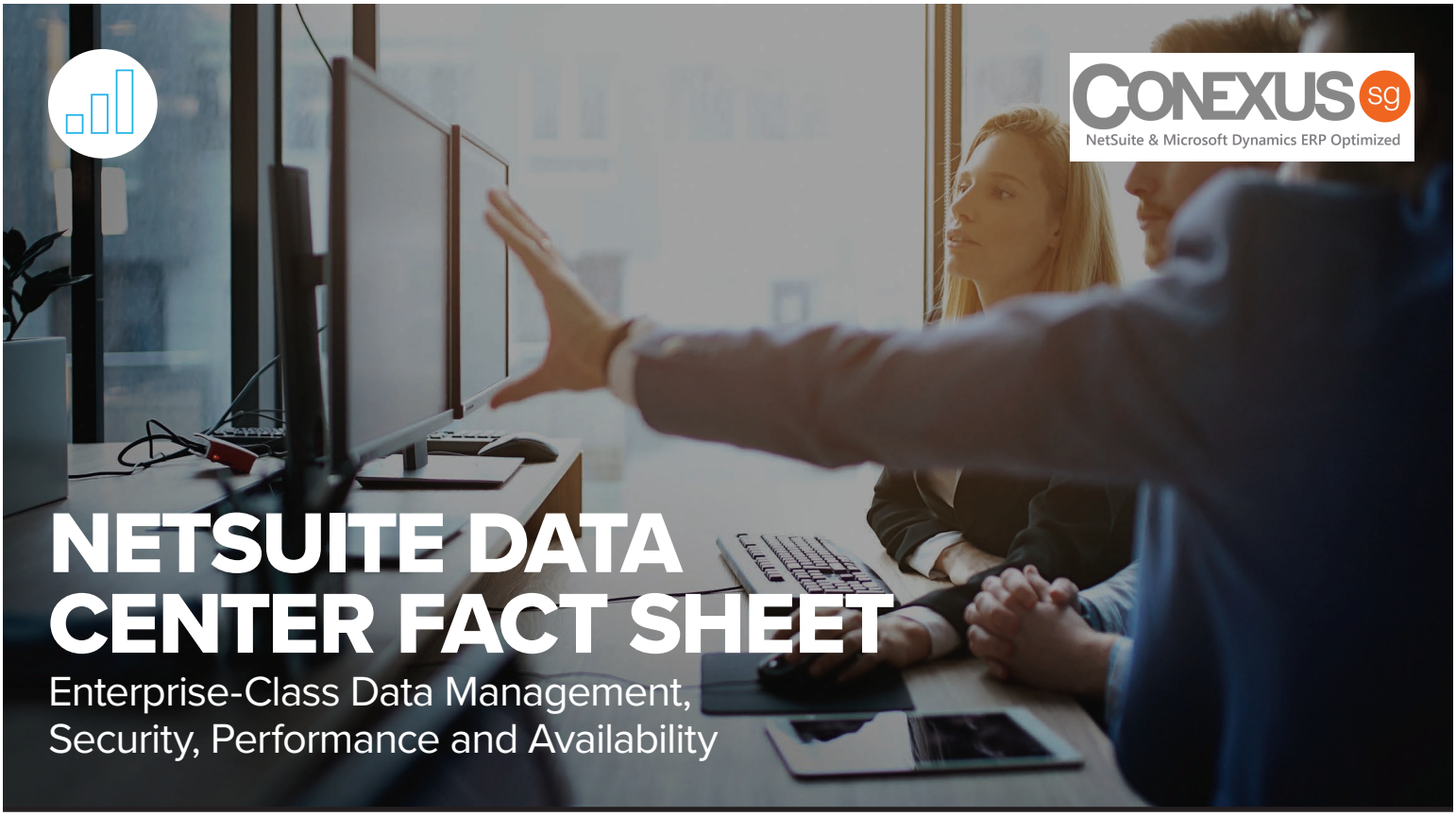


CONEXUS sg
NetSuite & Microsoft Dynamics ERP Optimized

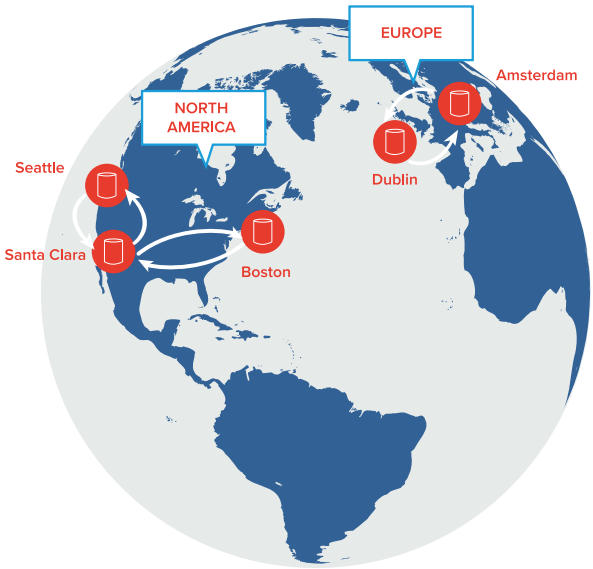
NETSUITE DATA CENTER FACT SHEET

Enterprise-Class Data Management, Security, Performance and Availability

NetSuite is the world's largest cloud ERP vendor, supporting over 40,000 organizations, processing over 500 million application requests per day with 9+ terabytes of data added every day. NetSuite also has a track record since 1998 of maintaining the security of our customers' records.

NetSuite Data Center Architecture

NetSuite operates five geographically separated data centers present in two Regions, US and Europe. The data centers operate in a hub-spoke architecture. Each region has a dedicated data center that provides data mirroring, disaster recovery and failover capabilities for the other data centers in that region in case any data center becomes non-operational. Customer data is not shared between the regions. All 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.



ORACLE + NETSUITE

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: Within one region, data is replicated and synchronized between the active data centers and the dedicated DR data center by way of a proprietary replication mechanism built in house. In the event that the primary data center fails, all operations fail over to the DR data center. This failover procedure is tested and proven on the live site twice annually. The failover procedure is automated and can be triggered in push button fashion. NetSuite has operations engineers geographically distributed from each other, as well as the data centers in order to be able to execute a failover in any disaster scenario. NetSuite conducts semi-annual DR exercises to ensure that systems and processes are in place, as well as to assess and enhance competency of all relevant personnel key to the successful implementation of DR activities. NetSuite data centers utilizes tape backups which supports customer-initiated data restores.
- Scalability: NetSuite supports over 40,000 organizations with over 500 million application requests per day with 9+ terabytes of data added every day. 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 industry standard protocol and cipher suite. NetSuite supports Custom Attribute encryption and provide encryption APIs. The application authentication is token based while end user authentication supports modern two factor authentication with mobile devices or authentication FOBs.
- 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 multi-factor 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.

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: All 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 multi-factor 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.
- Dedicated Security Team: NetSuite employs a global security team dedicated to enforcing security policies, monitoring alerts and investigating any anomalous behavior within the system. This team is active 24x7 from multiple worldwide locations. All access to production is reviewed and granted by the security team.
