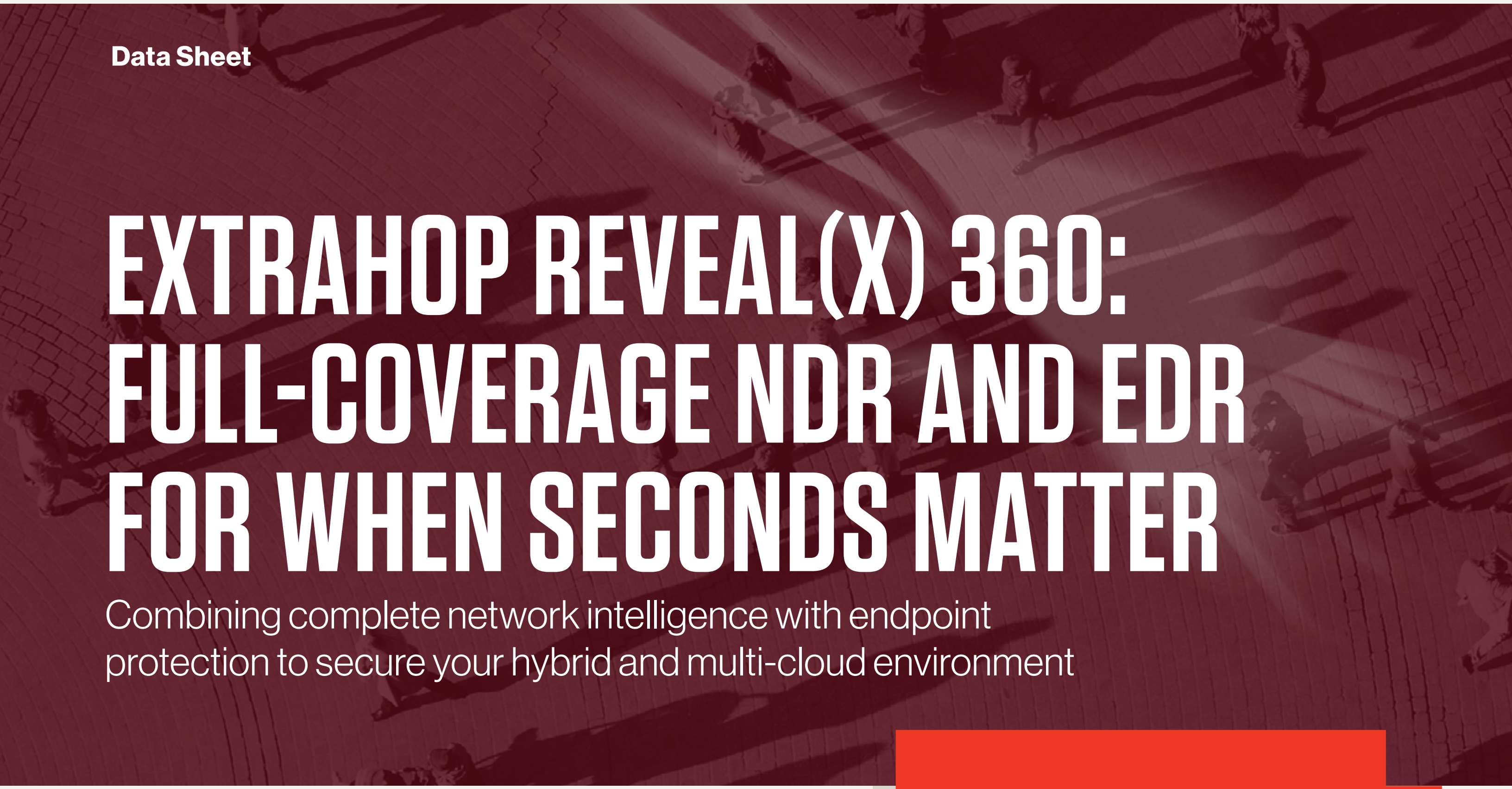


Data Sheet

EXTRAHOP REVEAL(X) 360: FULL-COVERAGE NDR AND EDR FOR WHEN SECONDS MATTER

Combining complete network intelligence with endpoint protection to secure your hybrid and multi-cloud environment

