Cisco XDR

Security Operations Simplified

October 2025

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco XDR Product Overview 4

Security Operations Simplified **4**

Use Cases 5

Accelerate Incident Responses with Streamlined Workflows and Prioritization **5**

Built-in Automation, with Low-to-No-Code Customization **5**

Conduct Truly Extended Detection and Response **5**

Assess Detection Coverage Across Your Environment **5**

Key Capabilities 6

Security Analytics and Correlation **6**

Network Telemetry Ingestion **6**

Asset Context **7**

Custom Automation Workflows **7**

Automation Workflow Exchange **8**

Incident Prioritization **8**

Incident Response **8**

Threat Intelligence **9**

Threat Hunting and Threat Investigation **9**

Digital Forensics and Incident Response **9**

Third-Party Telemetry **10**

Integrations 10

Application, Identity, and Device Management Integrations **10**

Collaboration, ITSM, and Ticketing **11**

Cloud Security Integrations **11**

Email Telemetry, Security, and Response Integrations **11**

Endpoint Telemetry, Detection, and Response Integrations **12**

Enterprise Backup **12**

Network Detection and Response Integrations **12**

Next-Generation Firewall Telemetry and Response Integrations **13**

Public Cloud Integrations **13**

Security Information and Event Management Integrations **13**

Threat Intelligence Integrations **14**

License Options 15

Cisco Managed Extended Detection and Response 16

Cisco Talos Incident Response Retainer Service 17

Cisco Technical Security Assessment 17

© 2025 Cisco and/or its affiliates. All rights reserved.

Support 17
Cisco XDR Software Support Service..... 17
Cisco Software Support Enhanced (included)..... 17
Cisco Software Support Premium (add-on)..... 17

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco XDR Product Overview

Security Operations Simplified

Cisco XDR simplifies security operations, accelerates responses, and empowers Security Operations Center (SOC) teams with AI-driven and proactive threat detection and response. It is designed to address the challenges faced by security analysts and offers a cloud-native, extensible solution that brings data from multiple security tools, and applies machine learning and analytics to arrive at correlated detections and accelerated response.

By moving beyond endpoint detection and response (EDR) or security information and event management (SIEM) centric approaches, Cisco XDR shifts the focus from endless investigation to remediating the highest priority incidents with evidence backed automation, helping SOC teams act with greater speed, efficiency, and confidence. While traditional SIEM technology provides management for log-centric data and measures outcomes in days, Cisco XDR focuses on telemetry-centric data and delivers outcomes in minutes.

Cisco XDR natively analyzes and correlates the six telemetry sources that Security Operations Center (SOC) operators say are critical for an extended detection and response (XDR) solution: endpoint, network, firewall, email, identity, and DNS. With Cisco XDR, security teams can detect threats beyond the endpoint by making telemetry and insights from other sources, including the network, equally foundational. Through turnkey, curated integrations with third-party security products as well as the extensive Cisco Security solutions portfolio, Cisco XDR delivers a seamless installation into existing architectures and delivers consistent outcomes regardless of vendor or solution.

Cisco XDR correlates telemetry, rather than just aggregating data. By doing so, it reduces false positives and delivers prioritized incidents based on potential risk and impact to your environment. In other words, it lets your teams focus on the threats that matter. And it enriches detections with threat intelligence from Cisco Talos to add context and asset insights, ensuring you are always seeing the complete picture. Cisco XDR Forensics extends the role of XDR in the breach response value chain by embedding equitable forensic capabilities within the platform to speed up forensic evidence collection and to accelerate response with targeted action through its remote shell capability. By doing XDR right, security teams can confidently respond to attacks, increase SOC efficiency, and automate tasks for a more proactive approach to security.

Cisco XDR is designed to deliver greater efficacy, better experience, and greater return on investment from your existing security stack through four key value pillars:

1. Detect the most sophisticated threats: You can investigate every corner of your environment by connecting the broad end-to-end Cisco security portfolio as well as a wide array of third-party security tools. Also, by providing the underlying threat intelligence from Cisco Talos to enrich incidents with added context and asset insights, we can detect and respond to the most sophisticated threats impacting a wide security stack, regardless of vendor or vector.
2. Act on what truly matters, faster: Prioritize the threats that pose the greatest material risk to your business. Validate impact of incidents through comprehensive forensic evidence. Unified context to streamline investigations, and evidence-backed recommendations.
3. Elevate productivity: Filter out the noise so that your analysts focus on what truly matters. Boost limited resources for maximum value. Built-in tools for equitable digital forensics and incident response. Automate tasks and focus on strategic tasks.

© 2025 Cisco and/or its affiliates. All rights reserved.

