Cisco Secure Email Cloud Gateway (formerly, "Cisco Cloud Email Security" or "CES")

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Secure Email Cloud Gateway (the "Service").

Secure Email Cloud Gateway is a cloud-based email 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 the Service 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 Secure Email Cloud Gateway in order to provide its functionality.

1. Overview

Secure Email Cloud Gateway is a cloud-based email security service that blocks spam and security threats from the internet and, depending on the features licensed, prevents the accidental or intentional leakage of customer data. Secure Email Cloud Gateway offers inbound protection and outbound control of email traffic. The following feature functionalities are available as part of the Service 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 Service
- Data Loss Prevention

The Service automatically enables the use of Cisco Secure Email and Web Manager which enables reporting, tracking and quarantine features. Cisco's processing of data for these Cisco Secure Email and Web Manager features is within the scope documented in this privacy data sheet.

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

2. Personal Data Processing

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

Personal Data Category	Type of Personal Data	Purpose of Processing
Registration Information	• Customer Name • Email address • Phone number • Billing address • Smart Account Usernames/IDs	• Product administration: Creating an account, validating license entitlements, general product support and administration
Admin Information	• Admin Information (e.g., name, email)	• Provide the Service • Allow Customer to access admin interface, set configurations, operate the Service

Email Information	• Sender Information (name, email, display name) • Recipient Information (name, email, display name) • Email Subject • Reply-to Headers (including CC/BCC) • Title of Attachment (but not the content of the Attachment) • IP Address	• Provide the Service
Email Body	• Email content and/or entire Attachment	• Provide the Service (e.g., evaluate email for threats and apply any customer created policies)
IP Address	• IP Address of users accessing the Service's admin portal	• IP Addresses are stored for security purposes as part of an audit log to identify IP addresses trying to access Customer's Cisco Secure Email Cloud Gateway instance, as well as for global threat intelligence research
Service Logs Data (Optional)	• Global Unique ID (GUID) for email message • IP address • Secure Malware Analytics disposition (e.g., malicious, neutral, unknown) • Message metadata (e.g., date, sender, recipient) • Filename[1]	• Global threat intelligence research (only processed if Customer has not disabled Service Logs).
Sender Domain Reputation Data (Optional)	• GUID for email message • Message ID • Email sender IP address • SMTP envelope fields (e.g., sender email addresses) • Display Name • List-Unsubscribe headers • Message ID header • SPF Result • DKIM Result • DMARC Result • Header data (e.g., marketing header, List-Unsubscribe header, reply-to header domain) • Fully qualified domain name	• Global threat intelligence research. Only processed if Customer enables the "Additional Attributes" feature of Sender Domain Reputation and also chooses to send the full email address.
Sender IP Reputation Data (Optional)	• IP address of the sending email server • GUID for connection (sender IP address)	• Global threat intelligence research. Only processed if Customer has not disabled Sender IP Reputation.
URL Reputation Data (Optional)	• GUID for email message • Sender IP address • URL in the email being queried	• Global threat intelligence research (only processed if customer has enabled URL Reputation). • Used to develop and deploy URL exploit detection models.

[1] Only processed if Customer has enabled IronPort Anti-Spam.

Email Submission Data (Optional)	• Email Envelope Header • Email Data Header • Email Body (email body and/or attachment)	• If Customer chooses to send false positive/false negative email samples to Cisco TAC, TAC may share with appropriate Cisco product teams and the third party subprocessors listed below for further analysis. • Global threat intelligence research and machine learning. • Technical Support
Submitted Attachment Data (Optional)	• Any personal data that may be contained in the files	• If Customer chooses to send erroneously blocked file attachments to Cisco TAC, TAC may share with Threat Intelligence teams and the third party subprocessors listed below for further analysis. • Technical support • Global threat intelligence research
IronPort Anti-Spam Engine (IPAS) Data (Optional)	• GUID for email message • Filename to the extent it includes personal data • IPAS results (spam score, rule hits, sender IP address)	• Global threat intelligence research (only processed if Customer has enabled IronPort Anti-Spam).
Email Metadata for Integration with Cisco Secure Email Phishing Defense (Optional)	• Email Envelope Header (Sender, Recipient, Host/IP address) • Email Data Header (From, To, Subject, Reply-to Headers)	• Enable integration between Cisco Secure Email Gateway and Cisco Advanced Phishing Protection. For more information see the Advanced Phising Protection Privacy Data Sheet. • Only proessed if Cisco Secure Email Gateway and Secure Email Phishing Defense has been integrated by Customer.

