



NETSUITE SECURITY & INFRASTRUCTURE

By adopting any one of NetSuite's applications, you automatically enjoy the advantages of our world-class data center and team of IT professionals. Our team has decades of experience managing both product and data center security. We ensure the highest levels of data security as well as guaranteed uptime and performance.

We organize our security efforts into two areas: Product Security and Data Center Security.

NetSuite Product Security

- **Prevention of Malicious Acts**

NetSuite takes proactive measures to ensure that the application is safe from Internet attacks. All of the servers are behind a firewall to prevent users from accessing them other than by specifically allowed protocols and methods. In addition to our Internet firewalls, we have an additional level of protection around the production databases, allowing access only from specific hosts.

- **128-bit Secure Socket Layer Data Encryption**

From the moment you or your employees access the NetSuite application login screen, the data is protected. Your unique ID and password, as well as all data in the subsequent connection are encrypted with 128-bit SSL, the same level of transaction security currently utilized for Web commerce.

- **Application-only Access**

The system is divided into layers that separate data from the application. Everyone who logs in only has access to the application layer so no one can access your data to maliciously alter it.

- **Role-level Access, Idle Disconnect and Account Lockout**

Every user is assigned a specific role with specific permissions to only see and use the features related to their own jobs. The system also detects idle connections and automatically locks your browser screen to prevent someone else from sitting at your computer and using your access. Also, if anyone tries to access the application by guessing at a person's ID and password, the account will be locked after three attempts.

- **Continual Monitoring**

We employ port scans and network intrusion detection systems (NIDS) to identify any vulnerability within our network. While we block unauthorized attempts to access our data center, we do log and investigate unauthorized connection attempts.



- **Complete Audit Trail**

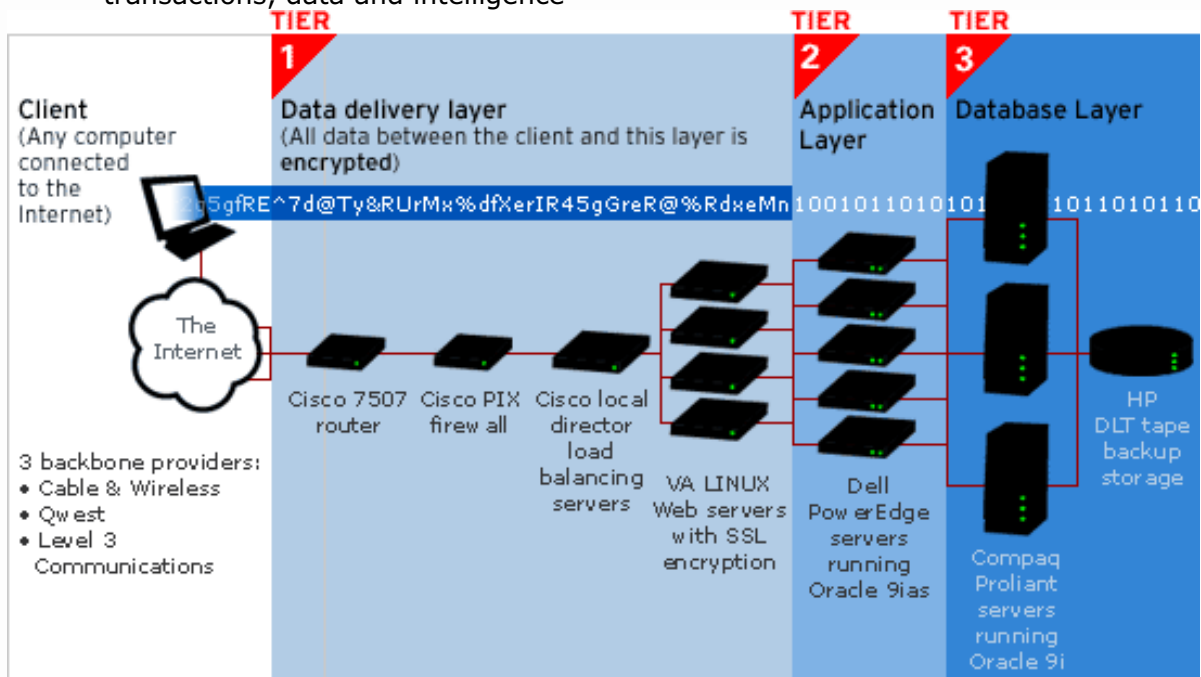
NetSuite continuously maintains a complete audit trail. It tracks who made the entry and when, referencing each transaction by the user login details.

- **Data Back-up**

All customer data is automatically backed up daily to tape. Tapes are taken offsite to a secure location that is designed to safeguard tapes under almost any environmental condition. The offsite facility exceeds industry storage requirements and is 100 miles away from the data center.

- **Security Architecture**

NetSuite’s architecture has been designed for high speed performance with flawless security. We have worked closely with our hardware and platform software partners to construct and tune NetSuite for absolute security of your transactions, data and intelligence



You can learn more about Oracle security by visiting www.oracle.com/security/. You can also learn about Cisco security by visiting www.cisco.com.

