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

CASE STUDY

“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 & places.

## HIGHLIGHTS

### CHALLENGES

- Protecting sensitive patient data in a highly vulnerable and often targeted industry: healthcare
- Remediating over 1 million folders with global access group permissions
- Accomplishing a huge remediation project quickly, safely, and accurately

### SOLUTION

The most robust data security platform:

- **DatAdvantage** maps who can and who does have access to sensitive data
- **Data Classification Engine** scans for and classifies sensitive data
- **DatAlert Suite** detects potential threats, such as ransomware and insider threats
- **Automation Engine** automates repairing and maintenance of file system permissions

### 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 over 1 million exposed files

When it comes to data breaches, healthcare organizations have a lot to lose. For the tenth year in a row, the healthcare industry incurred the highest average cost of a data breach—$7.13 million in 2020.

Healthcare organizations must protect critical information, but they face a perfect storm of risks. On average, they take the longest to identify and contain data breaches and they are less likely to use automation in their security approach.

But 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. Just one hacked account could **compromise the data of millions of patients.**

> They explain, "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 their environment, this still puts them at significant risk of a user accidentally moving, deleting, or copying 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.

> “While working at another hospital, I used Varonis for 11+ years. It did wonders for us. We were able to keep all of our data secure and restrict permissions to what people needed to do their job. I knew it would be a good fit in this environment as well.”

“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.”

# Solution

## Putting risk remediation on autopilot

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

**DatAdvantage** is the heart of the Varonis solution. It supports this healthcare organization's on-premises data stores and email by mapping who can access data, who does access data, and where users have too much access. It then enables the IT manager to safely make changes to control lists and security groups.

> "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."

**Data Classification Engine** provides context by automatically scanning for and identifying sensitive data in their environment. It helps them prioritize their remediation efforts and fix exposed HIPAA, PCI, PHI, and PII data first.

> "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."

**DatAlert Suite** monitors and alerts on critical systems. Detailed threat detection enables the IT team to quickly gather context and respond within minutes. DatAlert 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 DatAdvantage, they could see what was at-risk—but they still didn’t have the human resources to quickly find and fix permissions across their entire environment.

**Automation Engine** remedied that. If DatAdvantage simplifies the process of finding and fixing exposed files, Automation Engine puts it on autopilot. Now, instead of remediating dozens of files at a time, the organization is able to safely remove open access automatically from hundreds—even thousands—of files.

> “We’re still locking down files, but with the introduction of Automation Engine, we’re going to get there sooner.”

"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."

# Results

## Global access reduced by 82% in less than 8 weeks

With Automation Engine, the healthcare organization kicked off a major remediation project. It would have taken years for the small IT team to make any headway manually. But with Automation Engine, remediation was fast, safe, and simple.

**In less than 8 weeks, they 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 like this, that need to prove compliance with stringent data privacy regulations, having sensitive files locked down and clear audit trails to follow is invaluable.

> “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’re glad to have reliable support.

> “I hear this from my team a lot: out of any IT vendor they’ve ever had to work with, Varonis is just 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.”

With remediation underway and most of their sensitive data locked down, the healthcare provider is now exploring **DataPrivilege** as a way to manage permissions on an ongoing basis.

This new solution would allow data owners to manage and grant access to sensitive data on a need-to-have basis, while IT maintains a bird’s-eye view to ensure that least privilege is enforced.

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