CyberRes

Top Reasons

Ten Things That NetIQ Data Access Governance Can Do for You

Securing sensitive data from unauthorized access is a universal objective. But unfortunately, most organizations tend to focus on protecting regulated data, with less concern for the sensitive information in file-based data. That’s where NetIQ Data Access Governance (DAG) can help.

The traditional focus on data security has been on records stored in databases. Known as “structured data,” this data is 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.

An equally vulnerable, but historically less emphasized data set, is “unstructured data” or 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 can also contain sensitive information that needs to be protected. In some cases, it could be PII, but it can also 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.

NetIQ DAG helps secure access to sensitive unstructured data in many ways. Here are ten.

1. **Reduces risk.** Through the reporting capabilities built into DAG, you can determine where sensitive and high-value files are being stored and who has access to them—providing the details you need to take corrective action.

2. **Performs analysis and provides insight into data locations.** The reporting capabilities provide extensive details on the files themselves and answers such questions as: “What files are being stored?” “When was the last time a file was accessed?” “Who owns the file?” “Who can access this file?” and “How is a user’s access to a file derived?”

3. **Reduces your data footprint and exposure.** After performing an analysis of your stored data, you can have DAG take automated action by moving, deleting, or archiving files.

4. **Applies active data governance policies directly to designated locations.** Through Target-Driven policies that you apply to sensitive and high-value network folders or shares, you can lock down access to only authorized users, monitor unauthorized access attempts, and perform data cleanup actions.

Unstructured data can also contain sensitive information that needs to be protected. In some cases, it could be PII, but it can also be the "crown jewels" of a company's data.

Contact us at **CyberRes.com**

Like what you read? Share it.

5. **Engages line-of-business data owners in data management.** It's the line-of-business data owners who are familiar with the data being stored. Working with the network administrators, data owners can review DAG reports and analytics and then specify who should have access to folders or shares storing sensitive or high-value data, along with which files should be retained, archived, deleted, or secured.

6. **Corrects overexposure.** Through DAG's reporting and analytics capabilities, you can identify which sensitive and high-value data is accessible by unauthorized users—either through improper group membership access or the data being stored in a less secure location—and then implement policies or workloads to take action to remediate the risks.

7. **Enforces least privilege user access.** DAG protects your sensitive and high-value data repositories by limiting access permissions to only those users authorized through policy—preventing "privilege creep" that can occur over time.

8. **Outputs files, enabling large-scale data disposition.** DAG's reporting capabilities include the ability to output reports as .CSV files that can be imported into third-party applications that can perform large-scale move, copy, or cleanup operations of sensitive or high-value data.

9. **Enables access reviews.** In addition to generating security reports, DAG can generate an abstraction that can be utilized by NetIQ Identity Governance to conduct access reviews on unstructured data repositories. This enables you to provide attestation in an audit that only authorized users are able to access sensitive and high-value unstructured data.

10. **Connects IAM processes for automatic lifecycle management of data.** As NetIQ Identity Manager (or any other account provisioning system) provisions network application access to users, DAG can simultaneously provision personal network storage for users and provision and provide access to collaborative storage for teams and projects—all based on user identity and role.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/data-access-governance

769-000005-001 | M | 07/22 | © 2022 Micro Focus or one of its affiliates. Micro Focus, NetIQ, and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

CyberRes
A Micro Focus Line of Business