Cisco Secure Endpoint, Orbital, and Talos Threat Hunting

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Endpoint (formerly "AMP for Endpoints"), Orbital, and Talos Threat Hunting.

Secure Endpoint is a cloud-based advanced malware analysis solution made available by Cisco to companies or persons who acquire it for use by their authorized users. Orbital and Talos Threat Hunting are features available within the Advantage and Premier subscription tiers of Secure Endpoint.

Cisco will process personal data from Secure Endpoint, Orbital, and Talos Threat Hunting 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 Secure Endpoint, Orbital and Talos Threat Hunting in order to provide their functionality.

1. Overview

Secure Endpoint is a cloud-based advanced malware analysis and protection solution that provides protection against cyber threats and provides visibility and control over endpoint file activity via connectors that are installed on an endpoint (e.g., Mac, Windows, Linux). When file activity is detected, a file hash and related information are sent to the Secure Endpoint cloud to determine disposition (i.e., clean, malicious, unknown). Secure Endpoint system administrators can manage deployment, groups and policies, reporting, file and device trajectory via a management portal. The customer has the ability to configure Secure Endpoint to limit the amount of data sent to the Secure Endpoint cloud. Secure Endpoint is available in the following tier levels: Secure Endpoint Essential, Secure Endpoint Advantage and Secure Endpoint Premier.

Secure Endpoint Advantage: In addition to the features available in the Essential tier, your Secure Endpoint Advantage subscription includes Cisco Orbital. Orbital is a new advanced capability that is designed to make security investigation and threat hunting simple by providing over a hundred pre-canned and customizable queries, allowing customers to quickly run complex queries on any or all endpoints. Orbital enables customers to gain deeper visibility on any endpoint at any given time by taking a snapshot of its current state.

Secure Endpoint Premier: In addition to the features available in the Essential and Advantage tiers, your Secure Endpoint Premier subscription includes Cisco Talos Threat Hunting. Cisco Talos Threat Hunting leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. If you enroll in Talos Threat Hunting, the Talos team may monitor and access data from any of your provisioned Cisco products in order to provide the Talos Threat Hunting service. If a threat is detected, customers are notified if deemed necessary.

Secure Endpoint integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving personal data from Secure Endpoint. Secure Endpoint may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves Secure Endpoint 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 Secure Endpoint Essentials, Advantage and Premier tiers, please visit
https://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html

This product leverages Cisco's Security Cloud, a unified platform delivering a set of core security and networking services. Through the Cisco Security Cloud, customers have the benefit of threat intelligence delivered by Cisco's security subject matter experts, including Cisco Talos threat research team. Cisco's Security Cloud may enable you to use and manage your Cisco data across Cisco's security products and analyzes how you use your products to improve our services. Cisco's threat intelligence teams conduct research on a broad set of Cisco product data to identify emerging threats at early stages, assess regional and global threat landscapes, and take actions to proactively prevent attacks. Cisco works to continually improve and develop Cisco products to provide a relevant, efficient, and secure experience.

2. Personal Data Processing

The table below lists the personal data processed by Secure Endpoint 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.

Table 1. Personal Data Processed by Secure Endpoint Essentials, Advantage and Premier

