Cisco Email Security Appliance

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by the Cisco Email Security Appliance.

1. Overview of Cisco Email Security Appliance Capabilities

The Cisco Email Security Appliance ("ESA") is an on-premise email security solution that blocks spam and security threats from the Internet and, depending on the features licensed, prevents the accidental or intentional leakage of customer data.

ESA offers inbound protection and outbound control of your email traffic. The following feature functionalities are available depending on the licensed features purchased:

- Anti-spam
- Intelligent Multi-Scan Anti-spam
- Anti-virus
- Outbreak Filters
- Advanced Malware Protection
- Safe Unsubscribe
- Image Analysis
- Email Encryption (CRES)
- Data Loss Prevention

For more information about ESA, please see: https://cisco.com/go/emailsecurity.

Your ESA license gives you access to Cisco SecureX, Cisco's integrated security platform that aggregates threat intelligence (through SecureX threat response, also known as Cisco Threat Response), unifies visibility across various Cisco and third party security products, enables automated workflows, and more. The ESA license also includes the right to access and use Cognitive Intelligence, and also makes available integrations with various Cisco products. For more information regarding the processing of personal data by these features and integrations, please refer to the applicable Privacy Data Sheet.

In addition, ESA may integrate with third-party products. Protection of data within the applicable third-party system is governed by the contract(s) and policies of the applicable third party.

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from ESA and from the customer, and may share such data with Cisco Talos as set forth herein. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data. Cisco does not process this data for any other purpose than to assist the customer to resolve issues.

ESA is Smart License enabled. Personal data may be provided to Cisco in the form of a user credential to associate it with a related Cisco.com account (i.e. CCO) or Smart License account. For more information regarding Smart License accounts and related data collection, please refer to the Smart Software Licensing Privacy Data Sheet.

2. Personal Data Processing

The table below lists the personal data used by ESA and transferred to Cisco to carry out the services and describes why we process that personal data. Note that the processing of certain personal data by Cisco set forth below is determined by the customer's choice (i) to enable or disable (as applicable) the following Cisco Talos global threat intelligence services: Service Logs, Sender Domain Reputation, Sender IP Reputation, URL Reputation and IPAS (IronPort Anti-Spam), and/or (ii) to license additional Cisco products that integrate with ESA. Certain datasets listed below may not always qualify as personal data by itself, but for the purposes of this Privacy Data Sheet, Cisco shall treat it as personal data.

Important note: *ESA is an on-premise product that processes certain personal data which resides within ESA and the customer's data centers. The following table covers the personal data that may be transferred to Cisco for processing as described below.*

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Information	• Name • Email Address • Phone Number • Physical Address • Smart Account Usernames/IDs	• Creating an account • Validating license entitlements • Enable product operations and functionality.
Service Logs Data[1]	• Email address (e.g. jsmith@gmail.com) • Email display name (e.g. <john smith> • GUID for email message • GUID for connection (sender IP address) • AMP conviction • Message metadata (includes GUID that can tie back to individual email address) • Filename[2]	• Global threat intelligence research
Sender Domain Reputation Data[3]	• GUID for email message • GUID for connection (sender IP address) • ESA Message ID • Email sender IP address • SMTP envelope fields (sender and recipient email addresses) • Friendly "from" • List-Unsubscribe headers • Message ID header • FQDN (fully qualified domain name)	• Global threat intelligence research
Sender IP Reputation Data[4]	• IP address of the sending email server • GUID for connection (sender IP address).	• Global threat intelligence research
URL Reputation Data[5]	• GUID for email message • GUID for connection (sender IP address)	• Global threat intelligence research • Shared with Cisco Cognitive Intelligence to develop and deploy URL exploit detection models. For further information on how the URL Reputation Data is processed by Cognitive Intelligence, please refer to the Cognitive Intelligence Privacy Data Sheet.
Email Sample Data[6] (i.e. spam/ham/marketing emails)	• Email Envelope Header • Email Data Header • Email Body (email body and/or attachment)	• ESA technical support • Global threat intelligence research for false positive/false negative diagnosis and resolution

[1] Only processed if customer has not disabled Service Logs

[2] Only processed if customer has enabled IPAS

[3] Only processed if customer enables the "Additional Attributes" feature of Sender Domain Reputation and also chooses to send the full email address)

[4] Only processed if customer has not disabled Sender IP Reputation

[5] Only processed if customer has enabled URL Reputation

[6] If customer chooses to send false positive/false negative email samples to Cisco TAC, TAC may share with Cisco Talos and the third party subprocessors listed herein for further analysis

File attachments [7]	• Any personal data that may be contained in the files	• ESA technical support • Global threat intelligence research to correct erroneous blocking/detection of the files as malicious
IPAS (IronPort Anti-Spam Engine) Data[8]	• GUID for email message • Filename • IPAS results (spam score, rule hits, sender IP address)	• Global threat intelligence research
Email Metadata for Integration with Cisco[9] Advanced Phishing Protection ("APP")	• Email Envelope Header (Sender, Recipient, Host/IP address) • Email Data Header (From, To, Subject, Reply-to Headers	• To enable integration between ESA and APPand processing by APP for customers with both Cisco products. For further information on how this Email Metadata is processed by APP, please refer to the APP Privacy Data Sheet for details.

