Exaforce

EXTRAHOP

TURN NETWORK INTELLIGENCE INTO ACTION

ExtraHop + Exaforce for Autonomous Investigation and Response

SOLUTION BRIEF

The Challenge

Attackers automate credential theft, lateral movement, and data exfiltration, often hiding from legitimate tools and using trusted accounts. Network context exposes that activity, but analysts must still connect it with identity, endpoint, cloud, and application context.

Every manual pivot delays the investigation and leaves AI agents reasoning over incomplete evidence. Autonomous operations need a trusted, high-fidelity view of the environment to reason with accuracy.

The Solution

ExtraHop RevealX turns network traffic into structured records, behavioral detections, and packet evidence. By integrating ExtraHop with Exaforce, this network intelligence becomes the context layer for the agentic SOC, exposing activity that may appear routine in endpoint or identity tools alone.

Exaforce queries ExtraHop detections and selected records, enriches them with cross-domain context, and investigates each finding. Supporting records and packet evidence remain in RevealX and are retrieved on demand. Exabots chain related activity into one storyline and initiate response through connected controls and approval policies.

KEY HIGHLIGHTS

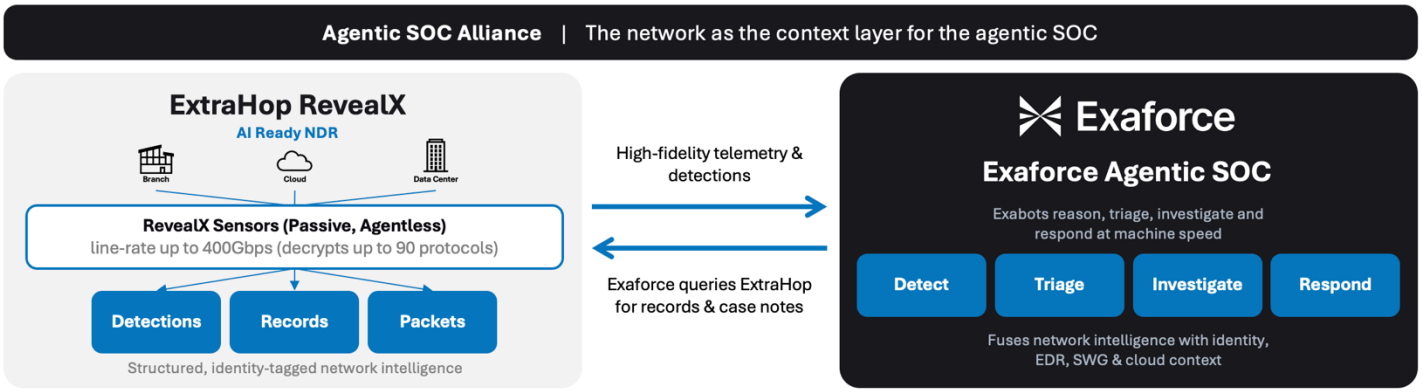
- **ExtraHop detections triaged and investigated, 24/7**
- **Network indicators enriched with asset, owner, and identity context**
- **Investigate network activity using natural language**
- **Attack chains assembled across network, endpoint, identity, SaaS, and cloud**
- **Unusual data movement connected to the user and device behind it**

Key Use Cases

USE CASE	SOLUTION	BENEFITS
Natural-language threat hunting	Exaforce queries connected ExtraHop records alongside identity, endpoint, SaaS, and cloud telemetry, allowing intelligence-driven hunts to include evidence derived from the network. Examples include being able to ask in natural language: ‘What network calls were made prior to authentication into an unusual internal service?’	Faster hunts without requiring every analyst to know the underlying network query language.
Insider threat & data movement	ExtraHop detects unusual data movement. Exaforce maps the source indicator to the device, owner, and identity, then examines related endpoint, identity, and cloud activity to determine whether the transfer is expected or suspicious.	The user, device, and surrounding behavior needed to judge intent - not an isolated source IP.
Attack chaining & autonomous investigation	Exabots connect ExtraHop evidence of East-West lateral movement with related endpoint, identity, SaaS, and cloud activity. Supporting records and packet evidence are retrieved from RevealX on demand, and validated threats can trigger actions through connected endpoint or identity controls.	One evidence-linked storyline from initial access through lateral movement and potential exfiltration.

