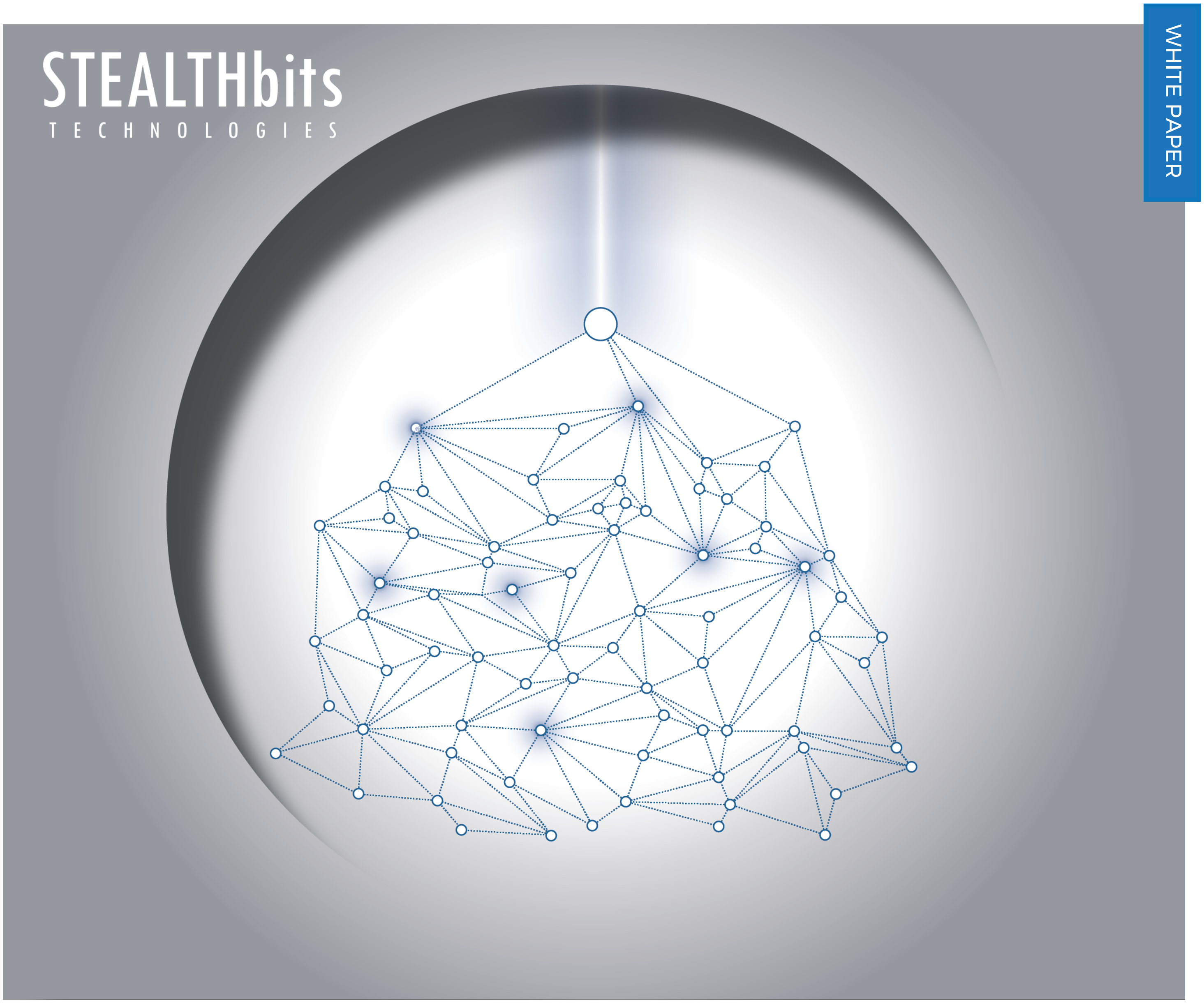
WHITE PAPER



5 CHALLENGES WITH COMBINING DATA ACCESS GOVERNANCE AND IDENTITY ACCESS MANAGEMENT

TABLE OF CONTENTS

INTRODUCTION

Unstructured data represents a significant risk for every organization. The files spread across file systems, SharePoint sites, and cloud applications continue to grow at a rapid pace, making it difficult to enforce proper security measures. For years, organizations have relied upon Identity and Access Management (IAM) solutions to provision users and manage access to their data. These solutions have primarily focused on controlling access to applications, and have ignored unstructured data due to its complexity. As data breaches and attacks on unstructured data continue to rise, companies are realizing the criticality of controlling access to this data. Data Access Governance (DAG) offers a solution, but integrating DAG with an IAM program introduces an entirely new set of challenges that are commonly overlooked. When planning a DAG initiative, being aware of these challenges can help avoid problems along the way.

