

# Simplify Security Operations with Cisco XDR

Detect more, act decisively, and elevate productivity

Cisco has changed the way security teams approach threat detection, investigation, and response (TDIR). Our cloud-based extended detection and response (XDR) solution is the fastest, easiest way to integrate TDIR into your security posture and simplify security operations, providing a streamlined approach to quickly detect, prioritize, and respond to sophisticated threats.

Cisco XDR collects and correlates data and telemetry across multiple sources – network, cloud, endpoint, email, identity, and applications – to provide unified visibility and deep context into advanced threats while reducing time-consuming false positives. One of the most open and flexible solutions, Cisco XDR includes built-in native network detection and response (NDR) capabilities while seamlessly integrating with Cisco security solutions and several third-party offerings. Powered by rich network insights, this multi-vector, multi-vendor approach provides more holistic visibility and detection capabilities than endpoint-centric XDR tools.

The [Cisco AI Assistant in XDR](#) helps make defenders more efficient by guiding response actions, reducing human error, and making remediation faster and more consistent. And built-in automation, orchestration, and customizable playbooks help defenders automate repetitive tasks and mitigate threats more effectively, empowering analysts of all levels with the details they need to take decisive action.



## Benefits



### Avoid blind spots

Simplify investigations with a unified view of high-fidelity, correlated detections across both Cisco and third-party telemetry sources.



### Accelerate threat detection and response

Drive analyst efficiency and speed through the Cisco AI Assistant in XDR, which provides data-driven guidance, next steps, and remediation tactics.



### Fortify your defense

Evaluate your environment to address gaps in security coverage using MITRE ATT&CK mappings.

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

### Detect complex threats sooner

- Gain a comprehensive view of attacks with deep network insights and visibility via integrations across the Cisco security portfolio and several third-party tools.
- Expose gaps in threat detection using actionable insights from network-powered defense, Cisco Talos and third-party threat intelligence, and MITRE ATT&CK coverage maps.

### Act on what matters most, faster

- Reduce mean time to respond (MTTR) with AI-driven guidance for identification, containment, eradication, and recovery for consistent and effective decision-making.
- Simplify investigations with unified context, prioritized alerts, and progressive disclosure to avoid information overload.

### Simplify network and security operations

- Unify visibility and context with enriched network telemetry from Meraki MX devices,

including traffic patterns, device behavior, and system changes.

- Reduce the risk of successful attacks while identifying potential threats earlier by combining network logs from Meraki MX devices with security telemetry within Cisco XDR.

### Accelerate response times

- Quickly remediate threats using customizable orchestration playbooks and deep integrations across various security tools.
- Get the right threat context and practical advice to guide next best actions via Cisco AI Assistant in XDR.

### Stop ransomware in its tracks

- Prevent data loss by triggering your backup and recovery solution to create a snapshot of high-value assets at the first signs of a ransomware attack.
- Restore your last known good configuration, getting your organization up and running with as little downtime and data loss as possible.

## Flexible options for every business

Cisco XDR is available in three license tiers:

- **Cisco XDR Essentials** delivers full XDR capabilities and integrates across the Cisco security portfolio. Ideal for Cisco-only environments.
- **Cisco XDR Advantage** adds integrations with select third-party security tools. Best option if you have a mixed security stack.
- **Cisco XDR Premier** delivers the full Advantage capabilities as a Managed Extended Detection and Response (MXDR) service provided by Cisco security experts.

You can purchase Cisco XDR a la carte or as part of the Cisco Breach Protection Suite.

## Find out more.

Cisco XDR: [cisco.com/go/xdr](https://cisco.com/go/xdr)

Cisco AI Assistant: [cisco.com/go/ai-assistant](https://cisco.com/go/ai-assistant)

Highlighted Features	Essentials Tier	Advantage Tier	Premier Tier
Security data analytics and correlation	x	x	x
Incident prioritization and AI-guided recommended actions	x	x	x
Talos and third-party threat intelligence integrations	x	x	x
Threat hunting with automated MITRE ATT&CK mappings	x	x	x
Customizable orchestration playbooks	x	x	x
Cisco NDR natively built in (Secure Cloud Analytics)	x	x	x
Simplified network and security operations (Meraki MX integration) <sup>1</sup>	x	x	x
90-day data retention via provided data repository standard <sup>2</sup>	x	x	x
Third-party data and telemetry integrations		x	x
Managed Extended Detection & Response			x
Talos Incident Response			x
Cisco Technical Security Assessments			x

For a complete list of features, visit the [Cisco XDR web page](#).

<sup>1</sup> Integration requires Meraki MX Advantage licensing tier

<sup>2</sup> Longer data retention periods available