4. Build security resilience: Close security gaps. Anticipate what's next through actionable intelligence. Get strong every day with continues, quantifiable improvement.

For more information, go to cisco.com/go/XDR.

Use Cases

Accelerate Incident Responses with Streamlined Workflows and Prioritization

By conducting the investigative process for you, Cisco XDR eliminates work effort on the part of Level 1 and Level 2 analysts, allowing incident response to begin immediately. Cisco XDR then provides clear guidance on the appropriate response to take based on the incident experienced, so analysts can act immediately to prevent further impact and eradicate the incident in your environment. XDR Forensics adds built-in capabilities to your incident workflow to comprehensively collect and preserve key digital forensic artifacts from impacted endpoints and remote shell capabilities to enable immediate targeted response actions to contain and eradicate the threat. Finally, by prioritizing incidents based on the material risk to your organization associated with respective MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) and the value of the affected assets, Cisco XDR ensures that your organization focuses on the potentially most impactful incidents.

Built-in Automation, with Low-to-No-Code Customization

Detection without response is insufficient, so response capabilities need to be built into an XDR solution. Enhancing this standard, Cisco XDR includes expertly curated automation and orchestration, extending response capabilities to automated workflows, reducing the effort required by SOC teams and analysts. When organizations need to expand on the built-in capabilities provided out-of-the-box by Cisco XDR, they can create and save customized workflows for executing their specific SOC processes. Workflows can be built using drag and drop actions in the low-to-no-code editor. Workflows are triggered through the guided Playbook, Automation Rules (with Incident, Email, Webhook and Schedule triggers), and more methods.

Conduct Truly Extended Detection and Response

How can you possibly evaluate incidents and threats to your environment if you are not doing so across all possible vectors, security data sources, non-security pertinent data sources, and countermeasures? Cisco XDR delivers native integrations with Cisco security solutions as well as non-Cisco tools across key vectors of endpoint, email, cloud, and network. Cisco XDR provides and maintains Cisco-curated integrations for market-leading third-party security countermeasures in endpoint, email, cloud, firewall, and network through established development agreements with these key partners, offloading the requirement for your organization to do so, to fully leverage your technology investments.

Assess Detection Coverage Across Your Environment

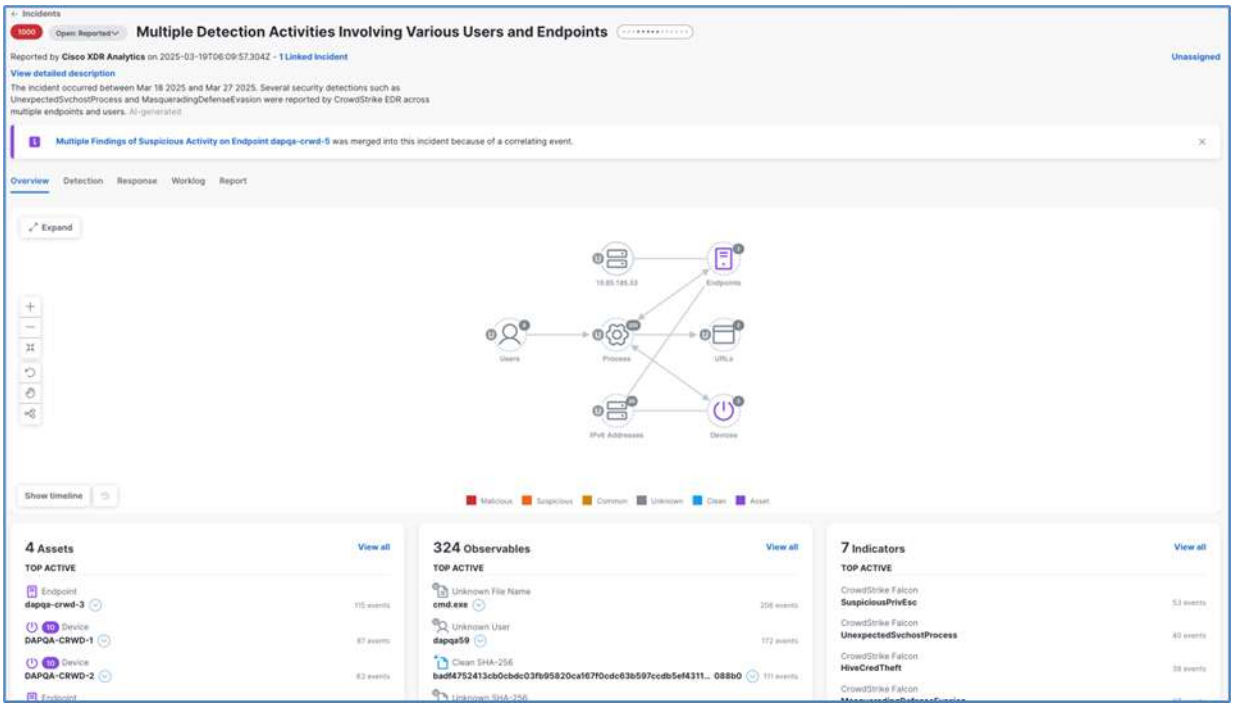
Cisco XDR helps you assess the amount of coverage that your Cisco XDR and relevant integrated products provide with respect to MITRE ATT&CK, the industry standard framework, by modeling scenarios of detection coverage from a combination of your tools and against selected adversarial MITRE Techniques and Tactics. For selected integrations, starting with Cisco Secure Endpoint, you can also assess the current dynamic configuration and what impact it has on the overall coverage of the solution. With Secure Endpoint Configuration Insights, you will receive actionable insights about the MITRE Techniques and Tactics that you have visibility into based on whether you have enabled the relevant product features or left them disabled. It provides continuous assessment against best practices and highlights endpoints and policies that you should review and adjust to improve MITRE coverage by optimizing your configuration.

