Expanding Your Identity Management System to Include Data Access Governance

For decades, identity management (IAM) systems have been the means of governing network application access based on user identity and role. Identity and role are not only the foundation on which IAM systems govern application access, but should also be the principal factors in granting or restricting access to unstructured data (the network-stored file-based data that oftentimes contains sensitive information). NetIQ Data Access Governance expands the security offered through your IAM system by securing and managing access to sensitive unstructured data.

NetIQ Data Access Governance at a Glance

Identify

Who can access sensitive files and how that access is derived.

Establish

Approved access for high-risk data locations.

Protect

Sensitive files from unauthorized access through policy.

Extend

Data Access Governance to include business level access reviews.

Identity Management Systems

Organizations deploy identity management (IAM) systems with the objective of ensuring that only authenticated users have access to the specific applications, records, systems, or IT environments to which they are authorized. Through user identity and role, IAM systems provide automated control over provisioning and the process of onboarding new users such as employees, partners, clients, and other stakeholders. Additional controls include separation of duties (SOD), the process of authorizing system permissions for existing users, and the offboarding of users who are no longer authorized to access the organization's systems.

In essence, an IAM system keeps your structured data (data stored in application databases) secure, protected, and in compliance with data privacy and data retention regulations. However, about 80 percent of an organization's stored network data is *unstructured* data, or more specifically, file-based data such as word processing, spreadsheet, media, and a myriad of other file types that aren't stored in databases. And just like structured records in a database that contain sensitive information such as personal identifiable information (PII), unstructured data can also contain sensitive information that needs to be secured.

Data Access Governance

Each year, without exception, there are many reported data breaches at high-profile organizations throughout the word. And while much of the data targeted by cyber thieves is PII, an increasing amount is targeted at intellectual property—often referred to as the "crown jewels" of an organization. Intellectual property is largely unstructured data. This includes sales forecasts located in spreadsheets, legal documents saved as word processing files, financial data in a presentation to shareholders, and even source code for proprietary software.

Recognizing the vulnerability of unauthorized access to unstructured data, analysts have identified and defined the "Data Access Governance" (DAG) market segment. Its objective is to identify stored unstructured data (including "dark data" that hasn't been accessed for years) and who has access to it and then provide the means of securing, protecting, archiving, or disposing of this data through automated processes.

Identity- and role-based management technologies have distinguished NetIQ as a leader in the DAG market, with the ability to address all objectives and requirements of DAG in a way that enhances the security capabilities of your IAM system.

Contact us at **CyberRes.com**
Like what you read? Share it.

Identity- and role-based management technologies have distinguished NetIQ as a leader in the DAG market, with the ability to address all objectives and requirements of DAG in a way that enhances the security capabilities of your IAM system.

NetIQ Data Access Governance

NetIQ Data Access Governance (DAG) provides an integrated product approach to identifying where sensitive files are stored and who has access to them and then provides the automated means of making needed corrections so that your sensitive unstructured data is secure, optimized, and in compliance.

Reporting

The first step in identifying your data access vulnerabilities is to know what files are being stored and who has access to them. This is accomplished through the first product in the DAG product suite, NetIQ File Reporter. File Reporter provides comprehensive reporting and analysis of user access to data stored on the network file system and the Microsoft 365 cloud.

Automated Access Control and Remediation

NetIQ File Dynamics is the second product in the DAG suite. File Dynamics is the "action engine" that, among other actions, establishes access controls and remediates improper access permissions to locations storing sensitive files. Identity-driven policies complement the lifecycle management of your IAM system by provisioning network user and group storage with the proper access permissions and restrictions. Target-driven policies provide additional risk mitigation through data location remediation, data access restrictions, recovery after data loss or corruption, and automated data owner notification when access permissions have changed.

Integration with NetIQ Identity Governance

For organizations that not only need to secure the access to sensitive unstructured data but also demonstrate compliance through access reviews, File Reporter integrates with NetIQ Identity Governance (IG) and extends the capabilities of IG to conduct access reviews on network folders storing sensitive files.

Conclusion

For decades, IAM systems have utilized identity and role to grant or restrict access to sensitive information stored as structured data in database applications. It is a reliable approach that NetIQ has duplicated to protect perhaps your most vulnerable data: the sensitive information located in unstructured data stored in files on your enterprise storage devices and Microsoft 365 cloud.

CyberRes
A Micro Focus Line of Business