- Data Center Performance Audits: NetSuite Operations management implements such auditing controls as appropriate for SSAE 16 Type II, ISAE 3402 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 SSAE 16 Type II and ISAE 3402 Type II audits, is certified for PCI-DSS, and is EU-US Privacy Shield Compliant. NetSuite has defined its Information Security Management System in accordance with NIST standards, including 800-53 and ISO27000 series standards.
  - NetSuite's SSAE 16 Type II and ISAE 3402 Type II audit is prepared by and audited by a Big Four audit firm. SSAE 16 Type II and ISAE 3402 Type II reports show 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.
  - NetSuite 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. NetSuite'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.

Performance

- Scalable Application Architecture: NetSuite's application runs on a three tiered architecture. All three tiers—web, application, and database—are horizontally scalable and support multi-data center deployment. NetSuite currently operates on over 4000 hosts in production.
- Performance Team: NetSuite invests heavily in performance at every layer. This includes a dedicated performance team of developers and DBAs whose sole purpose is to proactively verify application performance benchmarks and tune the application for maximum performance.
- High Performance Databases: NetSuite runs on high performance database server hardware with multiple cores and maximum RAM configuration. NetSuite production database servers run exclusively on flash SSD storage ensuring the fastest possible database IO performance available in the industry.
- Performance Monitoring Tool: NetSuite's Application Performance Monitoring tool provides a comprehensive performance dashboard that allows you to easily and quickly drill down and investigate the root cause of your site's performance issues. By capturing critical performance data and quickly identifying, analyzing and fixing the problem areas, you can optimize performance, improve customer experience and maintain critical transactions.

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 99.98% and provide customers a publicly available webpage to display system status at all times at http://status.netsuite.com.
- World Class Hosting Operations Team: NetSuite has a global team of dedicated hosting operations personnel with decades of cumulative experience running large cloud and SaaS business applications demanding high performance and high availability. This team proactively monitors the health of the entire system with industry leading alert and trend based tools designed to identify and resolve events before they impact the live site. This team provides 24x7 coverage to respond to any incident with automated recovery procedures.

- Redundant Internet Connections: The network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. All NetSuite data centers have three 10 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. Additionally, each data center has 2 dedicated 10 Gbps circuits for data replication.
- 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 all 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 data centers 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.