© 2025 Cisco and/or its affiliates. All rights reserved.

Key Capabilities

Security Analytics and Correlation

Cisco XDR has a built-in analytics and correlation engine, which can ingest a vast variety of events and telemetry. This ranges from EDR security events to public cloud and private network flow logs and more. It is possible to ingest both Cisco and third-party data into Cisco XDR (depending on license tier).



This analytics engine provides users with fully correlated incidents based on a variety of detections and correlation mechanisms. Security events are correlated over time revealing the bigger picture of a multi-stage attack. Incident activity is plotted on a timeline and visualization is provided by an attack graph, so that the analyst quickly understands the who, what, where, when of an attack. Incidents are assigned a priority score on a scale from 1 to 1000 that reflects the risk associated to the detection, which is related to the material risk associated with respective MITRE ATT&CK TTPs and the value of the affected assets. This incident also correlates related alerts based on common indicators to show the entire attack mapped to the MITRE ATT&CK framework.

Network Telemetry Ingestion

SecOps teams often face “blind spots” within their environments as the number of user devices on the private network grows and more workloads shift to the public cloud. Many attacks require adversaries to interact with the network to achieve their goal. Cisco XDR can collect network traffic from on-premises networks and public clouds to identify hosts, build an understanding of normal host behavior, and generate alerts when device behavior changes in a manner that is relevant to an organization’s network security. These alerts subsequently feed into the incident correlation process and are used for attack chains. In Cisco XDR, most of the native detections are mapped to MITRE TTPs, offering an industry-standard way to understand and respond to findings.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco XDR can ingest public cloud logs (AWS, Google Cloud Platform, and Microsoft Azure) using an agentless monitoring of workloads and API integrations to deliver threat detection and configuration monitoring. It integrates with additional Cloud Service Provider APIs (for example in AWS with VPC Flowlogs, Cloud Trail, Cloud Watch, Config, Inspector, Identity and Access Management (IAM) Lambda, and many more) to look for adversary behavior on the network and infiltrating deep into an organization's cloud environment.

To monitor on-premises networks, Cisco XDR includes an **XDR Connector** (formerly Secure Cloud Analytics Sensor / ONA), which can ingest network telemetry from many sources, like flow data (e.g., NetFlow, IPFIX, etc.), SPAN/mirror port traffic, and NGFW log information. The XDR Connector sends on-premises network telemetry to the SaaS-based data repository where this data is stored, analyzed, and correlated with all other available telemetry. Alternatively, customers can purchase **Cisco Telemetry Broker** (CTB) to direct network telemetry to Cisco XDR and other downstream consumers.

Cisco XDR also includes the **Network Visibility Module** (NVM) that can be directly deployed using cloud-managed Cisco Secure Client (formerly AnyConnect). NVM delivers a continuous feed of high-value endpoint telemetry which allows organizations to see endpoint and user behaviors on their networks. It collects flow logs directly from endpoints on- and off-premises, and valuable contexts like users, applications, devices, locations, and destinations. NVM telemetry can be crucial in correlating network telemetry with endpoint process information, as it contains both on a single log line.

Asset Context

The Cisco XDR Asset Insights feature extends the integration framework to collect data about device and user inventory and posture. A unique combination of data from security products and traditional device managers results in a unified asset inventory that can be used to provide context to investigations and meaningful reports. Each asset has a single page of information about it, merged from all sources. It also allows defining an asset's "value" which is used when scoring XDR incidents. If incidents contain assets, they will be visible when reviewing, investigating, and responding to the incident.

