VECTRA
SECURITY THAT THINKS.® | awsmarketplace

aws partner network
Advanced
Technology
Partner

SOLUTION BRIEF

Network threat detection and response for Amazon Web Services (AWS)

Secure AWS deployments across hybrid and Multi-Cloud architectures

As enterprises move their high-value data and services to the cloud, it's imperative to control cyber-risks that can take down businesses.

Vectra Detect for networks is the first solution that delivers intelligent threat detection and response on Amazon Web Services by focusing on the network traffic between workloads. By combining hosts, accounts, and privilege across the hybrid network, SOC teams can track and link attacks and the resources they use as they progress between cloud and on-premise.

The solution

Vectra Detect for Networks prevents data breaches in AWS by automatically detecting and prioritizing threats, accelerating investigations and enabling proactive threat hunting – leaving attackers with nowhere to hide.

Detect threats targeting IaaS workloads

- Integration with AWS virtual private cloud (VPC) traffic mirroring monitors and exposes attackers using infrastructure-as-a-service traffic

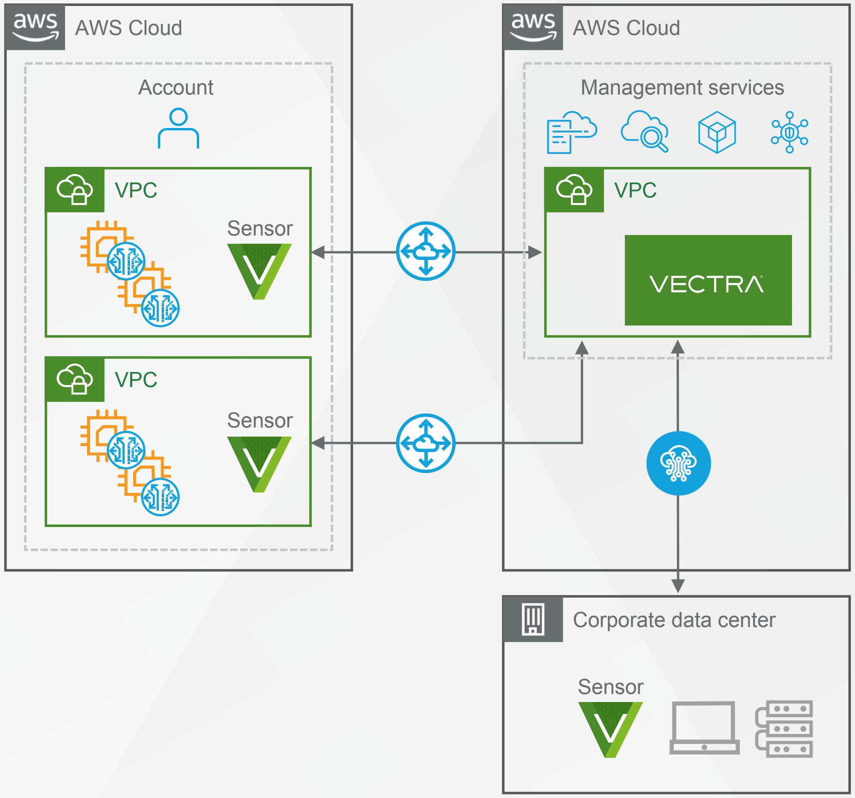
Investigate threats with security enriched data

- Context between cloud and ground for comprehensive investigation, or stream AWS activity into your data lake or SIEM as Zeek-formatted security-enriched network metadata

Respond with cloud native tools for targeted mitigation.

- Full integration with AWS Security Hub publishes Vectra definitions as findings in Security Hub, enabling you to correlate Vectra attacker detections with other data sources for faster threat hunting and incident investigations.

In addition to Network Detections, Vectra also provides agentless threat detection and response to attacks targeting applications running on AWS, as well as users, compute, and storage instances, including the AWS control plane itself with Vectra Detect for AWS.



The Vectra network threat detection and response platform secures AWS deployments across hybrid and multicloud architectures

AWS VPC Traffic Mirroring	The Vectra platform uses Amazon VPC Traffic Mirroring to monitor connections between Amazon EC2 and Amazon S3 instances and detect hidden threats without using agents.
Amazon CloudWatch	The performance and health of the Vectra platform can be fully monitored through Amazon CloudWatch, a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers.
AWS CloudFormation	Vectra is rapidly deployed using AWS CloudFormation, a tool that describes and provisions all the infrastructure resources in your cloud environment.
AWS Security Hub	Full integration with AWS Security Hub publishes Vectra detections as findings in Security Hub, enabling you to correlate Vectra attacker detections with other data sources for faster threat hunting and incident investigations.
Vectra Sensor	Vectra sensors are deployed across cloud, data center and enterprise networks, where they extract relevant metadata from traffic and ingest external threat intelligence as well as Active Directory and DHCP logs. The characteristics of every flow are recorded, including the ebb and flow, timing, traffic direction, and size of packets. Each flow is then attributed to a host and account rather than an IP address. The data is collected in the Vectra Cognito Platform, where scores of self-learning behavioral models that enrich the metadata from network traffic with machine learning-derived security insights and high-fidelity detections.

For more information or a free trial, read more at Vectra.ai/AWS or in the AWS Marketplace

Email info@vectra.ai vectra.ai

Version: **052621**