VARONIS

How Varonis is Helping a Major Technology Provider Monitor and Protect Active Directory

> “Varonis is the best way to see what’s going on with your data. It’s easy to use, and it’s the first thing I would recommend to a company in need of security solutions. If you can only afford one solution, make it Varonis.”

About this case study:

Our customer is a technology provider in the healthcare sector. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

- Gaining more insights into file security, access, and permissions
- Cleaning up stale data and tightening permissions in Active Directory
- Ensuring HIPAA, PCI, and PHI compliance

Solution

The Varonis Data Security Platform:

- Identifies and classifies regulated information
- Detects potential malware and internal data leaks
- Prevents perimeter threats (malware, APT intrusion, data exfiltration)

Results

- Protection for 1,300 end users
- Clear audit trails, making it easy to prove compliance
- 24/7 security, and alwayson customer support

CHALLENGES

Gaining visibility and control into their network

A major technology provider in the healthcare sector began a proof of concept of Varonis.

They had two simple goals:

- **Data security.** They wanted more visibility into who had access to sensitive files and clear analytics that would provide context and insight into network events and high risk areas.
- **Threat detection and response.** They needed an easy way to cut through the "noise" of incoming data and spot the signs of compromise or attack.

But the company had a more immediate need too.

According to their two security engineers (who requested anonymity for themselves and their company), their infrastructure was almost two decades old when they began their POC — and it was causing a lot of problems.

> **"We were receiving support tickets from people who needed permissions to folders they couldn't access on a daily basis — sometimes multiple times per day. Our access list, permissions list, and file and folder structures were a disaster."**
>
> **"Groups weren't set up right. We had full files and folders everywhere. Individual users were disabled but still listed in file permissions. And people needed access to specific subfolders, but the permissions didn't inherit properly—so that was broken."**

> **“We needed a solution that could identify all of those problems and fix them quickly.”**

As a major provider in the healthcare sector, the company needed a way to gain insights into security, access, and permissions surrounding their data.

They needed to ensure compliance with HIPAA regulations, and protect Payment Card Information (PCI) and Protected Health Information (PHI). They also needed to be able to prove compliance to pass regular data audits.

The security team chose Varonis because it would allow them to easily accomplish all of this and detect and prevent cyberthreats.

> **“We reviewed other solutions but they typically excelled at either data visibility or threat detection — not both.”**
>
> **“Varonis is the only one that does it all and presents the information cleanly and precisely. The level of detail you can get into is astounding.”**

“We were receiving support tickets from people who needed permissions to folders they couldn’t access on a daily basis — sometimes multiple times per day.”

SOLUTION

Data-centric, all-in-one security platform

Like many large companies, the healthcare technology provider relies on Active Directory for user authentication and authorization for their network.

Varonis allows the security engineers to watch for unusual activity within directory services, including:

- Brute-force prevention that detects abnormal login attempts based on each user's unique behavioral baseline.
- Accounts being used in unusual ways, such as logging into computers they're not normally associated with or logging in over a network when they usually log in locally.
- Computers on the inside connecting to computers on the outside, which could be signs of data exfiltration attempts.

The heart of this solution is the **Varonis Data Security Platform**, which automatically catalogs user accounts, group memberships, and permissions. It also allows the security team to see a complete audit trail of every file a suspicious individual touched, shared, or modified.

> **"We use Varonis every day. It's saved us a lot of time managing permissions, and a lot of problems as well. Now, when a high-level executive asks to see a list of all the subfolders within a certain file share or a list of everyone who has accessed it, Varonis allows us to quickly generate that report."**

Varonis automatically discovers and classifies regulated information. After Varonis identifies all of the sensitive data in the customer's environment, the next step is to review permissions and ensure only the people who need it have access.

> **"We do an entitlement review on existing permissions and run a PCI compliance report every 60 days. If we find anomalies, we can simulate and commit changes directly in Varonis knowing we won't cut off valid access."**

When Varonis does detect suspicious activity, the alerts the security engineers. Varonis provides detailed context around the problem, which allows the security team to investigate further.

> **“Varonis alerts us to authentication anomalies, permission modifications, administrator group changes — anything suspicious that’s happening within our Active Directory.”**
>
> **“Data access alerts include everything we need: file name, location, who did it, at what time, and where from. With that information, we can quickly contact the user, find the file, and resolve the issue.”**
>
> **“The best thing about Varonis is that you can instantly see: here’s the problem, here’s why it’s an issue, and here’s how you fix it.”**

Varonis helps the healthcare technology provider detect and prevent perimeter threats, such as malware, APT intrusion, and data exfiltration.

> **“Varonis is useful for tracking suspicious activity to its source. For example, Varonis alerted us to a potential malware event and we used it to drill down to the exact domain that caused the issue.”**

“The best thing about Varonis is that you can instantly see: here’s the problem, here’s why it’s an issue, and here’s how you fix it.”

RESULTS

Cleaned up infrastructure & clear audit trails

Using Varonis, the tech company's security engineers were able to quickly and effectively clean up their data infrastructure. Now they can ensure data protection more than 1,000 end users.

> **"Without Varonis, fixing things like file permissions would be a long, manual process. We'd have to drudge through each directory's ACLs. With Varonis, it's easy to review who has access and change permissions if need be. The time savings are immeasurable."**
>
> **"I couldn't imagine doing it without Varonis, especially with just the two of us. We probably would need two or three other people and it would still have been a huge undertaking."**

When the compliance department or a high-level executive asks for a report, it's easy to show them how permissions are set, give them a list of everyone with file permissions, or review the history of who has accessed a specific file.

> **"In minutes, I can prove: here's where that data lives, here's how it's secured, here's who has access to it. It's very simple."**
>
> **"The same thing goes for PCI, PHI, and specific client data. We can find it easily if we need to, and the only people who can access it are those who need to access it."**

But that's not even the best part. What the security engineers love most, from a user's perspective, is how intuitively Varonis is designed — and the top-notch support they receive whenever they reach out for help.

> **"Varonis is the best way to see what's going on with your data. It's easy to use, and it's the first thing I would recommend to a company in need of security solutions. If you can only afford one solution, make it Varonis."**
>
> **"I've never had a relationship with a vendor that's as good as the one we have with Varonis. Our Support Engineer is above the bar. They're always willing to help me out."**

“Without Varonis, fixing things like file permissions would be a long, manual process. With Varonis, it’s easy and the time savings are immeasurable.”

Secure sensitive data. Automate compliance.

Varonis takes the complexity out of file auditing, securing sensitive information, and maintaining compliance.

Request a demo