File System Auditor™ Comparison to Snapshot and Event Log Solutions

Product Feature	File System Auditor	Event Log Analysis/Consolidation Solutions	Snapshot Solutions
Collection of Events			
How events are collected	Runs as a file system driver, collecting each file system event as it occurs.	Relies on native file system auditing via Security Log entries	Establishes a "baseline" snapshot of the file system and uses subsequent snapshots to establish differences as events.
Reliability of events collected	**HIGH** - Each event (even one as complex as a file move) is captured and reported as a single event.	**MEDIUM** – Native event logs generate excessive entries that are difficult to traverse for each file system activity, but do account for each audited action.	**LOW** – Only the sum of changes between snapshots is determined. Each file system action between snapshots is not accounted for.
Configuration of events to be audited	Established per server based on file/folder path and event type(s) to be collected. Audits for all user access.	Established per server based on file/folder path and event type(s) to be collected. Audited users/groups must be individually specified.	Established per server based on file/folder paths. Since no individual events are collected, the file system is the lowest level of auditing granularity.
Ease of establishing auditing of specific file types.	**EASY** – File System Auditor allows the inclusion and/or exclusion of files to be audited based on file extensions.	**DIFFICULT** – Establishing the auditing of specific files types would either need to be done in a one-off basis, or by placing like files in a folder and configuring auditing at the folder level.	**EASY** – Snapshot solutions generally have the ability to include/exclude files based on extension.
Storage of Events	Stored on a centralized secure SQL Server	Depends on the solution. Event analysis solutions leave the logs on each server. Consolidation solutions centrally store the events, but usually require the administrator to define exactly which event IDs are to be collected.	Usually stored centrally for analysis
Reporting			
Ease of establishing a report of specific activity	**EASY** – Using six **criteria**, administrators can generate reports on file system activity. Most importantly is the task performed – with File System Auditor the task filter lists each of the tasks in plain English (such as “File – Moved”) rather than requiring knowledge of event IDs.	**DIFFICULT** – Event analysis and consolidation solutions still require the administrator to know exactly which event IDs should be reported on and usually do not provide enough selection granularity to easily provide a precise report.	**IMPOSSIBLE** – Snapshot solutions only show a summary of changes between snapshots

Compliance

Provides a secure audit trail	**YES** – All events are secured on an SQL server	**POSSIBLY** – Event analysis solutions run against event logs which have limited security. Event consolidation solutions may provide a secure storage location and, therefore, an audit trail.	**NO** – Snapshots provide no auditing detail that can be used as an audit trail.
Applicable to **Compliance Controls** requiring the recording of all user access to protected data	**YES** – File System Auditor records all user file system activity, clearly meeting these compliance controls.	**YES** – While requiring knowledge of event entries with the possibility of delving through hundreds or thousands of entries, event logs do contain enough data to meet these compliance controls.	**NO** – snapshot solutions do not record each and every instance of user access to protected data and are therefore not truly applicable