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	- Name - Address - Email Address - User ID	Creating an account Data collected for: Product enablement, product use notifications, training and support only
File Names and File Path*	- Name of file - File path name (see examples to the right)	Customer configurable. This feature is enabled at default, but the customer can opt-out. When enabled, the function of this feature is to provide endpoint security. Data collected for: - Product usage - Example: "JonhDoe.doc" - Example: "\\?\C:\Users\JohnDoe\AppData\Local\svc host.exe" - Threat intelligence research - Service delivery - Understand how the product is used - Product improvement and/or development
Network Host Data*	- Local URL, MAC Address, IP address - Remote URL, MAC address, IP address	Not customer configurable. The function of this feature is to provide endpoint security. Data collected for: - Product usage (e.g., Computer Management, Device Flow Correlation in Device Trajectory and Retrospective Security). - Example: "10.1.1.101" - Example: "http://malware-server.com" - Example: "00-14-22-01-23-45" - Threat intelligence research - Service delivery - Understand how the product is used - Product improvement and/or development
User Name*	Customer User Name (see examples to the right)	Customer configurable. This feature is enabled at default, but the customer can opt-out. When enabled, the function of this feature is to provide endpoint security. Data collected for: - Product usage (e.g., Events and Device Trajectory). - Disabled Example: "u@workstation-name" (the "u" is for "user") - Disabled Example: "a@workstation-name" (the "a" is for administrator) - Enabled Example: "johndoe@workstation-name" for user/administrator - Threat intelligence research - Service delivery - Understand how the product is used - Product improvement and/or development

File Analysis Data*	• Entire files captured as unstructured data (see example to the right)	Customer configurable. The customer must "opt-in". When this feature is enabled, the function of this feature is to provide endpoint security.
		Data collected for:
		• Product usage (E.g. File Repository and File Analysis).
		   o Example: "malware.exe" Executed files of low prevalence are fetched automatically (when enabled) and uploaded to Cisco Systems for File Analysis. The entire file is captured as unstructured data for further analysis.
		   o Example: "Document.doc" Administrator requested files are fetched on-demand (when enabled and requested) and uploaded to Cisco Systems for File Analysis. The entire file is captured as unstructured data for further analysis.
		• Threat intelligence research
		• Service delivery
		• Understand how the product is used
		• Product improvement and/or development

Usage Data	Product usage data (i.e.,data related to features utilized when accessing Secure Endpoint) which may include the following personal data: • User first name and last name • User email address	Product usage analytics for product improvement and product decision making. Customer Experience("C/X") initiatives which may include, but are not limited to, customer awareness and adoption activities (e.g. deployment guidance, digital journeys, etc.) and the C/X Cloud for Customers (for eligible customers). Please see the Customer Experience (C/X) Cloud Privacy Data Sheet at the [Cisco Trust Portal](#) for information regarding the processing of personal data by C/X.
User Feedback	• Customer Name • Product rating • Any personal data collected in the open text field[1]	Data captured for product feedback purposes.

* Data that may be processed as part of Cisco's Security Cloud (including Talos services). Cisco processes the data for this purpose in the United States as stated in Section 3 and 9 (subprocessors).

Table 2. Personal Data processed by Secure Endpoint Advantage (which includes Orbital) and Secure Endpoint Premier (which includes Talos Threat Hunting).

Personal Data processed by Secure Endpoint Advantage (which includes Orbital) and Secure Endpoint Premier includes all of the Personal Data from Table 1 and the following additional Personal Data which may be derived via osquery:

Personal Data Category	**Types of Personal Data**	**Purpose of Processing**

Operational Data	• Any data related to a device, including but not limited to: admin username, endpoint user username, all physical characteristics of the hardware on which the application is running, etc.	Data collected for:
		• Product usage (endpoint security)
		   o Example: johndoe, jdoe
		   o Example: Name of device
		   o Example: Installed applications
		   o Example: Hard drive space used/available
		• Threat intelligence research
		• Service delivery

---

[1] Cisco has the ability to tie an individual Secure Endpoint user to the feedback provided, but the subprocessor, Aha.io, listed in Section 3, will not. The personal data processed by Aha.io will be limited to any personal data the user chooses to include in the open text field.

