

Network Ground Truth for the Agentic SOC

Ensure accurate investigation and resolve threats faster with Prophet Security and ExtraHop

SOLUTION BRIEF

AI Agents Need the Right Context for Reliable Investigations

AI-enabled adversaries can now find a weakness, exploit it, and move laterally in seconds. Meanwhile, the typical enterprise SOC fields close to 1,000 alerts a day and leaves 28% of them uninvestigated.¹ AI SOC analysts help close that gap by investigating each alert, correlating signals across multiple tools, and prioritizing the most critical threats.

Endpoint, identity, and cloud security tools offer valuable visibility, but share major blind spots: unmanaged assets, tampered host logs, and encrypted traffic. This means activity such as lateral movement to an unmanaged server, hijacked encrypted sessions, or data exfiltration over trusted protocols goes undetected. Without high-fidelity network evidence, investigations stall as inconclusive or close on a confident, yet uninformed answer built from incomplete data.

ExtraHop Provides the Context. Prophet AI Delivers the Verdict.

Prophet Security is an agentic AI SOC platform that spans autonomous alert investigation and response, continuous threat hunting, and closed-loop detection engineering. Prophet AI correlates data across your security tools and investigates every detection.

Through a native integration, Prophet AI uses ExtraHop both as a source of network detections to investigate and as a source of network evidence to corroborate or refute any investigation, regardless of the security tool that originally raised the alert.

ExtraHop turns network traffic into structured, investigation-ready context, including a live inventory of every device communicating across a hybrid environment. This includes context your EDR likely missed: behavioral baselines, who-talked-to-whom connection history, and high-fidelity detections for lateral movement. ExtraHop detects command-and-control (C2) beaconing, living-off-the-land (LotL) techniques, ransomware, and data exfiltration. Because that context arrives already enriched and correlated, AI agents reason over defensible answers instead of raw data, keeping investigations fast, accurate, and token-efficient.

WHY AI SOC ANALYSTS NEED NETWORK CONTEXT

Post-Compromise Visibility:

EDR, identity, and cloud tools rarely show lateral movement, protocol abuse, or the full picture of network activity after initial compromise.

Coverage for Unmanaged Assets:

IoT, OT, contractor, and other unmanaged devices sit outside endpoint coverage, so attacker activity through them goes undetected.

Defensible AI Outcomes:

Network evidence helps AI agents reach definitive verdicts instead of wasting tokens or sending work back to analysts.

WHAT YOU GAIN

Complete Attack Narratives:

Network context joins endpoint, identity, and cloud signals to identify complex threats that siloed tools miss.

Fast, Accurate Investigations:

Prophet AI's runtime reasoning and ExtraHop's real-time network telemetry deliver rapid, context-rich determinations.

Defensible Verdicts:

ExtraHop decrypts traffic to expose credential misuse and data exfiltration, backed by wire evidence attackers can't alter.

1. Prophet Security, State of AI in the SOC 2026.

How ExtraHop and Prophet AI Work Together

The integration between ExtraHop RevealX™ and Prophet AI is available today at no additional charge and takes only minutes to configure.

Immutable Network Context for Alerts from Any Source

When an identity provider flags impossible travel or an EDR raises a process anomaly, Prophet AI queries ExtraHop mid-investigation: What did this host talk to? Was protocol use unusual? Did it contact anything on a watchlist? Prophet AI resolves the host to a RevealX device profile and reconstructs its connections, so investigations are grounded in what actually happened on the network.

Every Network Detection, Investigated End to End

Prophet AI automatically investigates each new RevealX detection, from lateral movement and C2 beaconing to ransomware indicators, exfiltration, and identity alerts. RevealX risk scores map to Prophet AI severity bands, and each investigation ends with a timeline and a determination of malicious or benign.

Closed-Loop Workflows Between Consoles

Prophet AI writes each determination back to the originating RevealX detection, including status, resolution, assignee, ticket ID, and a link to the full investigation. Analysts click straight from one console to the other, and RevealX stays clear of detections Prophet AI has already resolved.

Natural-Language Threat Hunting on Network Telemetry

Prophet AI Threat Hunter translates natural-language questions into ExtraHop record searches, so analysts can investigate across network telemetry without learning a new query language.

