opentext™ | Cybersecurity

Solution Flyer

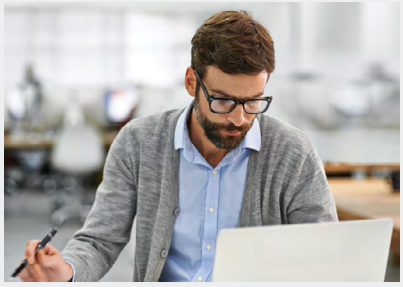
Mitigating Risk through Identity to Govern Access to Unstructured Data

The scope of Identity and Access Management (IAM) is evolving. Governing access to mission-critical data is imperative. Historically, the focus of data access was concentrated on application repositories associated with IAM systems. However, mission-critical data also lives as file-based, unstructured data. Unauthorized access of unstructured data is a risk that analysts, legislatures, CSOs, and compliance officers are all saying needs to be addressed. Fortunately, NetIQ by OpenText has a solution.

File Dynamics at a Glance
- Controls access to file system data
- Enforces access control through policies you define
- Notifies line-of-business data owners when access permissions have changed

File Reporter at a Glance
- Reports on and analyzes file system data
- Includes multiple types of permissions reports
- Integrates with NetIQ Identity Governance

Identity Governance at a Glance
- Performs access reviews on unstructured data
- Conducts periodic and ad-hoc reviews



Basis

Data Access Governance is all about the right people having the right access to the right data at the right time. When that doesn't happen, one of two bad things occur. First, when the wrong people have access to key data, your organization is at risk. Second, when the right people don't have access to the data they need, the organization is operating at less than efficient levels and people go out of band to share data, which can inherently put the data at risk.

If you aren't effectively governing access to your data, you can't meet the compliance requirements your organization might be facing and you will have challenges fulfilling audit requests or attestation needs. In addition, you won't be in a position to adapt to emerging and constantly evolving compliance requirements.

Leading analyst firms have identified a convergence with the NetIQ Data Access Governance (DAG) by OpenText, NetIQ Identity and Access Management (IAM) by OpenText, and NetIQ Identity Governance and Administration (IGA) by OpenText market segments. Without going into a detailed definition of each market segment, it's sufficient to say that what the analysts have determined is that a data access governance strategy ultimately comes down to individual users, their roles in organizations, and their access to data based on their roles.

Traditionally, leading IAM/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? Analysts have concluded that the elephant in the room is the lack of governance for organizations' unstructured data, that is, file-based data that makes up more than 80 percent of organizations' total data.

Recent news stories have demonstrated the devastation that can happen when hackers or other unauthorized individuals gain access to personal and sensitive information located within the unstructured data located on storage devices on the network. That's why everyone from IAM/IGA developers to CSOs are now making unstructured data a focus of their data access governance strategies.

Implementing an Effective DAG Solution

The elements of an effective DAG solution implementation are simple, but challenging. Here are a few strategic considerations:

- A key first step is to analyze your current environment and perform some level of permissions cleanup on high-value-target data areas. The entropy factor of security in unstructured data is typically high, especially in large, complex organizations

with storage environments that have evolved over a long period time or one in which management turnover has occurred.

- Second, the ability to apply policy automatically to data is critical. Again, identity and role are a central driver here, so the ability to drive security to data though identity is imperative.
- Next, you need to monitor security to key data areas and take appropriate action. This could involve notifying data owners* of changes to security or remediating changes in certain situations.
- Last, periodic certification of access to data is required. It is vital that the business-level data owners who understand the access needs of individuals and are ultimately responsible for the stewardship of the data conduct these certification reviews.

Solution

Fortunately, OpenText™ long ago recognized the risks inherent in storing unstructured data and developed industry-recognized tools for identifying what data you are storing, who has access to it, and an automated means of remediating access permissions, moving data, and even disposing of it as specified by regulations or policies.

OpenText is addressing the challenges of the larger Data Access Governance market with a set of integrated products with proven technology.

* The term "data owner" in File Dynamics refers to an individual assigned by a network administrator to perform a limited set of administrative tasks including data recovery, remediation, and lockdown of access permissions. Data owners are typically assigned based on a user's role, including business-level expertise, or association with a folder or share.

File Dynamics

File Dynamics controls access to data stored in the network file system according to identity and role. With File Dynamics, organizations are equipped to extend identity-based security and access management to the largest and oftentimes most vulnerable data segment—unstructured data. File Dynamics automates access assignments and remediation, prevents unauthorized access, mitigates risk, and helps to meet attestation for unstructured data access compliance.

File Dynamics is governed by Identity-Driven policies that you define. User home folders and group folders can be provisioned automatically with the access permissions that are specified in the policy.

