Cisco Umbrella

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

Cisco Umbrella is a cloud-based security solution made available by Cisco to companies or persons who obtain a Cisco Umbrella cloud service subscription.

Cisco will process personal data from Cisco Umbrella 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 and the Data Processor for the personal data processed by Cisco Umbrella in order to provide its functionality.

1. Overview

Cisco Umbrella is a cloud security product that unifies multiple security services in a single cloud-delivered platform to secure internet access and control cloud app usage from your network, branch offices, and roaming users. Depending on the package and deployment, Cisco Umbrella integrates secure web gateway, cloud-delivered firewall, DNS-layer security, cloud malware protection, application discovery, data loss prevention (DLP), remote browser isolation (RBI) and more, for effective protection anywhere users go. Before users connect to any online destination, Cisco Umbrella acts as a secure onramp to the Internet and delivers deep inspection and control to support compliance and block threats. Cisco Umbrella is backed by one of the largest threat intelligence teams in the world, Cisco Talos, and it provides interactive access to threat intelligence through Cisco Umbrella Investigate to aid in incident response and threat research. Cisco Umbrella Investigate provides access to certain Cisco threat intelligence about malicious domains, IPs, networks, and file hashes. Using a diverse dataset of billions of daily DNS requests and live views of the connections between different networks on the Internet, Cisco applies statistical models and human intelligence to identify attackers' infrastructures. Please consult the Umbrella Documentation for further information on its technical specifications, configuration requirements, features, and functionalities.

Because Cisco Umbrella processes, stores, and analyzes DNS, web and full traffic depending on package and deployment, and where applicable, processes and stores identity information, it processes certain personal data of the administrative users and other users who are protected by the service. The processed data is used to set-up and deliver the service, provide reporting, conduct threat intelligence security research, provide product improvements and for the other purposes described in this Privacy Data Sheet. Cisco's security research includes aggregating the processed data to track and predict threats and using such data to provide predictive threat intelligence for its customers. This Privacy Data Sheet describes which personal data Cisco processes to deliver its services, the location of that data and how it is secured in accordance with privacy principles, laws, and regulations.

If you are using a Cisco Umbrella package that includes the selective web proxy (also known as intelligent proxy) or full proxy capabilities, or the Cisco Umbrella cloud malware feature, Cisco Umbrella may send file hashes and/or files submitted to Cisco Umbrella to the Cisco Secure Malware Analytics cloud service for malware analysis and further threat intelligence research. For information regarding the processing of personal data by the Cisco Secure Malware Analytics cloud service, please see the Secure Malware Analytics Cloud Service Cisco Trust Portal.

Cisco Umbrella offers single sign-on through Cisco Security Cloud Sign-On. For information regarding the processing of personal data by Cisco Security Cloud Sign-On , please see Cisco Security Cloud Sign-On Privacy Data Sheet available on the Cisco Trust Portal.

Umbrella integrates with various Cisco cloud services including, but not limited to, those referenced above. If you elect to enable or leverage integration between Cisco Umbrella and another Cisco cloud service or feature, you should also review the data sheet of such other cloud service or feature for information regarding the personal data collected, processed, and stored by that cloud service or feature by visiting the Cisco Trust Portal. Cisco Umbrella also integrates with various third-party systems. You are responsible for ensuring You have the proper data protection agreement(s) in place with any third parties to whom You elect to send data.
For more information about Cisco Umbrella, visit https://umbrella.cisco.com/. To see which features are available with the Umbrella packages, see https://umbrella.cisco.com/products/umbrella-enterprise-security-packages.

2. Personal Data Processing

The table below lists the personal data processed by Cisco Umbrella to provide its services and describes why the data is processed. Only certain processed data is retained. The "Types of Personal Data Processed" column covers all data processed, not all of which is retained by Cisco after processing. Please see Section 6 of this Privacy Data Sheet for details on which personal data is retained and the duration of retention.

