Cisco CloudCenter Suite Trust Center

The sections below are provided for informational purposes only. For details, please review the Offer Description and Privacy Data Sheet.

Operations

Global Infrastructure	We deliver a highly available, scalable service designed to meet our customers' needs for performance and data residency via regional deployments. Our infrastructure is comprised of encrypted backups and warm sites at physically separate disaster recovery sites.
High-Availability Architecture	We employ multiple layers of redundancy to ensure the SaaS platform is highly available.
Disaster Recovery	Our built-in processes and workflows back up data for fast recovery times in the unlikely event of a local outage. We maintain comprehensive Disaster Recovery sites in North America and Europe and, as we expand to new geographic regions, additional DR sites will also be deployed. Our processes are designed to focus on the shortest path to resolution for all production issues.
Scalable Architecture	To support the rapid evolution of our service and provide you with the best experience possible, we use Infrastructure as a Code (IaC). Our SaaS architecture is built to scale to ensure that you have the access and capabilities you need to manage your hybrid cloud workloads.
Service Uptime	We stand behind our service level agreements guaranteeing uptime. To provide transparency, we publish uptime figures on http://status.cloudcenter.cisco.com/. We fully assess the impact of maintenance prior to scheduling and announcing maintenances to our customers. Please note that in some cases, scheduled maintenances may have a minimal impact to our platform availability which are excluded from our service uptime calculations presented on status.cloudcenter.cisco.com or the service level agreement uptime.
Proactive Monitoring & Alerting	Our Cloudcenter Suite SaaS platform offers infrastructure redundancy, proactive monitoring, remote availability monitoring, monitoring of all services and periodic synthetic monitoring to ensure that services are not only available but also fully functional.
Upgrades and Maintenance	In the event potentially impactful updates are to be applied to the deployed services, our Cloud Operations team will generate a notification of the schedule and details on expected customer experience during the maintenance. All platform maintenances are applied within a change control window and historical and real-time platform updates can be viewed via: http://status.cloudcenter.cisco.com/.
Follow-the-Sun Support	Our experienced Cloud Operations team is available 24x7 to deliver superior customer service across any geographic region, in respective time zones, following the sun. To open a ticket regarding the CloudCenter Suite SaaS platform, contact Technical Assistance Center (TAC).

Compliance & Privacy

Personnel Controls	All employees are required to undergo annual security training and must comply with Cisco's Global Personal Data Protection and Privacy Policy and binding corporate rules.
Privacy Policy and GDPR	The CloudCenter Suite SaaS platform is a highly-available, scalable service designed to meet your needs for performance and data residency. CloudCenter Suite SaaS is available in North America and Europe. Our privacy policy reflects our commitment to protecting personal data. It provides details on the type of personal information we collect, how we store it, how we use it, and what rights individuals have and how to exercise them. CloudCenter Suite SaaS is GDPR-Ready. Read our Privacy Data Sheet.
Third Party Vendors	Our team performs due diligence reviews of all third parties that support the delivery and availability of our products and services in keeping with Cisco best practices and standards. Prior to engaging any third party that accesses production infrastructure or processes customer data, our team performs due diligence reviews of each third party's information security program, privacy practices, confidentiality commitments and puts appropriate contractual terms in place to ensure that the processing will meet the high standards required by our team, and applicable laws.
Compliance	We are targeting ISO 27001 certification in early 2020, having undergone audits with minimal findings in calendar year 2019. We are evaluating SOC2 as a potential roadmap item.

Security

Architectural and Technical Controls	Our team leverages an array of layered operational and architectural controls designed to further secure our customer environments.
Continuous Monitoring	Our security operations team is responsible for continuously monitoring the day-to-day security of the SaaS solution. From endpoints to networks, cross-functional teams are continuously observing the operational environments for anomalous events, behaviors, and malware. As threats emerge, the focus shifts to investigating suspicious alerts, events, and incidents. We are vigilant about keeping your data and systems secure.
Secure Development Lifecycle	We have established a secure-by-design approach by working closely with our developers, product managers, and operations engineers early on to embed security and privacy into software development processes. We follow the Cisco defined development standard called the Cisco Secure Development Lifecycle (CSDL). This process is designed to ensure that we produce secure and resilient products by identifying and implementing specific processes or tools to enable engineers to detect, fix, mitigate and prevent design and code weaknesses that could become exploitable.
Security Automation	We follow a "DevSecOps" model that enables us to develop security automation that scales directly alongside our deployment methods so that we can ensure security standardization and architectural strength at scale.
Vulnerability Management	Our vulnerability management process seeks to continuously identify and remediate vulnerabilities in our infrastructure and our software. This is accomplished through regular inspection of our code and monitoring of our infrastructure for vulnerabilities using a variety of automated and manual methods to keep abreast of any changing conditions.

Authentication and Access Controls	We offer native standards-based integration with identity providers, and role-based access controls that allow our customers to restrict access to specific software features, data, and analytics queries. Our Cisco platform administrators also follow role-based access controls for the infrastructure and maintain the required software access controls per Cisco internal policy.
Encryption	Our team ensures the confidentiality and integrity of data for our SaaS environment while it is en route to our platform or stored there. For data in transit and rest, all traffic is encrypted via TLS, and all communication over public and non-CloudCenter Suite controlled networks is encrypted via SSL/TLS. All customer-identifiable and personally-identifiable data, including backups is encrypted at the system and storage levels.
Logging and Audit Controls	Our Cloud Operations and TAC teams have access to SaaS infrastructure and application log data. We provide limited assistance with audit requests. All log data is encrypted at rest and during transit.

Report a Security Issue Here

The CloudCenter Suite Operations team is committed to providing strong levels of security assurance for our customers, our partners, and our community. While we continually work hard to prevent and remove vulnerabilities from our software, there always remains the possibility of their existence. If you believe you have discovered a vulnerability in our product, services, websites or other infrastructure, or to report a suspected abuse issue, please contact our Technical Assistance Center.

Upon receipt of your inquiry, our security team will triage and respond to your request. We ask for your cooperation on any disclosure surrounding the issue and working responsibly with us toward a common goal of protecting our customers.

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 **https://www.cisco.com/go/offices**.