Offer Disclosure

Cisco Secure Access

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

Cisco Secure Access is a cloud security service edge solution designed to allow users to securely connect to the Internet and private applications from any device located anywhere. Cisco Secure Access is designed with common administrative controls, data structures, and policy management designed to ease interoperability with other synergistic components such as SD-WAN.

Cisco Secure Access includes, depending upon the package purchased or optional features used, features delivered through other Cisco offers including: (1) Secure Malware Analytics for inspection of suspicious files; (2) digital experience monitoring through ThousandEyes Users Embedded Agent[1]; (3) provisioning, subscription, identity management and access to Cisco AI Assistant through Cisco Security Cloud Control; (4) if you access Secure Access through Security Cloud Control, identity insights through Cisco Identity Intelligence (a Duo feature); (5) protection of Cisco applications through Duo Identity for Cisco Apps; (6) security information and event management through integration with Splunk (Splunk subscription required); (7) generative AI product assistance through Cisco AI Assistant; (8) TAC support ticket creation through Cisco AI Assistant for Support; (9) AI security through Cisco AI Defense (10) connectivity through Cisco Secure Client (formerly, AnyConnect); (11) Secure Access Service Edge (SASE) capabilities through integration with Cisco Meraki and Catalyst SD-WAN; (12) email security through Email Threat Defense; and (13) if you access Cisco Secure Access through Cisco Cloud Control, Cisco Cloud Control and Cisco AI Canvas for AI-native unified management experience (with their own embedded AI Assistant, distinct

[1] Customer's ThousandEyes account will be provisioned by default in the ThousandEyes U.S. data center, unless Customer has previously selected the EU region as part of creating their trial account. You may contact support@thousandeyes.com to make a request to change your data center location to ThousandEyes' EU data center.

from the AI Assistant directly within Secure Access and Security Cloud Control).[2] Your Secure Access data may be shared with these other Cisco offers. For information regarding the processing of your data by these offers (or other Cisco offers that Secure Access may integrate with), please see their Offer Disclosures in the Cisco Trust Portal.

Cisco Secure Access may also integrate with third-party products. Cisco is not responsible for customer data once it leaves Cisco's control for a non-Cisco product. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

For more information about Cisco Secure Access, visit:
https://www.cisco.com/c/en/us/products/collateral/security/secure-access/secure-access-cloud-security-sse-aag.html.

[2] As part of this integration, data from Cisco Secure Access is transferred and processed as outlined in the Cisco Cloud Control Offer Disclosure, the Cisco AI Canvas Offer Disclosure, and the Cisco AI Assistant Offer Disclosure. Cisco Cloud Control, AI Canvas, and their AI Assistant may use customer data to train their AI models. Please refer to the respective Offer Descriptions for more details, including how to opt out.

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[3].

Table 1: Customer Content

Data Category	Data Elements[4]	Purposes	Retention Period[5]
Connection Data[6] (ZTA, VPN-as-a-Service, Roaming)	**Personal Data:** End user registration information in administrative service logs: • User ID (username, email) • User Group IDs	• Provide, maintain, support, and improve the service • Enable secure connectivity to Internet and private applications	• Up to 90 days
	End user registration information in Event Logs: • User ID and/or username • User Group IDs		• Up to 90 days
Connection Data (ZTA, VPN-as-a-Service, Roaming)	**Non-Personal Data such as:** • Non-personal data in end user registration information in Event Logs	• See Purposes immediately above for Connection Data	• Up to 90 days
Secure Web Gateway Data	**Personal Data:** • Personal data included in body content (e.g., files) included in web traffic (HTTP/HTTPS) that is sent to Secure Access for analysis[7] • Personal data in inspected files	• Provide, maintain, support, and improve the service • Provide granular protection at URL and file level • Threat intelligence research	• Body content is not retained except for files as described herein • Retention period depends on how body content is inspected. Files are only held transiently by Cisco Secure Access and are purged after they are scanned by Secure Access. However, for files inspected by Secure Malware Analytics, see the Secure Malware Analytics Offer Disclosure at Cisco Trust Portal
Secure Web Gateway Data	**Non-Personal Data such as:** • Non-personal data in body content included in web traffic and files	• See Purposes immediately above for Secure Web Gateway Data	• Body content is not retained except for files as described above.

[3] For the most current details regarding the customer data elements reported in Event Logs, including DNS Security, DLP, Connection Data, Firewall-as-a Service and other services, please refer to the Log Formats and Versioning and the Reports sections within the Secure Access User Guide.

[4] Administrative service logs are Cisco Systems Information, however, to the extent customer Personal Data is processed, Cisco will treat such Personal Data in accordance with the Cisco General Disclosures.

