

Tampa General Hospital Gets Copilot-Ready with Varonis

“Varonis allowed us to deploy AI. Without it, I don’t think I would have been able to safely green light and recommend Copilot or other AI tools that will crawl our data in the environment.”

HIGHLIGHTS

Challenges

- + Securing sensitive patient data
- + Preparing for an org-wide Copilot rollout
- + Removing unnecessary access without breaking business processes

Solution

The Varonis cloud-native Data Security Platform:

- + Continuously discovers and classifies critical data across M365
- + Locks down permissions and prevents exposures
- + Proactively detects and helps prevent threats

Varonis for Microsoft 365 Copilot:

- + Safely adopt and continuously secure Microsoft 365 Copilot

Varonis Managed Data Detection and Response:

- + Managed 24x7x365 service dedicated to stopping threats at the data level.

Results

- + Moving to Copilot with confidence
- + Remediated 40k+ files in 1 week
- + Data security for 10k employees
- + Varonis MDDR as a first line of defense
- + Automated data security

CHALLENGES

Proving compliance and mitigating the risk of data breaches

Tampa General Hospital (TGH), also known as Florida Health Science Center, is a leading academic healthcare institution with multiple hospitals, clinics, specialty offices, and practices across Florida.

Securing sensitive patient PHI and PII is a top concern for healthcare organizations like TGH.

Gen AI tools like Microsoft Copilot introduce a new layer of complexity: If employees can access too much data, so can Copilot. In seconds, Copilot can retrieve MRN numbers or patient data, including highly sensitive information.

TGH wanted to use AI to automate repetitive tasks and allow staff to focus on providing high-quality care. But they needed to ensure they were fully prepared before unleashing the full power of gen AI. And that preparation started with data.

According to David Quigley, TGH's manager of Identity Protection and Access Management:

“Varonis plays a massive role with gen AI, because of the problems that can happen at scale and very rapidly. It’s very common for people to want to click the ‘easy’ button and share data with everyone in the organization, rather than taking the time to figure out who should have it, and managing those permissions correctly.”

“And so over time, you have a situation where everybody in the organization could have access to sensitive files, and that’s a big risk to the organization.”

David continued:

“Our CISO said, ‘We need to make sure that we don’t have files exposed to everyone in the organization.’ “Our goal was to create a secure foundation, so team members can leverage the benefits of AI in a way that’s safe for our patients.”

Before introducing Copilot, TGH sought to understand their petabytes of data better. They needed to know where their sensitive data lived, who should access it, and what they do with that access.

According to Jim Bowie, CISO for TGH:

“We realized that Varonis was best in class. We reached out to them and said, ‘What can you do for us?’ And that’s where our relationship started.”

Tampa General Hospital boldly and decisively sought to proactively classify and secure its critical data before rolling out Microsoft Copilot to its healthcare staff.

+ + +

+ + +

+ + +

+ + +

+ + +

“Our goal was to create a secure foundation, so team members can leverage the benefits of AI in a way that’s safe for our patients.”

SOLUTION

Preparing for gen AI with Varonis for Copilot

Safely rolling out gen AI is a big undertaking that takes ongoing commitment. As orgs create information and staff come and go, problems like permissions creep, sharing links, and files open to everyone are inevitable – and can only be solved using automation.

Because copilots can unintentionally expose sensitive information, gen AI brings data security problems to the forefront. Orgs can no longer ignore issues with overexposed data, out-of-control permissions, and sharing links that put critical data at risk.

For organizations bringing on gen AI, Jim provides this guidance:

“If you’re going to use gen AI in your organization, you need to clean up your data -- your permissions, shares, and exposures. That’s a massive project. Without automation, you’re going to do this project over and over again.”

TGH chose Varonis as their partner to get their data Copilot-ready. Varonis and Microsoft are helping organizations like TGH roll out AI confidently while continually assessing and improving their Microsoft 365 data security posture behind the scenes before, during, and after deployment.

With Varonis, TGH would gain real-time visibility and control over their cloud data, reducing their blast radius, improving their security posture with automation, and, importantly, preparing to roll out Copilot to 10,000 employees.

According to Jim, deploying Varonis was easy:

“That deployment was amazingly done by Varonis. It was a very seamless transition.”

Varonis’ cloud-native Data Security Platform secures data for TGH in Microsoft 365 and automatically discovers and remediates misconfigurations and toxic combinations that put data at risk.

According to David, Varonis provided visibility into the hospital’s data estate:

“Varonis was instrumental in allowing us to see all of the data, where it all was, and who had access to it.”

Varonis employs machine learning, a subset of artificial intelligence (AI), to enhance cybersecurity in various domains. Machine learning involves using algorithms and statistical techniques to enable computer systems to learn from data and make predictions or decisions without explicit programming. Athena AI is built on Azure Open AI and does not use customer data to train its models.

