stealthAUDIT

STEALTHAUDIT® FOR FILE SYSTEMS

Comprehensive file system security and governance

stealthbits
NOW PART OF netwrix

Every day, end users create files in the form of documents, spreadsheets, presentations, and hundreds of formats, and store them on Network File Shares. Managing and protecting this unstructured data presents significant challenges to organizations of every size. Why?...

1. **There's a lot of it** – Statistics show that unstructured data makes up >80% of all digital information in an organization.
2. **It's very difficult to keep track of it all** – It is constantly being created and updated by employees every day and stale data is not being routinely removed.
3. **It often contains sensitive data** – Files can contain virtually anything, including Personally Identifiable Information (PII) about patients and customers.

While the creation and updating of these documents is in the hands of the end-user, the act of protecting and securing access to this data falls into the hands of IT. Strict audit regulations like PCI-DSS, HIPAA, SOX, GDPR, and others, require organizations to know who has access to certain types of data, what they're doing with it, and how users were granted that access. Couple that with the threat of insider theft and data loss, as well as common, high-risk conditions like Open Access or Broken Inheritance in the File System, and it's clear today's IT administrators need help.

StealthAUDIT FOR FILE SYSTEMS

StealthAUDIT for File Systems allows organizations to satisfy stringent compliance requirements and reduce their risk exposure by enabling complete and automated access governance controls over unstructured data residing in the File System, whether on-premises or in the cloud.

REDUCE RISK

Without a proper security model in place, organizations are prone to a number of risks including insider threats, sensitive data loss, and unwanted conditions like Open Access. StealthAUDIT provides organizations with an accurate, up-to-date view of where risks lie and powerful workflows to remediate them, including sensitive data classification and Open Access remediation.

EMPOWER DATA OWNERS

Addressing access risks is important, but maintaining proper access over time means involving those outside IT with the right context to make decisions. To properly manage data, owners must be identified and enabled to control access to their data. StealthAUDIT provides proven ownership workflows to identify probable owners and the ability to confirm ownership to be sure the right people have been put in charge of important access decisions.

FULFILL AUDIT REQUIREMENTS

Addressing access risks is important, but maintaining proper access over time means involving those outside IT with the right context to make decisions. To properly manage data, owners must be identified and enabled to control access to their data. StealthAUDIT provides proven ownership workflows to identify probable owners and the ability to confirm ownership to be sure the right people have been put in charge of important access decisions.

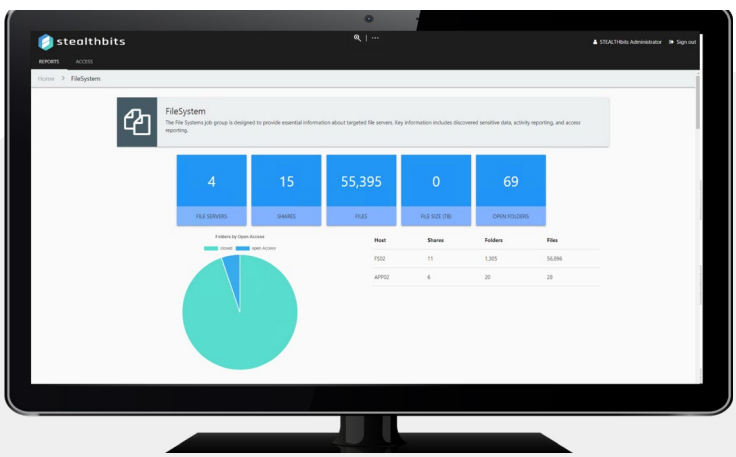
INTEGRATE WITH CURRENT APPLICATIONS

StealthAUDIT is highly extensible and offers seamless integration capabilities with third-party and home-grown applications. StealthAUDIT was built with an open architecture, meaning the data is stored in a highly optimized SQL database. Integration approaches are well-documented to ensure customers can truly get the most value out of the data.

KEY FEATURES

Permissions Auditing – Gather full permission details across every share, folder, and file, highlighting toxic conditions such as Broken Inheritance, Historical and Unresolved SIDs, Direct User Permissions, and Open Access.

- **Permissions Auditing –** Gather full permission details across every share, folder, and file, highlighting toxic conditions such as Broken Inheritance, Historical and Unresolved SIDs, Direct User Permissions, and Open Access.
- **Effective Access Calculation** – Gather all user permissions to shared folders and correlate the information with Active Directory, system-level rights, and policies to effectively determine each way a user can access a given resource, as well as the level of permission each access avenue grants.
- **File Metadata Collection** – Understand everything there is to know about every file, including file types, attributes, owner info, and even tags applied by other products or processes.
- **Probable Owner Identification** – Identify the Most Probable Owner of every share or folder via multiple layers of context, including common managers, content creators, and most active users.
- **Activity Monitoring** – Monitor activity across Windows and NAS File Systems for complete insight into which files, folders, and shares users are accessing, as well as what they're doing with the data.
- **Sensitive Data Discovery** – Determine where sensitive data resides to understand where access risk exists in order to strengthen your Data Loss Prevention initiatives.
- **File Classification** – Automatically tag files with their associated classifications in bulk, enriching document metadata and increasing the efficiency and effectiveness of other technology systems.
- **Governance Workflows** – Easily implement governance workflows like Entitlement Reviews and Self-Service Access Requests to safely provide data custodians the ability to control access to the data they own and end-users the ability to request access to the data they need.
- **Preconfigured Reporting** – Leverage dozens of preconfigured reports aligning to critical file security concepts, including Open Access, permissions violations, content, activity, ownership, sensitive data, clean-up, and more.
- **Broad Platform Support** – Target on-premises, hybrid, and cloud-based file system platforms including Windows, Unix, Linux, NAS (e.g. NetApp, Dell EMC, Hitachi), and Nasuni.
- **Scoping and Event Suppression** – Granular and flexible scoping and event suppression controls ensure only the data needed is actually collected, keeping audit trails neat and clean for human and machine consumers alike.



TOP USE CASES

- **Open Access Reporting & Remediation** – Quickly assess the open access in your organization to understand what is over-exposed and at risk, including file shares on-premises and in the cloud. Intelligent remediation workflows ensure that access is fixed safely and effectively.
- **Access Transformation** – Automatically assign a least privilege model to your file shares that can be used to govern access going forward. Do all this without interrupting regular business operation and user access to the files and folders they use the most.
- **Storage Reclamation** – Automatically identify and move stale or sensitive data in efforts to reduce storage costs and minimize data risks.
- **Forensic Investigation** – Easily browse all file activity to answer otherwise difficult questions like who accessed a file, when, from where, and what type of operation they performed.
- **IAM Integration** – Integrate unstructured data into leading IAM frameworks (IBM, Microsoft, RSA, Saviynt, and others) and home-grown systems, to provision, review, and revoke access to file share 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.