Offer Disclosure

Cisco Secure Endpoint, Orbital, and Talos Threat Hunting

This Offer Disclosure provides detailed information about data handling practices, security controls, and AI features specific to this Cisco Offer. It complements the General Disclosures, which outline Cisco's overarching approach to handling Customer Systems Information and Customer Content, and the Cisco Online Privacy Statement, which offers a more in-depth explanation of how Cisco manages personal data. Together, these documents provide transparency by addressing data handling at both a high level and an Offer specific level, helping you understand how Cisco protects and processes information across its Offers.

Capitalized words not otherwise defined in this Offer Disclosure have the meanings set forth in the Cisco General Terms or General Disclosures. To the extent this document differs from the Cisco Online Privacy Statement or General Disclosures, this document will take precedence regarding Offer specific information. If there is a difference in the translated, non-English versions of this document, the US-English version will take precedence.

Cisco will review and update this disclosure on an annual basis, or as needed, to reflect material changes in the processing of Customer Systems Information or Customer Content. For updates, subscribe via the "subscribe" option in the upper right corner of the Trust Portal.

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. In addition to the standard features, your subscription may also include access to Cisco Orbital and Cisco Talos Threat Hunting.

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.

©2025 Cisco and/or its affiliates. All rights reserved

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 Offer Disclosure Document(s) 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.

Many Cisco Offers either require that the Offer be accessed through Cisco Security Cloud Control or optionally allow access to the Offer through Cisco Security Cloud Control. If you access this Cisco Offer through Cisco Security Cloud Control, please see the Cisco Security Cloud Control Offer Disclosure for further details regarding data handling and security controls.

For more information about Cisco Secure Endpoint, Orbital and Talos Threat Hunting, visit https://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html.

2. Data Handling

2a. Collection, Purpose & Retention

Cisco believes in transparency when it comes to how Cisco handles Customer Content and Customer Systems Information. This disclosure provides details about the types of data Cisco collects, specific data elements involved, the purposes for which they are used, and how long Cisco retains them for this Cisco Offer.

The 'Purposes' reflected in this Offer Disclosure are complementary to, and do not limit, permissible purposes as set forth in the General Disclosures.

Table 1: Customer Content processed by **Secure Endpoint Essentials, Secure Endpoint Advantage and Secure Endpoint Premier**

Data Category	Data Elements	Purposes	Retention Period
File Name and File Path Data[1] ***Customer configurable. This feature is enabled at default, but the customer can opt-out.***	**Personal Data:** ▪ Any personal data contained in any of the following: File name; File path name *Examples:* ○ *JonhDoe.doc* ○ *\\?\C:\Users\JohnDoe\AppData\Local\svchost.exe* **Non-Personal Data:** ▪ Any non-personal data contained in any of the following: File name; File path name	▪ Product enablement ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	▪ Up to 30 days
Network Host Data[1]	**Personal Data:**		▪ Up to 30 days

©2026 Cisco and/or its affiliates. All rights reserved

Not customer configurable.	▪ Any personal data contained in any of the following: Local URL; Local MAC address; Local IP address; Remote URL; Remote MAC address; Remote IP address *Examples:* ○ *10.1.1.101* ○ *http://malware-server.com* ○ *00-14-22-01-23-45* **Non-Personal Data:** • Any non-personal data contained in any of the following: Local URL; Local MAC address; Local IP address; Remote URL; Remote MAC address; Remote IP address	▪ Product enablement (e.g., computer management, device flow correlation trajectory and retrospective security) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	
Username Data[1] ***Customer configurable. This feature is enabled at default, but the customer can opt-out.***	**Personal Data:** ▪ Any personal data contained in customer username *Disabled Examples:* ○ *u@workstation-name (the "u" is for "user")* ○ *a@workstation-name (the "a" is for administrator)* *Enabled Example:* ○ *johndoe@workstation-name for user/administrator* **Non-Personal Data:** ▪ Any non-personal data contained in customer username	▪ Product enablement (e.g., events and devices trajectory) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	▪ Up to 30 days
File Analysis Data[1] *Customer configurable. The customer must "opt-in".*	**Personal Data:** ▪ Any personal data contained in entire files capture as unstructured data Examples: ○ *"malware.exe" Executed files of low prevalence are fetched automatically (when enabled) and uploaded for File Analysis. The entire file is captured as unstructured data for further analysis.* ○ *"Document.doc" Administrator requested files are fetched on-demand (when enabled and requested) and uploaded for File Analysis. The entire file is captured as unstructured data for further analysis.* **Non-Personal Data:** ▪ Any non-personal data contained in entire files captured as unstructured data	▪ Product enablement (e.g., file repository and file analysis) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	▪ Up to 24 months[2]

