VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Cyberthreats Are No Match for This Resilient Retailer

Retail companies have no shortage of challenges to navigate these days, making it more important than ever to deploy cybersecurity solutions that they can rely on to detect malicious activity associated with today's critical threats. Not only do these tools need to outmatch threats like ransomware and account takeovers, but they also can't get in the way of the fast-paced operations of today's retailers.

This scenario is all too familiar for the Head of IT Security at a European global retailer, who is challenged with navigating through the complexities of cloud adoption, while making sure his security tools don't let any threats slip through the cracks. He began to evaluate at least five solutions to address his detection and response demands — and hasn't looked back since. While his initial short list of candidates included Darktrace and Cisco, after completing PoCs with each, he settled with confidence on the only one that was up to the task — Vectra Cognito, the AI-driven threat detection and response platform.

"Vectra AI said what they are able to do in terms of detection and performance, which they proved later in their technical PoC, to the point. They were actually the only ones who could," said the Head of IT Security.

"Vectra AI brings great visibility. Without it, we would be blind."

Head of IT Security
Global 2000 Retail Company

Organization

Global 2000 Retail Company

Industry

Retail

Challenge

Navigating through the complexities of cloud adoption and making sure deployed security tools don't let any threats slip through the cracks

Selection criteria

An AI-based network detection and response (NDR) solution that focuses on the most critical, severe detections

Results

- Received value to their security operations within two weeks of deployment
- Can rely on Vectra detections and its event generating mechanism to clearly focus on the most important priority one cases
- Optimal signal-to-noise ratio that gives confidence of having a realistic chance of catching and stopping real attacks in time

Less Noise, More Visibility in the Right Places

For this organization, part of being able to stop attacks in a timely manner means that the security team is receiving accurate detections that they can use to remediate an issue. Instead of sifting through hundreds of security alerts that may or may not indicate that something needs attention, Vectra Cognito makes it clear which alerts need attention.

"This solution is like the absolute base coverage for us. You don't get many alerts, and if you get one, you better look at it because it is a good quality alert," says the Head of IT Security.

Quality detections also help the team prioritize the most important projects, even when it comes to how each team member focuses their time and effort. This is especially important as they're use of cloud has expanded. Even with a small team, they're able to detect systems that aren't behaving correctly, or when access to a malicious site or domain exists — now they know when anything out of the ordinary happens and can quickly address it.

"We have a large network with a lot of points of sales and other geographical locations that are interconnected. We need visibility of all the client-initiated traffic to and from our main data centers and to the Internet," says the Head of IT Security.

He expressed that while their other security tools should be picking up potentially dangerous activity, they now have the coverage they need with Vectra — even throughout various hotspots in the environment. "Vectra AI brings great visibility. Without it, we would be blind," he continued.

Building a Secure Future

As a Vectra customer for four years and counting, this retailer is always looking for ways to get the most out of their deployment. One of the ways they've done this is by leveraging Cognito Stream — where customers can get the right security-enriched cloud and network metadata streamed to SIEMs and data lakes. Customers can then build custom tools and feed models to improve detections, investigations and threat hunting.

"This solution is like the absolute base coverage for us. You don't get many alerts, and if you get one, you better look at it because it is a good quality alert."

Head of IT Security
Global 2000 Retail Company

> "In terms of our security stack, this is the most essential cybersecurity tool we use. It has been designed by security people for security people."
>
> **Head of IT Security**
> *Global 2000 Retail Company*

"One of its strongest parts is that the solution captures network metadata at scale and enriches it with security information. We forward events to our team, then we can correlate them even better," said the Head of IT Security. "With Stream enabled, we can easily find out who is using SMB v1, as an example. So, it is a kind of hunting in the network."

He also appreciates the functionality offered by Detect for Microsoft 365. Stating that, "it will not only see the local traffic, i.e., the local user but also how the user is connecting to the cloud. If communication has been initiated within wour network, we would capture anomalies with on- premises mechanisms. If it is a connection from the Internet to M365 SaaS services, we gain visibility through the Vectra add-on."

In addition to Cognito and Detect for Microsoft 365, this retail company has supplemented their team with Vectra Sidekick Services. "We have a team of three people, mainly security officers, who are investigating or following up on detections and alerts. We also use the Vectra AI Sidekick Services, which helps a lot by providing a skillful set of people who look into things with a great customer perspective," he said.

Sidekick ensures that the team has Vectra analysts by their side 24/7 to proactively investigate any malicious activity. Sidekick analysts provide expert opinions to their team to make sure they're getting the most out of the deployment, and simultaneously build knowledge and skill within the internal team.

An Essential Piece to the Puzzle

For a team that values the security of its customers, employees and their entire environment — they refuse to have their business held back by any lurking cyberthreats now, and in the future.

They'll continue to be proactive in their approach to cybersecurity like they have been over the years with Vectra.

"In terms of our security stack, this is the most essential cybersecurity tool we use. It has been designed by security people for security people. It provides a very smooth and fast way to set up manual rules or triage filters. I would rate this solution as 10 out of 10," the Head of IT Security concluded.

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai

© 2021 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.Version: **120921**