CrowdStrike and ExtraHop: Unifying XDR Intelligence with NDR and EDR

ExtraHop

Table of Contents

Security teams are in a race against time

The biggest advantage attackers have is time. Extended detection and response (XDR) puts time back on the side of defenders to shut down phishing, ransomware, and other advanced threats before they evolve into breaches.

As a holistic solution that integrates multiple security products into a cohesive security operations system, XDR stops lateral movement in its tracks while your SOC team investigates and acts to contain threats in real time. In this ebook, we explain how you can leverage ExtraHop and CrowdStrike for a unified XDR strategy that seamlessly correlates endpoint, network, and threat intelligence for complete visibility across distributed environments.

We'll show how you can:

- Gain a more complete picture of your attack surface
- Hunt for, prioritize, and contain threats faster
- Move from detection to quarantine to investigation in one simple motion

RAISING THE STAKES ON DETECTION & RESPONSE

77%

of security professionals believe detection and response is becoming more difficult

46%

of IT decision-makers say their environment is more complex now than 2 years ago

47%

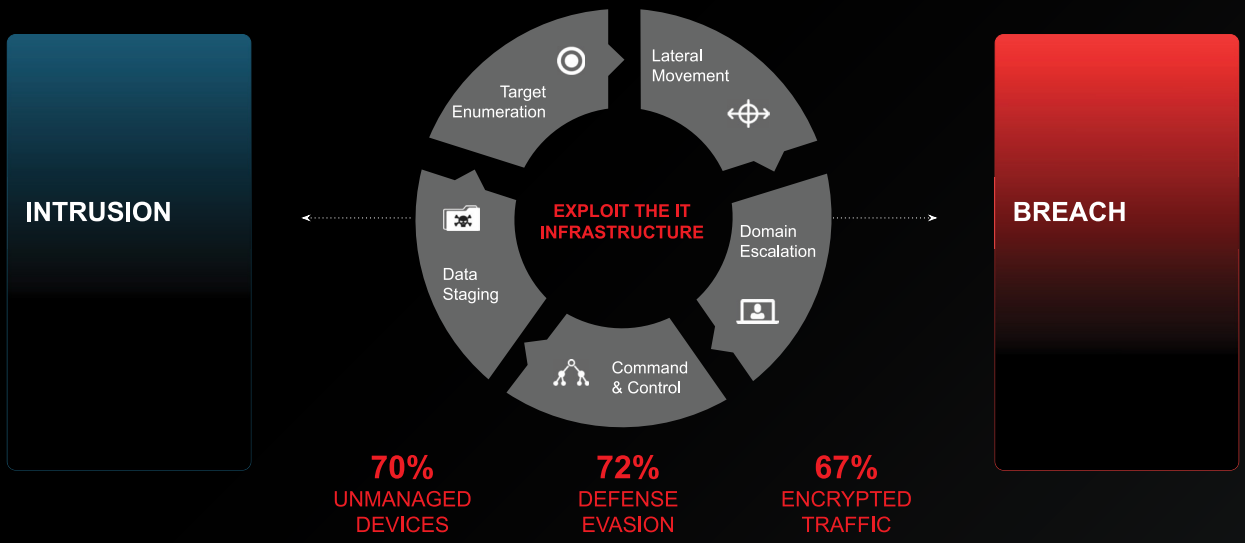
say disparate security tools — siloed solutions — are the #1 challenge for detection and response

Modern attacks exploit blind spots

Sophisticated cyber criminals know where to look to find gaps in your security infrastructure. They gain access through phishing campaigns, by exploiting known vulnerabilities, or even using credentials bought on the black market. Then they stealthily work their way through your network, biding time as they compromise assets until they reach active directories.

The longer it takes your SOC team to detect lateral movement, the greater the odds of hackers exfiltrating data to extort higher ransoms. While they fly under the radar, intruders leverage blind spots created by:

- The high volume of unmanaged devices
- Increased use of (intentionally) encrypted traffic
- Siloed security tools



Longer dwell times can lead to larger ransoms. Modern attacks use phishing, malware, and other tactics, techniques and procedures (TTPs) to compromise endpoints and start scanning the environment for vulnerable assets and workloads. The longer the dwell time, the closer attacks come to taking control of active directories and detonating ransomware and other "go big" attacks.

SILOED SOLUTIONS CAUSE FRICTION AND DELAYS

When disparate security tools generate data, they create gaps in visibility that can slow detection and response. With no way to pull the pieces of the puzzle together, SOC teams lack the context they need to act and waste valuable cycles chasing high volumes of dead-end alerts.

