Enterprise-Class Data Management, Security, and Availability

OpenAir Data Center

OpenAir runs in two geographically separated data centers: a primary data center in Virginia and a secondary data center in Arizona. The secondary data center provides data mirroring, disaster recovery, and failover capabilities should the primary data center become nonoperational. Both data center facilities are operated by leading collocation providers, which provide earthquake and fire protection, along with heating, cooling, and backup power. The OpenAir application is multi-tenant and all servers, storage, and hard drives are built on several layers of redundancy.

OpenAir Data Center Infrastructure

Data Management

Redundancy: Many layers in the OpenAir system implement multiple levels of redundancy. This design allows one or more elements to fail by having multiple, redundant systems online to automatically assume processing on behalf of the failed component.

Disaster Recovery: Data in the primary Virginia data center is periodically replicated and synchronized in the secondary Arizona data center. In the event that the primary data center fails, customers can be serviced from the secondary data center.

Scalability: OpenAir systems are designed to accommodate surges and spikes in usage, and to smoothly scale upward to address increased volume and transactions.

Application Security

Encryption: Transmission of users' unique ID and passwords, as well as all data in the resultant connection, are encrypted with AES 256-bit TLS.

Application-Only Access: The system is divided into layers that separate data from the OpenAir application itself. Users of the application can only access their data using the application features, and not the underlying database or other infrastructure components.

Role-Level Access and Idle Disconnect: Customers can assign each end user a specific role with specific permissions to only see and use those features related to his or her own job. There is a complete audit trail whereby changes to each transaction are tracked by the user login details and a timestamp for each change is provided. The system also detects idle connections and automatically locks the browser screen to prevent unauthorized access from an unattended computer screen.

IP Address Restrictions: Restrictions on accessing an OpenAir account from specific computers and/or locations can be enforced. This is very useful for customers who are concerned not only about who is able to access their OpenAir account, but from where they access it as well.

Robust Password Policies: OpenAir offers fine-grained password configuration options — from the length of the user's passwords to the expiration of a user's password on any timeframe they desire. Customers can set up strict password policies to ensure that new passwords vary from prior passwords, and that passwords are complex enough to include a combination of numbers, letters, and special characters. Accounts are also locked out after several unsuccessful attempts.

Operational Security

Continuous Monitoring: OpenAir employs both network and server-based Intrusion Detection Systems (IDS) to identify malicious traffic attempting to access its servers and networks. Security alerts and logs are sent to a Security Information and Event Management (SIEM) system for monitoring and response actions by a dedicated security team.

Separation of Duties: In addition to mandatory employee background checks at all levels of OpenAir operations, job responsibilities are separated. The Principle of Least Authority (POLA) is followed and employees are given only those privileges that are necessary to do their duties.

Physical Access: Both data centers maintain stringent physical security policies and controls including photo IDs, proximity access cards, biometrics, single person entry portals, and alarmed perimeters.

Guarded Premises: On-premises security guards monitor all alarms, personnel activities, access points, and shipping and receiving, and ensure that entry and exit procedures are correctly followed on a 24x7 basis. Guards are provided with ongoing awareness training and skills-building. Guards perform tours at random intervals. CCTV video surveillance cameras are located at points of entry and other secured areas. Video is monitored and is stored for review for non-repudiation.

Data Center Performance Audits: OpenAir Operations management implements such auditing controls as appropriate for SOC 1 Type II and SOC 2 Type II compliance. Periodic audits are carried out to help ensure that personnel performance, procedural compliance, equipment serviceability, updated authorization records, and key inventory rounds meet or exceed industry standards.

Security Certifications: OpenAir has undergone ISO 27001, ISO 27018, SOC 1 Type II, and SOC 2 Type II audits. OpenAir has defined its Information Security Management System in accordance with industry standards.

OpenAir's SOC 1 Type II and SOC 2 Type II audit reports show that it has been through an in-depth audit of the control environment, including controls over data and network security, backup and restoration procedures, system availability, and application development. The requirements of Section 404 of the Sarbanes-Oxley Act make a SOC 1 Type II and SOC 2 Type II audit reports essential to the process of reporting on the effectiveness of internal control over a company's financial reporting.

OpenAir has achieved the International Organization for Standardization (ISO) 27001* certification, the leading international standard for measuring Information Security Management Systems (ISMS). The standard requires a systematic examination of security risks, threats, vulnerabilities, and their impact. To achieve certification, an organization must design and implement a comprehensive suite of information security controls and adopt an overarching management process to ensure that information security controls continue to meet the organization's needs on an ongoing basis. OpenAir's compliance with this important industry certification demonstrates the company's continued commitment to maintaining and improving its information security management and data custodianship programs.

Oracle NetSuite performs reviews and annual audits, conducts privacy risk management and oversees remediations, oversees privacy by design in technology and processes, has a third-party vendor management program to ensure that the suppliers adhere to the privacy regulations, and is committed to maintaining and improving its privacy information management and data protection programs. Oracle NetSuite also provides Product Feature Guidance documents that describe how the service functionality is designed to assist customers with their privacy requirements.

- Oracle NetSuite has extended the ISO 27001 Information Security Management System to include the ISO 27018 control set, demonstrating protection and adequacy for processing Personal Information as a Public Cloud Hosting Provider.
- Oracle NetSuite's adherence to the EU Cloud Code of Conduct (CoC) has been verified and published on the monitoring body's public registry. The CoC has been designed to define general requirements for cloud service providers as processor, demonstrating sufficient guarantees under Art. 28.1-4 of EU General Data Protection Regulation (GDPR).
- Oracle Corporate (Oracle EMEA Ltd) has obtained EU/EEA-wide authorization from the European data protection authorities for its Binding Corporate Rules for Processors ("BCR-p"). This helps our customers address their privacy and security requirements under GDPR and other European data protection laws and regulations in the EU/EEA, the UK, and Switzerland ("European Data Protection Law"). See the Privacy Code for Processing Personal Information of Customer Individuals (Oracle Processor Code).

Availability

Service Level Commitment (SLC): An SLC guarantees a 99.7% uptime (outside the scheduled service windows) for the OpenAir production applications for all customers. A credit is available if OpenAir does not deliver its application services with 99.7% uptime.

Redundant Internet Connections: The network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity, and confidentiality. Both data centers have two pipes, burstable to 100mbps.

This redundancy ensures reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center.

Backup Power Systems: Uninterruptible power systems (UPSs) are provisioned in a redundant configuration to support environmental controls in the collocation spaces. Each UPS battery system is designed to carry full load for 15 minutes without a generator. Emergency generators typically provide backup power in less than 10 seconds and are sized to support the entire facility at maximum load.

HVAC Systems: Air conditioning is configured to allow for proper heat dissipation, permitting the sites to operate within an acceptable temperature range. To maintain the flow of air conditioning, an N+1 redundant system of HVAC units is employed within each location. The HVAC units are powered by normal and emergency electrical systems to maintain their availability.

Fire Suppression: The latest fire suppression methods have been employed at the data centers, augmented by heat detection and dry-pipe sprinkler systems.

Seismic Engineering: The secondary data center provides seismic isolation equipment to cushion facilities against movement, in addition to installing earthquake bracing on all equipment racks.