EXTRAHOP | Google Security Operations

Decision-Grade Context for Google Security Operations

ExtraHop RevealX™ sends Google Security Operations risk-scored detections linked to packet-level evidence



Logs Record Events. The Network Records Evidence.

Google Security Operations gives the SOC one place to search, detect, and respond across the enterprise. Logs record observations, and analysts still have to reach the verdict. Logs arrive late, get tampered with, or never exist for unmanaged devices and encrypted east-west traffic. Mandiant's M-Trends 2026 documented the BRICKSTORM backdoor reaching dwell times of nearly 400 days, far beyond a typical 90-day log retention window.

Analysts and their AI agents need trusted conclusions and defensible evidence. Recorrelating raw network data on every search adds cost and delay.

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 Correlates Once. Google Security Operations Acts Everywhere.

RevealX correlates upstream, joining entities, resolving identity, and scoring risk before a detection leaves the platform. Google Security Operations receives a compact, high-fidelity detection. Google Security Operations then applies its own search, detection, and response across the rest of your security data.

WHY GOOGLE SECURITY OPERATIONS NEEDS NETWORK DATA

Logs miss unmanaged devices and encrypted east-west traffic

Attackers wipe logs and outlast short retention windows

Raw network telemetry adds ingest without adding verdicts

WHAT YOU GAIN

Risk-scored, MITRE-mapped RevealX detections in your SecOps instance

A ready-made ExtraHop RevealX dashboard and alert rules by risk

One click from any alert to the records and packets behind it

The Best NDR for Google Security Operations Customers

The Google Security Operations SIEM integration sends RevealX detections to a Google Security Operations webhook feed, from RevealX 360 or RevealX Enterprise.*

Network Detections in Your SecOps Instance

Detection notification rules send detections to a Google Security Operations HTTPS webhook feed. Rules send directly or through a connected ExtraHop sensor acting as a proxy.

Send What Matters and Filter the Rest

Filters choose which detections reach Google Security Operations: recommendation for triage, minimum risk score, detection type or category, MITRE technique, offender, victim, device role, participant, or site. Teams use the default payload or define a custom JSON payload.

Detections With Context Attached

Each detection arrives with its title, description, risk score, categories, MITRE techniques, and RevealX triage recommendation. Each detection also lists the hostname, IP address, MAC address, role, and username of every offender and victim.

Alerts Prioritized by Risk

Three alert rules raise Google Security Operations alerts from RevealX detections by risk score: Low (1–30), Medium (31–79), and High (80–99). The highest-risk network findings reach analysts first.

ExtraHop RevealX Dashboard

A ready-made dashboard, available from the ExtraHop repository on GitHub, shows recommended and total detection events, maximum risk score, top MITRE techniques, source and destination maps, and recent detections.

One Click From Alert to Evidence

Every detection carries a link back to RevealX. Analysts move from the detection to the transaction records and then to the packets. Google Security Operations holds the alert, and RevealX holds the proof.

Network Context Beside Every Other Signal

RevealX detections land in your Google Security Operations instance next to endpoint, identity, and cloud telemetry. Analysts search and act on network findings with the workflows they already use.

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.

* Requires ExtraHop firmware 9.8.6 or later. Available for RevealX 360 and RevealX Enterprise.

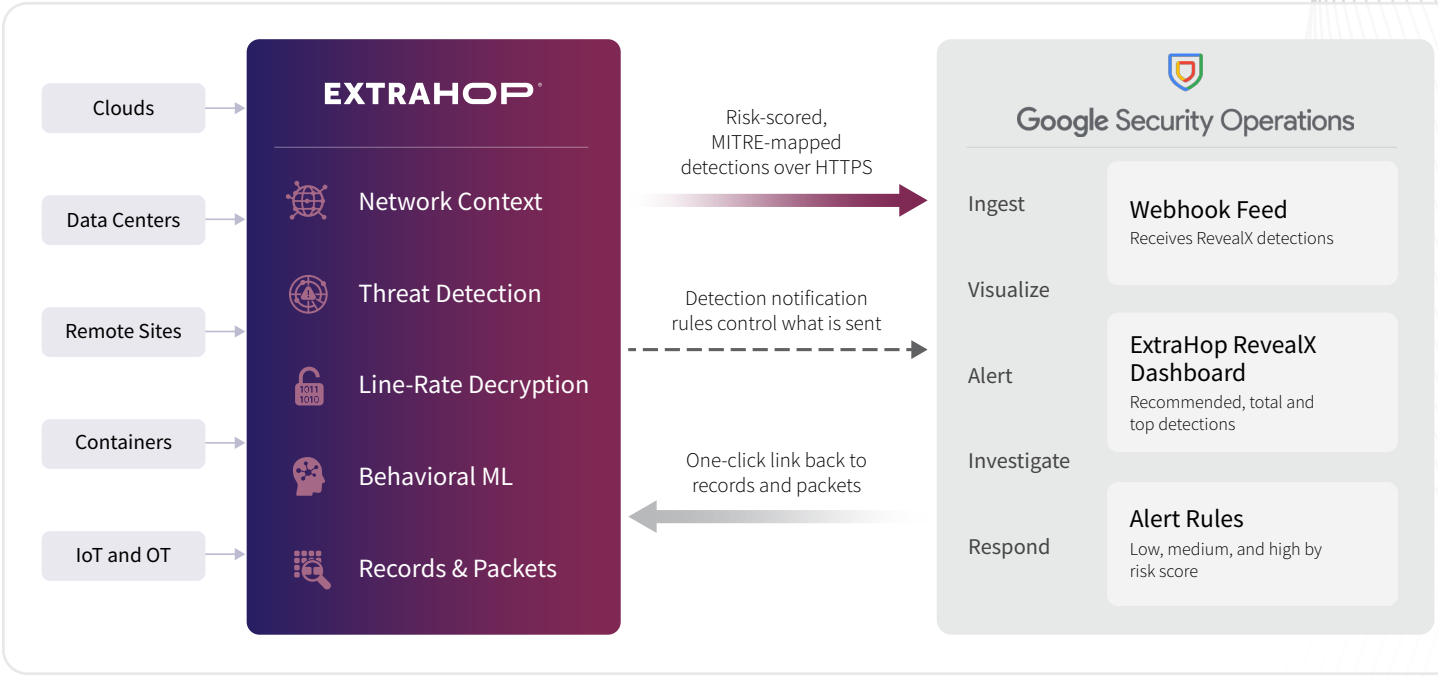


Figure 1: RevealX correlates once, upstream. Google Security Operations receives decision-grade detections linked to the evidence.

Without the Integration	With ExtraHop + Google Security Operations
Encrypted east-west traffic and unmanaged devices never appear in logs	RevealX decrypts east-west traffic and sends its findings to Google Security Operations
Raw network telemetry adds ingest and still needs correlation	Compact, pre-correlated, risk-scored detections keep ingest lean
Network alerts arrive without priority	Alert rules map RevealX risk scores to low, medium, and high
Alerts lack the evidence to confirm scope	One click from any alert to the records and packets behind it
Logs age out before a long-dwell intrusion is found	Automated Retrospective Detection rechecks stored traffic for new indicators

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. 1234A 10.30.26