Offer Disclosure

Cisco Umbrella

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" link in the upper right corner of the Trust Portal.

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 Offer Disclosure. 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 Offer Disclosure 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 Offer Disclosure on the Trust Portal. If you use Cisco Security Cloud Control, a unified deployment and management tool for select Cisco products that provide, amongst other things, single sign-on (SSO), please refer to the Security Cloud Control Offer Disclosure found on the Trust Portal for more information on how it processes personal data. 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 Offer Disclosures 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/.

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.

Table 1: Customer Content

Data Category	Data Elements	Purposes	Retention Period
DNS Layer Security[1] Data	**Personal Data:** If using optional selective proxy feature: • Personal data in body content (e.g., files) included in web traffic (HTTP/HTTPS) that is intercepted and proxied by selective proxy	• Provide granular protection at URL and file level and to implement customer policies. Note: • Body content is processed for malware inspection • Files sent to Cisco Umbrella are inspected to provide malware analysis and threat intelligence product function • Threat intelligence research	• Body content is not retained except for files as described herein • Retention period depends on how the file is inspected. Files are only held transiently by Cisco Umbrella and are purged after they are scanned by Umbrella. However, for files inspected by Secure Malware Analytics, see the Secure Malware Analytics Offer Disclosure at Cisco Trust Portal
DNS Layer Security[1] Data	**Non-Personal Data such as:** • If using optional selective proxy feature, non-personal data in body content included in web traffic	• See Purposes immediately above for DNS Layer Security Data	• See Retention Period immediately above for DNS Layer Security Data
Secure Web Gateway[1] Data	**Personal Data:** • Personal data included in body content (e.g., files) included in web traffic (HTTP/HTTPS) that is sent to Umbrella for analysis.	• Provide granular protection at URL and file level and to implement customer policies. Note: Body content (including files) is inspected for malware and data loss prion (DLP) • Threat intelligence research	• Body content is not retained except for files as described herein • Retention period depends on how the file is inspected. Files are only held transiently by Cisco Umbrella and are purged after they are scanned by Umbrella. However, for files inspected by Secure Malware Analytics, see the Secure Malware Analytics Offer Disclosure at Cisco Trust Portal

1 Identity data (e.g., active directory, Identity Provider ("IdP"), Google Workspace, username, userID and other identity information described under "Configuration Data") is not stored by Cisco with the DNS Layer Security or Secure Web Gateway Data. Cisco pairs such identity data with such data logged at time of display in the Umbrella Dashboard, for purposes of reporting using Reporting API, and upon exporting the logged data to a customer specific AWS S3 bucket. Customers have the option to have their 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.

Secure Web Gateway[1] Data	**Non-Personal Data such as:** • Non-personal data in body content included in web traffic	• See Purposes immediately above for Secure Web Gateway Data	• See Retention Period immediately above for Secure Web Gateway Data
Cloud Malware Data	**Personal Data:** • End user registration information: User ID and/or e-mail address, user first and last name • Any other personal data in files and application fields stored in applicable cloud environment that is inspected for malware	• 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	• End user registration information retained for 12 months plus an additional 7 days to for the backup to be deleted • Contents of inspected files/applications fields are retained only momentarily to calculate the hash for further inspection
Cloud Malware Data	**Non-Personal Data such as:** • Any non-personal data in files and application fields.	• See Purposes immediately above for Cloud Malware Data	• Contents of inspected files are retained only momentarily to calculate the hash for further inspection

Data Loss Prevention (DLP) Data	**Personal 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 – see Note
	• Snippet of policy violation (e.g., last 4 digits of credit card number) and surrounding text if policy violation detected
	For SaaS API-based DLP:
	• End user registration information:
	  • Email address and display name of users in customers' cloud (SaaS) environments that will be monitored with such service. If configured this data will be logged for policy violations.
	  • Email address and display name of collaborators of a changed file detected to be in violation with the DLP SaaS API rules and Discovery Scans. If configured this data will be logged for policy violations.
	For Real Time DLP:
	• End user registration information: if configured, user identity data through AD/IdP of user having sent the web request which was determined to contain the policy violation with the Real Time rules
		• 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
			• Up to 12 months
			Note: 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

