

salesforce



**Secure, private, and trustworthy:
enterprise cloud computing with Force.com**



Contents

Abstract	1
Introduction to security, privacy, and trust	1
Cloud computing and information security governance	1
Force.com cloud platform security	2
Force.com cloud application security	4
Force.com cloud platform privacy	5
Conclusion: the world's largest enterprises trust Force.com	6

Abstract

An ever-growing list of enterprises trusts the Force.com cloud computing platform to deliver critical business applications, in large part because of salesforce.com's commitment to security and privacy. This paper first explains the terms security, privacy, and trust, and then explores the basic requirements for secure cloud computing. Subsequent sections of this paper provide a comprehensive introduction to the inherent security and privacy features of the Force.com enterprise cloud computing platform as well as platform features application providers can in turn use to build and secure their applications and customer data.

Introduction to security, privacy, and trust

Polls and industry analysts consistently cite security and privacy concerns as the most significant barriers to the mainstream adoption of cloud computing, especially among enterprise customers. To gain the trust of organizations, a cloud provider must deliver levels of security and privacy (not to mention reliability, availability, and performance) that meet or exceed what is achievable with on-premises solutions.

In the context of computing, the terms security, privacy, and trust are related, but have different meanings. Security refers to a computing system's level of resistance to threats. Privacy most often concerns the digital collection, storage, and sharing of information and data, including the transparency of such practices. As the Venn diagram in Figure 1 shows, when a cloud computing system is reliably secure and private, its users develop trust in the system.

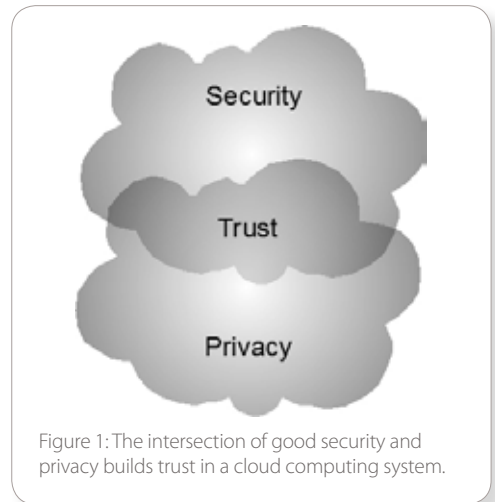


Figure 1: The intersection of good security and privacy builds trust in a cloud computing system.

Cloud computing and information security governance

Information security governance is a term that encompasses all the tools, people, and business processes an organization uses to ensure the security and privacy of the data that its systems maintain. Because cloud computing is a business model that includes a layered set of providers, secure and private cloud computing happens only when there is a commitment to information security governance from both the underlying platform provider as well as application providers that use the platform to deploy applications and manage data.

Figure 2 summarizes the security governance realms of cloud platform providers and cloud application providers. The platform provider's security governance realm includes the design and maintenance of a secure platform and policies that protect the privacy of its direct customers and all data. Meanwhile, an application provider's security governance realm includes the use of platform features to build secure applications and the implementation of security and privacy policies that ultimately protect end-user customer data from threats and privacy concerns.

Salesforce.com's approach to information security governance, structured around the ISO 27002 framework, consists of many components:

- **Employees** – All employees receive regular information security and privacy training. Employees in data-handling positions receive additional training specific to their roles.
- **Security staff** – Salesforce.com has a dedicated security staff, including a Chief Trust Officer, VP of Information Security, and a full staff of Certified Information Systems Security Professionals.

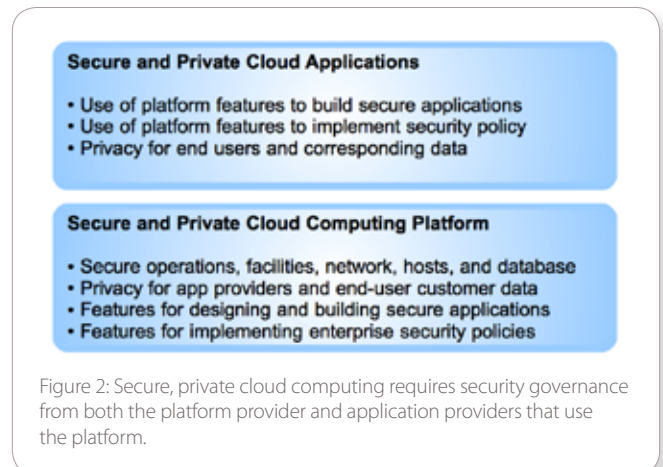


Figure 2: Secure, private cloud computing requires security governance from both the platform provider and application providers that use the platform.

- **Counsel** – Salesforce.com has a Global Privacy Counsel who is a Certified Information Privacy Professional (CIPP) with responsibility for helping ensure compliance with global privacy laws.
- **Assessments** – Salesforce.com regularly conducts both internal vulnerability assessments (for example, architecture reviews by security professionals) and external vulnerability assessments (for example, vulnerability assessments by managed security services providers, or MSSPs).
- **Policies** – Detailed internal policies dictate how salesforce.com handles security and privacy incidents, including detection, response, and forensics.

In particular, salesforce.com incorporates security into its platform development processes at all stages. From initial architecture considerations to post-release, all aspects of platform development consider security. Figure 3 summarizes some of the standard practices salesforce.com employs, which have made it the trusted provider that it is today.

