FileSure

Audit. Protect. Comply.

Audit all file accesses
Protect your sensitive data
Comply with regulations and policies

THE CHALLENGE

Auditing File Access

Who is accessing your files and what is being done with them? Native-Windows file auditing is inflexible, noisy and CPU-intensive. You probably have long since abandoned attempting to audit file access even though it is a critical need.

Protecting Data from Loss

In many cases, native-Windows ACLs (Access Control Lists) and user/group permissions are too restrictive and in other cases too porous. Once a user has access to a file, they can do anything with it. Furthermore, the native-windows security model doesn't provide a way to allow access to data/files based on the application or program. It only functions on user permissions. This makes it impossible to allow access to get legitimate work done, and concurrently block web mail attach, stop copies to removable media (USB drives, DVD, CD), etc.

Complying with Regulations and Policies

Information security regulations and policies require you to document information access, control/limit access, ensure file integrity and prevent theft. Proving compliance is often painful without customizable, schedulable, and flexible data views and reporting.

"Our compliance officer values the real time display showing access of critical data and the defense rules that ensure that proprietary data remains private! It's the only thing we found that meets our needs."

- Joe McDaniel, Director of Information Services for the Arkansas Foundation for Medical Care

THE SOLUTION – ByStorm FileSure

FileSure for Windows leverages patented technology that operates outside of native-Windows ACLs to provide file access auditing, file access control, and data loss protection. FileSure complements your existing user and group permissions and eliminates the need for you to ever touch an ACL again!

- **Know what files have been accessed and what has been done with them**
- **Protect your organization from insider data theft**
- **Meet file integrity requirements**
- **Identify changes that could impact confidentiality, integrity, or availability**
- **Achieve and maintain compliance**

www.bystorm.com info@bystorm.com **+1-877-BYSTORM (297-8676)**

FEATURES

Audit File Access & User Activity	No Windows Configuration or Windows auditing/logging necessary. Does not use native-Windows Access/Audit Control Lists (ACLs).
	Collects important file access information including reads, writes, creates, deletes, renames, security setting changes and denied access.
	Control file access auditing by user, domain group membership, time of day, program used to access the file, file name, file type, file location and much more.
	Watch the watchers - Track privileged user access activity and block privileged users as desired. Overrides Windows “Take Ownership”.
	Easily respond to user issues such as accidental moves, deletes or renames.
	Tiny CPU and memory footprint; optimized for real-time processing.
	Optionally hide FileSure process and prevent service shutdown.
	Track user session state changes, remote controls (i.e. RDP), and logon/logoff activity.
Protect Data via added *"Defense in Depth"*	Simplified file security through patented FileSure security grant/deny method.
	Ensure file integrity by monitoring all file changes and protect your known executables and configurations from being changed or maliciously replaced.
	Control access to files based on user, domain group membership, time of day, program used to access the file and much, much more.
	Prevent data move/copy to removable drives (USB, DVD, CD, etc.)
	Block executables from running from USB devices (aka "switchblade attack").
	Block unauthorized web-site changes.
	Lock down your web site content and source code from being changed so hackers cannot deface your site or land malicious payloads.
	Control when web site updates can occur; prevent introduction of unintended update errors during business hours.
	Protect from malware zero-day attacks that exploit signature based systems.
Comply with regulations and security policies	Meet data access control/audit and integrity requirements for HIPAA, NERC-CIP, PCI DSS, FISMA, FERPA, 21-CFR-11, SOX, and more.
	Track privileged user file/data access activity – know what they are doing.
	Meet file integrity monitoring requirements – prove that files and configurations have not changed and know when they do change and who changed them.
	Be aware of all system-level configuration changes.
	Identify when applications change.
	Protect from malware, wrong-doers, and inadvertent violations.
	Know where your data is, who is accessing it, and what they are doing with it.
	Control access to hospital patient records, financial data, HR data, customer data, proprietary designs & intellectual property, and even military data.
	Customizable report template library provided out of the box.
	Export data to Excel, Access, and others to meet those Auditor’s “random requests”.
	Extensive self-logging of FileSure rule changes and administrator access ensures the integrity of FileSure controls.
	Console security for limited access to program configuration and settings.
	Meet log archival requirements via existing backups since FileSure logs are file-based.