ORACLE SERVICE CLOUD

SECURITY OVERVIEW

PROVIDING UBIQUITOUS CONNECTIVITY, RELIABILITY AND SCALE ON SECURE AND RELIABLE CLOUD SERVICE

KEY FEATURES

- Physical security and best-in-class facilities
- Redundant power and network
- Disaster Recovery
- 24/7 environmental monitoring and alerting
- Security accreditations necessary for most organizations, governments, and industries
- Code review and third-party vulnerability assessment
- Resilient architecture with no single points of failure

KEY BENEFITS

- Peace of mind for mission-critical application services
- Delivery you can rely on
- Validated in the most demanding environments
- Provide a reliable, secure, and scalable cloud environment for all customer transactions
- Security policies that align with industry best practices

Oracle understands that the confidentiality, integrity, and availability of your information are vital to your business operations. That's where Oracle Service Cloud excels. You must have trust and confidence in your service provider, and Oracle takes this commitment seriously. Security is embedded in Oracle's "DNA"- within the product, the development cycle, and Cloud Operations practices – to ensure your information remains your information.

Physical Security

Full-time, 24/7 local operations and security staff ensure that only authorized individuals have the ability to access the data center. All data center access doors, including shipping and parking areas, are monitored and video recorded. All data center access is secured by access cards, biometric devices (hand scanners), man-traps, portals, or a combination thereof. Exterior walls, doors, and windows are taken into careful design considering the environment and are generally constructed according to the requirements to protect from natural hazards such as lightening and wind.

Server and network equipment is physically secured within locked cages/suites inside the data center. The listing of employees and cages are updated promptly to ensure access is limited to authorized personnel. Each data center provides centralized security operations and monitoring on a 24/7 basis, including prompt response to actual or suspected physical security incidents. In additional to administering and monitoring access to the data center, the operations and security teams monitor and enforce other security policies and environmental sensors and alarms. All security and environmental systems are supported by redundant power, uninterruptible power supply (UPS) devices, and stand-by generators.

Logical Security

Oracle Service Cloud requires management authorization for employee access to any critical applications and systems, and additional approval levels are required for all Cloud Services access. Access is granted according to a user's role and business need. Logical and physical access is immediately revoked from employees who have resigned or are terminated. Oracle Cloud Service continuously monitors logs, and audits system and network activities, including access or attempted access to customer data. This includes monitoring and auditing of systems for unauthorized or inappropriate access to customer data by Oracle employees.

Data Availability

Oracle Service Cloud is architected with availability, maintainability, scalability, and customer security at the top of the list. Every data center implementation meets or exceeds the following specifications:

- Redundant firewalls
- Redundant F5 load balancers with SSL acceleration

- Redundant web farms
- Multi-processor servers connected by multiple gigabit NICs
- Redundant database disk using real-time replication
- Redundant (failover) database servers
- Tape library for off-site data storage

In addition to the robust computing architecture, each data center supports the Oracle Service Cloud via:

- Dedicated substation on utility grid
- Four or more onsite diesel generators
- Independent rack power sources
- Dual entry network connectivity
- 3+ Internet backbone providers
- Less than 40% peak network utilization
- 99.999% availability of power and cooling

Environmental Controls

All data centers leverage advanced monitoring and reporting systems to monitor environmental controls and alert data center staff to potential or merging issues. Using these systems, the 24/7 staff monitor:

- All power systems, including generators, transfer switches, UPS, diesel generators and their fuel supplies
- Fire detection and suppression systems, and water sensors, as well as a double interlock pre-action and detection system

All data centers are equipped with independent utility sources originating from independent feeders or substations. The incoming services lines are connected to automatic transfer switches, which also connect to redundant standby diesel generators.

All mission-critical systems, including all server and network equipment, heating and cooling equipment, and security systems at the data centers are sourced by redundant UPS systems. All data centers have zoned temperature control systems, with multiple HVAC units at each center to verify correct temperature in critical areas. If temperatures vary outside preset limits, an alarm is generated. The HVAC units are powered by utility and generator systems for redundancy.

Disaster Recovery

Regardless of the quality of any system architecture, infrastructure, or robustness of any individual data center, unexpected situations can occur that potentially may impact Oracle Service Cloud operation, and limit ability to deliver service to customers. Oracle has established a recovery strategy and a detailed recovery plan, including recovery procedures for critical infrastructure components, to allow for a quick recovery of Oracle Service Cloud, with minimal disruptions to the customer's operations.

Each production customer's data is replicated in near real-time to two replication servers within the production data center, as well as to a geographically-remote Disaster Recovery (DR) facility. This creates multiple redundant copies of all customer data to guard against system, local disruptions, and even entire data center failure.

Intrusion Detection and Anti-Virus

Oracle Service Cloud operates an advanced intrusion detection system (IDS) on the internal and customer facing networks to monitor network traffic for unauthorized or suspicious activity. Traffic monitor correlates threats and provides event aggregation across all systems and networks, and sends events to the SIEM. All log summaries are reviewed daily, with certain alerts or events escalated as appropriate, and may invoke the Incident Response Plan.

All files sent to Oracle Cloud Service, regardless of the method used to transmit, are scanned for known attack signatures. Infected files are flagged and not permitted into the service.

Internal and Third-Party Testing and Assessments

New product features are tested prior to code completion to identify features that do not work properly. Security testing is integrated into feature testing and regression testing. Additional security testing is provided in the form of source code scans of modified or added code, and internal audits of the products. Every Oracle Service release is subjected to a third-party application vulnerability assessment prior to release.

Regulatory Compliance

Oracle Service Cloud is designed and certified to meet many of the compliance requirements of the most demanding environments. The security landscape continues to evolve, and you can rely on the Oracle Service Cloud to stay ahead of threats. Note that some compliance offerings are unique to the Oracle Service Cloud, and not all regulatory frameworks listed below are applicable to all available Oracle Service Cloud environments. Also note that other pricing considerations may apply.

PCI DSS Service Provider Level 1 (Payment Card Industry Data Security Standard)

HIPAA (Health Insurance Portability and Accountability Act)

Family Education Rights and Privacy Act

GLBA (Gramm-Leach-Bliley Act)

NIST 800-53 Moderate Control (National Institute of Standards and Technology 800-53)

FISMA (Federal Information Security Management Act)

U.K. Data Protection Act 1998, and all other E.U. National Legislation

E.U. Data Privacy Directive 95/46/EC

DIACAP (DoD Information Assurance Certification and Accreditation Process)

FIPS 140-2 (Federal Information Processing Standard)

SSAE 16 (Statement on Standards for Attestation Engagements 16)

E.U. – U.S. Safe Harbor Registration

SOC 1 / SOC 2 (Service Organization Controls)

Contact Us

For more information about Oracle RightNow Platform visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together