Datasheet

Blue Hexagon for AWS

AWS Threat Protection Harnessing the Power of Deep Learning

Security Retrofitted For Cloud Has Limitations

The migration to cloud is occurring rapidly. A recent study estimated that 83% of workloads will migrate to the cloud in 2020. In the same study, 66% of IT professionals surveyed said security was their biggest concern in adopting an enterprise cloud computing strategy.

The current security strategy for cloud has been trying to retrofit existing security solutions for the cloud, but this brings a number of limitations:

- Virtual versions of signature-based threat detection cannot keep up with threat variants. Additionally, it is almost impossible to run malware sandboxes in AWS because most popular offerings are cloud hosted themselves.
- Agent-based threat detection, where agents for threat detection solutions are installed on virtual machines, can be prohibitively expensive, deliver sub- optimal results, and isn't ideally for serverless architectures.
- Virtual versions of network traffic analytic solutions that identify anomalies have challenges in baselining what is normal due to the dynamic and short-lived nature of cloud workloads.

Blue Hexagon for AWS delivers threat protection powered by deep learning to detect threats accurately and at cloud speed, without requiring any agent deployment or architecture changes

What is needed is a threat detection solution that can seamlessly integrate into the network fabric of AWS and deliver a high efficacy threat detection solution. This is what Blue Hexagon for AWS delivers.

AWS Threat Protection Powered by Deep Learning

Blue Hexagon for AWS showcases an integration with Amazon Virtual Private Cloud (VPC) traffic mirroring feature. The Amazon Virtual Private Cloud (Amazon VPC) traffic mirroring replicates VPC traffic captured at the Elastic Network Interface (ENI) level along with full payload data for inspection by Blue Hexagon. Amazon VPC traffic mirroring can be enabled for **specific subnets, entire VPCs,** or for **select traffic** such as those traversing Internet Gateways or Virtual Gateways.

The Blue Hexagon unique deep learning approach is ideally suited to inspect this traffic because of the speed and accuracy of threat detection that keeps up with the speed of cloud. More importantly, agents do not need to be deployed on any virtual instance, enabling Blue Hexagon for AWS to be deployed in new and existing networks without any changes or IP reconfiguration.

AWS Threat Protection Powered By Real-time Deep Learning

Detect threats in less than a second

Detect known and unknown threats, even zero days seen for the first time, in less than a second

Seamlessly deploy without agents

Via integration with Amazon VPC traffic mirroring, any VPC traffic can be inspected

Proven efficacy in real-world deployments

Unmatched detection rates and low false positives compared to legacy solutions retrofitted for cloud

Orchestrate prevention to AWS Services

Enable notifications and invoke native AWS controls to quarantine or terminate compromised workload

[1]*LogicMonitor's Cloud Vision 2020: The Future of the Cloud Study*

Blue Hexagon for AWS

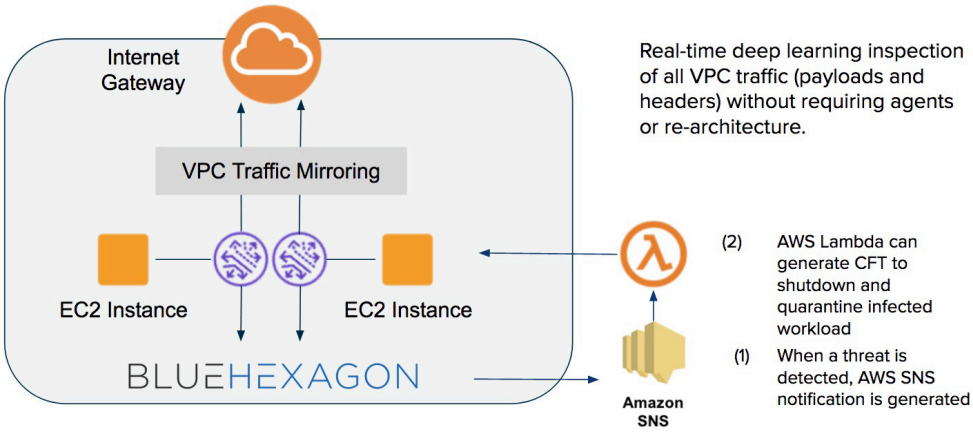

Figure 1: Blue Hexagon for AWS and Integration with Amazon VPC traffic mirroring

As shown in Figure 1, the Blue Hexagon Deep Learning-powered Threat Protection for AWS inspects a copy of the AWS VPC traffic, including payloads and headers, for threats. The Blue Hexagon platform can detect known and unknown threats including zero days **in less than a second, at almost 100% detection rates**. When a threat is detected, Blue Hexagon can generate a notification into AWS Simple Notification Service (SNS) which can be consumed and orchestrated by any downstream services like AWS GuardDuty or an AWS Lambda. These services can invoke a AWS Cloud Formation Template (CFT) to shut down or quarantine the impacted workload, ensuring complete security for business-critical applications.

Features:

High-Efficacy Threat Verdict - VPC traffic payloads and headers provide rich data for Blue Hexagon deep learning models to detect threats with very high efficacy. In addition, every threat detected is automatically classified by the HexNet™ neural networks in real-time. Threat family information and indicators of compromise are provided for deeper analysis.

Real-time Threat Verdicts - Blue Hexagon can rapidly uncover malicious threats moments after they appear within a workload without requiring any baselining or a priori knowledge of the traffic. This is ideal to address the ephemeral quality of cloud workloads.

Orchestrated Prevention - When a threat is detected, Blue Hexagon can generate a notification into the appropriate AWS SNS and invoke AWS Lambda to quarantine the infected workload, ensuring complete security for business-critical applications. Notifications can also be sent to SIEM integrations.

Auto-Scaling - The solution can support auto-scaling and can be deployed with a Network Load Balancer to meet any cloud scale needs.

Seamless Deployment - Unlike inline next-generation firewalls which require network changes when deployed in an existing network, Blue Hexagon for AWS can be easily deployed in new and existing networks without any changes or IP re-configuration.

Cloud Privacy - Blue Hexagon for AWS along with the Amazon VPC Traffic Mirroring is deployed in the customers' VPC. Inspection is performed in real-time in the VPC, not in a separate vendor cloud, ensuring privacy requirements are met.

One Dashboard - Security teams manage their on-premises and AWS deployments with the same dashboard. The Blue Hexagon dashboard provides comprehensive details on threats detected, including kill chain visibility and indicators of compromise.

Global Threat Cloud - Blue Hexagon incorporates deep learning to classify threats from various intelligence sources. This data is shared with all customers to deliver predictive intelligence into the types of attacks that are targeting specific industries.

Blue Hexagon Labs - Every customer deployment benefits from the elite deep learning and cybersecurity experts within Blue Hexagon, including in-depth analysis of major attacks.

Blue Hexagon is a deep learning innovator focused on protecting organizations from cyberthreats. The company's real-time deep learning platform is proven to detect known and unknown network threats with speed, efficacy, and coverage that set a new standard for cyber defense. Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. For more information, visit www.bluehexagon.ai or follow @bluehexagonai.

Headquarters
298 S. Sunnyvale Avenue, Suite 205
Sunnyvale, CA 94086
www.bluehexagon.ai
inquiries@bluehexagon.ai

BLUEHEXAGON