START BY BUILDING A STRONG FOUNDATION

The goal of a DAG initiative is to provide a process around reviewing and controlling access to unstructured data. Enabling data owners to review and control access to their data ensures only the necessary people maintain access. When planning for any Data Access Governance project there are fundamental capabilities that must be achieved. These include the following:

Platforms

Unstructured data can reside in a variety of locations stored as different file types. Do employees within your organization prefer to create documents, spreadsheets, or PDF files? Are those files stored on file servers, SharePoint sites, or in the cloud? The ability to automatically discover where files reside across all repositories, both on-premise and in the cloud, is critical to ensuring proper coverage during a DAG initiative.

Access

Users can gain access to files in many different ways. To understand access you need to be able to evaluate the permissions applied to a file or folder. Answering a simple question such as “Who has access to this file?” can involve very complex calculations. This requires knowledge of not only the permissions, but also Active Directory groups, security principals (e.g. Everyone), local groups (e.g. Administrators), and more. To distill this complex information into a simple format that can be integrated into an IAM product may sound easy, but it is not. Too much or too little information can negate the ability to act on the information effectively.

Ownership

There are typically more unstructured data repositories at a company than there are employees. To be able to review and remediate access, it is crucial to involve the people who understand the data. These data owners know the nature and sensitivity of the files, and can make decisions on who should have access to them. Being able to effectively identify owners is the difference between a successful and failed DAG implementation.

Activity

Knowing who can access data is important, but knowing who is accessing data regularly is invaluable. Evaluating access patterns can help decide who should and should not maintain their access. User activity can provide powerful recommendations on who should and should not have access to unstructured data. This streamlines the process of reviewing access and removing users who are not using their access rights.

Sensitive Data

With the massive amounts of unstructured data most organizations have, it is crucial to focus on securing the highest risk data first. By inspecting the content of documents, spreadsheets, and other files to identify where sensitive data resides, it is possible to understand the risk associated with each file.

5 COMMON DAG PITFALLS

Any DAG initiative must address the basics foundational elements in order to succeed, and most organizations are familiar with those concepts. However, there are several other capabilities that are often not realized until a DAG deployment is well underway. Without addressing these needs, even a well-planned DAG implementation may stall out or fail altogether.

Permission Cleanup

Many organizations attempt to implement a DAG program on top of their existing unstructured data security model. This approach almost never succeeds. Most file systems are over a decade old, and have grown more and more complex over the years. Permissions are typically applied sporadically and inconsistently, and without a predictable permissions model it is impossible to control access.

It is important to clean up permissions before rolling out a DAG solution. This typically involves the following steps:

1. **Agree upon a permission model that works for your organization.** Most companies will follow industry best practices such as creating Read and Read/ Write groups and applying these to where access needs to be provisioned.
2. **Assess the current state of the file shares, SharePoint sites , or other unstructured data repositories.** This will help identify where permissions are applied that do not abide by the permissions model. Common examples include the use of Everyone permissions or directly assigning user accounts to permissions.
3. **Clean up and apply new permissions.** This involves creating new groups, populating them with the members who currently have access, applying those

groups and ensuring permissions are being inherited appropriately.

By automating this process it is possible to create simple, clean permission models where it will be easy to provision users without the risk of giving them access to the wrong data.

Ad-Hoc Changes

Many DAG initiatives focus on performing periodic reviews of access, or handling requests for access. In an ideal situation, this is all that is required to give users the access they need and revoke unnecessary rights. However, most organizations move quickly and the needs of employees to get access to data may require immediate action. It is important to arm data owners with all the capabilities needed to properly secure their data. Owners need a fast, simple way to make changes to access on the fly, without responding to requests or certifications. If there is an immediate need to revoke somebody's access to a file, the owner must be able to satisfy that requirement quickly. A DAG solution should allow owners to add and remove access at any time in a simple, secure way.

