RAPID7

4 Ways XDR Levels Up Security Programs

Yes, it's early-stage, a buzzy acronym, and sometimes all talk. But it's real.

omniIT
INNOVATIVE TECHNOLOGY

TABLE OF CONTENTS

INTRODUCTION

In the beginning, we all worried about evil

Before networks, we password-protected computers. When the Department of Defense research project DARPA started connecting us, worms, viruses, and other malicious activity appeared. A NASA researcher invented the firewall. Hackers organized into groups and evolved faster than security solutions.

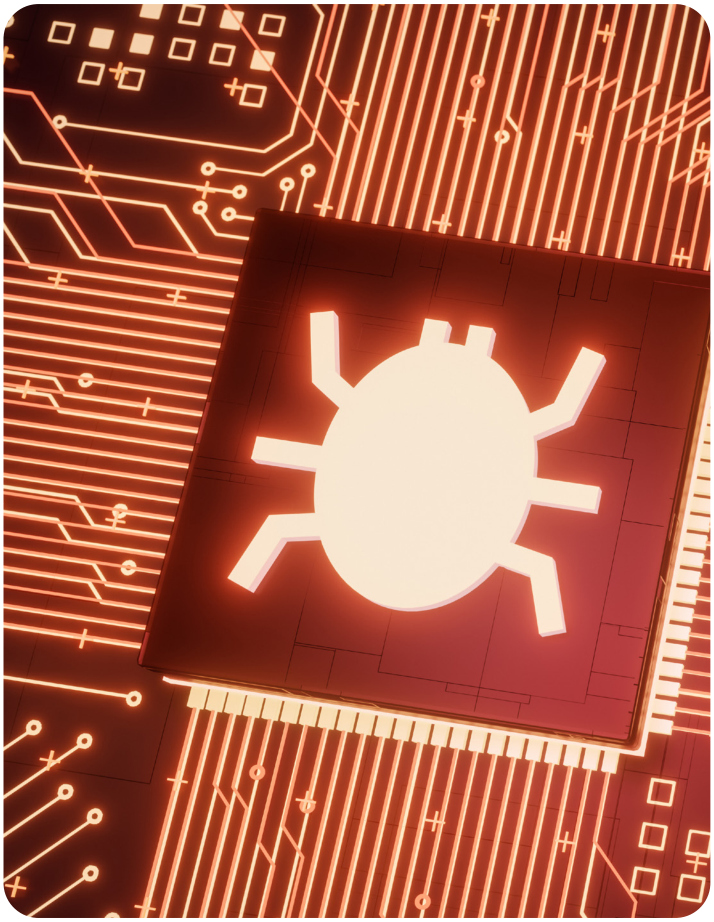
Eventually the perimeters we all protected stretched until they broke: by 2023, there will be three times more networked devices on Earth than people.[1] Which leaves us a new question: did we really connect everyone and everything without a plan?

XDR has arrived with answers (and also, questions)

Forrester defines XDR (Extended Detection and Response) as "the evolution of EDR" (Endpoint Detection and Response). XDR is a cloud-native platform that optimizes threat detection, investigation, response, and hunting in real time, with scalability and opportunities for automation.[2]

Gartner says XDR is a "detection and incident response tool that natively integrates multiple security products into a cohesive security operations system." And if vendors don't deliver on the promise? A single pane of glass? More signal, less noise? Gartner believes XDR "will die in the Trough of Disillusionment." [3]

Some vendors continue to debate exactly what XDR is. Is it a product? An approach to security? Some use the XDR acronym, but it's not clear they have the capability yet. Others say that, whatever it is, it's on a collision course with SIEM (Security Information & Event Management). In fact, maybe it is a SIEM. It's confusing out there. This guide is here to help.



> **90% of organizations have set aside a budget for XDR in the next year.[4] But most vendors are, objectively, at the start of their XDR journeys.**

[1] Cisco AIR white paper, 2020
[2] Forrester, analyst Allie Mellen blog, August 2, 2021
[3] Gartner, "Advancement Insight for Extended Reaction and Detection," 2020
[4] Dave Gruber, cybersecurity analyst, Enterprise Strategy Group (ESG), August 2021

WHAT IS XDR?

XDR promises to shift the advantage from attackers to you

What eludes security teams isn't really the attackers themselves — it's time.

- **Evil is escalating, there are too many alerts to chase**
- **The cybersecurity talent shortage is in its fifth straight year[5]**
- **Globally, 3.5 million cybersecurity jobs remain unfilled[6]**
- **Every organization is pursuing digital transformation**
- **Data is rushing to the cloud, where security is quite glibly called "everyone's job"**

A whopping 83% of organizations are increasing their threat detection and response budgets, 29% admit to "blind spots," 29% need to decrease time to recovery, and 27% want help knowing which threats to prioritize.[7]

The list could go on, but you get the idea. Without the time, resources, or better technology to do it all, you make trade-offs every day. This creates opportunities for attackers to get in. And for your life to tumble downhill fast, too.

