

---

Memory	512 MB
Hard disk	1 GB
Operating system	Windows 2000, XP, 2003, 2008, Vista and Windows 7. Both 32 and 64 bit
Supporting software	Microsoft .NET Framework 2.0 or later

---

## What is FileSure?

---

**FileSure** audits user's read, write, delete, deny, rename, and security setting change activities.

**You** set rules, combining user/group, file, and/or activity criteria to audit exactly what you need.

**FileSure** works with the file system, is lightweight, and is independent of Windows Auditing.

**All** file access information is saved to compressed, encrypted log files, making the data extremely easy to back up and fast to access for internal or external audits.

**FileSure Defend** expands on this solution by allowing you to *create rules that deny access*.

## Key Features of FileSure

---

- Simple, powerful, and versatile rules-based model
- Encrypted and compressed audit logs to ensure data integrity
- Easy installation with no external database requirement or hardware
- Threshold alerting keeps you informed of data misuse without spamming you with normal file activity
- Have one of over 30 predefined reports automatically delivered directly to your inbox
- No special backup requirements
- Integration with system monitoring tools through the Windows event log
- Service availability assurance through low-impact heartbeat
- Comprehensive logging of rules-model changes
- Comprehensive file auditing, including reads, writes, deletes, renames, security setting changes and denies ("Open for" and "Content" file accesses)
- Support for exporting audited data to .CSV, XML, HTML, and Microsoft Excel and Access
- Automated publishing of auditing data to Microsoft Access if desired
- Central rule management and distribution through a master server for multi-server environments or workstation deployments
- Central auditing data storage through a master server location for multi-server environments or workstation deployments
- IT compliance for various regulations, such as HIPAA, PCI, Sarbanes-Oxley, FISMA, and GLBA
- Find exactly the data you need by using the "Forensic" screen that allows easily "slicing and dicing" of the audit logs, or by using one of the many pre-configured reports