VARONIS

# How Varonis Helps a One-Person Security Team Save 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.

**About this case study:**

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

# HIGHLIGHTS

## Challenges

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

## Solution

The Varonis Data Security Platform:

- Discovers overpermissioned users
- Locks down access and safely enforces least privilege
- Continually monitors and alerts on data and systems

## Results

- 400+ hours saved annually
- Increased visibility, enabling a one-person team to stay ahead of ransomware
- Peace of mind since 2009, thanks to a Data Security Platform that grows with the hospital's needs

# CHALLENGES

## Protecting critical systems to help save lives

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

In May 2024, a large healthcare system experienced a ransomware attack that led to the data exposure of nearly 5.6 million people, including patients, residents, and employees. The attack forced the healthcare org to divert ambulances, close pharmacies, take critical IT systems offline, and revert to pen and paper for patient information.

Additionally, the attack locked providers out of systems that track and coordinate nearly every aspect of patient care.

Knowing an incident like this could happen at any time, one U.S. healthcare provider (anonymous by request) partnered with Varonis back in 2009.

Their Security Manager explained:

> **"One of our main concerns is ransomware 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, managing access and ensuring compliance would be a big job. For one person, it's an impossible undertaking — which is why the hospital 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

Varonis helps the one-person security team assess, prioritize, and mitigate the biggest security risks on the hospital's 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.

With Varonis supporting Active Directory, the hospital has a panoramic view of data access in their most critical systems, detecting and safely fixing problems with permissions, nested groups, and inheritance.

> **"We definitely had a need for Varonis for Active Directory because up until that point, we didn't know specifics about who, what, where, or how changes were occurring."**

Varonis also helps the security team uncover potential threats across the kill chain before they can escalate, which is pivotal in their fight against ransomware.

> **"Varonis 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 the robust cloud-native Data Security Platform, 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."**

“Varonis 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 the hospital is now able to lock down data and that the Incident Response team is just a quick call away gives the Security Manager and senior leaders 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 appreciates Varonis' ability to locate and remediate stale or overexposed data.

> **"Varonis finds things like stale accounts, incorrect permissions, and other at-risk areas."**

Healthcare is one of the most highly targeted sectors by ransomware and the effects of an attack can be widespread and crippling. Varonis helps hospitals secure sensitive patient data, reduce ransomware risk, and keep pace with evolving HIPAA regulations.

“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.”

# Your data. Our mission.

Varonis right-sizes permissions, finds and remediates exposed sensitive data, and detects abnormal behavior.

**Request a demo**