VARONIS

How a West Coast Public Healthcare Organization Protects PII, PHI, and PCI

> Varonis always hits it out of the park. It does what it's supposed to: helps us find PHI and fulfill contract obligations from the state. Without it, we wouldn't be able to fulfill HIPAA regulations.

About this case study:

Our customer is a public healthcare organization in the U.S. We have happily accommodated their request to anonymize all names and places.

HIGHLIGHTS

Challenges

+ Discovering PII, PHI, and PCI hidden throughout their network
+ Reporting on user activity and permissions on sensitive data for HIPAA compliance
+ Reducing their blast radius and defending against ransomware

Solution

The Varonis Data Security Platform:

+ Gives complete visibility and control over critical data and IT infrastructure
+ Finds and classifies sensitive data automatically
+ Monitors and alerts on abnormal behavior on critical systems

Results

+ Sensitive data locked down and moved to encrypted servers
+ Compliance reports and PRA requests fulfilled in seconds
+ Risk mitigation thanks to automated alerts on file activity

CHALLENGES

Achieving HIPAA compliance

A West Coast public healthcare organization (anonymous by request) faced the same challenges that every healthcare organization needs to contend with:

+ Discovering what sensitive data they have and where it was located
+ Reporting on who has access to sensitive data and who's accessing it on a regular basis
+ Protecting sensitive data including PII, PHI, PCI, and HIPAA data against threats like ransomware
+ Securing critical company data, like financial data and internal-only files

Gaining visibility into user data activity is essential for achieving HIPAA compliance. But before Varonis, the company had no way of pinpointing where this data lived in their environment. The Security Admin explains:

> **"Before Varonis, we tried to regulate PHI through policies, but we didn't have a tool that told us where PHI was stored on our network. With Varonis, we know exactly where all of our regulated data is."**

Limited visibility made proving regulatory compliance much harder. For example, if a patient submitted a Public Records Act (PRA) request, the organization had to manually gather all patient records, which could take days — or even weeks.

> **"We basically had to do a search for file extensions and open up every single document and read it to see if it contained PHI. It was ridiculous and very time consuming."**

SOLUTION

The means to find sensitive data and manage risk

The organization turned to Varonis to get a handle on their data and help manage permissions for Windows and SharePoint. By highlighting permissions, the Data Security Platform enables the Security Admin to discover when users have excessive access. Varonis' robust classification analyzes enterprise data to identify sensitive data, including PII, PHI, and PCI.

> **"Varonis scans all of our servers, all the file shares, and looks into documents for key medical phrases and terms. If it detects PHI, it tags it with the HIPAA classification."**

With Varonis, the Security Admin has complete visibility into where the company's sensitive data lives and who has access to it. If they need more context, they can right-click the file and see what keyword was considered sensitive. When they need to lock down data, the unified Data Security Platform enables them to safely remediate permissions.

> **"Varonis shows me where our PHI is located and I can drill in to see what type of PHI it is. When we get audited, we can generate reports to prove that we know exactly where our sensitive data is."**

The organization relies on Varonis to help them identify sensitive data, move it to encrypted servers, and enforce least privilege. Varonis also supports the healthcare organization's Active Directory by finding and fixing misconfigurations that threat actors commonly exploit to gain access, move laterally, persist, and ultimately steal data.

> **"Varonis gives us alerts on changes on the network that could be malicious, like a bunch of files being deleted or encrypted. When it detects suspicious activity, it enables us to immediately launch an investigation. Every alert has a description of the problem and how to fix it."**

Varonis helps mitigate the risk of ransomware by monitoring file activity for unusual user behavior and permission changes. Having high-fidelity alerting and automated response to threats helps the Security Admin rest easy.

RESULTS

Enterprise data blind spots eliminated

After partnering with Varonis, the Security Admin is confident that their organization is top of the class when it comes to data security and HIPAA compliance.

> **"Honestly, I don't know how other agencies achieve compliance without a solution like Varonis. I think we're doing a lot better than a lot of other organizations in the space and Varonis supports that."**

Varonis helped the organization achieve all of their goals:

+ They know exactly where PII, PHI, and PCI lives and who has access to it
+ They're able to generate compliance reports and fulfill PRAs in seconds
+ Varonis' real-time alerts help the healthcare org detect and defeat threats like ransomware

Using the knowledge of their most at-risk areas, the Security Admin has been able to take steps to reduce risk companywide, decrease the organization's blast radius, and defend against ransomware.

> **"Varonis always hits it out of the park. It does what it's supposed to do: helps us find PHI and fulfill contract obligations from the state. Without it, we wouldn't be able to fulfill HIPAA regulations."**

When something changes on their network, Varonis enables the Security Admin to understand and investigate the changes. If a Varonis alert ever indicates an attack, Varonis' Incident Response team is standing by to help the organization defend its data.

> **"Out of all the products that I've used in my 30-year IT career, Varonis has been one of the most reliable."**
>
> **"Before Varonis, we used to spend a lot of time fighting fires. After Varonis, we have a solution that finds problems and tells us exactly how to fix them."**

Your data. Our mission.

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

Request a demo