Table 1

Personal Data Category	Type of Personal Data	Purpose of Processing
Account/Contact Information	• Dashboard/console user email address and name • Company account information (Company name, street, city, state/region, country, phone number, Unique numerical account ID) • Billing contact name	• Activation of service • Billing/invoicing • Future notification of features/updates • Support • Authentication/Authorization • Managing subscription entitlements • Renewals
DNS Layer Security[1] Usage and Event Data	• Personal data contained in DNS query data (IP address/origin IP, destination domain name) • Personal data contained in DNS logs (IP address/origin ID, destination domain name, DNS record type, DNS response) • Device ID • Cloud apps associated with user or device	• DNS query data is initially processed to direct end user to domain being queried, to provide DNS layer security and content categorization and filtering (based on customer policies), to determine applications used, and to provide customer reporting • Threat intelligence research, product improvement, and service delivery through the Cisco Security Cloud platform, including Talos threat intelligence research (excludes DNS Layer Security Usage and Event Data of customers selecting EU data storage)
	If using DNS block page: • HTTP/HTTPS header info and URL, excluding HTTP/HTTPS body content	• Provide granular protection at URL and file level • Threat intelligence research, product improvement, and service delivery through the Cisco Security Cloud platform, including Talos threat intelligence research (excludes DNS Layer Security Usage and Event Data of customers selecting EU data storage)
	If using optional selective proxy feature: • Personal data included in web traffic (HTTP/HTTPS) that is intercepted and proxied by selective proxy (i.e., traffic associated with certain uncategorized or risky domains), including personal data in headers, URLs, and body content (e.g., files) • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs[2] • Cloud apps associated with user or device	Provide granular protection at URL and file level and to implement customer policies. Note: • Headers are processed to identify proxy specific headers • URLs are processed to identify malicious URLs, or URLs matching a customer URL destination or content category block list • Body content is processed for malware inspection

[1] Identity data (e.g., active directory, IdP, Google Workspace, username, userID and other identity information described under "Configuration Information") is not stored by Cisco with the DNS Layer Security or Secure Web Gateway Usage and Event Data. Cisco pairs such identity data with the Usage and Event Data at time of display in the Umbrella Dashboard, for purposes of reporting using Reporting API, and upon exporting the Usage and Event Data to a customer specific AWS S3 bucket. Customers have the option to have Usage and Event Data logs exported to a Cisco managed S3 bucket for up to 30 days or to have their logs exported to a customer managed S3 bucket. If customer opts to log HTTPS query, then the full query parameter is included in the log data exported to S3. If customer opts not to log HTTPs query, then query parameters are logged by Cisco only for HTTP and not for HTTPS.

[2] Logging all requests is the default setting for selective proxy. However, customers have the option to turn off logging for all requests or to limit logging to only security events (see: https://docs.umbrella.com/deployment-umbrella/docs/log-management)

		• Files sent to Cisco Umbrella are inspected to provide malware analysis and threat intelligence product function • Threat intelligence research, product improvement, and service delivery through the Cisco Security Cloud platform, including Talos threat intelligence research (excludes DNS Layer Security Usage and Event Data of customers selecting EU data storage)
Secure Web Gateway[1] Usage and Event Data	• Personal data included in web traffic (HTTP/HTTPS), including headers, URLs, and body content (e.g., files) • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs)[3] • Cloud apps associated with user or device • Device ID • Origin ID • End User IP • Username is included in transaction data sent to Umbrella but converts to a unique ID for storage in data warehouse. Like Umbrella, the identity data and username are paired with the log data in the dashboard for reporting purposes.	Provide granular protection at URL and file level and to implement customer policies. Note: • Headers are processed to identify proxy specific headers • URLs are processed to identify malicious URLs, or URLs matching a customer URL destination or content category block list • Body content (including files) is inspected for malware and DLP • Threat intelligence research, product improvement, and service delivery through the Cisco Security Cloud platform, including Talos threat intelligence research (excludes Secure Web Gateway Usage and Event Data of customers selecting EU data storage)
Cloud-Delivered Firewall Usage and Event Data	• All personal data included in ports and protocol meta information including packet content, source IP and port, destination IP and port, application (e.g., Webex), date, and timestamp[4]	• Provide granular protection at URL and file level (however, Cloud Delivered Firewall does not decrypt encrypted packet content)
Cloud Malware Usage and Event Data	• User ID and/or e-mail address • User first and last name • IP Addresses for end users • Any other personal data that may be inspected for malware because it is stored on the applicable cloud environment	• Discover, monitor, control, and act on malware (including personal data) stored in files and application fields by a customer's users in the applicable cloud (SaaS) environment

