ExtraHop

5 Reasons Why Customers Use CrowdStrike and ExtraHop Together

The longer attackers dwell, the greater the damage. Because threats come at every angle, analysts can't rely solely on one detection and response 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 and network intelligence work in tandem to maximize detection and response capabilities and help cut through the noise.

Dig deeper into why organizations integrate ExtraHop and CrowdStrike:

1 Regain the advantage with 87% faster MTTR

CrowdStrike Falcon Insight XDR provides the tools you need to detect and prevent the initial downloads of malware and stop other TTPs at the endpoint. But with a growing amount of attacks targeting unmanaged IoT and BYOD devices, you need to be able to identify unusual behavior during the "mid-game" dwelling phase before an attack unfolds. By combining endpoint and network intelligence, analysts have richer context at their fingertips no matter the attack vector. And if anomalous activity is detected, the integration allows analysts to triage threats and quarantine devices from a single console with "Push-Button Response" in ExtraHop Reveal(x) 360.

2 Alleviate fatigue with prioritized, contextual alerts

Alert fatigue is an ongoing issue in the SOC. CrowdStrike and ExtraHop work together to improve analyst efficiency and help them focus only on what matters. We do this by enriching security data across endpoints, cloud workloads, identities, and data with network intelligence to quickly surface malicious activity to detect and respond to potential attacks. When alerts come in, analysts can trust that they are high fidelity and must be addressed.

3 Easily integrate network intelligence with the existing tech stack

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 CrowdStrike Falcon Insight XDR and ExtraHop NDR allows analysts to investigate an incident to the packet level with a 90-day lookback. With this complete intelligence, they can find and block attacks at every stage, even zero-day attacks.

4 Continuous discovery of unmanaged devices on the network

Before you can secure devices, you have to know they exist. The integration allows you to continuously discover and monitor communications among unknown and unmanaged devices, mobile devices, IoT, BYOD, remote workforce, and more. Then, once found, you can identify if it can be instrumented with the CrowdStrike Falcon platform or use Reveal(x) to monitor behavior.

5 Automatic, retroactive forensics and 90-day lookback

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 complete attack forensics. Threat hunters and incident responders can quickly surmise activity from endpoints and network to maximize 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 is the cybersecurity partner enterprises trust to reveal the unknown and unmask the attack. The company's Reveal(x) 360 platform is the only network detection and response solution that delivers the 360-degree visibility needed to uncover the cybertruth. When organizations have full network transparency with ExtraHop, they see more, know more and stop more cyberattacks. Learn more at **www.extrahop.com**

ExtraHop

info@extrahop.com

www.extrahop.com