EXECUTIVE BRIEF

EXTRAHOP | CROWDSTRIKE

5 Reasons Why Customers Use ExtraHop and CrowdStrike Together

The longer attackers dwell, the greater the damage. Because threats come at every angle, analysts can't rely solely on one solution to keep time on their side.

For full-coverage security when seconds matter, ExtraHop and CrowdStrike have joined forces. Together, we deliver unified visibility of your hybrid and cloud environments. Endpoint visibility, network intelligence, and security telemetry from across the organization work cohesively to maximize detection, investigation, and response capabilities and help to reduce risk, accelerate mean time to respond, and build business resilience.

Dig deeper into why organizations integrate ExtraHop and CrowdStrike.

1 Improved Incident Detection & Correlation

CrowdStrike Falcon® Insight XDR provides the real-time monitoring you need to detect and prevent endpoint attacks, including the initial downloads of malware, fileless attacks, and other advanced TTPs. But with a growing amount of attacks targeting unmanaged IoT and BYOD devices, you need to be able to identify unusual behavior during the "midgame" dwelling phase before an attack unfolds. By combining CrowdStrike's endpoint telemetry and ExtraHop's network intelligence, analysts have richer context at their fingertips, no matter the attack vector. And if anomalous activity is detected, the integrations between platforms allow analysts to triage threats and quarantine devices from a single console with "Push-Button Response" in ExtraHop RevealX 360.

2 Network Visibility for NG-SIEM

Investigate smarter with correlated endpoint and network-based detections to accelerate incident investigation and time to respond. When high-fidelity network data is ingested and correlated with additional data sources within CrowdStrike Falcon® Next-Gen SIEM, analysts can trust that the related threat detections and alerts must be addressed, either by analyst-led response or automated response playbooks.

3 Understand and Contextualize Threats Faster

SOC teams need a complete view of activities in on-premises and cloud networks. But that often means piecing together the puzzle from disparate systems, which slows investigative time. Unified intelligence with Falcon Next-Gen SIEM and ExtraHop RevealX NDR allows analysts to investigate an incident to the packet level with a 90-day lookback, alongside additional data sources. With this comprehensive intelligence and in-depth threat context, analysts can find and block attacks at every stage, even zero-day attacks.

4 Expanded Attack Surface Coverage

Before you can secure devices, you have to know they exist. With CrowdStrike and ExtraHop, you can continuously discover and monitor communications among unknown and unmanaged devices, mobile devices, IoT, BYOD, remote workforce, and more. Once found, you can identify if an asset can be covered by the CrowdStrike Falcon® platform or you can use RevealX to monitor behavior.

5 Better Informed Network Telemetry

When an incident occurs, it's often challenging to get the details analysts need to mitigate the root cause of attack. Together, CrowdStrike and ExtraHop illuminate blind spots and deliver in-depth attack forensics with long-term storage of network intelligence and lightning-fast search within the Falcon platform. Threat hunters and incident responders can quickly surmise activity from endpoints to network and beyond, maximizing detection and response capabilities while streamlining forensic research.

Want to explore additional reasons security teams choose to integrate ExtraHop and CrowdStrike to gain unified threat protection?

Watch our integration videos for a first-hand view of our capabilities

ABOUT EXTRAHOP

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.