Data Loss Prevention Usage and Event Data	• For SaaS API-based DLP and Real-Time DLP
	  ◦ File name (if includes personal data)
	  ◦ Personal data in files, messages or other content inspected by DLP
	  ◦ Snippet of policy violation and surrounding text if policy violation detected
	• For SaaS API-based DLP:
	  ◦ the email address and display name of users in customers' cloud (SaaS) environments that will be monitored with such service
	  ◦ email address and display name of collaborators of a changed file
	  ◦ File id of file detected to contain data violations
	• For Real Time DLP:
	  ◦ If configured, user identity data through AD/IdP
	  ◦ Real Time DLP will scan outbound and certain inbound traffic and any personal data included in such traffic. See Secure Access User Guide for more information regarding Real Time DLP inbound and outbound scanning.
		• Discover, monitor, and act on (e.g., block) sensitive information (including personal data) in files, messages, and other content in transit through the Umbrella service (for Real Time DLP) and in the applicable cloud (SaaS) environment (for SaaS API-based DLP)
		• Detection of sensitive information is done using customer-selected or customer-defined policies, such as a policy that looks for a pattern or expression matching a credit card number or social security number. When a policy identifies a potential violation (i.e., match), a record is established
		• The content inspected by DLP is not stored in full. Cisco provided policies redact key sensitive content (e.g., providing only the last 4 digits of a credit card) with only the snippet of the policy violation and surrounding text being stored as part of the DLP Event Data per Section 6

[3] Logging all requests is the default setting for Secure Web Gateway (full proxy). However, customers have the option to turn off logging or to log only security events (see: https://docs.umbrella.com/umbrella-user-guide/docs/manage-your-logs)
[4] Logging is turned off by default for Cloud-Delivered Firewall but can be enabled by a customer (see: https://docs.umbrella.com/umbrella-user-guide/docs/add-a-firewall-policy)

Remote Browser Isolation	• Session ID (numeric session identifier) • Browser configuration (e.g., browser type, version, local settings, window dimensions, operating system, etc.) • User input in the isolation platform (e.g., keyboard strokes, mouse clicks, window resize events, etc.) • Any other personal data contained in user requests or user input in the isolation platform • Any other personal data present on pages that are isolated by the platform • User configuration (random numeric identifier and other browser information collected by persistent cookies to store browser configuration information)	• Authenticate and authorize access to the service. • Identify source of request • Provide access to website content in a secure manner while ensuring a native browsing experience • Prevent, detect, respond, and protect against potential or actual claims, liabilities, prohibited behavior, security risks, and criminal activity
Configuration Information	• Audit logs (administrator name) • Policy settings (administrator name, IP address) • Object labels (object labels such as network, roaming computer and mobile device names) • For Chromebook client: • Email address and/or device serial number and device OS) • Unique account ID	• Configuration Information is processed to log what policies were implemented and/or changed and the customer administrator who made the change • Provide information about the account
	For SaaS API-based DLP: • OAuth Keys including username and password of admin that authorized access[5] • email address and display name of all users in customer's SaaS environments that will be monitored with such service.	• Authentication and authorization to cloud (SaaS) environment to be scanned for DLP • Umbrella ability to inspect the file metadata and content of files stored in the applicable cloud environments and assess violations with SaaS API-based DLP configured DLP criteria
	For Cloud Malware: OAuth Key including username of admin that authorized access[5]	• Authentication and authorization of Umbrella Cloud Malware to scan the applicable cloud environment
	• If using Active Directory or cloud Identity Provider ("IdP") integration add-on: User identity (first name, last name, username, display name, email, GroupName)[6] • If using Active Directory add-on: Device id, Device name, UserID, GroupID	• Manage policies and pinpoint activity per user or device
Support Information	• First and last name • Email address • Phone number of the employee(s) appointed to open the service request • Customer account information: (Company name, street, city, state/region, country, Unique account ID)	• Remote access support • Review of the support service quality • Troubleshooting • Analysis of service
Business and Product Usage Analytics	Product usage, contact and user information, which may include the following types of personal data of the dashboard user: • First and last name, • Job title • Role within Umbrella service • Company name • Physical address (street, city, state/region, country) • Email address and corresponding unique numerical account ID • Username and/or ID • IP address • Phone number • Device type and device name • Timestamp for login	• Internal business and product analytics and reporting to inform data-driven business and product decisions • UserID and IP address used to provide users with a step-by-step tour and guidance on use of the product via Walkme • Product and feature usage analytics, sales support, renewal support, marketing/engagement email segmentation, product adoption and deployment assistance

