Cisco Secure Endpoint (formerly "AMP for Endpoints"); Orbital, SecureX Threat Hunting

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Endpoint, Orbital and SecureX 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 SecureX 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 SecureX 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 SecureX Threat Hunting in order to provide their functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

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: 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.

Please see the following link for more details on Orbital: https://orbital.amp.cisco.com/help/

Secure Endpoint Premier: Your Secure Endpoint Premier subscription includes Cisco SecureX Threat Hunting. Cisco SecureX Threat Hunting leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. Once threats are detected, customers are notified customers so they can begin remediation.

Please see the following link for more details on Cisco SecureX Threat Hunting:
https://www.cisco.com/c/dam/en/us/products/collateral/security/amp-for-endpoints/amp4e-premier-aag.pdf

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.

Note, 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

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.

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 is 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\svchost.exe"
		• Cisco global threat intelligence research

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"
		• Cisco global threat intelligence research

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
		• Cisco global threat intelligence research

Files 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).
		  ○ 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.
		  ○ 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.
		• Cisco global threat intelligence research.

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("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 CX.

User Feedback	• Customer Name • Product rating • Any personal data collected in the open text field[1]	Data captured for product feedback purposes.

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

-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) ○ Example: johndoe, jdoe ○ Example: Name of device ○ Example: Installed applications ○ Example: Hard drive space used/available
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) ○ Example: "JonhDoe.doc" ○ Example: "\\?\C:\Users\JohnDoe\AppData\Local\svchost.exe"
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). ○ Example: "10.1.1.101" ○ Example: "http://malware-server.com" ○ Example: "00-14-22-01-23-45"
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.

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. SecureX 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 Cisco Talos global threat intelligence research team processes data in an Equinix cloud located in the United States.

Data Center Locations	Location of Data Center
Amazon Web Services (AWS) North America Cloud (Secure Endpoint; Orbital; SecureX Threat Hunting regional infrastructure)	United States
Zayo North America Co-location Facility (Secure Endpoint infrastructure)	

[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.

Data Center Locations	Location of Data Center
Equinix Co-location Facilities (Talos global 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 SecureX 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
		  ○ Example: “JonhDoe.doc”
		  ○ Example: “\\?\C:\Users\JohnDoe\AppData\Local\svchost.exe”
		Cisco global threat intelligence research

Network Host Data	Customer	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) • Cisco global threat intelligence research
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).

		• Cisco global threat intelligence research
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). • Cisco global threat intelligence research.
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.
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.

6. Data Portability

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).

7. Data Deletion and Retention

The table below lists the personal data used by Secure Endpoint, Orbital and SecureX 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 • Global Threat Intelligence Research

File Analysis Data	• Up to twenty-four (24) months[2]	• Mining • Global Threat Intelligence Research
Operational Data	Orbital: • Three (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: • Three (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: • Three (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	Detect anomalious activity amongst key data points in the telemetry
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). Customer experience initiatives.
User Feedback	• Up to 24 months	Product feedback purposes.

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.

A note on Cisco Talos: Talos is Cisco's trusted global threat intelligence research team. In order to continually secure Cisco's Security portfolio, certain Security products share data with Talos, which Talos then processes for global threat intelligence research purposes. All data transferred to Talos from Cisco Security products is encrypted in transit. Upon arrival in the Talos data center, such data is in a continuous state of processing to determine whether it includes, or is indicative of, a malicious behavior or activity. If Talos determines the data is not malicious, it is deleted as noted in Section 7 herein. Any data that is determined to be malicious is retained by Talos, remaining in a constant state of processing, unless Talos determines it is no longer malicious, at which point, it will be deleted. Data within Cisco Talos is encrypted at rest.

Personal Data Category	Security Controls and Measures
Registration Information	• Data in transit in encrypted • Data at rest is stored unencrypted with strict access control.
File Names and File Path	• Data in transit for Secure Endpoint, Orbital, SecureX Threat Hunting and Talos is encrypted

[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 at rest within Secure Endpoint, Orbital and Securex Threat Hunting is stored unencrypted with strict access control • Data at rest within Talos is encrypted
Network Host Data	• Data in transit for Secure Endpoint, Orbital, SecureX Threat Hunting and Talos is encrypted • Data at rest within Secure Endpoint, Orbital and Securex Threat Hunting is stored unencrypted with strict access control • Data at rest within Talos is encrypted
User Name	• Data in transit for Secure Endpoint, Orbital, SecureX Threat Hunting and Talos is encrypted • Data at rest within Secure Endpoint, Orbital and Securex Threat Hunting is stored unencrypted with strict access control • Data at rest within Talos is encrypted
File Analysis Data	• Data in transit for Secure Endpoint, Orbital, SecureX Threat Hunting and Talos is encrypted • Data at rest within Secure Endpoint, Orbital and Securex Threat Hunting is stored unencrypted with strict access control • Data at rest within Talos is encrypted
Operational Data	• Data in transit for Orbital and SecureX Threat Hunting is encrypted • Data at rest within Orbital and SecureX Threat Hunting is stored unencrypted with strict access control
File Activity and File Metadata	• Data in transit for Orbital and SecureX Threat Hunting is encrypted • Data at rest within Orbital and SecureX Threat Hunting is stored unencrypted with strict access control
Network Metadata	• Data in transit for Orbital and SecureX Threat Hunting is encrypted • Data at rest within Orbital and SecureX Threat Hunting is stored unencrypted with strict access control
osquery Data	• Data in transit for Orbital and SecureX Threat Hunting is encrypted • Data at rest within Orbital and SecureX Threat Hunting is stored unencrypted with strict access control
Usage Data	• Data in transit for Secure Endpoint and C/X is encrypted • 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.

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 the service is below:

Sub-processor	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 SecureX 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 SecureX Threat Hunting.	Secure Endpoint and Orbital: United States, Japan, Ireland SecureX 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

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 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.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service 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:

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	**APJC Privacy Officer** Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	**EMEA Privacy Officer** Cisco Systems, Inc. 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, go to the Personal Data Privacy section of the Cisco Trust Center.