[5] Data processed at the edge data centers may be temporarily retained in cache. Also, in the unlikely event of a system crash, data in memory at the time of the crash (a "core dump") is automatically captured. A core dump is used to enable root cause analysis and remediation and may be retained in the U.S. to facilitate the engineering effort. Note, it may take up to 60 days to delete data pursuant to a data deletion request.

[6] If a Secure Firewall customer enables Universal ZTNA for their firewalls, the Connection Data will be transferred to Security Cloud Control – Firewall Management ("SCC-FM") and will be stored by such product in the customer's selected SCC-FM region. Please see SCC-FM Offer Disclosure for information on processing of customer data by such product.

[7] URL query parameters for HTTPS are not logged, however customers can opt-in to have full URL exported to an S3 bucket.

Cloud Malware Data	**Personal Data:** • End user registration information Event Logs: user first and last name, user ID and/or e-mail address • Any personal data in files and application fields scanned in cloud (SaaS) environment	• Provide, maintain, support, and improve the service • Discover, monitor, control, and act on malware (including personal data) stored in files and application fields by a customer's users in the applicable SaaS environment	• Event Logs are retained for 12 months plus an additional 7 days for the backup to be deleted • Contents of inspected files are retained only momentarily to calculate the hash for further inspection
Cloud Malware Data	**Non-Personal Data such as:** • 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:**
	• Any Personal Data scanned in SaaS environment, messages, emails, files, and other content inspected by DLP
	• SaaS API-based DLP, Real-Time DLP, Email DLP, Secure Client Endpoint DLP, AI Guardrails[8] Event Logs:
	  • File name
	  • Email subject
	  • Snippet of text triggering violation and surrounding text
	  • Endpoint DLP - justification for policy violation
	• SaaS API-based DLP Event Logs end user registration information:
	  • Email address and display name of users
	  • Email address and display name of collaborators of a changed file
	• Real Time DLP, Email DLP, Secure Client Endpoint DLP, AI Guardrails Event Logs end user registration information:
	User identity data, including through Active Directory ("AD") and/or Identity Provider ("IdP"), if configured
		• Provide, maintain, support, and improve the service
		• Discover, monitor, and act on (e.g., block) sensitive information (including personal data) in files, messages, AI queries, and other content in transit through the Secure Access service (for Real-Time DLP, Email DLP, Endpoint DLP, AI Guardrails) and in the applicable SaaS environment (for SaaS API-based DLP)
			• Event Logs are retained for up to 12 months
			• For SaaS API-based DLP customers who enable Data Security Posture Management (DSPM): customer file content is deleted immediately after classification completes. Other data (besides event logs) is retained until the customer Admin revokes the onboarded instance
			
			Note: The content inspected by DLP is not stored in full[9]. 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:** • Non-personal data scanned in SaaS environment, messages, emails, files, messages and other content	• See Purposes immediately above 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
Cloud App Discovery Data	**Personal Data:** Personal data in network traffic logs ingested by App Discovery based on the supported network data source(s), which includes end user registration information: • User ID and/or e-mail address • User first and last name	• Provide, maintain, support, and improve the service • Detect and provide risk score for cloud applications utilized by users	• 90 days

[8] See Cisco AI Defense Offer Disclosure for data shared with AI Defense.

[9] Customer may elect to store the violation file or payload in customer managed AWS S3 bucket. For more details, see this announcement.

Cloud App Discovery Data	**Non-Personal Data such as:** • Any non-personal data in end user registration information • Name of applications discovered	• See Purposes immediately above for Cloud App Discovery Data	• 90 days
User and Entity Behavior Analytics (UEBA) Data	• Personal data in file name, if any	• Provide, maintain, support, and improve the service • UEBA employs statistical analysis and heuristics to assess user activity and identify anomalous behavior and security risks	• 7 days
Control Plane Data – Configuration and Policy Data[8]	**Personal Data**[10]**:** • End user registration information: Chromebook client email ID and/or device serial number and operating system	• Configuration Information is processed to log policies implemented and/or changed and the customer administrator who made the change • Provide information about the account • Provide reports requested by Admin	• Deleted upon request
	End user registration information for SaaS API-based DLP: • OAuth Keys which include username and password of Admin that authorized access • Email address and display name of users in applicable SaaS environments	• Authentication and authorization to SaaS environment to be scanned for DLP • Secure Access ability to inspect the file metadata and content of files stored in the applicable SaaS environments and assess violations with configured DLP criteria	• Deleted upon request
	End user registration information for Cloud Malware: • OAuth Key which includes username of Admin that authorized access	• Authentication and authorization of Secure Access Cloud Malware to scan the applicable SaaS environment	• Deleted upon request
	• Any personal data typed into text field for comments by customer Admin	• Allow customer Admin to post comments	• Deleted upon request
Control Plane Data – Configuration and Policy Data	**Non-Personal Data such as:** • Any non-personal data in end user registration information • Any non-personal data typed into text field for comments by customer Admin	• See Purposes immediately above for Configuration and Policy Data	• Deleted upon request

