opentext™

WHITE PAPER

OpenText Data Access Governance Solutions

Securing confidential, sensitive, and high-value information stored as unstructured data

Contents

Traditionally, leading identity and access management (IAM) and identity governance and administration (IGA) products have focused on governing data access to applications and the data housed and controlled by those applications. But what about the data outside the scope of applications?

Security analysts have concluded that the “elephant in the room” is the lack of governance for an organization’s unstructured data; that is, the file-based data that comprises more than 80 percent of an organization’s total data according to multiple analysts’ estimates.[1]

When it comes to securing access to the confidential, sensitive, and even mission-critical files stored among this unstructured data, data access governance solutions from OpenText provide an integrated product approach to discovering sensitive files, reporting on permissions and metadata, securing files through permissions remediation and file management actions, and certifying proper access through access reviews.

1. Gartner, Voice of the Customer for Document Management, Peer Community, Contributor, 25 June 2025 - ID G00834882.
Note: This is just one of many Gartner publications where this statistic has been stated.

Introduction

In recent years, data breaches have been the subject of numerous news stories. In fact, the frequency of data breaches and the resulting exposure of sensitive information has become so common that these stories now tend to focus on the most extreme occurrences. Lest we forget or miss some of these reported incidents, publications such as *Business Insider*, *Wired*, and *Digital Information World* conclude each calendar year with their rankings of the worst cases of data breaches.

Data has value to both the organization that owns it and the outsiders who want to access and exploit it. However, unauthorized access to data is not always based on nefarious intent. For example, access permissions are assigned temporarily but not removed, roles change, group memberships are modified, and before you know it, an internal user has access to data he or she should not have.

With the ramifications of unauthorized access ranging from loss of consumer confidence to severe fines, securing data through access controls is a high-priority objective of all organizations.

Comparing risk: Structured and unstructured data

For analysts, security personnel, and legislators, the traditional focus on data security has been on the records stored in databases. Known as “structured data,” this data is a primary source for personally identifiable information (PII), health records, account numbers, passwords, and other confidential information that, when accessed by unauthorized individuals, can have potentially devastating consequences. To protect PII, health information, and other sensitive data, governments have established privacy regulations with which organizations must be in “compliance” or face potentially severe consequences. For this reason, organizations are required to periodically perform “access reviews” of who can access sensitive data.

Most applications that store structured data in a database have inherent security mechanisms in place relative to the application. For example, OpenText™ Identity Manager, along with OpenText™ Identity Governance, validates and reconciles access controls to these applications, inherently controlling access to the structured data.

An equally vulnerable, but historically less emphasized data set is “unstructured data.” Unstructured data is file-based data—word processing, spreadsheets, media, virtual images, and other files that make up more than 80 percent of an organization’s stored data. Unstructured data is stored mainly on file servers, storage area network devices (SANs), and in the cloud. And like structured data, unstructured data can also contain sensitive information that needs to be protected. In some cases, it could be PII exported from structured data sources. But it’s not just about PII. Unstructured data can be the “crown jewels” of a company’s data. Microsoft Excel files might contain profit and loss data, Microsoft Word files might include legal information, and Microsoft PowerPoint files might include sales forecasts.

Consequently, securing sensitive and confidential unstructured data from threats both inside and outside the firewall has become a growing area of concern. Nevertheless, organizations tend to consider the security of their structured data and unstructured data differently. As one data security analyst has stated, "Given the sheer volumes, can it be said that unstructured data receives proportional (or even anything like) the same consideration structured data receives? The answer is most likely 'no.'" [2]

Data access governance

Recognizing the vulnerability and potential costs pertaining to the unauthorized access of sensitive information in unstructured data, many research and advisory firms are advocating the implementation of data access governance (DAG) tools.

