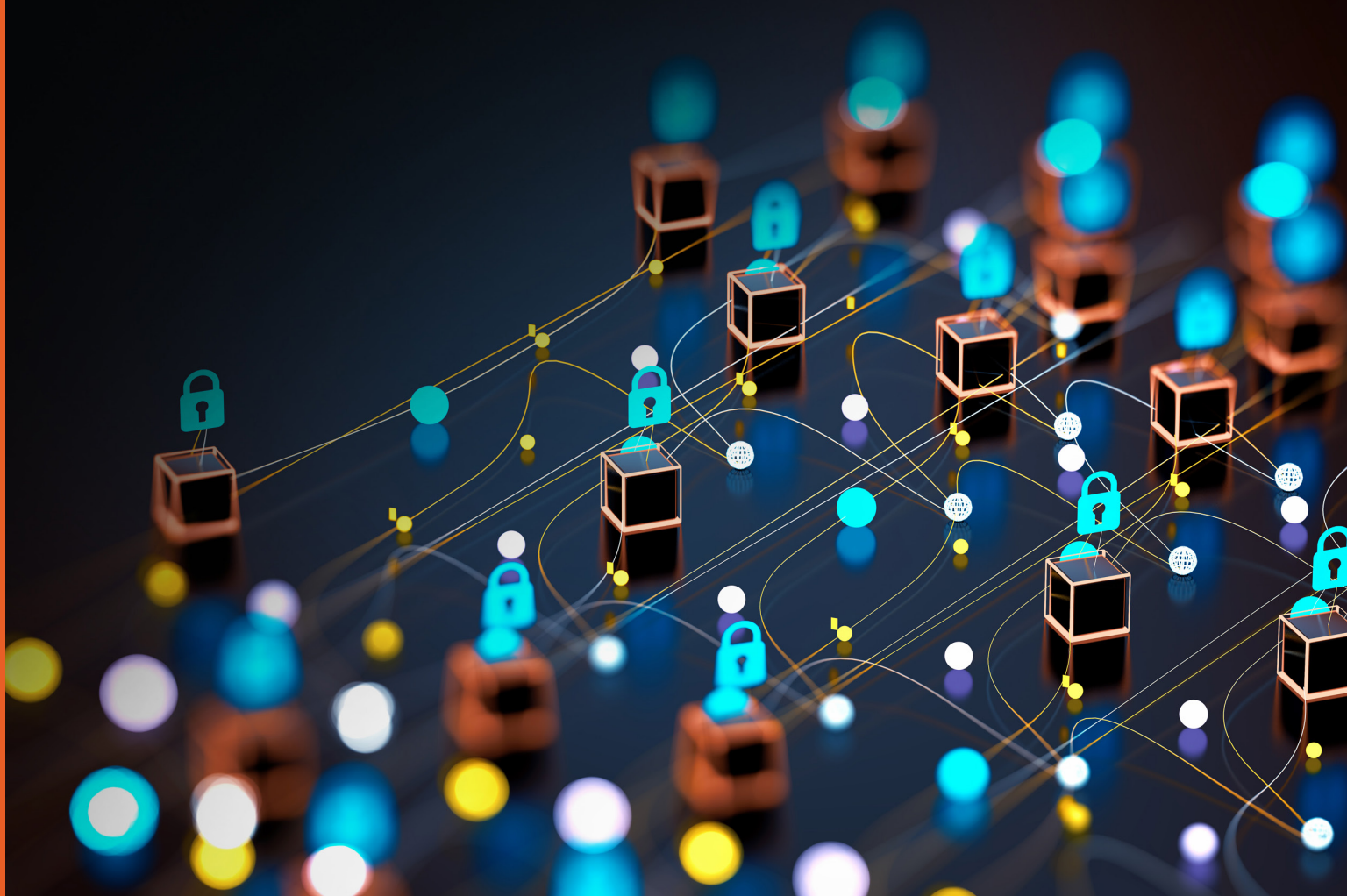
RAPID7

The Complete XDR Buyer's Guide 2023 Edition

Your guide to confidently evaluating Extended Detection and Response (XDR) for your security program



The good news: XDR can address many of the pressing issues that security teams face today like tool sprawl, alert fatigue, threat prioritization, even the skills gap. Here's what you need to know about selecting the right one for your business.

