

United States County Administration

NetIQ Data Access Governance provides data visibility and enables storage and backup savings through automated data management.



Managing Explosive Data Growth by Introducing Automated Data Governance

This large county is in a major US state with a fast-growing population. The county employs a small IT staff to serve over a million citizens and nearly 6,000 county employees. With limited IT funds, it made the decision to store a significant percentage of its production data on a single network attached storage (NAS) device. The county's Director of Information Technology Services explains more: "Over the years, we've seen a data explosion in line with our county's population growth. We now have many terabytes of unstructured data captured in over 150 million files. We didn't have any automated data management processes in place, and our staff is just not equipped to

"DAG felt like a natural extension to our existing NetIQ identity and access solutions. Its built-in and custom reports ensured that our IT department now has automated and dynamic reports identifying our ROT data so that we can take remediating actions immediately."

Director of Information Technology Services
United States County Administration

keep track of the data being stored by all county employees. This means we had little visibility into the age and value of our data. As a government organization, it is vital to get a clear handle on where our data resides and who has access to it so that we can start to apply structured data governance rules."

The county is a long-term user of NetIQ Identity Manager™ and Identity Governance™ to manage its user provisioning and access processes, so it made sense to look to NetIQ for this particular challenge. OpenText™ recognizes the risks inherent in storing unstructured data and has developed industry-leading solutions for identifying what data organizations store, where it is housed, and who has access to it. With an automated means of remediating access permissions, moving data, and even disposing of it as specified by regulations or policies, NetIQ Data Access Governance™ (DAG) consists of a set of integrated products with proven technology.

Identifying ROT Data Leads Directly to Storage and Backup Savings

Although the decision for DAG was easily made and justified, that was just the start of the county's work to extend its data access governance beyond the structured data managed and secured through Identity Manager and Identity Governance. The team

At a Glance

Industry

Government

Location

United States

Challenge

Manage explosive data growth and gain clear data visibility to reduce data footprint while complying with security regulations

Products and Services

[NetIQ Data Access Governance](#)

[NetIQ Identity Manager](#)

[NetIQ Identity Governance](#)

Success Highlights

- Reduced data footprint by identifying and managing ROT data
- User-friendly out-of-the box actionable reporting
- Clear data storage and backup savings through unstructured data management
- Improved data insight and regulation compliance
- Automation to support a small IT staff in managing 150 million data files

“Out-of-the-box reports in File Reporter gave us a clear overview of our ROT data. We created an automated duplicate file report as duplicate data forms the low-hanging fruit that we could address straight away to save on storage and back-up costs.”

Director of Information Technology Services
United States County Administration

Connect with Us

www.opentext.com/products/security-cloud



needed a good understanding of the opportunities DAG presents, and a tailor-made OpenText workshop gave them a high-level overview of how DAG could support the county's objectives. The county was particularly interested in identifying its redundant, obsolete, or trivial (ROT) data so that it could focus on reducing and restructuring its data footprint, which for an organization of its size is quite substantial. An in-depth OpenText training helped with this and ensured that the team felt empowered to implement DAG components to great effect.

Part of the county's challenge was to unravel complicated NTFS permissions and highlight any anomalies that could present a security risk. A key first step is to analyze the existing environment and review permissions. File Reporter, as part of DAG, was implemented to inventory metadata and NTFS permissions. The solution provides comprehensive reporting and analysis of user access to data stored on the network file system. The county generated an automated data analytics dashboard for full visibility.

“Out-of-the-box reports in File Reporter gave us a clear overview of our ROT data,” says the Director of Information Technology Services. “We created an automated duplicate file report as duplicate data forms the low-hanging fruit that we could address straight

away to save on storage and back-up costs.”

In addition, the team used the designer feature within File Reporter to create some custom reports, with support from OpenText. These custom query reports provided detailed and actionable information on both ROT and ad hoc data, including NTFS permissions.

DAG Automation and Scalability Provides Data Visibility and Regulation Compliance

As a government organization, the county is subject to stringent audits and regulatory requirements, so understanding data growth trends, the types of data it holds, and its relevance is vital. File Dynamics, as part of DAG, provides the ability to apply agreed data management policies automatically, including data cleanup. By taking coordinated action with Identity Manager, it uses identity and role as its central driver, so that data security is consistently driven through identity.

The Director of Information Technology Services concludes: “DAG felt like a natural extension to our existing NetIQ identity and access solutions. Its built-in and custom reports ensured that our IT department now has automated and dynamic reports identifying our ROT data so that we can take remediating actions immediately. With a small staff looking after our IT infrastructure and managing over 150 million data files,

we realize that automation and scalability are essential. We now work efficiently and ensure our regulatory compliance. We were pleased to reduce our data footprint with associated cost savings.”

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.