Cisco Defense Orchestrator

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

Cisco Defense Orchestrator is a cloud-based solution made available by Cisco to companies or persons who obtain a Cisco Defense Orchestrator subscription or a subscription to an offer that includes Cisco Defense Orchestrator access.

Cisco will process personal data from Cisco Defense Orchestrator 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 Cisco Defense Orchestrator to provide its functionality.

1. Overview of Cisco Defense Orchestrator

Cisco Defense Orchestrator ("CDO") is a cloud-based security policy management application that allows you to manage multiple Cisco security products with the following functionalities: policy change management, policy analysis and optimization, policy monitoring and reporting, and orchestration of policy changes. A CDO subscription includes access to single sign-on through Cisco Security Cloud Control and Security Cloud Sign On. For information regarding the processing of personal data by Cisco SecureX and Cisco Security Cloud Control and Security Cloud Sign On, please see their respective Privacy Data Sheets available on the Cisco Trust Portal. CDO also delivers cloud-delivered Firewall Management Center ("cdFMC"). This Privacy Data Sheet applies to Your use of CDO in connection with the cdFMC offer.

Note, CDO may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves CDO for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party. For more information on CDO, please see: https://www.cisco.com/c/en/us/products/security/defense-orchestrator/index.html.

2. Personal Data Processing

The table below lists the personal data processed by CDO to provide its services and describes why the data is processed. For more information on data management and the purpose of processing, please see our Trust Center on How We Manage Data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Email address • CCO or Smart License Account Credential[1] • Firewall Admin Credentials[2]	• Product administration: registration, account provisioning and login. • Customer success initiatives, including updates on new product features • Supporting customers (e.g., resetting second factor authentication device) • Firewall access[2]
VPN User Data	VPN users corporate email address, geolocation, and IP address	Monitoring users' VPN connection and displaying VPN information in CDO for customer's administrators.
Firewall Product Usage Data[3]	Product usage data (e.g., data related to features utilized by customer and configuration settings), which typically does not include personal data. However, if you are using cdFMC, this usage data may include the following personal data of the User Admin:	Firewall Product Usage Data is used for analytics for product improvement and product decision making. Firewall Product Usage Data is used for 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).

[1] Personal data may be provided to Cisco in the form of a user credential to associate it with a related Cisco.com account (i.e., CCO) or Smart License account. For more information regarding Smart License account and related data collection, please refer to the Smart Software Licensing Privacy Data Sheet on the Cisco Trust Portal.
[2] Contained in CDO cloud only if customer selects cloud option for its CDO secure device connector.
[3] A customer can opt-out of sending this usage data to Cisco in the CDO configuration settings.

	• First and last name • UserID • Email address • User address (including city and country)	Please see the CX Cloud for Customers Privacy Data Sheet at the Cisco Trust Portal for information regarding the processing of personal data by CX.[4]

The table below lists the additional personal data processed in active memory within CDO for viewing by customers licensed to Cisco Security Analytics and Logging ("SAL"). This data is stored by SAL and is not stored within CDO. Customer sets policies that determine which Firewall Event Data is collected. For information regarding the processing of personal data by SAL, please see its Privacy Data Sheet available on the Cisco Trust Portal.

The data in this table is also processed by the SecureX Eventing Service if enabled by a customer. For information regarding the processing of personal data by the SecureX Eventing Service, please see the SecureX Privacy Data Sheet available on the Cisco Trust Portal.

Personal Data Category	Types of Personal Data	Purpose of Processing
Firewall Event Data	• Username and/or User ID • Accessed URLs • IP addresses • Event Type • File names[5]	This data is processed within SAL, and within SecureX if the customer has enabled the SecureX Eventing Service, to enable customers to visualize device events and perform threat detection and analytics on such events.

If a customer contacts the Cisco Technical Assistance Center ("TAC") for problem diagnosis and resolution, Cisco TAC may receive and process personal data from CDO and SAL 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.

3. Data Center Locations

CDO leverages a third-party cloud hosting provider to provide services globally. Customers can select their data center region.[4]

Data Center	Description	Location
AWS	Production data centers for CDO	United States, European Union ("EU"), Japan, India, Australia

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in 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
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

[4] If the customer elects to use Cisco Success Track offer then CDO will send personal and non-personal data to Cisco's CX Cloud as part of that offer. For more information on the personal and non-personal data processed by CX Cloud, please consult the CX Cloud Privacy Data sheet.
[5] File names collected only if Customer is licensed to use Secure Malware Analytics (formerly, AMP Ecosystem and threat and advanced malware, or "TAM").

5. Access Control

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

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Cisco	• Registration, account provisioning and login, customer support • Customer success initiatives, including updates on new product features, and customer adoption motions to activate, maintain, support and improve the service. • Supporting customers (e.g., resetting second factor authentication device)
	Customers	• View who has access to CDO and SAL
VPN User Data	Cisco	• Product operations/support
	Customer	• Visualization of VPN activity
Firewall Event Data Note: Applies only if SAL ispurchased	Customers	• Visualization of device events, threat detection and analytics
	Cisco	• Product operations/support
Firewall Product Usage Data	Customers	• 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	• Product usage analytics and CX initiatives as described in Section 2.

6. Data Retention

The table below lists the personal data used by CDO, 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	• Deleted within 90 days after offer team is notified of contract expiration or receives a request from customer for data deletion.	• Provisioning, registration, support
VPN User Data	• Deleted on rolling 90-day period	• Visualization of VPN activity
Firewall Event Data Note: Applies only if SAL is purchased	• Not retained in CDO.	• Firewall Event data is collected for the purposes of enabling device event visualization, threat detection and analytics. This data does not persist in CDO.
Firewall Product Usage Data	• Retained for up to 2 years	• Product improvement and product decision making (such as where to focus future operational and development needs) • Customer experience initiatives

7. 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. These technical and organizational measures include the following:

Personal Data Category	Security Controls and Measures
Registration Information	Data is encrypted in transit and at rest
VPN User Data	Data is encrypted in transit and at rest
Firewall Event Data Note: Applies only if SAL is purchased	Data is encrypted in transit but does not persist in CDO.
Firewall Product Usage Data	Data is encrypted in transit and at rest

8. 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 the service is below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	• Registration Information • VPN User Data	Third party cloud-hosting service.	United States, EU, Japan, India, and Australia
Datadog	• Admin email address	To monitor infrastructure and service activity and aggregate administrative system and usage logs	United States
Amplitude	• Unique user identifer • Click interactions on CDO's graphic user interface (dashboard)	• Internal business and product analytics and reporting to inform data-driven business and product decisions and product improvements • Product and feature usage analytics, sales support, renewal support, product adoption and deployment assistance	United States

9. 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.

10. Certifications and Compliance with Privacy Laws

The Security and 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.

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

11. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, and / or deletion of the personal data processed by the Service as well as object to processing. Data portability requirements are not applicable to this product.

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
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

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.

12. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program, please visit The Cisco Trust Center. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco frequently evolves and updates its offerings. Cisco Privacy Data Sheets are subject to change, and are reviewed and updated on an annual basis, or as reasonably needed to reflect a material change in the processing of Personal Data. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the "Subscribe" link in the upper right corner of the Trust Portal.