How to Make Sense of XDR

Extended detection and response is far more than a buzzword. Learn what it means for your security operations center (SOC).

XDR (extended detection and response) has become a hot topic among CISOs and other security professionals. But the term itself can be confusing. Nearly half of IT professionals (45%) report that there is no clear, standard industry definition of XDR.

It's not hard to imagine why. When trying to learn about XDR, 51% look to technology vendors for help. But too many technology providers limit their definitions of XDR in ways that match the limits of their own offerings. This article, however, places no such limits on our definition. Read on to understand what XDR is, how it can benefit you, how you can avoid common pitfalls, and more.

What is XDR?

XDR stands for **extended detection and response**. XDR is a natural evolution of *endpoint detection and response (EDR)*, which provides visibility into the status of endpoints.

Think of XDR as a combination of tools and data that provides greater visibility, analysis, and response across endpoints, workloads, users, and networks. XDR unifies endpoint and workload security capabilities with visibility into the network and cloud. In doing so, XDR equips security teams to reduce blind spots, detect threats faster, and automate remediation via authoritative context across all these domains.

What does XDR protect?

- Endpoints
- Networks
- Cloud
- Workloads
- User identities/access

How XDR differs from EDR

EDR gives security professionals visibility into endpoints that might be compromised. EDR solutions continuously record and store endpoint activity data so security professionals can hunt threats in real time and visualize the complete attack kill chain. EDR is, without question, an essential solution for any SOC.

But as threats evolve and attackers gain more sophisticated techniques, it's not enough to focus solely on endpoints like computers, mobile phones, IoT devices and servers. When facing complex attacks, security teams need more context than EDR can provide. This is especially true for attacks involving lateral movement across multiple networks where cybercriminals may move through connected systems to gain access to sensitive data and other high-value assets. That’s where XDR comes in.

XDR provides a holistic view of activity across the system–enough to avoid visibility gaps. That holistic view allows security teams to understand where a threat comes from and how it’s spreading across the environment, which is essential to contain and eliminate the threat. XDR, in other words, enables telemetry, behavioral analysis and correlation across multiple security layers–not just endpoints. With XDR, security teams can see the big picture.

The need for XDR is intensifying

Security professionals know that threats are evolving rapidly–to the point where cyber defenses themselves are being attacked. Ransomware, for instance, is becoming vastly more prevalent for holding data (and organizations) hostage until ransoms are paid. Nearly 3,000 IT and security professionals surveyed by the Thales Group reported a 48% increase in ransomware attacks–and 59% say they’ve seen malware attacks increase in volume and severity.

This helps explain why organizations have made massive investments in cybersecurity solutions. A typical SOC will generally rely on a ubiquitous set of tools; a security information and event management (SIEM) tool, a Security Orchestration & Automated Response (SOAR) platform, threat intelligence feeds, EDR, and specialist tools to monitor and manage specific aspects of the computing environment. These include vulnerability management solutions, corporate email and messaging systems, applications, the cloud environment, user access, and security controls such as firewalls.

While they are all critical, those tools don’t provide a unified view of the enterprise environment—and thus they increase the risk of blind spots that could invite attacks and, worse, successful breaches. That’s why so many security leaders are turning to XDR.

How XDR works

XDR takes raw data collected across the environment, it can detect bad actors that are using legitimate software to gain access to the system. This is something SIEMs are often unable to do. XDR performs automated analysis and correlation of activity data, allowing security teams to contain threats more effectively. For example, it can extend to include network detections, lateral movement, anomalous connections, beacons, exfiltration, and delivery of malicious artifacts.

Like EDR, XDR responds to the threat so SOC teams can contain and remove it. But XDR can respond more effectively to the impacted asset, due to its superior data collection and integration with the environment. True XDR platforms provide the holistic visibility and context that security analysts need to respond to threats in a manner that is both targeted and effective. This tailored response helps to contain not only the threat itself, but also the impact of the response on systems. Think reducing downtime on critical servers.

How you benefit from XDR

XDR's capabilities give it several tangible benefits for securing an organization's IT environment. A December 2022 Forrester Consulting study commissioned by VMware finds that 79% of respondents who aren't currently using XDR say they need to improve speed and accuracy of threat detection. What about those who have already deployed XDR? They cite improved speed and accuracy of threat detection among their top five drivers for adoption.

