

# EXACTLY WHAT IS XDR?

**Extended detection and response (XDR)** is the next frontier for stopping today's sophisticated threats.

It's a holistic approach that streamlines security data ingestion, analysis and workflows across an organization's entire security stack.



## Extended

Supercharge your endpoint detection and response (EDR) with full-spectrum telemetry pulled and integrated across your security stack



## Detection

Identify and hunt threats faster with cross-platform attack indicators, insights and alerts within one unified console



## Response

Turn XDR insight into orchestrated action, and design and automate multiplatform response workflows for surgical and streamlined remediation

## WHY XDR NOW?

**Siloed security data and systems result in major blind spots**

**45**

average number of cybersecurity-related tools deployed on enterprise networks<sup>1</sup>

**Security teams need to be quick and nimble to respond to today's threats**

**92**

minutes before attackers begin moving laterally after gaining access<sup>2</sup>

**Maximize the value from your existing technology to reduce risk**

**59%**

of global security decision-makers reported their firm's sensitive data was breached at least once in the past year<sup>3</sup>

## DON'T FALL FOR FAUXDR

Lots of vendors will sell you "XDR" that is not the real deal:

**NOT XDR:**

**NDR ≠ XDR**

**SOAR ≠ XDR**

**SIEM ≠ XDR**

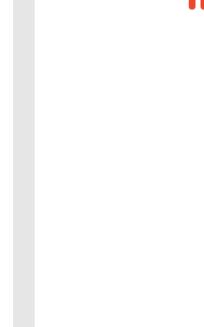
**NDR + SOAR + SIEM ≠ XDR**

## FASTER, HIGH-FIDELITY DETECTION



Extend protection technologies to third-party data sources for high-fidelity detection, investigation and hunting across the attack surface

## BEST-OF-BREED ECOSYSTEM



Unify relevant telemetry from multiple technologies and domains to enable faster response to threats, wherever they occur

## REDUCE TOTAL COST OF OWNERSHIP



Extend the value of your security stack by making it work together

## STREAMLINED RESPONSE



Empower security teams to design and automate multistage, multiplatform response workflows for surgical, full-stack remediation

## MORE EFFICIENT SECOPS



Intelligently correlate data from multiple sources – rapidly at scale – to deliver actionable security insights from a single console

## XDR – THE REAL DEAL

The ultimate solution for unified, cross-platform detection, investigation, hunting and response.

**FALCON XDR**

Extend beyond the endpoint

[Learn More](#)

"**GOOD XDR LIVES AND DIES BY THE FOUNDATION OF GOOD EDR.**"<sup>4</sup>

— Forrester Report: Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR —

© 2021 CrowdStrike, Inc. All rights reserved.

**CROWDSTRIKE**

WE STOP BREACHES

SOURCES:

<sup>1</sup> <https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/>

<sup>2</sup> <https://www.darkreading.com/threat-intelligence/attackers-moving-faster-inside-target-networks-report>

<sup>3</sup> <https://reprints2.forrester.com/assets/2/482/RES165773/report>