Contents

Introduction

XDR is driving consolidation (and other good things)

Gartner® identified vendor consolidation as a top security and risk management trend.[1]

Two years ago, the average enterprise was cobbling together a (sort of) full picture of their environment by managing 45 different cybersecurity-related tools. Now it's 76, with sprawl driven by a need to keep pace with cloud adoption and remote work. Security teams are spending more than half their time manually producing reports, pulling in data from multiple siloed tools. And silos present unacceptable risk.

While capabilities can vary across XDR vendors, the big idea is to integrate and correlate data from numerous security tools — and from across varying environments — to help customers prioritize and eliminate threats. Complexity and administrative work goes down and effectiveness goes up. Done well, it's low noise.

Gartner also warns that at least 30% of EDR and SIEM providers will claim to provide XDR though they'll lack core XDR functionality.[2] Caveat emptor, buyer beware. As a result, the vendor evaluation process isn't easy. But XDR is well worth it.

> **XDR allows security teams to "resolve alerts quickly and move on."**
>
> Peter Firstbrook, VP Analyst, Gartner [3]

[1] Gartner. Top Trends in Cybersecurity for 2022. Firstbrook, Olyaei, Shoard, Thielemann, Ruddy, Gaehtgens, Addiscott, Candrick. February 18, 2022.

[2] Gartner. Market Guide for Extended Detection and Response. Lawson, Firstbrook, Webber. November 8, 2021.

[3] Kyle Alspach, "XDR-driven security industry consolidation continues, with SentinelOne to acquire Attivo," VentureBeat, March 15, 2022, https://venturebeat.com/security/xdr-driven-security-industry-consolidation-continues-with-sentinelone-to-acquire-attivo/

Existing Detection and Response Technologies

Before XDR

SIEM combines log management and event management systems

Security Information and Event Management (SIEM) tools centralize, correlate, and analyze data across the IT network to detect security issues. Core functionality includes log management and centralization, security event detection and reporting, and search capabilities. This combination helps companies meet compliance needs and identify and contain attackers faster.

The first generation was introduced in 2005. Today's modern SIEMs don't quite resemble their original, log management counterparts. As the security landscape has evolved, SIEMs have evolved as well (at least, some of them have).

Next generation cloud-native SIEM solutions today include endpoint detection, accurate malware detection, comprehensive analysis of all infrastructure, fewer false positives, and the ability to learn new threats.

EDR detects stealthy compromise earlier in the attack chain

Endpoint Detection and Response (EDR) emerged in 2013 to deliver very detailed data so defenders know exactly what an attacker did to a compromised device.

EDR continuously monitors all endpoint activities to detect use of stolen credentials, unusual insider activity, lateral movement within networks, sophisticated threats like APTs, and other, often subtle anomalies. APTs in particular are engineered to get past primary defenses of endpoint protection platforms (EPP) once they're inside your environment.

This technology records all events that take place on endpoints and across the network so there's a comprehensive dataset for investigation and remediation, and is sometimes integrated with SIEM.

SOAR executes security tasks without human intervention

The term SOAR was coined in 2017 by Gartner.[4] Malicious actors became more sophisticated and the cybersecurity skills shortage really took hold, so automating both complex and basic security operations tasks became urgent. As malicious actors became more sophisticated and the cybersecurity skills shortage really took hold, automating tasks became urgent.

Security Orchestration, Automation, and Response (SOAR) refers to a collection of software solutions and tools that allow organizations to streamline security operations. It's focused on three key areas: threat and vulnerability management, incident response, and security automation.

SOAR scans for vulnerabilities, searching for logs, and handling manual, recurring, time-intensive tasks. Scarce talent is focused on impactful work and creative, human decision-making when it's most critical. When multiple teams need to collaborate, SOAR integration makes it easy.