Varonis Managed Data Detection and Response

TGH's in-house cybersecurity teams are supported 24x7x365 by Varonis Managed Data Detection and Response (MDDR), Varonis' managed service dedicated to stopping threats at the data level. MDDR stands apart in offering the industry's best SLA, with a 30-minute response for ransomware attacks and a 120-minute response for all other alerts.

According to Jim:

“Varonis’ MDDR is a major component of our cybersecurity strategy. It is one of our first lines of defense. Varonis will call us directly when they’re doing their investigations, and MDDR is critical to rapid response and remediating virtually any incidents.”

“We use Varonis’ automation, and we pair that with our own SOC and Varonis’ MDDR -- when things happen, we can fix them right away. It’s a lot easier to keep a room clean than to keep cleaning it every day after you’ve made it dirty.”

Automated outcomes

Before Varonis, IT and security would have to manually check permissions and search for sensitive data that is open to everyone in the organization. Now, Varonis provides TGH with unsurpassed visibility, putting everything together in a convenient dashboard.

Varonis provides deep visibility into data stores that would be impossible to achieve any other way.

According to David:

“You would have to inspect every single group — it’s like a scavenger hunt where you’re trying to find which site has incorrect permissions. Varonis makes it easy. Varonis has an intuitive dashboard where we can go in and see all of our files, where we have sensitive files, and what is shared org-wide externally. Rather than hunting and finding every file that might be a problem one day, it’s right there.”

RESULTS

Deploying Copilot with confidence


By partnering with Varonis, TGH could fully understand their data and deploy Microsoft Copilot with confidence.

Varonis played an instrumental role in helping TGH roll out gen AI. According to Jim:

“Varonis allowed us to deploy AI. Without it, I don’t think I would have been able to safely green light and recommend Copilot or other AI tools that will crawl our data in the environment.”

“With gen AI, problems can happen at scale and very rapidly. If you don’t have the fundamentals to ensure you’re doing the right things, you can very rapidly run into major issues.

“Varonis plays a massive role and is the only reason we can do any of it.”



“Varonis allowed us to deploy AI. Without it, I don’t think I would have been able to safely green light and recommend Copilot or other AI tools that will crawl our data in the environment.”

According to David:

“Varonis played a critical role in our AI readiness. At the end of the day, all these LLMs sit on top of a large data set. The last thing you want to do is have your data set overly exposed so it can read everything.”

“The only reason I’m prepared and feel safe in recommending our AI products through our AI Governance Committee is because we have Varonis. If we didn’t, we wouldn’t be able to move.”

A data security partnership

TGH is impressed with Varonis’s ability to deliver automated outcomes and confidently expedite their move to Copilot.

According to David, Varonis has made TGH’s gen AI preparedness possible:

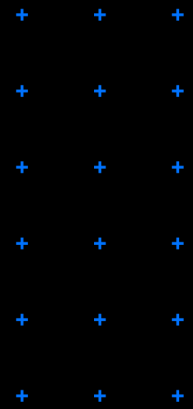
“As long as we have Varonis, I feel that we’re prepared for whatever gen AI wants to throw at us — we’ll be able to look at that data, understand it, and be able to classify it, and be able to mitigate any issues with oversharing and permissions. With Varonis on our side and gen AI, I feel very prepared. Again, it wouldn’t be possible without it.”

And Jim appreciates how the Varonis team is there to support them:

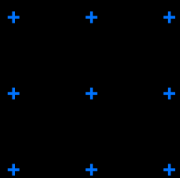
“My experience with Varonis has been amazing. 10 out of 10. I would recommend Varonis as one of the first tools I would bring to any organization.”

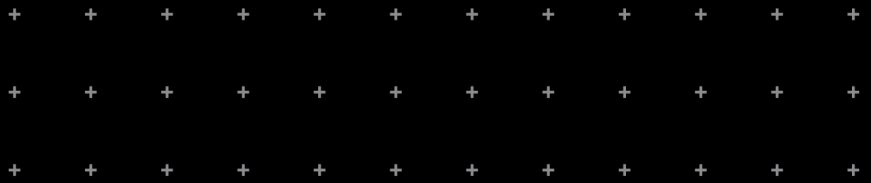
According to David:

“Varonis is a high-quality partner, and I enjoy working with them. Some vendors are just checking a box. But with Varonis, there’s a true business partnership, and they care. I’m going to sleep better at night because I know there’s not going to be data that’s just going to show up somewhere for someone who shouldn’t be allowed to see it.”



“My experience with Varonis has been amazing. 10 out of 10. I would recommend Varonis as one of the first tools I would bring to any organization.”





Safely deploy Copilot with confidence.

Varonis helps improve your security posture with automation and roll out gen AI safely.

[Request a demo](#)