Cisco Secure Workload as a Service

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Workload as a Service.

Cisco Secure Workload as a Service is a cloud-based security solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco Secure Workload as a Service 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 Secure Workload as a Service in order to provide its functionality.

1. Overview

Cisco Secure Workload as a Service dramatically improves data center security by enabling zero-trust operations. Using behavior-based application insight and machine learning, it provides customers with allow-list policy model enabling segmentation and microsegmentation through automated policy enforcement.

With Cisco Secure Workload as a Service, IT organizations can realize consistent workload protection by enabling allow-list-based segmentation and microsegmentation, behavior baselining and analysis, and detecting common vulnerabilities allowing users to proactively quarantine affected servers. Through an open policy model, workloads are secured consistently across bare metal, virtual and containerized workloads through a single pane of glass. With this holistic approach, Cisco Secure Workload as a Service significantly reduces the attack surface, minimizes lateral movement in case of security incidents, and more quickly identifies anomalies and suspicious behavior. The open policy can also be enforced across any vendor's infrastructure.

Cisco Secure Workload as a Service collects packet header metadata, process details and installed software package information. This is collected via the software sensors deployed on the workloads and made available as part of the solution. More detailed information is available in the Cisco Secure Workload as a Service product documentation. Below are the high-level details regarding the telemetry data that is collected by Cisco Secure Workload as a Service:

- Flow information: Contains details about flow endpoints, protocols, and ports, when the flow started, how long the flow was active, etc.
- Inter-packet variation: Captures any inter-packet variations seen within the flow, including variations in the packet's Time to Live (TTL), IP/TCP flags, packet length, etc.
- Process details: Captures processes executed on the server, including information about process parameters, start and stop time, process binary hash, etc.
- Software packages: Inventory of all software packages installed on the server along with the version and publisher information
- Cisco Secure Workload forensics capability: If a customer turns on the Cisco Secure Workload forensics capability, additional personal data may be collected.

Cisco Secure Workload as a Service will not capture customer data payload (the content of packets).

Cisco Secure Workload as a Service integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving/sending personal data from/to Cisco Secure Workload as a Service.

Note, Cisco Secure Workload as a Service may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves Secure Workload as a Service 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 about Cisco Secure Workload as a Service, visit https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_secure_workload_saas_offer_description.pdf.

2. Personal Data Processing

The table below lists the personal data processed by Cisco Secure Workload as a Service 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. Also described below are examples of non-personal data that is used by the Cisco Secure Workload as a Service solution that may in certain circumstances be correlated with personal data.

Table 1

Personal Data Category	Type of Personal Data	Purpose of Processing
Account and Registration Data	• First Name, Last Name • Email Address • User ID and Credentials	• Account creation • Activation of service • Billing/invoicing • Authentication, authorization, access to service • Future notification of features/updates • Support notifications, including upgrades/maintenances/incidents • Open and manage support cases, remote access support, and Cisco Customer Experience programs
Endpoint Visibility (optional integration with Cisco Secure Client and/or Identity Services Engine (ISE))	• Secure Client flow telemetry: ○ Flow/Source Destination IO Addresses, Protocols and Ports • Device name and OS version: ○ Endpoint Device (e.g., joesmith - Win and OS= Window10) • ISE Data may include: ○ SGT and Username ○ Device Type (IP phone, printer, etc.) ○ Device library version, antivirus, antispyware packages) • Secure ClientNetwork Visibility Module (NVM) Data: ○ User ID and/or username ○ IP address for endpoints ○ Host ID ○ MAC address ○ Destination host name for the applicable firewall ○ DNS information ○ Additional network activity contained with the network logs (e.g., URLs visited) Note: Secure Client and ISE administrators have the ability to turn off the user telemetry coming onto the Secure Workload platform	• If Endpoint visibility is enabled, Cisco Secure Workload using Secure Client and/or ISE agent processes this data to identify devices and individuals for application of policy and for Cisco Customer Experience programs • NVM data is processed for application of policy and Cisco Customer Experience programs only if the customer has enabled network visibility. NVM is required for Endpoint visibility for Secure Client agent integration

The “Other Data” identified in Table 2 below may potentially be connected to a person and therefore may constitute personal data, but for the most part is expected to relate only to servers in the data center and not be connected to an individual. For example, device names assigned by customers may include personal data depending on their configuration. Examples of this type of data appear below.

Table 2

Other Data	Examples of Personal Data	Purpose of Processing
Detailed Flow Metadata (data collected through various deployed agents and connectors)	• Source/Destination IP Addresses • Inter packet variations • TTL • Protocols • Ports • TCP/IP flags • Flow duration, length, bye count, time • Process ID • Process start/stop time • OS • Installed software packages (with publisher version) • Asset tags (user uploaded or with orchestrator integrations • Additional packet data	• Providing information on customer application dependencies for policy development and management • Enable implementation of zero-trust model in customer data centers • Required for Secure Workload as a Service protection fuctionality. • Securing and protecting customer workloads in multi-cloud data centers. This information supports: ○ Generate allow-list of zero-trust policy ○ Behavior baselining, analysis, and identification of cdeviations for processes ○ Detect common vulnerabilities and exposures assocated with the software packages installed on the servers • Cisco Customer Experience programs
Endpoint Visibility (optional integration with Cisco Secure Client and/or ISE)	• Process details: captures processes information (chrome.exe), including process ID, process binary hash, etc. • FQDN associated with the enpoint and also the flow Note: Secure Client and ISE administrators have the ability to turn off the user telemetry coming onto the Secure Workload platform	• If Endpoint visibility is enabled, Cisco Secure Workload using Secure Client and/or ISE agent processes this data to identify devices and individuals for application of policy and for Cisco Customer Experience programs
Summarized Flow Metadata	• Source/Destination IP Addresses • Protocols • Ports	• Providing information on customer application dependencies for policy development and managed used by Application Dependency Maps