Gartner: at least 30% of EDR and SIEM providers will claim to provide XDR though they'll lack core XDR functionality.[5]

[4] Stan Engelbrecht, "The Evolution of SOAR Platforms," SecurityWeek, Wired Business Media, July 27, 2018, https://www.securityweek.com/evolution-soar-platforms.

[5] Gartner. Market Guide for Extended Detection and Response. Lawson, Firstbrook, Webber. November 8, 2021.

Introducing Extended Detection & Response (XDR)

It's hyperefficient and it's here

XDR has arrived with answers, and some questions too

XDR is the security industry's answer as customers grapple with an increasingly complex set of environments and attacks. Everyone agrees it's promising. When everyone starts to define XDR and to debate how to evaluate it, things get tricky.

It wasn't long ago that most security leaders openly admitted they didn't have a good understanding of this much-buzzed-about acronym. "Maybe it's me," said ESG's Jon Oltsik, "but I don't think you'll be very successful when three-quarters of your customers are confused about what you are trying to sell them."[6] Today, ESG reports that two-thirds of CISOs believe they've already deployed XDR (only a handful really have).[7]

Keep your eyes fixed on the outcome, not the acronym

Forrester defines XDR as "the evolution of EDR." Others say SIEM is the foundation. In fact, Gartner says that as your operation matures into XDR you'll still need a SIEM.[8] There's debate about SIEM and XDR colliding, and separate but complementary use cases. IDC defines XDR as a "cloud-native, API- enabled platform that ingests and correlates telemetry from various sources to detect cyberattacks."

Have confidence in this: XDR optimizes threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation. Most important? It's the outcome it delivers to you: fast, effective decision making.

Cyberattacks are now the C-suite's #1 concern.[9] Your mission is to keep the CEO off the evening news (and maybe even get home in time to see it).

> **XDR goes beyond unifying data to correlate, attribute, and enrich diverse datasets into a single, harmonious picture.**

[6] Jon Oltsik, "8 Things CISOs Want To Hear From XDR Vendors," CSO, IDG Communications, April 22, 2021, https://www.csoonline.com/article/3615703/8-things-cisos-want-to-hear-from-xdr-vendors.html.

[7] ESG Research. SOC Modernization and the Role of XDR. Oltsik. October 24, 2022.

[8] Gartner. Market Guide for Extended Detection and Response. Lawson, Firstbrook, Webber. November 8, 2021l.

[9] "25th Annual Global CEO Survey," PwC, January 17, 2022, https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html.

What matters is what XDR does and lets you do

XDR is a cloud-native platform that optimizes threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation. It simplifies SecOps and can address many of the pressing issues that security teams face: alert overload, difficulty in prioritizing threats, tool sprawl.

And since threats are coming from anywhere and everywhere, multiple sources of telemetry and complete visibility give you a cohesive view of related events. You can detect threats faster, and elevate outcomes.

User-endpoint telemetry

User telemetry provides insights on file and network access, registry access or manipulation, memory management, and start-and-stop activity. Unusual behavior detected can include processes that spawn command shells, memory injection attempts, or accessing unusual file locations.

Server-endpoint telemetry

Server telemetry provides information on extremely differentiated data. Since servers handle so much crucial organizational functionality, XDR telemetry can help prioritize investigations and remediations of incidents on a more macro level.

Network telemetry

Network telemetry provides insights on traffic, particularly a sudden increase in volume, new network protocols, or anomalous privilege escalations. Advanced encryption methods can often hinder deeper network analysis that could otherwise thwart threat actors. But make no mistake, combined with endpoint telemetry network traffic analysis can be a cornerstone of an XDR offense.

Cloud telemetry

Cloud telemetry provides insights on infrastructure. This can include detecting security anomalies for any cloud workloads or components deployed. Attackers specifically targeting an organization's cloud components can easily gain access with the proper credentials, so it is of critical importance to leverage the advanced detection technology of XDR to hunt threats faster and fortify cloud environments.

XDR delivers the context a defender needs quickly, expert recommendations on what to do, and the response capabilities to do it.

