How Varonis Helps a Top-20 Operator of Urgent Care Clinics Resolve Security Incidents Quickly and Conclusively

CASE STUDY

"To go through our main file server and lock it down the way Varonis does—it would be a multi-year project, requiring my entire team, and we probably still wouldn't be done."

CHRIS M., System Engineer

ABOUT THIS CASE STUDY:

Our client is an operator of urgent care clinics. They've graciously allowed us to name the system engineer we interviewed. We've happily anonymized all other information.

HIGHLIGHTS

CHALLENGES

- Protecting critical data with a smaller security staff
- Gaining insight into alerts to stop threats before they can escalate
- Maintaining PCI and HIPAA compliance

SOLUTION

The most robust data security platform:

- **DatAdvantage** to assess, prioritize, and mitigate the biggest IT security risks
- **Data Classification Engine** to find and classify sensitive data wherever it's hiding

RESULTS

- Visibility and alerting into critical systems enables system engineers to quickly respond
- Automated reporting saves 150+ hours annually and simplifies PCI compliance
- Increased confidence despite more users working from home

Challenges

PROTECTING CRITICAL DATA WITH A SMALLER SECURITY STAFF

Chris was sitting in his office when a Varonis alert flashed across his screen. His breath caught in his throat.

> "One account had accessed a folder and touched everything—around 15,000 files. There's no way someone would do that unintentionally," he explains.

Time was of the essence. His company (anonymous by request) is a top-20 operator of urgent care clinics. It's responsible for protecting sensitive data, including PCI and HIPAA.

In a worst-case scenario—an exfiltration attempt—Chris had mere minutes to kill the attack before a major data breach. His small team needed to leap into immediate action.

Fortunately, Varonis gave Chris all the warning, insight, and control he needed to quickly get a handle on the situation.

> “Varonis warns me the moment it detects behavior that’s out of the norm. If a user typically touches 10 files a day, and suddenly they touch 3,000 files, we know something’s wrong.”

Chris’s company implemented Varonis months prior to rein in over-permissiveness and lock down sensitive data. Their top priorities: enforcing data security controls and gaining visibility into where sensitive data was stored and who had access to it.

> “We had policies in place, of course, but without a way to audit and enforce, you just don’t know. Varonis came in and opened our eyes to issues that we suspected but couldn’t prove.”

Because of this early adoption, the engineering team had already taken steps to move towards least privilege. They’d locked down sensitive financial data and the company was PCI compliant.

So when Chris received the alert, all he had to do was follow the trail of breadcrumbs using Varonis’ suite of security products to get to the bottom of the problem.

“We had policies in place, of course, but without a way to audit and enforce, you just don’t know.”

Solution

DATA-CENTRIC SECURITY PLATFORM

Part and parcel of the Varonis solution is advanced security insights, out-of-the-box threat analytics, and a playbook that tells Chris exactly how to respond to a security incident.

He was poised to deactivate the account if it had been compromised—but, thankfully, that wasn’t necessary.

> “The person had been tasked with moving data. It was a false alarm. But I’d much rather have a false alarm than be blind to someone exfiltrating out an entire directory,” Chris says.

In situations like this, **DatAdvantage** supplies the forensic evidence. With DatAdvantage, Chris has a comprehensive audit trail to follow—he knows exactly who's responsible, what's been accessed, and what's been changed. He can also perform remediation if a user has too much access.

> "I love the ease of investigation. We're no longer playing 'whodunit;' I can see the specific file that was changed, who was responsible, and the exact time the edit took place. I don't have to dig through audit logs—it's all there for me, in one spot," he says.

Data Classification Engine adds additional context to at-risk areas. It points out sensitive data that's been improperly stored, which helps the company maintain PCI and HIPAA compliance.

> "Varonis pointed out who was storing information in location A, when it should have been in location B—internal exposure concerns and compliance exposure concerns," Chris says.

These solutions work seamlessly together, enabling Chris to assess, prioritize, and mitigate the biggest IT security risks with ease. When it comes time to show his work, Varonis' built-in reports make it easy to prove compliance and showcase risk mitigation measures.

In fact, according to Chris, the insight Varonis provides is often on par with SIEM solutions. But while SIEMs produce a ton of logs that require a lot of manual labor to parse through for actionable insight, Varonis reports are crystal clear.

> “I send a lot of information to our main SIEM and I have to parse that data out. It’s labor-intensive and it means a lot of PowerShell scripting on my part to weed through the data,” Chris explains.
>
> “We didn’t feel the need to integrate it with our SIEM because Varonis does a good job on its own. The Varonis console and management pane gives us everything we need. I live in the report builder and it’s super easy to filter data,” he adds.

“We didn’t feel the need to integrate it with our SIEM because Varonis does a good job on its own. The Varonis console and management pane gives us everything we need.”

Results

MOVING PAST ASSUMPTIONS TO DATA-CENTRIC ASSURANCE

Before Varonis, Chris says his small team had been flying blind—relying on best guesses to fill gaps in their data security. By shining a light on their environments, Varonis takes the teeth out of security incidents like the user who touched 15,000 files.

> "Varonis, hands-down, frees up the need to have extra bodies looking for security holes, locking down permission shares, auditing, and everything in between," he says.

Varonis helps Chris and his small team stay nimble. It eliminates the need for full-time hires to monitor data logs, and it enables the team to instantly react to security incidents. According to Chris, the **reporting feature alone saves upwards of 150 hours annually.**

> "I used to have to create reports as best I could for our Head of Accounting. Now, it's all automated. Varonis sends them a weekly report and I don't have to lift a finger."
>
> "Automated reporting alone saves us two to three hours per week. As for auditing, I can't even give you a realistic number—it would be such a huge and involved project."

Varonis plays a leading role in helping his company achieve and maintain least privilege. It also provides 24/7 monitoring of some of the company's most critical folders.

> “To go through our main file server and lock it down the way Varonis does—it would be a multi-year project requiring my entire team, and we probably still wouldn’t be done.”

Chris expects Varonis to play an even more pivotal role in the months and years to come. As working from home slowly becomes the new norm, attack surfaces are increasing exponentially. His company may soon also be moving data to the cloud and, if that happens, having Varonis already on hand will be a huge advantage.

> “COVID was the stick of dynamite that blew the door open to telecommuting. If you’re serious about data security, you’ll realize the value of Varonis. My advice? Get it and don’t look back.”

“Automated reporting alone saves us 2–3 hours per week. As for auditing, I can’t even give you a realistic number—it would be such a huge and involved project.”

Don’t let threats slip by unnoticed.

Varonis helps you detect and respond to security incidents with confidence.

REQUEST A DEMO