White Paper

Cisco Cloud Web Security (CWS) and Data Privacy

Cisco CWS enforces a stringent privacy and security policy that outlines its commitment to protecting the confidentiality and safety of our customer data.

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

- Customer web requests are stored on a separate database and server that can be accessed by only a limited number of Cisco CWS employees. Cisco CWS only accesses data for threat and statistical purposes and only on an anonymized basis. Cisco segregates any personally identifiable information provided by customers.
- Cisco Cloud Web Security operates a multi-tenant architecture. Customers can access only their own data based on hierarchical access control via ScanCenter with a user-defined password. 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, UK. Data retention is one year for blocked data, and 45 days for allowed data. Allowed data retention can be extended to one year for a cost.

Physical Security

Cisco CWS utilizes high security facilities with biometric access control, stringent change 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 - the only access to data is through this team. Data is replicated locally and off-site in separate datacenters for DR or replication purposes. Any sensitive data such as user passwords or private keys is encrypted both in transfer and storage. Other non-sensitive data is not encrypted when it is stored; it is encrypted only during transfer.

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 ensures secure access to systems.

Centralized auditing and monitoring solutions ensure protection and delivery of service.

Network Security

Cisco CWS uses Cisco's firewall products to protect every point of entry. CWS also utilizes other host based protection measures and auditing tools. Furthermore, Cisco CWS utilizes multiple upstream providers for network connectivity with DDOS mitigation tools. Full access and traffic monitoring ensures capture and analysis of all potential attacks against the borders.

Cisco CWS's Stance with Regards to Safe Harbor

CWS (ScanSafe) is a wholly-owned subsidiary of Cisco Systems, Inc. and is covered by Cisco's Safe Harbor certification.

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 properly configured, maintained, and monitored. Deployment of a single product or set of products will not, in and of themselves, ensure HIPAA compliance.

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

Application Security

Customer administration is provided via a secure web portal. Each administrative account is accessed via a unique username/password and the entire session is encrypted using SSL.

Anonymizing users' personal details in web logs

In some locations it is necessary to protect users' identity within the reporting logs. This functionality can be configured through the web filtering policy via a rule with the action of Anonymize, and can be applied globally, or to specific groups of users (LDAP/AD/directory or custom). When 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.
- Prior to the tower forwarding the transaction details to the data warehouse in the Core DC (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 policy has been applied. Reports generated around the transaction details will not contain the specifics of the user’s identity, but will be replaced with the details noted above. The anonymization process happens locally at the tower at time of processing and the data sent back to the Core DC is already anonymized. If the anonymization process is activated after previously not being in use, any previously processed logs will remain with full details and will not get anonymized, and likewise, anonymization is final so if it is later removed, any anonymized logs already in the data warehouse will remain anonymized (i.e. Cisco CWS does not change any logs once they have been processed in the data warehouse). Anonymization is compatible with HTTPS Inspection.

User privacy with HTTPS traffic

When inspecting HTTPS traffic it is possible to select only the specific traffic that should get decrypted for inspection. This can be based on certain categories or a list of domains. Users can also list specific hosts and domains that should be excluded from HTTPS inspection, or choose to decrypt only applications covered in the list of AVC applications for decryption.

Note also that when HTTPS traffic gets scanned 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 hits 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 the user searched for)

For privacy reasons CWS will log only the Host and not the Path nor the Query for HTTPS traffic that is inspected.

Cisco CWS Stance on the US "Patriot" Act

The US ‘Patriot’ Act gives certain US law enforcement authorities the power to require US companies and their subsidiaries (which would include all Cisco CWS subsidiaries) to hand over data in their possession, which would potentially include any customer traffic data.

Note also that disclosure can only be required under the Patriot Act (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, or even domestic terrorism.

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

Transparency and Law Enforcement Requests for Customer Data

Cisco is committed to publishing data regarding requests or demands for customer data that we receive from law enforcement and national security agencies around the world. We will publish this data twice yearly (covering a reporting period of either January-June or July-December). Like other technology companies, we will publish 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, whereby Cisco believes 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 users.

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

- Cisco will 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 and in order to protect its customer's legitimate interests, Cisco will, through appropriate legal process or other means, challenge requests that prohibit notification to the customer.
- Cisco will only provide such data if the government agency has 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 US Government.
- Where appropriate, Cisco will 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, Cisco will challenge such request and invoke the mutual assistance mechanisms contained in international law where appropriate.
- Cisco will only make an exception to these commitments in emergency cases where we believe 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, and will include that disclosure in our semiannual transparency report.

http://www.cisco.com/web/about/doing_business/trust-center/transparency-report.html

CWS Service Description

For more information, please refer to the CWS Service Description document that includes details such as a SLA.

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.**

Printed in USA