USB Drive File Theft Deterrence

Gene Allen, Founder; ByStorm Software

USB drive file theft has gotten a lot of press because USB devices can be so small, common, and inexpensive—and hold several GB of data. USB drives represent one of the biggest threats in file theft. But, you may think you are safe since Microsoft added native support to block writing to USB drives in Windows XP Service Pack 2.

Why you still need a file theft deterrence solution

Unfortunately, data theft is still a problem for the following reasons:

- Most users have Administrator permissions on their local computer, which allow them to simply turn off any USB write blocks configured on their computers.

  They may have done this just to copy presentation files onto a pen drive for the conference. But then they forgot to turn it back on, and now thanks to their (ex)cubicle-mate, your sales list is the property of the competition.

- Have any home users? They may be accessing the network from a personal computer, and probably don't have USB write block security turned on.

- Even with USB write blocks turned on, users can still steal data from their workstations and laptops through other methods, such as sending it through webmail, using file transfer programs, uploading it to a web site, or instant messaging it to a friend.

Do you need theft detection or theft deterrence?

There are solutions that detect theft, and then there are solutions that attempt to stop it. FileSure can succeed at both in ways no other solution can, so let's look at them one at a time.

Instead of totally locking down files (and possibly hampering workflow), maybe you just need to know if data theft has occurred so you can take actions to address it. This would be theft detection, and with most solutions, it happens way after the fact.

With FileSure, you'll benefit from auditing alerts. Get alerted to file theft *as it occurs* so you can stop the leak, take disciplinary actions toward the employee, or in a worst-case scenario alert customers of the compromise. Because FileSure works on both servers and workstations you can get the complete picture of the access—what application or user accessed the data, when, and where it went. I've provided a couple of simple ways to keep an eye out for theft with FileSure's auditing capacity in the box below, and there is also a pre-configured "Possible Theft" report you can have set up to run on a recurring basis and sent to your inbox.

All that aside, there are most likely situations where you need to stop theft before it happens, not just know about it. FileSure can also do this—in a way that doesn't stop work.

Methods for Detecting File Theft Using FileSure's Auditing Functions
Most file theft happens in bulk, and normal usage doesn't. To detect theft:

1. Watch for read operations performed on large numbers of files. With this method, you will detect only bulk operations and ignore normal, file operations. To accomplish this, configure FileSure to "send me an alert only when someone reads over 100 files in a day".

2. Hide an extra file in folders containing sensitive documents, and tell FileSure to send out an alert when the file is read. Data thieves typically steal entire folders, rather than individual files within the folder. So, your dummy file would most likely only be read if someone was copying the entire folder, and you would receive an alert. The user with normal access to this folder could then add or remove other files to this folder without their work being affected or you being unnecessarily notified.

Deterring data theft

FileSure extends its reach to workstations and laptops (even when disconnected from the network) and lets you secure files from removal without blocking normal usage access. One way to configure FileSure to achieve this is *restricting 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:

- Copying spreadsheet to a USB 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.
- 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 the file to a pen drive on a remote/home user's computer which is NOT running FileSure: FileSure can detect when a file is being accessed remotely, and deny access.

This is just one configuration of FileSure, and yet it has achieved file theft deterrence across a great spectrum of possible security threats. Of course you can also lock down files by other criteria, like users & groups, time of day, types of access, and much more. Because it also has auditing and reporting, FileSure has other useful, simple ways to help you. You can see who last accessed files and when. You can quickly find lost files and folders. You can prove no one from IT has been looking at sensitive files. You can run pre-configured reports on usage, or have them automatically sent to you on a regular basis.

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.