Data Loss Prevention (DLP) Data	**Non-Personal Data such as:** • Any non-personal data in file name, scanned files, snippet of policy violation and surrounding text	• See Purposes immediately above for Data Loss Prevention Data	• Up to 12 months
Configuration Data	**Personal Data:** • End user registration information for Chromebook client: email address and/or device serial number and device OS)	• 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	• 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)

	• End user registration information 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
		• 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
			• 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

	End user registration information for Cloud Malware: • OAuth Key including username of admin that authorized access[2]	• Authentication and authorization of Umbrella Cloud Malware to scan the applicable cloud environment	• Data deleted upon request. Customer can revoke
	• If using Active Directory or cloud IdP integration add-on: User identity (first name, last name, username, display name, distinguished name, email, GroupName)[3] • If using Active Directory add-on: Device id, Device name, device IP address, UserID, GroupID	• Manage policies and pinpoint activity per user or device	• 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)
Configuration Data	**Non-Personal Data such as:** • Any non-personal data in end user registration information	• See Purposes immediately above for Configuration Data	• Data deleted upon request

Table 2: Customer Systems Information

Data Category	Data Elements (Examples)	Purposes	Retention Period
Account/Contact Information	**Personal Data:** • 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 • Authentication/Authorization • Managing subscription entitlements • Renewals	• Delete upon request
Account/Contact Information	**Non-Personal Data such as:** • Company account information (Company name, street, city, state/region, country, phone number, Unique numerical account ID)	• See Purposes immediately above for Account/Contact Information	• Delete upon request

2 Customer can revoke OAuth keys.
3 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.

DNS Layer Security[1] Data	**Personal Data:**
	• Personal data contained in DNS query data (IP address/origin IP, destination domain name)
	• DNS Logs:
	  • Personal data contained in DNS logs (IP address/origin ID, destination domain name, DNS record type, DNS response)
	  • Device ID
	  • Discovered cloud applications, Source IP addresses and associated cloud applications, destination URLs associated with discovered cloud application feature
		• 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
			• DNS logs retained for up to 90 days

	• 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	

	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
	• Proxy logs:
	  • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs[4]
	  • Cloud apps associated with user or device: User ID and/or email address, user first and last name, source IP addresses and associated cloud applications, destination URLs
		• Provide granular protection at URL and file level and to implement customer policies.
		• Threat intelligence research
		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
			• Proxy logs retained for up to 90 days

DNS Layer Security Data[1]	**Non-Personal Data such as:** • Non-personal data in DNS query logs, DNS block page • Discovered cloud applications	• See Purposes immediately above for DNS Layer Security Data	• Up to 90 days

4 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).

Secure Web Gateway[1] Data	• Personal data included in web traffic (HTTP/HTTPS), including headers, URLs • Cloud apps associated with user or device (User ID and/or email address, user first and last name, Source IP addresses and associated cloud applications, destination URLs) • 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. • Proxy logs: • Personal data contained in proxy logs, including source and destination IP addresses, timestamp, proxy specific headers, and URLs)[5]	• Provide granular protection at URL and file level and to implement customer policies. • Threat intelligence research 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	• Proxy logs retained up to 90 days
Secure Web Gateway[1] Data	**Non-Personal Data such as:** • Non-personal data in proxy logs	• See Purposes immediately above for Secure Web Gateway Data	• Proxy logs retained up to 90 days
Cloud-Delivered Firewall Data	**Personal Data:** • 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, origin ID[6]	• Provide granular protection at URL and file level (however, Cloud Delivered Firewall does not decrypt encrypted packet content) • Threat intelligence research	• Up to 90 days. Only the packet content for the packets that triggered an IPS rule are retained after processing
Cloud-Delivered Firewall Data	**Non-Personal Data such as:** • All non-personal data that is not Cisco Systems Information included in ports and protocol meta information	• See Purposes immediately above for Cloud-Delivered Firewall Data	• Up to 90 days. Only the packet content for the packets that triggered an IPS rule are retained after processing
Cloud Malware Data	**Personal Data:** • IP addresses for end users	• Discover, monitor, control, and act on malware (including personal data) stored in files and application fields by a customer's users in the	• Up to 12 months plus an additional 7days to for the backup to be deleted

5 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).

