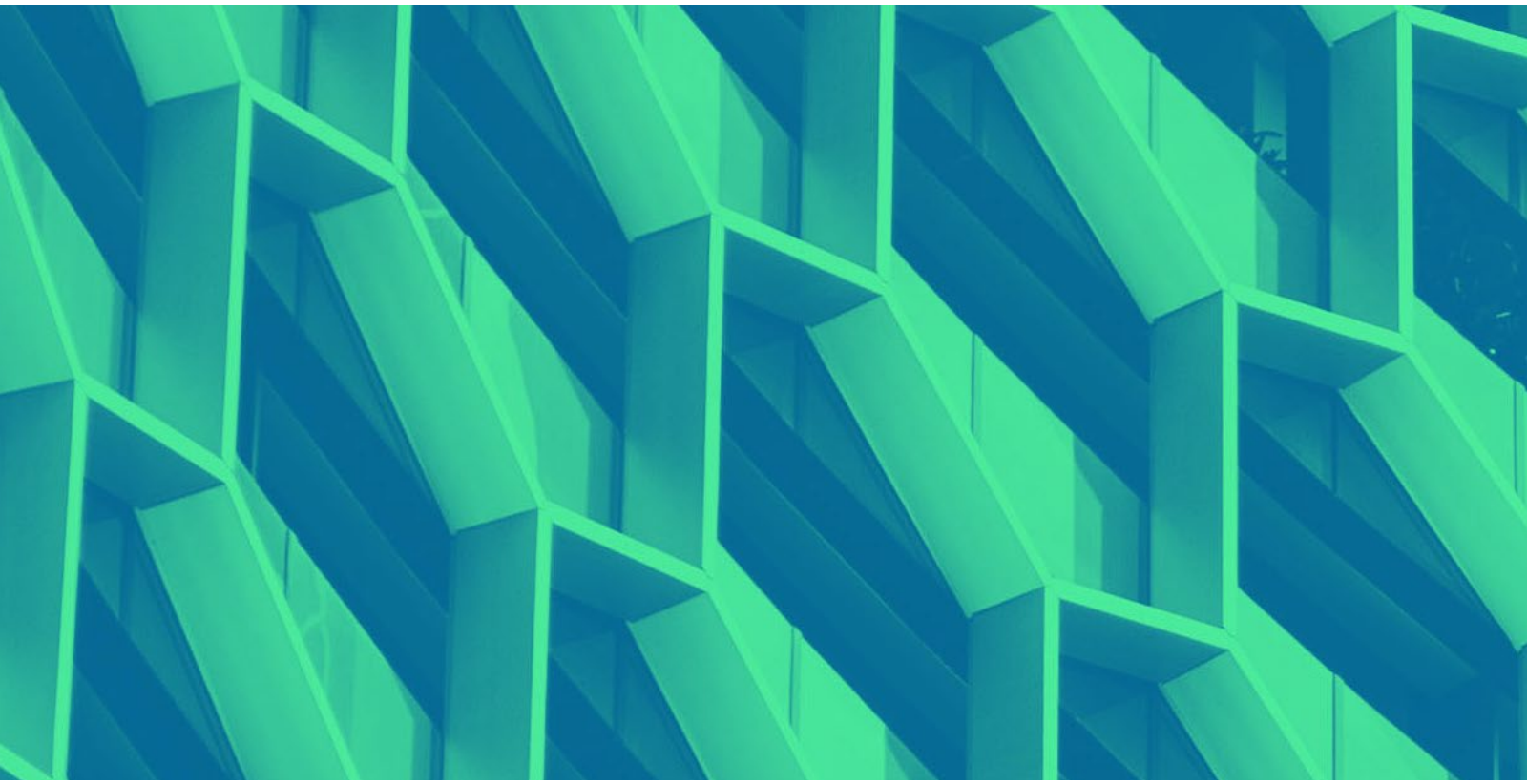
stealthbits

NOW PART OF netwrix

BUYER'S GUIDE

DATA ACCESS GOVERNANCE

Selecting the Right Solution to Protect Structured, Unstructured and Sensitive Data



ABOUT THIS GUIDE

Adopting a Data Access Governance (DAG) strategy will help any organization achieve stronger security and control over their Structured and Unstructured Data. Without such a strategy, companies are left highly exposed to growing risks of data breaches and insider threat. This guide is designed to assist organizations in understanding these risks and choosing the best available solution. The information contained within this guide can be used to create a request for information (RFI) or request for proposal (RFP) for evaluating Data Access Governance products.

