EXTRAHOP | Google Cloud

See Threats in Context Across Google Cloud

ExtraHop RevealX™ exposes encrypted Google Cloud attacks and alerts Google Security Operations



SOLUTION BRIEF

Cloud Logs Record API Calls. The Network Records Conversations.

Google Cloud gives teams speed and elastic scale. Attackers use the same speed. Google's Cloud Threat Horizons report for H1 2026 puts software vulnerabilities behind 44.5% of cloud intrusions. Intruders move between Compute Engine instances, Kubernetes pods, and data stores. Cloud logs record which API was called and omit the contents of encrypted east-west sessions. Short-lived workloads vanish before an agent can be installed.

Attackers who get in disable 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. Google Cloud Delivers It.

RevealX takes a copy of VPC traffic from Google Cloud Packet Mirroring and correlates the traffic once, upstream. Decision-grade detections go to Google Security Operations, with records and packets behind every detection. RevealX runs outside your workloads and outside the data path.

WHY GOOGLE CLOUD NEEDS NETWORK DATA

Logs record API calls, and encrypted session contents go unseen

Short-lived instances and pods outrun agent deployment

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

WHAT YOU GAIN

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

Risk-scored detections in Google Security Operations

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

The Best NDR for Google Cloud Customers

RevealX connects to Google Cloud through the network and security services you already run. Coverage follows your workloads as they scale.

Native Packet Mirroring

Virtual sensors run on Compute Engine and receive a copy of VPC traffic through an internal passthrough Network Load Balancer enabled for Packet Mirroring. One sensor runs network detection and response, network performance monitoring, and intrusion detection together. The original traffic flows on untouched.

Packet Forensics in the Cloud

Larger sensors add continuous packet capture for forensics. The EDA 8370v handles up to 20 Gbps with a Hyperdisk Throughput packetstore. RevealX Ultra sensors pair a sensor and packetstore at 1 or 10 Gbps.

Out-of-Band Mirroring at Scale

Broker mode uses Google Cloud out-of-band mirroring with mirroring endpoint groups and Geneve metadata. Broker mode delivers one workload stream to multiple destinations, including peered workload and capture VPCs. Large and multi-project environments scale without extra mirroring policies.

Detections in Google Security Operations

Detection notification rules send risk-scored, MITRE-mapped RevealX detections to a Google Security Operations webhook feed. A ready-made dashboard and alert rules by risk score come with the integration. See the companion Google Security Operations brief.*

Kubernetes, Down to the Pod

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

See Every Workload, Managed or Unmanaged

RevealX discovers and classifies every instance, pod, and service that communicates on mirrored VPC traffic. Short-lived and unregistered workloads are inventoried and assessed as soon as they communicate.

Expose Lateral Movement Across Projects and VPCs

Line-rate decryption of TLS 1.3, Kerberos, NTLM, and LDAP lets RevealX read the traffic between instances, pods, and data stores. RevealX catches credential abuse, remote execution, and command-and-control that cloud logs never record.

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.

*Google Security Operations SIEM integration: RevealX 360 and RevealX Enterprise, firmware 9.8.6 or later.

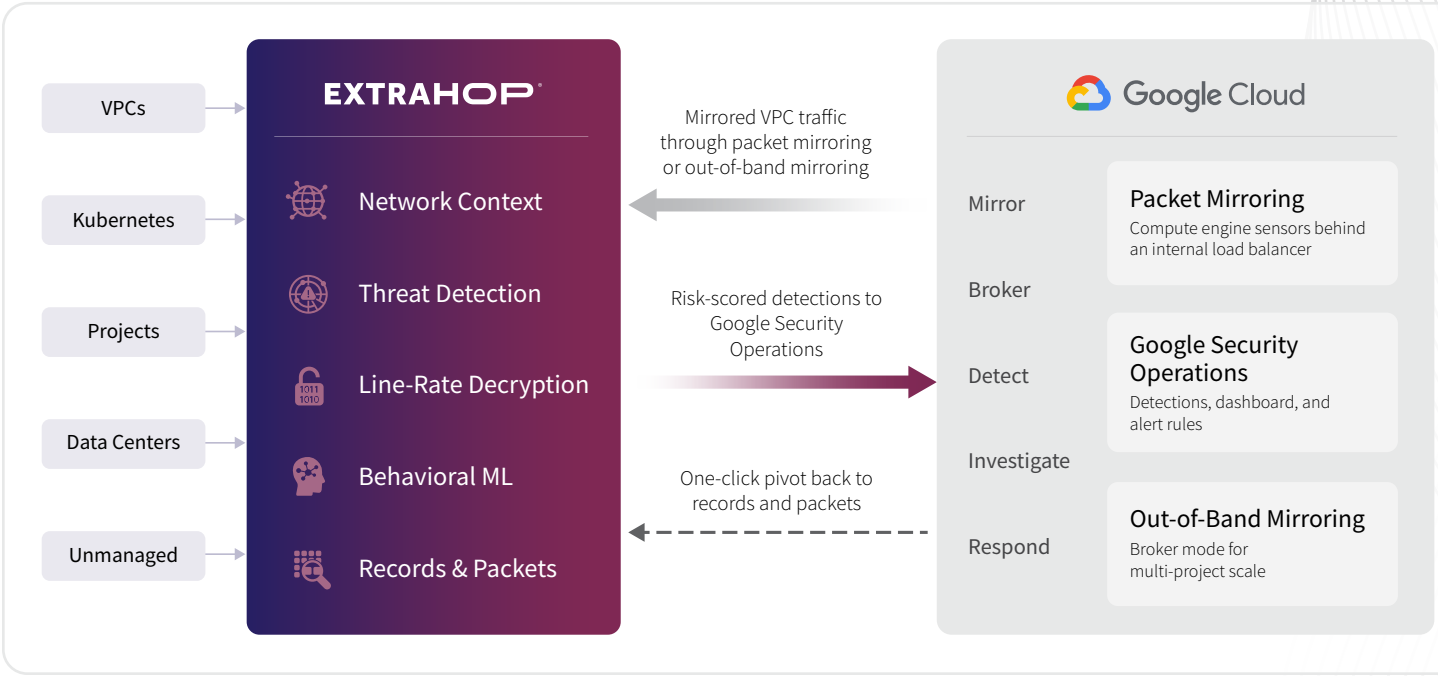


Figure 1: Mirrored packets in, decision-grade detections out to Google Security Operations, with record and packet-level evidence behind every detection.

Without the Integration	With Extrahop + Google Cloud
Logs record API calls, and encrypted session contents go unseen	RevealX decrypts and reconstructs east-west transactions from mirrored VPC traffic
Pods and short-lived instances vanish before an agent is installed	The Kubernetes integration and Packet Mirroring cover workloads as they run
An attacker who disables an agent or alters logs erases the trail	Out-of-band sensors keep recording, with records and packets behind every detection
Network findings live outside the SOC's primary console	Risk-scored detections land in Google Security Operations
Separate tools for security, performance, and intrusion detection	NDR, NPM, and IDS run on one sensor from the same wire data

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. 1237A 11.02.26