Table 2: Customer Content processed by **Secure Endpoint Advantage and Secure Endpoint Premier**

Data processed by Secure Endpoint Advantage (which includes Orbital) and Premier (which includes Talos Threat Hunting) includes all data categories from Table 1 and the following additional data categories which may be derived via osquery:

[1] These data categories may be processed as part of Cisco's Security Cloud Control (including Talos services). Cisco processes the data for this purpose in the United States as stated in Table 4 and Table 5.
[2] Customers have the ability to delete these files from their file repository (via the Secure Endpoints console). Neither Cisco nor the customer can view the file in Secure Endpoint.

©2026 Cisco and/or its affiliates. All rights reserved

Data Category	Data Elements	Purposes	Retention Period
osquery Data	**Personal Data:** ▪ Any personal data that customer may include in the query, or that customer may receive as the result of a query (e.g., filename, username, host names, etc. **Non-Personal Data:** ▪ Any non- personal data that customer may include in the query, or that customer may receive as the result of a query (e.g., filename, username, host names, etc.	▪ Customer audit purposes ▪ Product enablement ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	Orbital ▪ Up to 6 months Talos Threat Hunting ▪ Raw data: Up to 30 days
Data from Other Cisco Products	**Personal Data:** ▪ Any personal data retrieved from another provisioned Cisco product. 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. Talos will only pull in data that triggers an event. **Non-Personal Data:** • Any non-personal data retrieved from another provisioned Cisco product. 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. Talos will only pull in data that triggers an event	▪ Product enablement ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	▪ If your subscription includes 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.

Cisco Talos

Talos is Cisco's threat intelligence research organization, devoted to protecting Cisco 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.

Table 3: Customer Systems Information

Data Category	Data Elements	Purposes	Retention Period
Registration Data	**Personal Data:** ▪ Customer information, including first and last name, email address, and User ID **Non-Personal Data:** ▪ Company account information, including billing address, phone number, Smart Account username/ID	▪ Account creation ▪ Product enablement ▪ Product use notifications ▪ General product support and training	▪ Deletion upon request.
Usage and User Feedback Data	**Personal Data:**	▪ Product usage analytics	

©2026 Cisco and/or its affiliates. All rights reserved

	▪ Product usage data (i.e., data related to features utilized when accessing this Offer), which may include the following personal data and associated usage information: User first name and last name; User ID; Email address; Feedback (including any personal data included by a user in a free text field or survey response) **Non-Personal Data:** ▪ Product usage data (i.e., data related to features utilized when accessing this Offer, which may include the following non-personal usage data: Session data; Product usage data, such as pages visited, elements clicked, links clicked, user's browser and operating system, cookie information, session metadata, API usage; Feedback (including product rating, and any non-personal data included by a user in a free text field or survey response)	▪ Product improvement and/or development ▪ 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 Offer Disclosure Documents at the Cisco Trust Portal for information regarding the processing of data by the CX.	▪ Deletion upon request. Deletion request may be made by opening a Cisco TAC case or by sending an email to privacy@cisco.com. ▪ Stored by Cisco CX for up to two (2) years.
Operational Data	**Personal Data:** ▪ Any personal data included in data related to a device/endpoint, such as: admin username, endpoint user username, all physical characteristics of the hardware on which the application is running, etc. *Examples:* ◦ *johndoe, jdoe* ◦ *name of device* ◦ *installed applications* ◦ *hard drive space used/available* **Non-Personal Data:** ▪ Any non-personal data included in data related to a device/endpoint, such as admin username, endpoint user username, all physical characteristics of the hardware on which the application is running, etc.	▪ Product enablement (e.g., file repository and file analysis) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	Orbital ▪ Data from queries on an endpoint: 3 days Talos Threat Hunting ▪ Raw data: Up to 30 days ▪ Investigations data/notifications: Deletion upon request
File Activity and File Metadata	**Personal Data:** ▪ Any personal data included in data related to file activity or file metadata, such as file name, file path, cryptographic hash, fuzzy hash, machine learning fingerprint, etc. Examples: ◦ JohnDoe.doc ◦ \\?\C:\Users\JohnDoe\AppData\Local\svchost.exe **Non-Personal Data:** ▪ Any non-personal data included in data related to file activity or file metadata, such as file name, file path, cryptographic hash, fuzzy hash, machine learning fingerprint, etc.	▪ Product enablement (e.g., file repository and file analysis) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development ▪ Threat intelligence research	Orbital ▪ Data from queries on an endpoint: 3 days Talos Threat Hunting ▪ Raw data: Up to 30 days ▪ Investigations data/notifications: Deletion upon request
Network Metadata	**Personal Data:** ▪ Any personal data included in data related to the network, such as: Network host data (IP address, host, query, string, port), Local URL, Local MAC address, Local IP address, Remote URL Remote MAC address, Remote IP address, etc. Examples:	▪ Product enablement (e.g., file repository and file analysis) ▪ Analyze product/feature usage and functionality ▪ Product improvement and/or development	Orbital ▪ Data from queries on an endpoint: 3 days Talos Threat Hunting ▪ Raw data: Up to 30 days