		• Understand how the product is used • Product improvement and/or development

File Activity and File Metadata	• Any data related to file activity or file metadata including but not limited to: file name, file path, cryptographic hash, fuzzy hash, machine learning fingerprint, etc.	Data collected for:
		• Product usage (endpoint security)
		   o Example: "JonhDoe.doc"
		   o Example:
		       \\?\C:\Users\JohnDoe\ApData\Local\svchost.exe
		• Threat intelligence research
		• Service delivery
		• Understand how the product is used
		• Product improvement and/or development

Network Metadata	• Any data related to the network including but not limited to: Network Host Data (IP address, host, query, string, port), Local URL, MAC Address, IP address; Remote URL, MAC address, IP address, etc.	Data collected for:
		• Product usage (e.g., endpoint security, computer management, device flow correlation in device trajectory and retrospective security)
		   o Example: "10.1.1.101"
		   o Example: "http://malware-server.com"
		   o Example: "00-14-22-01-23-45"
		• Threat intelligence research
		• Service delivery
		• Understand how the product is used
		• Product improvement and/or development

osquery Data	• Any personal data that Customer may include in the query, or may receive as the result of a query (i.e. filename, username, host names, etc)	• Data collected for Customer audit purposes • Threat intelligence research • Service delivery • Understand how the product is used • Product improvement and/or development
Other Cisco Product Data	• If you enroll in Talos Threat Hunting, the Talos team may monitor and access data from any of your provisioned Cisco products in order to provide the Talos Threat Hunting service. • Will only pull in data that triggers an event	Data collected for: • Threat intelligence research • Service delivery • Understand how the product is used • Product improvement and/or development

Talos is Cisco's threat intelligence research organization, devoted to protecting Cisco's customers by understanding the broad security threat landscape and distilling security data into verifiable detection or actionable intelligence. In the event of a potential, suspected, or actual security incident, Secure Endpoint may share data collected from your use of the Secure Endpoint with Cisco's security intelligence subject matter experts, including Talos, for proactive and reactive security response purposes.

3. Data Center Locations

Cisco uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Orbital, which is available in both the Secure Endpoint Advantage and Premier subscriptions, processes the personal data in AWS regional clouds located in the United States, Germany and Japan. Talos Threat Hunting, which is available in the Secure Endpoint Premier subscription only, processes personal data in an AWS cloud located in the United States, and the Security Cloud platform (which includes Talos' threat intelligence research team) processes data in the United States.

Data Center Locations	Location of Data Center
Amazon Web Services (AWS) North America Cloud (Secure Endpoint; Orbital; Talos Threat Hunting regional infrastructure)	United States

Zayo North America Co-location Facility (Secure Endpoint infrastructure)	
Equinix Co-location Facilities (Talos threat intelligence research team infrastructure)	
Vazata Co-location Facility (Talos global threat intelligence research team infrastructure)	
AWS EU Cloud. (Secure Endpoint; Orbital regional infrastructure)	Ireland
AWS Asia Pacific Cloud (Secure Endpoint; Orbital regional nfrastructure)	Japan
Aha.io Data Center provider(s): AWS	United States

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 Secure Endpoint, Orbital and Talos Threat Hunting to carry out the service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
Registration Information	Customer	Viewing customer account information in the Secure Endpoint console
	Cisco	Creating an account • Data collected is for product enablement, product use notifications, training and support only
File Name and File Path	Customer	Incident investigation and threat hunting

	Cisco	When enabled, the function of this feature is to provide endpoint security.
		Data collected for:
		• Product usage
		   o Example: "JonhDoe.doc"
		   o Example: "\\?\C:\Users\JohnDoe\AppData\Local\svchost.exe"
		• Threat intelligence research
		• Service delivery
		• Understand how the product is used
		• Product improvement and/or development

Network Host Data	Customer	Data Incident investigation and threat hunting
	Cisco	The function of this feature is to provide endpoint security. Data Collected for: • Product usage (e.g., Computer Management, Device Flow Correlation in Device Trajectory and Retrospective Security) • Threat intelligence research