85% experience ransomware

72% paid the ransom

60% were hit more than once*

RANSOMWARE'S METEORIC RISE

Ransomware continues to enjoy explosive growth. To stop attacks that overwhelm enterprises with hard-to-detect techniques and lateral movement — and avoid paying exponentially higher ransoms — modern defenders need complete visibility and turnkey intelligence.

	2016	2018	2022
Target	Consumers	Employees	Enterprise
Strategy/initial access	"Spray and pray," malware, phishing, credentials, vulnerabilities	Spear phishing, malware, BYOD, misconfigurations	Land-n-pivot, lateral tooling, initial access brokers (IABs), supply chain
Average ransom	**$1K**	**$6.7K**	**$810K**

*Source: Wakefield Research, 2021

XDR turns the tables on would-be attackers

XDR collects threat data from previously siloed security tools across endpoints, network, cloud workloads, email, and more for easier and faster investigation, threat hunting, and response. Unified XDR makes sifting through and correlating alerts faster and easier so you can accurately hunt and detect malicious activity across multiple domains.

THE RIGHT TOOL FOR THE RIGHT JOB

In the early stages of attack, endpoint detection and response EDR enables your SOC team with continuous monitoring of end-user devices to detect and respond to cyber threats like ransomware and malware. Modern EDR products like CrowdStrike Falcon Insight XDR continuously monitor all endpoint activity and analyze the data in real time to automatically identify threat activity. This equips your defenders to both detect and prevent advanced threats as they happen. Falcon Insight XDR also applies security logic derived from CrowdStrike Intelligence to deliver the complete context of an attack, including attribution.

But in today's complex and remote work environments, attackers increasingly target the large number of Internet of Things (IoT) and BYOD devices that still go unmanaged. Here, your defenders need network detection and response (NDR) intelligence such as ExtraHop's Reveal(x) 360 to detect unusual behavior during the "mid-game" phase of unfolding attacks.

EDR and NDR work in tandem to give responders complete threat intelligence and the best odds of avoiding costly breaches.

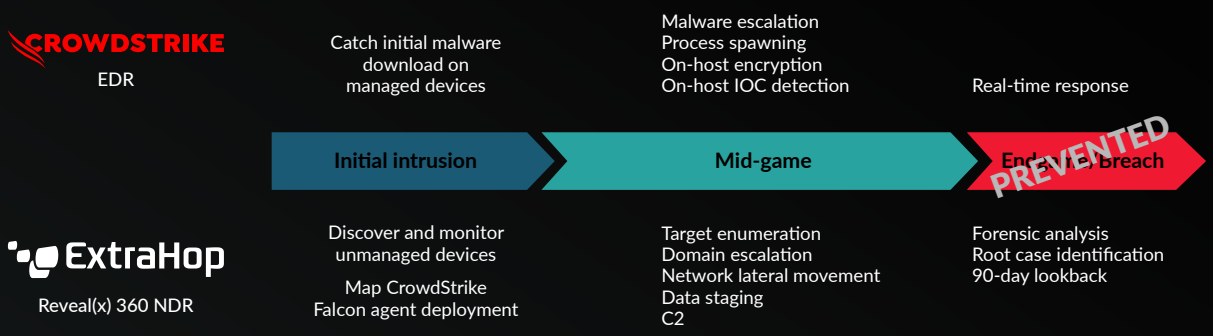
Arm defenders with complete intelligence

Many TTPs that cybercrime groups use to burrow deeper into your environment can be seen in real time — if you know where to look.

Your SOC team needs a complete view of what takes place on your on-premises and cloud networks — including threat activity — so you can respond faster and stop breaches from happening. Like best-of-breed EDR, network intelligence plays a foundational role in successful XDR.

As attackers enumerate and compromise targets, NDR covertly monitors traffic and flags network-based lateral movement such as domain escalation, data staging, command & control (C2) activity, and other mid-game tactics that leave behind visible signs. ExtraHop Reveal(x) 360 can:

- Spot unusual movement across hybrid network environments
- Detect unmanaged IoT or BYOD devices so you can shrink your attack surface
- Natively decrypt SSL/TLS traffic to detect unusual behavior in real time



INTELLIGENCE AT EVERY STAGE

Together, the CrowdStrike Falcon® platform and ExtraHop NDR products deliver integrated XDR to unify data and capabilities in order to find and block attacks at every stage. The ExtraHop and CrowdStrike integrations provide comprehensive visibility and control within your environment, enabling your SOC team to contain and quarantine potential attacks on managed endpoints with the click of a button — and detect unmanaged devices to plug the open holes in your network attack surface.

