Data Loss Prevention vs. Security Solutions and Your Data

Gene Allen, Founder; ByStorm Software

The Problem

Data Loss Prevention (DLP) is more than the latest buzzword. Loss of credit card and personal data causes irreparable harm to a company and can have a huge financial impact on both institutions and individuals. From HIPAA in the health care industry to PCI DSS (the Payment Card Industry Data Security Standard) for merchant accounts, new standards are being set every day for how businesses should strive to protect their—and their customers'—data.

Whether you are driven by compliance or an actual fear of loss--if you do a quick Google search on Data Loss Prevention you will see that many different companies offer their own solutions to the data loss problem and the various regulatory requirements. It is helpful to understand how those different approaches work (and don't work), so I've described that below. More importantly, it is crucial to understand the difference between DLP and *file security*.

Types of Solutions Marketed as DLP

Reporting solutions are based on detecting something that *might* be data loss. For it to work, you must invest time configuring monitoring for key items. Reporting solutions are after the fact—by the time you receive information from the reporting solution, the data has already been lost. Reporting solutions can also generate large amounts of false positives by reporting normal data operations as data loss.
→ In Sum: Lots of configuration and extraneous information, doesn't *stop* theft

Network DLP solutions use signature detection to help you detect and prevent data loss. These solutions scan network traffic on the wire and block packets that match a protected signature. Network DLP solutions work well until a user decides to encrypt a file before e-mailing it, or use secure FTP to transfer it. Both of these processes damage signatures so badly that network DLP solutions cannot detect the data loss.
→ In Sum: Can be outmaneuvered by encryption or secure FTP

USB/external drive-blocking solutions can be effective at blocking one of the most convenient ways for a malicious user to steal data: copying files onto a USB drive. However, flash drive protection solutions do not protect data from other data theft methods, such as sending files through webmail like Gmail. And with Gmail, malicious users don't even need to go through the trouble of purchasing an inexpensive flash drive in order to steal valuable data.
→ In Sum: Only one of the tools needed to fight data loss

Security vs. DLP

Of course, if you look you can find ways to totally lock down files. This is more aptly referred to as *file security*, and it has two downfalls:

1. You are affecting productivity by restricting access to files people need to work.
2. You are opening loopholes when you then allow access to those files by authorized users.

For example, security is when you want to ensure no one but Executive Joe has access to the financial projections. DLP is when you want to make sure Executive Joe, now holding a pink slip, doesn't do something he isn't supposed to with those financial projections to which he has access.

Why FileSure is a game-changer:
In short, FileSure works like no other product on the market. It provides reporting when you need it, security where you need it, but it also gives you DLP like no one else can. Why? *Because FileSure can allow access to files but block the ability to steal them.*

FileSure achieves this by extending its reach to workstations and laptops and allowing you to *restrict access to a file by application*. For example, you can configure FileSure to allow ***only*** Microsoft Excel to read spreadsheet files. As simple as this approach may seem, with this one rule, you can use FileSure to stop virtually all digital data loss of Microsoft Excel files. Consider the following examples:

- Emailing spreadsheet by email client: Outlook must be able to read the spreadsheet before it attaches it. FileSure can block this Outlook read operation and prevent anyone from attaching and sending the file.
- Emailing spreadsheet by Gmail, Yahoo, or any other web-based e-mail system: the browser that the web-based email system uses, whether it be Internet Explorer, Firefox, or some other browser, must be able to read the spreadsheet. FileSure can block the read operation by the browser and prevent the thief from attaching and sending the file.
- Copying spreadsheet to flash drive: Windows Explorer must be able to read the file before it can copy it to a flash dive. FileSure can prevent Windows Explorer from reading the file, which in turn prevents Windows Explorer from copying the file to a flash drive.
- Encryption: FileSure can block the encryption program from reading and encrypting the file.

So, Executive Joe wouldn't be able to email, copy, ftp, or in any way digitally remove that financial projections file from the previous example—even though he has full access to it.

Also, FileSure also has many other useful, simple ways to help you. If needed, you could see exactly when Joe last accessed the file. You could quickly find it if he "lost" it. You could prove no one from IT has been looking at the file. You could run a pre-configured report on usage, or have one automatically sent to you on a regular basis. You could use threshold alerts to notify you if Joe suddenly did some bulk operations on his last day at work. It even protects the files on his work laptop, when it is at his home, disconnected from the network.

No other product offers this noise-free auditing and reporting or patent-pending security technology—let alone both together in one solution: **FileSure.**

Try FileSure today, and see the difference for yourself.