6 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).

		applicable cloud (SaaS) environment	
Cloud Malware Data	**Non-Personal Data such as:** • Cloud vendor user IDs	• See Purposes immediately above for Cloud Malware Data	• Up to 12 months plus an additional 7 days to for the backup to be deleted
Data Loss Prevention (DLP) Data	**Personal Data:** • Personal data scanned by Real Time DLP, including outbound and certain inbound traffic. See Umbrella User Guide for more information regarding Real Time DLP inbound and outbound scanning • Destination URL for Real Time DLP	• 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	• Up to 12 months Note: 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
Data Loss Prevention (DLP) Data	**Non-Personal Data such as:** • File ID for SaaS API-based DLP, Real-Time DLP, AI Guardrails • Any non-personal data in outbound and certain inbound traffic scanned via Real Time DLP	• See immediately above Purposes for Data Loss Prevention Data	• Up to 12 months Note: 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
Remote Browser Isolation (RBI) Data	**Personal Data:** • User input in the isolation platform (e.g., keyboard strokes, mouse clicks) • User configuration (random numeric identifier and other browser information collected by persistent cookies to store browser configuration information) • 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	• Provide, maintain, support, and improve the service • 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	• Session ID is deleted within 24 hours • User configuration – delete upon request • All other data is transient
Remote Browser Isolation (RBI) Data	**Non-Personal Data such as:** • Session ID (numeric session identifier) • Browser configuration (e.g., browser type, version, local	• See immediately above Purposes for Remote Browser Isolation Data	• Transient

	settings, window dimensions, operating system, etc.)		
Configuration Data	**Personal Data:** • Audit logs (administrator name, email address and source IP address) • Policy settings (administrator name, IP address) • Object labels (e.g., network, roaming computer and mobile device names) • 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	• Audit logs-12 moths • All other data is deleted upon request. Certain data may take up to 60 days from request to complete deletion (e.g., identity data from cloud identity provider)
	• User attributes defined and configured by customer admins at their discretion	• Manage policies and pinpoint activity per user or device	
Configuration Data	**Non-Personal Data such as:** • Non-personal data in policy settings, audit logs, object labels	• See immediately above Purposes for Configuration Data	• Deleted upon request
Business Analytics Data	**Personal Data:** • Admin first and last name • Job title • Role within Umbrella service • Email address and corresponding unique numerical account ID • Username and/or ID • IP address • Phone number • Device type and device name • Timestamp for login • Product usage • Dashboard activity information	• 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	• Deleted upon request
Business Analytics Data	**Non-Personal Data such as:** • Company name • Company physical address	• See immediately above Purposes for Business Analytics Data	• Deleted upon request

For threat intelligence research purposes, please note that Personal Data listed in Tables 1 and 2 for DNS Layer Security Data, the Secure Web Gateway Data and Cloud-Delivered Firewall Data of customers who select EU storage will be retained in the EU data centers listed in the Talos Offer Disclosure on the Cisco Trust Portal.

2b. Storage and Processing

Cisco uses third-party infrastructure providers to deliver this Cisco Offer's capabilities globally.

Data Storage.

See the table below for data storage location based on Data Category.

Table 3: Data Center Storage

Data Category	Infrastructure Provider	Data Center Storage Locations *
Account/Contact Information	• AWS	• Oregon, Virginia, USA
DNS Layer Security Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Secure Web Gateway Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Cloud-Delivered Firewall Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Cloud Malware Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Data Loss Prevention (DLP) Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Remote Browser Isolation (RBI) Data	• AWS	• USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Configuration Data	• AWS	• Oregon, Virginia USA
Business Analytics Data	• AWS	• Oregon, Virginia USA

* Proxy logs are temporarily storage up to two hours of proxy logs at the applicable physical edge data center as described in Section 3a.

