

NetIQ Data Access Governance Solution

Traditionally, leading NetIQ Identity and Access Management (IAM) and NetIQ 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?

Table of Contents

Introduction	1
Comparing Risk: Structured and Unstructured Data	1
Data Access Governance	2
Detailing DAG Requirements	3
Coalescence with Identity Governance	4
The OpenText Approach to a Comprehensive DAG Solution	4
High-Value Targets and Risk	5
Addressing DAG Requirements	5
Conclusion	10
About NetIQ	10

Analysts have concluded that the “elephant in the room” is the lack of governance for organizations’ unstructured data, that is, file-based data that make up more than 80 percent of organizations’ total data. When it comes to access to sensitive files in unstructured data, the NetIQ Data Access Governance by OpenText™ solution provides an integrated product approach to reporting, correcting, and certifying proper access through access reviews.

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, organizations such as Business Insider, Wired, Digital Information World, and others concluded the 2018 calendar year with their rankings of the worst cases of data breaches for the year.

Data has value to both the organization that owns it as well as the outsiders that want to access it and exploit it. But 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, the securing of 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 are a primary source for personal 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 for 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 have structured data on the back end have inherent security mechanisms in place relative to the application. NetIQ Identity and Access Management (IAM) by OpenText™ and NetIQ Identity Governance and Access (IGA) by OpenText™ software vendors provide software that authorizes, validates, and reconciles access controls to these applications, inherently controlling access to the data.

When it comes to access to sensitive files in unstructured data, the NetIQ Data Access Governance solution provides an integrated product approach to reporting, correcting, and certifying proper access through access reviews.

An equally vulnerable, but historically less emphasized data set is “unstructured data.” Unstructured data are the file-based data—the word processing, spreadsheets, media, virtual images, and other files that make up more than 80 percent of an organization’s stored data. Unstructured data are 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. Excel files might contain profit and loss data, Word files might include legal information, and PowerPoint files might include sales forecasts.

Perhaps no area of data management though, has received more recent attention than data security. This includes threats both inside and outside the firewall, ranging from unauthorized access to files, to files corrupted through a ransomware attack.

As was pointed out in a Forbes article, “Most enterprises do not understand how much sensitive data they have, and when we consider how much unstructured data (emails, PDFs, and other documents) a typical enterprise has under management, the red flags are clear and present. ... This is a big data problem, to say the least. As the level of unstructured data rises and hackers shift their focus to it, unstructured data is an issue that can no longer be placed on the enterprise IT back burner.”¹

In defining the DAG market and requirements for addressing it, Gartner states: “Data access governance (DAG) provides data access assessment, management and real-time monitoring capabilities for unstructured and semi-structured data found in file repositories.”

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 recognizing a new Data Access Governance (DAG) market.

In defining the DAG market, Gartner states: “Data access governance (DAG) provides data access assessment, management and real-time monitoring capabilities for unstructured and semi-structured data found in file repositories. DAG’s primary purpose is to determine who has access to which data in an organization’s repositories, how that data is classified and what the history of access to that data has been.”²

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.

1. The Big (Unstructured) Data Problem, Juliette Rizkallah, Forbes, June 5, 2017
2. Gartner, Hype Cycle for Data Security, 2018, Brian Lowans, 24 July 2018

Detailing DAG Requirements

Corporate security practices, research, best practices, standards, legislation, and the ideas of thought leaders are all contributing to an evolving list of requirements for a comprehensive DAG solution. These can be categorized as follows:

- 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

Each of these categories is detailed later in this paper.

Since its initial product introduction in 2003, the team that develops what today is known as File Reporter and File Dynamics has continuously been addressing the objectives of what would years later be classified as the DAG market.



Figure 1. A comprehensive Data Access Governance solution includes capabilities offered in OpenText™ File Reporter, OpenText™ File Dynamics, NetIQ Identity Governance, and NetIQ Identity Manager.

Coalescence with Identity Governance

All security research organizations have slightly varying definitions of NetIQ Identity Governance, but a good overall definition would be a policy-based centralized system of user identity management and access control monitored proactively. A component of NetIQ Identity Governance is access reviews. As previously mentioned, NetIQ Identity and Access Governance (IGA) helps address enterprise IT security and regulatory compliance through access reviews.

