How Varonis Helps a One-Person Security Team Save Over 400 Hours Annually

CASE STUDY

"When it comes to data forensics and intensive analysis, a small team just doesn't have enough time. Varonis is invaluable in that regard—you need it to extend the capabilities of one person."

ABOUT THIS CASE STUDY:

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

HIGHLIGHTS

CHALLENGES

- Mitigating the threat of ransomware that could escalate into patient safety issues
- Protecting PHI and HIPAA information from insider and outsider threats
- Remediating at-risk areas with a one-person security team

SOLUTION

The most robust data security platform:

- **DatAdvantage** to discover where users have too much access and safely enforce least privilege
- **DatAlert Suite** for continuous monitoring and alerting on data and systems

RESULTS

- 400+ hours saved annually
- Visibility into on-prem servers enabling a one-person team to stay ahead of ransomware
- Peace of mind since 2009, thanks to a security solution that grows with the hospital's needs

Challenges

Protecting critical systems could save lives

For hospitals and healthcare organizations, stopping ransomware attacks is literally a matter of life and death.

In September 2020, responders were forced to take a patient with life-threatening injuries to a different hospital, 20 miles away, after the closest hospital was compromised. The patient died—and it's believed that the hour-long delay was a contributing factor.

Understanding the risk, one U.S. healthcare provider (anonymous by request) partnered with Varonis back in 2009.

> "One of our main concerns is ransomware," explains the Security Manager. "Ransomware could put us out of business... or worse. As a hospital, an attack could become a patient safety issue. If ransomware shut us down for a week or two weeks, that's a big hardship for our patients."
>
> "It's not just ransomware, either. If we don't stay on top of insider threats and data exfiltration, PII and PHI can be held as ransom in addition to the damage encrypted files would cause."

Hospital security teams are notoriously small. In this case, a one-person team is responsible for keeping data safe from ransomware attacks and ensuring compliance with HIPAA and PHI.

> “A lot of our files contain PHI and they fall under the protection of HIPAA security rules. We have to ensure that only need-to-know people are accessing it. Without a solution like Varonis, there’s no way we could keep up with who is accessing and who should have access to those files.”

Even for a large team, it would be a big job. For one person, it’s an impossible undertaking—which is why they adopted Varonis.

> “I would not have enough hours in the day to secure our network without Varonis. One person alone can’t do that job.”

“Ransomware could put us out of business… or worse. As a hospital, an attack could become a patient safety issue.”

Solution

Visibility and alerting on all critical files and systems

DatAdvantage for Windows helps the one-person security team assess, prioritize, and mitigate the biggest security risks on the hospital's on-prem servers. If a file is overexposed (i.e., open to everyone) or a user starts accessing, moving, or deleting data they don't normally touch, Varonis warns the Security Manager in real time.

The hospital later added **DatAdvantage for Directory Services**, which supports Active Directory, to their security lineup. They now have a panoramic view of data access in their most critical systems, and DatAdvantage helps by detecting and safely fixing problems with permissions, nested groups, and inheritance.

> "We started with DatAdvantage and added support for Directory Services, which monitors Active Directory for changes. We definitely had a need for it because up until that point, we didn't know specifics about who, what, where, or how changes were occurring."

The hospital also added **DatAlert Suite** to their security stack. By uncovering potential threats across the kill chain before they can escalate, DatAlert is pivotal in their fight against ransomware.

> "DatAlert stays on top of everything happening in our file servers and Active Directory. We would know right away if it detected ransomware or if an actual breach were to happen."

But even with all of these solutions, a one-person security team would have a difficult time stopping a concentrated attack on their own. That's when it's time to call for backup: **the Varonis Incident Response team**.

> "A vendor's product was compromised. The Incident Response team helped us confirm that the hacker hadn't gotten further than that one appliance. Without Varonis, it would have been a much harder, time-intensive, and labor-intensive task."

"DatAlert stays on top of everything happening in our file servers and Active Directory. We would know right away if it detected ransomware or if an actual breach were to happen."

Results

400+ hours saved annually

According to the Security Manager, the practical value of Varonis for a one-person team is time savings—**at least a full work day every week or over 400 hours annually.**

> “When it comes to data forensics and intensive analysis, a small team just doesn’t have enough time. Varonis is invaluable in that regard—you need it to extend the capabilities of one person.”
>
> “The time savings allow me to concentrate on other issues and review alerts that I otherwise wouldn’t have time to investigate.”

But while time savings are great, the peace of mind is even better. Knowing that they’re now able to lock down data and that the Incident Response team is just a quick call away fills the Security Manager and senior leaders with confidence.

> “In today’s security environment, peace of mind is hard to come by. Almost every day, you read about another hospital getting hacked or infected by ransomware. Having the tools to stop a bad situation from escalating helps me sleep at night.”

As the hospital assesses next steps, it’s committed to taking extra precautions to protect the data—and the lives—of its patients. To further that goal, the Security Manager hopes to add more Varonis solutions to their security lineup in the near future.

"Varonis has already found stuff like stale accounts, incorrect permissions, and other at-risk areas. We're looking at getting Automation Engine next, followed closely by Data Classification Engine."

"The time savings allow me to concentrate on other issues and review alerts that I otherwise wouldn't have time to investigate."

Varonis helps small teams stay ahead.

Gain visibility, data security, and the peace of mind that comes with having an experienced team in your corner.

REQUEST A DEMO