©2026 Cisco and/or its affiliates. All rights reserved

	○ *10.1.1.101* ○ *http://malware-server.com* ○ *00-14-22-01-23-45* **Non-Personal Data:** ▪ Any personal data included in data related to the network, such as: Network host data (IP address, host, query, string, port), Local URL, Local MAC address, Local IP address, Remote URL Remote MAC address, Remote IP address, etc.	▪ Threat intelligence research	▪ Investigations data/notifications: Deletion upon request
Configuration Data	**Personal Data:** ▪ Configuration data is typically non-personal data, such as setting and user preferences **Non-Personal Data:** ▪ Customer-specific requirements, preferences, and policy settings	▪ Tailor the functionality of the system to customer-specific requirements or preferences	▪ Retained throughout subscription ▪ Deletion upon request.

2b. Storage and Processing

Data Centers. Cisco uses 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 Control platform (which includes Talos' threat intelligence research team) processes data in the United States.

Table 4: Data Centers

Infrastructure Provider	Infrastructure Provider Locations	Description
Amazon Web Services ("AWS") North America Cloud	United States – Oregon, Virginia California (backup for Endpoint) Ohio (backup for Orbital)	Regional infrastructure for Secure Endpoint, Orbital, and Talos Threat Hunting
AWS EU Cloud	Germany France (backup)	Regional infrastructure for Orbital
AWS EU Cloud	Ireland Germany (backup)	Regional infrastructure for Secure Endpoint
AWS Asia Pacific Cloud	Japan Australia (backup for Endpoint) India (backup for Orbital)	Regional infrastructure for Secure Endpoint and Orbital
Equinix	United States	Co-location facility for Talos threat intelligence research team
Vazata	United States	Co-location facility for Talos threat intelligence research team
DataBank (formerly, Zayo)	United States - Virginia	Co-location facility for Secure Endpoint infrastructure

©2026 Cisco and/or its affiliates. All rights reserved

Service Providers

Cisco may share Customer Systems Information and Customer Content with a trusted ecosystem of suppliers. In each instance, each participant has agreed to confidentiality terms, compliance with applicable law, and adherence to information security, privacy, and other data processing requirements with Cisco that are consistent with Cisco's commitments to you.

Subcontractors assist with broader data processing services, while subprocessors specifically process Personal Data on Cisco's behalf to support the functionality of the Cisco Offer.. For updates, subscribe via the "subscribe" option in the upper right corner of the Trust Portal.

Cisco Secure Endpoint, Orbital and Talos Threat Hunting do not use subcontractors to provide its Offer capabilities.

Table 5: Subprocessors

Subprocessor	Personal Data	Service Type	Data Center Location
AWS	▪ File Name and File Path Data ▪ Network Host Data ▪ Username Data ▪ File Analysis Data ▪ Registration Data ▪ Operational Data ▪ File Active and File Metadata ▪ Network Metadata ▪ osquery Data ▪ Configuration 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: Japan Ireland United States – Virginia Talos Threat Hunting: United States
Aha!	▪ User Feedback Data	Feedback repository and roadmap tool for storing requests for product improvements to help prioritize features for development	United States – California, Ohio, Oregon, Virginia
Chaos Search	▪ File Name and File Path Data ▪ Network Host Data ▪ Username Data ▪ File Analysis Data	Data analytics	United States – Virginia
Databricks	▪ File Name and File Path Data ▪ Network Host Data ▪ Username Data ▪ File Analysis Data	Data analytics	United States – Virginia
Morphisec	▪ Any personal data that may be contained in logs or files submitted by customer for support	Support	Israel
Snowflake Computing	▪ Usage Data	Cloud data warehouse solution for CX	United States – Virginia

Technical Support and Operations

Customer support is provided by Cisco Technical Assistance (TAC), utilizing a 24/7 "follow the sun" technical support model. More information regarding Cisco TAC can be found in the Cisco TAC Offer Disclosure.