[5] Customer can revoke OAuth keys

[6] If using Cisco user management services to integrate Google Workspace identities via Google's APIs, Cisco will processing data received from Google in accordance with the Google API Services User Data Policy, including the Limited Use requirements.

	• Dashboard activity information	

Cisco Umbrella collects "System information" to assist Cisco with understanding product usage, enabling product improvements and adoption. Cisco also collects personal data to conduct analytics to perform internal security research, and to track and predict threats. For more information about how Cisco uses, shares and protects Systems Information, see the Cisco Trust Center. Any personal data that is processed as part of this Systems Information is protected in accordingly.

3. Data Center Locations

Cisco uses colocation facilities as well as third-party infrastructure providers to deliver the service globally.

3.1 Data Storage:
If a customer selects the EU geo, the customer's DNS Layer Security, Secure Web Gateway, Cloud-Delivered Firewall, and DLP and Cloud Malware Usage and Event Data are stored in the Cisco Umbrella EU data warehouse.

All other stored data is stored in the United States (except for temporary storage up to two hours of proxy logs at the applicable edge data center as described in Section 7). Please see Section 6 for location of storage for retained data by Personal Data Category. Cisco uses AWS for its data storage. See below for Usage and Event Data processed by Cisco Security Cloud and Threat Intelligence.

3.2 Cisco Security Cloud and Threat Intelligence:
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 unified assistants 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. For the data identified in Table 1 above as being shared with the Cisco Security Cloud platform, Cisco processes the data for this purpose in the United States. Usage and Event Data stored in Europe (for customers selecting EU Event Log storage) are not provided to Cisco's Security Cloud.

Table 2
Umbrella Data Center for Data Storage

Location	Provider
U.S., Germany, Ireland	AWS

3.3 Data Processing:
A customer's web traffic (i.e., DNS and/or HTTP/S)) can be routed to any of Umbrella's global edge data centers, dependent on service capability and connection type, although the traffic is usually routed to the closest available service-enabled physical or virtual edge data center to the individual initiating the DNS or HTTP/S query or to the selected Umbrella IPSec tunnels. Inspection of web traffic occurs at the applicable Umbrella global edge data center.

Table 3
Umbrella Data Centers for DLP and Cloud Malware

Service	Location	Provider
Cloud Malware	U.S.	AWS
Real-Time DLP	See Global Umbrella Edge Data Center below. If using Machine Learning based Document Classification feature, U.S. data center.	AWS
SaaS API-based DLP	U.S.	AWS

Umbrella Global Edge Data Centers

For the list of the Umbrella global edge data centers, see the Global Cloud Activity page. The Umbrella global edge data centers are colocation facilities. The providers are not sub-processors and are provided for informational purposes only.

