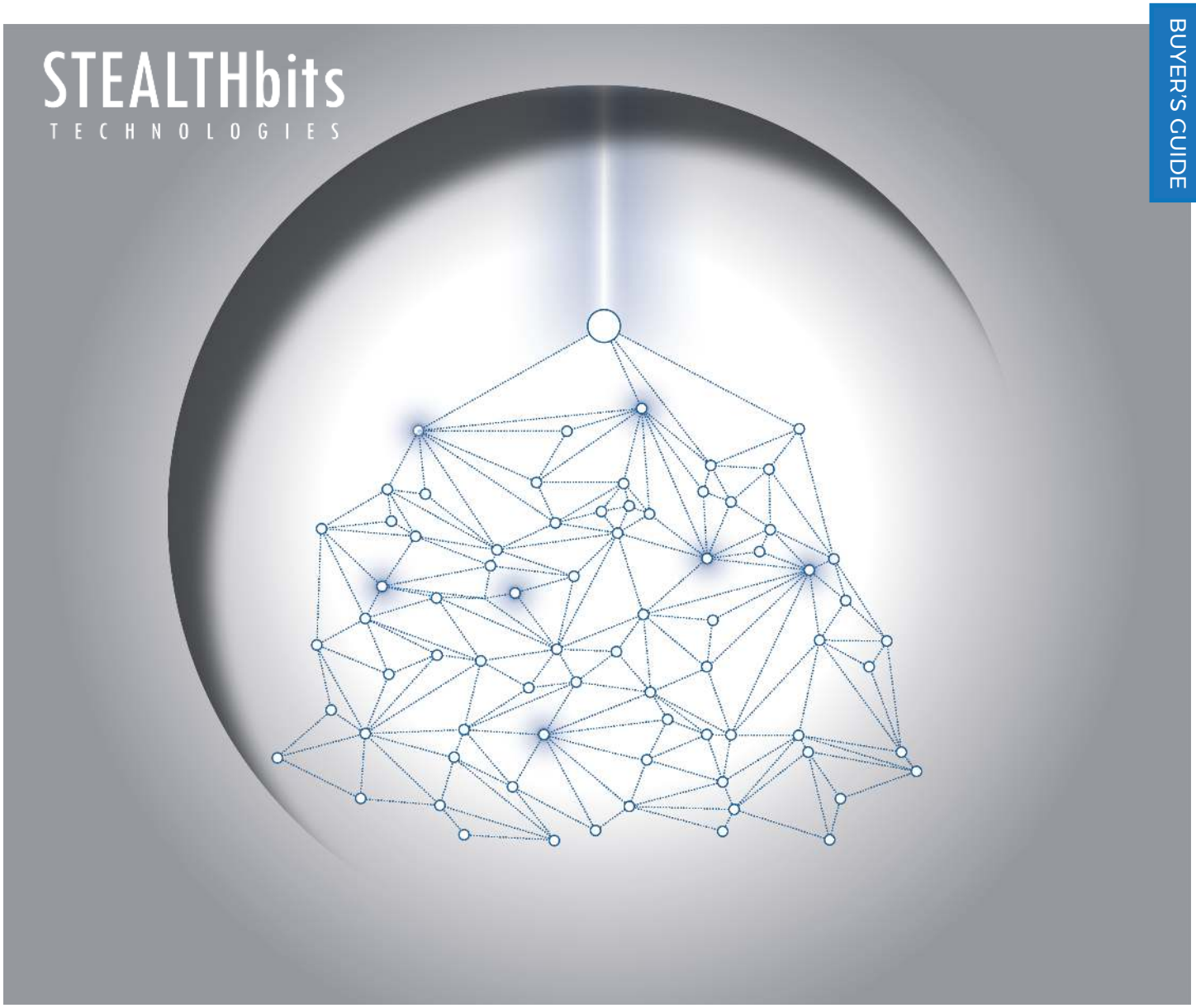
STEALTHbits
TECHNOLOGIES

BUYER'S GUIDE



DATA ACCESS GOVERNANCE

Selecting the Right Solution to Protect Unstructured and Sensitive Data

TABLE OF CONTENTS

ABOUT THIS GUIDE

Adopting a Data Access Governance (DAG) strategy will help any organization achieve stronger security and control over their Unstructured Data. Without such a strategy, companies are left highly exposed to growing risks of data breaches and insider theft. 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 in creating a request for information (RFI) or request for proposal (RFP) and 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 Unstructured Data. Unstructured Data includes the documents, spreadsheets, presentations and other files created by end users. These files are typically stored in shared folders, network filers (e.g. NetApp or EMC), SharePoint, and cloud repositories. 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 Identity and Access Management 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 preventing these threats is to understand where the greatest risk lies in your organization. To obtain this view, it is critical to properly govern data so that sensitive content is identified and handled with a higher priority than non-sensitive data.

- Insider Theft 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 will open the door to Insider Theft Attacks, like the one suffered by the NSA. And the damages caused to Brand, Reputation, and Revenue can be severe. But it's more than just administrators. 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 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 such as ethical wall principles.