Cisco Asset Insights for Devices leverages sources directly from Cisco XDR Integrations, while Asset Insights for Users natively leverages Cisco Identity Intelligence (CII) sources, via Cisco Security Cloud Control. Cisco XDR receives the correlated data from CII and presents it within User Insights. This mechanism enables the inclusion of additional Identity Providers (IDPs) as sources, and the addition of new identity security events to be leveraged by Cisco XDR.

Custom Automation Workflows

Cisco XDR Automation provides a no-to-low-code approach for building automated workflows. These workflows can interact with various types of resources and systems, whether from Cisco or a third-party vendor. Automation workflows are the parent component and are like a script in traditional programming, while Atomic Actions provide reusable building blocks which are like functions in traditional programming. Many out-of-the-box workflows and atomics are available; however, users can also customize these or make their own using the graphical user interface. A workflow can be simple and have only a few actions, or complex and string together many different actions for different products. Using the drag-and-drop interface, it is possible to create your own workflows, which can be triggered by a variety of schedules and events. Examples are new incidents, or incident status changes, an email or webhook received, schedules and much more. Automation Rules allow you to manage all workflows and triggers in a single holistic experience.

© 2025 Cisco and/or its affiliates. All rights reserved.

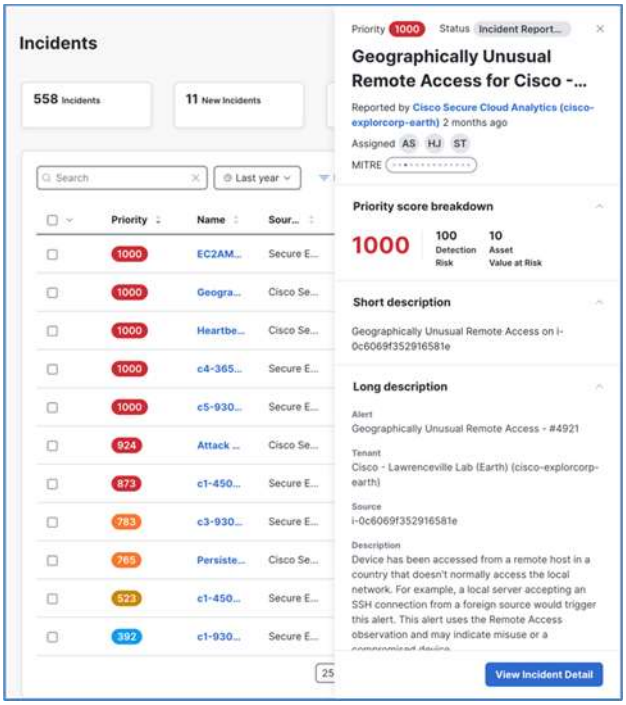
Automation Workflow Exchange

The Cisco XDR Automation Exchange allows you to quickly find new automation workflows, install them through an installation wizard to quickly discover new curated content, and operationalize the workflows within a few clicks. On the Exchange page, you can easily locate useful workflows and streamline the workflow import process using the 1-Click Install wizard. It is possible to filter Exchange by products, as well as view popular workflows.

Incident Prioritization

New incidents are assigned a priority score and are automatically enriched. New detections that are discovered in the enrichment process that are relevant to an incident are added to that incident. The incident priority score (1-1000) used to prioritize incidents is made up of Detection Risk (1-100) and Asset Value (1-10). The Detection Risk score is composed of the MITRE TTP financial risk, number of MITRE TTPs, and source severity. The Asset Value is a user defined value, which represents the value of the asset involved in the incident.

After an incident is prioritized, it shows up in a list form, sorted by priority score, enabling analysts to quickly decide what to investigate first and focus on the incident with the highest priority score. Various options for sorting, filtering, assignees, and status can be changed directly in the incident list.

