CrowdStrike Q&A

CROWDSTRIKE

XDR EXPLAINED

By an Industry Expert Analyst

ALLIE MELLEN

Sr. Analyst at Forrester Research

XDR is a hot topic across the cybersecurity industry. We posed these questions to Allie Mellen, guest speaker in our CrowdCast, **"The X Factor: Why XDR Must Start with EDR,"** to get her take on this popular subject — here's what she had to say.

GET US BEYOND THE BUZZWORD. WHAT EXACTLY IS XDR?

XDR, or extended detection and response, is an evolution of endpoint detection and response (EDR) technology. XDR addresses common challenges for security teams — namely, the evolving nature of IT threats and day-to-day tactical activities that take up too much of their time. It provides higher-quality detections by using the endpoint as an anchor and adding additional context from other security tools. However, instead of allowing any type of data, XDR vendors limit the ecosystem they support according to what will deliver high-efficacy detections. Because XDR is cloud-native, vendors can continuously provide new detections informed by the broad view across their customer base and threat intelligence programs.

XDR is an evolution of endpoint detection and response (EDR)

WHAT TRENDS ARE DRIVING THE NEED FOR XDR?

Every year, Forrester takes the pulse of security decision-makers by surveying them about their top challenges, priorities and details of their security strategy. Since 2019, security decision-makers have consistently cited the evolving nature of IT threats as a top challenge for their organization. Attacks are changing quickly, and the staff needed for a fully fledged detection engineering team is hard to hire and retain in an in-house security operations center (SOC). EDR has helped with some of this — because it's a cloud-native offering, EDR vendors can update detections and add new ones, and because of the quality of endpoint telemetry, EDR provides valuable context for investigation. However, incident responders need a more complete picture of an attack than EDR alone can provide. While the endpoint still serves as the common thread of many attacks, context from other tools can help security teams investigate and respond faster.

Incident responders need a more complete picture of an attack

HOW IMPORTANT IS EDR TO XDR, AND WHY?

EDR is foundational to XDR. An XDR solution's most important value proposition is the quality of detections it can provide. EDR provides actionable, contextual telemetry to make robust detections, which is only bolstered by the addition of other telemetry sources as vendors move to XDR. This is validated by the managed detection and response (MDR) market, where vendors have been incorporating other data sources for context and detection since 2020.

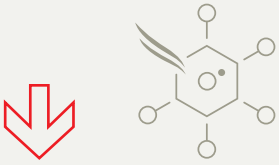
MANY VENDORS "SELL" XDR — WHAT SHOULD BUYERS BEWARE OF?

The simplest way to break down a market is into three different factors: capabilities, dependencies and time-to-value. Capabilities are what the technology does; dependencies are what maintenance is required to use it; and time-to-value is how much time and effort is required to get started. I only define a new market if a technology meets each of these requirements in a differentiated way and if there is enough traction in the industry. To determine if a vendor is selling a differentiated product, ask questions related to these three factors. If the vendor cannot answer questions about these factors in a way that differentiates their product from an existing market segment, the product is likely part of that existing market segment and should not be defined separately.

Ask questions

WHY SHOULD SECURITY LEADERS AS WELL AS THE C-SUITE AND BOARD MEMBERS CARE ABOUT XDR?

The SOC is the cornerstone of a strong security program, and XDR will be a key piece of it. Security leaders should consider XDR as part of their future security strategy because it has the potential to reduce work for their security staff. Security teams struggle with finding and retaining veteran talent for more complex tasks like detection engineering, and XDR takes some of that effort off the plate of security teams and puts it back on the vendor. While detection quality and investigation are where security teams are getting value from XDR today, in the future, XDR looks to provide a more comprehensive response as well.



Security leaders should consider **XDR** as part of their future

Hear more from Allie Mellen and CrowdStrike CTO Michael Sentonas in this on-demand webinar:

The X Factor
Why XDR Must Start with EDR

Access additional XDR resources including infographics, analyst reports and more.

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.**

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/**