VARONIS

How a U.S. Healthcare Organization Locked Down Over 1 Million Exposed Folders in Under 8 Weeks

> It helps us sleep at night — actively working to prevent data breaches and knowing that, if an attack does occur, Varonis will help us stop it.

About this case study:

Our client is a respected Midwest medical provider. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

- Protecting sensitive patient data in a highly vulnerable and often targeted industry
- Remediating over 1 million exposed files
- Accomplishing a huge remediation project quickly, safely, and accurately

Solution

The Varonis Data Security Platform:

- Provides complete visibility and control over critical data in M365 and on-prem
- Discovers and classifies sensitive data automatically
- Right-sizes and maintains file system permissions
- Monitors and alerts on abnormal behavior on critical systems

Results

- Remediation of over 1 million folders — 82% of global access in environment — in under 8 weeks
- HIPAA, PHI, PCI, and PII locked down — increasing data security for millions of patients

CHALLENGES

Remediating mountains of exposed data

When it comes to data breaches, healthcare organizations have a lot to lose. In 2024, the average cost of a healthcare data breach was nearly $10 million. Hospitals, clinics, and practices must protect critical information, but they face a perfect storm of risks.

The risk was even greater for one organization (anonymous by request). When a new IT manager joined, they discovered that most of the organization's files were open to every employee. With a blast radius that large, just one hacked account could compromise the data of millions of patients.

The IT Manager explained:

> **"Many file shares were open to almost the whole organization, including a lot of HIPAA, PCI, PHI, and PII data. We found gaping holes that weren't being protected."**

Over 1 million folders had global access group permissions. Even if a bad actor never infiltrated the org's environment, this still put them at significant risk. A user could accidentally move, delete, or copy data to somewhere it shouldn't be.

> **"Sensitive data could be all over. It could be in somebody's department drive and in their local home directory. That's what we were trying to uncover."**

Remediating that much exposed data felt like a mountain to climb — but the IT Manager had a solution.

They'd worked with Varonis during their tenure at a previous organization, and they knew it would help them find and remediate sensitive data wherever it lived.

SOLUTION

Reducing risk automatically

Varonis eliminates guesswork from file remediation. There's no longer any question of who has touched certain files during compliance audits.

The Varonis Data Security Platform is the heart of the healthcare org's data security strategy. Varonis supports their on-premises data stores and email by mapping who can access data, who does access data, and where users have too much access.

Varonis enables the IT Manager to safely change user access and close security gaps.

> **"Varonis saves me time now that I'm not going to these individual file shares or directories and asking, 'Who has access to these? How can I attempt to lock them down?' I just run a report, and it tells me what needs to be fixed."**

Varonis provides context by automatically discovering and identifying sensitive data in the org's environment. The unified platform helps the organization prioritize their remediation efforts and fix exposed HIPAA, PCI, PHI, and PII data.

According to the IT Manager:

> **"We can do everything in one spot. With Varonis, we can see this user is responsible for that data and analyze the risk; we don't have to go from one application to another to do the same thing."**