Because of headline-baring data breaches targeted at unstructured data repositories, analysts are now noting organizations' desires to expand access reviews to include access to unstructured data. According to Gartner, "access to unstructured data is driving interest in integration of IGA with data access governance products ... for more mature organizations."³ "Since DAG tools provide important context, their inclusion will be important for organizations looking to make use of security intelligence to improve their detection and response capabilities."⁴

The OpenText Approach to Comprehensive DAG Solution

Since its initial product introduction in 2003, the team that develops what today is known as File Reporter and File Dynamics has continuously been addressing the objectives of what would years later be classified as the DAG market. Through an identity-driven approach, these products reported on and controlled access to unstructured data located in the network file system, helping to ensure that only the right people had the right information at the right time.

With the eventual identification of the DAG market, the product team found that the associated analyst reports, findings, and projections for the direction of the market were in alignment 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, roadmaps, and new initiatives.

One of the first of these initiatives was integration between File Reporter and NetIQ Identity Governance, providing the ability for the latter to perform access reviews on unstructured data (in addition to access reviews on applications that the product could already do).

With a focus on identity-driven reporting, management, and access reviews combined with more than 30 years of continuous development and enhancements, the products comprising the NetIQ Data Access Governance solution are uniquely equipped to address the comprehensive requirements of a DAG solution.

-
3. Gartner, Magic Quadrant for Identity Governance and Administration, Felix Gaehtgens, Kevin Kampman, Brian Iverson, 21 February 2018
 4. Ibid

This product integration is part of an overall Data Governance solution that is comprised of the following products:

- **File Reporter.** Inventories network file system security along with identity and role information to deliver the detailed file storage intelligence needed to optimize and secure your network, mitigate risk, and ensure compliance.
- **File Dynamics.** Provides extensive data management services through automated, policy-based administration. Services include storage provisioning, storage lifecycle management, data migration, remediation, cleanup, security notification, protection from data corruption and downtime, and more.
- **NetIQ Identity Governance.** Provides a business-friendly interface built on a common governance model that spans all of your business processes relating to identity, access, and certification. Demonstrates compliance providing you confidence that your access recertification campaigns are done right.

High-Value Targets and Risk

The OpenText™ approach to Data Access Governance lets you implement the solution in a priority approach based on identifying and then protecting the “high-value targets” on your network. A high-value target is a network folder or share where files containing sensitive or confidential information are stored. Folders or shares containing financial, legal, and health information are examples of high-value targets, but in reality, it can be any network folder storing data that your organization might consider valuable.

Once you have identified these targets, you can verify or correct access permissions and then protect them through policies (detailed later in this paper). This approach does not need to be a monumental undertaking and can be done in phases. By simply creating policies on a few high-value targets, you will see benefits immediately.

Addressing DAG Requirements

With a focus on identity-driven reporting, management, and access reviews combined with more than 30 years of continuous development and enhancements, the products comprising the NetIQ Data Access Governance by OpenText™ solution are uniquely equipped to address the aforementioned comprehensive requirements of a DAG solution.

For each high-value target, 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 Ownership Reporting

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

By generating ownership reports using File Reporter, you can identify the owners of each file and then refer to those owners on 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 in the fact 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, 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 that 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.

Change Notifications

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


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.

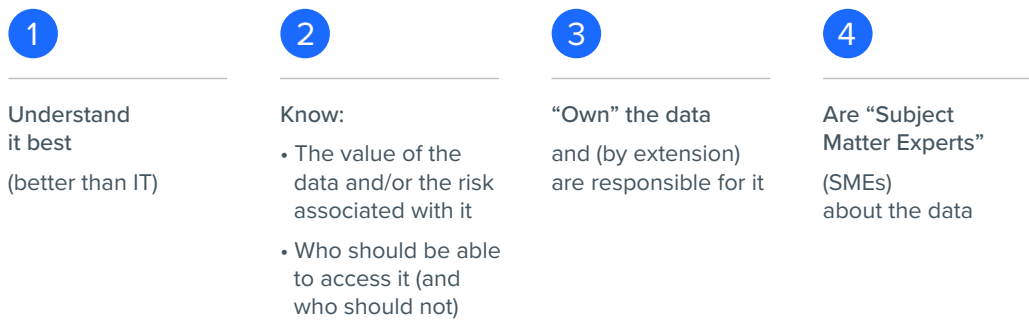
Access permission changes can occur directly through an individual user assignment or indirectly through a change in group membership.