CHALLENGES

Cyberattackers are growing more sophisticated at evading security measures, and businesses that are growing rapidly and dynamically 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 network detection and response (NDR) and endpoint detection and response (EDR) form the foundation for evolving security operations against both common and advanced threats. The purpose-built integration of ExtraHop Reveal(x) 360 with the CrowdStrike Falcon® platform combines complete network intelligence with world-class endpoint security into a single, seamless solution that delivers both NDR and EDR functionality as well as next-generation intrusion detection (NG-IDS) and network forensics with real-time decryption. This solution provides complete detection and response capabilities across every attack surface in your hybrid, multi-cloud enterprise.

KEY BENEFITS

Unified threat intelligence: Share IOCs across EDR and NDR solutions for unified threat detection

Real-time response: Automatically contain both network- and endpoint-based attacks

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

Complete MITRE ATT&CK® coverage: Cover the entire attack chain with endpoint and network TTPs

EDR and NDR forensics combined for full coverage: Endpoint details and network decryption and analysis are correlated in one place for rapid investigation and incident response

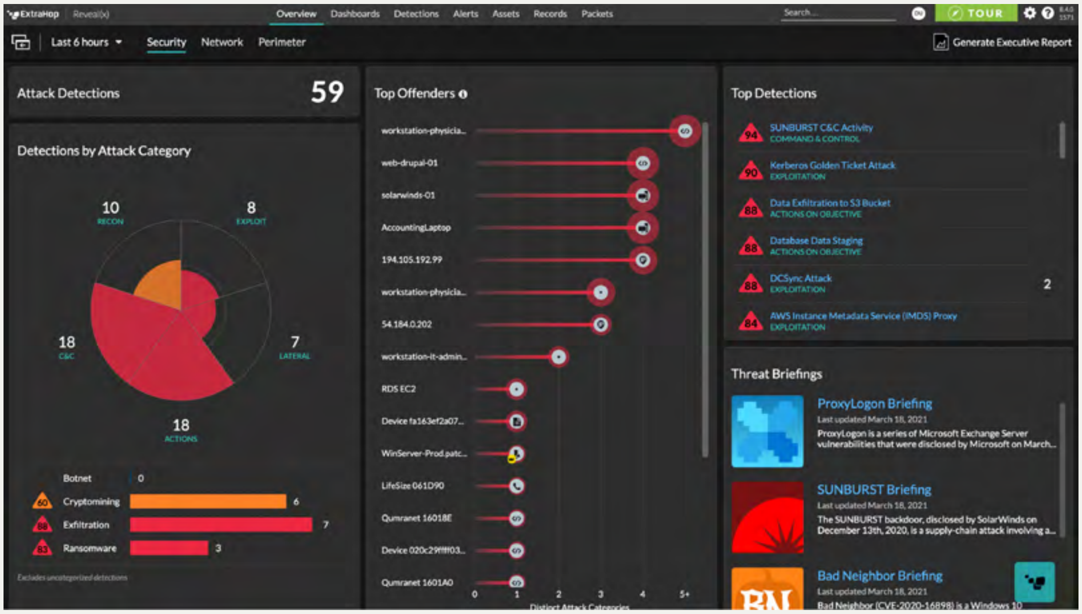
BUSINESS VALUE

Use Case / Challenge	Solution	Benefits
The attack surface is ballooning, with new unmanaged devices, remote workers and cloud services. How do you secure it?	Reveal(x) 360 automatically discovers and identifies every host that talks on the network, including unmanaged IoT, bring-your-own-device (BYOD) and third-party connections.	Security teams get a complete, always-up-to-date inventory of devices on their network, including whether each device has a CrowdStrike Falcon® agent installed. Reveal(x) 360 monitors and secures unmanaged devices for complete coverage.
Stealthy attackers evade detection and hide lateral movement in encrypted data. How do you catch and stop them?	Reveal(x) 360 decrypts and analyzes network traffic to detect advanced attacker tactics and correlates this information with endpoint details from the Falcon agent via the CrowdStrike Threat Graph™ database.	Security teams get complete, integrated visibility into attacker behavior on the endpoint and on the network, for a real-time, end-to-end view of an attacker's actions.
New attack tactics and indicators are discovered all of the time. How do you stay ahead?	Reveal(x) 360 correlates threat intelligence indicators of compromise (IOCs) from CrowdStrike Falcon Intelligence™ automated threat intel with network behavior details about IOC hosts and domains for complete coverage.	Security teams get visibility into network communications between hosts and domains that are known IOCs, so they can rapidly determine the scope and nature of the threat and resolve it quickly to stop the breach.
MITRE ATT&CK framework is the industry standard for mapping detection coverage. How well-covered is your environment?	Reveal(x) 360 detects network-based attack techniques from the MITRE ATT&CK framework, with coverage of multiple techniques within all 12 of MITRE's tactic categories.	Enterprises get greater MITRE ATT&CK coverage, particularly in the post-compromise ATT&CK phases such as lateral movement, command and control, and data exfiltration, often providing the last chance to short-circuit a compromise and stop the breach.

