Cisco XDR

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco XDR ("XDR").

Cisco will process personal data from Cisco XDR in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by XDR to provide its functionality.

1. Overview of Cisco XDR Capabilities

Cisco XDR enables teams to detect, prioritize, and respond to advanced threats. It is a cloud-based solution that streamlines security operations by consolidating data from various sources into a unified view, minimizing false positives and facilitating efficient investigations. Automation, orchestration and guided remediation recommendations help mitigate threats, reduce response times, and increase coverage without additional staff. With a data-driven approach, SOC teams can prioritize impactful events and strengthen overall security while enhancing resilience.

Cisco XDR provides several functions including cross-product metrics, investigations, incident management, security responses, and automation. It can collect threat intelligence and security detections from integrated modules and take control or mitigating actions driven by multiple Cisco and third-party sources.

All product integrations must be activated and as such are inherently and explicitly opt-in.

Information is collected from integrated products for various reasons described above. In some of those use cases, information may persist within portions of Cisco XDR for various lengths of time, as described below in this document.

Global Threat Intelligence Research: To continually secure Cisco's product portfolio, certain Cisco products share data with Cisco's global threat intelligence teams, including Cisco Talos and other trusted Cisco security and support personnel, which then processes the data for global threat intelligence and product improvement purposes. If our threat intelligence research determines the data is not related to any malicious activity, it is deleted on the schedule set forth in this section. Any data that is determined to be relevant to malicious behavior, as well as aggregated and de-identified data, including IP addresses, is retained by the threat intelligence team.

Cisco XDR offers identity and single sign-on through Cisco Security Cloud Sign-On and multi-factor authentication through Cisco Duo. For information regarding the data processed by Cisco Security Cloud Sign-On and Cisco Duo, please see the applicable Privacy Data Sheets.

Please see Cisco XDR for more details.

This Privacy Data Sheet does not address the processing of personal data by the integrated Cisco products. Please refer to the Cisco Privacy Data Sheets for the applicable integrated Cisco products for a description of the data categories and personal data collected, processed and stored by those products. If you elect to use third-party product data sources, including through integrations available via Cisco XDR, please contact the applicable third-party vendor for information regarding the data provided by such products.

2. Personal Data Processing

The table below lists the types of personal data used by XDR to carry out the services and describes why we process that data. XDR aggregates security information and context provided by integrated Cisco or third-party products.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Address • Email Address	Registration Information (name, address, email address, User ID) is collected for account creation, product enablement,

	• User ID	product use notifications, training, and support; configuration of on-premises device connections to Cisco XDR.
Integration Data	• Usernames • API keys • API locations/hosts • License details	This data enables Cisco XDR to work with on-prem and cloud products on the user's behalf. This may include such tools as firewalls, endpoint security solutions, DNS / web / email / etc. security solutions, cloud providers of threat intelligence, messaging systems, ticketing / ITSM systems, and more. These stored credentials and service locations are used to access the products and services to gather relevant threat information or take protective actions at the user's request.
User Search Data	• IP Address • Email address • URL • Domain name • File path/file name • Email/email subject • Username/ID • Any other personal data processed in connection with a user search	User Search Data is collected for queries against configured modules to return threat intelligence judgments and verdicts, and to find and display matched records from other security products licensed and configured by the user. These data elements are also referred to as "Observables." Observables are supplied by the user either as a search string in the Investigate box or via browser plug-in.
Network Visibility Module Data* ** Only collected by Cisco AnyConnect if customer chooses to enable the Network Visibility Module*	• User ID and/or user name • IP address for end points • Host ID • MAC address • User Passwords • Destination host name for the applicable firewall. • DNS information • Additional network activity contained with • the network logs (e.g. URL's visited by users)	To enable the customer to have visibility into and perform analytics on network related data.
Network Flow Metadata	• Source IP address • Destination IP address	Provide the security product functionality (i.e., threat and malware detection, identification of customer policy violations, misconfigured cloud assets and user error and misuse) and product improvements. Global threat intelligence research.
Enhanced Network Flow Metadata for Encrypted Traffic Analytics (ETA) ** ETA metadata is collected only if generated by the underlying enterprise network equipment.*	• Initial Data Packet ("IDP"), which may include IP Header, TLS Header, SNI (Server Name Identifier), Ciphersuites (Certificate, Organization, Issuer, Issued, Expiration)	Security analytics, forensics, efficacy research, general product functionality and usage. Global threat intelligence research.
Other Metadata ** Customer has the option to elect to send additional logs containing user data for threat detection.* ***Portal users have the option to add tags and comments related to security alerts, which may contain personal data if added by the user.*	Optional Additional Logs • User data • User ID • Username • User email address • User IP address • Device host name • Passive DNS logs • Tags and Comments	This data is used only to provide the security product functionality. Global threat intelligence research.

