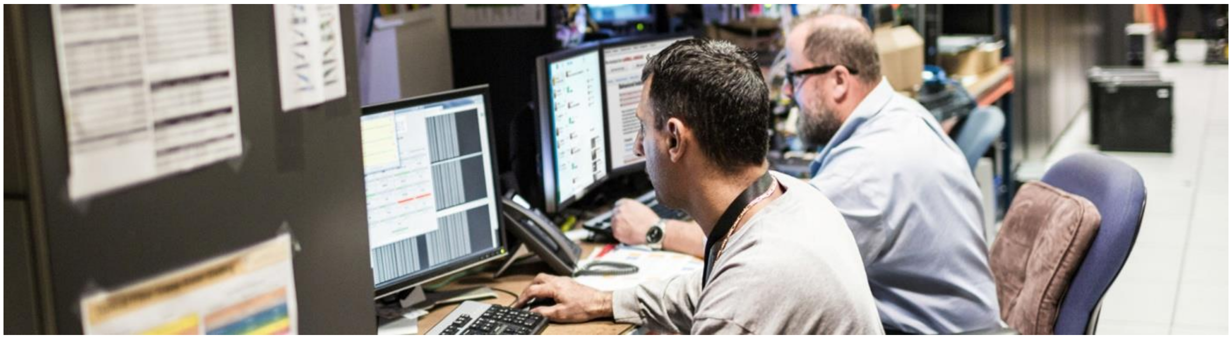

Cisco Cloud Web Security and Data Privacy

As part of our commitment to protecting the confidentiality and safety of our customer data, Cisco® Cloud Web Security (CWS) enforces a stringent privacy and security policy.

Access to private and confidential data on our systems is limited to those employees with a specific need to retrieve this information. Cisco CWS uses a number of computer security safeguards to protect its databases and servers against the risk of loss, unauthorized access, destruction, misuse, modification, or the inadvertent or improper disclosure of data.

- Customer web requests are stored on a separate database and server that can be accessed by a limited number of Cisco CWS employees on a need-to-know basis, with logging. Cisco CWS otherwise accesses data only for threat and statistical purposes and only on an anonymized basis. We segregate any personally identifiable information provided by customers.
- Cisco CWS operates on a multitenant architecture. Customers can access only their own data based on hierarchical access control through Cisco ScanCenter with a user-defined password that meets strict password requirements. Customer data is logically separated to prevent any accidental overlap.
- All data saved for reporting purposes is stored in a dedicated data warehouse located in London, England. Blocked traffic data is retained one year, and allowed traffic data is retained 45 days. The retention of allowed traffic data can be extended to one year at additional cost.

Physical Security

Cisco CWS uses high-security facilities with biometric access control and authorized access approval. Only a small number of trusted dedicated hands are allowed access and control of hardware and inventory globally.

Data Security

A dedicated data team manages and supports the data associated with our customers. Data is replicated locally and off site in separate data centers for disaster recovery purposes. Any sensitive data such as user passwords or private keys is encrypted both in transfer and storage. Nonsensitive data is not encrypted when it is stored; it is encrypted only during transfer.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Logical Security

The dedicated operations team is sandboxed from corporate networks for administration of the service. The use of best-practice procedures and tools following ITIL® workflows helps ensure highly secure access to systems.

Centralized auditing and monitoring solutions are in place to help ensure protection and delivery of the service.

Network Security

Cisco CWS uses Cisco firewall products to protect every point of entry. CWS also uses other host-based protection measures and auditing tools. Furthermore, Cisco CWS uses multiple upstream providers for network connectivity with DDoS-mitigation tools. Full access and traffic monitoring helps ensure the capture and analysis of all potential attacks.

Cisco CWS's Stance with Regard to Privacy Shield

Cisco CWS (ScanSafe) is a wholly owned subsidiary of Cisco Systems Inc. and is covered by Cisco’s Privacy Shield registration.

Is CWS compliant with the Health Insurance Portability and Accountability Act (HIPAA)?

Cisco provides a range of security products that can be used by customers to meet many of the requirements outlined in the HIPAA standards but only if they are properly configured, maintained, and monitored. Deployment of a single product or set of products will not, in and of itself, ensure HIPAA compliance.

Additional details on the HIPAA standard and how Cisco security products comply can be found in this blog post.

Application Security

Customer administration is provided through a highly secure web portal. Each administrative account is accessed by a unique username and password. The entire session is encrypted using SSL.