Don't think of it as a product or a "solution"

Yes, XDR aggregates threat detection and response across multiple controls, bringing multiple sources of telemetry into a single view. By unifying relevant security data from across your modern environment to detect real attacks, you get high context, actionable insights and can extinguish threats fast.

But the fact is, it's better to think of XDR as an approach to your security: it's a goal vendors achieve, and ultimately you achieve.

The foundation of XDR is SIEM and EDR with curation

Traditional SIEMs were built to consume massive amounts of log data and provide security teams with analytic capabilities. But from there, figuring out where the bad guys were and what to do was typically up to you.

The big data collection and analytics capability of SIEM remains a critical part of the security infrastructure: search, dashboarding, compliance, reporting, custom rules, and forensics capabilities are necessary. But now, leveraging an XDR approach with cloud SIEM at the core can take the high effort analysis and configuration off your plate (and let you put a good BBQ beef brisket on it).

An XDR approach is about curation: giving teams native, relevant, and actionable telemetry, high fidelity detections, and prescriptive response playbooks. Sounds like a strong approach, right? Let's dive into the key benefits.

> **80% of organizations are using their SIEM primarily for detection & response.[8]**

[5] "The Life and Times of Cybersecurity Professionals 2021," ISSA and ESG
[6] 2019/2020 Annual Cybersecurity Jobs Report
[7] Enterprise Strategy Group (ESG), February 2021
[8] The Forrester Wave™: Security Analytics Platforms, Q4 2020

FOUR KEY BENEFITS OF XDR

1. Simplified SecOps, Elevated Outcomes

Security analysts track multiple threat intelligence feeds and are drowning in alerts, most of which must be processed manually. Alerts are up 47% since the COVID-19 pandemic began, with remote workforces, and more apps and devices than ever.[9]

Mature XDR lets you focus on detections, not deployments

Most security products on the market stick you with arduous deployments, long ramp-ups, and heavy configurations. Hey, you've got time for that.

As you look at ways to begin your own XDR journey, ask the hard questions about deployment. A cloud-native infrastructure will mean it will scale with your business easily. SaaS delivery and software based data collection will make it easy to use and great for cross-team collaboration.

Also, the point of XDR is to free you and your time. So an interface and query language that isn't intuitive for even your newest analysts doesn't cut it.

Empower every analyst to be an expert

With a good XDR approach, analysts have curated detections, comprehensive investigations, automated response recommendations at their fingertips, and detailed, highly correlated threat events to accelerate their work. Analysts can review open incidents, zero in on the highest priorities, and respond with just a few clicks. And they'll always know where to go next.

XDR should also fundamentally change data analysis, investigation, and threat hunting. For example: analysts should be able to quickly consume massive amounts of data — and without massive amounts of analysis, use intuitive search and visualizations to identify anomalies or unique policy violations.

Get precise insights faster

The most adept of your adversaries need about 20 minutes to gain access to your environment. They wander around for an average of 11 days before they're detected, moving laterally and doing reconnaissance, credential dumping, data exfiltration.[10]

The mature XDR approach gives you the speed you need to garner insights, eliminating endless log searches, convoluted queries, and data splunking. Millions of daily events in your environment can be correlated directly to the users and assets behind them.

> **Most security professionals admit to ignoring alerts or adjusting policy to reduce them. XDR is the end of all that.**

[9] ThreatPost, 2021 Cybersecurity Trends

[10] Sophos, "The Active Adversary Playbook 2021"

FOUR KEY BENEFITS OF XDR

2. Scalable Security Transformation

As organizations pursue digital transformation and the cloud becomes the default, security teams struggle to bring legacy tools along. They manage an array of solutions, cobbling together a (sort of) full picture.

XDR should be the end of tab-hopping, providing a comprehensive, scalable hub so the modern Security Operations Center (SOC) can secure everything, no perimeter.

Unlock XDR across the modern environment

Your adversaries are lone hackers, groups like EvilCorp, and nation-states. And your list may even include Bob down the hall who keeps falling for phishing emails. To complicate matters, the COVID-19 pandemic changed everything:

- **Suddenly, nearly everyone was sent home to work**
- **Cloud adoption accelerated**
- **Lots of us installed new programs to support new ways of working**
- **The threat landscape now included the kids using your computer**
- **Personal machines accessed data outside the traditional protection of corporate networks**
- **The Internet of Things (IoT) — which has just begun to grow — has exposed devices to attacks that a few years ago would never have discussed**

Hybrid remote and office work is here to stay and so is the security challenge. XDR arrived none too soon, unifying the telemetry across remote users, network data, endpoints, cloud, and whatever comes next.

