How a Local Government Uses Varonis SaaS to Automatically Eliminate Data Exposure in Microsoft 365

> The strength of Varonis comes not only from the product but from its people. The product is excellent, but it's definitely supplemented by the people, their knowledge, and their ability to solve the problem for the customer.

About this case study:

Our customer is a U.S. based local government. We have happily accommodated their request for anonymity.

HIGHLIGHTS

Challenges

+ Protecting the sensitive data of county residents and employees
+ Complying with PCI, HIPAA, and CJIS regulations
+ Safeguarding critical public systems from cyberattacks

Solution

The Varonis Data Security platform:

+ Discovers and locks down sensitive data automatically
+ Monitors and notifies of abnormal behavior in critical systems
+ An incident response engineer to proactively investigate anomalous behavior

Results

+ Visibility and control of sensitive data and permissions for thousands of employees
+ Hundreds of thousands saved with Varonis versus in-house management
+ Easy transition to Varonis' cloud-hosted platform
+ Automated security outcomes

CHALLENGES

Overpermissive and risky permissions in Microsoft 365

The Chief Information Security Officer (CISO) at a large U.S. local municipal government knew that Microsoft 365 sharing and permissions had the possibility to expose sensitive data.

With millions of files across the organization created and shared by thousands of employees, it was a risk that would be virtually impossible to stay ahead of manually.

> **"What keeps me up at night is someone exposing sensitive data to everyone on the internet."**

As a local government, the county safeguards vital information that, if compromised, could not only grind operations to a halt, but in a worst-case scenario, disable the essential safety and lifesaving services people rely on.

> **"We have the responsibility to protect any type of local government data that you could imagine. Anything from credit card information to healthcare information of our citizens, to critical infrastructure, including traffic lights, water, sewer — and even 911 call operations."**

> **“If systems are breached, there’s a potential for someone to die.”**

The county also must comply with many data regulations, including PCI for credit cards, HIPAA for healthcare services, and CJIS for criminal justice services. All these regulations require strong access controls over systems and data under their care.

Before searching for an outside solution, the county turned to consulting services from a major IT software vendor for help to remediate access to sensitive information, but progress was slow. Using custom scripts from the vendor, it took a month to remediate permissions for 185 accounts — at that pace, it would take years just to make a dent in the project, let alone keep up with mounting risk as new files are created and shared.

The security leadership team knew that a manual approach to tackling this risk was not a viable option, so they turned to the leader in automated data security, Varonis, for help.

“These systems are critical. If systems are breached, there’s a potential for someone to die.”

SOLUTION

Safely eliminating exposed data with automation

With Varonis, the security team remediated thousands of excessive permissions in just two weeks. They even uncovered issues the county didn't know about, such as incorrect settings and abandoned services.

> **"It was a shock that Varonis could do it so quickly and that it worked smoothly. Varonis professional services even wrote some custom programs for us to do further analysis and remediation in our Microsoft 365 environment."**

Varonis looked across the millions of files that the county had in Microsoft 365—across OneDrive, SharePoint, and Outlook — and analyzed who actually was using those files and needed access, automatically eliminating unnecessary permissions, all with little intervention from the CISO or their team.

Detecting and responding to threats proactively

Cybercriminals have their sights set on U.S. state and local governments, and the CISO wanted to do everything possible to protect the county's sensitive data. Not only does the county use Varonis to monitor and alert on any unusual behavior in Microsoft 365, they also get help from a dedicated security analyst.

> **"We've been paired with an incident response engineer from Varonis who brings anything to our attention that has been validated as a potential security incident that needs our immediate attention."**
>
> **"We're using Varonis to consume our Microsoft 365 logs to allow us to detect and do further log analysis of security incidents that happen within that environment."**

The CISO's team prefers using Varonis over their own SIEM tool because it's easier to use, has more context, and has fewer false positives.

> **"Knowing with fairly high confidence that they are legitimate alerts that need attention rather than just noise saves my team a fair bit of time."**
>
> **"They don't have to click around or write custom queries to find it. They can just go through the interface, click, and drill down, and group events very easily."**

Reaping the benefits of SaaS

As a security leader who is focused on achieving security outcomes, the county's CISO saw huge benefits in transitioning to Varonis' cloud-native offering.

Not only would they receive faster feature delivery (without their team managing any upgrades), they also benefited from the added support from the Varonis Proactive Incident Response Team, who proactively monitors their alerts.

> **"Taking these products and moving up to the Varonis cloud makes it easier for us to manage the solution. We're in the process of implementing all the additional features that are part of their cloud service."**

The CISO was impressed with the support they received from Varonis during the move.

> **"The move over was actually very easy to install. When they discovered an issue or when I brought it to their attention...I was amazed at how quickly they were able to map everything out. It was very easy for us to do the actual move."**

“The strength of Varonis comes not only from the product but from its people. The product is excellent, but it’s definitely supplemented by the people, their knowledge, and their ability to solve the problem for the customer.”

RESULTS

Saving hundreds of thousands every year

By upgrading to Varonis' cloud-native data security platform, the county is positioned to achieve effortless security outcomes. With the automation built in to the Varonis Data Security Platform, and the additional support and expertise of the Proactive Incident Response Team, the team can not only manage, but also get ahead of risk.

The CISO estimates the county saves hundreds of thousands of dollars every year by having Varonis manage their cybersecurity.

> **"We're not having to manage databases or software upgrades. That's all handled by Varonis. And if we find we need to expand our capabilities, it's simple to set that up."**

At a time when budgets are strained and open security roles abound, the county is paying less for Varonis than they would pay to hire additional incident responders.

The CISO explains:

> **"The cost of Varonis was much cheaper than what we could hire an incident response engineer to begin with. We're able to extend the team without a lot of additional cost and get all the additional product features that are available with Varonis."**

Automating data security

The county's CISO knew from the beginning that a manual solution would not be able to effectively minimize their risk. Instead, they're harnessing automation to stay ahead of potential threats.

Today, the U.S. county is implementing automated responses to file-sharing and permission changes. If someone makes a permission change in the middle of the night, Varonis can detect that change and stop it in its tracks without any human intervention.

> **"If a police officer shares a file containing sensitive PII or credit card numbers — and they intended to send it to a single individual but instead shared it to the entire internet — Varonis will see that and automatically call back that permission. It's automatically handled in near real time, without any human interaction at all."**

With Varonis' intelligent automation, the security team can confidently revoke unnecessary access without impacting productivity.

> **"We have improved our existing file-sharing capabilities without impacting our users and, at the same time, can detect and respond to incidents within our Microsoft 365 environment much faster and without outside human help."**

This proactive permissions remediation, coupled with the data-level threat detection Varonis provides, helps the county not only monitor for potential incidents, but also limit the damage any actor could do, especially insiders who may not necessarily be acting maliciously and not trip alarms.

A partnership focused on outcomes

According to the CISO, working with Varonis is a true partnership:

> **"The product is very good. Their services are amazing. So, that's what working with Varonis is — it's more of a partnership than just buying a product and then once a year hear from the sales rep to get another year of support. Their whole focus is on making sure that everything runs smoothly and that you're happy with the solution."**

“We’re not having to manage databases or software upgrades. That’s all handled by Varonis engineers. And if we find we need to expand our capabilities, it’s a simple notification to set that up.”

Win the race against risk.

Achieve effortless security outcomes with Varonis SaaS.

Request a demo