EXTRAHOP | aws

Network Ground Truth Context for AWS

ExtraHop RevealX™ decrypts AWS traffic to expose attackers moving between workloads



SOLUTION BRIEF

Cloud Logs Record API Calls. The Network Records Conversations.

AWS gives teams speed and elastic scale. Attackers use the same speed. In one AI-assisted breach reported by Dark Reading in February 2026, an intruder went from initial access to administrator in about eight minutes. CloudTrail and VPC Flow Logs record which API was called and who connected to whom. CloudTrail and flow logs omit the contents of encrypted east-west sessions. Short-lived instances and pods vanish before an agent can be installed.

Attackers who get in disable endpoint agents and alter logs to erase the trail. Mandiant's M-Trends 2026 found that the median hand-off from initial access to a secondary threat group fell to 22 seconds in 2025. Analysts and their AI agents need evidence the attacker can't edit.

The Network Is the Ground Truth.

Every attack crosses the network. ExtraHop RevealX Network Detection and Response (NDR) runs agentless and out of band, leaving an attacker on the host with no sensor to switch off. RevealX decrypts TLS 1.3 traffic, including sessions protected by perfect forward secrecy. RevealX reconstructs full L2–L7 transactions across more than 90 protocols at line rate.

More than 450 machine learning and behavioral detectors, mapped to more than 150 MITRE ATT&CK® techniques, surface lateral movement, credential abuse, command-and-control, and living-off-the-land activity as it happens. Every detection carries the records and packets behind it. Automated Retrospective Detection rechecks stored traffic when a new indicator emerges.

ExtraHop Sees the Traffic. AWS Delivers It.

RevealX takes traffic from native AWS mirroring, Gateway Load Balancer endpoints, and VPC Flow Logs. RevealX correlates the traffic once, upstream, into decision-grade intelligence for analysts, SIEM, and SOAR tools and AI agents. RevealX runs outside your workloads and outside the data path.

WHY AWS ENVIRONMENTS NEED NETWORK DATA

Logs record API calls and connections, and encrypted session contents go unseen

Instances, containers, and pods appear and disappear faster than agents can follow

Mirrored traffic still crosses the wire after attackers disable agents and wipe logs

WHAT YOU GAIN

Agentless, out-of-band visibility across VPCs, accounts, and Kubernetes

Decrypted east-west evidence for lateral movement and credential abuse

NDR, NPM, and IDS from one sensor, with records and packets behind every detection

The Best NDR for AWS Customers

RevealX connects to AWS through the network services you already run. Coverage follows your workloads as they scale.

Native VPC Traffic Mirroring

Virtual sensors deploy from Amazon Machine Images and read mirrored VPC traffic. One sensor runs network detection and response, network performance monitoring, and intrusion detection together. Each sensor supports up to 500 mirror sessions.

Ultra Sensors With Packet Forensics

RevealX Ultra cloud sensors pair a sensor with a packetstore for continuous packet capture. A CloudFormation template deploys each Ultra sensor with an elastic network interface or a Network Load Balancer as the mirror target.[1]

Gateway Load Balancer at Scale

A Gateway Load Balancer endpoint can serve as the mirror target, including across AWS accounts. RevealX also analyzes Geneve-encapsulated traffic mirrored from inspection and firewall appliances.

VPC Flow Logs for Unmirrored VPCs

A RevealX flow sensor ingests VPC Flow Logs from Amazon S3 or Amazon Kinesis Data Firehose. Optional Amazon Route 53 Resolver query logs and cross-account roles add DNS and account context. Flow logs extend coverage to VPCs without packet mirroring.[2]

Coverage That Follows Your Workloads

A CloudFormation template uses Amazon EventBridge and AWS Lambda to create and remove mirror sessions for the instances you tag. New workloads gain coverage the moment they launch.[2]

Kubernetes, Down to the Pod

The RevealX Kubernetes integration installs with a Helm chart and mirrors pod-to-pod traffic, including pods on the same node. The integration adds pod, namespace, and label context. Optional TLS session key forwarding enables decryption on containerd clusters.

Expose Lateral Movement Across VPCs

Line-rate decryption of TLS 1.3, Kerberos, NTLM, and LDAP lets RevealX read the traffic between instances, accounts, and VPCs. RevealX catches credential abuse, remote execution, and command-and-control that look normal in flow logs.

Context Your AI Agents Can Act On

RevealX reaches SOC agents through a REST API, an MCP server, and a CLI, published at github.com/extrahop. RevealX joins entities, resolves identity, and precomputes risk and MITRE mapping before an agent asks. Each agent receives a conclusion with the evidence attached.

1. RevealX Ultra cloud sensors, recordstores, packetstores, and consoles deployed in AWS require RevealX Enterprise.
2. VPC Flow Logs ingestion and automated mirror-session creation are available with RevealX 360.