Cisco ISE Session Data	• User data • Username • Device IP address • Device host name • Device type • AD session data • Device OS info • MDM status • ANC policy	Enables detection on user and device sessions for anomalous activity. Provides user and device context and attribution to network sessions and detections on network traffic.
Event Data and Data Associated with Alerts and Observations	• Username and/or User ID, email address, asset groups • URLs accessed by an individual • User IP addresses, source IP, and destination IP, MAC address • File name • Host name • Event Type • Operating system • Organizationally Unique Identifier • Fully qualified Domain Name • Host Name • DHCP information (such as class identifier) • Browser user agent information (i.e., operating system run by the browser) • Other event details as included by reporting product	The customer has the option to elect to send some of this data to Cisco XDR for visualization, analytics, incident response. This data enables the customer to understand and view detections, perform threat detection and analytics on event data, manage and respond to incidents, and view event and response statistics within Cisco XDR. Global threat intelligence research.
Private Intelligence Store	• Casebooks • Incidents • Judgements • Indicators • Sightings • Events / Raw Data • Worklog	Storage of any information/data by user (at user's election) in the private repository is known as the Private Intelligence Store. The Private Intelligence repository is available to users as cloud storage of XDR-relevant, user-created or system created information like casebooks, incidents, judgements on observables, etc. Worklog keeps record of the user or automated response activity, changes to the status of an incident, and note taking within an incident.
Control Center: Tile Content Data	Any configured data defined by the customer and sent to Cisco XDR for display in the Control Center	Data collected for display including matched records from other Cisco and third-party security products licensed and configured by the customer. These data elements are supplied by the customer via API.
Automate Data	Customer defined workflow content. May optionally include: • Email addresses • Username • API keys • IP addresses • URL • Customer defined variables (can be encrypted by using secure string option) • Other personal data a customer elects to include in workflow record Encrypted session tokens include: • User ID • User roles • User workflow activity	Cisco XDR Automate data is used to simplify business processes through workflow automation. Cisco XDR Automate provides a no-to-low code approach for building automated workflows. These workflows can interact with various types of resources and systems. With Cisco XDR Automate, you can leverage Cisco and third-party multi-domain systems, applications, databases, and network devices in your environment to create workflows. Workflows and workflow variables may include sensitive or proprietary information if designed by the user to do so. The orchestration subsystem also leverages integration data to connect to configured integrated technologies and stores session tokens and other information to enable these communications.