Scale and analyze data faster

Good XDR is cloud-native and cloud-scalable. It can be expanded without technical limitations so you can manage growth or decrease resources efficiently, as needed. SaaS delivery will facilitate collaboration across the office or around the world. XDR should mean everyone is looking at the same interface and data all the time - no versioning.

Also, consider the different ways security teams search and visualize data. XDR should give you intuitive query languages, automatic attribution of data to specific users, correlation across events. Ideally, you'll find stuff in whatever way you like, with a lot of the parsing and analysis done for you.

XDR promises to remove the steep analytical requirements that burden security teams, so you can focus on recognizing and stopping evil fast.

Identify and anticipate threats early in the attack chain

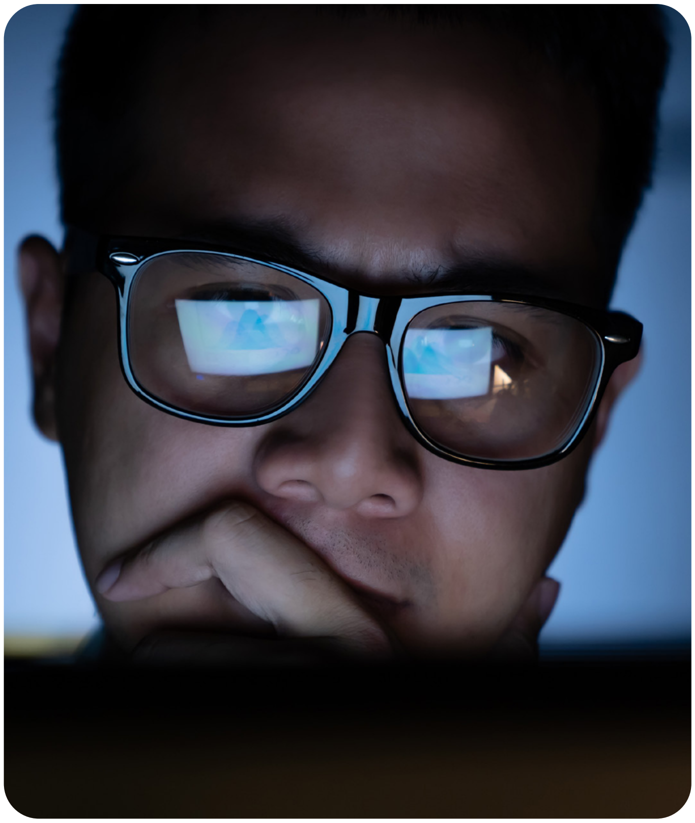
Good XDR collects endpoint data and combines it with network, cloud, sophisticated UEBA, and curated threat intelligence. This means no more parsing through tons of endpoint logs to find what matters. You get early detections and the ability to observe behaviors on your endpoints that indicate compromise. You'll see suspicious activities — local log deletions, privileged escalations — and shut down attacks before any damage is done.

> **Tab-hopping is officially called "multi-tasking" which is a myth: you're changing goals, and doing it so fast you don't notice your loss of focus.**

FOUR KEY BENEFITS OF XDR

3. High-Fidelity Detections

Many XDR technologies promise to unite disparate telemetry sets — but if it's simply aggregation without correlation and curated detections, you may only be getting SIEM or EDR with a swanky, fresh label. You want to trust detections out of the box, and XDR promises the end of chasing false alarms.



Stay ahead of new threats and tune out the noise

XDR promises you visibility into your entire attack surface and also reduces alerts dramatically.

It processes vast amounts of data from endpoints, network telemetries and other event sources or telemetry, information about vulnerabilities, threat intelligence, and users. This multi-layered detection approach is fused with machine learning and algorithms that enable you to zero in on real threats and feel confident acting on them.

Get meaningful insights across your environment

If there's a "secret sauce" to great XDR it's a correlation engine that unifies disparate data points and millions of daily events into one cohesive picture. (By the way, XDR is too elegant for only one secret sauce.)

You should see risk highlighted across your organization, where to search prioritized, and risky users and misconfigurations automatically identified. Analysts can expand, pivot, and focus on high-context, well-correlated investigations.

> **Here's a benefit: 95% of security professionals work way more than a 40-hour week, and 40% say it affects personal relationships.[11] Get life back.**

[11] CISO Stress Report,

FOUR KEY BENEFITS OF XDR

4. Accelerated Incident Response

Too many gloss over the R in XDR, assuming that with the right detections in place the right response actions will follow suit. This is not the case. When you're breached, the last thing you want is an analyst running around trying to figure out what to do next.

Expedite detection and response by eliminating context switching

When any of us jump between tasks and tools, it impacts our productivity. We may think we're great at it, but we're not. Multi-tasking increases the brain's production of our primary stress hormone, cortisol, and eventually makes us quite miserable.

