EXTRAHOP | CROWDSTRIKE

Complete, Real-Time Context for the AI-Powered SOC

Together, ExtraHop and CrowdStrike unify endpoint, network, and threat context to stop breaches faster.

SOLUTION BRIEF

The Attacker is Already Inside.

Today's adversaries move at machine speed. AI enables them to identify exploitable flaws, generate working exploits, and map lateral paths through your environment faster than any human analyst can respond. According to the CrowdStrike 2026 Global Threat Report, the average attacker breaks in and begins moving laterally in just 29 minutes, then disappears into the noise, impersonating legitimate users with legitimate tools.

Your endpoint agents only see one part of the picture. Your logs can arrive too late, or worse, they may have been tampered with. How can you ensure that your AI agents make autonomous decisions that are accurate and defensible? They are only as good as the context they're given.

The Network Doesn't Lie.

A network is an interconnected web of conversations. An attacker cannot get through that web without leaving a trail, despite their best efforts to cover their tracks.

Nothing crosses your network that ExtraHop doesn't see: lateral movement, command-and-control (C2) communications, living-off-the-land (LotL), and encrypted east-west traffic that bypasses endpoint detection entirely.

ExtraHop builds a continuous, real-time model of your environment — every device, identity, relationship, and behavior. It autonomously discovers and classifies everything communicating on the network, including assets your Falcon agent never touched. When behavior deviates from that baseline, ExtraHop detects it and understands why. When a threat surfaces, ExtraHop delivers an immediate, high-fidelity dossier: who talked to whom, in what sequence, and what actually happened. Your analysts and AI agents can act with confidence.

ExtraHop Provides Context. CrowdStrike Provides Action.

Together, ExtraHop and CrowdStrike offer multiple integrated solutions to help organizations stop AI-powered threats.

WHY THE AGENTIC SOC NEEDS NETWORK DATA

Attackers hide in encrypted east-west traffic endpoint agents never touch

Unmanaged devices create blind spots that grow every time the network changes

AI agents acting on incomplete context make expensive mistakes or miss the breach entirely

WHAT YOU GAIN

Query a full year of network context from within Falcon Next-Gen SIEM — no re-ingestion, no added cost

Gain network visibility beyond the endpoint — unmanaged devices, encrypted traffic, lateral movement

Give your AI agents real-time network context so autonomous decisions are accurate and defensible

The Best NDR for CrowdStrike Customers

ExtraHop RevealX™ Network Detection and Response (NDR) has numerous native integrations with the CrowdStrike Falcon platform to stop breaches faster.

Network Context for Falcon Next-Gen SIEM

With CrowdStrike Federated Search, analysts and AI agents alike can query network context stored with ExtraHop directly from Falcon Next-Gen SIEM.*

Automate Response and Containment

With Charlotte Agentic SOAR, events can be automatically enriched with network context from ExtraHop, and those insights can then trigger investigation, response, and containment actions — so analysts spend less time on manual triage and more time on real threats.

Catch Shadow AI, Rogue AI, and Unsanctioned Access

As AI agents proliferate across the enterprise, so does the risk of unsanctioned access and rogue behavior. ExtraHop monitors network traffic to and from web-based AI tools, revealing which internal IPs are using them and how much data is being transferred regardless of operating system, endpoint agent status, or encryption method. ExtraHop also monitors network traffic for all user identities — human and AI alike — establishing behavioral baselines and detecting anomalous patterns in real time. Whatever crosses the network, ExtraHop sees it. With Federated Search, these insights can be merged with Falcon telemetry to see a complete picture of AI activity.

Give Charlotte AI a Head Start on Every Investigation

ExtraHop's purpose-built AI agents deliver continuous time-series metrics and other real-time context from RevealX to Charlotte AI, exposing trends, anomalies, and subtle low-and-slow behavior that point-in-time scans miss entirely. ExtraHop keeps Charlotte AI continuously informed, automatically creating a case when findings require further action.

Catch Rogue Assets and Lateral Movement that May Have Otherwise Evaded Detection

CrowdStrike Endpoint Protection and ExtraHop NDR share correlated device data and detections to provide an integrated timeline, improve detection accuracy, and deliver greater defense-in-depth.

