SOLUTION BRIEF

EXTRAHOP | CROWDSTRIKE

Modernize the SOC with ExtraHop and CrowdStrike

Is your organization at risk due to limited threat detection, siloed security tools across complex, distributed environments, and slow, manual processes? Together, ExtraHop and CrowdStrike unify endpoint and network telemetry, threat intelligence, and the power of a next-gen SIEM to stop threats faster.

Adversaries Love Legacy Security Tools

Time is of the essence

The time it takes an adversary to break into a network and start moving laterally has reached an all-time low at just 48 minutes, according to CrowdStrike's 2025 Global Threat Report. The fastest breakout time was a mere 51 seconds. At that point, the adversary is impersonating a legitimate user and moving through multiple network systems to achieve their goal.

Legacy systems miss critical clues and can even be used maliciously

In today's geopolitical climate, organizations must anticipate that an adversary will someday succeed at getting inside the network and be prepared to stop them before they do damage. Once inside, however, there are plenty of ways for adversaries to hide their tracks. For example, they may use legitimate tools to blend in with normal activity to avoid detection, such as remote monitoring and management tools to maintain persistence, PowerShell for lateral movement and data exfiltration, or pen testing tools to establish command and control (C2) channels.

Security teams need modern solutions

Security teams need real-time visibility into suspicious activity happening on the network and to be able to respond to threats immediately. This requires modern solutions that eliminate visibility gaps, analyze data at petabyte scale to reveal the signal through the noise, and empower security teams to respond faster and automate containment.

To stop advanced attacks, ExtraHop and CrowdStrike are unifying real-time network and endpoint telemetry with world-class threat intelligence to deliver unmatched visibility and faster investigations and response. With an array of integrated solutions to meet customers where they are, together, ExtraHop and CrowdStrike secure complex, distributed environments when seconds matter.

KEY BENEFITS

- Complete visibility and analysis at petabyte scale
- Faster detection and response
- Reduced complexity and cost

WHY THE MODERN SOC NEEDS NETWORK DATA

- See stealth attacks only visible at the network level
- Gain a holistic view of east-west network traffic to reveal lateral movement, command and control, and more
- Detect complex threats earlier and with more accuracy
- Reconstruct attacker behavior from initial access to data exfiltration

4 Integrations for a More Proactive, Efficient SOC

Through native integration with the CrowdStrike Falcon platform, ExtraHop enables security teams to streamline and automate response workflows across hybrid environments.

1

World-Class Threat Intelligence Built In

CrowdStrike Adversary Intelligence Premium comes built-in at no additional cost for all ExtraHop network detection and response (NDR) customers. A feed of real-time indicators of compromise (IOCs) from trillions of global events enriches ExtraHop detections, allowing for faster investigation and remediation.

2

NDR and EDR, a Cybersecurity Power Duo

CrowdStrike Endpoint Protection provides unwavering, fleet-wide visibility across all endpoints and operating systems. Meanwhile, ExtraHop monitors all network traffic, detecting lateral movement, command and control communications, and other hidden threats within the network. Together, CrowdStrike and ExtraHop share device metadata to gain greater visibility and multi-layered defense covering both individual devices and the broader network. This integration minimizes blind spots and provides a more complete view of the security posture.

By querying the AI Search Assistant, “Show me all devices managed by CrowdStrike,” ExtraHop will instantly display all assets in the environment running the Falcon EDR agent. By querying the inverse, analysts can view all assets not running the agent and export this data for further action.

With the press of a button, users can immediately quarantine individual assets from a detection directly within the ExtraHop RevealX™ console and pivot seamlessly into an investigation workflow. ExtraHop communicates with CrowdStrike, and the Falcon agent isolates the machine from the network, neutralizing the threat.

3

Store and Query Network Metadata While Reducing Operational Costs

ExtraHop customers can easily store network metadata (“records”) long-term in CrowdStrike Falcon LogScale to support compliance requirements, threat-hunting operations, and rapid incident response. While other log management solutions slow down investigations and increase the risk of an attack, CrowdStrike Falcon LogScale collects logs at petabyte scale and rapidly accesses data with a sub-second latency. Moreover, as soon as new IOCs emerge, ExtraHop automatically searches the previous 30 days of records to find evidence of the newly discovered threat. Organizations can run new detections on old network data so they can quickly see if they’ve been compromised.

4

Essential Network Data for CrowdStrike Falcon Next-Gen SIEM

CrowdStrike Falcon Next-Gen SIEM unifies security data, including first-party Falcon data from endpoint, threat intelligence, identity, cloud, and more, and correlates it with data from third-party solutions—including network metadata and detections from ExtraHop—for unparalleled visibility and improved threat detection, investigation, and response.

With CrowdStrike Falcon Fusion SOAR, network data and detections from ExtraHop can be used to orchestrate and automate investigation and response actions. For example, ExtraHop monitors traffic to and from web-based generative AI tools, from which internal IPs, and how much data was transferred. The integration with Falcon Fusion SOAR allows security teams to detect, stop, and control shadow AI and automate containment actions to reduce the risk of sensitive data exposure.

For Falcon Complete Next-Gen MDR customers, the combination of CrowdStrike 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.

Unique ExtraHop Features

PETABYTE SCALE

A single ExtraHop sensor can process a sustained 100 Gbps of network traffic (more than a petabyte of data) per day, while a single ExtraHop console can monitor a million active devices. No other NDR solution comes close. Because ExtraHop excels at processing voluminous data at scale, its machine-learning models become more accurate with higher signal-to-noise ratio.

CLOUD-SCALE ML

ExtraHop performs machine learning (ML) in the cloud to enable continuous model updates and to take advantage of unlimited compute power for high-fidelity modeling of every aspect of a customer's environment. Legacy vendors perform ML analysis locally and independently on each appliance, which simply cannot fit sophisticated algorithms and requires frequent firmware updates to stay up to date on threats.

PROTOCOL FLUENCY

Protocols are how systems communicate with each other and move data across a network. ExtraHop is fluent in more than 90 protocols, more than any other NDR provider, which enables more accurate detection of advanced attack techniques.

DECRYPTION

ExtraHop uncovers threats hiding in encrypted traffic, with unique visibility into proprietary Microsoft authentication protocols used to gain access and elevate privileges (e.g., Kerberos golden ticket attacks), and Microsoft application protocols used to share data and manage systems (e.g., SMBv3 remote code execution).

FULL PCAP

ExtraHop sensors offer continuous packet capture (PCAP) for definitive insights and forensic detail to reduce mean time to respond and fulfill chain-of-custody requirements.

OUT-OF-BAND MONITORING

ExtraHop gets a copy of network traffic (from a network TAP, SPAN, SASE traffic replication, or VPC flow logs). The original communication is never impacted nor slowed.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. See a demo or visit our listing on the CrowdStrike Marketplace.

EXTRAHOP®

info@extrahop.com
extrahop.com

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from 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/