		• Service delivery • Understand how the product is used • Product improvement and/or development
User Name	Customer	Incident investigation and threat hunting
	Cisco	When enabled, the function of this feature is to provide endpoint security Data collected for: • Product usage (e.g., Events and Device Trajectory). • Threat intelligence research • Service delivery • Understand how the product is used • Product improvement and/or development
File Analysis Data	Customer	Review data, investigate incidents, and collect metrics.
	Cisco	When this feature is enabled, the function of this feature is to provide endpoint security. Data collected for: • Product usage (E.g. File Repository and File Analysis). • Threat intelligence research • Service delivery • Understand how the product is used • Product improvement and/or development
Usage Data	Customer	Product usage analytics and CX initiatives as described in Section 2
	Cisco	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)
User Feedback	Cisco	Product feedback purposes
Operational Data	Customer	Review data, investigate incidents, and collect metrics
	Cisco	Data collected for product usage (endpoint security)
File Activity and File Metadata	Customer	Review data, investigate incidents, and collect metrics
	Cisco	Data collected for product usage (endpoint security)
Network Metadata	Customer	Data Collected for product usage (e.g., endpoint security, computer management, device flow correlation in device trajectory and retrospective security)
	Cisco	Data Collected for product usage (e.g., endpoint security, computer management, device flow correlation in device trajectory and retrospective security)
osquery Data	Customer	Data collected for customer audit purposes
	Cisco	Data collected for customer audit purposes
Other Cisco Product Data	Cisco	Talos Threat Hunting service

6. Data Retention

The table below lists the personal data used by Secure Endpoint, Orbital, and Talos Threat Hunting, 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	• Indefinitely • Deletion upon request	• Creating an account • Product enablement • Product use notifications • Training and support
File Name and File Path **Network Host Data** **User Name**	• Up to 30 days	• Secure Endpoint Console usage • Reporting • Threat Intelligence Research
File Analysis Data	• Up to 24 months[2]	• Mining • Threat Intelligence Research
Usage Data	• Stored by Secure Endpoint until deletion requested by customer opening a TAC case. • Stored by C/X for up to two years	Product improvement and product decision making (such as where to focus future operational and development needs). C/X initiatives
User Feedback	Up to 24 months	Product feedback purposes
Operational Data	Orbital: • 3 days (data from queries on an endpoint) Threat Hunting • Up to 30 days (raw data) • Deletion upon request (investigation data/notifications)	Orbital: • Providing enhanced security analytics and forensics capabilities in product usage • Reporting purposes Threat Hunting: • Raw data—Detect anomalious activity amongst key data points in the telemetry. Internal training. • Investigation data: internal metrics; trend analysis
File Activity and File Metadata	Orbital: • 3 days (data from queries on an endpoint) Threat Hunting • Up to 30 days (raw data) • Deletion upon request (investigation data/notifications)	Orbital: • Providing enhanced security analytics and forensics capabilities in product usage • Reporting purposes Threat Hunting: • Raw data—Detect anomalious activity amongst key data points in the telemetry. Internal training. • Investigation data: internal metrics; trend analysis
Network Metadata	Orbital: • 3 days (data from queries on an endpoint) • Up to 90 days (audit logs) Threat Hunting • Up to 30 days (raw data) • Deletion upon request (investigation data/notifications)	Orbital: • Providing enhanced security analytics and forensics capabilities in product usage • Reporting purposes Threat Hunting: Detect anomalious activity amongst key data points in the telemetry, internal training. • Raw data—Detect anomalious activity amongst key data points in the telemetry. Internal training. • Investigation data: internal metrics; trend analysis
osquery Data	• Up to 6 months Threat Hunting • Up to 30 days (raw data)	Detect anomalious activity amongst key data points in the telemetry
Other Cisco Product Data	• If your subscription includes Talos Threat Hunting, the Talos team may monitor and access	Data collected for: • Threat intelligence research • Service delivery • Understand how the product is used

---

[2] Customers have the ability to delete (via their Secure Endpoints console) to delete these files from their file repository. Neither Cisco nor the customer can view the file in Secure Endpoint.

	data from any of your provisioned Cisco products in order to provide the Talos Threat Hunting service. • Talos Threat Hinting will only pull in data that triggers an event	• Product Improvement and/or development

If data is processed as part of the Security Cloud, such data will be retained for no longer than 6 months.   Any data that is determined to be malicious by Talos, aggregated or de-identified data may be retained for longer.

