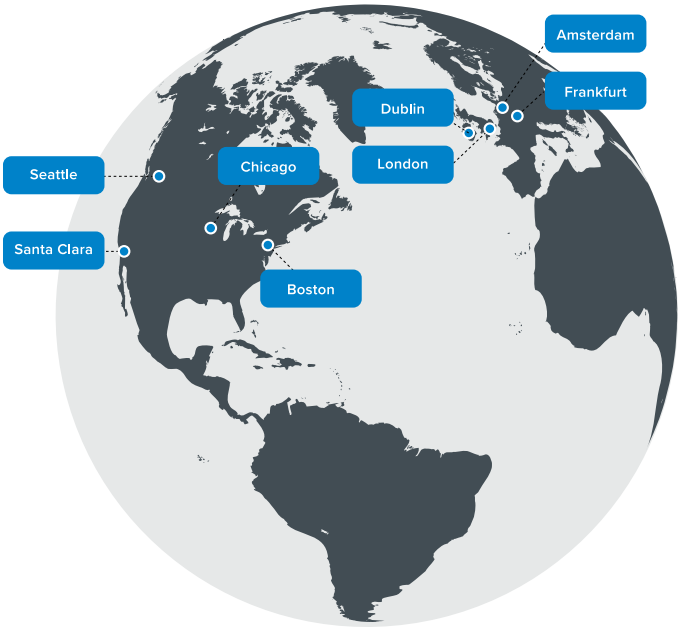
Enterprise-Class Data Management, Security, Performance and Availability

NetSuite Data Center

NetSuite currently operates eight geographically distinct data centers across North America and Europe. Each data center has a counterpart that provides data mirroring, disaster recovery and failover capabilities in its region in case any data center becomes non-operational. NetSuite data center facilities are operated by industry-leading collocation providers that offer fire protection, heating, cooling and backup power. The NetSuite service is natively multi-tenant and leverages cloud infrastructure designed around multiple layers of redundancy.



NetSuite Data Center Infrastructure

Data Management

- Redundancy. Many layers in the NetSuite system implement multiple levels of redundancy. This design allows uninterrupted service by having redundant systems online to automatically assume processing in the event that one or more elements fail.
- Disaster Recovery (DR). Within each region, data is replicated and synchronized between data centers. 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 utilize archival media backups which supports customer-initiated data restores for up to a year.
- Scalability. NetSuite supports over 19,000 customers with over 1.5 billion application requests per day and more than 6 petabytes of data under management. NetSuite has designed its systems to accommodate routine surges and spikes in usage, and to scale upward smoothly to address increased transaction volume. NetSuite is continuously expanding the delivery of the NetSuite service to new global data centers and regions.

Application Security

- Encryption. Transmission of user credentials, as well as all data in the resultant connection, are encrypted with industry standard protocol and cipher suite. NetSuite supports Custom Attribute encryption and provides encryption APIs. Application authentication is token based while end-user authentication is multi-factor.
- Role-Level Access and Idle Disconnect. Each end user can be assigned 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.
- 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, ranging from the length of the user's passwords to the password expiration policy. 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 text SMS, one-time passwords (OTP) and backup codes. In addition to entering their own passwords, users must possess TOTP-compatible devices to receive the 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 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 the operations organization, 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 maintain stringent physical security policies and controls including photo IDs, proximity access cards, biometrics, single person entry portals and alarmed perimeters.
- Dedicated Security Team. NetSuite employs a global security team dedicated to enforcing security policies, monitoring alerts and investigating any anomalous system behavior including unauthorized connection attempts and malicious software. Near real-time monitoring is in place with a 24x7 worldwide incident response capability. All access to production is approved and regularly reviewed by the security team.
- Data Center Performance Audits. NetSuite implements auditing controls appropriate for SOC 1 Type II, SOC 2 Type II, ISO 27001 and PCI compliance. NetSuite implements a comprehensive risk management process that 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 meet or exceed industry standards.
- Security Certifications. NetSuite issues reports upon the completion of periodic SOC 1 Type II and SOC 2 Type II audits and is certified for PCI DSS and ISO 27001:2013.
    - NetSuite has defined its Information Security Management System in accordance with NIST 800-53 and ISO 27000 series standards.

- NetSuite's SOC 1 Type II and SOC 2 Type II audits are prepared and audited by independent third-party auditors. A SOC 1 Type II audit report is essential to the reporting requirements on the effectiveness of internal controls over financial reporting of Section 404 of the Sarbanes-Oxley Act. SOC 2 Type II reports on controls that directly relate to the security, availability and confidentiality trust services criteria at a service organization.
- PCI DSS is a security standard designed to ensure that companies are processing, storing and transmitting payment card information in a secure environment. An Attestation of Compliance (AOC) is issued to NetSuite prepared by a PCI Qualified Security Assessor (QSA).

- Privacy Certifications. NetSuite is EU US Privacy Shield compliant and monitors the privacy landscape for regulatory changes. NetSuite provides Service Feature Guidance documents that describe how the functionality is designed to assist customers with their EU GDPR requirements. NetSuite also regularly performs privacy risk management. The company remains committed to maintaining and improving its privacy information management and data protection programs.

Performance

- Scalable Application Architecture. NetSuite's application runs on a three-tiered architecture supported by additional specialized services. All tiers are highly scalable and support multi-data center deployment.
- Performance Team. NetSuite invests heavily in performance at every layer. This includes a dedicated performance team of developers and database engineers 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 solid state storage ensuring the fastest possible database I/O performance available in the industry.
- Performance Monitoring Tool. The NetSuite Application Performance Management (APM) tool provides a comprehensive performance dashboard that allows users to easily and quickly drill down and investigate the root cause of a site's performance issues. By capturing critical performance data and quickly identifying, analyzing and fixing the problem areas, customers can optimize performance, improve user experience and maintain critical transactions.

Availability

- Service Level Commitment (SLC). The NetSuite SLC guarantees a 99.5% uptime (outside scheduled service windows) for the NetSuite production application for all customers. A credit is available if NetSuite does not deliver its application services with 99.5% uptime. A publicly available web page is provided to display system status at all times at https://status.netsuite.com that includes quantitative current and historic uptime metrics as well as up-to-the-minute announcements during disruptions.
- World-Class Hosting Operations Team. NetSuite has a global team of dedicated operations personnel. 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.
- Dedicated Event Response Team. NetSuite employs a global cloud event response team dedicated to expediting responses and resolutions while establishing communications and regular updates during service-impacting events. This team is active 24x7 from multiple worldwide locations.
- Network Design. The network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. The network design ensures reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center. Finally, NetSuite utilizes CDN to enhance network reliability and help protect against denial-of-service attacks.