VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Government Authority Achieves Complete Cloud Monitoring with Vectra AI and AWS

Executive Summary

"The country" is emerging as a leader in digital transformation. Located in the Middle East, this Government Authority manages and oversees all of the country's digital assets, information technology and data programs.

The Government Authority selected the Vectra Cognito platform to detect attacker behavior across the entire footprint, from datacenter to cloud, to protect its operations and manage compliance risks. The group is leveraging Amazon Web Services (AWS) to improve security operations efficiency by storing security metadata in its data lake to perform effective threat hunting and incident investigations.

A Government Running on Data

The Government Authority owns and maintains IT security for all of its critical systems, delivers statistics, processes payments and provides user authentication and authorization. It operates similarly to a service provider throughout all government agencies including healthcare, education, traffic and immigration.

Full integration with AWS Security Hub means that Vectra detections are published as findings in Security Hub, leading to faster incident investigations and remediation in the cloud.

Organization

Government Authority

Industry

Federal

Challenge

Needed to reduce the risk of a breach with advanced technologies that stay compliant, in order to avoid incurring regulatory fines or penalties.

Selection criteria

An AI-driven threat detection solution specifically built for AWS traffic

Results

- Full integration with AWS Security Hub
- Vectra detections are published as findings in Security Hub, enabling the correlation of Vectra attacker detections with other data sources
- Faster incident investigations and remediation in the cloud

Cybersecurity is a fundamental pillar protecting government institutions as they are a prime target for hackers. Securing network data requires advanced technologies to provide support and response services for government organizations that need to stay compliant in order to avoid incurring regulatory fines or penalties.

The Government Authority maintains and supports multiple core business functions at a large scale where compromised data or systems increase the risk of a breach. A breach in a government institution would impact critical systems that citizens rely on, demand remediation costs and require unplanned spending to close the gaps.

The security team needed to reduce the risk of a breach by having the ability to detect and respond to potential threats. However, they were overwhelmed with a large volume of unprioritized alerts, poor capability in detecting unknown threats and they lacked visibility into their cloud environment.

Continuing with limited visibility of the cloud and network would no longer support the Government Authority's digital transformation efforts, as they require the ability to detect and respond to any intrusions across the environment, protect sensitive information and improve the efficiency of security operations. To solve for this, they turned to Vectra AI and deployed the Cognito Platform for threat detection and response.

The deep integration into AWS allows the organization to deploy Vectra sensors and use AWS virtual private cloud (VPC) traffic mirroring to extend AI-driven detection and response to their additional AWS workloads.

AWS Provides Security to Sensitive Data

Due to the nature of government institutions, it's imperative to control dangerous cyber risks when moving high-value data and services to the cloud. The Government Authority required the full platform to be hosted in AWS given the sensitivity of applications and data.

As the industry's first threat detection and response solution in AWS, Vectra AI secures hybrid and multi-cloud deployments with 360-degree visibility that delivers a single view of hidden cyberattacks that move across cloud, data center and enterprise networks.

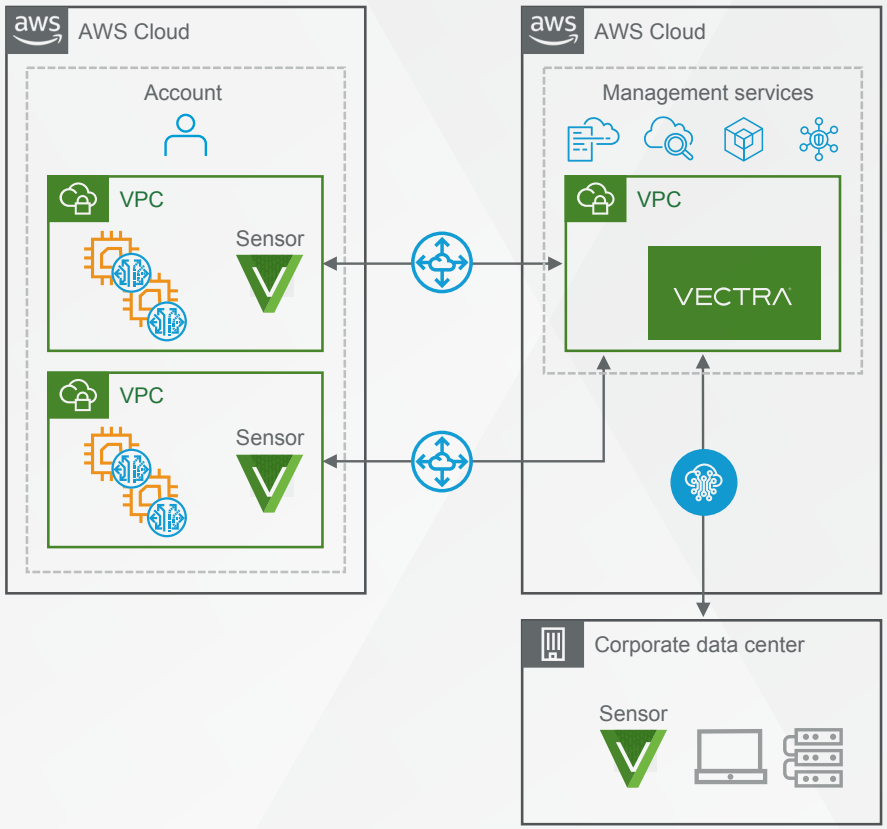
Extending digital transformation to the cloud

The Government Authority is taking a cloud-first approach, and security is no different. Vectra's AI-driven Cognito Platform delivers the most comprehensive insight across cloud including SaaS, IaaS, and PaaS, as well as data center and enterprise networks, uncovering hidden threats and empowering incident responders to act with confidence. The security-enriched data captures network metadata at scale, enriches it with machine learning security information and applies it across the platform, providing necessary details for effective threat hunting all stored in AWS.

The deep integration into AWS allows the organization to deploy Vectra sensors and use AWS virtual private cloud (VPC) traffic mirroring to extend AI-driven detection and response to their additional AWS workloads. Full integration with AWS Security Hub means that Vectra detections are also published as findings in Security Hub, enabling the correlation of Vectra attacker detections with other data sources for faster incident investigations and remediation in the cloud.

Beneficial Visibility

The Government Authority now has visibility across the entire network and can find active attacker techniques minimizing the high financial and liability risk caused by a breach. This insight has reduced the workload of the security operations team 40x and reduced the number of events to 2-3 per day with critical events reduced to 1-2 per day.



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

Email info@vectra.ai vectra.ai