CURRENT STATE OF DATA ACCESS GOVERNANCE

The goal of Data Access Governance solutions is to help organizations understand and secure their Structured and Unstructured Data. Structured data is contained in databases and business applications and user access is typically provisioned to these systems by an Identity and Access Management (IAM) platform. Unstructured Data includes the documents, spreadsheets, presentations and other files created by end users, and often results when business users export data from structured systems for further analysis and presentation. These files are typically stored in shared folders, network filers (e.g. NetApp or EMC), SharePoint, and cloud repositories like Box, DropBox and Amazon S3. Most importantly, these files often contain sensitive information – making their security a concern for every organization.

While most businesses recognize the importance of controlling access to this data, few have managed to do so. However, many companies have been able to implement proper security and processes around access to their structured application data (e.g. application access) as IAM solutions have matured and been widely adopted. The expansion of these controls into the Unstructured Data world is a natural progression, but with Data Access Governance comes a series of new challenges. How do you implement controls across data so distributed? With so many end users constantly creating and modifying the data in so many locations, it seems almost an impossible task to make sure users only have access to data they need.

Failure to address these challenges can lead to significant risk to your organization, including:

- **Data Breaches** - Data breaches are one of the most common and costly threats facing organizations of all sizes. The key to minimizing date loss due to these threats is to understand where the greatest risk lies in your organization. To obtain this view, it is critical to properly govern data access so that sensitive content is identified and handled with a higher priority than non-sensitive data.
- **Insider Threat Attacks** - One of the largest and growing threats to organizations today is the rogue Local Administrator, and the fear of what his or her elevated access rights can do to the organization. The Local Administrator job title made international headlines in 2013 due to the Edward Snowden/NSA case. Edward Snowden was an NSA contractor who was able to access extremely sensitive information due to his elevated access rights. Without an effective system in place to determine who has Local Administrator/Privileged Access Rights across your organization, and to monitor what these individuals are doing with that elevated access, you will be open to this kind of attack. And the damages caused to Brand, Reputation, and Revenue can be severe.
- **Excessive Access** - But it's more than just administrators. When first starting, employees are provisioned to systems and are given access to data that they need to do their job. Over time, these employees accumulate additional privileges as they work on projects or are promoted into new jobs and transfer departments. Rarely if ever are their privileges taken away. After all, they are long time trusted employees. If an attacker can compromise their account, they would have the same access as the long time employee, which represents elevated risk to your organization.

- **Open Shares** – If you have open shares with sensitive data sitting on them, anyone can be a threat regardless of how much or how little access they have.
- **Audit & Compliance** – Most organizations are faced with complex, constantly evolving audit requirements. Complying with these audit requirements, as well as an organization's own internal standards, can be a constant struggle specifically when dealing with Unstructured Data due to its decentralized storage and security. The ability to understand who has access to this data, how they got it, and the ability to secure it properly is necessary to satisfy audits and ensure compliance with regulatory standards.

The landscape of Data access is constantly changing and evolving, and can no longer be managed manually. In order to stay ahead of these threats it is critical to choose the right Data Access Governance solution and put a proper implementation plan together. The remainder of this document will provide important use cases and product features that should be evaluated when making this decision to ensure your organization can adequately mitigate these risks.

