VECTRA

Customer Story | Healthcare

Healthcare Organization Strengthens Microsoft Security with Better AI

This Finland-based healthcare organization delivers essential health and emergency services across a large regional footprint. Supporting nearly 8,000 professionals, the organization operates in a highly regulated environment where continuity of care, coordination across services, and strong security oversight are critical.

With responsibility for both day-to-day healthcare delivery and emergency response, the organization must ensure its systems are resilient and capable of supporting uninterrupted care while meeting evolving national cybersecurity requirements.

Industry
Healthcare

The Challenge
While using Darktrace, the healthcare organization faced persistent alert noise, ongoing tuning, and limited investigative context, making it difficult to clearly assess threats across its hybrid and Microsoft environments.

The Solution
Through a structured proof of value and offensive security assessment, the security team evaluated Vectra AI's ability to deliver deeper detection accuracy and clearer investigative context across network, identity, and cloud activity.

The Results
By adopting the Vectra AI Platform, the organization reduced alert noise, accelerated investigations, and strengthened the resilience of its security operations.

Security Transformation

Platform value at a glance

Vectra AI's Impact	Outcome
Reduced cyber risk exposure	• Unified observability across on-prem network traffic, Microsoft 365, Entra ID, and Azure gave the healthcare organization consistent visibility across its hybrid environment, closing gaps that remained despite existing Microsoft E5 investments.
Improved SOC efficiency	• Behavior-based detections reduced alert noise and surfaced clear risk signals, helping analysts quickly understand which activity warranted investigation. • Fourteen-day metadata retention added deeper forensic context when more detailed investigation was required.
Faster mean time to respond	• Built-in response automation and native integrations with SOAR and existing infrastructure enabled faster, more confident action while simplifying ongoing security operations.

VECTRA

The Challenge

Fragmented visibility, alert noise, and limited context slowed day-to-day investigations

As the healthcare organization approached the end of its Darktrace contract, the security team reassessed whether the platform was truly supporting their detection and investigation efforts.

"Because we handle sensitive healthcare data and support critical services, the bar for security is incredibly high," said the healthcare organization's lead security architect.

In practice, persistent alert noise and ongoing tuning that never seemed to stick slowed the team down. Analysts spent time recreating rules and adjusting thresholds, yet alerts often arrived without enough context to quickly understand scope, impact, or next steps.

Visibility gaps added to the challenge. Despite having Microsoft E5 licenses in place, coverage across Microsoft 365, Entra ID, Azure, and on-prem network activity remained fragmented, limiting observability and making it difficult to connect identity, cloud, and network behavior during investigations.

As the lead security architect noted, "Microsoft security is an important part of our stack, but it isn't sufficient on its own. NDR was the missing component, and that gap couldn't be addressed with Microsoft products alone."

With Finland's new Cybersecurity Act raising expectations for network and identity monitoring, they needed a solution that unified visibility, reduced noise, and delivered clearer investigative context across its hybrid environment.

The Solution

Connecting signals to drive more confident action

The healthcare organization evaluated alternatives through a structured proof of value that included network, Microsoft 365, and Entra ID coverage alongside an offensive security assessment.

During testing, the security team observed clear differences in detection depth and investigative context. Darktrace surfaced only a single low-severity alert, while Vectra AI surfaced attack behavior across the complete kill chain, allowing analysts to understand how activity unfolded rather than responding to isolated alerts.

"With our previous tools, alerts arrived without enough context to act quickly. Vectra AI gave us the ability to see how activity unfolded across identity, cloud, and network, which significantly reduced the time spent trying to understand what was actually happening," explained the lead security architect.

Beyond detection, they saw the value of consolidating network, identity, and cloud signals into a single investigation experience built on shared context. Behavior-based detections, built-in response automation, and 14-day metadata retention provided the foundation needed to investigate efficiently and reduce exposure without adding operational complexity.

Following the evaluation, the healthcare organization consolidated coverage into the Vectra AI Platform, replacing Darktrace and extending protection across its hybrid and Microsoft environments.

"With increasing regulatory expectations around identity and network monitoring, we needed confidence that we could detect and investigate real threats quickly. Vectra AI gave us that confidence without adding operational complexity," said the lead security architect.

"With increasing regulatory expectations around identity and network monitoring, we needed confidence that we could detect and investigate real threats quickly. Vectra AI gave us that confidence without adding operational complexity"

LEAD SECURITY ARCHITECT
Healthcare Organization

"With our previous tools, alerts arrived without enough context to act quickly. Vectra AI gave us the ability to see how activity unfolded across identity, cloud, and network, which significantly reduced the time spent trying to understand what was actually happening."

LEAD SECURITY ARCHITECT
Healthcare Organization

The Results

Security operations built to last

By implementing Vectra AI, the healthcare organization established a more sustainable security model:

- Unified observability across network, identity, and cloud, supporting resilient operations across the organization's hybrid environment
- Faster investigations with clearer signal, driven by behavior-based detections and metadata-rich context that reduced time spent chasing low-value alerts
- Simpler security operations, enabled by built-in response automation and native integrations that lowered manual effort without adding operational complexity
- Improved readiness for evolving regulatory requirements, including Finland's Cybersecurity Act, through stronger network and identity monitoring.

"Vectra AI has strengthened our overall security posture and brought greater consistency to how we manage risk across the environment," shared the lead security architect.

"Vectra AI has strengthened our overall security posture and brought greater consistency to how we manage risk across the environment."

LEAD SECURITY ARCHITECT
Healthcare Organization

Read more customer stories

For more information please contact us: Email: info@vectra.ai | vectra.ai