XDR can extend your team, too

Does your in-house operation need 24x7x365 expert staff?

Because of cybersecurity's well-known 0% unemployment and the relentless pace and sophistication of attacks, Managed Detection and Response (MDR) is having a moment.

XDR security can also be delivered to you as an end-to-end, turnkey service. The right MDR partner can be a game-changer, with always-on threat detection, incident validation, and response, such as threat containment in your environment, as an extension of your in-house team. Some providers offer features like threat intelligence, human-led threat hunting, behavior analytics, automation, and more to your capabilities.

ESG reports a 85% of surveyed organizations currently use or plan to use MDR for their security operations. And 88% say they will increase their use of it in the next 1-2 years.[10]

The right MDR with transparent XDR can upskill your team

An MDR provider should be a true partnership, sharing XDR technology with your in-house operation, and working in step with your team. Your analysts should be able to observe your environment, do their own threat hunting, and more – whatever level of collaboration you'd like to see. (For the MDR Buyer's Guide, go here.)

Need to create, accelerate, or augment existing in-house security operations? Consider MDR expertise using XDR technology.

[10] ESG Research. SOC Modernization and the Role of XDR. Oltsik. October 24, 2022.

Requirement Overview

XDR requirement: Full visibility

Integrated threat intelligence

You stay ahead of attacks by knowing in near-real time about real-world attacks others have prevented. Expect continuously updated internal and external threat intelligence gathered across a global network (e.g. open source communities), Indicators of Compromise IOCs and customized coverage should be at your fingertips.

Unified and correlated telemetry

XDR integrates telemetry from across your modern environment and provides correlation and context to data sources. This helps you better understand how various events are linked and when certain behavior/movement is suspicious based on context. The important thing? Teams get more data (and actionable data) so they can confidently, efficiently and effectively detect and respond to threat.

Analysis of internal and external threat landscape

Typically, detection and response tools provide insight on an external attacker. It's not enough. Security teams need internal and external threat intelligence, including the deep and dark web analyzed against internal components identifying anomalies and potential malicious behavior. XDR should give you complete visibility across your attack surface so you know where threats are coming from and where they're moving towards.

XDR requirement: Faster detection with threat hunting and analytics

Intuitive dashboards and reporting

Dashboards and reports take event data and turn it into informational visuals to assist in seeing patterns, or identifying activity that is not forming a standard pattern. You get a visual overview of your environment, and insight into critical details, and the information necessary to make actionable decisions.

XDR should invite you to create custom dashboards easily from a library of pre-built, curated ones. Add, edit, resize, and rearrange data visualization cards to tailor the data view to you and your organization's needs.

Breadth of detection content

With a variety of detection types—User Behavior Analytics (UBA), Attacker Behavior Analytics (ABA), and custom detections— teams are covered against it all, from lateral movement to unique attacker behaviors and everything in between.

Defense in depth helps ensure that organizations are protecting their systems as effectively as possible. Teams need to account for potential failures. By leveraging various detection types, security professionals can reduce the chance of a single point of failure occurring in their systems.

Prioritization and vetting of alerts

While security teams need to review and triage alerts, massive numbers of them based on activity will never be high profile threats, which can quickly lead to burnout. Look for strong signal-to-noise with XDR and security alerts that are quantified and scored.

XDR requirement: Smarter responses and incident investigations

High context investigations

To successfully conduct an investigation, it's important to understand the context in which that incident took place. Teams can make informed decisions to properly respond to threats and attacks.

XDR accelerates incident response by eliminating context switching and ensuring teams have high context and correlated investigation details that blend relevant data from across different event sources into a single coherent picture.

Automated responses

Automation reduces the repetitive, manual work and enables teams to focus on what matters most to their organization. XDR should deliver these automation features, including prebuilt workflows for containing threats on an endpoint, suspending user accounts, and integration with ticketing systems – and let you automate new tasks.

Also, look for expert guidance and one-click response playbooks. Analysts should always know what to do next.