The landscape of Unstructured Data access is constantly changing and evolving, and 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. Also, focusing on the most blatant security violations such as locations with high volumes.

Get the Data Custodians Involved

It is unrealistic to expect security and engineering teams to take on the task of securing Unstructured Data access. Not only is there too much data and too much constant change, in most cases they cannot answer the foundational questions of access governance such as "Who should have access to this data?" A successful strategy will involve business owners who are responsible for the data and enable them 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 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 Unstructured Data and applications 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 let you lose sight of the larger workflows and projects that these features can be used to accomplish. These are some common workflows that 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 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 on. Nearly all organizations have too many users with privileged access to their File Systems and SharePoint systems, and no visibility into what these users are doing with those privileges.

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 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 recommend changes can provide powerful results in the effort to secure Unstructured Data. Most organizations quickly find that far too many people have access to data. Commonly this is from past roles and responsibilities. Identifying and revoking this access can help accomplish the principal of least privilege.

Active Directory Clean-up

Active Directory is the user store most often used to provide access to Unstructured Data. Most organizations struggle to control their Active Directory groups and how those groups are used to garner 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 to choose the right solution and ensure a successful project. Evaluation of the following features and capabilities will help guarantee the chosen solution can address these goals.

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		
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 determine the effective membership of a group by recursively expanding nested groups?	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		

Permissions and Access	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, including 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 2007 farms?	YES		
Does the solution support scanning of permissions from SharePoint 2010 farms?	YES		
Does the solution support scanning of permissions from SharePoint 2013 farms?	YES		

Permissions and Access (Continued)	STEALTHbits	Other Vendor	Other Vendor
Can the solution identify share permissions?	YES		
Can the solution identify folder 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" to a shared folder 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, 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		
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 and Domain Users 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 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		

Activity and Changes	STEALTHbits	Other Vendor	Other Vendor
Does the solution support tracking of activity and change events for Windows Servers?	YES		
Does the solution support tracking of activity and change events for Network-Attached Storage (NAS) Devices including NetApp and EMC, including Isilon?	YES		
Can the product report on creations, deletions, renames, moves, permission changes and modifications at the file?	YES		
Can the product report on creations, deletions, renames, moves, permission changes and modifications at the folder level?	YES		
Does the product provide an easy interface to understand all activity events that have taken place within a particular resource?	YES		
Will the solution identify the most active users for a resource?	YES		
Does the product identify abnormal behavior by identifying activity patterns that deviates from normal activity levels?	YES		
Can the solution recommend changes to access based on activity to resources, effectively providing the path to "least privilege access"?	YES		
Can the solution identify "high risk activity" where users take advantage of open conditions to gain access to resources?	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 credit cards and social security numbers?	YES		
Is the solution capable of scanning for sensitive data within image files using Optical Character Recognition (OCR)?	YES		
Does the product support customizable keyword and expression-based pattern definitions?	YES		
Does the product support prioritizing scans based on risk? (e.g. Scan files in Open Shares first)	YES		
Can the product correlate access and activity information with this information in order to understand who can and who has accessed the data?	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		

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 SharePoint?	YES		
Does the product support on-demand remediation?	YES		
Does the product support scheduled remediation?	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 membership 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?	YES		
Does the product support ownership of Active Directory groups?	YES		
Will the product identify the most probable owners of resources including shared folders and SharePoint sites based on multiple criteria including activity, content ownership and management hierarchy?	YES		
Can the product survey owners to confirm their responsibilities 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		

Entitlement Reviews Continued)	STEALTHbits	Other Vendor	Other Vendor
Will the workflow allow users to make changes that they see fit?	YES		
Can the product recommend changes to the owner based off of 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 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		
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 support thousands of resources dispersed across multiple data centers and joined to multiple domains?	YES		
Can the solution operate from a single centrally managed installation and only require a single database back-end?	YES		
Can the product leverage the following scanning approaches?	YES		
Agentless?	YES		
Applet-based?	YES		
Proxy scanning?	YES		
Does the product support on-demand scans?	YES		

Product Architecture (Continued)	STEALTHbits	Other Vendor	Other Vendor
Does the product support scheduled scans?	YES		
Can scheduled scans be configured to run during a time-window? Will active scans be "paused" at the end of the time window so the scan can be resumed during the next scanning 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 documentation on its API for integration?	YES		
Does the product offer integrations into the leading IAM solutions on the market 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		
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		

INTRODUCING StealthAUDIT FOR DATA ACCESS GOVERNANCE

With StealthAUDIT for Data Access Governance, you can pass those compliance regulations and reduce your organization's risk exposure by enabling complete and automated access governance controls over unstructured data residing in the File System and SharePoint. 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 architecture approach to centralize the collection of this data while providing minimal impact to 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 Data Access Governance deployment.

STEALTHbits TECHNOLOGIES

STEALTHbits Technologies is a cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data.