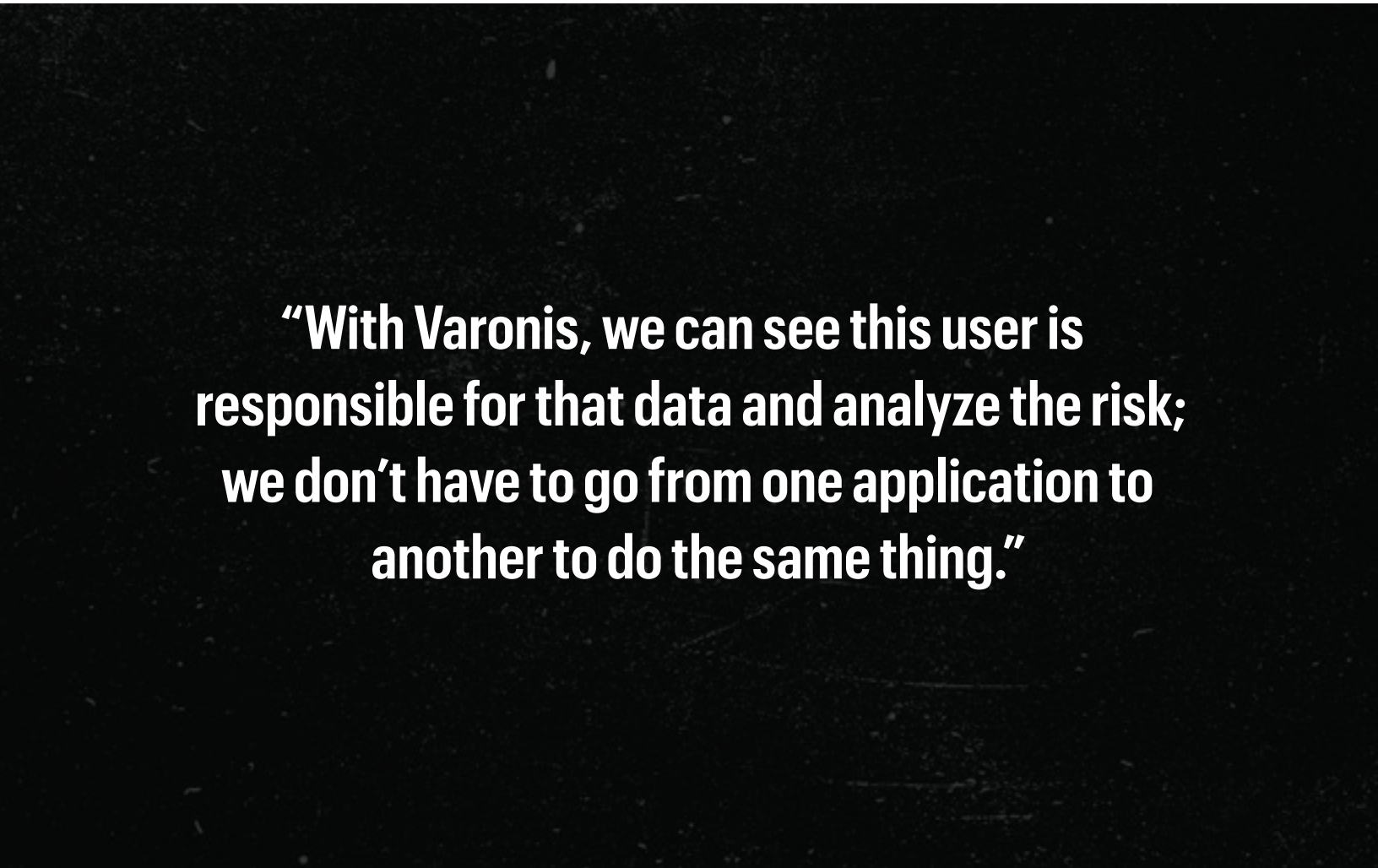
Varonis monitors and alerts on critical systems. Detailed threat detection enables the IT team to quickly gather context and respond within minutes. The Data Security Platform recently helped the IT Manager resolve a situation where thousands of files vanished.

> **"We received an alert: 41 files removed within one minute. We were able to quickly restore those files and figure out that a user had moved them accidentally."**
>
> **"We decided to audit their file touches just to be safe... and suddenly found over 6,000 files that had been moved. Being able to track that kind of stuff is important."**

But the biggest obstacle for the healthcare provider was the sheer amount of data they had to secure.

With Varonis, they could not only see what was at risk — they could quickly find and fix permissions across their entire environment with automation.

Now, instead of remediating dozens of files at a time, the organization safely removes open access from thousands of files automatically.



RESULTS

Global access reduced by 82% in less than 8 weeks

With Varonis, the healthcare organization kicked off a major remediation project. It would have taken years for the small IT team to make any headway manually. Thanks to Varonis, remediation was fast, safe, and simple. In less than 8 weeks, the org remediated over 82% of the global access in their environment — fixing global access groups on over 1.15 million folders.

> **"I have nothing but positive praise for Varonis. It's in the background, helping us monitor folders, uncover security issues, and fix permissions."**
>
> **"It helps us sleep at night — actively working to prevent data breaches and knowing that, if an attack does occur, Varonis will help us stop it."**

For organizations that need to prove compliance with stringent data privacy regulations, it's essential to lock down sensitive files and maintain clear audit trails.

> **"If something happens in our environment, we see it. We can quickly run reports, figure out what happened, and audit who touched the files and where they went."**

Having the Varonis Incident Response team on standby adds even more peace of mind. If the IT Manager or their team ever encounters a threat that appears malicious, they appreciate having reliable support.

> **"I hear this from my team a lot: out of any IT vendor they've ever worked with, Varonis is the best because they're always there. They don't just steer you in the right direction, they actually walk you through the solutions and spend endless hours on the phone with you to help."**
>
> **"Anytime you need anything, they're there."**

Recently, the healthcare organization made the switch to **Varonis' cloud-native Data Security Platform.**

Now, the company benefits from even more automation, and the IT Manager can focus on improving their data security posture without having to think about updates — because everything is handled by Varonis automatically.

“I have nothing but positive praise for Varonis. It’s in the background, helping us monitor folders, uncover security issues, and fix permissions.”

Your Data. Our Mission.

Automatically find and fix exposed HIPAA, PCI, PHI, and PII data with Varonis.

Request a demo