White Paper

Cisco Cloud Web Security (CWS) Data Center Standards

Cisco® Cloud Web Security (CWS) takes standards and procedures very seriously as a Security-as-a-Service provider. In the data center and networking industries, although certain Service Provider and Accreditation standards do exist, there is no central governing body regulating data center standards and procedures for cloud services. In many ways, providers define their own best practices. Cisco CWS data centers provide best in class cloud delivered security, with best in class infrastructure security and integrity, strict standards, true multi-tenant service, high resiliency and scalability.

Service Provider Accreditation and Best Practice

As mentioned, although there is no central governing body, all of Cisco CWS partners are accredited or follow best practices as defined by various bodies in relation to their standards and procedures. These include, but are not limited to:

- SSAE16 SOC-1 Type II / SOC-2 Type II
- ISO 27001
- ISO 9001
- ISO 20000

Cisco CWS European Datacenter providers are ISO27001:2005 Security Management certified (Germany IDW PS 951 certified), which ensures the proper selection of adequate and proportionate security controls to protect all information assets in Datacenters.

Service-Providing Infrastructure Standards and Procedures

Cisco CWS maintains the following standards and undertakes the following procedures in relation to the infrastructure that provides its services:

- Stress testing of all production design prior to deployment
- Dual redundant power supplies on all applicable equipment to assist maximum uptime
- Redundant ISP circuits with diverse POP as a minimum. In most cases, completely redundant ISP with diverse entry to the DC
- RAID 1 or RAID 5 storage volumes to assist data integrity and maximum uptime
- All network capability is built in a 2N architecture for full redundancy
- A combination of 4hr response parts replacement and local spares pooling to aid maximum uptime
- BIOS level deletion of degraded/failed disks prior to replacement to assist data protection and security
- Continuous monitoring of all components, sub-components, and internal/external/front-end/back-end applications to assist infrastructure and service integrity

Infrastructure and Redundant Power

Cisco CWS Datacenters providers have a global average uptime of >99.999%. That means each of the Cisco CWS Datacenters typically experiences outages totalling less than 5 minutes and 15 seconds over the course of a year.

To ensure power is always available, Cisco CWS Datacenter providers have a minimum of N+1 power redundancy, meaning every mission-critical component has at least one backup power feed fed by UPS and with generator backup. Each Datacenter location also stores fuel on site to provide emergency power in the event of an ongoing power outage, and contractual agreements exist with fuel suppliers to ensure long term continuous operation.

Network Security

The network is protected by a number of layers:

- Use of leading firewalls to protect every point of entry + other host based protection measures/auditing tools. This includes Cisco's Next Generation Unified Fabric Datacenter and Campus Core hardware, such as:
    - ASA5585-X firewalls
    - ASR9000 series routers
    - Nexus 7000 and 5000 series switches
    - UCS
- Utilization of multiple upstream providers for network connectivity
- Full access/traffic monitoring to ensure capture and analysis of all potential attacks against the borders

In addition, CWS proxies will reject any web requests that do not include a valid license key from a current customer, or originate from non-recognized sources.

Physical Security

Access to the buildings, data floors and individual areas is monitored by 24/7 security. Personnel access each of the Cisco CWS Datacenter facilities by using a combination of biometrics and passcode security required at both building entry and the DC floor. Standardized procedures also ensure that only nominated staff gains access to our equipment whenever required, day or night.

Entry to each facility is tightly controlled, with strict procedures in place to monitor and control visitor access both into and within the Datacenter. Extensive CCTV video camera surveillance is in place across each facility, along with security breach alarms, biometric checks and controlled physical barriers.

Minimum Datacenter Facility Standards

For a datacenter facility to be considered as a location to host Cisco CWS equipment, the following is required:

- Locked cages or cabinets
- Onsite physical security provided by one or more of the following:
  - Onsite security guard patrols
  - Strategically positioned cameras
  - Biometric/RFID access controls to critical areas
  - Alarms to alert against unauthorized intrusions
- Uninterrupted power source through one or more of the following:
  - Physically diverse power feeds
  - Diverse power utility companies
  - Battery-powered uninterruptible power supplies
  - Onsite generator with re-fuelling agreement to maintain power until resumption of normal utility service
  - Testing of backup power sources on full-load at least once a year
- Sufficient HVAC capabilities with monitored temperature and humidity controls
- The presence of fire and smoke suppression systems that are regularly maintained
- 24x7x365 audited physical access to the facility for authorized Cisco CWS staff only
- 24x7x365 remote hands and eyes by experienced engineers responding to requests from authorized Cisco CWS staff only

Minimum Network Service Standards

For a network service to be considered suitable for access to Cisco CWS, the following is required:

- 24x7x365 monitoring of site's network infrastructure and alerting of authorized Cisco CWS staff in the event of major service disruptions
- 24x7x365 customer service desk with to respond to incidents and service requests raised by authorized Cisco CWS staff only
- Minimum of 99.9% network uptime service level agreement on the part of the network service
- Consistent low-latency traffic within country/region
- Diverse network feeds into the data center site

Energy efficient

Cisco CWS takes cooling very seriously in its Datacenters and uses a combination of water-based, fully-redundant air conditioning. In addition hot aisles/cold aisle designs and innovate containment solutions are used for the best cooling. Energy efficiency has been at the forefront of the design and build of Cisco CWS Datacenters. Many Cisco CWS Datacenters benefit from free cooling systems which enable significant savings when the external ambient temperatures fall below a certain level.

For More Information

For more information, please refer to the CWS Service Description document and the CWS Privacy document.

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.**