

Protecting your data from unauthorized access requires a governance approach for all your data



Three-component solution for data security

OpenText Identity Manager

Automated identity provisioned/deprovisioned access to applications and associated structured data

OpenText Identity Governance

Identity-based access review, analytics, and approval system for sensitive and regulated structured data

OpenText Data Access Governance

Identification, remediation, and protection of sensitive and high-value unstructured data from unauthorized users

An organization's confidential and high-value data needs to be protected from unauthorized users. There's not only the risk of noncompliance with privacy regulations, but there's also the threat of a data breach of proprietary financial, legal, and competitive data that comprise the "crown jewels" of an organization.

OpenText has a three-component solution for governing access to all of this data.

Three-component solution for data security

When it comes to governing access to data, the three-legged stool analogy demonstrates the principle that data access is supported by three main "legs." Each leg needs to be equal in strength, otherwise the stool—representing the organization's overall data access security—will topple. If one leg fails or is nonexistent, the integrity of the organization's data access security is compromised.

Because "data powers everything we do"¹ and is the "raw material"² of business, it is imperative that an organization's data—no matter how it is stored digitally—is available to those who should have access and is restricted from those who should not. OpenText offers a complete, three-component solution for securing sensitive and high-value structured and unstructured data, which keeps organizations safe from data breaches, compliant with regulations, and competitive as a business.

1. Jeff Weiner, Former Chief Executive Officer, LinkedIn

2. Craig Mundie, Former Senior Advisor to the CEO, Microsoft

Just as the function and effectiveness of a stool changes with the addition of the stabilizing third leg, so can the overall security of an organization improve dramatically when it focuses on protecting access to both its structured and unstructured data with the addition of OpenText Data Access Governance.

OpenText Identity Manager

The technology that today is known as OpenText™ Identity Manager helped launch the identity and access management (IAM) market and continues to be a leader and innovator in this market space. With the ability to automate the management of user access and restrictions to applications, systems, websites, and other tools through a centralized, single user authentication profile, organizations can drive down management costs, guard against unauthorized access to sensitive records stored in application databases, provision workflow, and more.

OpenText Identity Governance

OpenText™ Identity Governance was introduced as a means of auditing and certifying what users do once they have been given access to systems. Through this solution, organizations can demonstrate compliance with regulations through access reviews. Furthermore, OpenText Identity Governance is the means for submitting and approving access requests for applications, identifying any risks by approving requests, and much more.

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 data is not only PII, but an organization's intellectual property—the "crown jewels" of an organization, such as sales forecasts located in spreadsheets, legal documents saved as word processing files, financial data in a presentation to shareholders, and more. 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.



The addition of OpenText Data Access Governance is like the addition of the stabilizing third leg to a stool.

Protect access to both structured and unstructured data

Just as the function and effectiveness of a stool changes with the addition of the stabilizing third leg, so can the overall security of an organization improve dramatically when it focuses on protecting access to both its structured and unstructured data with the addition of OpenText Data Access Governance.

For example, by adding OpenText™ File Reporter—which is included in the suite of products in OpenText Data Access Governance—OpenText Identity Governance becomes enabled to not only conduct access reviews on structured data, but on unstructured data repositories as well. This might include access reviews on network folders storing financial, legal, or other sensitive proprietary documents.

Additionally, when OpenText™ File Dynamics—another product in OpenText Data Access Governance—is deployed at organizations running OpenText Identity Manager, OpenText File Dynamics can provide access to user role-based network storage locations as Identity Manager grants access to role-based applications. For example, as a new hire in the finance department is provisioned access to financial applications, he can be simultaneously granted access rights to the finance network share storing financial documents.

Talk to your account executive

Talk to your OpenText account executive about how to complete your data access security through OpenText Data Access Governance. They can also set up a call with an OpenText Data Access Governance product expert to answer questions and give a demo. Learn more by downloading the [OpenText Data Access Governance solution overview](#).