Optional Integrations and Personal Data
Secure Workload users also have the option to upload identification tags, either directly via a file or via orchestrator integrations (AWS, vCenter, Kubernetes, etc.), and can use Secure Workload Apps and APIs to integrate Secure Workload with Cisco and/or third-party applications. It is possible, but not recommended, that an admin/ Secure Workload user could add personal data within the tags (e.g. the name of the individual associated an asset, IP address or process), or that with use of Secure Workload Apps, APIs or other integrations to come, Secure Workload data would include personally identifiable information.

Cisco is not responsible for customer data once it leaves Secure Workload 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.

3. Data Center and Point of Presence Locations

Cisco uses its own data centers to deliver the service globally.

Cisco Secure Workload as a Service does not use PoPs.

Cisco Data Center Locations
United States (Iowa, Northern Virginia)

Europe (Belgium, Netherlands)

Note: When you purchase a service subscription, Cisco always creates, processes, and stores your information in the United States regardless of the subsequent provisioning of your accounts in a chosen regional cloud. All data are encrypted in transit.

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

5. Access Control

The table below lists the personal data used by Cisco Secure Workload as a Service to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Account and Registration Data	Customer	Configure, manage and operate the service
	Cisco Secure Workload as a Service Operations team & TAC	Customer support (including Cisco Customer Experience programs), maintaining, upgrading and improvement of the service (see Table 1, purpose of processing) Note: This is only to access the platform. The Cisco team does not have access to any customer data or flow or policy information unless granted specifically by the customer during troubleshooting an issue. This is documented under the TAC support ticket and the access to customer meta-data and policy is revoked once the support ticket is closed. Learn more about it in customer support access.
Endpoint Visibility	Customer	Secure Workload cloud protection use cases. Secure Workload Operations as well as Cisco TAC do not have access to this data.

6. Data Retention

Upon request directed to Cisco Secure Workload as a Service support or submitting a request via the Privacy Request Form for removal of Account and Registration Data that constitutes personal data, Cisco will use reasonable commercial efforts to deactivate and then delete such data.

Retention of Data Identified in Table 1:
Secure Workload as a Service collects data identified in Table 1 to provide the featured functionality. The data cannot be selectively deleted but is deleted soon after each customer's subscription is terminated or expires. Customers may request deletion immediately after termination or expiration by sending a Zendesk Support Ticket. Otherwise, a Cisco employee managing the customer's subscription will initiate the deletion process, which takes approximately 30 days.

Retention of Data Identified in Table 2:
Detailed Flow Metadata described in Table 2: Cisco Secure Workload as a Service offers retention of 150 million most recent flow observations per every 100 active workload licenses. The retention period varies and will depend on multiple

factors such as –

- Flow Rate – rate of flows being reported will vary widely by workload (for example - Internet facing servers, DNS server may generate high amount of flows) and ingest data sources.
- Data Ingest Sources – sources of flow data including workload agents and network sources such as ASA/FTD/NetFlow/ERSPAN/VPC Flow Logs via ingest connectors. It is recommended to use filtering mechanism at the source to selectively report flows of interest.
- Flow Fidelity – configurable per workload agent, with detailed flow data (default) consuming more resources than conversation-only flow data. It is recommended to use conversation mode unless there are specific requirements for detailed flow metadata.
- Inventory Labels – metadata associated with each flow record based on quantity and length of value data fields, i.e., inventory data from external orchestrators and CMDB.

Summarized Flow Metadata described in Table 2: All Detailed Flow Metadata is converted into Summarized Flow Metadata and retained separately for a period of up to 12 months to enable policy generation.

7. Personal Data Security

Cisco Secure Workload as a Service is offered in a SOC-II, ISO27001 compliant facility. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means.

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
Account and Registration Data	• Data is encrypted in transit (TLS 1.2 or later). Data at rest is stored unencrypted with strict access control.
Endpoint Visibility	• Data is encrypted in transit (TLS 1.2 or later). Currently, any secret is encrypted and split acroos the system in 3 ways. There is very controlled physically access in to the IaaS environment, and there are security measures in place to now allow anyone access to cutomer data.

Secure Workload flow Metadata is encrypted in transit (TLS 1.2 or later). Currently, any secret is encrypted and split across the system in 3 ways. There is very controlled physical access into the IaaS environment, and there are security measures in place to prevent access to customer data.

8. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors is set out below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Type of Personal Data	Service Type	Location of Data Center
Okta	• Account and Registration Data	Single Sign On and Authentication	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 Requirements

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.

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, object to processing, suspension of processing, deletion of the personal data processed by the service. 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 redirected to their employer for a response.

Requests can also 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.

This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement. To the extent this document differs from the Cisco Online Privacy Statement, this document will take precedence. If there is a difference in translated, non-English versions of this document, the U.S.-English version will take precedence.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. 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.