IDEAL DATA ACCESS GOVERNANCE

Faced with these challenges, the right strategy must involve gaining visibility immediately while working towards a self-sustaining system in the long-term. Some important factors to keep in mind when building a successful DAG strategy include:

Get Short-Term Wins, Plan for Long-Term Success

Many times customers take on too much too soon when it comes to their Data Access Governance strategy. A successful plan will focus on gaining short-term wins first, and growing into a more complete solution over time. Short-term wins include achieving audit and compliance goals of being able to quickly report on who has access to what data and track activity of users so there is an audit trail for changes that occur. Longer term, periodic access reviews must be implemented to ensure that the environment remains in compliance.

Get the Data Custodians Involved

It is unrealistic to expect security and operations teams to take on the task of securing Unstructured Data access. Not only is there too much data and constant change, in most cases they cannot answer the foundational questions of access governance such as "Who should have access to this data? And "Do we still need this data?" A successful strategy will involve business owners who are responsible for the data and enabled to take control of reviewing, revoking and approving access to this data.

Define Policies and Enforce Them

Often what will prevent successful implementation of a Data Access Governance solution is the failure to define policies around access to data. This involves collaboration between lines of business, security, operations and compliance teams. Many companies know what problems they want to look for, but don't consider how to handle the problems once they are identified. Once policies and remediation strategies are agreed upon, the Data Access Governance solution can provide the data collection, analysis and remediation to enforce these policies.

Complement IAM, Don't Duplicate It

A Data Access Governance strategy should complement any existing Identity & Access Management solutions in place, not duplicate them. Access to Structured and Unstructured Data may pose different challenges as far as implementation, but the goals are the same. This integration does not necessarily need to happen immediately, but the long-term plan of integrated governance across structured and unstructured data should be considered.

COMMON USE CASES

As you evaluate Data Access Governance solutions, it is important to evaluate all available features. However, this should not prevent you from losing sight of the larger workflows and projects that these features can be used to accomplish. These are some common workflows that should become part of Data Access Governance deployments.

Open Access Remediation

In an ideal situation, users are granted access to data they need based on their job function, geographic location, organizational structure or other factors that contribute to that user's identity. Open File Shares and SharePoint sites are locations that are often improperly secured so that anyone within the organization can access the data stored within them, regardless of their identity. When permissions are granted to "Everyone" or "Authenticated Users", serious security issues can arise and the best-laid DAG strategy can become irrelevant. It is critical to identify these open access locations and close them down to put them under the proper control of a Data Access Governance solution.

Privileged Access Control

One of the most common causes of data breaches occurs when users take advantage of their administrative access to collect sensitive information from documents stored on systems they have elevated rights to. Nearly all organizations have too many users with privileged access to their business applications, File Systems and SharePoint sites, and no visibility into what these users are doing with those privileges. Restricting and managing privileged activity is critical.

Self-Service Access Provisioning

Just as data is in a constant state of growth, access to that data is also constantly changing. Every day users need new access rights to effectively collaborate with colleagues, and the granting of these rights typically falls on IT personnel. Enabling business owners to approve requests for access to applications, file shares and SharePoint sites can alleviate this burden from IT. Moreover, this allows the decisions regarding who should have access to data to be made by the right people who actually understand the data.

Entitlement Reviews

Enabling business owners and data custodians to review who has access to their data and recommending changes can provide powerful results in the effort to secure data access. Most organizations find that far too many people have access to data, usually from past roles and responsibilities. Identifying and revoking this access with an automated Entitlement Review process can help accomplish the principal of least privilege.

Active Directory Clean-up

Active Directory is the directory most often used to provide access to Structured and Unstructured Data. Most organizations struggle to control their Active Directory groups and how those groups are used to grant access to data. Gaining visibility into Active Directory groups, where they are used and what access they provide is a critical step to implementing a proper Data Access Governance solution.

SELECTING THE RIGHT SOLUTION

Making sure a Data Access Governance product aligns with business goals is important when choosing the right solution and ensuring a successful project. Evaluation of the following features and capabilities will help guarantee the chosen solution can address these goals.