Table 4
Threat Intelligence Data Centers

Location	Provider
United States	AWS
Ashburn, VA	Equinix
Sunnyvale, CA	Equinix

Table 5
Remote Browser Isolation Data Centers[7]

Location	Provider
United States, United Kingdom, Germany, Singapore, Japan, Australia, Brazil, Bahrain, South Africa	AWS

When a user's browser session is isolated, the browser session executes in one of the global data centers listed above in Table 5 based on user location. Data is not retained except for the Session ID and User Configuration data as stated in Section 6 below. The retained data is stored in the AWS, U.S. data center.

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

Cisco's Data Protection Agreement (DPA) is available to any customer requesting it. The DPA includes the Standard Contractual

[7] Delivered through Cisco's sub-processor, Menlo Security. Please see Section 8.

Clauses and Cisco's applicable technical and organizational safeguards. For a sample of Cisco's DPA, please see DPA.

5. Access Control

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

Table 6

Personal Data Category	Who has Access	Purpose of the Access
Account/Contact Information	Customer administrator(s)	Modify and control certain admin information
	Authorized Cisco Employees with Business, Support and Operational roles	Provision customer's account; billing/invoicing; supporting the service subject to applicable data access and security controls
DNS Layer Security Usage and Event Data	Authorized Cisco Employees	Deliver, support, maintain, improve the service, and perform threat intelligence research through Cisco Security Cloud platform subject to applicable data access and security controls
	Customer administrator(s)	Set policies on customer network; monitor customer network
Secure Web Gateway Usage and Event Data	Authorized Cisco Employees	Deliver, support, maintain, improve the service, and perform threat intelligence research through Cisco Security Cloud platform subject to applicable data access and security controls
	Customer administrator(s)	Set policies on customer network; monitor customer network
Cloud-Delivered Firewall Usage and Event Data	Authorized Cisco Employees	Deliver, support, maintain, improve the service, and perform threat intelligence research through Cisco Security Cloud platform subject to applicable data access and security controls
Cloud Malware Usage and Event Data	Authorized Cisco Employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer administrator(s)	View malware and alerts and take actions
Data Loss Prevention Usage and Event Data	Authorized Cisco Employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer administrator(s)	View DLP incidents
Remote Browser Isolation	Authorized Cisco Employees[8]	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer administrator(s)	Set policies and browser configuration; monitor use
Configuration Information	Authorized Cisco Employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
	Customer administrator(s)	Manage and configure account
Dashboard Activity Information	Authorized Cisco Employees	Deliver, support, maintain and improve the service, subject to applicable data access and security controls
Support Information	Authorized Cisco Employees	Provide support for the service and troubleshoot customer issues

[8] In the context of Remote Browser Isolation, the Authorized Cisco Umbrella Employee includes employees of Cisco's sub-processor, Menlo Security.

	Customer administrator(s)	Provide feedback, point out technical issues
Business and Product Usage Analytics	Authorized Cisco Employees	Organize, analyze, and report on business and product usage data; improve the service

Access to customer information is subject to Cisco's Access Management Policy. Access is protected by multiple authentication and authorization mechanisms. Cisco has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based by roles and job functions. Shared accounts are prohibited. All usernames are traceable to a specific human user. User access credentials are promptly removed when user access is no longer authorized (e.g., Cisco employment terminates).

Remote user access by Cisco personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA is required.

Refer to the Cisco Umbrella and Cisco Enterprise Services SOC 2 reports for additional details on the logical access processes leveraged by Cisco Umbrella available on the Cisco Trust Portal.

6. Data Retention

The table below lists the personal data used by Cisco Umbrella, the length of time that data needs to be retained, why we retain it, and location of storage.

A data subject may request deletion of his or her Personal Data by sending a data subject request as described in Section 11 of this Privacy Data Sheet.

A customer may request data deletion by submitting a ticket to Cisco Umbrella support at umbrella-support@cisco.com. When a customer makes a request for deletion, Cisco will purge the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records).

