How a U.S. County Decreased Incident Response Times by 500% with Varonis

CASE STUDY

"Varonis has given us the ability to respond faster. It used to take us 25 minutes and three teams to hunt down and fix a problem. **Now one user can solve the same problem within five minutes**."

ABOUT THIS CASE STUDY:

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

HIGHLIGHTS

CHALLENGES

- Protecting over 3,000 users and over one million residents who would be affected by attacks
- Addressing ransomware quickly, before it can move laterally to infect other systems and devices
- Gaining visibility into file shares and Active Directory to find and eliminate overexposed data

SOLUTION

The most robust data security platform:

- **DatAdvantage** maps user activity and permissions across data stores, email, and Active Directory
- **DatAlert Suite** provides advanced threat detection and file monitoring
- **Data Transport Engine** automatically moves, archives, and deletes stale sensitive data
- **Automation Engine** automatically fixes tens of thousands of folders with global group access
- **Edge** provides perimeter telemetry by analyzing metadata from DNS, VPN, and web proxies

RESULTS

- 500% faster threat detection and response time
- Automated systems to detect and eliminate malware before it spreads—and prevent infection in the first place
- Visibility into overexposed data in file shares and Active Directory attack paths

Challenges

MITIGATING THE THREAT TO GOVERNMENT AGENCIES

When ransomware attacks hit U.S. cities and counties, they affect millions of lives by disabling vital public services for days (or even weeks) and requiring costly remediation to get systems back online.

One U.S. county (anonymous by request) refused to be the next victim. Its Chief Security Officer (CSO) had witnessed firsthand how costly and devastating those attacks could be.

> “There’s no way to describe the feeling of opening a folder and seeing a wall of encrypted files and a ransom note. It makes your stomach drop.”

The threat was real. In their state, nearly a dozen neighboring municipalities had already been hit with ransomware. If this county was next, it risked disrupting daily life for over a million residents.

> “When you’re faced with a ransomware attack, you have **less than five minutes to respond before your entire environment is at risk.**”

> “There’s no way my team could respond that fast. We had zero visibility into our file shares and zero control when it came down to permissions.”

In a best-case scenario, the CSO says it would have taken 25 minutes to mobilize three teams, investigate an alert, find the source of the threat, kill it, and then either disable the port or restore the file share. In that scenario they might contain the problem, but they would have no way of knowing what files had been touched.

The security team needed a way to improve their response time and gain more visibility into their environment. So they approached Varonis.

But after deploying Varonis, they discovered that the county was far more vulnerable than they’d previously imagined.

> “To find out that we had so many folders open for everyone to access… that blew my mind. I had no idea a misconfiguration on the file share had left a huge swath of files vulnerable. It was an enormous problem that we wouldn’t have discovered without Varonis.”

If they’d fallen victim to an attack, over 3,000 users and tens of thousands of files could have been compromised in mere minutes. Remediation had to happen—and fast.

> “Varonis threw a bright light on our current situation and showed us that we had big security gaps we needed to fill in.”

"When you're faced with a ransomware attack you have less than five minutes to respond before your entire environment is at risk. There's no way my team could respond that fast."

Solution

DATA-CENTRIC APPROACH HELPS INCREASE EFFICIENCY AND REDUCE RISK

Varonis works hand-in-hand with businesses to help them monitor, protect, and manage their data. For the U.S. county, this **operational journey** started with DatAdvantage for Windows.

DatAdvantage enables the CSO to discover privileged accounts and gives them more visibility into the county's data risk profile. With DatAdvantage, they discovered and identified tens of thousands of exposed files that were increasing the county's attack surface.

> “Consider what would happen if you didn’t have that level of visibility, and an audit comes along. How do you respond? If you don’t have the ability to identify all of your files or know when something has changed, how can you possibly hope to respond to ransomware in your environment?”

With DatAdvantage, it was finally possible to find and fix overexposed data. But remediation takes time—time the CSO didn’t have with an entire county’s data security at risk. So to expedite the process, they adopted Automation Engine.

Automation Engine helps organizations remove global group access to a large number of folders quickly and safely. While DatAdvantage is great for remediating dozens of folders at a time, organizations with tens or even hundreds of thousands of overexposed folders need Automation Engine.

> “According to the county’s Information Security Officer, “Automation is integral for our environment. It lifts the workload off of our engineers, freeing them up to focus on investigating the root cause of issues instead of firefighting all the time.”

At the same time, the county deployed **DatAlert Suite**. DatAlert’s robust threat detection capabilities combined with its deep forensic insight helps the security team understand and investigate every potential threat. It also enables them to stop hackers in their tracks before they can expand into other network systems and devices.

> “The moment Varonis detects signs of an attack, it immediately kicks the affected user off of the network and stops the attack. By the time we receive an alert, Varonis has already acted on it. That gives us time to go back and investigate what happened.”

The county also uses **Data Transport Engine** to automatically move, archive, quarantine, and delete stale sensitive data. This preventative measure simplifies permission structures—reducing complexity and risk and dramatically increasing operational efficiency.

More recently, the CSO has been demoing **Edge**. Edge analyzes metadata from DNS, VPN, and web proxies to spot even the most subtle signs of attack. Varonis combines this perimeter telemetry with knowledge of Active Directory and file server activity to give the CSO a 360-degree view of the county’s data security.

> “Varonis Edge is now giving us visibility into the network, our VPN, and also our DNS and web proxies. Going from this initial investment to what we have now—Varonis has definitely surprised us.”

“Automation is integral for our environment. It lifts the workload off of our engineers, freeing them up to focus on investigating the root cause of issues instead of firefighting all the time.”

Results

500% FASTER THREAT DETECTION AND RESPONSE TIMES

When the county approached Varonis, its main goal was to gain visibility into file servers and boost incident response procedures. The CSO expected an improvement—but was blown away when Varonis helped them **decrease incident response times by 500%.**

> “Varonis has given us the ability to respond faster. It used to take us 25 minutes and three teams to hunt down and fix a problem. Now one user can solve the same problem within five minutes.”

With Varonis—especially Automation Engine—they’ve cleaned up thousands of overexposed files, thereby mitigating risk to files shares and dramatically decreasing the county’s attack surface. They’re also able to prevent a repeat occurrence; Varonis automatically finds and fixes new folders that are created and accidentally left open to all users.

The county has never had more visibility into file shares and Active Directory. And, as they prepare to expand their use of cloud storage, they’re also considering Varonis for Office 365.

> “It just makes sense that the next evolution of what we do is add Varonis into our security stack going into the cloud. We want to aggressively move to Office 365. We need the same protection there that Varonis is providing for us onsite.”

The only negative part of partnering with Varonis? According to the CSO, it's that they now have unreasonably high expectations whenever they interview potential new vendors.

> "I hate Varonis for setting the bar so high," they laugh. "I've worked with other service providers before and it took them forever to get engaged. The Varonis Incident Response Team will jump in on any issue for free—any time, any day. That's immensely valuable."

"The Varonis Incident Response Team will jump in on any issue for free—any time, any day. That's immensely valuable."

Does your cybersecurity start at the heart?

Get a customized data risk assessment and start your operational journey today.

REQUEST A DEMO