NetSuite Data Center Fact Sheet

Enterprise-Class Data Management, Security and Availability

NetSuite is the world's largest cloud ERP vendor, supporting over 10,000 organizations, processing 1.5 billion transactions per quarter, investing over $35 million in R&D annually, and having 2.2 million unique logins per quarter. NetSuite also has a 12-year track record of maintaining the security of our customers' records.

NetSuite Data Center Architecture

NetSuite operates two geographically separated data centers: a primary data center in California, and a secondary data center in Massachusetts. The secondary data center provides data mirroring, disaster recovery and failover capabilities should the primary data center become non-operational. 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 NetSuite application is multi-tenant, and all servers, storage and hard drives are built on several layers of redundancy.

NetSuite Provides Both a Primary and a Secondary Data Center

U.S. - EU Safe Harbor Certified

TRUSTe Certified Privacy

PCI Security Standards Council

SAS70 Completed Type II Audit

Facts about NetSuite's Data Center Infrastructure

Data Management

- **Redundancy:** Many layers in the NetSuite system implement multiple levels of redundancy. This design allows one or more elements to fail without any interruption in service by having multiple, redundant systems online to automatically assume processing on behalf of the failed component.
- **Disaster Recovery:** Data in the primary California data center is replicated and synchronized in the secondary Massachusetts data center. In the event that the primary data center fails, all operations fail over to the secondary data center.
- **Scalability:** As of January 2011, trailing 12 months, NetSuite supports over 10,000 organizations with over 4 billion customer requests per month. NetSuite 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 128-bit SSL. At rest data is encrypted using contemporary encryption standards such as AES for symmetrical applications and SHA2 for hashing applications, as required by the PCI-DSS.
- **Application-Only Access:** The system is divided into layers that separate data from the NetSuite application itself. Users of the application can only access 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 a NetSuite 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 NetSuite account, but from where they access it as well. This feature significantly reduces the risk of unauthorized third parties accessing a user's account.
- **Robust Password Policies:** NetSuite 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. For customers who desire a higher level of access control, NetSuite offers multifactor authentication using a simple physical token. In addition to entering their own passwords, users must possess physical tokens that generate random one-time passwords. These cryptographically robust passwords prevent key loggers, shoulder surfers, phishers and password crackers from accessing a user's account.

U.S. - EU Safe Harbor Certified

TRUSTe Certified Privacy

PCI Security Standards Council

SAS70 Completed Type II Audit

Operational Security

- **Continuous Monitoring:** NetSuite employs numerous 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 NetSuite 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 to allow unescorted access to pre-authorized NetSuite Operations personnel:

  - The first layer of security includes photo ID proximity access cards and a biometric identification system. This multifactor authentication system provides additional assurance against lost badge risks or other attempts at impersonation. Proximity card reader devices are located at major points of entry and are used to secure critical areas within the data centers.
  - Single-person portals and T-DAR man traps guarantee that only one person is authenticated at one time to prevent tailgating. Reliable detection and prevention of tailgating and piggybacking through secure doors significantly increases the effectiveness of the access control system.
  - In addition, 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. Vegetation and other objects around the data center are landscaped in a manner such that an intruder would not be concealed.

- **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. Numerous CCTV video surveillance cameras with pan-tilt-zoom capabilities are located at points of entry to the collocation and other secured areas within the perimeter. Video is monitored and is stored for review for non-repudiation.
- **Data Center Performance Audits:** NetSuite Operations management implements such auditing controls as appropriate for SAS70 Type II and PCI compliance. NetSuite's comprehensive risk management process has been modeled after the National Institute of Standards and Technology's (NIST) special publication 800-30 and the ISO 27000 series of standards. Periodic audits are carried out to help ensure that personnel performance, procedural compliance, equipment serviceability, updated authorization records and key inventory rounds are above par.
- **Security Certifications:** NetSuite has passed a SAS 70 Type II audit, is certified for PCI-DSS, and is EU-US Safe Harbor certified. NetSuite has defined its Information Security Management System in accordance with NIST standards, including 800-53 and ISO27000 series standards.
  - NetSuite's SAS 70 Type II audit is prepared by and audited by a Big Four audit firm. Our SAS 70 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 SAS 70 Type II audit report essential to the process of reporting on the effectiveness of internal control over a company's financial reporting.
  - In complying with PCI-DSS requirements, NetSuite offers optional 3D Secure credit card authentication—also known as Verified by Visa and MasterCard SecureCode. 3D Secure adds a higher level of credit card fraud protection. It requests shoppers to create authentication passwords for their credit cards, or requires them to enter their password if they already have one assigned.

U.S. - EU Safe Harbor Certified

TRUSTe Certified Privacy

PCI Security Standards Council

SAS70 Completed Type II Audit

– 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 U.S.-EU Safe Harbor Framework provide "adequate" privacy protection, as defined in the European Commission's Directive on Data Protection. NetSuite adheres to the Safe Harbor Privacy Principles published by US Department of Commerce with respect to personal data about individuals in the EEA received from its subsidiaries, customers and other business partners. NetSuite's participation in the U.S.-EU Safe Harbor program can be confirmed by viewing the public list of Safe Harbor organizations posted on http://safeharbor.export.gov/list.aspx.

Availability

- **Service Level Commitment:** NetSuite's SLC guarantees a 99.5% uptime (outside the scheduled service windows) for the NetSuite production applications for all our customers. A credit is available if NetSuite does not deliver its application services with 99.5% uptime. We have consistently averaged an actual uptime of 99.97% and provide customers a publicly available webpage to display system status at all times at http://status.netsuite.com.
- **Redundant Internet Connections:** The network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. Both NetSuite data centers have three 1 GBps diverse-path pipes, designed so that any two connections can simultaneously fail without impacting user experience. This redundancy ensures reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center.
- **Backup Power Systems:** NetSuite has designed a solution for clean, continuous power. 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. In addition to UPS systems, NetSuite makes use of power management modules and power distribution units on data center floors for a physically integrated and electrically redundant system for source selection, isolation, distribution, monitoring and control of power to computer equipment loads.
- **HVAC Systems:** Air conditioning in both data centers 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. Additionally, cold water tanks have been installed to keep air conditioning units functioning when transition from direct power to generator power during emergencies is required.
- **Fire Suppression:** The latest fire suppression methods have been employed at NetSuite's data centers. The systems utilize state-of-the-art "sniffer" systems, augmented by heat detection and dry-pipe sprinkler systems.
- **Seismic Engineering:** NetSuite-operated datacenters provide seismic isolation equipment to cushion facilities against movement, in addition to installing earthquake bracing on all equipment racks. Racks are anchored to the concrete slab below the site's raised floor.

U.S. - EU Safe Harbor Certified

TRUSTe Certified Privacy

PCI Security Standards Council

SAS70 Completed Type II Audit