NETSUITE OPENAIR DATA CENTER

Enterprise-Class Data Management, Security and Availability

OpenAir Data Center Architecture

OpenAir runs in two geographically separated data centers: a primary data center in Massachusetts, and a secondary data center in California. 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 a leading collocation provider, which provides 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.

Facts about OpenAir's 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 Massachusetts data center is periodically replicated and synchronized in the secondary California data center. In the event that the primary data center fails, customers can be serviced from the secondary data center.

Scalability: As of September 2014, trailing 12 months, OpenAir supports over 125,000 users with over 455 million customer requests per month. OpenAir has designed its systems to accommodate surges and spikes in usage, and to scale upward smoothly 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 128 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 at 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.

OpenAir runs in both a primary and a secondary data center.

Operational Security

Continuous Monitoring: OpenAir employs Intrusion Detection Systems (IDS) to identify malicious traffic attempting to access its networks. Unauthorized attempts to access the data center are blocked and any unauthorized connection attempts are logged and investigated. Enterprise-grade anti-virus software is also in place to guard against trojans, worms, viruses and other malware from affecting the corporate software and applications.

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' operators maintain stringent physical security policies and controls:

- The first layer of security includes photo ID proximity access cards and a biometric identification system, located at all entry points. This multi-factor authentication system provides additional assurance against lost badge risks or other attempts at impersonation.
- Single-person portals and T-DAR man traps guarantee that only one person is authenticated at one time to prevent tailgating or piggybacking.
- All perimeter doors are alarmed and monitored and all exterior perimeter walls, doors, windows and the main interior entry are constructed of materials that afford Underwriters Laboratory (UL) rated ballistic protection.

Guarded Premises: On-premise 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 SSAE 16/ ISAE 3402 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 an SSAE 16/ISAE 3402 Type II audit, and is EU-US Safe Harbor certified. OpenAir has defined its Information Security Management System in accordance with industry standards.

OpenAir's SSAE 16 Type II and ISAE 3402 Type II audit report shows that we have been through an in-depth audit of our 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 SSAE 16/ISAE 3402 Type II audit report essential to the process of reporting on the effectiveness of internal control over a company's financial reporting.

The EU-US Safe Harbor is key for the transfer of personal data from European Union (EU) countries to the United States. EU organizations know that organizations that self-certifying to the EU-US Safe Harbor Framework provide "adequate" privacy protection, as defined in the European Commission's Directive on Data Protection. OpenAir adheres to the Safe Harbor Privacy Principles published by US Department of Commerce with respect to personal data about individuals in the EEA received fromits subsidiaries, customers and other business partners.

Availability

Service Level Commitment: OpenAir's SLC guarantees a 99.5% uptime (outside the scheduled service windows) for the OpenAir production applications for all our customers. A credit is available if OpenAir does not deliver its application services with 99.5% 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 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 which utilizes state-of-the-art "sniffer" systems, 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.