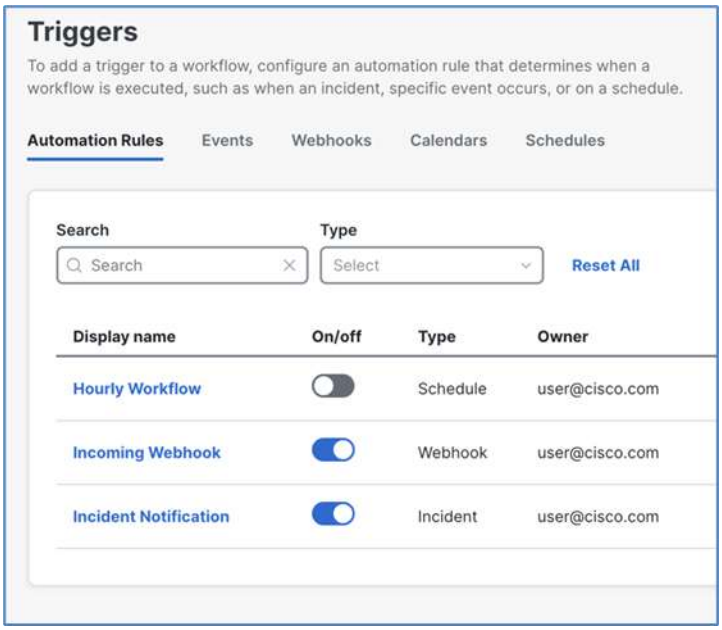


Incident Response

When an incident is created, prioritized, and enriched, it is critical to quickly respond to a breach. The built-in Response Playbook allows security analysts and incident responders to do this. Contextual playbooks provide a step-by-step, guided response for incidents that follows the SANS “PICERL” incident response model. Many actions in the playbook are powered by native XDR Automation workflows. These workflows take actions based on which products you have integrated accelerating how you respond. The incident’s Worklog allows you to view work already completed for the incident, post notes with important details, and collaborate with your team. You can also review the history of actions taken, including the execution of automated response actions in the response playbook. While an out-of-the-box, product agnostic Playbook with built-in Workflows is available and managed by Cisco. the Playbook framework allows for

© 2025 Cisco and/or its affiliates. All rights reserved.

rich customization. It is possible to duplicate and edit the Playbook or create them from scratch. It is also possible to build other Incident Response workflows using the template in Automation. They can also be found in the Exchange by filtering on this Incident Response template. Playbook Assignment Rules allow users to define with conditional logic which Playbook to assign to what type of Incident.



Threat Intelligence

In the Cisco XDR platform, it is possible to combine multiple sources of threat intelligence in addition to the built-in threat intelligence from Cisco Talos and other sources. This offers crucial context during enrichment of incidents, further investigation and validation of incidents, or while doing threat hunts. This threat intelligence can include simple reputations, or more complex relationships between attack tools, techniques, and known threat actors. Users can enable multiple Cisco and third-party intelligence providers and access all of them in unison natively in investigations through the Cisco XDR Investigate feature.

Threat Hunting and Threat Investigation

With the Cisco XDR Investigate feature, it is possible to do advanced threat hunting with a comprehensive, yet simple user experience. While doing an investigation, Cisco XDR will query all integrations, retrieving both local and global threat intelligence as well as any reported sightings of the investigated items in your environment. After this, it is possible to see a graph view of all the artifacts you are investigating, with an adjustable timeline. You can also use graph filters and a table view to quickly focus on specific items. Start an investigation based on an existing incident, a set of observables, or even by copy pasting a piece of text (e.g., a blog post). Using the rich Cisco XDR APIs, it is even possible to do an investigation completely automated, allowing you to automatically keep on top of recently reported threats in the wild, and be alerted proactively if evidence of them is found in your environment.

Digital Forensics and Incident Response

Cisco XDR Advantage and Premier license customers benefit from XDR Forensics built-in to Cisco XDR's incident workflow. The XDR Forensics capability changes the game for security operations teams by triggering digital forensics to collect over 350 artifacts on endpoints, including compromised or partially encrypted ones. This evidence preserves chain-of-custody of registry files, memory dumps, activity logs, and hundreds of other pieces of information, mandatory for forensic investigations. XDR Forensics extends

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco XDR's role in the breach response value chain with comprehensive response and recovery capabilities. It includes a remote endpoint interactive response shell, forensic acquisition, and reporting, enabling you to determine the root cause and next steps for high confidence incident response to contain, eradicate the threat and recover the endpoint.

Third-Party Telemetry

Cisco XDR Advantage customers will benefit from commercially supported and curated integrations with select third-party tools across a range of vectors, EDR, email threat defense (ETD), next-generation firewall (NGFW), network detection and response (NDR), and security information and event management (SIEM). The list of third-party integrations supported and curated by Cisco is dynamic, so please speak with your Cisco representative for the current list.

Integrations

The following is a list of integrations supported by Cisco XDR. Our open ecosystem allows integrations to be written not only by Cisco engineering, but also by development partners, third parties, and even users. Product names with the 'C' designation are Cisco Managed integrations, written by Cisco. Those with a 'V' are Cisco-verified integrations written by partners but verified by Cisco QA. Both are supported out-of-the-box. The products without a designation are solutions that can be integrated into Cisco XDR by the customer but may not have been tested and validated. This list is representative, does not guarantee that the solutions listed here will successfully integrate with Cisco XDR, is not intended to be complete, and is subject to change at any time without notice. Each integration will vary based on the product capabilities and use cases that can be supported by the product vendor and Cisco XDR.