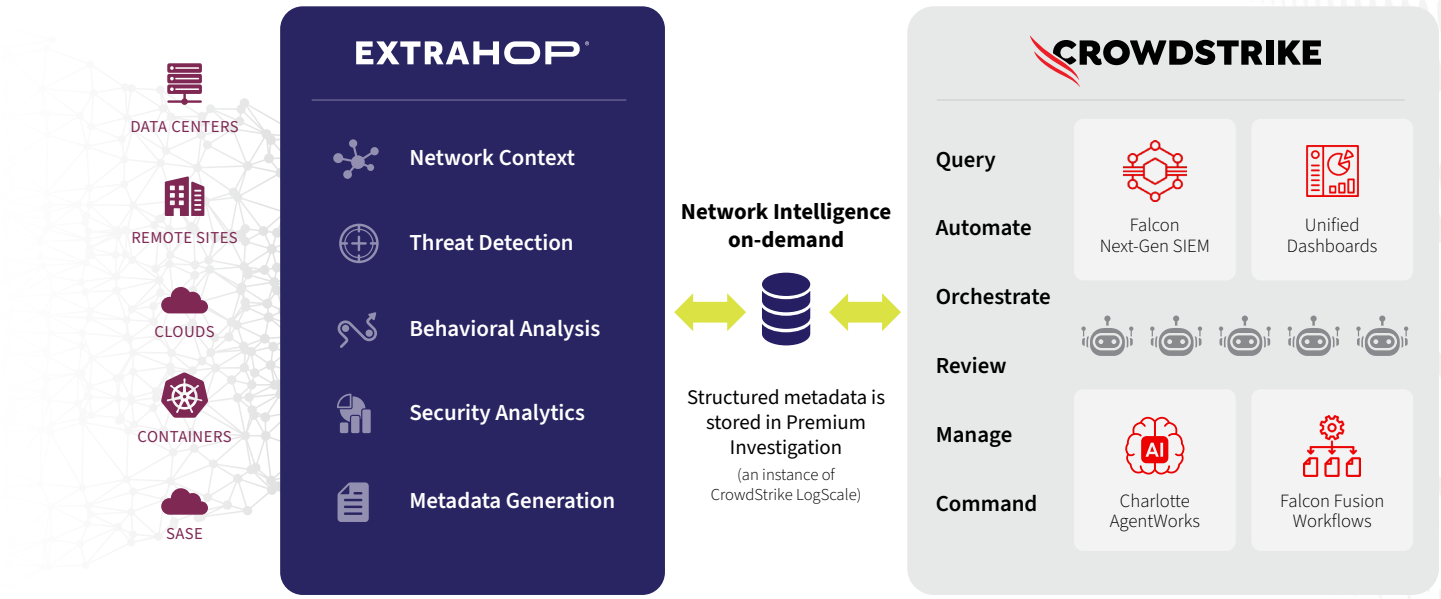
Automatically Enrich ExtraHop Detections with Real-Time IOCs from Trillions of Global Events

World-class threat intelligence from CrowdStrike Adversary Intelligence Premium comes built-in at no additional cost for all ExtraHop NDR customers. As new indicators of compromise (IOCs) emerge, ExtraHop automatically searches the previous 30 days of network records to find evidence of the newly discovered threat.*

Total MDR for the AI Era

For CrowdStrike Falcon Complete Next-Gen MDR customers, the combination of Falcon Next-Gen SIEM with ExtraHop network data expands detection coverage and accelerates investigation and analysis, enabling the Falcon Complete team to stop breaches earlier in the kill chain.

* Requires ExtraHop Premium Investigation



Query a full year of network context from within Falcon Next-Gen SIEM — no re-ingestion, no duplication, no added cost

ABOUT EXTRAHOP

ExtraHop is a leader in real-time network intelligence, empowering organizations with the high-fidelity context they need to power security and IT AI automation, detect risks faster, and respond with confidence.

ExtraHop anchors AI agents with the real-time, ground-truth foundation they need to operate reliably in the SOC and NOC. For security, that means surfacing threats and providing definitive evidence to investigate and respond to novel AI attacks and unsanctioned usage at machine speed. For IT operations, it means identifying and resolving performance issues in seconds to keep critical systems running.

Engineered for unmatched scale, the ExtraHop RevealX platform delivers a complete, unified view of the network for the largest enterprises in the world. Capturing and analyzing network data across data centers, campus, branch, cloud, and AI environments, ExtraHop combines behavioral analysis with deep visibility into encrypted traffic to uncover what others miss.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP

info@extrahop.com
extrahop.com

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/