



How Varonis Helped a Regional Healthcare Network Lock Down At-Risk PII and PHI Across Their Hybrid Cloud

CASE STUDY



“If you work within a regional healthcare network, and your organization is poised for growth like we were, you need a way to prove that you have visibility and control over your unstructured data. If you don’t have a solution like Varonis, you open yourself up to a lot of risk.”

ABOUT THIS CASE STUDY:

Our client is a mid-sized hospital and regional healthcare provider network in the US. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Protecting PII, PHI, and other sensitive information during a time of rapid business growth
- Minimizing attack surface despite increasing use of shared drives and remote connectivity
- Ensuring data privacy protection measures continue to meet HIPAA standards

SOLUTION

The most robust data security platform:

- **DatAdvantage** to support on-prem data stores and email.
- **Data Classification Engine** to scan for and automatically classify HIPAA-regulated data
- **DatAlert** to monitor and alert on anomalous activity that could lead to a data breach
- **Data Transport Engine** to automatically move, archive, or delete stale and sensitive data
- **DatAnswers** to simplify compliance and e-discovery

RESULTS

- Enhanced data privacy and security for over 2,500 employees
- More visibility into unstructured data and clear audit trails that show which users are accessing data
- Varonis products that simplify DSARs, internal audits, and prove HIPAA compliance

Challenges

ENSURING DATA PRIVACY DURING RAPID BUSINESS GROWTH

Hospitals and regional healthcare networks in the US store terabytes of sensitive data on their servers. This includes information about employees, patients, projects, and other business-related content. But as businesses grow, it can be difficult to keep track of where this data lives and who has access to it.

That was the challenge faced by the Network Admin of a mid-sized hospital and regional healthcare provider network (anonymous by request):

“

“When I started at the hospital, we had 4 servers and 50 desktops. Now, we have over 300 servers and 2,500 desktops.”

”

For this organization, rapid growth mandated the use of shared drives to facilitate collaboration across multiple locations. But remote connectivity posed risks. Improper file sharing was creating security vulnerabilities and increasing this hospital’s attack surface.

“

“Having all of our locations remotely connected forced us to think about security concerns that didn’t exist 20 years ago.”

”

As a business operating within the healthcare industry, keeping track of sensitive data was especially important.

It was their responsibility to ensure data privacy for all Personally Identifiable Information (PII) and Protected Health Information (PHI), both of which are protected under HIPAA.

But this organization had data spread out across on-premises servers, saved on employees' computers, archived in email folders, and housed in the cloud. **A lack of visibility and control was putting over 2,500 employees at risk and jeopardizing HIPAA compliance.**

“

“Employees knew they shouldn't do things like save PHI to personal computers or create folders with Global Group Access, but not everyone was adhering to those standards.”

”

They purchased Varonis to help identify, protect, retrieve, and discover highly sensitive data in their network.

“

“When I started at the hospital, we had 4 servers and 50 desktops. Now, we have over 300 servers and 2,500 desktops.”

Solution

DATA CLASSIFICATION, AUDITING, AND REMEDIATION UNDER ONE ROOF

The regional healthcare network purchased five critical Varonis products. Having classification, auditing, remediation, and entitlement capabilities all in one dashboard enabled them to get in control of their unstructured data.

DatAdvantage for Windows and SharePoint is the pillar that supports all of their on-premises data stores. It gives visibility into where data lives, who has permission to access it, and who is actually accessing it.

Data Classification Engine automatically scans and classifies their data stores for sensitive information, including PHI, PII, financial records, and other HIPAA-regulated data.

“

“Gaining visibility into PHI improperly stored in shared drives or users accessing data that they probably don’t need is eye-opening. No other solution we tried gave us all of that information behind a single pane of glass.”

”

DatAlert provides continuous monitoring and alerting for their on-prem data stores. According to the Network Admin, having a behavior-based threat detection system gives them tremendous peace of mind.

“

“We have alerts set up that warn us when a user is added to a security group, if a folder is shared incorrectly, or if a large amount of files are modified within a small time frame. Basically, Varonis warns us about anything that doesn’t look like typical user activity.”

”

Data Transport Engine helps ensure that sensitive data stays secure and that it is properly moved, archived, quarantined, or deleted based on predetermined parameters.

“

“Data Transport Engine has helped us automatically organize data and it allows us to say definitively that we know where data lives. Cleaning up stale data used to be a very long and manual and process, but not anymore.”

”

Finally, **DatAnswers** is an elevated search function that simplifies compliance and e-discovery. It helps the Network Admin fulfill data subject access requests (DSAR) by making it easy to pinpoint files containing PII, PHI, and other HIPAA data.

“

“I call DatAnswers the ‘search engine’ of Varonis. When a user doesn’t know exactly where they put a sensitive file, we use DatAnswers to track it down. We also use DatAnswers for all of our legal team’s searches. I appreciate the ease and functionality of being able to do that through a web browser.”

”

“

“Gaining visibility into PHI improperly stored in shared drives or users accessing data that they probably don’t need is eye-opening. No other solution we tried gave us all of that information behind a single pane of glass.”

Results

ENHANCED PRIVACY AND PROTECTION FOR 2,500 END USERS

The organization's Network Admin has seen firsthand how quickly the cybersecurity industry has evolved. They've witnessed other healthcare organizations [fined millions of dollars](#) for failing to protect user privacy and meet HIPAA compliance standards.

They're thankful that they have a solution like Varonis keeping a watchful eye on their unstructured data environments.

“

“To be honest, I don't know how we would meet regulatory requirements without Varonis. The tools that Windows gives you natively aren't enough—system and application event logs don't get into the weeds of who is doing what in your file shares the way Varonis does.”

”

For an organization in the healthcare industry, having visibility and control capable of scaling with their business growth has been essential. Despite a 7,400% increase in active servers to manage, they feel like they now have more control over their unstructured data than ever before.

“

“If you work within a regional healthcare network, and your organization is poised for growth like we were, you need a way to prove that you have visibility and control over your unstructured data. If you don't have a solution like Varonis, you open yourself up to a lot of risk.”

”

According to the Network Admin, having Varonis in their corner, and knowing that Varonis' team is always proactively working to improve their products, gives them confidence.

“

“Varonis performs a ‘health check’ every quarter. The constant contact—them asking how we’re doing, what we need, and how they can help—that’s huge. I really appreciate that Varonis is always willing to help and find ways to serve us better.”

”

“

“To be honest, I don’t know how we would meet regulatory requirements without Varonis.”



**Don't leave HIPAA data,
including PII and PHI, vulnerable
to insider and outsider threats.**

Varonis helps you hunt down and secure personal information across your on-prem servers, cloud environments, and shared drives.

[REQUEST A DEMO](#)