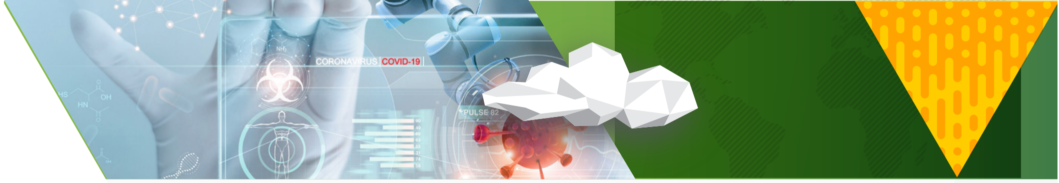
VECTRA
SECURITY THAT THINKS.®



CASE STUDY

Pennine Care NHS counts on Vectra to stop cyberattacks

The NHS Foundation Trust is no stranger to cyberattacks

Threats have been top-of-mind among NHS trusts since they fell victim to the 2017 WannaCry ransomware attack that affected more than 150 countries and disrupted a third of NHS operations.

Although no patient data was compromised or stolen and they stopped the attack from spreading, all NHS trusts have since stepped up security to identify and stop future cyberthreats.

The challenge: Stop hidden cyberthreats

Never has this been more apparent than at the Pennine Care NHS Trust in northern England, which since 2002 has provided vital mental health and learning disability services in parts of Greater Manchester and Derbyshire.

ICT security manager Rizwan Majeed was entrusted to protect Pennine Care NHS from cyberthreats. After consulting with NHS Digital, the IT and security arm for the trusts, and other NHS facilities, he began to evaluate potential solutions, including network detection and response (NDR).

> “We considered open-source Nagios Core to monitor our systems, networks and infrastructure,” says Majeed. “But it was complicated to use and the daily cost of storing 20 GB of maintenance logs from six servers was prohibitive.”

NHS
Pennine Care
NHS Foundation Trust

Organization

Pennine Care NHS Foundation Trust

Industry

Healthcare

Challenge

Continuously monitor and detect hidden cyberattackers that could impact mental health care, operations and patient safety

Selection criteria

Automated threat detection to reveal hidden attacks and provide more time to investigate and hunt for threats

Results

- Automated detection and response, giving more time to investigate and hunt for threats
- Collection and storage of historical metadata to protect data privacy and support GDPR
- Information needed to reveal attacker’s behavior is one click away

The solution: Detect, hunt and investigate

After learning and observing how another facility, Bolton NHS Foundation, deployed the Cognito® platform from Vectra® to identify and stop cyberattackers in real time, Majeed was convinced that this was the optimal NDR solution.

"We selected Cognito Detect™ and Cognito Recall™ software, both of which operate on the Cognito platform," says Majeed.

Cognito Detect applies AI-derived machine learning algorithms to automatically detect and respond to in-progress cyberattack behaviors in cloud/SaaS, data center, IoT, and enterprise networks.

Attack behaviors that pose the greatest risk with the highest degree of certainty are automatically prioritized, enabling Majeed to immediately determine where to start remediation, hunting and investigating.

To further reduce time and resources, Cognito Detect rolls-up multiple alerts into a single incident or attack campaign for investigation. AI-based machine learning automatically ties related threats into one chain of connected events.

"With Vectra, I don't have to sift through endless logs to identify real threats," notes Majeed. "Cognito Detect automates detection and response, which gives me more time to investigate and hunt for threats using Cognito Recall."

AI-driven Cognito Recall is a cloud-hosted investigative workbench that uses security-enriched metadata for more productive threat hunting and conclusive incident investigations.

The Cognito platform extracts, analyzes and stores relevant logs, cloud events and metadata at scale from all network traffic – from cloud/SaaS and data center workloads to user and IoT devices.

This metadata is then enriched with deep security insights and context about attacks. This gives Pennine Care NHS unprecedented visibility to detect, respond, hunt and investigate cyberthreats with greater efficiency and precision.

Cognito Recall metadata is arranged by host name, not just IP address. This eliminates rifling through DHCP logs to find a host device that was using an IP address and identifying IP address changes during an investigation. Searching by device saves time when speed is essential.

“Cognito Recall collects and stores all this historical metadata, instead of packet payloads, to protect data privacy and support GDPR,” says Majeed. “There’s no big data infrastructure to buy, install or manage.”

The Cognito platform was deployed at Pennine Care NHS on a weekend and began firing detections once the AI and machine learning became familiar with behaviors in the local network environment.

“I cannot say enough about Vectra support,” says Majeed. “If I make a support call or email inquiry, I get a response in under 10 minutes. The support I get from Vectra is simply brilliant.”

Under suspicion

One challenge that Vectra helped solve centered around slow Citrix VPN traffic.

“We didn’t know what was causing the problem,” Majeed says. “We worked with Citrix for several months and they couldn’t solve it either. Then Vectra stepped in and suggested that we check the ciphers we were using for the VPN.”

Instead of reading a static list of ciphers that were in place, Cognito Recall with one click can determine if encryption, such as TLS, is actively used. The predefined rules in Cognito Recall are designed to ensure security compliance and hygiene.

“Vectra showed us that weak ciphers were being used, which creates a sizable security risk,” says Majeed. “But instead of spending three weeks to find the list of the devices, it’s just one click to see what’s in use and where.”

In another incident, the Cognito platform detected a user uploading 10 GB of data each day on YouTube.

“This might have been an internal threat exfiltrating private healthcare information,” recalls Majeed. “I immediately contacted the user and it turned out to be a trainer in the clinic department uploading training videos.”

“What I like most about Vectra is that the information you need – who, where and what attackers are doing – is usually just a click away,” he concludes. “Vectra tells you everything you need to know about cyberattacks.”

For more information please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai