VECTRA
SECURITY THAT THINKS.®

CASE STUDY

University healthcare system counts on Vectra to expose the truth about cyberattacks

Information security professionals would agree that it's important to ensure that end users are empowered to do their job as efficiently and securely as possible.

"There's a fine line between efficiency and security and it requires some give and take between the two," says a senior security engineer at a major university healthcare system in the Northeastern United States.

"You have to know when to get out of the way of efficiency and when to step in if security is threatened," he says. "This is the concept behind the Cognito network detection and response platform from Vectra."

The Cognito® NDR platform automates the hunt for cyberattackers, shows where they're hiding and tells you what they're doing. The highest-risk threats are instantly correlated to compromised host devices and prioritized so security teams can respond fast to stop the spread of attacks and avert data breaches.

"Vectra delivered a customer-focused solution that allows us to tailor the Cognito NDR platform to fit our specific requirements."

Senior Security Engineer
Major University Healthcare System

"Cognito Detect gives us poignant, actionable alerts and reduces anomalous noise and unintelligible events."

Senior Security Engineer
Major University Healthcare System

Organization

Major university healthcare system

Industry

Healthcare

Challenge

Needed a proactive approach to understand threats, threat actors and the methods they employ in the internal threat landscape.

Selection criteria

A network-centric detection and response solution that was endpoint agnostic and would bring clarity to internal network traffic.

Results

- Poignant, actionable alerts that reduce anomalous noise and unintelligible events.
- AI and machine learning that detects threat behaviors in the network and stops the progression of attacks.
- A customer-focused solution that allows the Cognito NDR platform to fit and be tailored to specific requirements.

Logs, agents and IoT

Before deploying Vectra®, the healthcare system had in place anti-virus, anti-malware and email filters to protect end users.

"This was useful to detect phishing emails aimed at users, but it was reactive instead of proactive," says the senior security engineer. "We have Windows machines, IoT and regulated medical devices on the network that cannot support agents for endpoint detection."

The healthcare system had used a log and event manager to identify potential cyberthreats but it created a lot work for the security team. It relied on the vendor to integrate the log and event manager with other security systems, which resulted in a deluge of anomalous alerts that didn't make sense and were incompatible with security feeds that flowed into it.

"We were mostly blind to cyberthreats inside the network," says the senior security engineer. "This reactive approach lacked any sort of intelligence or ability to truly understand the threats, the threat actors, the methods they employ or our internal threat landscape."

At this point, one thing was understood: The university healthcare system needed a network-centric detection and response solution that was endpoint agnostic and which would help bring clarity to internal network traffic.

The Vectra trifecta

The healthcare system deployed the full trifecta of Vectra solutions, which are currently running on the Cognito NDR platform – Cognito Detect™, Cognito Recall™ and Cognito Stream™.

Cognito Detect identifies and stops cyberattackers in cloud, data center, IoT, and enterprise environments. It uses AI-derived machine learning models to deliver real-time attack visibility and put attack details at your fingertips.

> "It is one of those rare products that works the way it's supposed to. The technology and science behind Vectra complement each other in one incredible solution that ensures your investment is well spent."
>
> **Senior Security Engineer**
> *Major University Healthcare System*

"Cognito Detect gives us poignant, actionable alerts and reduces anomalous noise and unintelligible events," says the senior security engineer. "This helps us to quickly identify the most critical alerts and makes us more efficient."

Cognito Recall performs AI-assisted threat hunting in cloud and data center workloads and user and IoT devices. As a comprehensive source of security-enriched network metadata stored in the Vectra cloud, Cognito Recall also empowers the security team to conduct more conclusive incident investigations.

Using Cognito Recall, the healthcare security team can hunt proactively for threats, diagnose problems, and examine who and what was communicating with compromised hosts based on user identity and account privileges.

Cognito Stream delivers deep security insights and context needed to build custom tooling as well as feed models to detect, investigate and hunt. Delivered in open-source Zeek, it integrates seamlessly with the customer's SIEM without the overhead and scale limitations associated with open-source Zeek.

With Cognito Stream, the security team's SIEM ingests security-enriched metadata and relevant logs captured from all network traffic in cloud, data center, IoT, and enterprise networks.

"Cognito lets us correlate Vectra detections with data from other systems in our security stack," says the senior security engineer. "It's easy to get useful, in-depth information about security events, actually see and understand the data, identify trends, and create investigative and compliance reports."

The senior network engineer also points out that the Vectra support team was critical to ensuring the security team extracted maximum value from the Cognito NDR platform.

"The level of support has been amazing," he says. "Vectra delivered a customer-focused solution that allows us to tailor the Cognito NDR platform to fit our specific requirements."

"The truth is in the network traffic and Vectra uncovers that truth."

Senior Security Engineer
Major University Healthcare System

Post-deployment enjoyment

To gather behavioral information from traffic, the security team deployed Vectra sensors in the network core and distribution layers for unobstructed visibility into the lateral movements of attackers from east to west.

"Vectra gave us internal visibility without relying on software agents," says the senior network engineer. "And by leveraging the platform, its AI and machine learning, we are now better positioned to detect threat behaviors in the network and stop the progression of attacks that we previously couldn't see. These were the big selling points for us."

The university healthcare system also received unexpected benefits from Vectra. Many employees were still using old legacy systems with unsecure protocols and poor workflows, which enabled users to access data in an unsecured manner.

"Vectra helped us identify weaknesses in security policies and workflows," says the senior security engineer. "Employees had grown too accustomed to doing things in ways that were not secure."

"It was a big deal to me too because it helped me better understand the user's mindset," he adds. "There are lots of intuitive benefits about the Cognito platform that you won't find on a data sheet."

Since then, the security team has easily identified and fixed network vulnerability and hygiene issues. In fact, this led to a company-wide initiative to target and eliminate the use of unsecure legacy protocols.

"The truth is in the network traffic and Vectra uncovers that truth," says the senior network engineer. "It is one of those rare products that works the way it's supposed to. The technology and science behind Vectra complement each other in one incredible solution that ensures your investment is well spent."

> "There are lots of intuitive benefits about the Cognito platform that you won't find on a data sheet."
>
> **Senior Security Engineer**
> *Major University Healthcare System*

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai