True File Security—Preventing Unauthorized Access

Gene Allen, Founder; ByStorm Software

Like many system administrators, you may not believe that unauthorized file access is a problem in your organization. You know that if you don't want someone to access a file, you can simply configure security on the file to block unauthorized access.

The problem you don't think is a problem

Unfortunately, the elevated permissions given to most IT staff at one time or another expose sensitive data files to unauthorized access. Whether it is via a master account, or by logging in with a Domain Admin or Master Administrator account and then using the built-in administrative shares (such as \\CEOLAPTOP\C$ in Windows), IT staff have access to sensitive files. Seem like acceptable risk? This is the kind of security breach that is the most dangerous—because it goes virtually unnoticed until it is a major problem.

- Problem one: an IT employee could cause a data breach
- Problem two: an IT employee could be blamed for a data breach they didn't commit

Let's say an IT employee who likes to play the stock market accesses files stored on a CFO or corporate attorney's computer while doing legitimate work, but notices file names suggesting a pending merger or acquisition and can't resist reading. If the IT employee acts on the information and executes large trades on the stock market, this can draw the attention of the SEC. An SEC investigation and other undesirable consequences may follow for the company.

Conversely, let's say that IT employee is you—and you were on the CFO's computer but didn't read the files and just got lucky in the stock market. How are you going to prove you didn't see them?

So, you need a security solution that will

- Block access to sensitive files—even in the face of elevated permissions
- Audit, report and alert on unauthorized accesses when they happen (or don't)

Blocking access to sensitive files

Using native Windows tools, you can block access to sensitive files, but you have the giant loophole of the local Administrator account. For example, an IT employee logging on using a local Administrator account can take ownership of a folder and quickly and easily change security settings, including the security settings initially configured to protect the files. If you want to fully protect sensitive files stored on local computers, you need an extra layer of protection that blocks access *outside of Windows*.

FileSure Defend uses its patent-pending Venn technology to stop file access on servers and workstations (and laptops, even when disconnected from the network) by using simple rules that run independently from Windows. For example, if you configure FileSure Defend to allow only

users named CEO to read spreadsheet files on the local computer, FileSure Defend blocks everyone not named CEO, including Windows Domain Admins, from accessing spreadsheet files.

You can restrict access by users, groups, time of day—even programs—to create your custom security model. FileSure Defend records any unauthorized access attempts and has simple, fast reports that prove files have not been compromised by anyone, including IT staff.

Auditing and alerting on unauthorized file access

For some limited needs, native Windows file auditing does work. However, in most cases native Windows auditing is not effective due to the large amounts of auditing noise it generates. Administrators must sift through thousands of irrelevant auditing events in order to find one event that may indicate unauthorized access.

For example, if you wanted to use native tools to audit every spreadsheet on a file server, you would have to configure file auditing on all of the drives on the server (and generate oodles of auditing data). In comparison, FileSure would intercept file operations and check to see if the file operation is related to a spreadsheet before logging an event. You just turn it on once, and it leaves you much more useful data.

And it alerts you. Email alerts, automatic recurring reports, the real-time file monitor, desktop alerts—there are many ways FileSure lets you know what is happening to the files you are concerned with.

The real challenge: even it you have a successful model for auditing on your server, extending that to workstations has been virtually impossible in the past.

In response to customer requests, ByStorm Software created FileSure for Workstations. Same simple rules and centralized control, but with a great big reach.

For example, using FileSure for Workstations, you could set up a single rule to generate an alert when someone other than the person using each computer accesses a Microsoft Office file. You can also configure the alert to display in the tray area of the user desktop. When the local user, say an executive such as the CEO, sees the alert they can immediately recognize that unauthorized file access is occurring and respond by contacting the CIO. The CIO can then immediately identify the user that is improperly accessing the CEO's sensitive files.

So, from our original example, using FileSure Defend for Workstations, the CFO's sensitive files would not have been able to be accessed even by a local Administrator, the CFO (and IT) would have been alerted if any data breach had occurred, and you could easily run a report proving that no one aside from the CFO had opened/read/copied or in any way accessed the files.

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.