XDR Use Case 1:

Unified, Modern Environment Visibility

The challenge

Your attack surface sprawls with endpoints, networks, users, cloud infrastructure, private applications. Security has too many tools and layers up and down the stack, with mounting pressure from digital transformation, remote and hybrid work, the convergence of IT and IoT initiatives, and more.

Why it's important

You can't stop what you can't see: single-screen, 360o, end-to-end visibility is required for fast, informed decisions that eliminate threats.

Key considerations

- Which data does the XDR solution capture?
- Does it capture both external and internal data? Spanning across risks and threats?
- How do security professionals engage with the captured data? Is it easy and intuitive?
- Can the XDR solution detect attacker tactics and techniques through MITRE ATT&CK Evaluations?

XDR Use Case 2:

Enriched Alerts with Relevant Threat Intelligence

The challenge

Security teams need more, relevant, and actionable data so they know which events are threats and which aren't. Without immediate, comprehensive context, how can analysts make fast, data-driven decisions?

Why it's important

Incident triage and investigations need to move fast. And applied threat intelligence lets you be proactive by delivering an always-on stream of new research about malware, tactics, techniques, and procedures (TTPs), phishing scams, and other threat actors. XDR should give you access to dark web chatter and details on what's coming next.

Key considerations

- What are the XDR vendor's sources of threat intelligence?
- Does the vendor do its own threat hunting? Who and how often? How are you updated?
- Is the XDR vendor able to group related alerts from various sources into a single incident?
- How does the XDR vendor prioritize alerts?
- Are you able to get alerts on known malicious objects with IoC rules?

XDR Use Case 3:

Robust 3rd Party Integrations with Leading Cloud Providers

The challenge

Cloud providers are a critical part of your organization's business ecosystem. People use integrations and applications every day, and you need to continuously collect, analyze, and read activity data (securely of course).

Why it's important

To detect and respond to cloud-based attacks with confident XDR outcomes, you'll want extensions, integrations and workflows that include Google, AWS, Teams, Cisco, Slack, Jira, Proofpoint, and more.

Key considerations

- Does the XDR solution provide visibility across a modern environment, including cloud?
- Does the XDR solution integrate with major cloud providers such as AWS, Azure, GCP, etc.?
- Are you able to see the movements and understand the intent of a threat across your environment?
- Will you get a real-time view of your cloud environment or just information based on hourly or daily scans?

XDR Use Case 4:

High Efficiency, Early Detection

The challenge

Noisy, false positives: teams are driven nuts by alerts, learn to ignore them, or change the criteria and sensitivity (which means you can miss things).

Why it's important

Security programs succeed when they have a library of curated, high-fidelity detections backed by threat intelligence that they can trust out-of-the-box. Anything else is a low performance guesswork.

Key considerations

- Is the XDR solution able to detect threats and terminate them early in the attack kill chain?
- Does the XDR solution provide a high signal-to-noise ratio?
- How are detections curated and by whom?
- Can security professionals get a view of the threat as well as relevant information to not only assess the alert but suggestions for moving forward?

XDR Use Case 5:

Efficient Incident Investigation & Response

The challenge

Your mean time to respond (MTTR) performance probably doesn't hit your goal. And it's very likely that your staff is too small and too inexperienced.

Why it's important

Time is money in detection, and it's the same with your response. XDR should ensure fast, effective investigations by providing all the relevant facts, events, and intelligence around an attack, playbooks, and one-click automation.

Key considerations

- Does the XDR solution provide all the relevant actionable information for security professionals to make data-driven decisions?
- Is Security Orchestration, Automation, and Response (SOAR) a part of the XDR solution?
- Does the XDR solution allow for end-to-end management of incidents?

Conclusion

There really isn't any more time to waste

The cybersecurity skills gap isn't going anywhere. And the most tech savvy generation in human history – Gen Z, the latest entrants to adulthood and the workforce – will not take jobs that turn their lives shambolic.

XDR, done properly, reorganizes your efforts, and simplifies, guides, and creates success.

As you start to evaluate your options, consider making a list of the things that most challenge you and most matter to you. Rapid7 works in genuine partnership with our customers. We're ready to talk when you are.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/