Application, Identity, and Device Management Integrations

These sources have their own inventories of devices, device objects, or users, and these integrations bring information about these assets into a centralized location within Cisco XDR. This comprehensive view provides the data and context needed to better identify vulnerabilities, prevent threats, and prioritize remediations.

- Cisco Duo C
- Cisco Identity Intelligence
- Cisco Identity Services Engine (ISE) C
- Cisco Orbital
- Cisco Vulnerability Management (formerly Kenna) C
- Google Chromebooks C
- Ivanti Neurons C
- Jamf Pro C
- Microsoft Entra ID C
- Microsoft Intune C
- Okta C
- VMWare Workspace One UEM C

© 2025 Cisco and/or its affiliates. All rights reserved.

Collaboration, ITSM, and Ticketing

Collaboration, ITSM, and Ticketing tools allow SOC teams to work more effectively together to track their actions and rapidly perform group tasks. In Cisco XDR, these integrations can provide automated means of leveraging these tools in time-critical or compliance use cases.

- Cisco Webex C
- Jira Cloud C
- Microsoft Teams C
- PagerDuty C
- ServiceNow C
- Slack C
- XMatters C
- ZenDesk C

Cloud Security Integrations

Cloud security integrations are valuable in reducing security and compliance risks, managing security policies across multiple products, determining which vulnerabilities pose the highest risk and which can be deprioritized, and securing applications in hybrid work environments. Additional capabilities from these integrations include protection against DDoS threats and OWASP attacks and extending web security.

- Cisco Defense Orchestrator C
- Cisco Secure Cloud DDoS Protection C
- Cisco Secure Cloud WAF Service C
- Cisco Secure Workload C
- Cisco Secure Web Appliance C
- Akamai C
- Amazon Guard Duty C
- Microsoft Graph Security API C
- Radware Cloud DDoS Protection V
- Radware Cloud WAF V
- Signal Sciences Next-Gen WAF V

Email Telemetry, Security, and Response Integrations

These integrations provide understanding of email as a threat vector by visualizing message, sender, and target relationships in the context of a threat. Email integrations provide tiles to Control Center, as well as actions for orchestration, so practitioners can build automated workflows, helping to obtain better context of a threat to combat phishing attacks, business email compromise, malware, and ransomware.

- Cisco Secure Email and Web Manager C
- Cisco Secure Email Gateway C
- Cisco Secure Email Threat Defense C

© 2025 Cisco and/or its affiliates. All rights reserved.

- Microsoft Defender for Office 365 C
- Microsoft Defender for Office 365 GCC C
- Proofpoint Email Protection C

Endpoint Telemetry, Detection, and Response Integrations

EDRs provide a list of all managed endpoints and their details are extracted and stored within a centralized location of Cisco XDR, allowing devices to be uniquely identified and acted upon without depending on unreliable IP addresses. Endpoint context allows investigation on files and processes matching a SHA256 hash across and URLs these key data points are correlated to promote week alerts to high efficacy incidents. They are essential for taking response steps (one-click or fully automated) to mitigate, contain, eradicate, or recover from an attack.

- Cisco Secure Client C
- Cisco Secure Endpoint C
- CrowdStrike Falcon Insight C
- Cybereason Endpoint Detection and Response C
- Microsoft Defender for Endpoint C
- Microsoft Defender for Endpoint GCC C
- Palo Alto Networks Cortex XDR C
- SentinelOne Singularity C
- Trend Vision One C
- Qualys IOC

Enterprise Backup

Backup strategies are part of any effective security practice. In Cisco XDR, integrations with backup technologies can drive manual and automated backups, snapshots, and restore actions, as part of both preventative and response workflows. Integrations with our backup technology partners are the driving force behind the Cisco XDR Automated Ransomware Recovery capabilities.

- Cohesity Data Protect –coming soon!
- Rubrik V
- PureStorage
- Veeam – Coming Soon!

Network Detection and Response Integrations

NDR is a core foundational integration of Cisco XDR as it enriches threat detection with agentless behavioral and anomaly detection capabilities and unique network device context. It can be combined with sources of global threat intelligence and internal visibility to develop confirmed threat alerts based on known incidents of compromise. NDRs also offer a rich set of network device context which is essential to ascertain incident criticality. This historical network data is queried by Cisco XDR to enrich threat hunting and forensic audits and XDR incidents, simplifies visibility, and increases response efficiency.

- Cisco Secure Network Analytics C
- Darktrace Respond & Detect C

© 2025 Cisco and/or its affiliates. All rights reserved.