Secure Email Cloud Gateway collects "Systems Information" to assist Cisco with understanding product usage and enabling product improvements. For more information, see the Systems Information brief. Customers can opt-out of sending Systems Information to Cisco Customer Success. Similarly, non-personally identifiable Systems Information is transferred to Google Analytics to assist Cisco with product usage analysis and continuous product improvement. Customers may opt-out of sending such non-personally identifiable Systems Information to Google Analytics. For more information on the collection and use of Systems Information, please see https://www.cisco.com/c/en/us/about/trust-center/systems-information.html.

Cisco and Third Party Integrations

Secure Email Cloud Gateway integrates with various Cisco products. Please see the applicable Privacy Data Sheet for details regarding processing of personal data by the Cisco product receiving personal data from the Service. The Secure Email Cloud Gateway subscription includes the right to access and use SecureX threat response. For more information regarding the processing of personal data by Cisco Threat Response, please refer to the Cisco SecureX threat response Privacy Data Sheet. If you utilize the Threat Defense Connector with the Service, a copy of the customer email, including any attachments (referenced as "Journaled Email Data") is processed by Cisco as set forth in the Cisco Secure Email Threat Defense Privacy Data Sheet.

In addition, Secure Email Cloud Gateway 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.

TAC

If a customer contacts the Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service and from the Customer, and may share such data with appropriate Cisco product teams as set forth herein. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

Smart Licensing

Secure Email Gateway 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.

3. Data Center Locations

Cisco uses its own data centers as well as third-party infrastructure providers to deliver the Service globally. Secure Email Cloud Gateway uses the following regional infrastructure providers. The Admin Information, Email Information, Email Body and IP Address will be stored in the region where Customer chooses to provision its Service. Registration Information will be stored in the United States.

Secure Email Cloud Gateway Data Center Locations

Data Center	Description	Location of Data Center
Equinix (co-location facilities)	The infrastructure for the Cisco Secure Email Cloud Gateway cloud runs on Equinix co-location facilities in North America, the EU and APJC	United States Canada United Kingdom Netherlands Germany Japan
Q9	The infrastructure for the Cisco Secure Email Cloud Gatewaycloud runs on Q9 co-location facilities in Canada	Canada
Getronics/KPN	The infrastructure for the Cisco Secure Email Cloud Gateway cloud runs on Getronics/KPN co-locations factilites in the Netherlands	Netherlands
NextDC	The infrastructure for the Cisco Secure Email Cloud Gateway cloud runs on NextDC co-location facilities in Australia	Australia
Switch	The infrastructure for the Cisco Secure Email Cloud Gateway cloud runs on Switch co-location facilities in the United States	United States

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 U.S. data centers described below and use the subprocessors in the locations set forth in Section 9 below. This is necessary for the delivery of Secure Email Cloud Gateway, as threat intelligence analytics requires the examination of worldwide data in real time.

Global Threat Intelligence Data Warehouse Center Locations

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, intrustion 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/soc-faqs/

With respect to data collected 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 Secure Email Cloud Gateway deployment. The data sent to the Global Co-location Data Center Network is transient in nature, and is not stored in those locations. This is necessary for the delivery of Secure Email Cloud Gateway , as threat intelligence analytics requires the examination of worldwide data in real time.

Global Co-location Data Center Network Locations

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
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

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
- EU-U.S. Data Privacy Framework and the U.K. Extension to the EU-U.S. Data Privacy Framework
- Swiss-U.S. Data Privacy Framework

5. Access Control

The table below lists the personal data used by Secure Email Cloud Gateway 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	Administration and operations
	Cisco	Creating an account and validating license entitlements and general product support and operations
Admin Information	Customer	Administration and operations
	Cicso	Provide the Service; support the Service
Email Information	Customer	Administration and operation
	Cisco	Providing security analytics and forensics for product usage
Email Body	Customer	Administration and operations
	Cisco	Provide the Service
IP Address	Customer	Administration and operations
	Cisco	Security monitoring, maintain audit logs, and global threat intelligence research
Service Logs Data	Customer	Administration and operations
	Cisco	Global threat intelligence research
Sender Domain Reputation Data (Optional)	Customer	Administration and operations
	Cisco	Global threat intelligence research
Sender IP Reputation Data (Optional)	Customer	Administration and operations
	Cisco	Global threat intelligence research
URL Reputation Data (Optional)	Customer	Administration and operations
	Cisco	Global threat intelligence research
Email Submission Data (Optional)	Customer	Administration and operations

	Cisco	Technical support; global threat intelligence research and machine learning
Submitted Attachment Data (Optional)	Customer	Administration and operations
	Cisco	Technical support; global threat intelligence research
IronPort Anti-Spam Engine (IPAS) Data (Optional)	Customer	Administration and operations
	Cisco	Global threat intelligence research
Email Metadata for Integration with Cisco Secure Email Phishing Defense (Optional)	Customer	Administration and Operations
	Cisco	Enable the integration

6. Data Portability

Customer has the ability to export data from the Service via its reporting capabilities.

