filtering applications have the ability to perform pattern matching to detect the presence of words or phrases that may be indicative of confidential information. It may be possible to leverage this functionality as part of an overall DLP solution.

#### ***4.2 What Happens When Data Leaks Are Detected?***

The company must decide what action will be taken if the DLP solution does find sensitive data. The three most common actions that a DLP solution will take are to quarantine the data, automatically encrypt it or block it's transmission. The first impulse may be to block it and issue an alert. However, the Help Desk may find themselves overwhelmed with calls from irate users, especially if some of these alerts turn out to be false positives. If the company already possesses an intrusion detection/prevention system, the personnel in charge of this system will be well acquainted with the issue of false positives and would be a useful resource for a DLP project also.

A clear policy needs to be established on how sensitive data will be handled within the company. The user community then needs to be educated with respect to this policy. Only then should a DLP solution be implemented.

#### ***4.3 Should Data Be Encrypted?***

Some DLP solutions include the capability to automatically encrypt sensitive data before it is allowed to pass. While this may be a very useful capability when used wisely, data encryption requires careful management of encryption keys, otherwise the poor Help Desk may again be flooded with phone calls over lost keys. If the company already has a facility for encrypting data, perhaps as part of a public key infrastructure, extending this facility to a DLP environment may be very worthwhile. In other instances, the complexity and administration overhead of encryption may prove to be excessive.

#### **4.4 Should Users Be Part Of The Solution?**

Some DLP solutions include a mechanism for alerting the user when sensitive data is about to be transmitted e.g. “Do you really want to send the payroll file to this person?” Such a feature can be very beneficial, as gentle reminders such as these can reinforce good practices on the part of employees and make them less likely to repeat the same mistakes. In this way, the number of accidental data leakage incidents can be greatly reduced simply by educating the user community.

*Ian Parker is the president of Sentinel Ridge Consulting Group, a firm specializing in the security of corporate computer networks. You can reach him at [sentinelridgeconsulting.com](http://sentinelridgeconsulting.com).*