In defining the DAG market, Gartner states: "Data access governance (DAG) provides assessments, management, and real-time monitoring for unstructured and semistructured data in file repositories. Its primary purpose is to determine, manage, and monitor who has access to which data, rectify oversharing, and secure usage of data with generative AI (GenAI). DAG provides an audit trail of access and permission activities."[3]

With this recognition by Gartner and other research organizations, we believe it's apparent that regulations and compliance objectives will soon be updated to include the security and access protection of unstructured data.

OpenText data access governance solutions

Since the introduction of the products now known as OpenText™ File Reporter and OpenText™ File Dynamics, the engineering team developing them has continuously been addressing the objectives of what is now classified as the DAG market. Through an identity-driven approach, these products report on and control access to unstructured data stored in the network file system, ensuring that only the right people have access to the right information at the right time.

With the eventual designation of the DAG market, the product team found that the associated analyst reports, findings, and projections for the market's direction aligned with the team's independent research. Soon, there was regular interaction between the team and DAG analysts as the team began to develop product requirements and roadmaps, and introduced two DAG solutions.

OpenText Data Access Governance

Comprising OpenText File Reporter and OpenText File Dynamics, OpenText™ Data Access Governance identifies and secures an organization's sensitive and high-value unstructured data from unauthorized access. This data not only includes PII, but also an organization's intellectual property. OpenText Data Access Governance employs an identity-based approach to identify the location of sensitive and valuable files and determine who has access to them. It then makes necessary changes to locations and permissions, ensuring that sensitive and high-value data remains secure from unauthorized access.

2. Omdia, *Are We Doing Enough to Protect Our Unstructured Data?*, March 15, 2023

3. Gartner, 2024 Strategic Roadmap for World-Class Security of Unstructured Data, Joerg Fritsch, 6 May 2024 - ID G00809463

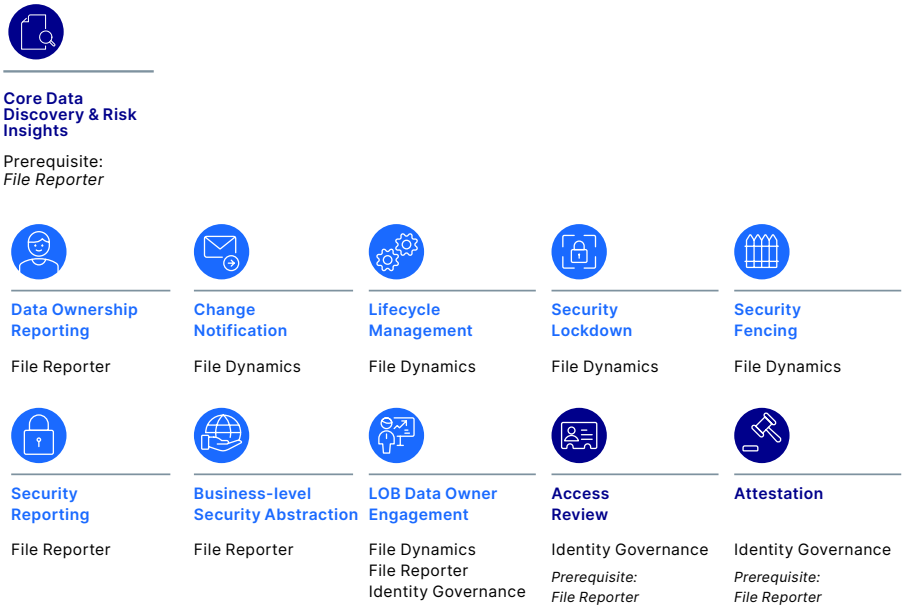
OpenText broad-spectrum data access governance solution

When OpenText Data Access Governance is combined with OpenText™ Core Data Discovery & Risk Insights and OpenText™ Identity Governance, it creates an integrated “broad-spectrum DAG solution” that offers data discovery; access permissions insight; data insight; automated data management, including moving files, remediating access permissions, and cleaning up files; and finally, the means of conducting access reviews on unstructured data repositories .