System Security

NetSuite uses tightly controlled passwords on its servers and network equipment. NetSuite limits access to production systems to authorized personnel only. Passwords are changed on a regular basis. Security updates to the operating systems are tracked and updated as necessary.

**System Reliability**

NetSuite looks at its application as well as the infrastructure as a tightly integrated system. All aspects of the system are designed to be reliable to ensure availability whenever a component fails. All web and application servers are configured in a redundant manner, so that no single server will bring down the system and the service is not interrupted. We have spare servers ready to deploy at a moments notice when there is an equipment failure. The networking equipment is also configured in a redundant manner with replacement equipment available in a few hours. NetSuite chooses equipment of the highest quality to power the solution. NetSuite has in place an expert team to provide services for server and network management, monitoring, backups, and other necessary maintenance. System administrators respond to monitoring alerts 24x7 and repair critical failures immediately.

Data and Backups

Customer data is stored on a server that is configured with RAID 5 redundancy with an onboard hot spare. In the event of a disk failure, the customer will not experience an interruption of service. In addition to the server configured with RAID 5, data is also stored on network-attached storage, which has its own built in redundancy, thus providing an extra layer of data protection. A redundant facility has recently opened in Australia as well. All customer data is automatically backed up daily to tape library system. Tapes are taken offsite to a secure location that is designed to safeguard tapes under almost any environmental condition. The offsite facility exceeds industry storage requirements and is 100 miles away from the data center.



Level 3 Communications Data Center Security

NetSuite data centre is colocated at Level(3) Communications in Sunnyvale, California. Level 3 ensures security and redundancy across its global operations. To learn more about Level 3 Communications visit their website at www.levelthree.com.

With the goal of providing the highest level of security possible, Level 3 protects the physical and electronic infrastructure of their global network. The network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality.

Security features are designed to deter, detect, and deny access to unauthorized parties. Continuous network monitoring by Network Operations Centres (NOCs) allows Level 3 to maintain uninterrupted service through immediate detection and remediation.

Level 3 Secure Facilities



NetSuite Data Center: Fortress within a Fortress

NetSuite maintains a data center within a data center at the Level 3 facility. With Level 3 security for the greater facility and NetSuite-only access for the NetSuite collocation, your system will be managed in a fortress within a fortress.

- **Gateway & Colocation Access Security Systems**

The Level 3 Gateways feature stringent physical security policies and controls to allow unescorted access to the Colocation areas for pre-authorized personnel. The



first layer of security includes Photo ID proximity Access Cards. Proximity and card reader devices are located at major points of entry and are used to secure critical areas within the Gateway. All perimeter doors are alarmed and monitored. Authorized customers and vendors are required to have a validated palm scan to enter the collocation area. The access control system continuously monitors and logs all entry ways. Access records are stored for reference.

- **Photo ID Card**

Customers and their contractors with authorized access to the collocation areas are issued cards upon their Installation date at the Gateways. Pictures are taken on-site and imprinted onto their security card, and then the card is issued to the customer.

- **Palm Identification System**

The Palm Identification System is linked to the access card system. Once the individual swipes the card, he or she must place a hand in the palm scan for final authorization.



- **Video Surveillance**

Gateways feature video surveillance cameras 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.

- **Sprinkler Design Approach**

The fire protection sprinkler system is a double-interlocked pre-action system designed to provide the best security against accidental discharge of water from the sprinklers. The pre-action system interfaces with a fire alarm system. Water will discharge only from the sprinklers that have been subjected to enough heat to melt the fusible link on the water head. This fusible link is the second interlock in the system.

- **HVAC Systems**

All of the air conditioning equipment is furnished to support typical computer room equipment. Steam generating humidifiers and electric reheat coils are provided to control humidity. The collocation room has an 18-inch access flooring system, which is dedicated for air distribution only.

- **Backup Power Systems—Uninterruptible Power Sources (UPSs)**

UPSs are provisioned in an N+1 configuration and range in size from 125kVA with 480 VAC, 3-phase input and output. The UPSs support all customer AC equipment. Each UPS battery system is designed to carry full load for 15 minutes without a



generator. Emergency generators typically provide back-up power in less than 10 seconds and are sized to support the entire facility at maximum load.

- **Earthquake Preparedness**

Level 3 complies with local and national earthquake codes and standard practices in all seismically classified geographical areas. Modifications to facilities include but are not limited to the following:

- Seismic bracing for the raised floor
- Seismic bracing for cabinets
- Seismic bracing for electrical switchboards
- Seismic bracing for overhead distribution trays and troughs
- Seismic bracing for the piping and associated supports
- Redundant DC power plants that are also seismically braced

- **Redundant Internet Connection**

While the NetSuite application was designed to run with minimal bandwidth, the data center has 2 x DS3 (45/Mbps) pipes to the two major Internet backbone providers. This redundancy ensures reliable connectivity with no data transmission bottlenecks to or from the data center.

For more information about Level 3's security, email GlobalSecurity@Level3.com