Non-Personal Data Usage:
In addition to the non-personal data processed by ESA, non-personal usage data may be provided to Cisco Customer Success to assist with customer journeys, product deployment and similar customer success initiatives. This data may include, by way of example, which licensed features are activated by a customer. Customer Success is able to associate the data with a specific customer but not with the applicable end user. Customers can opt-out of sending data to Cisco Customer Success. Similarly, non-personal interface usage data is transferred to Google Analytics to assist Cisco with product usage analysis and continuous product improvement. Customers can opt-out of sending such interface usage data to Google Analytics.

3. Cross-Border Transfers

If a Personal Data Category above is processed for the purposes of "Global threat intelligence research," then the processing and storage of such personal data is conducted by Cisco's global threat intelligence teams, which have data centers in the U.S. only.

With respect to data collected by by the global threat intelligence teams, the Global Co-location Data Center Networks below use dynamic Anycast routing decisions to route each customer's Service Log Data, Sender Domain Reputation Data, Sender IP Reputation Data, URL Reputation Data and IPAS Data to any data center facility listed below (provided the features are enabled as described herein), although normally the data center in which the data is routed will be to the closest physical location to the ESA deployment.

By default, Service Logs Data, Sender Domain Reputation Data, Sender IP Reputation Data, URL Reputation Data, Email Sample Data and IPAS Data are also processed in the following global threat intelligence data warehouses in the United States (1) Amazon Web Services (AWS) data centers; (2) Equinix; and (3) Vazata for additional processing, threat intelligence analysis, and storage. This is necessary for the delivery of ESA, as threat intelligence analytics requires the examination of worldwide data in real time.

Global Co-location Data Center Network

Location	Provider	Certification
Amsterdam, Netherlands	Interxion	ISO27001/ISO22301
Ashburn, VA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Atlanta, GA	Digital Reality	SOC2/SOC3/PCI-DSS/ISO 27001
Bucharest, Romania	NX DATA	ISO9001/ISO27001
Chicago, IL	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Copenhagen, Denmark	Interxion	ISO27001/ISO22301
Dallas, TX	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Denver, CO	CoreSite	ISO 27001/SOC 1 Type 2/SOC 2 Type 2/PCI DSS/HIPAA
Dubai, United Arab Emirates	Equinix	ISO27001/OHSAS/PCI/SOC1/SOC2

[7] If customer chooses to send erroneously blocked file attachments to Cisco TAC, TAC may share with Cisco Talos and the third party subprocessors listed herein for further analysis
[8] Only processed if customer has enabled IPAS
[9]This personal data is shared with APP for customers who are using both ESA and APP

Dublin, Ireland	Interxion	ISO27001/ISO9001/ISO22301
Frankfurt, Germany	Equinix	ISO27001/PCI/SOC1/SOC2/ISO9001
Hong Kong	Equinix	ISO27001/PCI/SOC1
Johannesburg, South Africa	Teraco	ISO27001/PCI/ISO9001
London, UK	Equinix	ISO27001/PCI/SOC1/SOC2/ISO9001
Los Angeles, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Melbourne, Australia	NEXT DC	ISO27001/ISO9001/UpTime Institute Certified Tier 4
Miami, FL	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Milan, Italy	Equinix	ISO27001/ISO9001/PCI
Mumbai, India	STT	ISO27001/ISO20000/ISO14001/TL9000/PCI-DSS
New York, NY	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Palo Alto, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Paris, France	Equinix	ISO27001/ISO9001/SOC1/SOC2/PCI-DSS/ISO50001/ISO14001/OHSAS18001
Prague, Czech Republic	CECOLO	ISO27001/ISO14001/ISO18001(OHSAS)/ISO9001
Reston, VA	Coresite	ISO27001/HIPAA/PCI/SOC1/SOC2
Rio de Janeiro, Brazil	Equinix	ISO 22301, SOC 1 Type II, PCI-DSS, SOC 2 Type II, ISO 9001-2008, ISO 27001
San Jose, CA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Sao Paulo, Brazil	Equinix	ISO27001/ISO9001/SOC1/SOC2
Seattle, WA	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Singapore	Equinix	ISO27001/PCI/SOC1/SOC2/SS564
Sydney, Australia	Equinix	ISO27001/PCI/SOC1/SCO2
Tokyo, Japan	Equinix	ISO27001/PCI-DSS/SOC1/SOC2
Toronto, Canada	Equinix	ISO27001/HIPAA/FISMA/PCI/SOC1/SOC2
Vancouver, BC	Cologix	PCI/SOC1/SCO2/HIPAA
Warsaw, Poland	EdgeConneX	ISO27001/ISO9001/PCI-DSS

