Cisco XDR

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.

Integrations: *(lists not comprehensive)*

Cisco: [1]

- Attack Surface Management
- Cisco Defense Orchestrator
- Cisco Duo
- Cisco Orbital
- Cisco Threat Intelligence API
- Cisco Vulnerability Management
- Email Threat Defense
- Identity Services Engine [3]
- Meraki
- Secure Client
- Secure Email (Appliance)
- Secure Email & Web Mgr.
- Secure Endpoint
- Secure Firewall
- Secure Malware Analytics
- Secure Network Analytics
- Secure Web Appliance (SMA)
- Secure Workload
- Umbrella
- XDR Analytics (Cloud Analytics)

[3] Relies on XDR Analytics

Third-Party Integrations: [2]

- Akamai
- Amazon GuardDuty
- AWS
- Check Point
- Cohesity
  - Data Protection
- CrowdStrike
- Cybereason
- Darktrace Respond
- Exabeam
- ExtraHop Reveal
- Fortinet FortiGate
- Google Chronicle
- Google Cloud Platform
- IBM X-Force Exchange
- Jamf Pro
- LogRhythm
- Microsoft 0365
- Microsoft Azure
- Microsoft Azure AD
- Microsoft Defender
- Microsoft Intune
- Microsoft Sentinel
- Palo Alto Networks AutoFocus
- Palo Alto Networks Cortex XDR
- Palo Alto Networks NFGW
- Proofpoint Email Protection
- Qualys IOC
- Radware Cloud DDoS Protection
- Radware Cloud WAF Service
- SentinelOne Endpoint Security
- ServiceNow SecOps
- Shodan
- Splunk Relay module
- Trend Micro Vision One
- VirusTotal
- VMWare Workspace ONE

Many more...

Cisco XDR Packages:

	Essentials	Advantage	Premier
Security Analytics & Correlation	✓	✓	✓
Threat Intelligence	✓	✓	✓
Threat Hunting	✓	✓	✓
Incident Response Actions	✓	✓	✓
Incident Prioritization	✓	✓	✓
Asset Context	✓	✓	✓
User Context	✓	✓	✓
Custom Automation Workflows	✓	✓	✓
Automation Workflow Exchange	✓	✓	✓
Cisco Software Support Services (SWSS) Enhanced	✓	✓	✓
Third-Party Integrations		✓	✓
Cisco Managed Detection and Response (MDR)			✓
Cisco Talos Incident Response (Talos IR)			✓
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).

Telemetry Broker: Optimizes telemetry pipelines for the hybrid cloud.

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:

- SalesConnect Order Guide
- XDR Buyers Guide
- Licensing
- EDU Licensing
- At-a-Glance
- Integrations
- XDR PoV for Partners
- XDR Premier Service
- XDR for Dummies (e-book)
- Ransomware Recovery
- XDR Resources
- Self Guided Demo
- What is XDR?
- Public page

[1] Included in all tiers | [2] Included in Cisco XDR Advantage - Check Integrations docs page for capabilities.

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