FileSure

Why We’re Different

Our features work for you because they were requested by our customers.

You won’t invest time you don’t have in learning/maintaining a security system

- Installed and running in under five minutes
- Tamper-proof and compressed datastore requires no database
- No need to set up Windows Auditing, FileSure doesn’t use it
- Efficient tech support with a senior engineer and no long reporting calls
- Extensive two-minute how-to video library, learn just what you need quickly at any time

You will be proactive and efficient when auditing for security

- Interactive UI to search audit data fast, slice and dice it on the fly
- Ground-breaking Search for Trends interface: find things you didn’t know to look for
- Scheduled reports show up in your inbox and you quickly browse for issues
- Threshold alerting—real-time security from the auditing functions

You’ll stop theft not work

- Allow access but not removal or copying
- Adjust security model to thresholds such as: block bulk operations not normal behavior
- Enjoy virtually no impact on system resources
- Targeted filters ensure you only block what you need to, when you need to

Complicated security model design is now easy

- You make simple rules, FileSure follows them
- Combine common-sense filter choices to make specific security rules
- Choose from things like user and group name, type of file access (read, write, etc), type of file, location, time of day, programs accessing the file, file access behaviors, and more
- FileSure can either watch these actions or stop these actions
- Find out what’s happening real-time, or access the information later
- Centralized control and data storage for servers and workstations, easy backups

Reach places you never knew you could with a security solution

- Non windows servers, NAS, SANs
- Pen drives on PCs not even running FileSure accessing your network via remote access
- Company workstations/laptops—even when not hooked up to the network
- Watch the watchers—audit or block access by administrators
- Know what programs are being used to access files—catch or stop malware
- FileSure even audits itself by logging all changes to event log, syslog and datastore
- Block anyone from stopping the FileSure service

Use one solution for all DLP and file security compliance issues

- Meet compliance for HIPAA, PCI, FERPA, GLMA, SOX, and more
- Stop file copying or removal via USB, external drives, webmail, CD/DVDs, secure FTP, "save as" and more—on servers and workstations
- Lock down files completely if desired or necessary
- Save desired Windows Event Log entries with datastore, audit logons, logoffs and more
- Opt to auto-publish data to database for external integration (or use with web console)
- FileSure reports to syslog or event log for easy consolidation into other systems

Reclaim your time

- Web console/publishing—let others get the audit data at their desktops
- Find lost files and folders fast
- Over 40 built-in reports, just pick what you need and go
- FileSure avoids audit storms, collapses duplicate events, etc, to get targeted data
- Centralized control of applications on all workstations and central view of all data
- 5 choices for exported data type, don't convert anything

Requirements

The following table summarizes the minimum requirements—for both servers and workstations running FileSure.

Category	Minimum Requirement
Memory	512 MB
Hard disk	1 GB
Operating system	One of the following operating systems and service packs (32 and 64 bit): • Windows 2000 SP4 Rollup 1 or later • Windows XP SP2 or later • Windows 2003 SP1 or later • Windows 2008 • Windows Vista • Windows 7
Supporting software	Microsoft .NET Framework 2.0 or later

For FileSure Workstation—To use the Server FileWall® there is an OS requirement of Windows Server 2008, Windows 7, or Vista

Simple, Powerful, Versatile. FileSure.