

It's Time for Simpler Detection and Response

Security teams face an expanding threat landscape and an environment that is rife with friction – making security efficacy elusive. Incompatible tools and siloed context force teams to toggle between consoles, trying to manually correlate attack information. This approach isn't viable and pushes dwell times up to 280 days on average¹.

To simplify detection and response, security teams need to be able to turn weak signals into reliable alerts and act on them with confidence. Extended Detection and Response (XDR) helps to provide this confidence with context gathered from every corner of the environment consolidated into a single view that is easy to explore and act on.

Cisco offers the broadest XDR functionality available

The Cisco XDR solution...

- Unifies first- and third-party detection technologies
- Accelerates response action throughout the full security environment
- Deploys in any environment, regardless of vendor
- Normalizes and centralizes data efficiently
- Leverages machine learning and automation across the environment
- Facilitates proactive threat hunting and automated incident response



Cisco delivers the fastest route to XDR

Our approach to XDR starts with an evolution of two existing detection and response frameworks – EDR and NDR. By bringing these two technologies together, and providing them with telemetry and insight from the rest of your security environment, we can deliver:²



Reduction in analytics effort per incident



Decreased risk of a data breach



Decreased cost of a data breach



Unified, enriched
context



Accurate, correlated
detections



Faster, orchestrated
responses

“You understand threats more when you have this amazing visibility instead of poking around. It’s like going from a little flashlight to a floodlight.”

IT Administrator
Healthcare Organization

8 elements Cisco brings to XDR no other vendor can touch

1. We deliver the best and most comprehensive XDR capabilities across detection, investigation, and remediation.
2. Our cloud-native platform is built into all of our products, setting the foundation for an extensible XDR approach.
3. We have invested billions in integrating third-party solutions, so you don’t have to.
4. We have all of the pieces you’ll need for XDR, security, and more, in one place.
5. We have a superior ability to ingest telemetry from more data inputs than any other vendor.
6. We offer powerful automation to solve human-scale problems.
7. We support every layer of detection with the most actionable, comprehensive intelligence.
8. Our platform-based portfolio positions you for further security transformation.

¹Ponemon Institute research featured in IBM’s Cost of a Data Breach Report, 2020. | ²The Total Economic Impact™ of Cisco SecureX, Forrester, July 2021.

Ready to start your XDR journey?

- Sign up for [SecureX](#) and start integrating your environment
- Get 30 days of premiere [endpoint visibility](#) through Cisco Secure Endpoint