Control Plane Data - User and Device Identity Data[11]	**Personal Data:**
	End user registration information:
	• If using AD or IdP add-on AD/IDP User and device identity such as:
	  • First name, last name, username, common name, display name
	  • Distinguished name,
	  • Email
	  • Group Name
	  • Device ID, device name
	  • Device IP address
	  • User ID
	  • Group IDs)
	  • User Principal Name (UPN)
		• Manage policies and pinpoint activity per user or device to deliver the service
		• Authenticate user and/or device
			• Deleted upon request

[10] Customer can revoke OAuth Keys at any time.

[11] Identity data (e.g., active directory, IdP, Google Workspace ID, username, user ID and other identity information) described under "Control Plane - Configuration and Policy Data" is not stored by Cisco with Event Logs. Cisco pairs identity data with Event Logs at time of display in the dashboard, for purposes of reporting using Reporting API, and upon exporting Event Logs to a customer specific AWS S3 bucket if customers elect S3 export option.

	• Google Workspace ID, username and email, directory group (if using Google Workspace integration)[12]		
Control Plane Data – User and Device Identity Data	**Non-Personal Data such as:** • Any non-personal data in end user registration information, including AD directory identifier (e.g., tenant ID, domain SID)	• See Purposes immediately above for User and Device Identity Data	• Data deleted upon request
Prompt Data from Secure Access & Security Cloud Control AI Assistant[13]	**Personal Data:** • Personal data in prompts typed into text field by Admin	• Large language AI model that extracts key words for the purpose of assisting customer Admin in creating security policies and answering product related queries	• Up to 12 months after prompt/response thread becomes inactive (user is no longer adding to the thread)
Prompt Data from Secure Access & Security Cloud Control AI Assistant[13]	**Non-Personal Data such as:** • Any non-personal data in prompts typed into text field by Admin	• See Purposes immediately above for Cisco AI Assistant Data	• Up to 12 months after prompt/response thread becomes inactive (user is no longer adding to the thread)

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

[13] If an end-user enters Customer Systems Information, Cisco Systems Information, Cisco Content, or data owned by a third party into a prompt, it retains its original status and does not become Customer Content because of its inclusion in an AI Assistant prompt. AI Assistant Prompt Data may also be included in AI Assistant responses. The AI Assistant available within Secure Access and Security Cloud Control is distinct from the AI Assistant in Cisco Cloud Control and AI Canvas. More information on how the Cisco Cloud Control/Canvas AI Assistant handles data is available in the Cisco AI Assistant Offer Disclosure.

Table 2: Customer Systems Information

Data Category	Data Elements[4]	Purposes	Retention Period[5]
Account Data	**Personal Data:** • Dashboard/console users (each an "Admin") first and last name • Admin email address • Admin IP Address	• Activate, maintain, support, and improve the service • Billing, invoicing, and tax compliance • Export compliance • Notification of features and other updates • Authentication and authorization • Managing entitlements and renewals	• Deleted upon request
Account Data	**Non-Personal Data such as:** • Company name • Company street, city, state/region, country • Company phone number	• See Purposes immediately above for Account Data	• Deleted upon request
Connection Data (ZTA, VPN-as-a-Service, Roaming)[6]	**Personal Data:** Event Logs: • Device public/private IP address • User Group IDs • Device IDs • Device IP addresses • Destination private application information (application ID, IP, category, FQDNs) • Destination IP address, URL, port • Ingress IP and region • Hostname • Device OS and version • Secure Client version • VPN profile • Device configuration properties • Geolocation (derived from public IP address) • Timestamp	• Provide, maintain, support, and improve the service • Enable secure connectivity to Internet and private applications	• Up to 90 days
	Administrative service logs: • Device private and/or public IP address • User Group IDs • Device IDs • Device name • Hardware UUID • Destination private application information (application ID, category, IP, FQDNs) • Device Posture Data, excluding WiFi fingerprint (below) • Personal data included in web traffic (HTTP/HTTPS), including headers, URLs, and cookies		• Up to 90 days

Connection Data (ZTA, VPN-as-a-Service, Roaming)	**Non-Personal Data such as:**
	• Event Logs/administrative service logs:
	  • Org ID
	  • Connection method/event
	  • Transaction ID
	  • Enforcement point
	  • Tunnel type
	  • Rule name/identity
	  • Tenant list and ID
	  • Session type (e.g., TLS)
		• See Purposes immediately above for Connection Data	• Event Logs are retained for up to 90 days
			• Administrative service logs are retained for up to 90 days

