CrowdStrike White Paper

CROWDSTRIKE

MAKING THE MOVE TO EXTENDED DETECTION AND RESPONSE (XDR)

Understand how to best protect against threats beyond your endpoints

WHY SILOED DETECTION AND RESPONSE NO LONGER CUTS IT

Today, many organizations rely on a collection of disparate security tools to identify and mitigate threats. These siloed security implementations are inherently inefficient and ineffective. Detecting, isolating and remediating security incidents is resource-intensive, time-consuming and error-prone, and involves multiple platforms and administrative interfaces. To get to the bottom of an issue, security analysts are often forced to manually sift through and piece together volumes of diverse alert and event data generated by different systems.

To make matters worse, today's sophisticated threat actors know where to look for gaps in security silos. They can slip between defenses and move laterally across the network, flying under the radar for extended periods of time, lying in wait and gathering reconnaissance data for future attacks.

Businesses looking to enhance their endpoint security game want access to more telemetry from the wide set of security solutions in which they have already invested — without adding more complexity to their security stack. One of the primary roles **extended detection and response (XDR)** plays is easily connecting the dots among siloed security solutions, extending visibility and detection and ultimately speeding up response and protection across the infrastructure.

Taking the right approach to XDR on a platform that can fully support its capabilities can improve visibility in an increasingly complex threat landscape and accelerate better-informed threat detection and response.

This white paper discusses what to look for in an XDR solution to gain maximum benefit.

HOW XDR WORKS: BUILDING ON AN EDR FOUNDATION

Security buyers have invested in many individual security solutions over the years to protect specific parts of their overall environment — from endpoint and identity protection to email, network and cloud security. Unfortunately, most of these security solutions, and the data they contain, remain siloed today, operating independently over an increasingly complex IT environment where the chances of security gaps that go unnoticed continue to heighten and the likelihood of a breach is all but inevitable.

Attackers take advantage of the fact that security teams lack this cross-domain visibility and cannot see malicious activity occurring between and across the gaps of siloed security solutions. Once attackers successfully infiltrate an organization, they begin to move laterally to search for additional exposures and find the golden data troves they can monetize, hold for ransomware or otherwise exploit.

However, just because the systems are siloed doesn't mean the high volumes of data they generate are meaningless. Quite the contrary, in fact. This data, when un-siloed and correlated with other high-signal data like **endpoint detection and response (EDR)** telemetry, can offer incredibly valuable context for threat detection and response — turning low-confidence signals into high-confidence alerts.

XDR does exactly this. It breaks down the barriers between siloed security solutions so they can work together to improve threat visibility, detection and response time. When implemented on a cloud-native platform, XDR has the scalability and power to:

- Ingest and centralize the volumes of data from endpoints and security solutions across the enterprise
- Leverage advanced automation and technologies such as artificial intelligence (AI) and machine learning (ML) to parse data, correlate it to the attack surface that was penetrated, and perform analysis and prioritization
- Normalize the data, reorganizing it so that users can properly utilize it for further queries and analysis in threat hunting and investigation
- Present security teams with this data in a single console that not only allows users to access cross-domain information for hunting and investigation but also to direct and orchestrate response

XDR delivered from a cloud-native platform dramatically improves threat visibility and reduces the length of time required to identify and respond to an attack, enabling advanced forensic investigation and threat hunting capabilities across multiple domains from a single console.

DISTINGUISHING XDR FROM EDR AND MDR

It's important to understand where EDR and **managed detection and response (MDR)** stop and XDR begins.

EDR solutions use software agents to continuously monitor and capture endpoint activity, storing it in a centralized repository. EDR solutions deliver visibility, context for events occurring on the endpoint and in-depth analysis to automatically detect suspicious activity.

The key is that EDR focuses on endpoint data, while XDR builds on the principles and processes that EDR establishes to optimize and extend them.

XDR gathers, analyzes and provides insights from telemetry generated from solutions protecting endpoints and from other parts of the infrastructure beyond endpoints. XDR connects the dots in this combined telemetry to provide richer context for detecting, as well as proactively hunting, the most dangerous threats. And by producing high-fidelity alerts from individual signals generated by the many solutions in your security stack, XDR gives you additional value without adding further complexity to the stack.

