Cisco Secure Email Phishing Defense

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Email Phishing Defense.

Cisco Secure Email Phishing Defense 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 Cisco Secure Email Phishing Defense 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 Secure Email Phishing Defense in order to provide its functionality.

1. Overview

Cisco Secure Email Phishing Defense stops identity deception-based attacks such as social engineering, impostors and business email compromise and provides local email intelligence and advanced machine learning techniques to model trusted email behavior on the internet, within organizations and between individuals. Cisco Secure Email Phishing Defense integrates machine learning techniques to drive daily model updates, maintaining a real-time understanding of email behavior to stop identity deception.

For more information about Cisco Secure Email Phishing Defense, please see:
https://www.cisco.com/c/en/us/products/security/email-security/index.html

Cisco Secure Email Phishing Defense integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco.

Note, Cisco Secure Email Phishing Defense may also be integrated with third-party products. Cisco is not responsible for customer data once it leaves Cisco Secure Email Phishing Defense 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.

2. Personal Data Processing

The table below lists the personal data processed by Cisco Secure Email Phishing Defense to provide its services and describes why the data is processed.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Address • Email Address • User ID	• Product administration: Creating an account, validating license entitlements, general product support and administration. • Product notifications • Product training
Email Metadata[1]	• Email From header • Email friendly From header • Email “rcpt to” header • Email friendly To header	Message Scoring • Data used to determine the authenticity and reputation of the underlying identity.
Email Metadata	• Email Subject	Email Subject Message Scoring • Data used to assist in message identification. • This data can be suppressed at the customer’s discretion.

[1] For customers also licensing Cisco Secure Email Gateway and Cisco Secure Email Cloud Gateway, all Email Metadata is provided directly form those products.

Email Metadata	- Attachment Filename - Attachment file format and presence of macros/malicious code - Attachment Hash (e.g. encrypted MDS or SHA1 format) - Uniform Resource Identifier (URI)	Attachment Filename and URI Analysis Message Scoring - Data used to assist in message identification and threat classification and to determine the authenticity and reputation of the underlying identity assertion. - This data can be suppressed at the customer's discretion.
Email Message Content	- Personal data, if any, included in email message including attachments. However, this applies only if the Hosted Sensor option is selected. See Section 3.	Metadata Extraction - The Cisco Secure Email Phishing Defense Sensor ingests the email message content, extracts the required metadata, and sends the metadata to Cisco Secure Email Phishing Defense for analysis. See Section 3.

Cisco Secure Email Phishing Defense collects "System information" to assist Cisco with understanding product usage and enabling product improvements. Customers have the option of disabling the transmission of Systems Information. For more information on Cisco Secure Email Phishing Defense collection and use of Systems Information, see the Systems Information Data Brief. Any personal data that is processed as part of this Systems Information is protected in accordance.

3. Data Ingest Process

Cisco Secure Email Phishing Defense provides insight into the traffic coming into a customer's enterprise. To realize this value, and except as provided under Cisco Email Security Customers below, customers configure their Secure Email Gateways to copy all incoming messages to the Cisco Secure Email Phishing Defense "Sensor". The sensor component receives the full email message including the body and any attachments present. The Sensor extracts the Email Metadata (as described in Section 2 above), forwards the metadata into the Cisco Secure Email Phishing Defense pipeline and then immediately deletes the message (including attachments). The Sensor can either be located "on premises", within the enterprise's internal network or by Cisco ("Hosted Sensors").

On Premises
Customers have complete control over the sensor including full "root" level access to the operating system and host application. Cisco employees cannot access an on premises Sensor without the permission of the customer.