Asset Data	• User's first and/or last name • Address / office location • Username / display name • Email address • Phone number • IP address • Host/Device name • MAC address • Device geolocation • Device activity timestamp • Device configuration settings (e.g., security products enabled etc.) • Mobile Device Management (MDM) data, including device registration status, MDM compliance status, disk encryption on/off, PIN lock on/off, jailbroken yes/no, device manufacturer, device model, device serial number, operating system version, International Mobile Equipment Identity (IMEI) number, Unique Device Identifier (UDID) number, device phone number	Cisco XDR Asset Data is used to deliver the optional Assets feature within Cisco XDR. This feature is designed to consolidate, discover, normalize, and work with a customer's asset inventory within Cisco XDR, including devices and users. It aims to unify data from multiple device and user management tools, endpoint detection and response, anti-virus and other endpoint security products and surfacing these details within a unified view in Cisco XDR.
Usage Data	Product usage data (i.e., data related to features utilized when accessing Cisco XDR) which may include the following personal data and associated usage information and other non-personal usage data • User first and last name • User ID • Email address • User address (including city and country) • Session Data • XDR product usage data such as pages visited, elements clicked, links clicked, user's browser and operating system, cookie information, session metadata, timestamp, URL, API usage, etc. • Country and city of user • Feedback, including any personal data included by a user in a free text field or survey response	Product usage analytics and session data for product troubleshooting, improvement and decision making. Customer Experience ("CX") initiatives which may include, but are not limited to, customer awareness and adoption activities (e.g., deployment guidance, digital journeys, etc.) and the CX Cloud for Customers (for eligible customers). Please see the Customer Experience (CX) Cloud Privacy Data Sheet at the Cisco Trust Portal for information regarding the processing of personal data by the CX Cloud.

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from XDR that is provided by customer. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to resolve issues. For more information, please refer to the TAC Service Delivery Privacy Data Sheet.

3. Data Center Locations

Cisco XDR leverages third-party cloud hosting providers to provide services globally.

Data Center Locations	Description	Location of Data Center
Amazon Web Services ("AWS") North America Cloud	The North American infrastructure for XDR cloud (multiple availability zones).	United States
AWS EU Cloud	The European infrastructure for XDR (multiple availability zones).	Ireland

Data Center Locations	Description	Location of Data Center
		Germany
AWS Asia Pacific Cloud	The Asia Pacific infrastructure for XDR (multiple availability zones).	Japan Singapore Australia (Cisco XDR Analytics)
Equinix	Cloud co-location facility for Cisco Talos	United States
Vazata	Cloud co-location facility for Cisco Talos	United States

Usage Data is also transferred to the United States for product usage analytics and CX initiatives even if the EU or Asia Pacific regions are selected by the customer.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by XDR to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Customers	Security administration and operations
	Cisco	Creating an account and validating license entitlements and general product support and operations
Integration Data	Customers	Security administration and operations
	Cisco	Product operations/support, product analysis
User Search Data	Customers	Threat research based on product functionality
	Cisco	Product operations/support, product analysis, improve product functionality
Network Visibility Module Data	Customers	Investigation of network connections
	Cisco	Product operations/support, product analysis, improve product functionality
Network Flow Metadata	Customer	Threat research based on product functionality, troubleshooting
	Cisco	Product operations/support, product analysis, improve product functionality

Enhanced Network Flow Metadata for Encrypted Traffic Analytics (ETA)	Customer	Threat research based on product functionality, troubleshooting
	Cisco	Product operations/support, product analysis, improve product functionality
Other Metadata	Customer	Threat research based on product functionality, troubleshooting
	Cisco	Product operations/support, product analysis, improve product functionality
Cisco ISE Session Data	Customer	Investigation of ISE sessions
	Cisco	Product operations/support, product analysis, improve product functionality
Event Data and Data Associated with Alerts and Observations	Customer	Visualization of incidents and threat research based on product functionality
	Cisco	Product operations/support Global threat intelligence research
Private Intelligence Store	Customer	Threat research based on product functionality. Addition of user notes, observations, judgements, and other security context and content to ongoing investigations, incidents, or responses
	Cisco	Product operations/support
Control Center: Tile Content Data	Customer	Security monitoring based on product functionality. Ability to visualize data displayed in dashboard
	Cisco	Product operations/support
Automate Data	Customer	Creation and execution of customer-defined workflows.
	Cisco	Product operations/support
Asset Data	Customer	Device visibility and consolidation as described in Section 2
	Cisco	Product operations/support
Usage Data	Customer	Customers with access to the CX Cloud for Customers have access to their usage data for internal analysis. Customer can elect through the CX Cloud for Customers to share data with designated Cisco partner(s)
	Cisco[1]	Product usage analytics and CX initiatives as described in Section 2

6. Data Portability

Data portability requirements are not applicable to the Cloud Service.

