Cisco Cognitive Intelligence

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

Cisco Cognitive Intelligence is a cloud-based security solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cognitive Intelligence in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Cognitive Intelligence in order to provide its functionality.

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

1. Overview

Cisco Cognitive Intelligence is a cloud-based malware behavioral analysis solution for threat detection and analytics that leverages (1) web proxy logs from a Cisco web gateway solution such as Cisco Secure Web Appliance, Cloud Web Security, or third-party web proxies and (2) NetFlow from Cisco Secure Network Analytics and/or Cisco Secure Cloud Analytics (which may include Enhanced NetFlow if the customer enables Cisco Encrypted Traffic Analytics) and (3) Event Log Data from Cisco Secure Endpoint. The web proxy logs and/or NetFlow help identify malware present within a customer's environment and allow a customer to research related active malicious behaviors. Cognitive Intelligence is available via (a) Secure Endpoint, (b) Secure Endpoint on Secure Web Appliance, (c) Secure Network Analytics and (d) Secure Cloud Analytics. Finally, Cognitive Intelligence's implementation of machine learning based on its Static File Analysis capability is also available to Secure Endpoint customers via an integration with Cisco Secure Malware Analytics.

For more information about Cognitive Intelligence, visit https://www.cisco.com/c/en/us/products/security/cognitive-threat-analytics/index.html.

Cognitive Intelligence integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving and/or sending personal data from/to Cognitive Intelligence.

2. Personal Data Processing

The table below lists the personal data processed by Cognitive Intelligence to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Registration Information	• Name • Address • Email address • Phone number	• Account creation • Product enablement, product use notifications, training and support

Web Log Usage and Event Data	• Username[1] • Device IP address • Destination IP address	• Security analytics, forensics, and efficacy research • Product enablement • Global threat intelligence research
NetFlow Usage and Event Data	• Device IP address • Destination IP address • Device MAC address • Customer Group ID[2] • Customer TrustSec Security Group Tag ID and Name	• Security analytics, forensics, and efficacy research • Product enablement • Global threat intelligence research
Firewall Event Data and Logs[3]	• Username • IP address • Event type • File name • Accessed URLs • Device host name • Passive DNS logs	• Global threat intelligence research
Enhanced NetFlow Usage and Event Data for Encrypted Traffic Analytics (ETA)[4]	• Any personal data contained in the Initial Data Packet (IDP)[5]	• Security analytics, forensics, and efficacy research • Product enablement • Global threat intelligence research
Web and API Usage Log	• Identity of device used to upload telemetry data (ex: serial number or name designated by user) • Name of end user who accessed the logs	• Security analytics, forensics, and efficacy research • Product enablement • Global threat intelligence research
Secure Endpoint Event Log and Usage Data	• Username • File name • File path name • Local URL, MAC address, IP address • Remote URL, MAC address, IP address	• Security analytics, forensics, and efficacy research • Product enablement • Global threat intelligence research
Customer Submitted Files[6]	• Any personal data that may be contained in a file submitted for analysis	• Security analytics, forensics, and efficacy research • Product enablement
SPAD Reports[7]	• Username • Computer name • IP address	• Improve customer experience, configuration and deployment support, assist with interpretation of threat detections, general product enablement, and integration with other Cisco and third-party products

[1] Customer username collection is an opt-in feature that can be enabled through configuration settings.

[2] Also known as Secure Network Analytics Host Groups; can be configured to capture internal traffic telemetry in addition to external traffic telemetry.

[3] Only applies to customers using Cognitive Intelligence as part of a Secure Cloud Analytics subscription.

[4] Enhanced NetFlow usage and event data is provided in addition to NetFlow usage and event data if generated by the underlying enterprise network equipment.

[5] IDP includes any data sent in the first packet of the communication, which may include sensitive data for unencrypted protocols (examples include DNS traffic, plain-text HTTP URL, cookies, username, password, IP header, TLS header, Service Name Identifier, and Cipher suites.

[6] Files are collected via Cognitive Intelligence' "Static File Analysis" available via integration with Secure Endpoint and/or Secure Malware Analytics.

[7] "SPAD Report" means the Simple Portal for Administration report created within the Cognitive Intelligence portal, which provides a preview of the customer's reports generated by Cognitive Intelligence. SPAD Report data is only processed if access is granted.

3. Data Center Locations

Cognitive Intelligence leverages third party cloud hosting providers to provide services globally.

Infrastructure Provider	Description	Location
AWS US Cloud	Cloud infrastructure provider	United States – Virginia
AWS EU Cloud	Cloud infrastructure provider	Ireland
Equinix	Cloud co-location facility for Cisco Talos global threat intelligence	United States – Virginia
Vazata	Cloud co-location facility for Cisco Threat Intelligence Platform (TIP)	United States - Texas

Note: When you purchase a service subscription, Cisco always creates, processes, and stores your information in the United States regardless of the subsequent provisioning of your accounts in a chosen regional cloud: US, EU (Ireland), or Asia Pacific (Japan). All data are encrypted in transit.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

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

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Customer	Security administration and operations
	Cisco	Account creation, license entitlement validation, and general product support and operations
WebLog Usage and Event Data	Customer	Security administration and operations
	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
NetFlow Usage and Event Data	Customer	Security administration and operations
	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
Firewall Event Data and Logs	Customer	Security administration and operations
	Cisco	Global threat intelligence research

Enhanced NetFlow Usage and Event Data for Encrypted Traffic Analytics (ETA)	Customer	Security administration and operations
	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
Web and API Usage Log	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
Secure Endpoint Event Log Usage and Event Data	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
Customer Submitted Files	Cisco	Security analytics, forensics, efficacy research, general product enablement, and global threat intelligence research
SPAD Reports	Customer	Security administration and operations
	Cisco	Improve customer experience, configuration and deployment support, assist with interpretation of threat detections, general product enablement, and integration with other Cisco and third-party products

6. Data Portability

Data Portability Requirements are not applicable to this product.

