CISCO
SECURE

XDR Buyer's Guide

Navigating the emerging Extended Detection and Response market like a pro

cisco SECURE

Understanding Extended Detection and Response (XDR)

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 recent shift to remote and/or hybrid work has added new layers of complexity. The attack surface is constantly expanding. There are endless alerts. Security tools are incompatible. With so much friction between both people and technology, it's no wonder that security efficacy is stagnant and average dwell times remain around 280 days[1].

This new normal calls for security resilience – the ability to protect the integrity of every aspect of the business to withstand unpredictable threats or changes and then emerge stronger. And security resilience calls for more than what the past has offered.

Key reasons to explore XDR:

1. Reduce alert fatigue
2. Speed time to detect
3. Increase visibility across tools
4. Gain better threat context

So what exactly is XDR and why do I care?

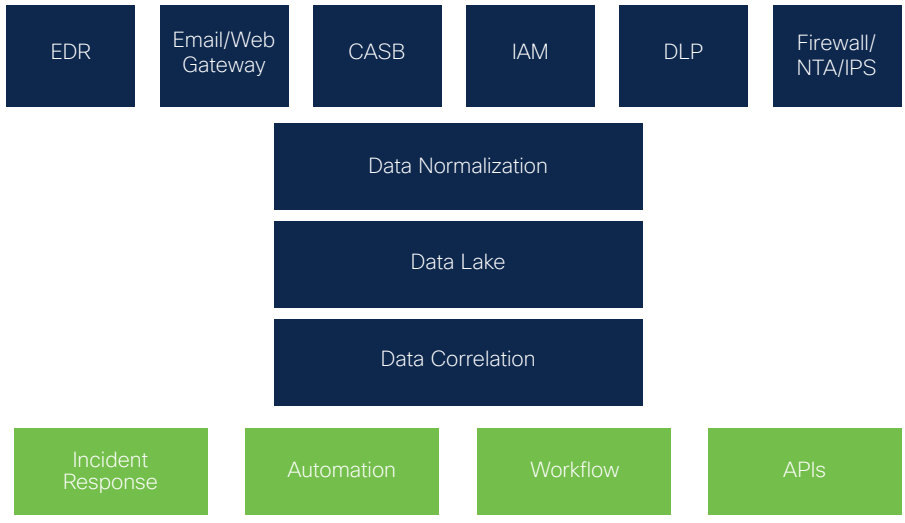
While integration with native security point solutions within XDR is extremely beneficial, it is also critical for an XDR platform to leverage and easily connect to existing third-party technology, providing better ROI and richer context to all data sources. This is a significant paradigm shift from 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.

XDR conceptual architecture



1. PonemonInstitute research featured in IBM's Cost of a Data Breach Report 2020

cisco SECURE

5 key elements of XDR done right

1 Coordinated telemetry from anywhere in your environment

Fundamental to XDR must be breadth of visibility and depth of insight. At this moment in time, vendors are positioning their existing products as key components in XDR. But 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. With XDR, organizations can close the gaps and achieve a pervasive defense throughout the ecosystem with an open, integrated platform across campus, data center, cloud, and cloud edge. With the rich context drawn from each of these integrated solutions inside of XDR, you can find vulnerabilities and fix them faster.

Key Functions	Questions to Ask
Full environment insights	How does your solution provide me with more than just visibility into my network?
Actionable telemetry	Are you using a data lake to deliver insights or something that provides more impactful telemetry?
Reliable sources of data	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 of XDR, it's critical for an XDR solution to be built with an open platform approach that easily connects with third-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 critical to XDR, so make sure the platform you choose works with your whole stack.

Key Functions	Questions to Ask
Leverage your solutions	How many of my existing investments can your approach to XDR leverage?
Vendor agnosticism	How are your detection technologies different than others that are on the market?
Ingests third-party analytics	Which of your solutions have out of the box integrations with one another?

3 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. Effective XDR requires native response and remediation capabilities, such as isolating a host or deleting a malicious email out of all inboxes. Ideally, these actions would be possible with just a click or two. XDR should also make it easy to create custom response actions so that teams can evolve their security as time goes on.

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

4 Ongoing opportunities for automation and orchestration for machine-scale problems

Following convoluted, manual, and outdated workflows exposes your business to threats and human error. The right XDR platform will have strong orchestration and automation capabilities and make repetitive security tasks easier and more efficient without a massive learning curve to get up and running. Automating critical workflows helps team respond to alerts faster, leaving more time and energy for critical tasks like threat hunting.

Key Functions	Questions to Ask
More automation	For your third-party integrations, do vendors' API changes break your automation scripts?
See through security noise	How can you help me orchestrate and automate workflows across my existing solutions?
Overcome humanscale limitations	How does your solution support monitoring to and from cloud-based workloads?

5 A single investigative viewpoint that makes isolation and remediation simpler

XDR should expand the essential tools in an incident response team's kit, providing them with visibility into additional telemetry beyond the endpoint. A single console enables direct remediation, access to threat intelligence, and tools to provide a unified view of an alert. Plus, 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 – and make it easier to anticipate what's next.

Key Functions	Questions to Ask
Improve MTTR	Where does your solution aid and/or accelerate remediation?
Enable more threat hunting	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. Ensure that potential vendors are prioritizing 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. Does your XDR offering cover Network Detection and Response, and other security layers like email, cloud, and firewall?
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 tie into other security initiatives like SASE or Zero Trust?

cisco SECURE

XDR + Security Resilience

Today, uncertainty is a guarantee, from operations to finances to supply chain. Companies are investing in resilience – the ability to withstand unforeseen shocks and emerge stronger. But these will fall short without investment in security resilience.

There are five dimensions of security resilience:

1. Activate billions of signals across your ecosystem
2. Anticipate what's next through shared intelligence
3. Prioritize alerts wtih risk-based context analysis
4. Close gaps across the ecosystem with integrations
5. Grow stronger through orchestration and automation

The right XDR platform delivers on each of these dimensions. And only Cisco delivers on the promise of XDR today, through unified context, correlated detections, and faster responses.

SecureX, our built-in security platform, is an entitlement with all Cisco security products, and easily integrates with solutions in your environment using open APIs. This unified detection and response layer correlates telemetry from all control points into a single investigative viewpoint and makes prioritizing and taking actions much simpler. Also, built-in orchestration enables you to automate responses and offload routine tasks to free up teams for more proactive duties, 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!

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

cisco SECURE

XDR Vendor Validation Worksheet

Use this table format and the questions provided 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.

Questions/Notes	Compelling answers
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	
Question:	
Notes:	


CISCO
SECURE