Table 7

Personal Data Category	Type of Personal Data	Retention Period	Purpose for Retention
Account/Contact Information (Stored in United States)	• Dashboard/console user email address and name • Company account information (Company name, street, city, state/region, country, phone number, Unique account ID) • Billing contact name	Delete upon request	Retention of administrative data required for legitimate business purposes (e.g., billing, notifications, support, managing entitlements and renewals) records
DNS Layer Security Usage and Event Data (Stored in United States by default. Customer can select Europe for storage)	• DNS query data contained in DNS logs (domain, DNS record type, DNS response, IP address/Origin ID) • Device ID • Cloud apps associated with user or device	12 months. If data is processed as part of the Security Cloud, such data will be retained for no longer than 6 months. Any data determined to be malicious by Talos, is aggregated or de-identified data and may be retained for longer.	• Ongoing feature usage and reporting for which access to historical data is important • Threat intelligence, product improvement, and service delivery through the Cisco Security Cloud platform, including the Talos threat intelligence research
	If using DNS block page: • HTTP header and URL info but excluding HTTP body content and HTTP query parameters	12 months. If data is processed as part of the Security Cloud, such data will be retained for no longer than 6 months. Any data determined to be malicious by Talos is aggregated or de-identified data and may be retained for longer.	• Ongoing feature usage and reporting for which access to historical data is important • Threat intelligence, product improvement, and service delivery through the Cisco Security Cloud platform, including the Talos threat intelligence research

	If using optional selective proxy feature: • Personal data contained in proxy logs (includes source and destination IP addresses, timestamp, proxy specific headers, and URLs. Body content is not retained. • Cloud apps associated with user or device	60 days for Umbrella service. If data is processed as part of the Security Cloud, such data will be retained for no longer than 6 months. Any data determined to be malicious by Talos is aggregated or de-identified data and may be retained for longer.	• Ongoing feature usage and reporting for which access to historical data is important • Threat intelligence, product improvement, and service delivery through the Cisco Security Cloud platform, including the Talos threat intelligence research
Secure Web Gateway Usage and Event Data (Stored in United States by default. Customer can select Europe for storage)	• Personal data contained in proxy logs- includes source and destination IP addresses, timestamp, proxy specific headers, and URLs. Body content is not retained except for files as described below for threat intelligence research.	Up to 60 days for Umbrella service If data is processed as part of the Security Cloud, such data will be retained for no longer than 6 months. Any data determined to be malicious by Talos is aggregated or de-identified data may be retained for longer.	• Ongoing feature usage and reporting for which access to historical data is important • Threat intelligence, product improvement, and service delivery through the Cisco Security Cloud platform, including the Talos threat intelligence research
	Data contained in customer files sent to Cisco Umbrella for analysis	Retention period depends on how file is inspected. Files are only held transiently by Cisco Umbrella and are purged after they are scanned by Cisco Umbrella. However, for files also inspected by Secure Malware Analytics, see the Secure Malware Analytics Privacy Data Sheet at Cisco Trust Portal	• Ongoing feature usage and reporting for which access to historical data is important • Threat intelligence, product improvement, and service delivery through the Cisco Security Cloud platform, including the Talos threat intelligence research
Cloud-Delivered Firewall Usage and Event Data (Stored in United States by default. Customer can select Europe for storage)	• All personal data included in ports and protocol meta information, including source IP and port, destination IP and port, application (e.g., Webex), date, and timestamp • Only the packet content for the packets that triggered an IPS rule are retained after processing	Up to 60 days	Ongoing feature usage and reporting for which access to historical data is important
Cloud Malware Usage and Event Data (Stored in United States by default. Customer can select Europe for storage)	Usernames, email addresses and cloud vendor user ID's	12 months plus an additional seven days to for the backup to be deleted	• Ongoing feature usage and reporting for which access to historical data is important • Except for usernames, email addresses and cloud vendor user ID's, all contents of inspected files are retained only momentarily to calculate the hash for further inspection
	OAuth Keys including username of admin that authorized access	Data deleted upon request Customer can revoke	Authentication to cloud environment to be scanned for malware