7. Data Deletion and Retention

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

Type of Personal Data	Retention Period	Reason for Retention
Registration Information[8]	• Upon request	• Security administration and operations • General product enablement
Web Log Usage and Event Data[9]	• 90 days • Upon request	• 90 days: Security administration and operations, providing security analytics, forensics, and general product enablement • Deleted upon request: product improvement, applied research, efficacy research, and global threat intelligence research
NetFlow Usage and Event Data	• 90 days • Upon request	• 90 days: Security administration and operations, providing security analytics, forensics, and general product enablement • Deleted upon request: product improvement, applied research, efficacy research, and global threat intelligence research

[8] Registration Information data is currently retained indefinitely in the UK data center. When a customer terminates its Cognitive Intelligence subscription, it can specifically request that its Registration Information be purged from Cisco's data storage and backups by opening a Cisco TAC case.

[9] For event data, ninety (90) day time-based "First-in-First-Out" data store is used to capture and store usage and event data for presentation of customer specific threat events Cognitive Intelligence. The prescribed retention period is defined in accordance with a look-back window for which threat events and forensic information is available to the customer within Cognitive Intelligence. A large portion of event data collected are behaviors, statistics and metadata extracted from the source telemetry. Event Data may be kept for mining, efficacy research, and global threat intelligence research purposes. When a customer terminates its subscription, it can specifically request that its data be purge from Cisco's data storage and backups by opening a Cisco TAC case. For source telemetry, data will be deleted ninety (90) days after processing. However, for any source telemetry directly associated with suspected or confirmed infections may be retained indefinitely for data mining, efficacy research and global threat intelligence purposes.

Firewall Event Data and Logs	• 90 days • Upon request	• 90 days: Security administration and operations, providing security analytics, forensics, and general product enablement • Deleted upon request: product improvement, applied research, efficacy research, and global threat intelligence research
Enhanced NetFlow Usage and Event Data for Encrypted Traffic Analytics (ETA)	• 90 days • Upon request	• 90 days: Security administration and operations, providing security analytics, forensics, and general product enablement • Deleted upon request: product improvement, applied research, efficacy research, and global threat intelligence research
Web and API Usage Log	• 3 years	• Security administration and operations, providing security analytics, forensics, and general product enablement
Secure Endpoint Event Log Usage and Event Data	• 90 days • Upon request	• 90 days: Security administration and operations, providing security analytics, forensics, and general product enablement • Deleted upon request: product improvement, applied research, efficacy research, and global threat intelligence research
Customer Submitted Files	• 24 months	• Product improvement, applied research, efficacy research, and global threat intelligence research
SPAD Reports	• 90 days	• Improve customer experience, advise on appropriate configuration and deployment, assist with interpretation of threat detections, general product enablement, and integration with other Cisco and third-party products

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure

Personal Data Category	Security Controls and Measures
Registration Information	• Encrypted in transit via TLS/SSL • Encrypted at rest
Web Log Usage and Event Data	• Cisco/AWS: Encrypted in transit via TLS/SSL; encrypted at rest • Equinix/Vazata; Encrypted in transit via TLS/SSL; protected at rest by access control
NetFlow Usage and Event Data	• Cisco/AWS: Encrypted in transit via TLS/SSL; encrypted at rest • Equinix/Vazata; Encrypted in transit via TLS/SSL; protected at rest by access control
Firewall Event Data and Logs	• Cisco/AWS: Encrypted in transit via TLS/SSL; encrypted at rest • Equinix/Vazata; Encrypted in transit via TLS/SSL; protected at rest by access control
Enhanced NetFlow Usage and Event Data for Encrypted Traffic Analytics (ETA)	• Cisco/AWS: Encrypted in transit via TLS/SSL; encrypted at rest • Equinix/Vazata; Encrypted in transit via TLS/SSL; protected at rest by access control
Web and API Usage Log	• Encrypted in transit via TLS/SSL • Encrypted at rest
Secure Endpoint Event Log Usage and Event Data	• Encrypted in transit via TLS/SSL • Encrypted at rest
Customer Submitted Files	• Encrypted in transit via TLS/SSL • Encrypted at rest
SPAD Reports	• Encrypted in transit via TLS/SSL • Encrypted at rest

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
AWS	• Web Log Usage and Event Data • NetFlow Usage and Event Data • Enhanced Netflow Usage and Event Data for Encrypted Traffic Analytics (ETA) • Web and API Usage Log • Secure Endpoint Event Log Usage and Event Data • Customer Submitted Files	Cisco leverages the AWS cloud to help provide security assurance, service elasticity, and resilience to Cognitive Intelligence	Ireland USA - Virginia
Equinix	• Any personal data that may be contained in a file submitted for analysis	Equinix is a Cisco-approved third party co-location facility used by Cisco Talos for global threat intelligence research	USA – California, Texas, Virginia
Vazata	• Any personal data that may be contained in a file submitted for analysis	Vazata is a Cisco-approved third party co-location facility used by Cisco TIP for global threat intelligence research	USA - Texas

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

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

Requests can be made by submitting a request via:

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

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

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

13. General Information

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

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

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