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 4: Data Center Processing

Data Category	Infrastructure Provider	Data Center Processing Locations
Account/Contact Information	• AWS	• Oregon, Virginia, USA
DNS Layer Security Data	• See Global Edge Data Centers (colocation providers leveraged from Cisco Umbrella data center network)	• See Global Edge Data Centers
	• AWS	• California, Virginia, Minnesota, Texas, Washington, USA • Australia • Brazil • Canada • France • UK • Italy • India • Japan • Brazil • Singapore • The Netherlands
Secure Web Gateway Data	• See Global Edge Data Centers	• See Global Edge Data Centers

Cloud-Delivered Firewall Data	• See Global Edge Data Centers	• See Global Edge Data Centers
Cloud Malware Data	• AWS	• Oregon, USA • Virginia, USA
Data Loss Prevention Data: Real-Time DLP	• See Global Edge Data Centers • Document classification feature – AWS	• See Global Edge Data Centers • If using machine learning based Document Classification feature, USA data center
Data Loss Prevention Data: SaaS API-based DLP	• AWS	• Oregon, USA • Virginia, USA
Remote Browser Isolation (RBI)* Data	• Google Cloud Platform (GCP)	• California, Nevada, Ohio, Virginia USA • Australia • Brazil • Canada • Germany • France • India • Indonesia • Isreal • Italy • Japan • Hong Kong • Qatar • Singapore • South Africa • South Korea • Switzerland • United Kingdom
Configuration Data	• AWS	• Oregon, Virginia, USA
Business Analytics Data	• AWS	• Oregon, Virginia, USA

* When a user's browser session is isolated, the browser session executes in one of the global data centers listed based on user location.

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

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. Both are listed below. For updates, subscribe via the "subscribe" link in the upper right corner of the Trust Portal.

Table 5: Subcontractors & Subprocessors

Name	Service Type	Data Center Location
See the Global Cloud Activity page (subcontractor)	Colocation infrastructure provider	• See the Global Cloud Activity page

Amazon Web Services (AWS) (subcontractor)	Cloud infrastructure provider, Cisco Umbrella data warehouse, foundation AI Model provider – Llama used in DLP	• DNS Layer Security Data:
		  • California, Virginia, Minnesota, Texas, Washington USA
		  • Australia
		  • Brazil
		  • Canada
		  • France
		  • UK
		  • Italy
		  • India
		  • Japan
		  • Brazil
		  • Singapore
		  • The Netherlands
		• Other Umbrella services hosted in AWS:
		  • Oregon, United States
		  • Virginia, United States
		  • Germany
		  • Ireland

Amplitude (subprocessor)	To analyze Business Analytics Data for feature usage and product functionality	• Oregon USA
Catchpoint Systems (subcontractor)	Subcontractor: Monitor application performance	• Neveda, USA
Databricks (subprocessor)	To analyze log data	• Oregon, USA
Datadog (subprocessor)	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	• Virginia, USA
Grafana Labs (subprocessor)	To monitor infrastructure and service activity, aggregate administrative logs, perform service troubleshooting and diagnostics	• Iowa, USA
Kentik (subprocessor)	Network analyzer	• Virginia, USA
Menlo Security (subprocessor)	RBI provider	• California, Nevada, Ohio, Virginia, USA • Australia • Brazil • Canada • Germany • France • India • Indonesia • Isreal • Italy • Japan • Hong Kong • Qatar • Singapore • South Africa • South Korea • Switzerland • United Kingdom
MessageBird (subprocessor)	Automated in-product emails such as password reset and account provisioning emails	• Oregon, USA
PagerDuty (subcontractor)	• Automated incident alerts	• California, USA • Ohio, USA • Oregon, USA •

Salesforce (subprocessor)	To provision the service and provide support	• Dallas, TX, USA • Phoenix, AZ, USA.
Snowflake Cloud Data Warehouse Solution (subprocessor)	Business Analytics Data warehouse	• Virginia, USA
Walkme (subprocessor)	Provides users with a step-by-step tour and guidance on product usage	• California, USA • Oregon, USA

2c. Access and Sharing

Customers and their authorized third parties may directly access readily available data by using standard APIs, to the extent those are described in the API documentation found here, subject to the provisions of Cisco's API license.