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 in transit in encrypted using TLS v1.2 • Data at rest is stored unencrypted with strict access control
File Names and File Path	• Data in transit for Secure Endpoint, Orbital is encrypted using TLS v1.2 • Data at rest within Secure Endpoint, Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
Network Host Data	• Data in transit for Secure Endpoint, Orbital is encrypted using TLS v1.2 • Data at rest within Secure Endpoint, Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
User Name	• Data in transit for Secure Endpoint, Orbital, is encrypted using TLS v1.2 • Data at rest within Secure Endpoint, Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
File Analysis Data	• Data in transit for Secure Endpoint, Orbital is encrypted using TLS v1.2 • Data at rest within Secure Endpoint, Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
Usage Data	• Data in transit for Secure Endpoint and C/X is encrypted using TLS v1.2 • Data at rest within Secure Endpoint is stored unencrypted with strict access control • Data at rest within C/X is encrypted
User Feedback	• Data at rest within Secure Endpoint is stored unencrypted with strict access control
Operational Data	• Data in transit for Orbital is encrypted using TLS v1.2 • Data at rest within Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
File Activity and File Metadata	• Data in transit for Orbital is encrypted using TLS v1.2 • Data at rest within Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
Network Metadata	• Data in transit for Orbital is encrypted using TLS v1.2 • Data at rest within Orbital is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest

osquery Data	• Data in transit for Orbital and Talos Threat Hunting is encrypted using TLS v1.2 • Data at rest within Orbital and Talos Threat Hunting is stored unencrypted with strict access control • Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) is encrypted in transit and at rest
Other Cisco Product Data	• Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 • Data collected by the Security Cloud (including Talos) 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	Type of Personal Data	Service Type	Location of Data Center
AWS	• Registration Information • File Names and File Path • Network Host Data • User Name • File Analysis Data • Operational Data • File Activity and File Metadata • Network Metadata • osquery Data	Secure Endpoint, Orbital and Talos Threat Hunting leverages cloud technology to provide improved malware protection capabilities. Amazon Web Services Cloud helps provide a global service footprint, security assurance, service elasticity and resilience to Secure Endpoint, Orbital and Talos Threat Hunting.	Secure Endpoint and Orbital: United States, Japan, Ireland Talos Threat Hunting: United States
Snowflake Computing	• Usage Data	Cloud data warehouse solution for C/X	AWS United States
Aha.io	• User Feedback	Feedback repository and roadmap tool for storing requests for product improvements to help prioritize features for development	AWS United States
Databricks	• File names and File Path • Network Host Data • Username • File Analysis Data	Data Analytics	United States
Chaos Search	• File names and File Path • Network Host Data • Username • File Analysis Data	Data Analytics	United States
Morphisec	• Any personal data that may be contained in log or files submitted by customer for support	Support	Israel

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), the Advanced Security Initiatives Group (ASIG), and Cisco Legal.

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 Services are built with security and privacy in mind and are designed so that they can be used by Cisco customers in a manner consistent with global security and privacy requirements.

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

11. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, data portability and / or deletion of the personal data processed by the Service as well as object to processing. Except with respect to Registration Information, the customer has the ability to forward the personal data processed by Secure Endpoint to a third party data store. Customers may request assistance from Secure Endpoint Engineering for a large scale movement of data (e.g. customer does not renew subscription and asks for all data to be transferred to a third party data store).

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:

Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES

Americas Privacy Officer	**APJC Privacy Officer**	**EMEA Privacy Officer**
Cisco Systems, Inc.	Cisco Systems, Inc.	Cisco Systems, Inc.
170 W. Tasman Drive	Bldg 80, Lvl 25, Mapletree Biz City,	Haarlerbergweg 13-19, 1101 CH
San Jose, CA 95134	80 Pasir Panjang Road,	Amsterdam-Zuidoost NETHERLANDS
UNITED STATES	Singapore, 117372	
	SINGAPORE	

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 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.

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.