Permissions and Access (Continued)	Stealthbits	Other Vendor	Other Vendor
Does the solution support scanning of permissions for Windows Servers ?	YES		
Does the solution support scanning of permissions for Network-Attached Storage (NAS) Devices including NetApp and EMC Isilon?	YES		
Does the solution support scanning of permissions for UNIX and Linux machines?	YES		
Does the solution support scanning of permissions from SharePoint 2010, 2013, 2016 & 2019 farms?	YES		
Does the solution support scanning of permissions from SharePoint Online?	YES		
Does the solution support scanning of permissions from OneDrive?	YES		
Does the solution support scanning of permissions from SQL Server and Azure SQL?	YES		
Does the solutions support scanning of permissions from Oracle?	YES		
Does the solution support real-time alerting and rollback of high-risk permission changes?	YES		
Can the solution identify folder and share permissions?	YES		
Does the scanning collect local groups and their memberships such as the local Administrators group?	YES		
Can the product determine the "effective access" by evaluating all permissions set on the share and the folder and expanding all levels of domain and local groups?	YES		
Can the product determine the "effective access" to a SharePoint resource (site, list, library, OneDrive etc.) by evaluating all permissions set on the resource as well as all web application policies and Site Collection Administrators and expanding all levels of nested domain and SharePoint groups?	YES		
Can the solution identify Shadow Access which could be used by attackers to move laterally, escalate privileges, compromise entire domains, and gain access to sensitive data?	YES		

Permissions and Access (Continued)	Stealthbits	Other Vendor	Other Vendor
Will the solution easily identify all resources where a particular user or group has effective access as well as direct permissions?	YES		
Does the product have the ability to identify "open" resources that trustees including Everyone, Authenticated Users, Domain Users and via Anonymous Access Links, have access to?	YES		
Will the solution identify permissions that should be removed or are "toxic" such as permissions granted directly to user accounts, unresolved SID permissions, stale/disabled user permissions, and permissions granted to "high risk trustees" such as Everyone?	YES		
Does the product support bulk remediation actions?	YES		
Can the product apply a new permissions model across all shares?	YES		
Can the product automatically create and populate new resource-based security groups?	YES		
Can the product apply those groups to ACLs and remove direct permissions?	YES		
Can the product remove stale users and data as defined by company policy?	YES		
Does the product maintain an audit history of all remediation actions?	YES		
Can the product simulate changes, such as changing membership of an Active Directory group, to provide insight into the impact the change will have before making the change?	YES		
Will the solution easily display locations where inheritance of permissions has been broken and identify the access rights that have been changed from the parent to the child?	YES		
Can the product collect Exchange permissions for all mailboxes?	YES		
Can the product collect Exchange permissions for public folders?	YES		
Can the product audit Microsoft Teams sites?	YES		
Can the product determine permissions on Amazon S3 buckets?	YES		

Sensitive Data Discovery	Stealthbits	Other Vendor	Other Vendor
Is the solution capable of scanning within content of files to determine the existence of sensitive data such as PII? (e.g credit cards, passport numbers, SSNs etc)	YES		
Is the solution capable of scanning for sensitive data within image files using Optical Character Recognition (OCR)?	YES		
Can the solution scan Exchange emails for sensitive data?	YES		
Can the solution scan Exchange Public folder contents for sensitive data?	YES		
Can the solution scan SharePoint Online, OneDrive and Teams for sensitive data?	YES		
Can the solution scan SQL Server and Azure SQL for sensitive data?	YES		
Can the solution scan Oracle for sensitive data?	YES		
Can the solution scan Amazon S3 buckets for sensitive data?	YES		
Can the solution scan NFS (Unix & Linux) file systems for sensitive data?	YES		
Does the product support customizable keyword and expression-based pattern definitions of sensitive data?	YES		
Can the product alert and take action on patterns of sensitive data access via defined criteria?	YES		
Can the product alert on abnormal sensitive data access?	YES		
Can the solution automatically update file metadata tags to mark the level of sensitivity or denote the type of content contained in the file?	YES		
Can the product integrate with 3rd party data classification solutions to read applied metadata tags or feed context about legacy data for automated classification?	YES		
Can the product scan and report on Microsoft Azure Information Protection (AIP) labels?	YES		

