How Varonis Helps a U.S. State Agency Shield Sensitive Federal Tax Information Against Cyberthreats

CASE STUDY

“Get the Data Risk Assessment. You’ll see how much you stand to benefit from having Varonis in your security stack. We thought we were covering everything, but the assessment showed us areas where we were still at risk and helped us take the steps needed to mitigate that risk.”

ABOUT THIS CASE STUDY:

Our client is a U.S. state agency. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Combating “permission creep” and remediating overexposed data
- Classifying and deleting stale data to meet regulatory standards
- Reducing attack surface by eliminating security gaps that leave them vulnerable to cyberthreats

SOLUTION

The most robust data security platform:

- **DatAdvantage** for Windows to support their on-premises data stores
- **Data Classification Engine** for Windows and SharePoint to scan and classify personal data
- **Data Transport Engine** to automate data migration based on predefined rule sets
- **DatAlert Suite** for threat monitoring and incident response

RESULTS

- Least privilege for more data security
- Efficient and thorough incident response procedures
- Compliance reports created within minutes

Challenges

FIXING SECURITY GAPS THAT COULD LEAD TO DATA BREACHES

In 2019, more than half of all reported ransomware attacks in the United States targeted state or local governments. From January to October, there were over 140 attacks targeting public government agencies and healthcare providers—a 64.7% increase since 2018.

Seeing the rising threat, one U.S. state agency (anonymous by request) has taken steps to proactively mitigate risk. They have a centralized IT section handling front-end defenses, and Varonis providing visibility into their infrastructure and real-time alerting.

As the agency’s Information Security Analyst says:

> “In the information and cybersecurity industries, you have to be proactive. If you’re reactive, you won’t be able to protect your organization or its end users.”

Like many organizations, years of employee turnover and internal role changes had led to “permission creep” within their agency. A lot of their folders were overexposed, leaving sensitive data at risk.

> “We manage and use federal tax information. Because of that, we need to have specific safeguard controls in place so we can tell the IRS that we know where all of the information is, who has access to it, and who’s getting into it and why.”

They chose Varonis based on the recommendation of another state department. They saw firsthand how it helped that other agency gain more visibility, find and classify personal information, and detect anomalous activity.

> “We were trying to get a handle on all of the data in our servers. We thought we knew where it was, but a Data Risk Assessment revealed a lot of data that we didn’t know about. We didn’t realize we had so many folders with open permissions.”

“In the information and cybersecurity industries, you have to be proactive. If you’re reactive, you won’t be able to protect your organization or its end users.”

Solution

IMPROVED VISIBILITY AND RISK REMEDIATION

Varonis' Data Risk Assessment was instrumental in helping the Information Security Analyst and their team communicate the risk present in their servers to leadership.

The initial assessment gave them hard proof that almost 68,000 folders were open to Global Group Access, and 48.6% of their data was stale.

> "Having concrete figures to back up our claims and prove why we needed to fix overexposed files helped us convey that information to our leadership and communicate the importance of remediation."

Varonis shows them where they are most at risk and outlines steps they can take to mitigate that risk. It also helps them solve three major challenges:

#1. Cleaning up overexposed and stale data

Using DatAdvantage and Data Classification Engine, the state agency has a clear understanding of where sensitive information lives, and they have the ability to clean up permissions and correct overexposure.

> "Before Varonis, all of our taxpayer service center information was open to everyone in our department. That's not least privilege. That's not what you want. Varonis enabled us to go through all of our taxpayer service center shared drives and limit who has access to sensitive data like federal tax information."

According to the Information Security Analyst, manual remediation was beyond the pale of what they were able to do before Varonis.

> “We have ten service centers. Having to go through each of them manually would have been a nightmare. I wouldn’t even attempt it without Varonis.”

To expedite remediation, the state department also implemented Data Transport Engine. Data Transport Engine allows them to create rules to enforce security policies based on context, activity, classification, and permissions, and then it automatically moves sensitive and stale data to where it belongs.

#2. Defending personal data from insider and outsider threats

DatAlert Suite helps the state agency improve their incident response and threat monitoring capabilities. With it, they’re alerted to any and all potential issues, including anomalous user behavior and early warning signs that could be indicative of potential attacks.

> “We’ve been using Varonis in conjunction with our central IT team to detect potential problems, such as people visiting websites that they shouldn’t—websites that might infect their device with malware.”

#3. Proving compliance with data protection regulations

As a department of the state, the agency needs to perform annual audits to prove compliance under IRS publication 1075. In other words, they need to demonstrate that they have safeguards in place to protect federal tax information and personal user data.

> “We used to scan our network for NESA compliance, and that was about it. With Varonis, we’re able to prove that we know where information lives and that it’s protected. We can also demonstrate that we are capable of addressing concerns quickly and limiting the impact of potential threats.”

They used to have to create compliance reports manually. With Varonis, comprehensive compliance reports are ready within minutes, whenever they’re needed.

> “Generating reports used to be a time-consuming and labor-intensive process. Now we get the same information in 5–10 minutes. It’s wonderful.”

> “Varonis enabled us to go through all of our taxpayer service center shared drives and limit who has access to sensitive data like federal tax information.”

Results

ROBUST DATA VISIBILITY AND SECURITY

According to their Information Security Analyst, Varonis revolutionized their data clean-up effort and it had a major impact on their threat detection and incident response procedures.

> “Our old solution would notify us about some things, but we weren’t getting the big picture. With Varonis, we see every potential anomaly. It speeds up our incident response procedures 100x or more.”

Looking back, they’re pleased that they decided to move forward with the initial risk assessment. That first step showed them that even though they thought all of their data was secure, there were still unknown gaps in their defenses.

> “Get the Data Risk Assessment. You’ll see how much you stand to benefit from having Varonis in your security stack. We thought we were covering everything, but the assessment showed us areas where we were still at risk and helped us take the steps needed to mitigate that risk.”

But even with all of those improvements, the agency isn’t stopping there. They’re now considering adding other Varonis solutions that will give them even more visibility and control into their on-prem and cloud environments.

> “We are looking at adding DataPrivilege and Automation Engine. DataPrivilege would give us a good data access governance solution, and Automation Engine would help remove the burden on my team when it comes to repairing and maintaining file system permissions.”

“With Varonis, we see every potential threat and anomaly. It speeds up our incident response procedures 100x or more.”

VARONIS

Overexposed data increases your risk of attacks and leaves you vulnerable to data breaches.

Discover where you’re vulnerable and solve your biggest security gaps with Varonis.

REQUEST A DEMO