stealthAUDIT

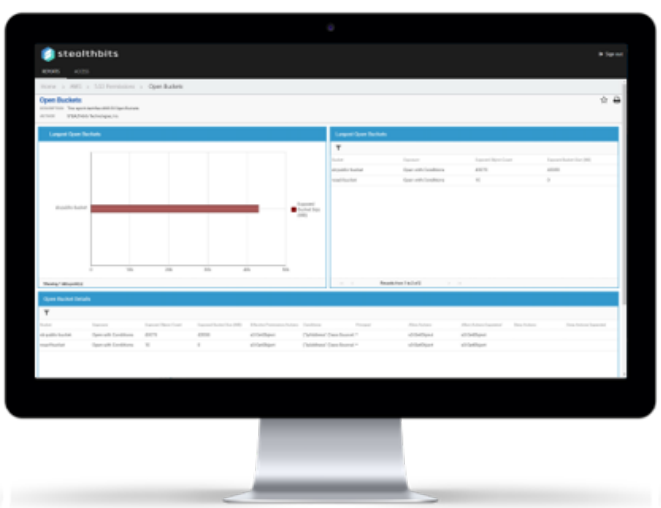
STEALTHAUDIT® FOR AWS

Comprehensive AWS IAM and S3 auditing, monitoring, and governance for security and compliance

stealthbits

Amazon Simple Storage Service (S3) has quickly become one of the world's most popular object storage platforms, housing data for thousands of organizations around the globe. Essentially the equivalent of a share or folder within a traditional file system, S3 "buckets" have become enormously popular as a less expensive, infinitely scalable storage option for file data within the cloud. However, user error with regards to complex and confusing access management controls and other factors have left large amounts of sensitive information within S3 buckets exposed, in some cases openly accessible to anyone with an internet connection, leading to data breach and concerns regarding the ability to secure data properly within the S3 ecosystem.

StealthAUDIT for AWS allows organizations to secure their S3 repositories through proactive and automated insight into where their risks exist. With robust, preconfigured reporting around AWS IAM and S3 Users, Groups, Roles, Policies, Permissions, Activity, and Content, users not only get greater visibility into the security stature of their S3 environment, but more cost-effective, efficient scanning of sensitive data in comparison with native toolsets.



KEY FEATURES & BENEFITS

Automated Data Collection & Analysis

StealthAUDIT's preconfigured AWS solution automates all aspects of data collection and analysis, including scan configurations, audit and report scheduling, publishing, and delivery, notifications, and more.

Preconfigured Reporting

Preconfigured reports focused on Users, Groups, Roles, Policies, Permissions, Activity, and Content make it easy to get instant and long-lasting value, while also making it easy to customize existing reports or create entirely new reports aligned to organization-specific requirements.

Interactive Search

StealthAUDIT's powerful Access Information Center (AIC) provides users with the ability to search and browse all S3 permission, activity, and content details with ease. User and Group access details are represented in easy-to-understand, normalized views alongside any other platform information that has been collected across the dozens of unstructured and structured data repositories, directories, and systems StealthAUDIT supports.

Cost-Efficient Sensitive Data Scanning

StealthAUDIT's sensitive data scanning architecture can produce cost savings of up to 98-99% in comparison with native AWS facilities, making it possible to scan S3 repositories of virtually any size at high frequency and low cost.

StealthAUDIT FOR AWS DELIVERS

- **S3 Permissions Assessment** – Obtain detailed information and views on permissions assigned to AWS S3 Buckets, highlighting specific threats like "Open" Buckets and Broken Inheritance.
- **S3 Sensitive Data Discovery** – Audit and analyze S3 Bucket content and object details, including the identification of sensitive content such as Credit Card and Social Security numbers, personal health information, and dozens of other types of Personally Identifiable Information (PII). Also search for custom criteria specific to an organization such as Employee ID numbers, trade secrets, product formulas, and more.
- **S3 Activity Analysis** – Collect, analyze, and report upon all activity events stored in CloudTrail logs including information such as the user performing the activity, their role, time of access, the accessing user's IP address, and other important details.
- **Root Account Security** – Audit and analyze AWS root accounts for important security settings, including access keys and MFA configuration.
- **IAM User Security** – Audit and analyze AWS IAM user accounts which have not rotated their access keys for an extended amount of time or have never used it, as well as the MFA status of each AWS user.
- **Inactive Access** – Identify user accounts which no have not logged into AWS for an extended amount of time or have never logged in. A user account is considered stale if the last logon is over 60 days ago or the password has never been used.
- **Group Membership Analysis** – Understand group memberships and obtain summarized views on the policies assigned to each group.
- **Stale Group Conditions** – Identify group conditions that could indicate staleness such as Orphaned Groups that have no policies assigned to them and Empty Sensitive Security Groups and Groups with Stale Membership that are no longer needed.
- **Sensitive Security Groups** – Track the membership of groups that have sensitive or higher-level security policies assigned to them for security and compliance.
- **IAM Roles** – Inventory IAM roles, along with associated details and configurations.
- **IAM Policy Analysis –** Inventory and analyze all AWS policies (AWS and Custom Managed, and Inline), as well as Duplicate and Unused policies that can be consolidated or removed.

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.