It's hard to imagine anyone with a more fragmented workday than a cybersecurity analyst.

The promise of XDR is the basics, automated: enriching data, isolating endpoints, blocking IP addresses, quarantining systems, and more. "The best XDR solutions," says CSO Online, "will let security teams customize and build on these turnkey automated remediation tasks while providing new ones on a regular basis."[12]

Know what to do next, extinguish threats faster

Security teams need efficiency. Good XDR requires a prescriptive approach to attacks, which can be the difference between a breach and a non-event. Expect prebuilt workflows for things like:

- **Containing threats on an endpoint**
- **Suspending user accounts**
- **Integrating with ticketing systems like Jira and ServiceNow**

You should also expect to kickoff workflows and expert response playbooks with the click of a button. XDR opens up end-to-end automation opportunities and reduces alert noise and remediation time.

[12] 5 Observations about XDR, by Jon Oltsik, CSO, September 20, 2021

MAKING A CHOICE FOR YOUR BUSINESS

XDR is a big advance, a buzzy acronym, and sometimes a broken promise

The industry is talking all-XDR all the time, debating exactly what it means, and telling you it's the answer to your sleep disturbances. As you talk about it, here's our best guidance:

1. Ask: what's in the box?

Many vendors promising XDR outcomes are assuming you'll integrate (and pay for) the many other technologies you'll need for the complete telemetry set and extended environment visibility. Endpoint agents. Network sensors. Cloud hookups. User behavior analytics. Log ingestion.

These are all critical pieces of the XDR puzzle. It's important to understand what's included and what you may be expected to bring yourself. Too many integrations may start to negate the consolidation and efficiency benefits of XDR.

2. Understand the detection philosophy

One of the most anticipated outcomes of XDR: a promise to end noisy alerts and deliver the high-fidelity detections often recognized with EDR tools across the broader environment and data set. However, it's important that you understand exactly how detections are curated and maintained.

Ask about the methodology, threat intelligence, and diligence behind the detection library. It will offer insight into its efficacy and scalability. Understand the philosophy and proof-of-concepts. Experience detections firsthand. Look at objective third-party analysis or reviews to learn more.

3. Don't forget the "R"

What's automated? Are analysts primed for action? Is guidance embedded? XDR takes the monotonous, repetitive work away and leaves you the interesting work you trained for, that you enjoy. People seem to spend a lot of time on the X. Remember the R.

ABOUT RAPID7

We were doing XDR before XDR was even a thing

Rapid7 has been building a safer cyberworld for more than 20 years. We remember when email first proliferated and a hacker hijacked an AOL account to unleash the Melissa virus. At the time, the call for help went to the FBI.

Since then, security has been Rapid7's mission and expertise.

One reason we're so ahead and so trusted? We vet ideas and "drink our own champagne" in our global MDR (Managed Detection and Response) SOC. We understand your user experience.

It's also why, six years ago, Rapid7 was able to lay the foundation for XDR. We purpose-built the cloud-native InsightIDR platform to give security teams time to focus on successful, proactive, and complete threat detection and response programs. Today, it's your freedom to focus on what matters most (including lunch).

InsightIDR unifies SIEM and XDR outcomes for customers

Analysts say XDR and SIEM are on a collision course. We prefer to call it a unified approach.

Most SIEMs out there were not built to support detection and response for today's modern environments. InsightIDR was.

Users detect 73% earlier, and contain 71% faster. And in a recent survey of customers in our Voice program (a group that provides input as we develop new ideas) 42% said they are using InsightIDR to achieve XDR right now. They're also benefiting from our internal and external threat intelligence that stretches into the deep web and dark web.

Open-source wins: security is a challenge too big to face alone

The methodology behind InsightIDR, the work of our Threat Intelligence and Detections Engineers, and our Detections Library are informed by exceptional open-source platforms:

- **Metasploit is the world's most used penetration testing framework**
- **Velociraptor is a library of forensic artifacts, providing next generation endpoint monitoring, investigations, and incident response**
- **Project Sonar scans the public internet to gain insights into global exposure to common vulnerabilities**
- **Project Heisenberg builds relationships with other internet-scale researchers and forums for collaboration and confirmation when new threats arise**

Rapid7 believes in the power of collaborative communities. We're all connected to everyone and everything anyway. It's how evil arose in our midst and how the good guys will prevail.

Like you, security is what we do

It might be why we understand your stressors, your aspirations, and why we care about the 0% unemployment rate in cybersecurity that contributes to your too-long hours.[13] And it may be why our XDR journey started in 2015, not last March.

Want more information? Visit Rapid7.com, today.

[13] 2019/2020 Annual Cybersecurity Jobs Report