XDR certainly delivers those benefits. But organizations gain so much more, including:

- **Visibility and context**: Unlike EDR (which is limited to endpoints and workloads) and third-party security services (which often have a limited view), XDR provides a full, 360-degree view of the security environment. It allows security analysts to see threats—even those that leverage legitimate software, ports and protocols to gain entry—on any security layer, as well as how an attack happened, the blueprint, the entry point, who else is affected, where the threat originated, and how it spread. This additional context, as well as the analytics required to make sense of it, is crucial to a speedy response to threats.
- **Prioritization:** IT and security teams often struggle to keep up with thousands of alerts generated by their security services. XDR's data analysis and correlation capabilities allow it to group related alerts across the MITRE ATT&CK framework, prioritize them and surface only the most important ones.
- **Automation:** XDR's use of automation speeds up detection and response and removes manual steps from security processes, allowing IT teams to handle a large volume of security data and carry out complex processes in a repeatable way.
- **Operational efficiency:** Instead of a fragmented collection of security tools, XDR provides a holistic view of threats throughout the entire environment. It offers centralized data collection and response tightly integrated into the environment and security ecosystem.
- **Faster detection and response:** All these advantages add up to a more robust and effective security posture. XDR's added efficiency allows it to detect and respond to threats faster—which is crucial in today's security landscape.
- **More sophisticated responses:** Traditional EDR often responds to a threat by quarantining the affected endpoint, which is fine when that endpoint is a user device—but could pose a problem when a critical server is infected. XDR's more sophisticated capabilities and greater visibility allow it to tailor the response to the specific system and leverage other control points to minimize the overall impact.

The 3 Components of XDR

Telemetry and data analysis: XDR monitors and collects data across multiple security layers. It uses data analysis to correlate context from thousands of alerts from those layers to surface high-priority alerts.

Detection: XDR's superior visibility allows it to sift through alerts and report on those that require a response.

Response: Just like EDR, XDR has the capability to contain and remove threats it detects, as well as update security policies to prevent a similar breach from occurring again.

Key Use Cases for XDR

Threat hunting: XDR's telemetry and automation capabilities allow much of this work to be done automatically, allowing SOC teams to carry out threat hunting alongside their other tasks, intervening only when necessary.

Triage: XDR helps sift through the noise by using powerful analytics to correlate thousands of alerts into a small number of high-priority ones.

Investigation: Security teams can quickly and easily establish where a threat originated, how it spread, and what other users or devices might be affected. This is crucial to both removing the threat and hardening the network against future threats.

XDR deployment: Mistakes to avoid

XDR is a powerful security strategy—but to realize its full benefits, it's important to choose a solution that makes the most of its capabilities. When choosing a platform, keep an eye out for the following problems:

- **Lack of integration:** XDR is only effective when it is fully integrated within the IT environment. Complex integrations that require work to maintain could take time away from your IT teams and make your XDR solution less effective.
- **Insufficient automation:** Automation is one of the most powerful capabilities of XDR, so an effective platform needs to be able to adapt to current conditions and carry out a targeted response that goes beyond simply blocking traffic to the affected device.
- **Operational complexity:** A useful XDR solution needs to be cohesive and accessible to security and IT teams; otherwise, the time your team gains by implementing it will be offset by the time and effort put into learning it and setting it up.

VMware Carbon Black XDR: Where precision meets protection

Not all XDR solutions are the same. VMware Carbon Black XDR is the only XDR solution that natively combines telemetry from EDR with network telemetry, intrusion detection system (IDS) observations, network traffic analysis (NTA), identity intelligence, and more –all without requiring customers to rip and replace existing solutions or to add physical network taps to their infrastructure. Carbon Black XDR provides pervasive visibility across endpoints, workloads, networks, and users in an open ecosystem. This pervasive visibility saves time for not just SOC teams but also for NOC (network operations center) teams, who traditionally would have to provide SOC analysts with network telemetry.

By unraveling the complexities of evolving threats, Carbon Black XDR Is more than a solution: It's a strategic advantage that ensures your organization's safety with deep visibility and precision. With VMware Carbon Black XDR, you can:

- Transform your endpoints into a distributed network sensor
- Gain pervasive visibility across endpoints, workloads, networks, and users with an open scalable ecosystem approach
- Reduce blind spots and leave attackers nowhere to hide
- Deploy with no changes to infrastructure

VMware Carbon Black XDR helps close the Risk Gap

Traditional “status quo” solutions tend to lack full visibility across multiple security layers, which you need to detect and respond to threats throughout your environment.

This is **the Risk Gap**—the growing distance between an organization's status quo defenses and its exposure to directed attacks and the associated burden of meeting compliance and governance requirements. By unifying security tools to enable pervasive visibility, VMware Carbon Black XDR delivers the comprehensive context necessary to know what’s happening and to stop attacks before they move laterally.

Clearly, XDR is more than a buzzword. It’s a vital weapon in your CISO’s ongoing effort to reduce risk and operational costs–and to make life easier for SOC analysts and their colleagues.

Learn more about VMware Carbon Back XDR.

vmware® Carbon Black