	• Syslog info • Non-personal data included in web traffic		
Device Posture Data	**Personal Data:** Application logs: • Device public IP address • User ID/email • Device identifiers (e.g., device ID, email associated with device, device/host name, machine GUID) • Device OS and version • Device policy/configuration properties (e.g., is password set, is disk encryption enabled, is screen lock enabled)	• Provide, maintain, support, and improve the service • Assess and validate device's security and status in order to determine whether the device should be authorized to connect to the network or private application	• Up to 90 days
	• Mobile device management (MDM) enrollment and compliance status • Device OS and version • Wi-Fi fingerprint (snapshot of device location represented by hash value derived from visible SSID at time of capture)		• Transient, refreshed around every 10 minutes
	• Posture records: User ID/email		• Deleted upon request
	• Routing logs: device public IP address		• Up to 12 months
Device Posture Data	**Non-Personal Data such as:** • Routing logs: Org ID	• See Purposes immediately above for Device Posture Data	• Up to 12 months
DNS Security Data	**Personal Data:** Event Logs: • Source and destination IP address • Destination domain name • Origin ID • Device type • Device IDs (e.g., Chromebook ID, VPNID) • Client reporting ID	• Provide, maintain, support, and improve the service • Conduct analytics and statistical analysis in aggregate form to track and predict threats • Threat intelligence research	• Up to 90 days
	If using DNS block page: • Origin ID • User/device IP address • HTTP/HTTPS headers and URL, excluding HTTP/HTTPS body content[7]		• Up to 3 days on block page hosted on applicable edge data center
DNS Security Data	**Non-Personal Data such as:** • Event Logs/DNS block page: Org ID	• See Purposes immediately above for DNS Security Data	• Up to 90 days

Secure Web Gateway Data	**Personal Data:**
	• Personal data included in web traffic (e.g., headers, URLs, body content)[6]
	• Cloud apps associated with user or device
	• Event Logs:
	  • Source and destination IP address
	  • Origin ID
	  • Device ID
	  • Timestamp
	  • Proxy specific headers
	  • URLs
		• Provide, maintain, support, and improve the service
		• Provide granular protection at URL and file level
		• Threat intelligence research
			• Event Logs retained for up to 90 days.
			• Body content is not retained except for files as described above in Table 1 (Customer Content)

Secure Web Gateway Data	**Non-Personal Data such as:** • Event Logs: Org ID	• See Purposes immediately above for Secure Web Gateway Data	• Up to 90 days

Firewall-as-a-Service Data	**Personal Data:**
	• Event Logs:
	  • Private and/or public source and destination IP addresses
	  • User ID
	  • Origin ID
	• Personal data in packet content (for IPS feature)
		• Provide, maintain, support, and improve the service
		• Provide granular protection at URL and file level
		• Threat intelligence research
			• Event Logs retained for up to 90 days
			• Administrative service logs (generally no Personal Data, but may be captured in error logs) retained for up to 30 days

Firewall-as-a-Service Data	**Non-Personal Data such as:** • Event Logs: Org ID, application ID (public/private) • Non-personal data in packet content (for IPS feature)	• See Purposes immediately above for Firewall-as-a-Service Data	• Event Logs retained for up to 90 days
Cloud Malware Data	**Personal Data:** • Event Logs: Source IP addresses • Any other personal data in scanned cloud (SaaS) environment	• Provide, maintain, support, and improve the service • Discover, monitor, control, and act on malware (including personal data) stored in files and application fields by a customer's users in the applicable SaaS environment	• Event Logs retained for 12 months plus an additional 7 days for the backup to be deleted
Cloud Malware Data	**Non-Personal Data such as:** • Non-personal data in Event Logs	See Purposes immediately above for Cloud Malware Data	• Event Logs retained for 1 year plus an additional seven days for the backup to be deleted

Data Loss Prevention (DLP) Data	**Personal Data:**
	• Real Time DLP, Email DLP, Secure Client Endpoint DLP, AI Guardrails Event Logs:
	  • Destination URL
	  • Action (e.g., blocked)
	  • Violation timestamp
	  • Web application name
	  • Content type (e.g., text, form data)
	  • File size
	  • Timestamp
	• Personal data scanned by Real Time DLP, Email DLP, Secure Client Endpoint DLP, AI Guardrails. See Secure Access User Guide for more information regarding Real Time DLP inbound and outbound scanning.
	• If you use SaaS API-based DLP and enable Data Security Posture Management (DSPM), the
		• Provide, maintain, support, and improve the service
		• Discover, monitor, and act on (e.g., block) sensitive information (including personal data) in files, AI queries, messages, and other content in transit through the Secure Access service (for Real-Time DLP, Email DLP, Endpoint DLP, AI Guardrails) and in the applicable SaaS environment (for SaaS API-based DLP)
		• For additional data collected if customer enables DSPM: discover, catalogue, and classify customer data assets across supported SaaS and cloud sources; generate DSPM
			• Event Logs retained for up to 12 months
			• Other than event logs, additional data processed to provide DSPM is retained until the customer admin revokes the onboarded instance
			