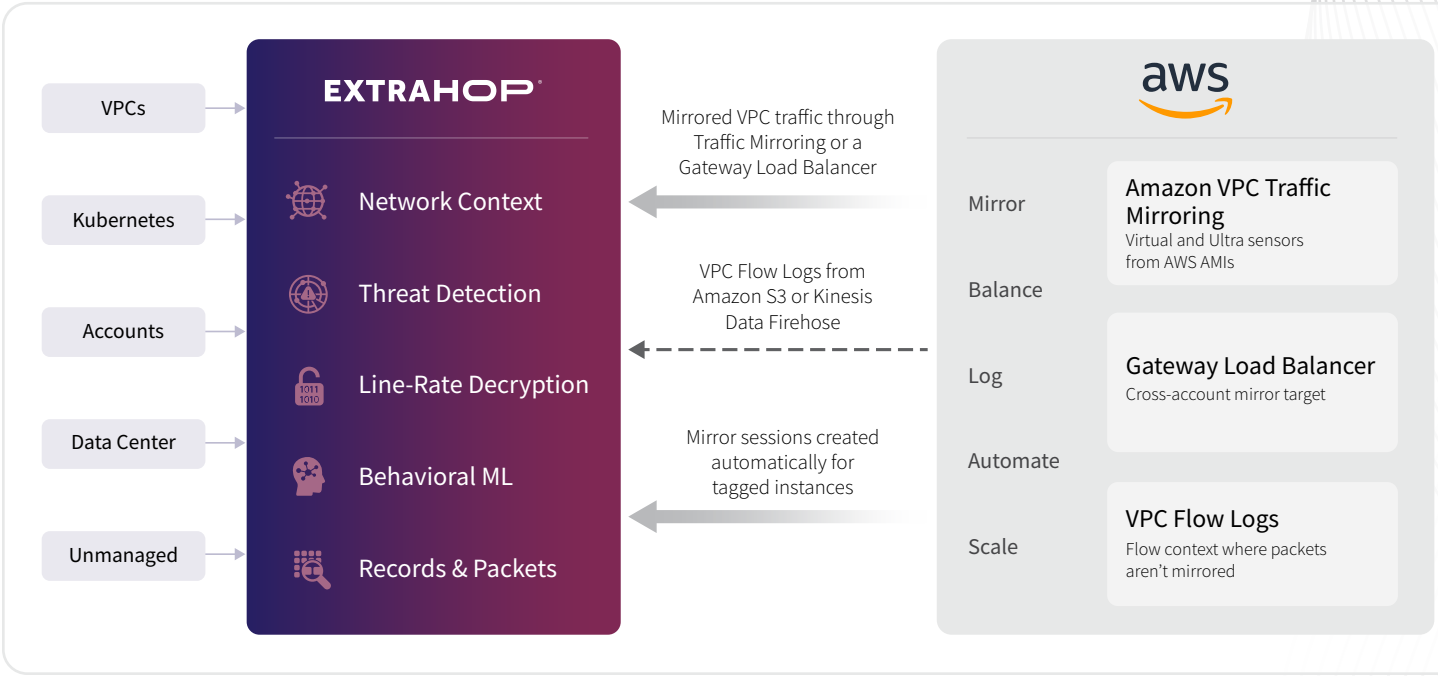


Figure 1: Mirrored packets, Gateway Load Balancer traffic, and flow logs feed one out-of-band platform outside your workloads.

Without the Integration	With ExtraHop + AWS
Logs record API calls and connections, and encrypted session contents go unseen	RevealX decrypts and reconstructs east-west transactions from mirrored VPC traffic
Short-lived instances and pods disappear before an agent is installed	Automated mirroring and the Kubernetes integration cover workloads the moment they launch
An attacker who disables an agent or wipes logs erases the trail	Out-of-band sensors keep recording, with records and packets behind every detection
Separate tools for security, performance, and intrusion detection	NDR, NPM, and IDS run on one sensor from the same wire data
Analysts and AI agents reason over raw logs	Pre-correlated, decision-grade detections through the REST API, MCP server, and CLI

ABOUT EXTRAHOP

ExtraHop is a leader in real-time network intelligence, giving organizations the high-fidelity context to power security and IT AI automation, detect risks faster, and respond with confidence. AI agents rely on ExtraHop's real-time, ground-truth data to operate reliably in the SOC and NOC. For security teams, that means surfacing threats and definitive evidence to investigate them at machine speed. For IT operations, it means resolving performance issues in seconds. Engineered for unmatched scale, the ExtraHop RevealX platform delivers a unified view of the network across data centers, campus, branch, cloud, and AI environments. To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP

info@extrahop.com
extrahop.com

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1236A 11.02.26