VECTRA
SECURITY THAT THINKS.®

CASE STUDY

# Manufacturing Company Saves More Than Just Their Network with Vectra

Securing a geographically dispersed environment comes with no shortage of challenges in today's threat landscape. This is exactly why the Senior Security Engineer at a distributor in North America took the initiative to seek out a Network Detection and Response (NDR) solution capable of increasing visibility across their environment.

With a centralized data center and numerous physical locations across the country, their network is very distributed, and traditional security vendors continued to fall short when it came to stranger peripherals such as printers, scan guns, tablets, and guest devices. Ultimately, the Vectra Threat Detection and Response Platform met the criteria demanded to protect this environment. "Now, we're able to actually see those devices hit our internal LAN instead of our guest networks, and we can properly move them over, whereas earlier, we were blind," said the Sr. Security Engineer.

Using the Vectra Threat Detection and Response Platform provides visibility across the full attack lifecycle and beyond the internet gateway. "Now, we have some reasonable assurance that our internal tablets, scan guns, and things like that are not performing abnormal network behavior," he continues.

> "There are $50,000 to $100,000 storage cost savings." **Sr. Security Engineer**
> *Distribution company*

### Organization

Distribution Company

### Industry

Manufacturing

### Challenge

Lack of network monitoring

### Selection criteria

An AI-based Network Detection and Response (NDR) solution that allowed for custom rules and increased network visibility

### Results

- $50,000 to $100,000 storage cost savings
- Ability conduct more conclusive incident investigations by searching and creating custom rules
- Assurance that internal tablets and scan guns are not performing abnormal network behavior

## Filling the Gap

The Vectra Platform uses AI-derived machine learning to automatically detect and respond to cyberattacks across cloud, data center, IT, and IoT networks. It also enables security operations teams to perform conclusive incident investigations and AI-assisted threat hunting.

"Before we deployed Vectra, we were not monitoring network traffic. So, there was definitely a need and a gap, and Vectra has filled it," says the Sr. Security Engineer. With Vectra, the ease of deployment allows this security team to maintain and administer several hundred locations without having to think twice.

"Vectra, with being so easy to deploy and so easy to maintain and administer, has saved us hundreds of hours just on deployment and standing up the environment alone," he recalls.

> "With Vectra, you're picking reliable and fast. As we grow, we'll deploy more Vectra sensors to capture that extra traffic."
>
> **Sr. Security Engineer**
> *Distribution company*

## Deploy and Detect

While exploring NDR solutions, this manufacturing company also evaluated Corelight before selecting the entire Vectra Platform, including Detect, Recall, and Stream. They chose Vectra for the quick deployment time and routine administration costs as well as its ability to create rules for major events, ML, and AI engines on top of allowing custom rule detection.

"The time it would take to maintain the environment was significantly lower than the other solutions," he explains. "This was the only solution that was easy and fast to deploy and maintain, and that was giving us all three options for rule detection," he continued.

Detect uses AI machine learning models to deliver real-time attack visibility and make attack details easily accessible.

Additionally, Recall performs AI-assisted threat hunting in cloud and data center workloads as well as user and IoT devices. As a comprehensive source of security enriched network metadata stored in the Vectra cloud, Recall empowers this security team to conduct more conclusive incident investigations. Using Recall and Stream, "allows us to search and create custom rules and then we pull data from that environment into our on-prem environment," says the Sr. Security Engineer.

"We spend 99% of our time in Vectra investigating cases, responding to incidents, or hunting, and only around 1% of our time is spent patching, troubleshooting, or doing anything else."

## Saving More Than Just Their Network

Vectra significantly saves this team time and effort that they can now use to respond to incidents. The Sr. Security Engineer notes that "because Vectra only PCAPs the session when it triggers a detection, we didn't have to deploy hundreds of terabytes of storage across our network."

By rolling-up multiple alerts into a single incident or attack campaign for investigation, Detect eliminates the need for excessive storage, leading to other savings for this manufacturing company.

"There are $50,000 to $100,000 storage cost savings because it only captures the full packet capture for traffic that triggers detections. In terms of time, it has saved hundreds of hours. I can't even explain how happy we are with the amount of time it has saved us."

"With Vectra, you're picking reliable and fast," he says. "As we grow, we'll deploy more Vectra sensors to capture that extra traffic."

> "[Vectra] has saved hundreds of hours. I can't even explain how happy we are with the amount of time it has saved us."
>
> **Sr. Security Engineer**
> *Distribution company*

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

Email info@vectra.ai vectra.ai