VARONIS

How Varonis Helps TPMG Guard Against Ransomware and Gain Cyber Insurance Compliance

> “We’ve set up malware recognition and automated remediation. If we detect malware on one of our servers, Varonis immediately locks down that client session, logs them out, and notifies us.

HIGHLIGHTS

Challenges

- Proving compliance measures are in place for cyber insurance
- Protecting HIPAA-regulated patient data and other sensitive information
- Defending against ransomware attacks proactively

Solution

The Varonis Data Security Platform:

- Provides complete visibility and control over critical data and IT infrastructure
- Discovers and classifies sensitive data automatically
- Right-sizes and maintains file system permissions
- Monitors and alerts on abnormal behavior on critical systems
- Dtects helps prevent attacks against DNS, VPN, and web proxies

Results

- Gained compliance required for cyber insurance
- Implemented automated malware detection & response
- Reduced unique permissions by 86%
- Eliminated broken permissions

CHALLENGES

Mitigating risk to sensitive patient information

As part of its ongoing cybersecurity risk management strategy, Tidewater Physicians Multispecialty Group (TPMG) wanted to purchase cyber insurance. But first, they needed to implement compliance software and demonstrate their ability to detect and stop threats like ransomware.

CIO Brett Brickey was tasked with finding the best solution for TPMG and then making a case for shareholders.

> **"TPMG's shareholders are an exceptional group of doctors. They all assume full risk. So even though their focus is on medicine, surgery, and the health of patients, they want to know what data we have that we need to protect."**

Mr. Brickey keeps a finger on the pulse of the industry, and he knows that threats like ransomware are on the rise.

In fact, several other healthcare groups suffered major attacks in recent years. TPMG wasn't willing to gamble with the safety of patient data.

Mr. Brickey said:

> **"There have been enough high-profile cases of HIPAA breaches in other medical groups that I didn't have a hard time convincing shareholders that this was a good insurance policy. What I needed to explain was where the dollars were going."**

Mr. Brickey engaged Varonis to come in and perform a Proof of Concept (POC). He suspected that sensitive data lived on their network but with nearly 80 million files, there was too much data to monitor manually. He lacked visibility.

Mr. Brickey explained:

> **“As a medical group, we have tons of compliance regulations we need to deal with. But we’ve grown continuously for the past 20+ years and, because of that, sometimes documents get stored on the network and then forgotten about.”**

Varonis came in and performed a free POC. It revealed exactly where sensitive data like social security numbers, credit card numbers, and HIPAA-regulated data, was stored in their environment and where it was overexposed.

Mr. Brickey made a strong case for shareholders and demonstrated that locking down sensitive data was a breeze with Varonis.

“We discovered several areas where we were not following a good minimum access policy. Remediation would have taken multiple staff days of work, but we did it in an hour with Varonis.”

SOLUTION

Visibility and control over sensitive data

Mr. Brickey kicked off remediation by leveraging Varonis for Windows and Active Directory. With Varonis, Mr. Brickey has complete visibility into TPMG's IT infrastructure. He's able to spot overexposed data at a glance and see exactly where data lives, when it's touched, and who's accessing it.

Mr. Brickey explained:

> **"Varonis is helping us discover where things are and figure out what to do with them. This is big — especially when it comes to scanned documents. We had tens or maybe hundreds of thousands of PDFs, but Varonis was able to crawl them all and figure out what's going on."**

The Varonis Data Security Platform discovers and classifies sensitive data. This helps TPMG find and lock down patient information, especially HIPAA data.

According to Mr. Brickey:

> **"Protecting patient medical data is our top priority. So that's HIPAA compliance. We also have PCI compliance."**

Even with these insights, remediating over 22 TB of data was a huge task. So TPMG invested in automation to make that process painless and keep risk low over time. Now they can identify—and then prioritize the remediation of—the sensitive data that's most vulnerable.

Finally, the company uses Varonis for threat detection and response: Varonis monitors all critical systems and alert on abnormal user behavior, and helps the company gain insight into DNS, VPN, and web proxy activity.

Mr. Brickey said:

> **"We've set up malware recognition and automated remediation. If we detect malware on one of our servers, it immediately locks down that client session, logs them out, and notifies us. That helps me sleep a bit better. We've also fine-tuned our alerts a lot over the past year. Whenever an alert comes through we definitely pay attention."**

Mr. Brickey and two other TPMG employees also went through optimization with a Varonis professional to dig into business goals and fine-tune the platform to fit their needs.

The TPMG team is now able to navigate the Varonis interface to detect and investigate threats with confidence. They're also comfortable managing and configuring Varonis detection and response capabilities.

The strong partnership and ongoing support is one of Mr. Brickey favorite things about Varonis.

> **"The Varonis team is one of the biggest bonuses. They've been tremendously supportive and patient. I've had great interactions with everybody from Varonis."**

"We had tens or maybe hundreds of thousands of PDFs. Varonis was able to crawl them all and figure out what's going on in our environment."

RESULTS

Comprehensive Data Security Posture Management

With Varonis in place, TPMG has the proof of compliance they need to get cyber insurance. Mr. Brickey and his team continue to use Varonis daily to enforce good data governance and keep a watchful eye on sensitive patient information.

In just five months, Mr. Brickey leveraged Varonis to:

- Reduce unique permissions on folders by **86%**
- Remediate over **212,000** folders with open access
- Completely **eliminate** broken permissions

According to Mr. Brickey:

> **"We've done a lot of work to limit our blast radius. Nobody logs in as a domain admin anymore unless they have a specific purpose — and that was a Varonis recommendation."**

Varonis's built-in analytics have made it easier for Mr. Brickey to keep the board of directors updated on new developments. When data is at risk, or when he needs to make a case for a new Varonis product, he has the information at his fingertips.

> **"We decided we were going to give the board a presentation every month on risk analysis and management. Varonis gives me hard data to present to our board of directors and the ability to identify where we have issues that we need to address for compliance purposes."**

And if a worst-case scenario should ever occur, Mr. Brickey is glad that TPMG has the systems in place to alert on ransomware and stop it in its tracks. He now recommends a Varonis POC wholeheartedly to anyone else with sensitive data to protect.

> **"The ease at which infections can occur keeps me up at night. But having the monitoring in place helps me sleep better. The POC is the real eye-opener. Talking about it isn't good enough — put in the effort and do the POC, because that will give you the data you need to justify the purchase to decision-makers in your organization."**

Your Data. Our Mission.

Varonis helps you improve your data security posture.

Request a demo