ExtraHop

Reveal(x) AMI for AWS

Cloud-Native Security for Hybrid Enterprises, powered by Amazon VPC Traffic Mirroring

Threat Detection, Investigation and Response

Security teams have the difficult task of keeping up with the speed of cloud while ensuring data, applications, and workloads are secure. In order to stay ahead, SecOps needs visibility and control across the hybrid enterprise, including AWS cloud environments. For SecOps, it's all about managing risk and enabling the rest of the organization to move at the speed needed to transform and scale the business. ExtraHop provides visibility and investigation to Virtual Private Cloud (VPC) environments, allowing SecOps to confidently secure their AWS cloud environment from the inside out.

ExtraHop brings threat detection, investigation, and response to AWS workloads, allowing SecOps to track rogue instances and eliminate risks created by misconfigurations, insecure APIs, and unauthorized access.

USE CASES

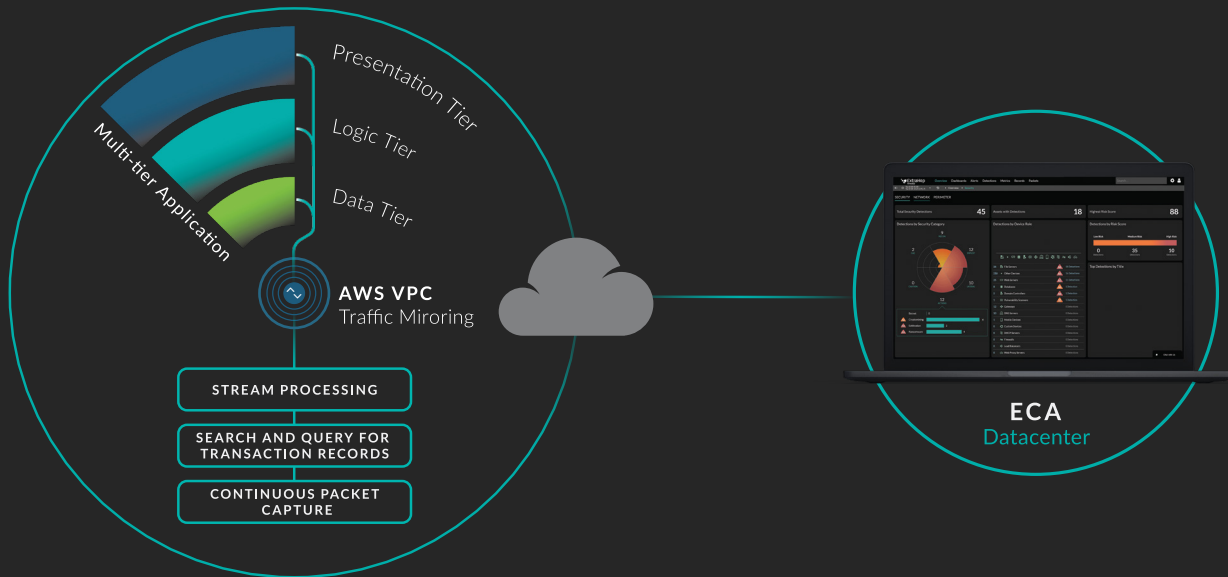| Data Security | Access Control | Inventory & Config |
| Dependency Mapping | Compliance & Audit | Vulnerability Assessment |
| Threat Detection | Investigation | Threat Hunting |

Interested in a cloud-native security solution?

LEARN MORE extrahop.com/cloud

HOW IT WORKS

Multi-tier Application
Presentation Tier
Logic Tier
Data Tier

AWS VPC
Traffic Miroring

STREAM PROCESSING

SEARCH AND QUERY FOR
TRANSACTION RECORDS

CONTINUOUS PACKET
CAPTURE

ECA
Datacenter

As enterprises migrate more business-critical applications to the cloud to take advantage of greater scale and efficiency, the pressure is placed on SOC teams to move security with them. ExtraHop powered by Amazon VPC Traffic Mirroring, gives SecOps the power to analyze every transaction in the cloud, detect threats, and quickly respond to attacks.

Amazon VPC Traffic Mirroring is a new feature from AWS that allows customers to gain insight into the network traffic across their VPC infrastructure for content inspection and threat monitoring. With this feature, customers can copy network traffic from Elastic Network Interfaces (ENI) of their Elastic Compute Cloud (EC2) instances in their VPCs, and send it to ExtraHop with no loss of throughput or fidelity.

By combining automated discovery and asset classification with full payload analysis and machine learning for high-fidelity threat detection, ExtraHop gives cloud-focused SecOps teams the power to proactively monitor and respond to threats.

Interested in a cloud-native security solution?
Learn more about our SaaS product, Reveal(x) Cloud: www.extrahop.com/cloud

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyzes all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

info@extrahop.com
www.extrahop.com