

Securing AWS with Vectra AI



About

Navigating security in a cloud era

Cloud benefits are seemingly endless, however, when viewed through the lens of a security professional—the speed, scale and connectivity gained can also open the door for cyberattackers. These days securing the cloud requires a new way of thinking, which comes as no surprise to Mirza Baig, IT Security Manager at Municipal Property Assessment Corporation (MPAC), Ontario’s property expert that delivers property values, insights and services to taxpayers, municipalities, government and businesses.

Mirza and his small but mighty team operate as an Amazon Web Services (AWS) shop that is responsible for securing the organization’s information, data and domains from an operational, compliance, and risk management perspective. They prioritize visibility across their environment by utilizing different security controls to help keep tabs on any abnormalities.

Organization
Municipal Property Assessment Corporation

Industry
Professional Services

The Challenge
Lack of lateral movement visibility within organization

The Solution
An AI-based Network Detection and Response (NDR) solution to automate SOC inefficiencies and increase lateral movement visibility

The Results

- Detection of lateral movement within organization
- Full visibility into AWS Nitro-based instances
- Detection of abnormal activity within their AWS environment and infrastructure

Security Transformation

Platform value at a glance

Vectra AI's Impact	Outcome
Coverage	• Full visibility into AWS Nitro-based instances via VPC Traffic Mirroring • Detection of lateral movement across workloads
Clarity	• SOC informed of abnormal but non-malicious activity (e.g., developer updates) that could have security implications • AI-driven detection highlights attacker behaviors that bypass MFA or endpoint controls
Control	• Automated triage and prioritization of highest-risk threats • Faster investigations with streamlined workflows

Before achieving these outcomes, the MPAC team first had to contend with gaps in visibility across their environment.

The Challenge**No lateral movement allowed**

As an IT security veteran, but newer to MPAC, Mirza needed to get the lay of the land in terms of the security solutions the team was utilizing. He was pleased to find that the team had already prioritized removing any blind spots, which is key to having the ability to detect attacker behavior. One of the solutions the team had in place was Vectra AI, an AI-driven network detection and response solution that among other things, helps MPAC stop any lateral movement across cloud or enterprise workloads.

“The blind side that we had before Vectra AI was the lateral movement within the organization. We didn’t have good visibility,” said Mirza.

When it comes to identifying lateral movement, Vectra AI is able to find attackers who have bypassed preventative tools like multi-factor authentication (MFA) or endpoint solutions and spot their activity before an attack occurs.

Mirza added, “Now we are aware and have really good visibility.”

In addition to detecting lateral movement, Vectra AI allows MPAC’s SOC to augment their skills with artificial intelligence (AI) so they can automate the prioritization of threats based on risk and privilege, triage the highest-risk threats and investigate behavior-based threat signals. Mirza says they have other security controls along with Vectra AI, which makes things really challenging for any threats to get in, but the team really values the investigation features Vectra AI provides compared to other solutions.

“Vectra AI makes investigation easy. Vectra has an edge over their competitors when it comes to this,” he said.

The Solution**Small shop at heart, big cloud usage**

For a small shop, this team has made AWS a big part of their overall infrastructure strategy, and are not willing to sacrifice visibility across their environment—in AWS or otherwise as they continue to deploy cloud workloads down the road.

“We are an AWS shop,” says Mirza. “Using AWS VPC Traffic Mirroring, Vectra AI gives us full visibility into our Nitro-based instances.”

“Sometimes we have some abnormal activity within AWS or within our infrastructure and Vectra alerts on those activities,” says the IT Security Manager. Mirza explains that not all detections mean something malicious has happened, but his SOC team still needs to know about them. “Like when a developer makes an update or changes something that could have security implications. When this is the case, my team needs to know in case any security controls need to be adjusted.”

In addition to keeping the team informed, these are instances that would otherwise go undetected and could even include attacker behavior. With Vectra AI, Mirza and his team can detect more of what matters, expand their reach as a team with AI lending a hand and respond to any in-progress threats that occur.

“We are an AWS shop. Using AWS VPC Traffic Mirroring, Vectra AI gives us full visibility into our Nitro-based instances.”

MIRZA BAIG

IT Security Manager at Municipal Property Assessment Corporation (MPAC)

“The blind side that we had before Vectra AI was the lateral movement within the organization. We didn’t have good visibility”

MIRZA BAIG

IT Security Manager at Municipal Property Assessment Corporation (MPAC)

The Results**Cloud or on-prem, any place can be a happy place with visibility**

Certainly, new technology environments can create challenges, especially for security professionals busy sifting through alerts and constantly adjusting to any new or existing threats. The SOC team at MPAC is no different. By leveraging the right security solutions and controls, the team is visibly secure—and happy.

“We love Vectra AI! My entire team loves Vectra AI. I am not looking to move to any other NDR solution in the near future.”

“We love Vectra AI! My entire team loves Vectra AI. I am not looking to move to any other NDR solution in the near future.”

MIRZA BAIG
IT Security Manager at Municipal
Property Assessment Corporation
(MPAC)

Read more customer stories

About Vectra AI

Vectra AI is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Powered by patented Attack Signal Intelligence, it empowers security teams to rapidly prioritize, investigate and respond to the most advanced cyber-attacks. With 35 patents in AI-driven threat detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI to move at the speed and scale of hybrid attack. For more information, visit www.vectra.ai.

For more information please contact us: Email: info@vectra.ai | [vectra.ai](https://www.vectra.ai)

© 2025 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and the Vectra Threat Labs, Threat Certainty Index and Attack Signal Intelligence are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: 092325