Anonymizing Users’ Personal Details in Web Logs

In some locations it is necessary for our customers to protect their users' identity within the reporting logs. A customer can configure this functionality through the web filtering policy. The rule with the action Anonymize can be applied globally or to specific groups of users (LDAP, Active Directory, directory, or custom). When the rule is applied, the following actions occur:

- User identity is still read by the tower at the time a web request is processed
- Web filtering policy is applied according to user identity
- Before the tower forwards the transaction details to the data warehouse in the core data center (in London), the following user identity attributes are stripped out:
  - User is replaced with “Undisclosed”
  - Group is replaced with “Undisclosed”
  - Internal IP is replaced with “0.0.0.0”
  - External IP is replaced with “0.0.0.0”

The web filtering policy is still applied normally to anonymized users, but the details of their identity are not retained after the policy has been applied. Reports generated around the transaction details will not contain the specifics of the user’s identity. They will be replaced with the details noted above. The anonymization process happens locally at the cloud proxy at the time of processing, and the data sent back to the core data center is already anonymized. Anonymization is compatible with HTTPS inspection.

User Privacy with HTTPS Traffic

When HTTPS traffic is decrypted for inspection, it is possible to select only specific traffic that will be decrypted. The selection can be based on certain categories or a list of domains. Customers can also list specific hosts and domains that should be excluded from HTTPS inspection. Or they can choose to decrypt only the applications covered by the Application Visibility and Control settings.

Note also that when HTTPS traffic gets inspected, CWS does not log the **Path** and **Query** attributes of the URL. Only the **Host** will be logged. For example, if a user browses to Google and searches for “cisco cloud web security” and presses Enter, the full URL will be: https://www.google.com/?gws_rd=ssl#q=cisco+cloud+web+security

That full URL can be broken down to these three attributes:

- Host: https://www.google.com
- Path: ?gws_rd=ssl# (where on the site the user went to)
- Query: q=cisco+cloud+web+security (what they searched for)

So for privacy reasons CWS will log only the **Host** and not the **Path** or the **Query** for HTTPS traffic that is inspected.

Cisco CWS's Stance with Regard to the U.S. Patriot Act

The U.S. Patriot Act gives certain U.S. law enforcement authorities the power to require U.S. companies and their subsidiaries (which would include all Cisco subsidiaries) to hand over data in their possession. This data would potentially include customer traffic data.

Note also that disclosure can be required under the Patriot Act only (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) “to protect against international terrorism or clandestine intelligence activities.” It cannot be used to investigate ordinary crimes.

Where permitted by law to do so, we will always consult with the customer before releasing any of their data.

Transparency and Law Enforcement Requests for Customer Data

We are committed to publishing information regarding the requests or demands for customer data that we receive from law enforcement and national security agencies around the world. We publish this data twice yearly (covering a reporting period of either January-June or July-December). Like other technology companies, Cisco publishes this data six months after the end of a given reporting period, in compliance with restrictions on the timing of such reports.

Cisco's Principled Approach

CWS follows Cisco’s approach to data privacy. We believe that law enforcement and national security agencies should go directly to our business and government customers to obtain information or data regarding those entities, their employees, and their users.

If a law enforcement or intelligence agency ("government agency," generically) requests customer data from Cisco, we take the following steps to protect our customer's interests:

- We notify the customer that its data has been requested (so that the customer may attempt to limit or prevent disclosure), unless applicable law prohibits notification. Where appropriate, we protect our customer's legitimate interests through the legal process or other means, and we challenge requests that prohibit notification to the customer.

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

- We provide such data only if the government agency has the appropriate authority under applicable law to require Cisco to provide such data. For example, absent a valid warrant or court order, we will not provide any customer data to the U.S. government.
- Where appropriate, we seek to narrow (including moving to formally modify by judicial mandate) any government agency request or demand for customer data to only the specific information required to respond.
- Where compliance with a valid government agency request for customer data would put Cisco in potential breach of applicable data protection and/or privacy-related laws in another country that has jurisdiction or authority over the customer data, we will challenge the request and invoke the mutual assistance mechanisms contained in international law where appropriate.
- We make an exception to these commitments only in emergency cases where we believe that disclosing customer data will prevent imminent death or serious physical harm to an individual. We will notify the customer promptly if such an exception is made (unless applicable law prohibits notification) and will include that disclosure in our semiannual transparency report.

CWS Service Description

For more information, please refer to the CWS Service Description document that includes details such as the applicable service-level agreements (SLAs).

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C22-738633-00 02/17

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.