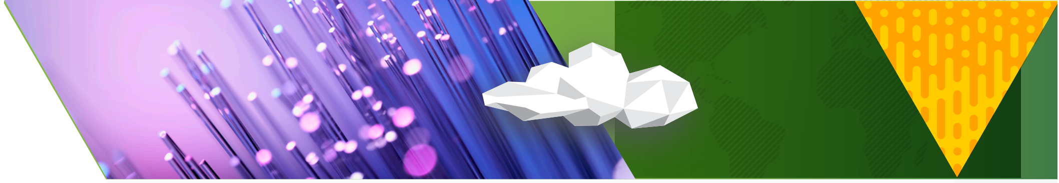
VECTRA
SECURITY THAT THINKS.®



CASE STUDY

So Secure, It’s Boring

Executive Summary

Having a deep understanding about the skills and tactics used by today’s motivated cybercriminals, this Head of IT Operations and IT Security at this telematics company prioritizes security when designing internal systems. He knows security simply can’t be overlooked as their business provides telematic services to insurance clients, requiring them to store and transfer sensitive customer information on a regular basis. So, this must mean they have a dedicated SOC team with the freedom to deploy just about any security tool they need on a whim, right? Well, not so much.

In fact, with the company currently around 100 total employees, its IT operations team sits with five employees who are tasked with handling everything IT related, including security. With limited financial ability to fund a SOC team, it became a priority to find alternatives within their budget.

> “Our selection of software and certain architecture designs are with security in mind, so we try to prevent a number of tickets from happening from the beginning.”
>
> **– Head of IT Operations and IT Security**
> *Telematics Company*

Organization

Telematics Company

Industry

Telecommunications

Challenge

Limited resources and budget

Selection criteria

An AI-based Network Detection and Response (NDR) solution that was software and operating system agnostic

Results

- Can now detect abnormalities in traffic moving from workstations to locations either inside or outside of their environment
- Cognito Recall assists the security team for their threat-hunting needs
- Vectra produced a more holistic view of their environment

Security Minded, Resource Constrained

Even with limited resources, security remains top of mind for this organization where the risks of letting cybercriminals roam free in their environment are well understood. In order to address the threat of today's sophisticated attacks such as account takeovers and ransomware, they started looking for ways to ramp up their ability to see and address malicious behavior before it becomes a serious issue. The next step was to start evaluating solutions that could help solve this challenge.

In addition to budget limitations, this telematics company had another requirement. "What we want has to be software and operating system agnostic," says the Head of IT Operations and IT Security.

With a technical background as an engineer, the Head of IT Operations and IT Security prefers to avoid agent-based solutions and detection systems that cater towards one specific type of software or operating system. Still, they needed to prioritize threat detection but knew the small team didn't have the cycles to be bogged down with alert fatigue. Rather, he wanted to focus on finding a way to identify and respond to attacker behavior if and when the time comes.

To expand the organizations' security capabilities, they started evaluating network detection and response (NDR) solutions to help detect attacker behavior, increase their human expertise with artificial intelligence (AI) and address any threat or abnormal activity. After evaluating different solutions in their environment, this telematics company selected Vectra Cognito Detect as it met their technical demands.

> "With Vectra, we had a system that was quicker and easier to read."
>
> **Head of IT Operations and IT Security**
> *Telematics Company*

Get in and get out

A number of factors ultimately came into play for the decision to move forward with Vectra. Vectra was agnostic, but it also produced a more holistic view of their environment.

"With Vectra, we had a system that was quicker and easier to read," says the Head of IT Operations and IT Security.

Just to make sure that Vectra was up to the challenge, the company also evaluated Darktrace, but determined that Vectra did a better job of presenting information in plain sight and made digging into the data much easier, according to the Head of IT Operations and IT Security.

> "With Darktrace, I have to go through lots of flashy things, not necessarily useful things. Whereas Vectra is far more accessible and readable from the start."

Head of IT Operations and IT Security
Telematics Company

He went on to point out that coming from a technical background as an engineer and working with a small multi-purpose team—they can't afford to spend time looking for detection details. But rather that they need the ability to get in and out quickly with the right detection information.

Now seeing… all threats

These days, any abnormal traffic that comes through the company's environment is flagged by Vectra Cognito Detect, and they specifically rely on it for detecting abnormalities in traffic moving from workstations to locations either inside or outside of their environment.

Additionally, since they work on behalf of insurance companies and commonly deal with personally identifiable information (PII) data, they're now able to detect when any abnormal transfers are made. And while that remains their primary way of detection and response, the company also uses Cognito Recall for times when its team wants to take their threat-hunting skills to the next level.

The team also leverages Amazon Web Services (AWS) for public cloud services and have been using Amazon GuardDuty for threat detection and monitoring of cloud accounts, workloads and data.

Using both AWS and Vectra, this telematics company is able to efficiently protect all of its data throughout the environment both on-premises and in AWS cloud instances. "We operate in AWS and utilize GuardDuty to augment what Vectra provides in our local systems. Having both tools has been great," says the Head of IT Operations and IT Security.

This small team has done its security homework, and isn't interested in letting any threats squeak by unnoticed regardless of where or how they try to get in. By creating an environment that prioritizes security and doesn't just stand back waiting for something bad to happen, they've setup a secure, yet perhaps even "boring" environment when it comes to threat activity.

> "Our security approach along with Vectra kind of generates this very boring environment, which is good. We're happy where we are!"

Head of IT Operations and IT Security
Telematics Company

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

Email info@vectra.ai vectra.ai