Hosted Sensors
Cisco Secure Email Phishing Protection's Hosted Sensors are provisioned in a dedicated and separate Amazon Web Services account. Hosted Sensors are not "multi-tenant". Each customer gets their own Virtual Private Cloud (VPC), their own Elastic Load Balancer (ELB), and their own EC2 Autoscale Group (ASG). The underlying AWS IaaS is multitenant. Cisco engineers cannot access the Hosted Sensor EC2 instances using the root account and only authorized Cisco engineers have access to the Hosted Sensor environment. All Hosted Sensor actions are logged locally and can be reviewed with the customer. This includes evidence that each message is deleted post-processing.

Cisco Secure Email Customers:
For Cisco customers using either Cisco Secure Email Gateway or Cisco Secure Email Cloud Gateway, the Cisco email security solution acts as a sensor and provides the Email Metadata as described in Section 2 to Cisco Secure Email Phishing Defense via API.

4. Cross-Border Data Transfer Mechanisms

When a customer purchases a subscription to Cisco Secure Email Phishing Defense, that customer's information (both the data relating to the customer's employees who are in contact with Cisco to procure and administer the products on behalf of customers, and the data processed through Cisco's delivery of its services to customers) is processed and stored in the United States. A cross- border transfer occurs if a customer's account and contact information is transmitted to Cisco from outside the United States and if the personal data described in Section 2 is transmitted to Cisco Secure Email Phishing Defense from outside of the United States. Cisco Secure Email Phishing Defense is hosted in the United States. Please see Section 9 for information regarding sub-processors and data center location(s).

Cisco has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- 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 Cisco Secure Email Phishing Defense to carry out the service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Information	Customers	Granting and managing access to their own account
	Cisco Employees – Sales Administration, Licensing Operations, Engineering and Support staff only	Creating an account and validating license entitlements and general product support and operations
Email Metadata	Customers	Security administration and operations
	Cisco Employees – Sales Administration, Licensing Operations, Engineering and Support staff only	Providing message trust scores and general product support and operations
Email Message Content (for Hosted Sensor deployment)	Customers	Security administration and operations
	Limited group of Cisco Engineers	Providing message trust scores and general product support and operations

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 Cisco Secure Email Phishing Defense, 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	Subscription period	Validating license entitlements and general product support and operations
Email Metadata	60 days (active data stores) Subscription period (application and backup/archive)	Providing message trust scores and general product support and operations
Email Message Content (for Hosted Sensor deployment)	Processing period only	Not retained

Note: Customer's Registration Information and Email Metadata will be purged from Cisco Secure Email Phishing Defense upon request by opening a Cisco TAC case.

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 (TLS) and at rest (AES 256)
Email Metadata	Encrypted in transit and at rest in primary data stores and S3 buckets
Email Message Content (for Hosted Sensor deployment)	While being processed by a Hosted Sensor, message level data is encrypted both in transit and, if temporarily persisted, at rest using encrypted Elastic Block Storage (EBS) volumes

9. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to you by Cisco. The current list of sub-processors is set out below. Sub-processors may change from time to time and this Privacy Data Sheet will be updated to reflect those changes.

Sub-processor	Personal Data	Service Type	Location of Data Center
Agari Data, Inc. (www.agari.com)	Registration Information Email Metadata Email Message Content (for Hosted Sensor deployment)	Cisco utilizes Agari Data, Inc. (www.agari.com) as a third-party provider for Cisco Secure Email Phishing Defense. Where Cisco refers to Cisco employees in this data sheet, this includes authorized employees of Agari Data, Inc.	United States
Amazon Web Services (“AWS”)	Registration Information Email Metadata Email Message Content (for Hosted Sensor deployment)	Cisco Secure Email Phishing Defense is hosted in the United States by Amazon Web Services (AWS). For information regarding AWS compliance/certification, please refer to documentation online at https://aws.amazon.com/compliance/.	United States (AWS U.S. West region)
Pendo (www.pendo.io)	User names (i.e. email address)	Pendo (www.pendo.io) is utilized for product usage analytics.	United States (Google Cloud)

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:

Chief Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES

Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES

APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE

EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH
Amsterdam-Zuidoost NETHERLANDS

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.