Verdicts You Can Defend, Down to the Packet Level

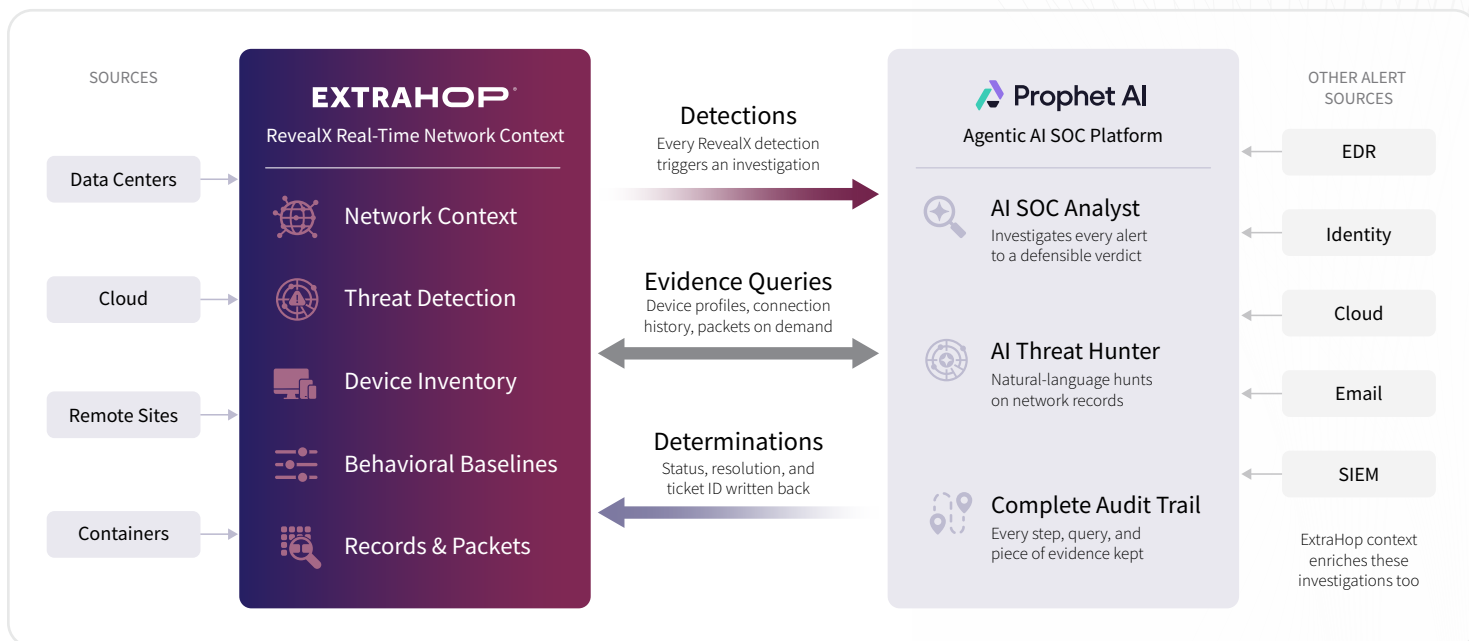
Every question Prophet AI asks, query it runs, and piece of evidence it retrieves is preserved and documented for analysts. Structured network records drive each investigation, and when a finding needs deeper proof, Prophet AI can retrieve packet-level evidence through the RevealX REST API.

Integration at a Glance

Capability	What It Does	Requirements
Detection intake	Prophet AI checks RevealX 360 for new detections and each detection starts an investigation. RevealX risk scores (1–99) map to Prophet AI severity: 80–99 Critical, 60–79 High, 31–59 Medium, 1–30 Low. Every Prophet AI alert links back to its originating detection.	RevealX 360; OAuth2 client credentials
GetAssetInfo	Resolves an IP address, hostname, MAC address, or device ID to a RevealX device profile (role, criticality, VLAN, vendor, and first/last seen). Works for alerts raised by any tool.	None beyond base integration
GetNetworkConnections	Reconstructs who-talked-to-whom for a given IP: source and destination IP and port, protocol, bytes transferred, domain or URI, and user.	Connected recordstore
RawHTTPRequest	Calls any RevealX REST API endpoint during a “Dig Deeper” investigation, such as downloading a packet capture.	Connected packetstore
Write-back	Writes status, resolution, notes, assignee, and ticket ID to the RevealX detection, with a link to the full Prophet AI investigation.	System-write permission; detection tracking enabled

“Bringing ExtraHop’s high-fidelity network data into the Prophet AI SOC Platform provides critical context and ground truth for our AI agents as they investigate alerts and perform threat hunts. This integrated approach gives enterprises the transparency and confidence to trust autonomous security operations.”

VIBHAV SREEKANTI
CTO
Prophet Security



ExtraHop sends detections to Prophet AI and answers its evidence queries in real time. Prophet AI writes determinations back to RevealX.

Get started. Joint customers can enable the integration through their Prophet or ExtraHop account representative or at support@prophetsecurity.ai.

New to either platform? Contact your ExtraHop or Prophet Security account team to request a joint demo.

Built on the Agentic SOC Alliance Operating Model

ExtraHop and Prophet Security are founding members of the Agentic SOC Alliance, which defines an open operating model for autonomous security operations across three layers: context, harness, and model. ExtraHop delivers the real-time context layer. Prophet AI brings the specialized agents, with built-in orchestration, guardrails, and audit trails, that turn that evidence into defensible verdicts.

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](https://www.linkedin.com/company/extrahop).

EXTRAHOP®

info@extrahop.com
extrahop.com

ABOUT PROPHET SECURITY

Prophet Security's mission is to be a force multiplier for security teams by delivering a comprehensive Agentic AI SOC Platform that automates the manual processes across security operations - from alert triage, investigation and incident response to threat hunting, and detection engineering. Prophet AI reduces mean time to investigate, mean time to respond, and delivers a 10x increase in team productivity. The platform reduces risk by finding and closing the gaps in your detection coverage that let attackers operate undetected. Prophet Security's investors include Accel, Bain Capital Ventures, Amex Ventures and Citi Ventures. Learn more at prophetsecurity.ai.