Data Loss Prevention Usage and Event Data (Stored in the United States by default, but customer can select Europe for storage).	"DLP Event Data" which includes: • Snippet of policy violation (e.g., last 4 digits of a credit card number) and surrounding text for content triggering a customer DLP policy violation • File name / File ID •For Real Time DLP, DLP Event data includes, if configured user identity data through Active Directory or IdP of user having sent the web request which was determined to contain the policy violation with the Real Time rules. •For SaaS API-based DLP, DLP Event Data also includes email address and display name of users, email and display name of collaborators of changed file detected to be in violation with the DLP SaaS API rules and Discovery Scans.	Data deleted upon request	• Deliver, support, maintain and improve the service • Customers visibility into the data violations with their Data Protection Policy. • Customer ability to review and perform investigative and remediation operations on the data incidents in their organization.
Remote Browser Isolation (Stored in the United States)	• Browser Configuration • User input in the isolation platform • Any other personal data contained in user requests or user input in the isolation platform • Any other personal data present on pages that are isolated by the platform	Transient	n/a
	Session ID	Deleted after 24 hours	n/a
	User configuration	Data deleted upon request	n/a
Configuration Information (Stored in the United States)	• Audit logs (administrator name) • Policy settings (administrator name, IP address) • Object labels (object labels such as network, roaming computer and mobile device names) • Chromebook client ID (email ID) • Unique account ID	Data deleted upon request. Certain data may take up to 60 days from request to complete deletion (e.g., identity data from cloud identity provider)	Ongoing feature usage and reporting for which access to historical data is important
	• For SaaS API-based DLP: • OAuth Keys including username and password of admin that authorized access • email address and display name of all users in customer's SaaS environments that will be monitored with such service.	Data deleted upon request Customers can revoke the Oauth Keys at any time at their discretion. Revocation of the keys will disable Cisco Umbrella's access to the applicable cloud environment.	• Authentication and authorization to cloud (SaaS) environment to be scanned for DLP • Umbrella ability to inspect the file metadata and content of files stored in the applicable cloud environments and assess violations with SaaS API's configured DLP criteria.

	• If using Active Directory or cloud Identity Provider (IdP) integration add-on: User identity (first name, last name, username, display name, email, GroupName) • If using Active Directory add-on: Device id, Device name, UserID, GroupID	Data deleted upon request. Certain data may take up to 60 days from request to complete deletion (e.g., identity data from cloud identity provider)	Ongoing feature usage and reporting for which access to historical data is important
Dashboard Activity Information (Stored in the United States)	• See Table 1	Data deleted upon request	Ongoing feature usage analytics
Support Information (Stored in the United States)	• See Table 1	Data deleted upon request	Ongoing support and service quality analytics
Business and Product Usage Analytics (Stored in the United States)	• See Table 1	Data deleted upon request	Ongoing business and product usage

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.

For additional information on Cisco Umbrella's data security program, please refer to Section 9 below.

Table 8

Personal Data Category	Type of Personal Data	Security Controls and Measures (Subject to notes below this Table 8*)
Account/Contact Information	See Table 1	Encryption in transit and at rest
DNS Layer Security Usage and Event Data	See Table 1	Encryption in transit and at rest
Secure Web Gateway Usage and Event Data	See Table 1	Encryption in transit and at rest
Cloud-Delivered Firewall Usage and Event Data	See Table 1	Encryption in transit and at rest
Cloud Malware Usage and Event Data	See Table 1	Encryption in transit and at rest
Data Loss Prevention Usage and Event Data	See Table 1	Encryption in transit and at rest
Remote Browser Isolation	See Table 1	Encryption in transit and at rest
Configuration Information	See Table 1	Encryption in transit and at rest