Since its introduction, 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 that 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.

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 was 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 take place.

Line of Business Data Owners

 People working in the business with the data...



The features of the NetIQ Data Access Governance solution delivers 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.

Figure 2. Data owners are subject matter experts that know the value of the data and who should have and not have access to it.

Line-of-Business Data Owner Engagement

In any sized organization, no one knows the relevancy, value, or sensitivity of data than those who work with the data. A user in the H.R. department of an organization, for example, will be a much better judge of what H.R. data to store, delete, and secure through limited access in comparison to a regular network administrator.

For each high-value target, 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.

Business-Level Security Abstraction

When conducting an access review, auditors must determine what access permissions a user has and if those permissions are in compliance 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 so as part of the integration between File Reporter and NetIQ Identity Governance, File Reporter performs 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 utilize Identity Management (IDM) software to manage application access based on user role. For example, a new user in the H.R. Department can automatically be granted access permissions to the H.R. applications and associated data.

While the IDM 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 File Dynamics comes in.

Since it uses the same directory service as your identity management system, File Dynamics can take user storage action while the identity management system takes user account action.

While the identity management 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, 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 Security Lockdown policy but might nevertheless want to secure the access to only authorized users or roles.

Fencing policies in File Dynamics lets 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

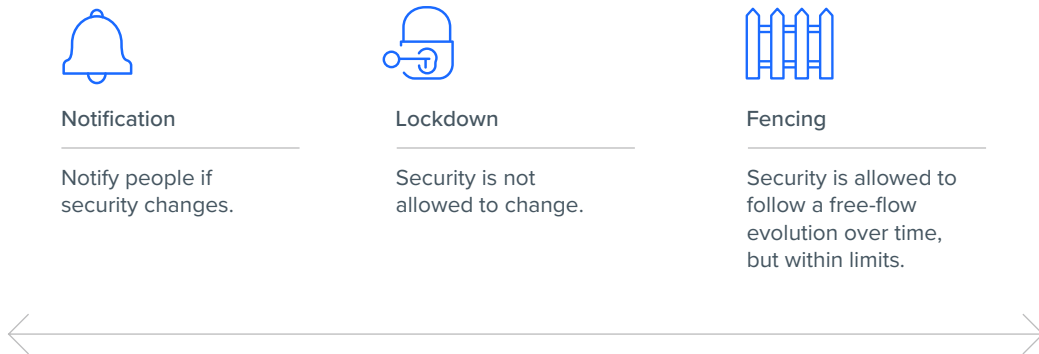


Figure 3. Target-Driven security policies include Security Notification, Lockdown, and Fencing policies. Each is designed to assist data owners in limiting access to sensitive data to only authorized users.

Access Review

Many regulated industries require periodic access reviews, which are the means of providing certification (also referred to as “attestation”) to compliance of 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 NetIQ Data Access Governance 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.

Integration between File Reporter and NetIQ Identity Governance allows for permissions scans conducted in File Reporter to be imported into NetIQ 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 is in compliance with security and access regulations or policies. Depending on the regulation, attestation is dependent on a number of specifications including when the review is conducted, by whom, how the review is conducted, and much more.

The features of the NetIQ Data Access Governance 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.

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 NetIQ Data Access Governance is to protect organizations from unauthorized access through an extensive set of defined requirements.

The NetIQ Data Access Governance solution, with its identity-driven reporting, management, and access review capabilities, is 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.

About NetIQ by OpenText

OpenText provides security solutions that help organizations with workforce and consumer identity and access management at enterprise-scale. By providing secure access, effective governance, scalable automation, and actionable insight, OpenText customers can achieve greater confidence in their IT security posture across cloud, mobile, and data platforms.

Visit the NetIQ by OpenText homepage at www.cyberres.com/netiq to learn more. Watch video demos on our NetIQ Unplugged YouTube channel at www.youtube.com/c/NetIQUnplugged.

NetIQ is part of Cybersecurity, an OpenText line of business.

Connect with Us
www.CyberRes.com

