VECTRA
SECURITY THAT THINKS.®

CASE STUDY

Online gaming company bets on Vectra and AWS for cyberattack detection and monitoring

Executive summary

The popularity of online gaming continues to explode, and this operator runs many of the most beloved sites and collections of brands in its sector. Located in North America, the company has operations in more than a dozen locations around the globe in order to serve its expanding worldwide customer base.

Due to its large audience, cybersecurity is paramount for the gaming community as cybercriminals view these sites as prime attack targets for their new wave of threats. That's why in order to detect stealthy, in-progress cyberattacks, the organization selected the Cognito® threat detection and response platform from Vectra® to detect complex, multistage attacks across cloud, data center, IoT, and enterprise networks.

Additionally, the online gaming firm leverages AWS to improve security operations by storing security-enriched metadata from all traffic in its data lake to dramatically improve threat hunting and incident investigations.

Deep integration between Cognito and AWS allows the company to deploy Vectra sensors in AWS virtual private clouds (VPCs).

Organization

Online Gaming

Industry

Software

Challenge

Limited visibility into threat behaviors inside its network.

Selection criteria

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

Results

- Integration between Cognito and AWS allows the company to deploy Vectra sensors in AWS virtual private clouds (VPCs)
- Increased visibility into network threat behaviors
- Cognito NDR definitions are published as findings in AWS Security Hub, where they can be correlated with other data sources for faster threat hunting and incident investigations in the cloud

Staying vigilant against threats

"The threat landscape is in rapid and constant flux," says the company's head of information security. Gaming companies are lucrative targets for cybercriminals, who range from solo actors to organized crime rings. An outage or data breach can cause material damage to the firm's income, customer retention and long-term value. As a publicly traded company, it is required to meet a wide range of regulatory and compliance mandates, including PCI-DSS and GDPR.

The gaming firm needs to be able to detect threats and attacks, which means having the ability to hunt for malicious activity around the clock without requiring security teams to be on site 24/7. At the same time, security analysts were overwhelmed by the volume of alerts from their security tools, such as SIEMs, firewalls and other defenses.

Before selecting Vectra's AI-driven platform, the company experienced limited visibility into threat behaviors inside its networks, which did not support the company's priorities to deliver the best experience for gamers, guard its operations against attacks, and protect its brands and intellectual property.

Cognito captures all network metadata at scale and enriches it with machine learning-derived security context, and reliably stores it in AWS for proactive threat hunting and conclusive incident investigations.

Satisfying the need for faster incident response

The security team knew that extending Vectra's AI-driven threat detection and hunting to AWS workloads would reduce the risk of security gaps and blind spots in dynamic cloud environments.

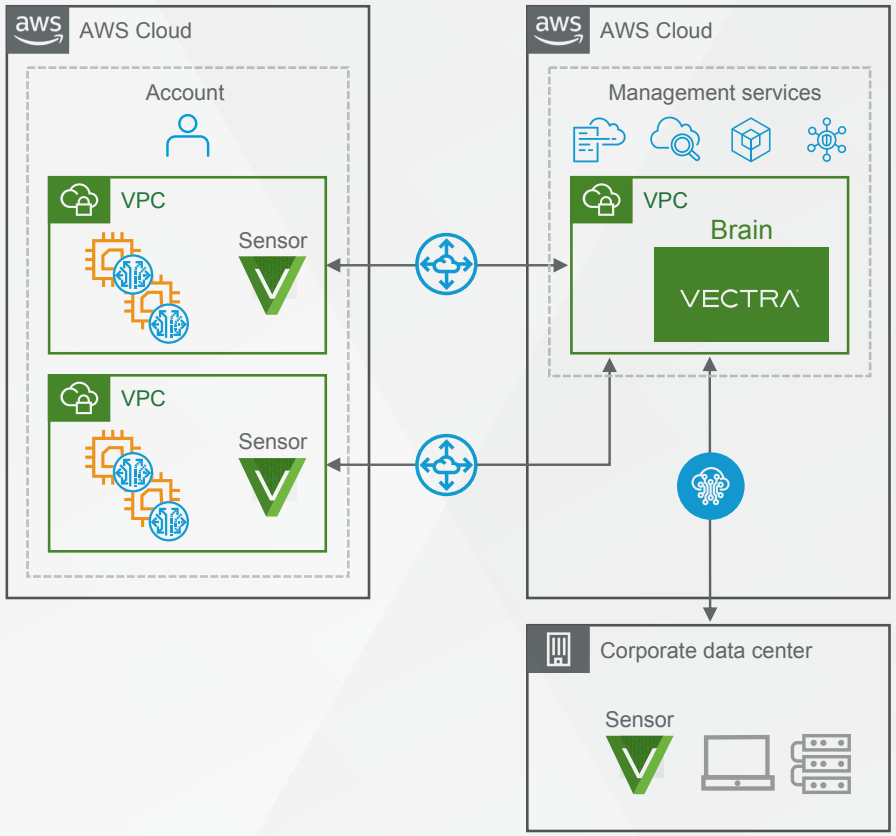
The Cognito platform from Vectra automatically identifies hidden cyberattacks and stops data breaches in hybrid and cloud deployments. With 360-degree visibility, the Cognito delivers a single view of all threat behaviors—across cloud, data center, IoT and enterprise networks, while providing invaluable security insights and context about attacks.

Extending digital transformation to the cloud

The company relies on AWS for flexible, scalable workloads and any disruptions could seriously damage the online gaming firm's reputation. Cognito automatically detects and responds to hidden cyberattack behaviors across the entire network. Cognito captures all network metadata at scale and enriches it with machine learning-derived security context, and reliably stores it in AWS for proactive threat hunting and conclusive incident investigations.

Deep integration between Cognito and AWS allows the company to deploy Vectra sensors in AWS virtual private clouds (VPCs), which use traffic mirroring to extend AI-driven cyberattacker detection and response to AWS workloads. Integration with AWS Security Hub ensures that Cognito definitions are published as findings in Security Hub, where they can be correlated with other data sources for faster threat hunting and incident investigations in the cloud.

Extending AI-driven detection and threat hunting to AWS workloads would reduce the risk of security gaps and blind spots in dynamic cloud environments.



For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai