FEATURED TECHNOLOGY PARTNER

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.

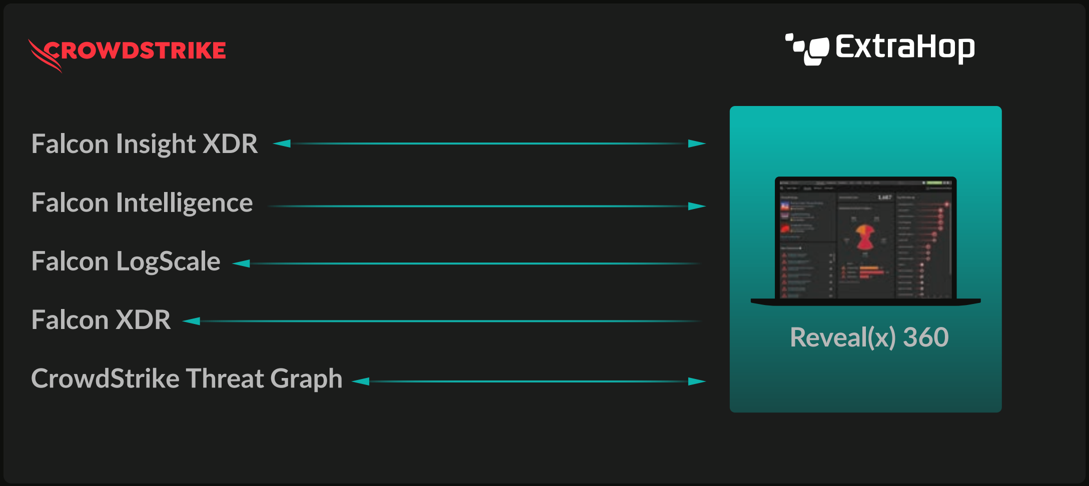
Challenges

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.

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, and correlates that with endpoint details via Falcon Threat Graph or Falcon LogScale.	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) and threat intelligence from CrowdStrike Falcon Intelligence with network behavior details for complete coverage of managed and unmanaged hosts.	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 Intelligence, 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 (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.

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/   Learn more: https://www.crowdstrike.com/

ABOUT EXTRAHOP NETWORKS

Real-time detection and response from ExtraHop uses cloud-scale AI to help enterprises stop advanced threats–before they compromise your business. Learn more at www.extrahop.com.

ExtraHop

info@extrahop.com
www.extrahop.com