

Security

WORLD-CLASS SECURITY INFRASTRUCTURE

Salesforce.com provides state-of-the-art security to ensure that your customer data is never compromised. At salesforce.com, we know that security is crucial to you — that's why security is our top priority. We devote significant resources to continually develop our world-class security infrastructure. The result: unsurpassed security and privacy for our customers' information.

With salesforce.com, you enjoy protection and peace of mind that only our world-class security infrastructure can provide. Among other security measures, salesforce.com provides:

- :: Experienced, professional engineers and security specialists dedicated to round-the-clock data and systems protection
- :: Continuous deployment of proven, up-to-date security technologies, including proprietary products developed for salesforce.com
- :: Ongoing evaluation of emerging security developments and threats
- :: Complete redundancy throughout the entire salesforce.com online infrastructure
- :: Total commitment to a secure, scalable, private, collocated system (unlike a hosted system arrangement, salesforce.com manages all aspects of its operations)

SECURITY DETAILS

Salesforce.com is as secure as the leading online financial services company. Configured by experts and rigorously tested before going into production, our world-class security infrastructure includes proven, up-to-date firewall protection, intrusion detection systems, SSL encryption, and other security technologies, including proprietary products developed specifically for salesforce.com.

Physical Security. Our production equipment is located in Sunnyvale, California at a facility that provides 24-hour physical security, palm print and picture identification systems, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers continually up and running.

Perimeter Defense. The network perimeter is protected by multiple firewalls and monitored by intrusion detection systems — all sourced from industry-leading security vendors. In addition, salesforce.com monitors and analyzes firewall logs to proactively identify security threats. Salesforce.com also contracts with a third-party security firm that proactively monitors our security configurations for changes, vulnerabilities, and errors and regularly conducts vulnerability threat assessments including penetration tests.

Data Encryption. Salesforce.com uses the strongest encryption products to protect customer data and communications, including 128-bit VeriSign SSL Certification and 1024-bit RSA public keys. The lock icon in the browser indicates that data is fully shielded from access while in transit.

User Authentication. Users access Salesforce only with a valid username and password combination, which is encrypted via SSL while in transmission. Users are prevented from choosing weak or obvious passwords. An encrypted session ID cookie is used to uniquely identify each user. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security. Our robust application security model prevents one salesforce.com customer from accessing another's data. This security model is reapplied with every request and enforced for the entire duration of a user session.

Internal Systems Security. Inside of the perimeter firewalls, the systems are safeguarded by network



Salesforce.com Named to
Aberdeen Group's
"What Works" CRM Top 10
2001, 2002 & 2003

address translation, port redirection, IP masquerading, non-routable IP addressing schemes, and more. The specific details of these features are proprietary.

Operating System Security. Salesforce.com enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts with strong passwords, and production servers do not share a master password database. All operating systems are maintained at each vendor's recommended patch levels for security and are hardened by disabling and/or removing any unnecessary users, protocols, and processes.

Database Security. Whenever possible, database access is controlled at the operating system and database connection level for additional security. Access to production databases is restricted to a limited number of points, and production databases do not share a master password database.

Server Management Security. All data entered into the Salesforce application by a customer is owned by that customer. Salesforce.com employees do not have direct access to the salesforce.com production equipment, except where necessary for system management, maintenance, monitoring, and backups. Salesforce.com does not currently utilize any managed service providers. The salesforce.com systems engineering team provides all system management, maintenance, monitoring, and backups.

Reliability and Backup. All networking components, SSL accelerators, load balancers, Web servers, and application servers are configured in a redundant configuration. All customer data is stored on a database served by a database server cluster for redundancy. All customer data is stored on carrier-class disk storage using RAID disks and multiple data paths. All customer data, up to the last committed transaction, is automatically backed up to a primary tape library on a nightly basis. Backup tapes are immediately cloned to verify their integrity, and the clones are moved to secure, fire-resistant, off-site storage on a regular basis.

Disaster Recovery. Salesforce.com has an agreement in place with a third-party provider of availability services to provide access to a geographically remote disaster recovery facility — along with required hardware, software, and Internet connectivity — in the event our production facilities were to be rendered unavailable. Salesforce.com has disaster recovery plans in place and tests them regularly — in our QA environment on a quarterly basis and off-site with the third-party provider on an annual basis.

Use of the salesforce.com service is subject to the terms and conditions of the customer's subscription agreement with salesforce.com. Salesforce.com may modify its security infrastructure and/or this security datasheet from time to time.

THE AMERICAS

The Landmark @ One Market
Suite 300
San Francisco, CA 94105
United States of America
1-800-NO-SOFTWARE
www.salesforce.com

JAPAN

Ebisu Business Tower 18F
1-19-19 Ebisu, Shibuya-ku
Tokyo, 150-0013
Japan
+81-3-5793-8301
www.salesforce.com/jp

AUSTRALIA & NEW ZEALAND

Level 39, Citigroup Centre
2 Park Street
Sydney, NSW 2000
Australia
+612-9004-7849
www.salesforce.com/au

EUROPE, MIDDLE EAST & AFRICA

South County Business Park
Leopardstown
Dublin 18
Ireland
+353-1-2723-500
www.salesforce.com

Austria: 0800 292 027 France: 0800 908 534 Germany: 0800 18 22 338 Ireland: 1 800 444456 Italy: 800 782 619
Spain: 900 938 976 Switzerland: 0800 564 005 United Kingdom: 0800 092 1223

salesforce.com[®]
experience success.™

Copyright ©2005, salesforce.com, inc. All rights reserved. Salesforce.com and the "no software" logo are U.S.-registered trademarks of salesforce.com, inc. All other trademarks mentioned in this document are the properties of their respective owners.

