Broad-spectrum data access governance

Identify and address threats that can come from unauthorized access to strategic and mission-critical unstructured data through a comprehensive approach.

Solution Components

- OpenText Core Data Discovery & Risk Insights
- OpenText File Reporter
- OpenText File Dynamics
- OpenText Identity Governance

Organizations store a tremendous amount of data, 80 percent of which is unstructured, file-based data. Many of these files contain sensitive, confidential, and high-value information that needs to be secured from unauthorized users. That's what data access governance, or DAG, is all about. And only OpenText offers a broad-spectrum DAG solution that spans from data discovery to compliance attestation.

Securing Unstructured Data

The definitive objective of data security is to make information available to those who need it, while keeping it safe from those who don't. Data and user role, i.e., identity, are therefore interconnected with data security. HR workers, for example, should be able to see personnel records containing PII, while IT workers should not.

Privacy regulations have been the driving force for developing and adopting identity-based security for structured data stored in application databases, for example, a patient's medical records. However, most of an organization's data is "unstructured data," file-based data stored on servers, storage devices, and the cloud. These word processing files, spreadsheets, presentations, and other file types can also include PII, along with other confidential information that must be secured from unauthorized access.

Data access governance

Following a series of high-profile unstructured data breaches in the 2010s at major companies, Gartner® began to not only write about the risks of unauthorized access to confidential unstructured data, but also specified the requirements to address a new software market segment to address these risks, which it termed data access governance (DAG).

According to Gartner: “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.”[1]

OpenText and DAG

Long before the designation of the DAG market segment, engineers who now develop software for OpenText were building identity-based reporting and management software for unstructured data, which identified access risks, remediated improper access rights, moved data to more secure locations, and cleaned up expired data. These products are now known as OpenText™ File Reporter and OpenText™ File Dynamics and comprise OpenText Data Access Governance.

OpenText Data Access Governance identifies, secures, and protects an organization’s sensitive and high-value unstructured data from unauthorized access. This includes PII, as well as items such as sales forecasts detailed in spreadsheets, legal documents saved as word processing files, or financial data in a presentation to shareholders. OpenText Data Access Governance uses an identity-based approach to identify where sensitive and valuable files are located and who has access to them, then makes needed changes to locations and permissions, and assures that sensitive and high-value data remains secure from unauthorized access.

Expanding capabilities through integration with other OpenText technologies

OpenText develops an extensive portfolio of information management software, including data analytics, enterprise information management, cloud solutions, security, AI, and identity management and governance, which can expand and enhance DAG capabilities.

OpenText Core Data Discovery & Risk Insights

OpenText™ Core Data Discovery & Risk Insights performs 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.

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.[2]

OpenText Identity Governance

OpenText™ Identity Governance helps organizations run effective access certification campaigns and implement identity governance controls to meet compliance mandates while mitigating risk. It collects user entitlement information across multiple systems, applications, and data into a consolidated view. This provides easy-to-understand reports for line-of-business managers to validate whether existing employee access privileges are appropriate, initiate immediate action to revoke any access, and provide attestation of compliance with regulations.

[1] Gartner®, Hype Cycle for Data Security Technologies, 2025, Andrew Bales, 10 July 2025 - ID G00828131

[2] Gartner, 2024 Strategic Roadmap for World-Class Security of Unstructured Data, Joerg Fritsch, 6 May 2024 - I D G00809463

Resources

OpenText Core Data Discovery & Risk Insights product page ›

OpenText Data Access Governance product page ›

OpenText Identity Governance product page ›

What is Data Access Governance? ›

OpenText Data Access Governance integration

Recognizing the benefits to customers of a “broad-spectrum DAG” offering that could be initiated through a data discovery process and concluded through an access review, OpenText Data Access Governance developers worked to make it a reality through extensive product integration work.

The result is a unique DAG solution that can:

- Discover sensitive and confidential files and specify where they are being stored.
- Pinpoint through reports and analytics who has access to those files and how they got that access.
- Provide the automated means of moving, archiving, or deleting files.
- Put security policies in place that secure files from unauthorized access.
- Provide notifications to line-of-business data owners when any access permissions are modified.
- Conduct access reviews following all of the corrective actions taken, certifying and attesting that all users and their role-based permissions comply with privacy and other regulations.

Product integration details

Once OpenText Core Data Discovery & Risk Insights has performed data discovery, identified files with sensitive content, and put the results in a workbook, a new Report Permissions option appears via OpenText™ File Reporter (a component of OpenText Data Access Governance). Clicking this option triggers OpenText File Reporter to report all users with access to these sensitive files. These reports can be generated as simple reports or through rich graphical analytics via Power BI.

With the information from the report, OpenText™ File Dynamics (the other component of OpenText Data Access Governance) takes needed action through policies that you create. These policies can move files to more secure locations, archive or delete expired files, and secure folders and shares storing confidential information.

Finally, the OpenText broad-spectrum DAG solution lets you perform access reviews on unstructured data by making unstructured data folders and shares visible for review and converting and consolidating NTFS permissions to the OpenText Identity Governance permissions of Read, Write, and Change Permissions. This enables organizations to certify and provide attestation of compliance with regulations that only authorized users have access to confidential and sensitive files.

Integration provides even more protection

Since the designation of the DAG market segment, OpenText has provided tools and solutions for addressing its objectives. With the integration of additional products, OpenText further enables organizations to identify, secure, protect, and manage their unstructured data.

Contact your OpenText sales rep to learn more ›