XDR Buyer’s Guide
Navigating the emerging Extended Detection and Response market like a pro
Why does the world need another security approach?

Even the most confident, well-funded security teams know that they are facing overwhelming external pressures. The attack surface is constantly expanding. The recent shift to remote and/or hybrid work has added a new layers of complexity. The sheer volume of off-the-shelf malware produces a sea of endless alerts. And the incompatibility in security tool sets means that context is isolated in silos, automation is out of reach, and each investigation requires a significant, manual effort that is beyond the resources of the average team.

With so much friction between both people and technology, its no wonder that security efficacy is stagnant and average dwell times remain around 280¹.

So what exactly is XDR and why do I care?

As defined by Gartner, Extended Detection and Response (XDR) is a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components². This is a significant paradigm shift from existing strategies where most detection and response is done within individual product silos and teams. The unity that XDR offers impacts several key areas for every security team:

First, it delivers fast value for teams with little-to-no calibration. For teams that have already done work setting up a SIEMs or SOAR, XDR platforms build on those benefits.

Second, it solves the alert fatigue that plagues so many teams – as the platform aggregates and correlates all the disparate events caused by the same breach into incidents.

Third, it delivers out-of-box automation and orchestration elements that help teams to eliminate routine tasks for their daily activities.

1. Ponemon Institute research featured in IBM’s Cost of a Data Breach Report 2020

---

Understanding Extended Detection and Response (XDR)
5 key elements of XDR done right

1. Coordinated telemetry from all the areas in your environment where threats can appear

Fundamental to XDR must be breadth of visibility and depth of insight. At this moment in time, vendors are positioning their existing products as a key component in XDR. But for XDR to have the impact it promises, “extended” really needs to mean everywhere threats show up. True XDR must bridge together not just data, but telemetry from the widest variety of security control categories, data repositories, and threat intelligence vendors to determine the likelihood of malicious intent. The goal must be a holistic view of your network, the activities that take place on it, and anything happening on devices that come and go. After this is achieved, speed of analysis is key. It’s not enough to just dump system data in yet another data lake, you need intelligent data streams that provide teams with context-rich telemetry.

Key Functions
1. Full environment insights
2. Actionable telemetry
3. Reliable sources of data

Questions to Ask
• How does your solution provide me with more than just visibility into my network?
• Are you using a data lake to deliver insights or something that provides more impactful telemetry?
• How does your solution ensure I’m getting context into all the endpoints, devices, and traffic coming into and out of my network?

2. Leverage detection functionality from your existing investments, regardless of vendor

While Gartner mentions proprietary components in their definition, it’s absolutely critical for an XDR platform to be designed in an open manner, easily connecting with 3rd party technology. Each component in your security stack has unique detection elements – IoC detection, machine learning, behavioral analytics, etc. – that become more powerful when brought together. Weak signals from silos become strong signals in aggregate. Detection working together is a critical to XDR, so make sure the platform you choose works with your whole stack.

Key Functions
1. Leverage your solutions
2. Vendor agnosticism
3. Ingests 3rd party analytics

Questions to Ask
• How many of my existing investments can your approach to XDR leverage?
• How are your detection technologies different than others that are on the market?
• Which of your solutions have out of the box integrations with one another?
Unified context from reliable sources of truth that support fast, accurate response

Unifying insights from the network, endpoint, and email (to name a few) provides a more accurate understanding of what has happened, how it progressed and what steps need to be taken in order to remediate the threat. Unity isn’t the point – there is no XDR without native response capabilities, preferably within just a click or two. Response actions like isolating a host, deleting a malicious email out of all inboxes, or extract observable need to be readily available. XDR should also make it easy to create custom response actions so that teams can evolve their security as time goes on.

Key Functions
1. Context-driven intelligence
2. Multiple sources of truth
3. Improve MTTD

Questions to Ask
- Can I use your XDR to understand the impact of a threat, the scope of the breach, and take single click actions from one interface?
- What sort of threat intelligence is feeding your detection and where does that intelligence come from?
- How do you validate the data sources you use in your solution?

Ongoing opportunities for automation and orchestration for machine-scale problems

Following convoluted, manual, and outdated workflows exposes your business to the risk of threats and human error. You want an XDR that makes automating repetitive security tasks easy while not requiring a massive learning curve to get that automation up and running. Automating critical workflows frees up your teams across the full lifecycle to go from discovering an alert to taking a response action quickly. This means time and energy to put towards critical tasks like threat hunting.

Key Functions
1. More automation
2. See through security noise
3. Overcome human-scale limitations

Questions to Ask
- For your 3rd party integrations, do vendors’ API changes break your automation scripts?
- How can you help me orchestrate and automate workflows across my existing solutions?
- How does your solution support monitoring to and from cloud-based workloads?
A single investigative viewpoint that makes isolation and remediation simpler

With telemetry unified from all the detection and response elements, you want a single console for direct remediation, access to threat intelligence, and tools to provide a unified view of an alert. With all this information in one place, the knowledge and experience on your team ability to do threat investigation scale with greater efficiency, efficacy, reliability, and speed. XDR should expand an essential tool in an incident response team’s kit, providing them with visibility into additional telemetry beyond the endpoint in one place. XDR that facilitates threat hunting through models such as MITRE ATT&CK will make hypothesis-driven threat hunting accessible for those new to the process.

### Key Functions

| 1. | Improve MTTR |
| 2. | Enable more threat hunting |

### Questions to Ask

- Where does your solution aid and/or accelerate remediation?
- How does your solution help my team in their threat hunting endeavors?

---

Moving forward with XDR

We recommend working with XDR stakeholders to determine which XDR strategy is right for you. Always be listening for a prioritization of automation and integration.

Start with these questions but make sure you understand the various functions and requirements of your current stack so you can achieve measurable outcomes and improve ROI.

1. How do you provide Network Detection and Response within XDR?
2. How will you help me take better, more informed security actions?
3. How does your XDR help me to automate blocking or remediation?
4. Which of your solutions have out of the box integrations with one another?
5. How does your XDR approach set me up to achieve security outcomes like SASE or ZTNA?
Cisco + XDR

Only Cisco delivers on the promise of XDR today, through unified context, correlated detections, and faster responses. How? Our platform, SecureX, is already built into Cisco security products and easily integrates with solutions in your environment using open APIs. This results in a unified detection and response layer that correlates telemetry from all control points and makes taking actions easier. High-fidelity alerting helps you prioritize incidents. A single investigative viewpoint helps you do root cause analysis and informs the right next action, which you can take with one click. Built-in orchestration enables you to automate responses and offload routine tasks. So your teams are more effective and have time to do proactive security work like threat hunting.

No more running in place – It’s time to race.

To learn more about Cisco’s approach to XDR, connect with your sales rep today!
Use this table format and the questions listed previously in this document to prepare for conversations with XDR vendors. Choose 8-10 questions that are most relevant to your environment and copy/paste them below.

<table>
<thead>
<tr>
<th>Question/Notes</th>
<th>Compelling answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td>Yes</td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
<tr>
<td>Question:</td>
<td></td>
</tr>
<tr>
<td>Notes:</td>
<td></td>
</tr>
</tbody>
</table>