MDR is usually just EDR purchased as a service. The vendor's staff — hopefully with a solid track record in using EDR — provides continuous monitoring of endpoints to aid in mitigating, eliminating and remediating threats.

PUTTING THE X IN XDR

Forrester defines XDR as: The evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools, such as NAV, email security, identity and access management (IAM), cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

Allie Mellen, *"Introducing The Forrester New Tech: Extended Detection And Response (XDR) — A Battle Between Precedent And Innovation,"* Forrester Research, August 2, 2021.

In some cases, expanded MDR services can serve as a managed security operations center (SOC) with access to security solutions and logs beyond the endpoint. They can perform what is essentially "manual XDR," where they pivot between different siloed solutions, trying to bridge the gaps between them.

Their level of success depends on attacks falling within the scope they can detect and how well they can execute a response coordinating the tools they use, such as an SIEM, a network traffic analysis (NTA) solution, an endpoint protection platform (EPP) or an intrusion detection system (IDS).

In contrast to EDR and MDR, an XDR solution delivered from a cloud-native platform can extend detection and response across the infrastructure to improve visibility, response time and, ultimately, protection. It scales to meet the needs of today's growing, data-rich enterprises, ingesting and analyzing vast amounts of telemetry — far beyond what can be accomplished manually. Data is normalized and presented to staff through a single console.

FINDING THE RIGHT XDR SOLUTION

To fully deliver on its promise for optimum detection, investigation, hunting and response, any XDR solution you are considering must demonstrate some key capabilities.

- **Runs on a cloud-native platform.** It operates at sufficient scale, with the ability to ingest data from multiple sources, provides broad visibility and detection capabilities across all data, and is positioned to orchestrate response.
- **Extends endpoint security.** It continues to focus protection on endpoints but extends visibility, detection and response beyond them through best-of-breed integrations with security solutions through an open data scheme.
- **Focuses on threats.** It automatically detects stealthy threats, eliminating the need to write, tune and maintain detection rules.
- **Offers broad, relevant and enriched telemetry.** It incorporates a broad, diverse set of systems and applications for more comprehensive contextualization and correlation, including network analysis and visibility (NAV), next-generation firewall (NGFW), email security, identity and access management (IAM), cloud workload protection (CWP), cloud access security broker (CASB) and others.
- **Communicates with security tools.** It leverages open, well-defined schemas for data exchanges with additional IT security systems to ensure enrichment and correlation take place in a consistent and comprehensive fashion with key objectives and outcomes in mind.
- **Ensures investigations are meaningful.** It emphasizes data fidelity and detection quality to ensure XDR events and investigations are meaningful and efficient, minimizing false positives.
- **Expedites response.** With multistage, multiplatform response workflows, it enables security teams to take swift — even automated — action to mitigate and remediate threats detected.
- **Continues to search for unknowns.** Applies advanced analytics, AI and ML to continuously search for previously hidden threats using aggregation and understanding of multiple, disparate weaker signals from different security domains across the security stack.

XDR: THE PAYOFF

XDR improves an organization's cybersecurity posture by:

- Delivering faster, high-fidelity detection than siloed security tools
- Turning insight into orchestrated action, streamlining response for surgical, full-stack remediation
- Coordinating insight from a diverse array of the best security solutions IT systems and networks
- Enabling analysts to quickly hunt for suspicious activity or further investigate detections against cross-domain data
- Making SecOps more efficient and freer to focus on threats that matter, with the context needed to make threat detection and response analysis faster and more accurate

By selecting the right XDR solution, you can streamline your security journey and make the most of your technology investments.

TAKE THE NEXT STEP

- Visit the **CrowdStrike Falcon XDR™ solution page** to learn more about extending the detection and response capabilities of your organization.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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, 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.**

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

Start Free Trial
of Falcon X

Learn more at **www.crowdstrike.com**