Active Directory Reporting	Stealthbits	Other Vendor	Other Vendor
Does the product collect information about Users, from multiple Active Directory forests and domains into a single repository for reporting?	YES		

Active Directory Reporting	Stealthbits	Other Vendor	Other Vendor
Does the product collect information about Groups, from multiple Active Directory forests and domains into a single repository for reporting?	YES		
Does the product collect information from Computers, from multiple Active Directory forests and domains into a single repository for reporting?	YES		
Does the product collect information about Group Membership, from multiple Active Directory forests and domains into a single repository for reporting?	YES		
Can the product report on AD permissions for users, groups, computers, sites, OUs and domains?	YES		
Can the product determine the effective membership of a group by recursively expanding nested groups?	YES		
Can the product determine 'Shadow Access' to resources through permissions that grant elevated rights that can be leveraged to move laterally or escalate privileges during an attack.	YES		
Will the solution identify "toxic conditions" for groups that may cause security and access issues such as circularly nested groups, large and deeply nested groups and stale groups?	YES		
Will the solution identify "toxic conditions" for users that may cause security and access issues such as circularly nested groups, large and deeply nested groups and stale groups?	YES		
Can the product provide insight into changes that are taking place within Active Directory that affect access without reading logs or installing an agent on domain controllers?	YES		
Can the solution detect and alert on abnormal AD activity and changes based on User behavior?	YES		
Does the solution support scanning for weak AD passwords?	YES		

Remediation	Stealthbits	Other Vendor	Other Vendor
Does the product support remediation of access issues such as open access across File Systems?	YES		
Does the product support remediation of access issues such as open access across all versions of SharePoint (Server and Online)?	YES		
Does the product support remediation for Exchange mailbox and public folder permissions and content?	YES		

Remediation	Stealthbits	Other Vendor	Other Vendor
Can the product report on AD permissions for users, groups, computers, sites, OUs and domains?	YES		
Does the product survey data owners before remediation to get approval for recommended changes?	YES		
Does the product support both on-demand or scheduled re-mediation?	YES		
Is the solution capable of performing remediation across multiple distributed Active Directory domains from a single deployment?	YES		
Can the product roll-back actions taken?	YES		
Will the product support one-at-a-time remediation actions?	YES		
Will the product support bulk remediation actions?	YES		
Does the product maintain an audit history of all remediation actions taken?	YES		
Can the product simulate changes, such as changing member-ship of an Active Directory group, to provide insight into the impact the change will have before making the change?	YES		

Data Ownership	Stealthbits	Other Vendor	Other Vendor
Does the product support ownership of shared folders?	YES		
Does the product support ownership of SharePoint sites in-cluding OneDrive and Teams?	YES		
Does the product support ownership of Active Directory groups?	YES		
Will the product identify the most probable owners of re-sources including shared folders and SharePoint sites based on multiple criteria including activity, content ownership and management hierarchy?	YES		
Can the product survey data owners to confirm their responsi-bilities and track their responses?	YES		
Does the solution offer data owners a portal to report on their owned resources and investigate access and activity as well as modify access?	YES		

Entitlement Reviews	Stealthbits	Other Vendor	Other Vendor
Does the solution offer entitlement review / attestation workflows for access to resources?	YES		
Does the solution offer entitlement review / attestation workflows for permissions to resources?	YES		
Does the solution offer entitlement review / attestation workflows for Active Directory group membership?	YES		
Does the solution offer entitlement reviews for sensitive data that has been identified.	YES		
Does the solution leverage data owners to make entitlement decisions, getting the IT team out of the process?	YES		
Will the workflow allow data owners to make changes that they see fit?	YES		
Can the product recommend changes to the owner based on metrics such as activity?	YES		
When reviewing access to a resource, will the product be intelligent enough to automatically include child resources where permissions have been changed in the review so that those changes will not be missed?	YES		
Does the product provide flexible remediation options allowing the owner to either make changes directly from the review, or to have an approval workflow where the recommended changes are first reviewed?	YES		
Can the product offer customizable email messages notifying owners when reviews are launched that require their input?	YES		
Does the product support recurring reviews?	YES		
During recurring reviews, can the solution intelligently inform the owner of changes that have taken place since the last review and only require the owner to attest to those changes?	YES		