Cisco Umbrella APIs support both structured and unstructured data sets depending on the particular data set requested from Cisco Umbrella. Depending on the standard implemented by the API, structured data sets may use JSON, XML, or other standardized data formats; while unstructured data sets may be in the form of text, PDF or other unstructured data file formats. For more details, please consult the API documentation referenced above.

If available, customers may send requests for expanded API or data interface capabilities through their usual Cisco support or account management channels.

In accordance with the EU Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council), customers and their authorized third parties may directly access their readily available data by using service-standardized data interfaces, to the extent those are described in API documentation found here, subject to the provisions of the written or electronic agreement between you and Cisco for the provision of the Cisco Offer to you or any other terms where the parties expressly agree to this document (e.g. the Cisco General Terms).

In accordance with the EU Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council), Cisco may make your data available, as described in the API documentation referenced above, for porting and service switching in a structured, commonly used and machine-readable format, through the standardized and applicable APIs, consistent with the specifications provided in Cisco API Guidelines and subject to the provisions of the written or electronic agreement between you and Cisco for the provision of the Cisco Offer to you or any other terms where the parties expressly agree to this document (e.g. the Cisco General Terms).

At Cisco, we are committed to protecting the security, privacy, integrity, and confidentiality of Customer Content and Customer Systems Information in our possession. We believe governments, including law enforcement and national security agencies, should go directly to our customers to gain access to their data, including data about their employees and their users. We do not create backdoors in our solutions to allow governments surreptitious access to data, the solutions Cisco provides, or anything else. For more information please see our Principled Approach to Government Demands for Data.

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 (Subject to notes below this Table*)
Account/Contact Information	Authorized Cisco Employees	• Provision customer's account; billing/invoicing; supporting the service subject to applicable data access and security	• Encryption in transit and at rest
	Customer administrator(s)	• Provision customer's account; billing/invoicing; supporting the service subject to applicable data access and security • Modify and control certain admin information controls	
DNS Layer Security Data	Authorized Cisco Employees	• Deliver, support, maintain, improve the service, and perform threat intelligence research	• Encryption in transit and at rest
	Customer administrator(s)	• Set policies on customer network; monitor customer network	
Secure Web Gateway Data	Authorized Cisco Employees Customer administrator(s)	• Deliver, support, maintain, improve the service, and perform threat intelligence research	• Encryption in transit and at rest
	Customer administrator(s)	• Set policies on customer network; monitor customer network	
Cloud-Delivered Firewall Data	Authorized Cisco Employees	• Deliver, support, maintain, improve the service, and perform threat intelligence research	• Encryption in transit and at rest
Cloud Malware Data	Authorized Cisco Employees	• Deliver, support, maintain, improve the service, and perform threat intelligence research	• Encryption in transit and at rest
	Customer administrator(s)	• View malware and alerts and take actions	
Data Loss Prevention (DLP) Data	Authorized Cisco Employees	• Deliver, support, maintain and improve the service, subject to applicable data access and security controls	• Encryption in transit and at rest
	Customer administrator(s)	• View DLP incidents	

Remote Browser Isolation (RBI) Data	Authorized Cisco Employees[7]	• Deliver, support, maintain and improve the service, subject to applicable data access and security controls	• Encryption in transit and at rest
	Customer administrator(s)	• Set policies and browser configuration; monitor use	
Configuration Data	Authorized Cisco Employees	• Deliver, support, maintain and improve the service, subject to applicable data access and security controls • 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
	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	• Encryption in transit and at rest
Business Analytics Data	Authorized Cisco Employees	• Organize, analyze, and report on business and product usage data; improve the service	• Encryption in transit and at rest

*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.

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).

[7] In the context of Remote Browser Isolation, the Authorized Cisco Umbrella Employee includes the employees of Menlo Security, Cisco's subprocessor.

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.
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.

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 Offer:

- Trust Package
- SOC 27001
- SOC 2
- SOC 3
- CAIQ
- CSA STAR Certification
- ENS Certification