			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

	following additional data is processed to provide DSPM: • Sharing recipient name • Group member names • Access Control List entries	posture score, risk findings, recommendations	

Data Loss Prevention (DLP) Data	**Non-Personal Data such as:**
	• SaaS API-based DLP, Real-Time DLP, Email DLP, Secure Client Endpoint DLP, AI Guardrails Event Logs:
	  • File ID, type
	  • Event type (e.g., Real Time DLP, AI Guardrails)
	  • Resource name
	  • Data classification type
	  • Product traffic source
	  • Quarantine path
	  • Tenant info
	• Any non-personal data in outbound and certain inbound traffic scanned via Real-Time DLP and AI Guardrails
	• If you use SaaS API-based DLP and enable Data Security Posture Management (DSPM), the following additional data is processed to provide DSPM:
	  • S3 Bucket policies
	  • Identity access management policies
	  • Trust policies
	  • Access Control List entries
		• See Purposes immediately above for DLP Data and DSPM	• Event Logs retained for up to 12 months
			• For SaaS API-based DLP customers who enable DSPM: customer file content is deleted immediately after classification completes. Other data (besides event logs) is retained until the customer Admin revokes the onboarded instance
			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

Cloud App Discovery Data	**Personal Data:** Network traffic logs ingested by App Discovery based on the supported network data source(s), which may include: • Source IP address and associated cloud applications • Destination URLs	• Provide, maintain, support, and improve the service • Detect and provide risk score for cloud applications utilized by users	• 90 days
Cloud App Discovery Data	**Non-Personal Data such as:** • Non-personal data that is not Cisco Systems Information in network traffic logs ingested by App Discovery	• See Purposes immediately above for Cloud App Discovery Data	• 90 days
Remote Browser Isolation (RBI) Data	**Personal Data:** Standard RBI, Advanced Isolation Controls: • User input in the isolation platform (e.g., keyboard strokes, mouse clicks) • 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	• Transient
	Standard RBI, Advanced Isolation Controls: • Personal data in origin ID (e.g., user device		• Deleted after 24 hours. To the extent certain Data Elements are logged, retention is up to 90 days
	Standard RBI, Advanced Isolation Controls: • Browser configuration (e.g., browser type, version) • User input in the isolation platform (e.g., keyboard strokes, mouse clicks) • User configuration (random numeric identifier, user preferences and other browser information collected by persistent cookies to store browser configuration information)		• Data deleted upon request

Remote Browser Isolation (RBI) Data	**Non-Personal Data such as:**
	• Standard RBI, Advanced Isolation Controls:
	  • Org ID
	  • Non-personal data in Origin ID (e.g., network ID, tunnel ID)
	  • Session ID (numeric session identifier)
	• Advanced Isolation Controls
	  • Tenant ID
	  • Isolation profile ID
		• See Purposes immediately above for RBI Data	• Deleted after 24 hours. To the extent certain Data Elements are logged, retention is up to 90 days.

Semantic Inspection Data	**Personal Data:** Semantic Inspection Event Logs: • Personal Data in agent name (e.g., user email, username) that initiated the Model Context Protocol (MCP) connection • Action (e.g., blocked, allowed) • Violation timestamp • Source IP address • Destination IP address, URL	• Provide, maintain, support, and improve the service • Analyzes MCP traffic to determine AI agent behavior	• 90 days Note: The content inspected by Semantic Inspection is not stored in full. Cisco provided policies redact key sensitive content with only the snippet of the policy violation
Semantic Inspection Data	**Non-Personal Data such as:** Semantic Inspection Event Logs • Non-personal data in agent name that initiated MCP connection • MCP server name • Tenant info • Hostname • Application name, category	• See Purposes immediately above for Semantic Inspection Data	• 90 days Note: The content inspected by Semantic Inspection is not stored in full. Cisco provided policies redact key sensitive content with only the snippet of the policy violation
User and Entity Behavior Analytics (UEBA) Data	**Personal Data:** Cisco Identity Intelligence (a Duo feature) user trust level (e.g., Trusted, Favorable, Not Trusted) and explainability	• Provide, maintain, support, and improve the service • UEBA employs statistical analysis and heuristics to assess user activity and identify anomalous behavior and potential security incidents	• Refreshed every 24 hours

	• Impossible Travel
	  • Login timestamps
	  • Login geolocations
	  • Login URLs
	  • Anomaly type
	• Bulk File Transfers - metadata around file movement, such as:
	  • File type
	  • File action/anomaly type (e.g., delete download)
	  • Timestamp of file action
	  • Destination URL
	  • Geolocation
	  • Anomaly type
			• 7 days
			• 7 days

