VECTRA

Customer Story | Financial Company

Global Financial Services Firm Banks on NDR to Stop Cyberattacks

When this global financial services company deployed Vectra Network Detection and Response (NDR), "it was as if the fog suddenly lifted from our security operations," says the firm's head of cybersecurity.

Vectra NDR allows the team to confidently stop attackers targeting the network and cloud by finding real attacks through less noise while making the investigation and response process simple.

With over $118 billion in assets, visibility into the hidden actions of cyberattackers is critically important to this independent financial services company, whose rich history in banking and asset management dates back 150 years.

Organization
Anonymous

Industry
Financial company

The Challenge
Their security team was in constant reactive mode. They were working off of homegrown solutions that required a lot of software patches.

Selection Criteria
A platform that would enable their security team to proactively detect and respond to hidden threats inside their networks.

The Results

- Gained more value from Vectra NDR in a week than from configuring their SIEM for an entire year
- No longer have to sift though DHCP logs or identify IP address changes during an investigation
- Vectra NDR tells his team every critical alert worth investigating and how to go about resolving it

The Challenge

From zero to 100

"We went from zero to 100 percent visibility into attacker behaviors with Vectra AI," says the company's head of cybersecurity. "We were amazed at what Vectra AI could see inside network traffic. We get context and details about every attack and know which ones are the most critical."

However, the road to success was not easy to navigate.

"When I first started, we already had a SIEM," he explains. "But nobody really took care of it, so it was outdated and required a lot of software patches. We rebooted it and leveraged the security tools we had but it was still quite a challenge."

In those early days, the company's the security operations center (SOC) was in constant reactive mode. According to the head of cybersecurity, it was like putting out fires. The SOC team would see smoke and rush over to investigate.

The company started to evaluate potential NDR solutions, including Darktrace and Vectra AI. The SOC team hoped that the right NDR solution would enable them to proactively detect and respond to hidden threats inside the network.

"We weren't convinced by Darktrace," says the head of cybersecurity. "It had a dazzling interface but didn't operate very efficiently."

Conversely, the company's SOC team described its first experience with Vectra AI as "quite pleasant" and "empowering" to use. Vectra AI even detects attacker behaviors in encrypted traffic without requiring any decryption or deep packet inspection.

"Vectra AI was up and running quickly" said the head of cybersecurity. "It was easy to use and the graphical dashboard was very intuitive to navigate. You don't have to be a cybersecurity expert to use Vectra AI."

In addition to Vectra NDR, the company also relies on Vectra Cloud Detection and Reponse (CDR) for Microsoft 365 for signal clarity around attacks targeting its SaaS environment.

"We went from zero to 100 percent visibility into attack behaviors with Vectra."

Head of security
Global financial services firm

The Solution

A hunting we will go

Credential abuse is the leading cyberattack method used against Microsoft 365, which has more than 345 million current users. Smart attackers will exploit human behavior to hijack passwords, takeover accounts and steal critical business-data.

To combat this, the company's SIEM had been receiving Microsoft 365 logs, which required the SOC team to configure time-consuming setup rules. But that tedious, manual work has been eliminated since deploying Vectra CDR for M365.

"We gained more value from Vectra AI in a week than we gained from configuring our SIEM for an entire year," says the head of cybersecurity.

Vectra CDR for M365 ingests activity logs from multiple services like Microsoft 365, Microsoft Entra ID, SharePoint, OneDrive and Exchange. Vectra AI analyzes logins, file creation and manipulation, DLP configuration, and mailbox routing configuration and automation changes.

Vectra AI applies AI-derived machine learning algorithms to proactively detect and respond to attack behaviors in these services to avert damage and theft. Detections are correlated to accounts and prioritized based on risk, giving security professionals a complete attack narrative to quickly stop and mitigate threats.

"Vectra AI gives all the necessary threat information to our SOC analysts," says the head of cybersecurity. "Vectra CDR for M365 is priceless."

The Results

The power to The power to detect and investigate

In the enterprise, the financial services company relies on Vectra NDR to identify and stop in-progress cyberattackers that can easily evade firewalls, IDPS and other perimeter security.

"Vectra NDR is absolutely essential," says the head of cybersecurity. "It extracts value out of the box in a short amount of time. Every critical alert that appears in the dashboard is worth investigating, and Vectra AI tells you exactly how to go about it."

He also likes the flexibility to deploy sensors anywhere they are needed in the network. "I can deploy as many sensors as I want to get rid of blind spots in traffic," he notes. "The entire platform is easy to use, fast and well-integrated."

Vectra AI makes investigations easy: Instant Investigation arms analysts of all skill-levels with lighted pathways that serve as a quick start guide to investigate detections, while Advanced Investigation enables analysts to query Entra ID, M365 or AWS Control Plane logs directly in the platform UI, streamlining threat investigations and hunting.

The metadata also includes host names, not just IP addresses. "We don't have to sift through DHCP logs to find a device IP address or identify IP address changes during an investigation," says the head of cybersecurity. "Searching for host names is much faster when you have little time."

For this financial services company, Vectra AI is an essential part of its SOC, enabling the organization to take a proactive approach to identifying and stopping potentially catastrophic cyberattackers.

"I can deploy as many sensors as I want to get rid of blind spots in traffic. The entire platform is easy to use, fast and well-integrated."

Head of security
Global financial services firm

Read more customer stories

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

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