7. Data Deletion and Retention

The table below lists the personal data used by Secure Email Cloud Gateway, 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	• Data will be deleted upon customer request	• Product registration and enablement, product use notifications, training and support
Admin Information	• Admin Information will be deleted upon customer request • 14 days after account is terminated or decommissioned	• Provide customer admin interface; provide the Service
Email Information	• As configured by Customer in quarantice policy (default configuration is 14 days)[2] • 14 days after account is terminated or decommissioned • For the Message Tracking and Reporting features, the retention period depends on customer's disk storage availability	• Providing security analytics and forensics for product usage
Email Body (only if the customer enables the Quarantine feature)	• As configured by Customer in quarantice policy (default configuration is 14 days) • At least 14 days if customer licenses the Data Loss Prevention (DLP) feature and "Matched Content Logging" is enabled. Message Tracking will store that portion of the Email Body that matched the customer created "Matched Content Logging" criteria for a DLP violation.	• Providing security analytics and forensics for product usage for customer review (Cisco does not review)

[2] Pre-defined Quarantine features may be disabled by customer. However, disabling these features may limit the functionality and security provided by Secure Email Cloud Gateway. Please see the Secure Email Cloud Gateway product documentation for more information.

	• 14 days after account is terminated or decommissioned	
IP Address	• 14 days • For IP Addresses contained within the Message Tracking and Reporting features, the retention period depends on customer's email volume and disk storage availability • 14 days after account is terminated or decommissioned	• Security Monitoring
Service Logs Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research
Sender Domain Reputation Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research
Sender IP Reputation Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research
URL Reputation Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research
Email Submission Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research for false positive/false negative diagnosis and resolution; machine learning.
Submitted Attachment Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research to correct erroneous blocking/detection of the files as malicious.
IronPort Anti-Spam Engine (IPAS) Data (Optional)	• Data will be deleted upon request	• Global threat intelligence research
Email Metadata for Integration with Cisco Secure Email Phishing Defense (Optional)	• Data will be deleted upon request	• Global threat intelligence research.

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.

A note on Cisco Talos: Talos is Cisco's trusted global threat intelligence research team. In order to continually secure Cisco's Security portfolio, certain Security products share data with Talos, which Talos then processes for global threat intelligence research purposes. All data transferred to Talos from Cisco Security products is encrypted in transit.

Personal Data Category	Security controls and measures
Registration Information	• Data encrypted in transit and at rest
Admin Information	• Data encrypted in transit and at rest
Email Information	• Data encrypted in transit and at rest

Email Body	• Data encrypted in transit and at rest
IP Address	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Service Logs Data (Optional)	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Sender Domain Reputation Data (Optional)	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Sender IP Reputation Data (Optional)	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
URL Reputation Data (Optional)	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Email Submission Data	• Data is Encrypted in transit and at rest
Submitted Attachment Data (Optional)	• Data is Encrypted in transit and at rest
IronPort Anti-Spam Engine (IPAS) Data (Optional)	• In transit: Data is SSL encrypted • At rest: Data at rest is stored unencrypted with strict access controls
Email Metadata for Integration with Cisco Secure Email Phishing Defense (Optional)	• Encrypted in transit. For further encryption details, please see the Advanced Phising Protection Privacy Data Sheet.

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
Vade Secure	• Email Sample Data	Global threat intelligence research	France
Sophos	• File Attachment Data	Global threat intelligence research	United Kingdom
McAfee	• File Attachment Data	Global threat intelligence research	United States
BitDefender	• File Attachment Data	Global threat intelligence research	Ireland Romania
Reversing Labs	• File Attachment Data	Global threat intelligence research	Croatia
Google Cloud Translate		Translation services to assist with global threat intelligence research	United States

	• Emal Sample Data[3]		

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 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. 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.

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 redirect to their employer for a response.

[3] When analyzing Email Sample Data, Cisco may manually share a necessary portion of the email body text with Google Cloud Translate for the sole purpose of translation through the Google Cloud Translate API. Such text is retained by Google Cloud Translate for only enough time to perform the translation and then it is deleted.

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.