Addressing DAG requirements

With a focus on identity-driven reporting, automated management, and capabilities offered through integration with other OpenText products, OpenText DAG solutions are uniquely equipped to address today’s specified DAG requirements, supporting capabilities to help address these requirements, and what we perceive will be DAG requirements in the future. These include the following:

- Data discovery
- Data ownership reporting
- Security reporting
- Change notifications
- Line-of-business data owner engagement
- Business-level security abstraction
- Lifecycle management
- Security lockdown
- Security fencing
- Access review
- Attestation



Data discovery

Gartner does not specify a requirement for data discovery in its DAG definition, but has mentioned that some vendors identified in the DAG market segment provide this capability.[4] Data discovery through OpenText Core Data Discovery & Risk Insights is offered in the broad-spectrum data access governance solution.

OpenText Core Data Discovery & Risk Insights helps secure both structured and unstructured data by performing robust sensitive data discovery and classification through grammars, patterns, and risk score tagging. For unstructured data, this means the capability to review the content of all files in a specified target path and locate PII, credit card numbers, word patterns such as “acquisition” or “merger,” or any other data strings that could classify the file as sensitive.

Data ownership reporting

Unstructured data repositories are a natural target for outsiders and unauthorized insiders due to the immense amount of content stored there. While there are plenty of redundant, outdated, and trivial (ROT) data that should probably be deleted, there are certainly also numerous files containing sensitive information.

By generating ownership reports using OpenText File Reporter, you can identify the owners of each file and then refer to those owners to determine whether the file should be kept where it is, deleted, archived, or moved to a more secure location. For those files that are kept or secured, an access review of the files can determine if the file’s owner is correct or if a new owner needs to be assigned.

Security reporting

Before you can implement measures to govern access to unstructured data, you must first determine who has access permissions to the data. With this knowledge, you can make any needed changes to directly assigned access permissions or group memberships.

The challenge is that identifying unstructured data permissions is much more complex than identifying application permissions. Contributing to this complexity are all of the NTFS permission types, security principles, security identifiers, inheritance, group memberships, Active Directory access control lists, and other factors. The difficulty in determining accurate access permissions is a major reason why most IG vendors do not offer the ability to provide access reviews for unstructured data.

Since its introduction, OpenText File Reporter has been able to report assigned and effective file system user permissions for all folders and subfolders from a specified file system path. Furthermore, you can identify all users who have any type of access permissions to a specified network folder, as well as all of the network folders that a specified user can access.

OpenText File Reporter can also report on the access permissions located in Microsoft 365 cloud applications (Teams, OneDrive, and SharePoint Online), including who has access to a specified document library and all document libraries that a specified user can access.

4. Gartner, 2024 Strategic Roadmap for World-Class Security of Unstructured Data, Joerg Fritsch, 6 May 2024 - ID G00809463

Change notifications

Once you expend the time to review access permissions, make needed adjustments, participate in an audit, and demonstrate compliance with any corporate policies or government regulations, the last thing you want is to jeopardize that compliance through an unauthorized change in access permissions.

OpenText File Dynamics lets you create security notification policies assigned to specific high-value targets on your network so that data owners—designated users familiar with the contents and security of the high-value target—can review access permission changes.