> "The power of EDR and NDR isn't some imagined future state. Our customers are already using the best-of-breed integration between ExtraHop and CrowdStrike, combining real-time endpoint and network telemetry to defend against the most advanced cyberattacks."
>
> **Raja Mukerji,**
> Co-founder and Chief Customer Officer, ExtraHop

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, and then uses cloud-scale machine learning to detect stealthy advanced attack behaviors across the entire network and provide over 90 days of forensic data for every investigation. Reveal(x) 360 pulls indicators of compromise from Falcon Intelligence and endpoint security event data from Threat Graph, and correlates that data with observed network behavior and network threat detections in the Reveal(x) 360 console. Data can also be pushed from Reveal(x) 360 to the Falcon platform to trigger automated containment against active network-based threats.



ProxyLogon Briefing
Last updated March 18, 2021
ProxyLogon is a series of Microsoft Exchange Server vulnerabilities that were disclosed by Microsoft on March...

SUNBURST Briefing
Last updated March 18, 2021
The SUNBURST backdoor, disclosed by SolarWinds on December 13th, 2020, is a supply-chain attack involving a...

Bad Neighbor Briefing
Last updated March 18, 2021
Bad Neighbor (CVE-2020-16898) is a Windows 10

KEY CAPABILITIES

Reveal(x) 360 integrates with several CrowdStrike Falcon products to correlate network intelligence and insights from Reveal(x) 360 with endpoint behavior details and indicators of compromise from Falcon.

- **Reveal(x) 360 + CrowdStrike Falcon Intelligence**
  The Reveal(x) 360 integration with Falcon Intelligence correlates IPs and domains listed as IOCs in Falcon Intelligence with network behavior data about those IPs and domains, providing rapid investigation of potential attacks in progress.
- **Reveal(x) 360 + CrowdStrike Falcon Real Time Response**
  Reveal(x) 360 detects network-based threats that may soon impact specific endpoints but have not yet conducted malicious behavior on the endpoint itself. Reveal(x) 360 can notify the Falcon agent about affected endpoints to contain the endpoint, preventing further spread of the threat.
- **Reveal(x) 360 + CrowdStrike Threat Graph**
  Reveal(x) 360 gathers network transaction metrics, transaction records and full packets and decrypts them in real time, providing complete network intelligence at cloud speed and scale.
- **Reveal(x) 360 for Unmanaged IoT, BYOD and Remote Connections**
  Reveal(x) 360 can discover and identify any device that communicates on the network and identify whether the Falcon agent is installed on the device by observing network traffic, helping customers ensure complete coverage, and security detection and response capabilities — even for unmanaged or unmanageable devices.

ABOUT EXTRAHOP

ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyzes all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behavior and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI 50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop breaches 84% faster — get started at **www.extrahop.com/freetrial**

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, 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/

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

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