	• OAuth Keys for Cloud Malware, including username of admin that authorized access • OAuth Keys for SaaS API-based DLP, including username and password of admin that authorized access	• Encryption in transit and at rest • Field level encryption on the OAuth Key • Customer can revoke OAuth key thereby terminating Cisco's access to the applicable cloud (SaaS) environment
Dashboard Activity Information	See Table 1	Encrypted in transit and at rest
Support Information	See Table 1	Encrypted in transit and at rest
Business and Product Usage Analytics	See Table 1	Encrypted in transit and at rest

***Notes**:
Data in Transit: Encryption in transit means data is encrypted between Cisco Umbrella data centers while traveling over the internet. Data is encrypted in transit from the user to the Umbrella edge data center if the customer uses HTTPS or another encrypted communication method such as an Umbrella SIG tunnel or DNScrypt. Some data may be unencrypted in transit between Umbrella services within the same data center.

Data at Rest: All data stored by Cisco Umbrella (including back-ups) is encrypted at rest except as described in this paragraph. For performance and troubleshooting purposes, proxy logs generated by Umbrella are unencrypted at rest for a maximum of 2 hours at the applicable edge data center. In addition, the Umbrella Investigate research team is still in the process of completing its encryption at rest project. DNS query logs for all customers other than those selecting the EU log storage location are currently unencrypted in some environments. These query logs contain the source IP and timestamp.

Active Processing at the Edge: Files and other traffic content are processed unencrypted, in memory, at the edge data center to complete the inspection and apply policies. Identity data is hashed while in the edge DC for processing using a randomly generated numeric ID. While a customer has the option for some Umbrella packages to configure their traffic so that it will not be unencrypted at the edge data center, without this decryption, security can only be applied based on the IP address and Domain metadata and a customer will not have the benefit of the full Umbrella security. In addition, for selective proxy and Secure Web Gateway, Customers can elect to use the Umbrella selective decryption feature to identify certain trusted domains that Umbrella cannot decrypt for processing.

AWS: AWS offers robust controls to maintain security and data protection. 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. The AWS SOC reports provide additional details on the specific control activities executed by AWS. More details can be found at: https://aws.amazon.com/compliance/ and https://aws.amazon.com/security/.

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:

Table 9

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	Personal Data listed in Table 1 other than Support Information and Business and Product Analytics	Cloud infrastructure provider. Foundation model provider. Cisco Umbrella data warehouse	AWS U.S., Germany, Ireland
Salesforce	Account/Contact and Support Information (see Table 1)	To provision the service and provide support	Dallas, TX, U.S. Phoenix, AZ, U.S.

Zendesk	Support Information (see Table 1)	To provide support	West Coast, USA Backup site in East Coast, U.S.
Amplitude	Dashboard users' UserID, role, dashboard activity usage metrics	To analyze feature usage and product functionality	U.S.
Chaos Search	Data processed through Cisco Security Cloud platform as set forth in Table 1	To analyze log data	U.S.
Datadog	Personal data may be included in administrative, service level logs stored with Datadog (e.g., Origin ID, URLs)	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	AWS U.S.
Grafana Labs	Personal data may be included in administrative, service level logs stored with Grafana Labs (e.g., Origin ID, IP Address, URLs)	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	U.S.
Databricks	Personal data in proxy and DNS logs (does not include logs of customers selecting the EU geo) Data processed through Cisco's Security Cloud platform as set forth in Table 1.	To analyze log data	U.S.
Menlo Security	Remote Browser Isolation (See Table 1)	To enable remote browser isolation feature	AWS U.S.
Snowflake Cloud data warehouse solution	Business and Product Analytics (see Table 1)	Business intelligence data warehouse	AWS U.S.
Walkme	UserID IP Address	Provides users with a step-by-step tour and guidance on product usage	AWS U.S.
Sparkpost	Email Header data Email body	Automated in-product emails such as password reset and account provisioning emails.	AWS U.S.
Kentik	IP Address	Network analyzer	U.S.
Skilljar	Administrator Registration Information	Integrated training platform	U.S.

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 (also known as Security Visibility and Incident Command), 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 Service is built with security and privacy in mind and is designed so that it 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.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEA Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

12. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

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.

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