User and Entity Behavior Analytics (UEBA) Data	**Non-Personal Data such as:** • Transaction ID • Event ID • Origin ID, type • Org ID	See Purposes immediately above for UEBA Data	• 7 days
Control Plane Data - Configuration and Policy Data	**Personal Data:** • Audit logs which include Admin name, email address, and source IP address	• Configuration Information is processed to log policies implemented and/or changed	• Deleted upon request

	• Policy settings which include Admin name and IP address • Object labels (e.g., roaming device and mobile device names) • Any personal data in reports generated within dashboard (reports pull data from Event Logs stored in US and EU)	and the customer administrator who made the change • Provide information about the account • Provide reports requested by Admin	• Deleted upon request
Control Plane Data - Configuration and Policy Data	**Non-Personal Data such as:** • Unique account ID (e.g., Org ID) • Non-personal data in policy settings and object logs (e.g., network name)	• See Purposes immediately above for Configuration and Policy Data	• Deleted upon request
	• Non-personal data in audit logs		• Deleted upon request
Control Plane Data – User and Device Identity Data	**Personal Data:** • Source IP address • Device hostname • Device key (device ID format depends on device, for example for Chromebook it is a user's email or id or device's serial number) • Device serial number	• Manage policies and pinpoint activity per user or device to deliver the service • Authenticate user and/or device	• Deleted upon request
Control Plane Data – User and Device Identity Data	**Non-Personal Data such as:** • Non-personal in device hostname • Device operating system	• See Purposes immediately above for User and Device Identity Data	• Deleted upon request
AI Assistant Data	**Personal Data:** • Admin username and/or ID	• Large language AI model that extracts key words for the purpose of assisting customer Admin in creating, optimizing and querying security policies and answering product related queries.	• Up to 12 months after prompt/response thread becomes inactive (user is no longer adding to the thread)
AI Assistant Data	**Non-Personal Data such as** • Org ID	• See Purposes immediately above for AI Assistant Data	• Up to 12 months after prompt/response thread becomes inactive (user is no longer adding to the thread)
Business Analytics Data	**Personal Data:** • Admin first and last name • Job title • Admin role within Secure Access service • Admin Email address • Admin username and/or ID • Admin device type and device name	• Internal business and product analytics and reporting to inform data-driven business and product decisions and product improvements • Product and feature usage analytics, sales support, renewal support, product adoption and deployment assistance	• Deleted upon request
Business Analytics Data	**Non-Personal Data such as:** • Account information (e.g., Company name, Org ID, etc.) • Install base data (e.g. license type, # of provisioned users, VPN profile data, etc.) • Feature usage data (e.g. bandwidth, # of policies/types, configured features)	• See Purposes immediately above for Business Analytics Data	• Deleted upon request

For threat intelligence research purposes, please note that the Personal Data listed in Tables 1 and 2 for DNS Security Event Logs, Secure Web Gateway Event Logs and Firewall-as-a-Service Event Logs 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. Secure Access uses Amazon Web Services (AWS) data centers in the United States for the Cisco Secure Access configuration, policies, reporting, and control plane (collectively, the "Control Plane"). Cisco uses a combination of AWS (virtual) and colocation (physical) edge data centers for connecting customers to Cisco Secure Access and for data processing to provide security and enforce customer policies (collectively, the "Data Plane") to deliver the service globally. Please see tables and additional detail below.

Data Storage

Data Plane usage and event data ("Event Logs") to the extent logging is enabled, and Control Plane Data, are stored in the locations set forth in Table 3 (Data Center Storage). Customers have the option for most Event Logs to log nothing, log everything, or log only security data. Please see the Secure Access product documentation for details on logging. Logging for intrusion prevention (IPS) is always on.

Table 3: Data Center Storage

Data Category	Infrastructure Provider	Data Center Storage Locations
Account Data	• AWS	• Oregon, Virginia, USA
Connection Data (ZTA, VPN-as-a-Service, Roaming)	• AWS	• Administrative service logs: Oregon, Virginia, USA • Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Device Posture Data	• AWS	• Posture logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection • All other logs: Oregon, Virginia, USA
DNS Security Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection • If using DNS block page, hosted on applicable Global Edge Data Centers
Secure Web Gateway Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Firewall-as-a Service Data	• AWS	• Administrative service logs: Oregon, Virginia, USA • Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Cloud Malware Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
DLP Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
DSPM Data	• AWS	• Both Event Logs and non-Event Log data: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Cloud App Discovery Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
Remote Browser Isolation (RBI) Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection

Semantic Inspection Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection
UEBA Data	• AWS	• Event Logs: USA (Oregon, Virginia) region or EU (Germany, Ireland) region upon customer selection • Cisco Identity Intelligence: Oregon, Virginia USA
Control Plane Data	• AWS	• Oregon, Virginia USA • Global Edge Data Centers (distributed to Global Edge Data Centers for policy enforcement) *Audit Logs are stored in USA only
Cisco AI Assistant Data	• AWS	• Oregon, USA
Business Analytics Data	• AWS	• Oregon, Virginia, USA

Data Processing

A user's connection to Cisco Secure Access is usually through the closest available service-enabled edge data center or designated IPSec tunnel or VPN region location if applicable.

