ExtraHop + CROWDSTRIKE

Reveal(x) 360

Empower XDR with Network Intelligence

CrowdXDR Alliance

BUILT TO RESPOND WHEN SECONDS MATTER

Secure your hybrid and multi-cloud environment and stop breaches faster.

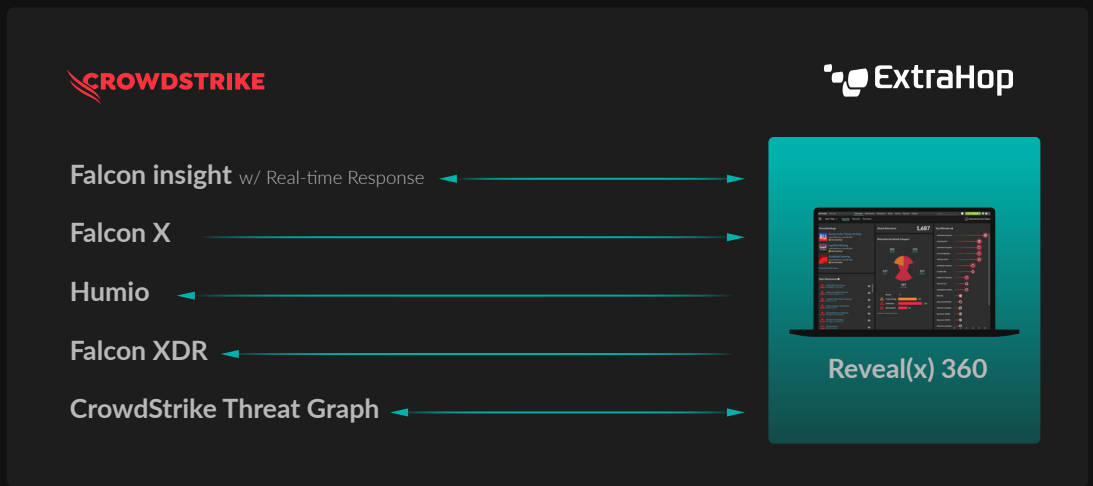
Challenges

Cyberattackers are growing more sophisticated at evading security measures. Businesses are growing rapidly and need security that can keep up without introducing friction. But security staffing is more challenging than ever, and siloed legacy technology and bolted-on security solutions can't keep pace.

Solution

Tightly integrated extended detection and response (XDR) with network detection and response (NDR) helps to enrich endpoint data with relevant network intelligence, alongside additional telemetry across multiple domains, to empower security teams to defend against common and advanced threats.

The robust integration of ExtraHop Reveal(x) 360 with the CrowdStrike Falcon® platform combines complete network intelligence with world-class security telemetry into a single, seamless solution. Automatically contain network-based attacks including lateral movement, ransomware, data exfiltration, and more.



Fast, focused response
Streamline detection, investigation, and response. Quarantine devices in just one click.

Cancel out the noise
High-fidelity detections with sophisticated tuning capabilities cancel out low-risk alerts.

Unified threat intelligence
Investigate an incident to the packet level with 90 days of traffic data records available for investigation.

Security for every device
Discover and monitor unmanaged devices, mobile devices, IoT, BYOD, remote workforce and more.

Full coverage forensics
Analyze endpoint details and encrypted network traffic all in one place.

ExtraHop + CROWDSTRIKE

FEATURED TECHNOLOGY PARTNER

Use Case	Solution	Benefits
Secure the ever-expanding attack surface	Reveal(x) 360 automatically discovers and identifies every host that talks on the network including unmanaged devices, mobile devices, IoT, bring-your-own-device (BYOD), legacy systems, remote workforce, and third-party providers.	A comprehensive, always-up-to-date inventory of all devices on your network, including whether the device has a Falcon agent installed for additional visibility.
Catch stealthy attackers hiding malicious payloads and lateral movement	Reveal(x) 360 decrypts and analyzes network traffic to detect encrypted attacks. This network intelligence is correlated with endpoint details from the Falcon agent via the CrowdStrike Threat Graph.	A real-time, end-to-end view of threat activity and an attacker's behavior on your network.
Stay ahead of new and evolving attack tactics and indicators	Reveal(x) 360 correlates indicators of compromise (IOCs) from CrowdStrike Falcon X with network details surrounding IOC hosts and domains for complete coverage.	Complete visibility into network communication between hosts and domains that are known IOCs, so you can rapidly determine the scope and nature of a threat.
Map threats to the MITRE ATT&CK Framework to determine their phase in the attack lifecycle, assess risk, and prioritize response	Reveal(x) 360 automatically associates threats with tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK framework.	Proactive analysis of gaps in defense and SOC maturity with efficient categorization of adversary behavior to stop breaches quickly.

Technical Solution

Reveal(x) 360 performs full-stream analysis on network traffic from multi-cloud, on-premises, and hybrid environments including AWS, GCP, and Azure. It then uses cloud-scale machine learning to detect anomalous behaviors, and correlates that with IOCs pulled from Falcon X, and enriched endpoint telemetry from CrowdStrike Threat Graph. Within the Reveal(x) 360 console, users can view threat intelligence data, instantly quarantine a device with just one click, and perform thorough investigations with 90 days of forensic data. Network intelligence signals can also be pushed from Reveal(x) 360 to the Falcon platform to automatically contain network-based threats.

CROWDSTRIKE store — More information is available in the CrowdStrike Store.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.
Learn more: https://www.crowdstrike.com/

ABOUT EXTRAHOP NETWORKS

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform uses cloud-scale AI to help enterprises detect and respond to advanced threats—before they compromise your business. When you don't have to choose between protecting your business and moving it forward, that's security, uncompromised. Learn more at www.extrahop.com.

ExtraHop

info@extrahop.com
www.extrahop.com