Stop breaches faster with the push of a button

XDR solutions help map coverage across hosts, assets, and workloads in your hybrid environment, and automatically correlate intelligence. A unified view from a single console equips security professionals to:

- Enrich endpoint data with network intelligence and telemetry from other vectors
- Push new detections fast so teams can act quickly during urgent attacks
- Use the right tool for the right job — working in tandem
- Gain greater value from existing solutions

TAKE XDR TO THE NEXT LEVEL

CrowdStrike Falcon Insight XDR

- Threat-centric data
- Purpose-built integrations
- Single unified view

ExtraHop Reveal(x) 360

- Breadth and depth of visibility
- Reduced false positives
- Native traffic decryption
- Detection tuning

XDR Empowered with Network Intelligence

- Eliminates blind spots, silos, and friction
- Streamlines workflows for urgent threats
- Provides cloud-delivered intelligence
- Reduces need to write detection rules
- Delivers ontinuous value
- Steadily shrinks your attack surface

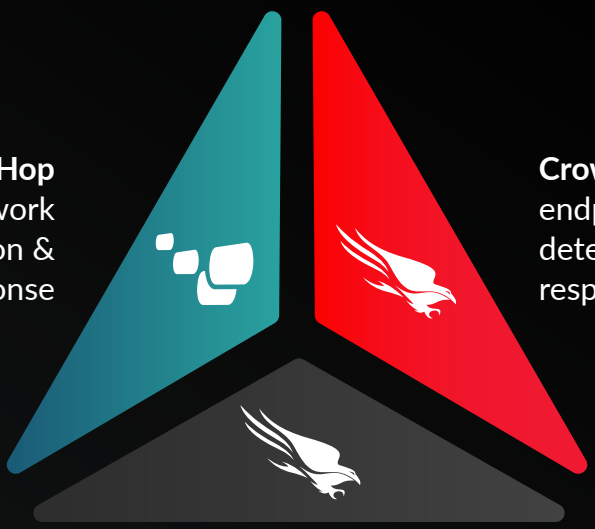
Push-Button Response, a streamlined integration between the CrowdStrike and ExtraHop platforms, lets responders contain threats detected on managed endpoints with the click of a button. When Reveal(x) 360 detects network-based threats, defenders click “Contain devices in CrowdStrike,” and the Falcon platform immediately quarantines the relevant device to stop attacks from progressing to your active directory.

Once threats are contained, your SOC team can work backward to figure out where a threat originated. Reveal(x) 360 automatically maps coverage to show which hosts and workloads have Falcon agents installed so you can eliminate monitoring blind spots and silos.

Keep time on your defenders' side

Threats come from any angle, across diverse endpoints and networks. SOC teams need reliable endpoint visibility and network intelligence to know which potential threats to prioritize.

Together, CrowdStrike and ExtraHop deliver on the promise of XDR to illuminate blind spots in your security domain. Unified XDR — with endpoint visibility and network intelligence working in tandem — maximizes detection and response capabilities and helps cut through the noise.



Robust integration between CrowdStrike Falcon Insight XDR, ExtraHop Reveal(x) 360, and CrowdStrike Falcon LogScale for log management creates seamless integration solutions for automated XDR and rapid response.

GAIN COMPLETE VISIBILITY ACROSS EVERY ENVIRONMENT

Integrated detection, incident workflows, forensics, and log management data promotes:

- Comprehensive MITRE ATT&CK® coverage
- Proactive threat hunting
- Greater return on existing tool investments

AUTOMATE REAL-TIME RESPONSE

Based on threat stages or actions detected on an endpoint or network, a policy-based response can stop malware and other TTPs from progressing to detonate sophisticated attacks.

IMPROVE FORENSICS

Complete attack data shows threat hunters and incident responders what took place on endpoints so they can find and eradicate the root cause of attack.

STEADILY SHRINK YOUR ATTACK SURFACE

Real-time mapping of endpoint coverage lets defenders add Falcon agents and educate users as new IoT and BYOD devices come online.

Stay ahead of advanced threats

ABOUT CROWDSTRIKE FALCON XDR

CrowdStrike (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 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.

ABOUT EXTRAHOP REVEAL(X) 360

ExtraHop's SaaS-based Reveal(x) 360 delivers advanced network detection and response (NDR) that unifies security controls across hybrid, multi-cloud, containerized, and IoT environments. Unified, cloud-native security across on-premises and cloud environments delivers 360-degree visibility and situational intelligence without the friction and management burden of traditional approaches.

Get Started

Learn more about what XDR can do for your business

Request a demo

Speak with a sales associate

Learn more about CrowdStrike

Start a free CrowdStrike trial today

ExtraHop

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats — before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behavior, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others.

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**