DNS resolution utilizes a network of globally distributed edge data centers. Routing of the DNS query is based on the Anycast protocol which usually routes the DNS query to the closest available service-enabled edge data center. DNS processing may be offloaded from time to time as needed to one of the AWS locations listed in the table below. Cloud Malware and SaaS API-Based DLP content inspection occur at AWS in the United States. Email DLP inspection is typically performed at the data center closest to Cisco Email Threat Defense's data centers. Refer to the Email Threat Defense Offer Disclosure on the Cisco Trust Portal for more details. All other security processing occurs at an applicable service-enabled AWS edge data center listed in the table below, usually at the data center closest to the user or to the selected IPSec or VPN region if applicable.

For Secure Internet Access, security processing and enforcement occur at the same data center that served as the user's connection point to Cisco Secure Access. However, for Secure Private Access (to private applications), Resource Connectors are used to connect the private application content to an edge data center closest to the application (rather than the user) in order to ensure optimum performance.

Table 4: Data Center Processing

Data Category	Infrastructure Provider	Data Center Processing Locations
Account Data	• AWS	• Oregon, Virginia, USA
Connection Data (ZTA, VPN-as-a-Service, Roaming)	• Global Edge Data Centers (colocation providers leveraged from Cisco Secure Access data center network)	• See Global Edge Data Centers
Device Posture Data	• See Global Edge Data Centers	• See Global Edge Data Centers
DNS Security Data	• See Global Edge Data Centers	• See Global Edge Data Centers
	• AWS	• California, Virginia, Minnesota, Texas, Washington, USA • Australia • Brazil • Canada • France • UK • Italy • India • Japan • Singapore • The Netherlands
DNS Block Page Hosts	• See Global Edge Data Centers	• See Global Edge Data Centers

Secure Web Gateway Data	• See Global Edge Data Centers	• See Global Edge Data Centers
Firewall-as-a-Service 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, Email DLP, Secure Client Endpoint DLP, AI Guardrails	• See Global Edge Data Centers • Machine learning based Document Classification feature - AWS	• See Global Edge Data Centers • For machine learning based Document Classification feature, Oregon, Virginia USA data centers • For Email DLP, processing is performed at the Global Edge Data Centers closest to Email Threat Defense's data centers.
Data Loss Prevention Data - SaaS API-based DLP	• AWS	• Oregon, USA • Virginia, USA
Semantic Inspection	• AWS (Cisco operated data centers listed in Global Edge Data Centers are targeted for the future)	• See Global Edge Data Centers
EUBA Data	• AWS	• Oregon, USA • Virginia, USA • Germany
Cloud App Discovery Data	• See Global Edge Data Centers	• See Global Edge Data Centers
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
Control Plane Data	• AWS	• Oregon, Virginia, USA • Global Edge Data Center (distributed to Global Edge Data Centers for policy enforcement)
Cisco AI Assistant Data	• AWS Bedrock	• Oregon, Virginia, USA
	• Azure Open AI	• Arizona, USA • California, USA • Georgia, USA • Illinois, USA • Iowa, USA • Texas, USA • Virginia, USA • Washington, USA • Wyoming, USA • Canada • Sweden
Business Analytics Data	• AWS	• Oregon, Virginia, USA

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	Data Elements	Service Type	Data Center Locations
See Global Edge Data Center for colocation providers (subcontractor)	• N/A	• Colocation infrastructure provider	• See Global Edge Data Center

AWS (subprocessor)	• See Tables 1 and 2	• Cloud infrastructure provider, Event Log data warehouse, AWS Bedrock - foundation AI Model provider.	• See Global Edge Data Center
			• Additional data centers for DNS Security Data:
			  • California, Virginia, Minnesota, Texas, Washington, USA
			  • Australia
			  • Brazil
			  • Canada
			  • France
			  • UK
			  • Italy
			  • India
			  • Japan
			  • Brazil
			  • Singapore
			  • The Netherlands

