rubrik

Williamson County Gains Peace Of Mind With Rubrik Sensitive Data Discovery

"As a small team, we cannot be monitoring our environment at all times. Sensitive Data Discovery automates that, providing 24/7 monitoring and alerts to any anomalies."

Rory Tierney
IT Infrastructure Manager

Williamson County, located in central Texas, is home to over 600,000 residents. Information technology lies at the heart of the County's operations with all County services relying on IT infrastructure for critical services, including public safety, 911, and court systems.

Rory Tierney, IT Infrastructure Manager at Williamson County, manages all aspects of virtualization, networking, and disaster recovery for the data center. With a small infrastructure team consisting of four people, Rory Tierney, Thomas Gillespie, Chis Ball, and Nick Delhoussaye, the County needs solutions that deliver high operational efficiencies while reducing costs. At the same time, the County is faced with a growing population and continuously increasing the footprint of sensitive data.

"Prior to Sensitive Data Discovery, we did not have a solution in place for comprehensive data governance. Now, we have greater visibility and control over how our citizens and employees' sensitive data is managed," said Tierney.

Reducing Time Spent On Audits For HIPAA And CJIS Compliance

As a local government, Williamson County must comply with several industry and federal regulations, including Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Criminal Justice Information Systems (CJIS). For the latter, local, state, and federal governments access CJIS databases for law enforcement activities, including performing background checks and tracking criminal activity.

"Ensuring CJIS data does not fall in the wrong hands is absolutely critical. Non-compliance or failing a CJIS audit could mean losing our ability to run queries for criminal histories. On the other hand, HIPAA violations can range from $100 to $50,000 per violation or record depending on how much data is exposed," said Tierney.

"In the past, finding data for audit requests was like searching for a needle in a haystack, compounded by massive data sprawl across various systems and locations. Sensitive Data Discovery helps to automate and reduce the time spent on discovery tasks," said Tierney.

"With Sensitive Data Discovery, we can also create and share reports with our leadership team. As a result, we have begun defining data governance policies to better manage our sensitive data."

INDUSTRY

Local Government

RESULTS

- 1 day to resolve internal investigation request (vs. thousands of hours with manual processes)
- Minimized risk of CJIS and HIPAA violations with continuous compliance
- Zero production impact

THE CHALLENGE

- Time-consuming manual data discovery processes for audits or internal projects
- Small team managing an ever-increasing amount of sensitive data
- Inability to monitor 24/7 what sensitive data resides where for compliance requirements

Faster Time To Resolution For Internal Investigations With Automated Search

When faced with a critical internal investigation, the team leveraged Sensitive Data Discovery to automate data discovery processes, resulting in faster time to resolution.

“We ran a custom report with Sensitive Data Discovery in order to find a specific data set across all our records. Sensitive Data Discovery provided easy customization of search requests so that we could refine our results to a specific set of files. This would have been extremely difficult prior to Sensitive Data Discovery, requiring us to comb through millions of files to find a specific keyword match. We were able to complete this task with Sensitive Data Discovery in one day versus what would have been thousands of hours,” said Tierney.

When Williamson County ran an initial scan across its environment, it found upwards of 8 million hits for PII and HIPAA data.

“Sensitive Data Discovery provided us with an instant baseline into what types of sensitive data was being stored where. As a result, we could quickly remedy any inaccuracies as well as confirm or whitelist locations with known sensitive data,” said Tierney.

“Furthermore, as a small team, we cannot be monitoring our environment at all times. Sensitive Data Discovery automates that, providing 24/7 monitoring and alerts to any anomalies.”

Choosing Rubrik Sensitive Data Discovery For Simplicity And Support

A key reason Williamson County chose Rubrik Sensitive Data Discovery was for its management simplicity and exceptional 24/7 support.

Tierney said, “Sensitive Data Discovery is extremely easy to use. From setup to daily management, the UI is very intuitive and anyone can learn it without training. Also, we had a great experience with the entire Sensitive Data Discovery team to quickly resolve support issues. As an early adopter, we even worked closely with the Sensitive Data Discovery product and engineering team to develop a custom CJIS policy and helped define the analyzers for a pre-built policy moving forward, including FBI and state identification numbers.”