Self-Service Access	Stealthbits	Other Vendor	Other Vendor
Does the solution offer a workflow to allow business users to request access to file shares, SharePoint sites and Active Directory groups?	YES		
Will the solution automate the process of seeking approval for the request from the owner of the resource?	YES		

Self-Service Access	Stealthbits	Other Vendor	Other Vendor
Is the solution capable of committing the requested change, allowing access to be granted automatically upon approval by the owner?	YES		
Does the workflow enable both the owner and the requester to be able to track all pending and past requests?	YES		

Product Architecture	Stealthbits	Other Vendor	Other Vendor
Does the solution offer a workflow to allow business users to request access to file shares, SharePoint sites and Active Directory groups?	YES		
Will the solution automate the process of seeking approval for the request from the owner of the resource?	YES		
Can the product leverage the following scanning approaches?	YES		
Agent based?	YES		
Agentless?	YES		
Applet-based?	YES		
Proxy scanning?	YES		
Does the product support scheduled scans?	YES		
Can scheduled scans be configured to run during a time-window?	YES		
Will active scans be "paused" at the end of the time window so the scan can be resumed during the next scanning window?	YES		
Does the product provide documentation on its database schema?	YES		
Does the product provide a REST API for easy integration with third party platforms?	YES		
Does the product offer integrations into the leading IAM solutions to ensure the data gathered can be reused if needed?	YES		
Does the product offer integrations into home-grown IAM solutions to ensure the data gathered can be reused if needed?	YES		
Does the product offer integration with SIEM platforms?	YES		
Does the product support custom authoring of Reports?	YES		

Product Architecture	Stealthbits	Other Vendor	Other Vendor
Does the product support custom authoring of Data collection routines?	YES		
Does the product support custom authoring of Data analysis?	YES		
Does the product support custom authoring of Remediation jobs?	YES		
Does the product support data export to Microsoft PowerBI?	YES		
Does the product support data export to Tableau?	YES		
Does the product support the import of data from other non-standard data sources?	YES		
Does the product support data export to third party platforms? e.g. SIEM?	YES		
Can the product scan unsupported data sources using available REST APIs?	YES		

INTRODUCING StealthAUDIT FOR DATA ACCESS GOVERNANCE

With StealthAUDIT for Data Access Governance, you can pass compliance regulations and reduce your organization's risk exposure by enabling complete and automated access governance controls over structured and unstructured data residing in Applications, Databases, File Systems and SharePoint sites. StealthAUDIT was designed with a scalable, flexible, and agent-less architecture that allows your organization to meet present and future requirements without depleting your budget.

WHY STEALTHBITS?

Stealthbits is the premier vendor of Data Access Governance solutions, providing all the necessary features with the ability to scale to the largest environments. Customers choose Stealthbits over the competition for a variety of reasons, including:

Scalability

Stealthbits products are designed with the largest, most complex enterprise customers in mind. This is particularly critical when it comes to Unstructured Data, which can require insight into trillions of permissions spread across thousands of servers in dozens of data centers joined to multiple Active Directory forests. Stealthbits offers a unique architectural approach to centralize the collection of this data while minimally impacting the performance of the systems on which the data resides.

Open Architecture

StealthAUDIT was designed with integration in mind, which is critical for a Data Access Governance product. Stealthbits offers a variety of ways to extend and integrate with the solution. This will commonly be used to take the permissions and activity data and share it with other applications such as IAM, or to ingest additional data such as HR feeds.

Industry Experience

Stealthbits has been helping organizations implement Data Access Governance products across all verticals and organization sizes. With this extensive experience, the Professional Services team at Stealthbits can offer assistance ranging from training, consultation, product customizations and managed services to help customers design and implement a successful Data Access Governance deployment.

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