Global Threat Intelligence Data Warehouse Centers

Location	Data Center	Security Assurance
US: California, Texas, Virginia	Equinix (co-location facility)	CA facility has SOC 2 Type II, ISO 27001 and SSAE16 SOC 1 Type 1 TX facility has NIST 800- 53/FISMA, ISO 27001, SOC 1 Type II, SOC 2 Type II, PCI DSS and HIPPA VA facility has NIST 800- 53/FISMA, ISO 27001, SOC 1 Type II, SOC 2 Type II, PCI DSS and HIPPA.
US:	AWS	AWS offers robust controls to maintain security and data protection. Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC reports provide additional details on the specific control activities executed by AWS. More details can be found at: https://aws.amazon.com/compliance/ and https://aws.amazon.com/security/.
US	Vazata (co-location facility)	SSAE 18 SOC I Type 2

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

- Binding Corporate Rules
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- EU Standard Contractual Clauses

4. Access Control

Personal Data Category	Who has access	Purpose of the access
Registration Information	Customer	Security administration and operations
	Cisco	Creating an account and validating license entitlements and general product support and operations.
Service Logs Data	Customer	Security administration and operations
	Cisco	Global threat intelligence research
Sender Domain Reputation Data	Customer	Security administration and operations
	Cisco	Global threat intelligence research
Sender IP Reputation Data	Customer	Security administration and operations
	Cisco	Global threat intelligence research
URL Reputation Data	Customer	Security administration and operations
	Cisco	Global threat intelligence research
Email Sample Data	Customer	Security administration and operations
	Cisco	ESA technical support; global threat intelligence research for false positive/false negative diagnosis and resolution
File Attachment Data	Customer	Security administration and operations
	Cisco	ESA technical support; global threat intelligence research to correct erroneous blocking/detection of the files as malicious
IPAS Data	Customer Cisco	Security administration and operations Security administration and operations Global threat intelligence research

5. Data Portability

Not applicable based on the data sent to Cisco.

6. Data Deletion & Retention

Customer may request a deletion of specific personal data at any time by emailing privacy@cisco.com or by opening a support request with Cisco TAC. For the purposes of this Table, "GTIR" means "global threat intelligence research."

Personal Data Category	Retention Period	Reason for Retention
Registration Information	• Data will be deleted upon customer request	Product registration and enablement, product use notifications, training and support.
Service Logs	• Equinix, AWS GTIR Cloud: Data will be deleted upon request • Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	Global threat intelligence research
Sender Domain Reputation Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request • Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	Global threat intelligence research
Sender IP Reputation Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request • Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	Global threat intelligence research
URL Reputation Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request	Global threat intelligence research

	• Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	
Email Sample Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request • Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	Global threat intelligence research for false positive/false negative diagnosis and resolution
File Attachment Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious
IPAS Data	• Equinix, AWS GTIR Cloud: Data will be deleted upon request • Vazata GTIR Cloud: Four (4) months; automatically deleted after 4 months	Global threat intelligence research

7. Personal Data Security

Personal Data Category	Type of Encryption
Registration Information	Encrypted in transit and at rest.
Service Logs	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
Sender IP Reputation Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
Sender Domian Reputation Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
URL Reputation Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
Email Sample Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
File Attachment Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.
IPAS Data	In transit: Data is SSL encrypted. At rest: Data at rest is stored unencrypted with strict access controls.

8. Third Party Service Providers (Sub-processors)

Cisco partners with service providers who 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	• Service Logs • Sender Domain Reputation • Sender IP Reputation Data • URL Reputation Data • Email Sample Data • IPAS Data	With respect to data collected by Talos via ESA, Talos leverages AWS cloud technology to assist in providing its global threat intelligence capabilities.	United States
Vade Secure	• Email Sample Data	Global threat intelligence research for false positive/false negative diagnosis and resolution	France
Sophos	• File Attachment Data	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious	United Kingdom
McAfee	• File Attrachment Data	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious	United States
BitDefender	• File Attachment Data	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious	Ireland Romania
Reversing Labs	• File Attachment Data	Global threat intelligence research to correct erroneous blocking/detection of the files as malicious	Croatia

Google Translate	• Email Sample Data[10]	Translation services to assist with global threat intelligence research for false positive/false negative diagnosis and resolution	https://cloud.google.com/compute/docs/regions-zones#locations

9. Information Security Incident Management

Breach and Incident Notification Processes
The Data Protection & Privacy 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.

10. Certifications and Compliance with Privacy Laws

The Security and 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. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world. Cisco leverages privacy transfer mechanisms related to the lawful use of data across jurisdictions. *See Section 3, above.*

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

11. General Information and GDPR FAQ

For more general information and FAQs related to Cisco's Security Compliance Program and Cisco's GDPR readiness 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, please see https://www.cisco.com/c/en/us/about/trust-center/solutions-privacy-data-sheets.html.

[10] Manual process whereby Cisco only shares that portion of the email body text for translation. Cisco does not share entire emails, headers or attachments with Google Translate.