System Level Entitlements

Typical DAG solutions focus on who has permissions to the data, but almost all ignore who has access to the system the data is stored on. Administrators of file systems have full access to all data stored on that file system, regardless of what the permissions to the shared folders may be. Developers who were given access to a production server also may be looking at all of the files stored on that system, even though they do not need to.

To fully secure unstructured data and have an efficient DAG process, system-level access must be reviewed and controlled the same way data access is. Privileged access is the most common path to data exfiltration and abuse. It wouldn't make sense to consider a DAG program without system-level entitlements being a major focus.

File Reviews

Most DAG initiatives focus on reviewing access to file repositories, but do not focus on the files themselves. In any organization, more than half of the files stored within file shares or other file repositories are stale, unused, and outdated. In many cases, the data is also sensitive in nature, making it a significant risk.

If the purpose of a DAG solution is securing data, it only makes sense to review the data itself and remove, archive, or segregate unused files so owners only need to focus on the security of what is being actively used. Doing so effectively can significantly streamline the efficiency of a DAG initiative.

However, cleaning up stale data is not as simple as it may seem. Data owners must serve an integral role in this process, since they are the ones who understand the nature of the data and whether it is needed by the business. A valuable way to immediately improve any DAG initiative is to have owners review the sensitive files that they are responsible for and flag any unnecessary files. These files can then be remediated appropriately and will immediately reduce the risk of sensitive data falling into the wrong hands.

Environmental Nuances

There are many ways files can be shared within any organization, and most organizations do not follow the same standards even internally. A good DAG initiative must account for these differences. Some commonly overlooked environmental nuances include:

- Distributed File Systems (DFS) – The use of DFS creates a virtual path to a folder that abstracts the actual host where the folder is located. A DAG solution must be able to resolve and represent the DFS path, because most users will only recognize this path and have no awareness of the physical location of the files.
- List vs. Read – Many organizations break down granular levels of read access that can be granted on file shares so that some users can read the data and others can just enumerate the folders or files. This is done through List Folder Contents permissions within File Systems or Limited Access on SharePoint.
- Local Policies – Local policies on a server can change the way users can access the data. Settings including "Bypass Traverse Checking" and "Access this Computer from the Network" can be configured so that a user may seem to have access through the permissions applied to a folder, but in reality they will not be able to access the data. Understanding these policies is necessary to accurately comprehend and control access to data.

ADDITIONAL CONSIDERATIONS

Defining the requirements for a Data Access Governance solution can greatly improve the success of integrating DAG into an IAM solution. However, it is not only the requirements that matter, but how those requirements are met. There are architectural considerations that should be made when deciding on the right solution for addressing these requirements.

Integrations

To successfully implement DAG as part of IAM, it is important to design a solution that fits into your organization and integrates with established processes and applications. Having a DAG product that offers integrations with your existing Identity platform is, of course, a strong requirement. However, there are many other often overlooked integrations that may make a DAG program much more successful. One common example is integration with a Configuration Management Database (CMDB) to pull a list of production hosts to scan. Also, integrations with DLP, vulnerability scanners, and HR systems can provide significant value.

Open Architecture

All organizations are unique, and a DAG solution must be flexible and open enough to adapt to the needs of the organization. There must be ways to customize the inputs and outputs and provide full and easy access to the data that is collected.

Lightweight Scans

To be able to adapt quickly to the constantly changing state of an organization, it is important to be able to quickly scan and assess unstructured data repositories. Performing scans without requiring agents provides a fast and easy way to discover and assess unstructured data repositories and quickly get them integrated into the DAG solution.

CONCLUSION

Protecting unstructured data is a critical component of any organization's security strategy. More and more companies are adding Data Access Governance to their Identity Management solutions to achieve this security. There are a variety of capabilities that must not be overlooked when planning for this type of integration. To achieve a successful DAG integration, software solutions that provide the full set of foundational and additional capabilities, such as those offered by STEALTHbits, should be used.

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. WP-DAGIAM-1016