©2026 Cisco and/or its affiliates. All rights reserved

2c. Access and Sharing

Cisco makes certain Customer Systems Information available to Customers and their authorized third parties in a structured, commonly used machine-readable format through the following standardized APIs, consistent with the specifications provided in the Cisco API Guidelines.

- Cisco Secure Endpoint API: https://developer.cisco.com/docs/secure-endpoint/.

Customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels.

3. Security

3a. Access Control and Encryption

Cisco has implemented reasonable and appropriate technical and organizational measures designed to protect data from accidental loss, unavailability, and unauthorized access, use, alteration, and disclosure.

Table 6: Access & Controls

Data Category	Who Has Access	Purpose of Access	Security Controls
File Name and File Path Data	Customer	Incident investigation; threat hunting	▪ Data in transit for Secure Endpoint and Orbital is encrypted using TLS v1.2 ▪ Data at rest within Secure Endpoint and 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
Network Host Data	Customer	Data review; incident investigation; threat hunting	▪ Data in transit for Secure Endpoint and Orbital is encrypted using TLS v1.2 ▪ Data at rest within Secure Endpoint and 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
Username Data	Customer	Incident investigation; threat hunting	▪ Data in transit for Secure Endpoint and Orbital is encrypted using TLS v1.2 ▪ Data at rest within Secure Endpoint and 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
File Analysis Data	Customer	Data review; incident investigation; metric collection	▪ Data in transit for Secure Endpoint and Orbital is encrypted using TLS v1.2

©2026 Cisco and/or its affiliates. All rights reserved

	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	▪ Data at rest within Secure Endpoint and 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
osquery Data	Customer	Customer audit purposes	▪ 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
		Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
Data From Other Cisco Products	Cisco	Product enablement for Talos Threat Hunting service	▪ Data collected by Talos Threat Hunting is stored in transit and at rest using TLS v1.2 ▪ Data collected by Security Cloud Control (including Talos) is encrypted in transit and at rest
Registration Data	Customer	Account administration and operations	▪ Data in transit is encrypted using TLS v1.2 ▪ Data at rest is stored unencrypted with strict access control
	Cisco	Account creation; product enablement; product use notifications; general product support and training	
Usage and User Feedback Data	Customer	Customers with access to the CX Cloud for Customers have access to their usage data for internal analysis. Customer can elect to share data with designated Cisco partners through the CX Cloud for Customers	▪ Data in transit for Secure Endpoint and CX is encrypted using TLS v1.2 ▪ Data at rest within Secure Endpoint is stored unencrypted with strict access control ▪ Data at rest within CX is encrypted
	Cisco	Product usage analytics; product feedback; CX initiatives	
Operational Data	Customer	Data review; incident investigation; metric collection	▪ 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
File Activity and File Metadata	Customer	Data review; incident investigation; metric collection	▪ 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
Network Data	Customer	Product usage (e.g., endpoint security, computer management, device flow	▪ Data in transit for Orbital is encrypted using TLS v1.2

©2026 Cisco and/or its affiliates. All rights reserved

		correlation in device trajectory and retrospective security)	▪ 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 Security Cloud Control (including Talos) is encrypted in transit and at rest
	Cisco	Product enablement; product usage analytics; product improvement and/or development; threat intelligence research	
Configuration Data	Customer	Account administration and operations	Data is encrypted in transit and at rest
	Cisco	Product enablement	

3b. Reports & Resources

In addition to complying with internal standards, Cisco maintains third-party validations and certifications to demonstrate its commitment to robust information security and privacy. The General Disclosures describe Cisco's enterprise-wide certifications. The following additional resources and certifications apply specifically to this Cisco Offer:

- SOC 2 Type 2
- ISO/IEC 27001:2013
- Cloud Computing Compliance Criteria Catalog (C5)
- CAIQ
- ENS
- Texas Risk and Authorization Management Program (TX-RAMP)

©2026 Cisco and/or its affiliates. All rights reserved