How it Works

The Integration At-a-glance



Book-ended AI: an AI-ready data source feeding an AI-driven SOC

Operational Outcomes

24/7
triage and investigation of ExtraHop detections

PLAIN ENGLISH
threat hunting across connected network evidence

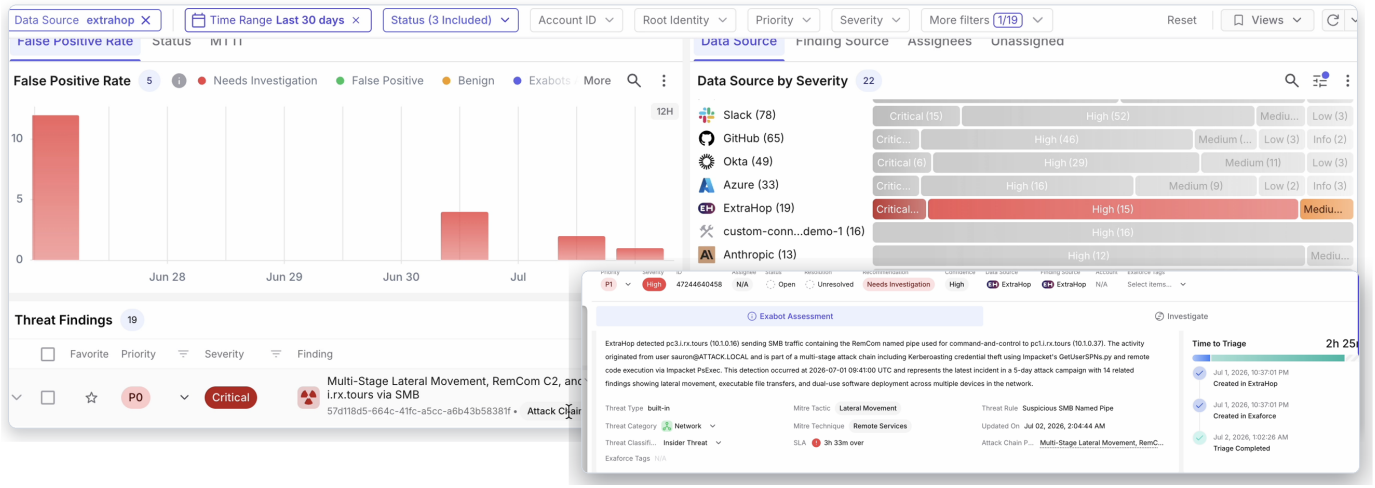
ONE STORYLINE
network, endpoint, identity, SaaS, and cloud context

ON DEMAND
supporting RevealX records and packet evidence

Exaforce connects to ExtraHop RevealX and your identity, endpoint, SASE/SSE, and cloud tools in minutes through least-privilege integrations. The Exaforce data platform queries ExtraHop detections, records, and packet-level evidence alongside the rest of your security telemetry. It enriches every finding with the context analysts normally assemble by hand: who acted, what they touched, where the activity originated, and why it matters. A Source IP address without any additional context or enrichment is resolved to the underlying asset, device owner, and identity using endpoint and identity data - context network telemetry alone cannot provide.

Exabots investigate every detection against Exaforce's real-time knowledge graph. Benign activity is closed with a clear verdict and rationale, while genuine threats are investigated end-to-end with supporting evidence, timelines, and root cause analysis. Related alerts from ExtraHop, endpoint, identity, SaaS, and cloud sources are chained into one attack storyline, so one campaign becomes one investigation rather than a dozen disconnected alerts. Response is executed through the controls you already operate. When additional evidence is needed, Exaforce queries ExtraHop for the relevant records and adds them to analyst-ready case notes. Together, ExtraHop supplies AI-ready network intelligence, and Exaforce turns it into validated decisions and responses at machine speed. The example below shows an ExtraHop finding arriving in Exaforce and being fully assessed, investigated, and triaged.

The Integration in Action



An ExtraHop finding in Exaforce, showing the evidence-linked assessment and the timeline from detection creation to completed triage.

From network detection to an evidence-linked decision - without the manual pivots.

About Exaforce

Exaforce delivers an agentic SOC platform that helps security teams detect, triage, investigate, hunt, and respond to threats with greater speed and consistency. Its task-specific Exabots operate on a shared reasoning foundation and a unified, real-time view of the environment, enabling transparent, evidence-linked decisions across the full SOC lifecycle. Exaforce is available as a SaaS platform or as a fully managed 24/7 MDR service supported by experienced analysts, detection engineers, and incident response experts. The platform is designed for strong tenant isolation and enterprise security requirements, with support for SOC 2, HITRUST, HIPAA, ISO 27001, PCI DSS, and GDPR compliance. Read our customer case studies, explore the platform, or learn more at exaforce.com.

About ExtraHop

ExtraHop is a Leader in the Gartner Magic Quadrant for Network Detection and Response and the founding coordinator of Agentic SOC Alliance. ExtraHop is to the network what EDR is to the endpoint: a platform for every use case that depends on network telemetry, from threat detection and forensics to identity and cloud investigations. RevealX uses passive sensors to decrypt and decode enterprise traffic at line-rate speeds up to 400 Gbps, turning packets into structured, identity-tagged records and behavioral, machine-learning detections across hundreds of MITRE ATT&CK techniques. Trusted across highly regulated industries such as finance and banking, RevealX retains packet-level evidence for forensics and up to 365 days of records for retrospective detection, making it a foundational source of truth for SOC teams. Learn more at extrahop.com.

Request an Exaforce + ExtraHop demo today

See how Exaforce and ExtraHop close the loop on your network as part of Project AgentStream. Visit exaforce.com or scan the code to book a demo.

exaforce.com