- Endace Probe V
- ExtraHop Reveal(x) 360 C
- Gigamon ThreatInsight
- NETSCOUT Omnis Cyber Intelligence V

Next-Generation Firewall Telemetry and Response Integrations

The integration of NGFW devices provides sightings of IP addresses, URLs, and domains as additional context and to further forensic investigations in Cisco XDR. Additionally, users can leverage Secure Firepower to block IPs at the perimeter. Secure Firewall devices can also be configured to provide alerts to Cisco XDR to be triaged and correlated, displaying the most pressing alerts in the Cisco XDR incident manager. The querying of all configured firewall devices to enrich observables related to an XDR incident improves visibility and understanding of attacks. Combined with automated response capabilities and using them in coordinated, single-click defenses simplifies visibility and increases response efficiency.

- Cisco Secure Firewall C
- Cisco Meraki MX C
- Check Point Quantum Smart-1 Cloud C
- Cisco Adaptive Security Appliance C
- Fortinet FortiGate C
- Palo Alto Networks NGFW C
- Palo Alto Panorama C

Public Cloud Integrations

Integrate Cisco XDR with the leading public cloud providers to gather network meta data from Flow Logs, proprietary logs and APIs providing a powerful source for entity modeling, baselining, and detecting malicious network activity. Entity modeling uses flow meta data to build a model of normal activity from observed device behavior and uses this model to spot changes in behavior that may be due to misuse, malware, or compromise. By integrating cloud providers, Cisco XDR helps security operation centers (SOCs) stop chasing cybercriminals and their never-ending myriads of exploits, malware, and other threats by trying to keep up with their signatures. Instead, the SOC can focus security efforts on a small, prioritized number of significant and automatically detected deviations from established patterns and activities, as identified by entity modeling.

- Amazon Web Services (AWS) C
- Microsoft Azure C
- Google Cloud Platform (GCP) C
- Oracle OCI – coming soon! C

Security Information and Event Management Integrations

Cisco XDR can utilize SIEMs during threat investigation, as a source of observations and reputations on queried threat artifacts and targets. Supported observable types include IPv4 addresses, IPv6 addresses, domains, file names, and SHA256 file hashes. These integrations enable an investigator to collect Sightings from many data sources, by using the integration as a translation layer between data models withing Cisco XDR workflows.

© 2025 Cisco and/or its affiliates. All rights reserved.

- Cisco CESA C
- Cisco Splunk Cloud C
- Cisco Splunk Enterprise C
- Devo
- Google Chronicle
- Google SecOps – coming soon! C
- Graylog
- Microsoft Sentinel - coming soon! C
- Sumo Logic Cloud SIEM
- Sumo Logic Log Management

Threat Intelligence Integrations

Access to numerous threat intelligence sources is included with Cisco XDR at no additional cost. These include the Cisco Talos database, the default Cisco threat intelligence architecture, and a private repository into which users can upload their own threat intelligence, whether generated in house or acquired from other sources. Integration of Cisco Secure Malware Analytics within Cisco XDR allows users to get detailed intelligence about malware, associated network traffic, system changes, and more to gain heightened malware threat intelligence via automated detonation of suspected files from a global user base.

- Cisco Secure Malware Analytics C
- Cisco Talos Intelligence C
- Cisco Secure Endpoint File Reputation C
- AbuseIPDB IP Checker C
- AlienVault Open Threat Exchange C
- alphaMountain.ai Threat Intelligence
- Alspera CriminalIP
- APIVoid C
- Censys
- CyberCrime Tracker C
- Farsight Security DNSDB
- Google Safe Browsing C
- Have I Been Pwned C
- IBM X-Force Exchange C
- IsItPhishing
- MISP
- Palo Alto Networks AutoFocus
- Pulsedive C

© 2025 Cisco and/or its affiliates. All rights reserved.

- Recorded Future
- Red Sift Pulse V
- SecurityTrails
- Shodan C
- Sixgill Darkfeed
- SpyCloud Account Takeover Prevention
- Stealthmole V
- Threatscore | Cyberprotect C
- urlscan.io C
- VirusTotal C

License Options

There are three license tiers in which Cisco XDR is available: Essentials, Advantage, and Premier.

Cisco XDR Essentials delivers the full XDR features and integrates across the Cisco Security portfolio, with a few exceptions. Cisco XDR Advantage builds upon the capabilities delivered in Essentials by adding Cisco-curated integrations with select third-party security tools. Cisco XDR Premier delivers the full Advantage capabilities as a Managed Service provided by Cisco security experts and includes security validation through penetration testing and select Cisco Talos Incident Response services.