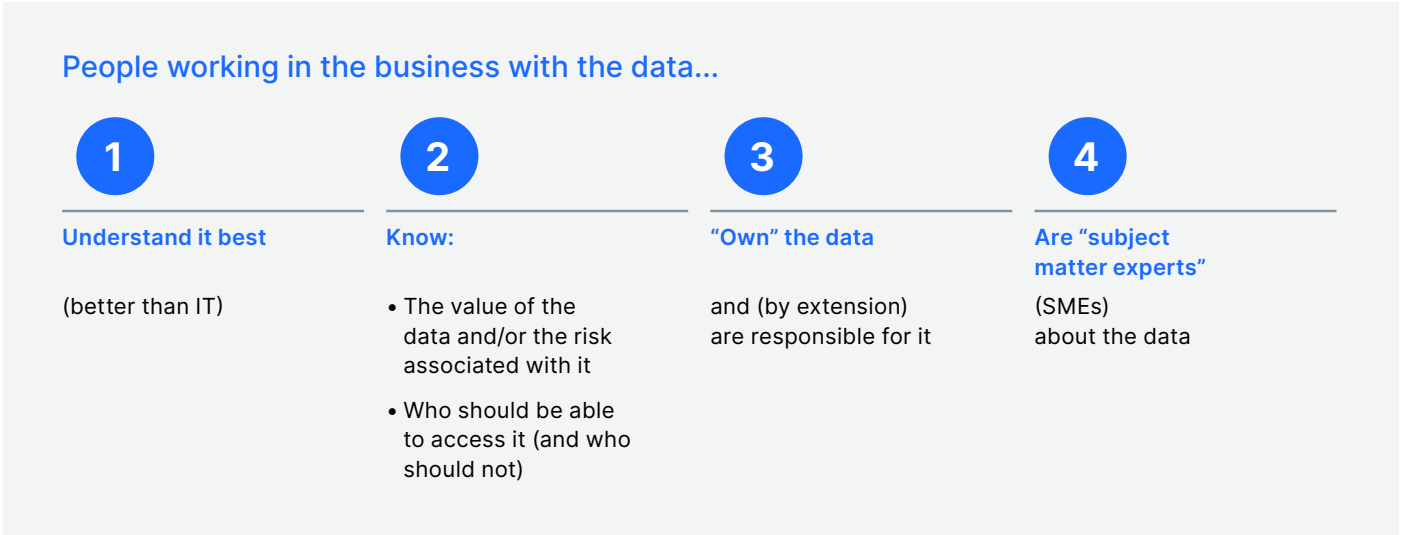
Access permission changes can occur directly through an individual user assignment or indirectly through a change in group membership.

Security notification policies are granular enough in scope to provide just the right level of desired control. For example, if a security notification policy were assigned to the finance folder and a new member were added to a group that had access permissions to that folder, a notification would be sent to the data owner so that the data owner could then decide if any responsive action needed to be taken.

Line-of-business data owner engagement

In organizations of any size, no one knows the relevance, value, or sensitivity of data more than those who work with the data. A user in the HR department, for example, will be a much better judge of what HR data to store, delete, and secure through limited access in comparison to a regular network administrator.

For each high-value target, OpenText File Dynamics lets you designate data owners who, depending on the type of policy involved, are notified when access permissions have changed, review permissions logs, determine who should have access and what type of access, lock down access permissions, and more.



Data owners are subject matter experts who know the value of the data and who should have and not have access to it.

Business-level security abstraction

When conducting an access review, auditors must determine what access permissions a user has and if those permissions comply with corporate policy or government regulations. For example, a user might have Write Access to an application when she should have only Read Access, or another user might have Full Control when he should have Write Access.

Unfortunately, Windows NTFS file system permissions are much broader than these three designations. As part of the integration between OpenText File Reporter and OpenText Identity Governance, OpenText File Reporter performs a business-level abstraction of the NTFS permissions so that the business-level people performing access reviews on unstructured data (and not familiar with NTFS permissions) can review them with classifications that they understand. For example, the NTFS access mask flag of “delete subfolders and files” becomes “write,” while “take ownership” becomes “change permissions.”

Lifecycle management

Many organizations use IAM software to manage application access based on user role. For example, a new user in the HR department can automatically be granted access permissions to the HR applications and associated data.

While the IAM system can provision access rights to applications and application-based data based on role, it cannot provision network file system access based on role—that’s where OpenText File Dynamics comes in.

Since it uses the same directory service (Microsoft Active Directory) as your IAM system, OpenText File Dynamics can take user storage action while the IAM system takes user account action.

