VECTRA
SECURITY THAT THINKS.®

CASE STUDY

# Major real estate firm replaces IDS/IPS with AI-driven network detection and response

All publicly traded companies risk being targeted by cyberattackers, and this $5 billion U.S. real estate and relocation services firm is no exception. In fact, that realization kept the security operations team up at night.

"Phishing and malware are so prevalent today," says the company's deputy chief information security officer. "It's easy for cybercriminals to trick people and get inside the network. We have over 11,000 employees so it's a constant worry."

The company owns several widely known real estate brands, brokerages, relocation, and title services. To keep everything humming 24x7, the company has three major data centers and many dozens of offices across the country.

## Challenges

The security operations team determined it was time to modernize the way the it dealt with potential cyberthreats.

The company had combined intrusion detection and intrusion prevention systems to catch threats at the network perimeter. However, their performance didn't scale and they offered zero visibility inside the network and data center.

Security operations teams are also overburdened by manually investigating thousands of threat alerts per day that might or might not be an attack. Chasing-down every indicator causes significant alert fatigue and gives real attacks more time to spread.

"IDS has way too much alert noise," says the company's director of cybersecurity. "The performance of our IDS and IPS couldn't keep up and was virtually unusable."

"IDS has way too much alert noise. The performance of our IDS and IPS couldn't keep up and was virtually unusable."

**Company director of cybersecurity**
*Major Real Estate Firm*

### Organization

Real estate organization

### Industry

Real estate, brokerage, title, relocation and settlement services

### Challenge

Modernize response to cyberthreats

### Selection criteria

Network threat detection and response that scaled and provides visibility into their network.

### Results

- Real-time context and insights about threat behaviors
- Reduction of alerts from thousands a day to 2-3 alerts a day
- Full scope of threat activity across their

"We'd get thousands of alerts in just 20 seconds," the director of cybersecurity says, adding "That makes it impossible to do anything. Where do you start when you're inundated with thousands of alerts?"

The deputy CISO echoed those sentiments, saying that "There was absolutely no intelligence, no context about threats, and everything was based on rules. It required a lot of manually-intensive work."

## Network detection and response over IDS/IPS

The security team considered Vectra and Darktrace, and eventually passed on Darktrace.

"When I first saw a demo of Vectra Cognito, it had a fresh, next-generation approach to detecting threat behaviors and handling alerts," says the director of cybersecurity. "It shows what's happening inside the network."

"I immediately liked what I saw," says the deputy CISO. "Unlike IDS and IPS, there were no signatures and no rules. We knew at that point the Vectra approach to AI and machine learning was the way to go."

"I immediately liked what I saw." Unlike IDS and IPS, there were no signatures and no rules. We knew at that point the Vectra approach to AI and machine learning was the way to go."

**Deputy CISO**
*Major Real Estate Firm*

The Cognito NDR platform prioritizes in-progress attacks that pose the highest business risk so the security operations team knows instantly where to focus its time and attention.

The Cognito® Network Detection and Response platform from Vectra® is light years beyond the security industry's definition of NDR. It takes a huge leap forward in solving many formidable challenges faced by security operations teams who are entrusted to protect critical business data.

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

"Unlike IDS and IPS, Cognito has incredible intelligence," says the deputy CISO. "The machine learning gives us real-time context and insights about threat behaviors – where they are, what they're doing and what's affected."

The Cognito NDR platform prioritizes in-progress attacks that pose the highest business risk so the security operations team knows instantly where to focus its time and attention.

"Cognito gives us time to stay ahead of attacks," says the director of cybersecurity. "Instead of getting thousands of alerts, we only get about 2-3 a day that we investigate. We don't waste time chasing-down false positives."

## Detecting attackers is incomplete without a quick response, and Vectra responds with deliberate speed. The Cognito NDR platform integrates with a vast ecosystem of third-party security solutions to accelerate response time.

Along with the Cognito NDR platform, the company uses Carbon Black for endpoint detection and response (EDR), a SIEM from Splunk, and Cybersponse for security orchestration, automation and response (SOAR).

"Everything goes into Splunk," says the director of cybersecurity. "If I want to see all threats in a specific server, the SIEM shows everything from Vectra and Carbon Black. We get the full scope of threat activity across our multivendor security stack."

Driven by AI, the Cognito NDR platform automates manual and mundane security tasks. This reduces the security operations workload and enables the security operations team to work on assignments of greater importance.

"The data from Cognito is very useful," says the director of cybersecurity. "I can easily search for threats and run reports about what I find. Instead of a burden, Cognito is fun and challenging to use, especially in threat investigations."

Driven by AI, the Cognito NDR platform automates manual and mundane security tasks.

Email info@vectra.ai vectra.ai



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