Auxiliary storage policies can be the means of provisioning and protecting files with personal identifiable information (PII) from users who should not have access to that information. For example, when John Taylor joins the organization and is provisioned a network home folder through an Identity-Driven policy, an Auxiliary Storage policy will create a separate John Taylor folder in the H.R. Department share where files containing PII can be stored safely and accessed only be members of the H.R. group.

In addition to Identity-Driven policies, Target-Driven policies can be set for any network folder or share. Target-Driven policies can 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.

Many organizations must comply with security regulations that require vigilance in user access to areas of the network containing personal data or other restricted or sensitive information, so being notified of any changes to access permissions can be critical. Security Notification policies let you specify the shares or folders to be analyzed, the frequency of this analysis through scheduled scans, and the data owners who are to be notified when changes in access permissions take place.

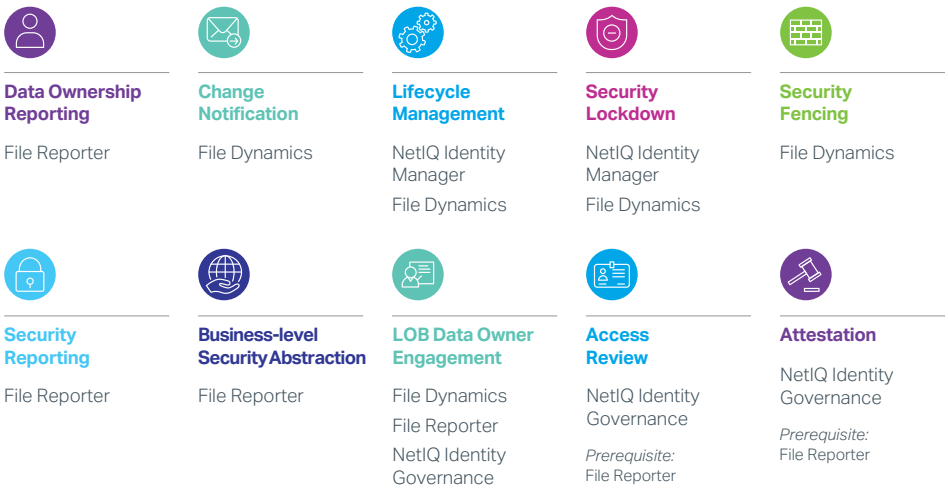


Figure 1. Product map for NetIQ DAG market solution.

OpenText long ago recognized the risks inherent in storing unstructured data and has developed industry-recognized tools for identifying what data you are storing, who has access to it, and the automated means of remediating access permissions, moving data, and even disposing of it as specified by regulations or policies.

Security Notification policies notify data owners of:

- Direct or indirect changes involving who can access designated data
- The details of those changes

Direct access changes involve permissions modification while indirect changes might involve changes in role in the identity system itself. Both of these levels ultimately impact who can access the data and the data owner might want to know about these changes.

Lockdown policies restrict access permissions to a specific set of individual users either through direct assignments or group memberships. Fencing policies set access permissions to authorized users and groups based on roles that can change over time.

File Reporter
File Reporter provides comprehensive reporting and analysis of user access to data stored on the network file system. With File Reporter, administrators can determine quickly if their organization is in compliance with regulations pertaining to security and access to unstructured data.

File Reporter reports on:

- Assigned user permissions for all folders and subfolders from a specified file system path
- All users who can access a specific network folder
- All of the network folders that a particular user can access
- Files containing personal or sensitive information
- The owners of individual files
- And much more

In the process, File Reporter mitigates the risk of unauthorized access, noncompliance, and data breaches.

These capabilities enable organizations to meet both internal and external security goals and also quickly and efficiently respond to audit and attestation challenges.

Identity Governance
Finally and significantly, File Reporter is united with NetIQ Identity Governance by OpenText to provide an extensible framework for business-level data owners to perform periodic access reviews for unstructured data located on high-value targets. This allows the people who are ultimately responsible for the data to certify access to it.

Critically, a business-level abstraction of potentially complex security is presented during the review process, allowing the reviewer to function confidently without subject matter expertise in unstructured data security.

The File Reporter integration with NetIQ Identity Governance allows these certifications to occur alongside access reviews and certifications to applications and application data, following the same paradigm. This ultimately fulfills the requirements that the market and analysts have dictated as convergence occurs.

Additional Features

Because File Dynamics and File Reporter are powered by long-established OpenText file system network technologies, each product offers additional network file system reporting and management features that can ease the workload of storage administrators. For File Dynamics, these features include automated storage provisioning, user and group storage lifecycle management, data load balancing, and disk quota management. File Reporter offers an extensive set of file system reports and a variety of storage analytics tools.

761-000001-004 | O | 10/23 | © 2023 Open Text