Cisco XDR

Cisco Partner
https://cs.co/1page

Cisco XDR is an Extended Detection and Response solution that lets customers leverage the broad Cisco Secure portfolio of solutions and their existing investment into their company's security infrastructure. This helps customers detect, investigate, and prioritize incidents better with added telemetry sources and contextual insights.

Benefits:

Detect the most sophisticated threats: Gain visibility and actionable threat intel with a multi-vector, multi-vendor approach optimized for open environments.

Act on what truly matters: Equip your security teams with effective threat prioritization, streamlined investigations, and evidence-backed recommendations.

Elevate productivity: Eliminate noise and ease the skill shortage with automation capabilities to boost your security teams resources for optimal value.

Build resilience: Close security gaps and anticipate and prepare for future threats. Get stronger every day with continuous improvement.

Cisco Integrations: *(Includes all tiers. lists not comprehensive)*

- Attack Surface Management
- Cisco Duo
- Cisco Orbital
- Cisco Threat Intelligence API
- Cisco Vulnerability Mgmt.
- Cyber Vision
- Email Threat Defense
- Meraki
- Secure Access
- Secure Email (Appliance)
- Secure Email & Web Mgr.
- Secure Endpoint
- Secure Firewall
- Secure Malware Analytics
- Secure Network Analytics
- Secure Web Appliance
- Secure Workload
- Security Cloud Control
- Splunk Cloud
- Umbrella
- WebEx
- XDR Analytics (Cloud Analytics)

Third-Party Integrations: [1]

- APIVoid
- AbuseIPDB IPChecker
- AlienVault
- Check Point
- Cohesity Data Cloud
- CrowdStrike
- Cybereason
- Darktrace /NETWORK
- Elastic Cloud
- ExtraHop Reveal(x)
- Ivanti Neurons (MDM)
- Jamf Pro
- Jira Pro
- Microsoft Defender
- Microsoft Graph Security API
- Microsoft Intune
- MISP
- PagerDuty
- Palo Alto Networks Firewalls
- Palo Alto Networks Cortex XDR
- Proofpoint Threat Protection
- Pulsedive
- Radware Cloud DDoS Protection
- Radware Cloud WAF Service
- Red Sift Pulse
- Rubrik Security Cloud
- SentinelOne
- ServiceNow
- Shodan
- Slack
- Threatscore
- Trend Vision One
- urlscan.io
- VirusTotal
- VMWare Workspace One
- xMatters
- Zendesk

Many more…

[1] Included in Cisco XDR Advantage - Check Integrations docs page for capabilities.

Cisco XDR Packages:

	Essentials	Advantage	Premier (min 1000 users)
Security Analytics & Correlation	✓	✓	✓
Threat Intelligence	✓	✓	✓
Threat Hunting	✓	✓	✓
Incident Response Actions	✓	✓	✓
Incident Prioritization	✓	✓	✓
Incident Management	✓	✓	✓
Case Prioritization	✓	✓	✓
Asset Context	✓	✓	✓
Custom Automation Workflows	✓	✓	✓
Automation Workflow Exchange	✓	✓	✓
Cisco Software Support Services (SWSS) Enhanced	✓	✓	✓
XDR Forensics		✓	✓
Third-Party Integrations		✓	✓
Cisco Managed Detection and Response (MDR)			✓
Cisco Talos Incident Response (Talos IR)	Available as add-on	Available as add-on	✓
Cisco Technical Security Assessment (CTSA)			✓

Components:

XDR Analytics (Previously Cloud Analytics): Provides visibility and threat detection across all major cloud environments (e.g., AWS, Azure, GCP).

Network Visibility Module (NVM): Collect flow context from an endpoint (via AnyConnect/Secure Client) and provide visibility into network connected devices.

Conversation Starters:

- Do you know where you are most exposed to risk?
- How good are you at detecting attacks early?
- Do you prioritize attacks that represent the largest impacts to your business?
- How quickly can you determine the full scope and entry vectors of an attack?
- How fast can you respond to an attack? How much can you automate?

Resources:

- SalesResources
- Order Guide
- Buyers Guide
- Licensing
- At-a-Glance
- Integrations
- Integration Status
- Ransomware Recovery
- Secure Trials Console
- PoV Setup Guide
- Premier Service
- XDR Status
- XDR Resources
- What is XDR?
- Public page

Example SKU: ***XDR-SEC-SUB***