SOLUTION BRIEF

15 USE CASES FOR FILE ACTIVITY MONITORING

stealthbits
NOW PART OF netwrix

FILE ACTIVITY MONITORING

For many organizations, monitoring file activity is challenging due to the configuration complexity and performance concerns associated with native auditing. As a result, administrators do not have a way to answer some of their most critical questions. Below are 15 real-life use cases where Stealthbits file activity monitoring solutions play a key role in solving critical change and access issues without the use of native logs.

FILE ACTIVITY MONITORING USE CASES

#	USE CASE	DESCRIPTION	STEALTHBITS FILE ACTIVITY MONITOR
1	Pre-Departure Data Exfiltration	An employee plans to leave an organization and is copying valuable data to her local drive or removable storage device to share with a competitor.	Allows admins to see what files the user has accessed and copied, delivering an audit trail with full details.
2	Unexpected Access Loss	An administrator or data owner modified permissions to data that mistakenly prevents an authorized user from accessing needed data.	Provides an audit trail showing what permissions were modified, who modified them, and the before and after values of the change.
3	Accidental File Deletions	Dealing with the accidental deletion of files is a common issue for helpdesk staff, resulting in wasted time and productivity for admins and end users.	Delivers an audit trail showing what files were deleted and who deleted them.
4	File Renames	A file gets renamed, causing confusion and leading users to believe that the file had been moved or deleted.	Offers an audit trail showing who renamed the file and to what the file was renamed.
5	Accidental File Misplacement	A user accidentally or carelessly moves data from one location to another. This prevents other users from being able to access the data.	Leaves an audit trail of all file activity, allowing admins to quickly locate files that have been moved from one location to another on monitored systems.
6	File Tampering	A user modifies the contents of a file such as spreadsheet calculations or other data.	Automatically records who modified the spreadsheet (or other file), when, and from where.
7	Administrator Activity Auditing	An administrator exploits his admin rights to access files with sensitive data.	Provides an audit trail of all administrator access, enabling the identification of privileged account misuse or abuse.
8	Sensitive Data Auditing	The law, or other regulations, require organizations to record access events to files containing sensitive data.	Works with a DLP or sensitive data discovery solution to provide an audit trail of access events to files with sensitive data. *StealthAUDIT can do also.

#	USE CASE	DESCRIPTION	STEALTHBITS FILE ACTIVITY MONITOR
9	Ransomware Detection	Large numbers of files accessed and modified in a short time period can be indicative of crypto ransomware.	Combines with a SIEM solution like Splunk or QRadar to send an alert when a large number of file access and modification events occur. *StealthAUDIT or StealthINTERCEPT can also do.
10	Data Sabotage	File deletions (individually or in bulk) can indicate attempts to sabotage data or individuals.	Provides an audit trail of all file deletions within an environment, allowing administrators to catch perpetrators and stop them from deleting data.
11	Stale File Clean-up	Knowing which files are being actively accessed helps identify stale data for removal from active management, reclaiming storage space and reducing an organization's risk surface.	Allows organizations to identify stale data and files that have not been modified or accessed within a designated timeframe.
12	Data Ownership	The ability to understand who accesses data, how often, and what actions they perform enable organizations to calculate data ownership, especially in the absence of quality file metadata.	Provides administrators with the ability to collect and analyze file activity, metadata, and user attributes to easily calculate data ownership.
13	Data Access Clean-up	Knowing who is using their access privileges and what types of operations they perform helps reduce elevated access privileges that aren't needed and remove access that isn't be utilized.	Enables administrators to understand who is using their access and what they are using it for so they can implement a least privilege access model.
14	Group Membership Formulation	Understanding who is using their access privileges, what types of operations they perform, and other attributes about users like department and location helps to group users into like roles to ease the burden of access management.	Permits administrators to collect and analyze the data needed to properly mine roles and streamline access management.
15	Open Access Remediation	Knowing who is leveraging their access privileges and what types of operations they perform helps create the right group memberships and data access privileges when closing down open access.	Analyzes the activity within open resources like file shares and SharePoint sites, calculates and implements resource-based groups and their memberships to shut down open access and secure critical data resources.

NEXT STEPS

Schedule a demo
stealthbits.com/demo

Download a free trial
stealthbits.com/free-trial

Contact us
info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix