ExtraHop

Cloud Threat Defense

Defend Your Cloud Without Friction

aws PARTNER Security Software Competency

Cloud security teams are outnumbered and under siege. As developers deploy assets at a breakneck pace and adversaries continue to evolve their attacks on mission-critical applications and workloads, the status quo of prevent and protect can't keep up with the current realities of advanced threats.

Reveal(x) 360 Cloud Threat Defense for AWS is purpose-built to stop advanced threats like ransomware, software supply chain attacks, and more. With real-time analysis of all sources of network telemetry, Reveal(x) 360 detects malicious activity across workloads without introducing friction.

What is Cloud Threat Defense?

Continuous Visibility

Cloud threat defense starts with visibility across your hybrid enterprise. It lights up dark space to detect adversaries and advanced threats after they've slipped past perimeter defenses.

Real-time Data Visualization

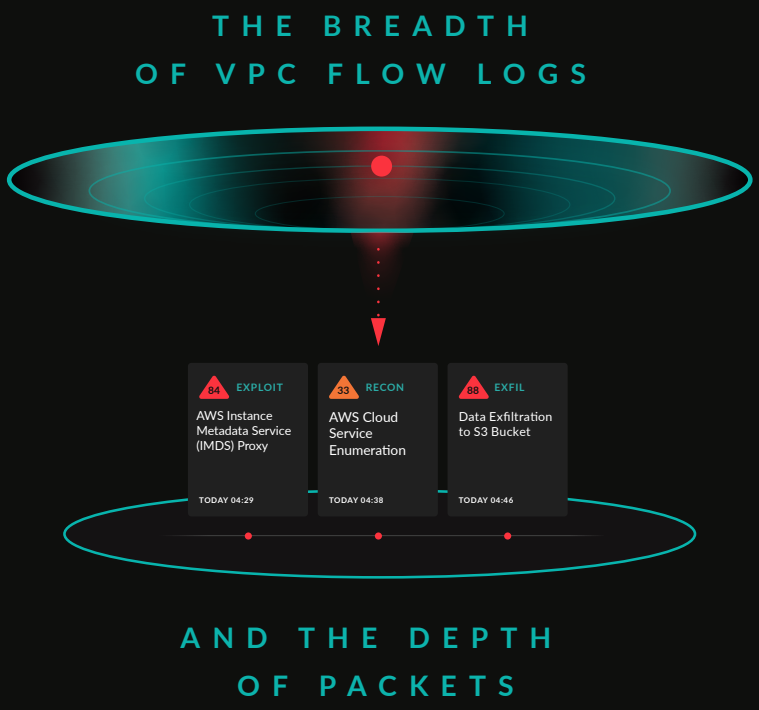
Cloud threat defense provides the depth and breadth of network telemetry needed to visualize, investigate, and respond to hotspots of malicious activity in a single management pane.

Advanced AI analysis

Cloud threat defense empowers you to stop attacks before they become breaches. It provides AI analysis that evolves with threats, powering proactive threat hunting and network forensics.

Additional Managed Security Service

Accelerate threat defense capabilities and shorten dwell times with proactive threat hunting, detection response, incident investigation, and cloud security assessments.



Reveal(x) 360 combines the simplicity of VPC Flow Logs with the power of packets, providing security teams with the breadth of coverage and depth of network telemetry they need to make fast, informed decisions when advanced threats arise.

Security teams can use VPC Flow Logs for broad coverage and packets for deep forensic investigation. ExtraHop analyzes both layers of network telemetry with cloud-scale AI to create accurate behavioral detections and high-fidelity alerts. Augmented investigation workflows help analysts quickly get to ground truth, slashing dwell time.

With cloud threat detection and network forensics from Reveal(x) 360, security teams can mitigate the blast radius of advanced threats like ransomware, supply chain attacks, and more.

Reveal(x) 360 for AWS Subscriptions

Reveal(x) 360 offers several subscription layers for cloud threat defense in AWS. All leverage ExtraHop's advanced AI analysis and cloud-hosted services.

Reveal(x) 360
STANDARD FOR AWS

Complete & Continuous Visiblity

Extend the power of Reveal(x) 360 in AWS by leveraging the breadth and simplicity of VPC Flow Logs

Reveal(x) 360
PREMIUM FOR AWS

Advanced Threat Detection

Addition of packets provide the depth of network telemetry needed for extended visibility, expanded threat detection and investigation.

Reveal(x) 360
ULTRA FOR AWS

Packet-level Forensics

Continuous packet capture allows for extended lookback and deep forensic investigations accessible immediately.

You can use the new Reveal(x) 360 Standard subscription as a standalone option for AWS security or combine it with Premium or Ultra packages for multi-layered cloud threat defense. For pricing, visit our AWS Marketplace listing.

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, uses cloud-scale AI to help enterprises detect and respond to advanced threats––before they compromise your business. With complete visibility from ExtraHop, enterprises can detect intrusions, hunt threats, and investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised.

ExtraHop

info@extrahop.com
www.extrahop.com