Table 1. Cisco XDR License Options

Features	Essentials	Advantage	Premier
Security Analytics and Correlation	✓	✓	✓
Attack Storyboard with Instant Attack Verification	✓	✓	✓
Threat Intelligence	✓	✓	✓
Threat Hunting	✓	✓	✓
Incident Response Actions	✓	✓	✓
Incident Prioritization	✓	✓	✓
Case Prioritization	✓	✓	✓
Asset Context	✓	✓	✓
Custom Workflows	✓	✓	✓
Automation Workflow Exchange	✓	✓	✓
Data Ingestion / Data Retention	✓	✓	✓

© 2025 Cisco and/or its affiliates. All rights reserved.

Features	Essentials	Advantage	Premier
Cisco Software Support Enhanced	✓	✓	✓
Cisco Identity Intelligence	✓	✓	✓
Third-party Telemetry		✓	✓
XDR Forensics		✓	✓
Cisco Managed Extended Detection and Response			✓
Cisco Talos Incident Response (Talos IR)			✓
Cisco Technical Security Assessment (CTSA)			✓

Data retention: A data retention period of 90 days is included by default. Customers can purchase additional retention periods of 180 or 365 days.

Data ingestion: Each tier includes a data ingestion limit of 2GB per user per month. Customers can purchase additional GBs beyond the 2GB default, measured in units of GB per user per month.

Cisco Managed Extended Detection and Response

The Cisco XDR Premier license tier is a managed detection and response service using the Cisco XDR solution provided by Cisco security experts. It includes security validation through penetration testing and select Cisco Talos Incident Response Retainer Services. Cisco Managed Extended Detection and Response (MXDR) powered by Cisco XDR uses a combination of Cisco's team of researchers, investigators, and responders, the Cisco XDR solution, integrated tool sets, and additional Cisco security technologies (where available) to monitor for and respond to potential security threats and breaches.

The Cisco MXDR service includes:

- **24x7x365 monitoring:** Global security incident and alert monitoring by expert security investigators.
- **Unmatched Cisco expertise:** Cisco's team of researchers, investigators, and responders leverage both Talos Threat Intelligence and defined investigation and response playbooks to help detect, investigate, and respond to threats and alerts. Cisco's responses may include additional information, recommendations, or changes based on the type of threat or indication of compromise.
- **Quarterly threat briefings:** The Cisco MXDR intelligence team hosts remote review meetings on a quarterly basis open to all MXDR customers, co-delivered by Cisco Talos Incident Response. This quarterly briefing provides updates on current threat patterns, detection volumes, and trending events.
- **Dedicated service portal:** The dedicated Cisco MXDR service portal provides security incident lifecycle management, dashboards metrics, knowledge base, SOC communication, and more.
- **Threat advisories:** Cisco MXDR issues threat advisories for new threats discovered helping customers to proactively prevent incidents or compromises through the implementation of mitigating controls. All past intelligence articles and advisories are available from the MDR powered by Cisco XDR Portal Knowledge Base.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Talos Incident Response Retainer Service

Cisco Talos Incident Response Retainer Service provides a full suite of proactive and emergency incident response services to help you prepare, respond, and recover from a cybersecurity incident. With this flexible service, you enjoy:

- **Incident response expertise:** Our global team of seasoned incident responders is available during active incidents and to help strengthen your overall defenses.
- **Swift action:** One of our incident responders can be remotely dispatched within four (4) hours of reporting an active incident, which minimizes downtime and accelerates incident resolution.
- **Intelligence-enriched analysis:** Driven by an evergreen library of threat intelligence and backed by proven incident response processes.

Cisco Technical Security Assessment

Cisco Technical Security Assessment provides a suite of proactive services to assess a customer's cyber security posture and advice on the threats they face, the likelihood of those threats being realized, and the impact on their operational resilience if they are. This includes but is not limited to:

- Threat Modelling
- Penetration Testing
- Red Team Threat Simulation
- Security Architecture Assessment
- Application Security Assessment
- Security Operations Assessment
- Development Operations Security Assessment
- Device Configuration and Build Reviews

Support

Cisco XDR Software Support Service

There are two levels of support available:

- Cisco Software Support Enhanced is included with all Cisco XDR License Tiers at no additional cost
- Cisco Software Support Premium is available for purchase at an additional fee

Cisco Software Support Enhanced (included)

- Solution Support (Reactive Technical Support):
  24x7 with 30-minute response time service level objective (SLO)
- Onboarding guidance
- Ongoing digital adoption
- Periodic Security Health Checks: One (1) per year for the covered environment

Cisco Software Support Premium (add-on)

- Cisco Software Support Enhanced

© 2025 Cisco and/or its affiliates. All rights reserved.

- Designated Customer Success Point of Contact
- Extended adoption sessions: Up to six (6) adoption sessions per year
- Periodic business and success review

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA 10/25

© 2025 Cisco and/or its affiliates. All rights reserved.