While the IAM system creates a new user account in Active Directory, makes the user a member of one or more groups, and sets the user’s network access, OpenText File Dynamics can establish a network home folder, access permissions, and storage quota according to the user’s role. In addition, it can establish access to role-based collaborative storage areas.

Security lockdown

Sensitive data should be accessible on a “need to know” basis, meaning that only a limited set of individuals, based on their roles, should have access to this sensitive data. Furthermore, data owners—those most familiar with the sensitivity of the data and who should have access to it—should be empowered to be the ultimate decision makers.

Once you have established the proper access permissions for a high-value target, you can establish the archetype of access permissions for the high-value target that will be strictly enforced through a lockdown policy. When unauthorized access permission changes are made to the high-value target, the new permissions are removed, and the permissions specified in the lockdown policy are restored.

Security fencing

There might be some high-value targets on which you might not want to place the same level of restrictions as a lockdown policy, but might nevertheless want to secure access to only authorized users or roles.

Fencing policies in OpenText File Dynamics let you set limits on how access permissions may change over time. Using a set of ALLOW/DENY statements to define a "fence," the policy specifies Active Directory containers, users, or groups that might conceivably be given permissions to a high-value target in the future without an issue or should never be given rights in the future, as in restrictions specified in GDPR.

Target-driven security policy family

Notification	Lockdown	Fencing
Notify people if security changes	Security is not allowed to change	Security is allowed to follow a free-flow evolution over time, but within limits

Target-driven security policies include security notification, lockdown, and fencing policies. Each is designed to assist data owners in limiting access to sensitive data to only authorized users.

Access review

Gartner does not specify a requirement for access reviews in its DAG definition. However, we believe the logical culmination of all the actions associated with DAG is the conducting of access reviews to verify that only authorized users have access to sensitive and confidential information stored in unstructured data.

Many regulated industries require periodic access reviews, which are the means of providing certification (also referred to as "attestation") to comply with specific regulations. For most of these organizations, access reviews are the means of:

- Enabling organizations to manage group memberships.
- Reviewing and reconciling access to enterprise applications.
- Reconciling role assignments.

The OpenText broad-spectrum DAG solution allows you to not only meet these requirements but also conduct access reviews on perhaps the repository most vulnerable to data breaches—the network file system.

Resources

What is data access governance? ›

OpenText Data Access Governance product page ›

Success story: Large aerospace organization ›

Success story: United States county administration ›

Integration between OpenText File Reporter and OpenText Identity Governance allows for permissions scans conducted in OpenText File Reporter to be imported into OpenText Identity Governance, where access reviews on the high-value target can be conducted.

Attestation

As a simple definition, “attestation” is the process of validating that something is true. When it comes to access reviews, attestation is the certification that an organization complies with security and access regulations or policies. Depending on the regulation, attestation is dependent on several specifications, including when the review is conducted, by whom, how the review is conducted, and much more.

The capabilities of the OpenText broad-spectrum DAG solution deliver you the means of providing auditors and line of business managers with intuitive, user-friendly, and automated access certification processes and reports to demonstrate compliance and provide attestation.

Gartner does not specify an attestation requirement in its definition of DAG, but as the desired outcome of an access review, we include this as a logical DAG requirement.

Conclusion

Comprising more than 80 percent of an organization’s stored files, unstructured data and the sensitive information contained within are targets for internal and external data breaches, posing risks to organizations of all sizes and in all industries. The objective of OpenText DAG solutions is to protect organizations from unauthorized access through an extensive set of integrated product capabilities.

The OpenText DAG solutions, with their identity-driven reporting, management, data discovery, and access review capabilities, are uniquely equipped and qualified to address the comprehensive requirements of a complete DAG solution. As the threats of data breaches become more sophisticated, as new regulations are introduced, and as data stores continue to grow exponentially, you can feel confident that you are addressing these challenges and all others with the expertise of a recognized industry leader in OpenText.

opentext™