Simplify Security Operations with Cisco XDR

Detect more, act faster and elevate productivity

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritise and respond to the most sophisticated threats. Integrating with the broad Cisco security portfolio and a collection of key third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

Designed by security practitioners for security practitioners, Cisco XDR helps analysts aggregate and correlate data from multiple sources into a unified view to streamline investigations, reduce false positives, prioritise alerts and achieve the shortest path from detection to response.

Built-in automation, orchestration and guided remediation recommendations help analysts to automate repetitive tasks and mitigate threats more effectively, freeing up time and resources to focus on other critical security tasks.

The data-driven Cisco XDR approach allows SOC teams to define the most impactful events and focus remediation strategies there first, strengthening the organisation's overall security posture and increasing resilience.

Benefits

Unify visibility regardless of vendor or vector to avoid blind spots

Gain visibility and identify threats across network, cloud, endpoint, email and applications for effective security across multi-vendor, multi-vector environment.

By correlating data from multiple disparate detection technologies into a unified view, Cisco XDR enables faster, more simplified investigations and streamlines incident response.

Accelerate threat detection and response to act on what truly matters

Correlate detections across multiple telemetry sources to prioritise threats by greatest risk.

By leveraging AI and machine learning, Cisco XDR enables high-fidelity correlated detection, reduces clutter and effectively aligns security risk with business risk.

Automate response with evidence backed recommendations to minimise impact

Remediate threats confidently using automation and guided response recommendations across all relevant control points.

By compressing investigation time and accelerating responses, Cisco XDR stops levels-up SOC teams and builds resilience.

Deliver comprehensive threat detection and response actions with data-backed insights

Detect complex threats sooner

- Cisco XDR offers the broadest range of built-in integrations across endpoint, email, network, cloud, firewall and more, as well as select third-party integrations for the most flexible, scalable and effective XDR strategy.
- Leverage telemetry from on-prem networks and public and private clouds to detect threats on managed and unmanaged devices and gain critical context when correlating events, including where attacks start and how they spread through the network.
- Talos threat intelligence strengthens detection capabilities, so analysts gain an unrivalled collection of actionable information to expose known and emerging threats with deeper context and awareness of real-world threat behaviour.

Prioritise threats by impact and act on what matters most, faster

- Risk-based prioritisation helps SOC analysts focus on the alerts that pose the greatest threat, allowing them to take rapid and effective action. This unique approach provides a unified view of alerts, prioritised by real-world severity.
- Reduce the mean time to respond (MTTR) with guided responses for identification, containment, eradication and recovery from threats, and embedded response actions, which combine to enable consistent and effective decision making.

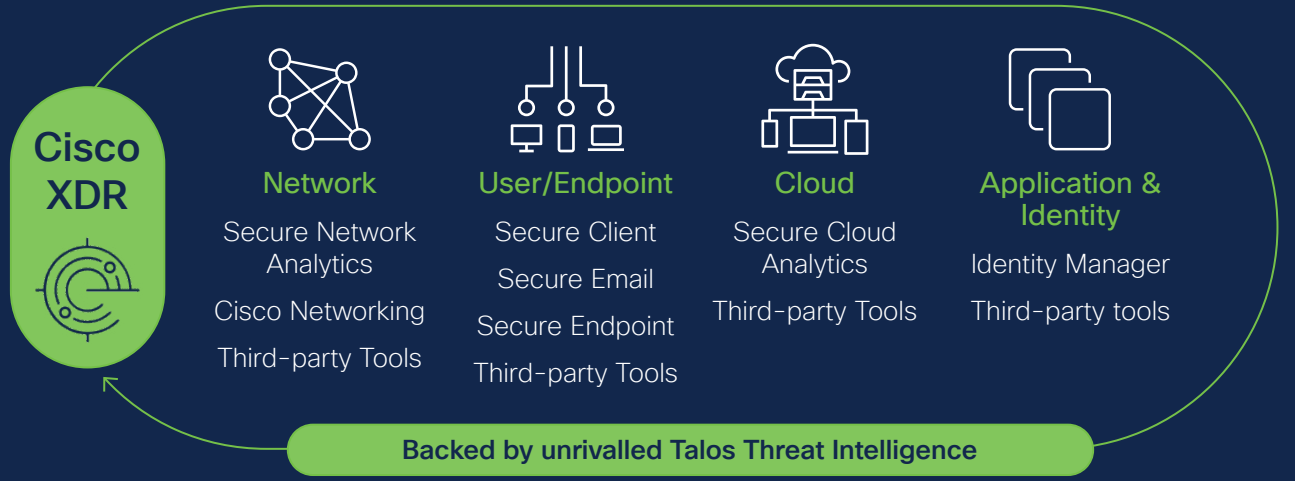
Accelerate response times

- Rapidly remediate threats with built-in response actions and orchestration. With Cisco XDR, SOC teams can leverage a range of pre-built or customisable orchestration workbooks to help shut down threats and mitigate risk with just a few clicks.
- Boost limited resources for maximum value by automating repetitive and time-consuming tasks and providing SOC teams with out-of-the-box best practices. When automation is not suitable, Cisco XDR provides guided response suggestions and recommendations to help SOC analysts take effective response actions.
- Quickly push response actions across a broad range of security tools through deep integrations with varying security control points, both built-in Cisco solutions and third-party. Take a proactive role in threat hunting by surveying across disparate alert logs as you learn of new tactics, techniques and indicators of compromise.

Streamline Investigations:

- Simplify and compress investigation times with unified context and progressive disclosure techniques. Cisco XDR shows analysts the information they need to address current tasks without inundating them with extraneous data leading to analysis paralysis. When needed, more information to enrich investigations is always just a click away.
- SOC analysts can aggregate alerts, global intelligence and local context to understand root cause and full scope of impact, to always be action ready.

Delivering XDR to meet you where you are



Leveraging the Cisco Security Cloud: Combining core capabilities including a frictionless experience, open and extensible ecosystem and automation

Find out more about Cisco XDR: cisco.com/go/xdr