[1] Includes Cisco sub-processor for Usage Data referenced in Section 9.

7. Data Deletion & Retention

The table below lists the personal data used by XDR, the length of time that data needs to be retained, and why we retain it.

Personal Data Category	Retention Period	Reason for Retention
Registration Information	Retained throughout the customer's subscription. Deletion upon request. A customer may request deletion of Registration Information by opening a Cisco TAC case or by sending an email to privacy@cisco.com.	Creating an account, product enablement, product use notifications, training, support, and service delivery.
Integration Data	Customer integration data is deleted upon expiration or termination of customer's subscription following same principles as Registration Information.	Configuration parameters of the customer integrations, used for product operations and delivering key functionality
User Search Data	Retained only for current session unless explicitly saved as a saved investigation or via a casebook by the user.	Key customer experience functionality for reference and utility for future sessions.
Network Visibility Module Data	Network Visibility Module Data, which represents network traffic telemetry, is retained for a limited period of time in accordance with the licensed data retention period of either 90 days, 180 days, or 365 days. Some data may be kept longer for efficacy and threat research purposes.	Threat detection, hunting, and query based on desired customer retention period.
Data Associated with Alerts and Observations	Service alerts and observations are retained for the length of the customer's subscription.	Service delivery
Network Flow Metadata	Network flow metadata that is not retained in connection with alerts and observations as described above are automatically deleted from the service databases within twelve (12) months.	Service delivery
Enhanced Network Flow Metadata for Encrypted Traffic Analytics (ETA)	Network flow metadata that is not retained in connection with alerts and observations as described above are automatically deleted from the service databases within twelve (12) months.	Service delivery
Other Metadata	Network flow metadata that is not retained in connection with alerts and observations as described above are automatically deleted from the service databases within twelve (12) months.	Service delivery
Cisco ISE Session Data	ISE sessions that are not retained in connection with alerts and observations as described above are automatically deleted from the service databases within twelve (12) months.	Service delivery
Event Data	For limited sources, namely Cisco Firewall and Secure Network Analytics: Retained within Eventing Service temporarily and deleted from Eventing Service on a rolling seven (7) day basis. Event Data promoted to incident status is retained in the Incident Manager for a limited period of time in accordance with the licensed data retention period of either 90 days, 180 days or 365 days. Some data may be kept longer for efficacy and threat research purposes. Event Data transferred to Talos is retained indefinitely in Talos Data Center. A customer may request deletion of Event Data from Incident Manager and/or Talos by opening a Cisco TAC case. For customers who have purchased firewall logging from Cisco, firewall events that are not retained in connection with alerts and observations as described above are	Event data is collected for the purposes of enabling (i) the filtering of events that are incidents for security threat research and analysis, and (ii) data sharing with Cisco Talos for global threat intelligence research purposes and data sharing with Cisco Data Science and Engineering for efficacy research.

	automatically deleted from the service databases within twelve (12) months.	
Private Intelligence Store	Stored until explicit deletion by user or a customer may request deletion by opening a Cisco TAC case. Incident related data and telemetry is retained in accordance with the licensed data retention period of either 90 days, 180 days or 365 days. Some data may be kept longer for efficacy and threat research purposes.	Key customer experience functionality for reference and utility for future sessions.
Control Center: Tile Content Data	Stored in module cache for duration specified by the applicable underlying product.	Data visualization
Automate Data	Automation workflow related data, such as input and output parameters, are retained in accordance with the licensed data retention period of either 90 days, 180 days or 365 days. Encrypted session tokens are processed during session but do not persist and are not stored. Automation data related to any nested workflows (and activity inside workflows) is only stored for thirty (30) days. This is for debugging purposes only; in order to limit storage and optimize performance.	Carry out workflows defined by customer.
Asset Data	Attributes of an asset are only retained as long as the asset has been observed as active within the licensed data retention period of either 90 days, 180 days or 365 days. Currently active assets are not deleted. Inactive assets outside of retention period may be deleted.	Enable Cisco XDR Assets feature with the appropriate duration of historical data (90, 180, or 365 days respectively).
Usage Data	Stored by XDR until deletion requested by customer by opening a Cisco TAC case. Stored by CX for up to two (2) years.	Product improvement and product decision making (such as where to focus future operational and development needs). Customer experience initiatives.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure

Personal Data Category	Security Controls and Measures
Registration Information	Data is encrypted in transit and at rest.
Integration Data	Data is encrypted in transit and at rest.
User Search Data	Data is encrypted in transit and is not stored.
Network Visibility Module Data	Data is encrypted in transit and at rest.
Network Flow Metadata	Data is encrypted in transit and at rest.
Enhanced Network Flow Metadata for Encrypted Traffic Analytics (ETA)	Data is encrypted in transit and at rest.
Other Metadata	Data is encrypted in transit and at rest.
Cisco ISE Session Data	Data is encrypted in transit and at rest.
Event Data and Data Associated with Alerts and Observations	Data encrypted in transit to Eventing Service, XDR Incident Manager and Talos. Events promoted to incident status encrypted at rest in XDR Incident Manager.

Personal Data Category	Security Controls and Measures
Private Intelligence Store	Event Data shared with Talos and Event Data stored temporarily in Eventing Service (see Section 5) not encrypted at rest.
Private Intelligence Store	Data is encrypted in transit and at rest.
Control Center: Tile Content Data	Data is encrypted in transit and at rest (in cache).
Automate Data	Data is encrypted in transit and at rest.
Asset Data	Data is encrypted in transit and at rest.
Usage Data	Data is encrypted in transit and at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for XDR is set forth below:

Sub-processor	Personal Data	Service Type	Location of Data Center	Security Assurance
Amazon Web Services (AWS)	• Registration Information • Portal User Account Information • User Search Data • Event Data • Data Associated with Alerts and Observations • Private Intelligence Store • Dashboard Investigation Data • Orchestration Data • Usage Data	XDR leverages cloud technology to provide improved malware and threat detection and protection capabilities, security process automation, and KPI display. AWS Cloud helps provide a global service footprint, security assurance, service elasticity and resilience to XDR.	See Section 3	For information regarding AWS compliance/certification please refer to documentation online at https://aws.amazon.com/compliance/. Certifications and SOC reports are listed on this webpage and corresponding links under "Assurance Programs".
Snowflake Computing	• Usage Data	Cloud Data Warehouse Solution	AWS United States	See AWS above. Also see https://www.snowflake.com/product/security-and-trust-center/
Datadog	Any personal data in workflow logs	To monitor infrastructure activity and aggregate administrative logs	AWS United States	For information regarding Datadog's compliance/certifications, please see https://www.datadoghq.com/security/
Marketo	Administrator and trial requestor contact information (name, company, address, email, phone number)	Marketing automation platform containing administrator/requestor contact information. Supplements Salesforce to assist with activation, onboarding, authentication, entitlement, service notifications and inquiries, and customer success purposes	United States	For information regarding Marketo's compliance/certifications, please see https://www.adobe.com/trust.html
Auth0	Username and/or user ID (e.g., email address)	Single Sign On	United States	For information regarding Auth0's compliance/certifications, please see https://auth0.com/security

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Laws

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

12. Exercising Data Subject Rights

Users whose personal data is processed by Cisco XDR have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,</td><td>EMEA Privacy Officer
Cisco Systems, Inc.</td></tr>
</table>

San Jose, CA 95134 UNITED STATES	80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, please see to Cisco Trust Portal.