Amplitude (subprocessor)	• Admin User ID, role, dashboard activity usage metrics	• To analyze Business Analytics Data for feature usage and product functionality	• Oregon, USA
Catchpoint Systems (subcontractor)	• Cisco Systems Information	• Subcontractor: Monitor application performance	• Neveda, USA
Databricks (subprocessor)	• Event Logs. Personal data in proxy and DNS logs (does not include logs of customers selecting EU geo)	• To analyze log data	• Oregon, USA
Kentik (subprocessor)	• IP address	• Network analyzer	• Virginia, USA
Menlo Security (subprocessor)	• Remote Browser Isolation Data	• 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)	• Email header data • Email body	• Automated in-product emails such as password reset and account provisioning emails	• Oregon, USA

Microsoft Azure OpenAI Services subprocessor)	• Cisco AI Assistant Data	• Foundation AI model provider for AI Assistant	• Arizona, USA • California, USA • Georgia, USA • Illinois, USA • Iowa, USA • Texas, USA • Virginia, USA • Washington, USA • Wyoming, USA • Canada • Sweden
PagerDuty (subcontractor)	• Cisco Systems Information, Cisco Content	• Automated incident alerts	• California, USA • Ohio, USA • Oregon, USA
Salesforce (subprocessor)	• Account Data	• To provision the service and provide support	• Texas, USA • Arizona, USA.
Snowflake Cloud Data Warehouse Solution (subprocessor)	• Cisco Analytics Data	• Business Analytics Data warehouse	• Virginia, USA
Walkme (subprocessor)	• User ID • IP address • Clickstream data	• Provides users with a step-by-step tour and guidance on product usage	• California, USA • Oregon, USA

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 Cisco TAC’s Offer Disclosure.

For comprehensive technical support and to diagnose complex network issues, Cisco may perform packet captures. These captures include source and destination IP addresses and may also contain more sensitive information if your network traffic is unencrypted. All data collected is securely handled by authorized personnel for troubleshooting and promptly deleted once the support issue is resolved.

2c. Access and Sharing

The categories, volume, and frequency of Customer Systems Information generated by this Cisco Offer are dependent on the Customer’s configuration and use case(s). This Cisco Offer’s support web pages provide more detailed information.

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 Baseline API Terms.

- Cisco Cloud Security API

  Customers may send requests for expanded API or data interface capabilities through their 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
Account Data	Authorized Cisco Employees	• Provision customer's account; billing/invoicing and tax compliance; export compliance; supporting the service subject to applicable data access and security controls	• Encryption in transit and at rest
	Customer Admins	• Enter, modify, control Admin data	
Connection Data (ZTN, VPN-as-a-Service, Roaming)	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 Admins	• View data on UI and through reporting. Data can be exported to S3 by opting into the data export option	
Device Posture 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
• **DNS Security Data** • **Secure Web Gateway Data** • **Firewall-as-a-Service Data** • **Cloud Malware Data** • **DLP Data** • **Cloud App Discovery Data** • **RBI Data** • **Semantic Inspection** • **EUBA Data**	Authorized Cisco Employees	• Deliver, support, maintain, improve the service, and perform threat intelligence research, subject to applicable data access and security controls	• Encryption in transit and at rest
	Customer Admins	• View data on UI and through reporting. Data can be exported to S3 by opting into the data export option	• Encryption in transit and at rest
Control Plane Data: • **Configuration and Policy Data** • **User and Device Identity 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 Admins	• Manage and configure account, establish, and maintain policies	
Cisco AI Assistant Data	Authorized Cisco Employees	• Deliver, support, troubleshoot, maintain, improve the service, subject to applicable data access and security controls	• Encryption in transit and at rest
	Customer Admins	• Refer to saved prompts and response conversations	
Business Analytics Data	Authorized Cisco Employees	• Organize, analyze, and report on business and product usage data; improve the service, subject to applicable data access and security controls	• Encryption in transit and at rest

Encryption in transit means data is encrypted between Cisco Secure Access data centers while traveling over the internet. Data is encrypted in transit from the user to the Secure Access edge data center if the customer uses

HTTPS or another encrypted communication method such as a secure tunnel or DNSCrypt. Some data may be unencrypted in transit between Secure Access services within the same data center. All data stored by Cisco Secure Access (including back-ups) is encrypted at rest except as described in this paragraph. For performance and troubleshooting purposes, Event Logs generated by Secure Web Gateway are unencrypted at rest for a maximum of 2 hours at the applicable edge data center. In addition, the Secure Access Investigate research team is still in the process of completing its encryption at rest project. DNS Security Event Logs for all customers other than those selecting the EU Event Log storage location are currently unencrypted in some environments. These DNS Security Event Logs contain the source IP and timestamp.

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 data center for processing using a randomly generated numeric ID. While a customer has the option for some Secure Access 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 Secure Access security.

Access to customer information is subject to Cisco's access management policy and 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.

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:

- Trust Package
- ISO 27001
- ISO 27017
- ISO 27018
- ISMAP
- SOC 2
- C5
- CAIQ
- CSA STAR
- ENS Certification