- **Design phase** – Guiding security principles and required security training help ensure salesforce.com technologists make the best security decisions possible. Threat assessments on high-risk features help to identify potential security issues as early in the development lifecycle as possible.
- **Coding phase** – Salesforce.com addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis tools to identify security flaws.
- **Testing phase** – Internal salesforce.com staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues.
- **Prior to release** – Salesforce.com validates that the functionality being developed and maintained meets its internal security requirements. Post-release, salesforce.com uses independent security service providers to analyze and monitor the product for potential security issues. These reports are made available to prospects and customers under a non-disclosure agreement.



Figure 3: Salesforce.com incorporates security into every phase of its development lifecycle to ensure the security of its platform.

Force.com cloud platform security

Figure 4 on the following page illustrates the many layers of defense the Force.com cloud platform uses to resist various types of threats and achieve SAS 70 Type II, SysTrust, and ISO 27001 certifications—all without sacrificing application performance.

At the operational layer, salesforce.com strictly manages access to its facilities and the work operators can perform once inside a facility. Before being granted access, every employee and contractor must pass a thorough background check. Once a person is employed, salesforce.com limits that operator's actions using secure workstations (to prevent operations such as cut/paste, public IM, and data copying), private networks, and tight segregation of duties (least privileges).

The physical security of each salesforce.com facility is comparable to the best civilian data centers in the world. The exterior perimeter of each anonymous building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and cages at all times.

Force.com secures its network on many different fronts. For example:

- **Stateful packet inspection (SPI)** firewalls inspect all network packets and prevent unauthorized connections.
- **Bastion hosts** (special-purpose computers designed to withstand attacks) act as hardened barriers between the perimeter and core firewalls.
- **Two-factor authentication processes** verify the identity of access requests to internal systems.
- **End-to-end TLS/SSL** cryptographic protocols encrypt all network data transmissions.

Salesforce.com implements industry-accepted best practices to harden all underlying host computers that support the various software layers of the Force.com cloud platform. For instance, all hosts use Linux or Solaris distributions with non-default software configurations and minimal processes, user accounts, and network protocols. Host services never execute under root, and they log their activity in a remote, central location for safekeeping.

The underlying database layer of Force.com also plays a significant role in platform security. For example, the database protects customer passwords by storing them after applying an MD5 one-way cryptographic hash function, and supports the encryption of field data in custom fields. Salesforce.com enforces strict control of powerful database administrator access.

Force.com's innovative metadata-driven, multitenant database architecture delivers operational and cost efficiencies for cloud-based applications without compromising the security of each organization's data.

- When a user establishes a connection, Force.com assigns the session a client hash value.
- Along with the formation and execution of each application request, Force.com confirms that the user context (an organization ID, or orgID) accompanies each request and includes it in the WHERE clause of all SQL statements to ensure the request targets the correct organization's data. On the flip side, Force.com validates that every row in the return set of a database query matches the session's orgID.
- Before the rendering of a Web page that corresponds to an application request, Force.com confirms that the calculated client hash value matches the client hash value that was set during the login phase.

And finally, salesforce.com employs a number of sophisticated security tools that monitor platform activity in real time to expose many types of malicious events, threats, and intrusion attempts. For example, state-of-the-art intrusion detection systems (IDSs) detect some common types of external attacks. Force.com also monitors application and database activity and uses event management tools that actively correlate user actions and event data and then call attention to potential internal and external threats.

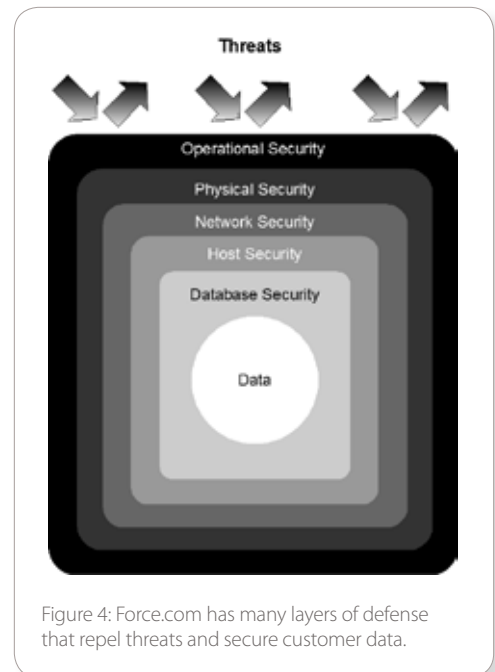


Figure 4: Force.com has many layers of defense that repel threats and secure customer data.



Figure 5: Force.com security monitors detect all types of suspicious activity and threats before they can cause harm.

Force.com cloud application security

Application providers that design, build, and manage platform applications are responsible for using and exposing the platform tools and features Force.com provides to ensure the ultimate security of the data their customers generate. This section introduces many of the Force.com features application providers and their customers can use to implement security policies governing exactly who, what, from where, when, and how users can access specific IT systems and data, along with related auditing requirements.

Force.com's default user authentication mechanism requests that a user provide a username and password (credentials) to establish a connection. Force.com does not use cookies to store confidential user and session information.

Many organizations use single sign-on mechanisms to simplify and standardize user authentication across a portfolio of applications. Force.com supports two single sign-on options:

- **Federated authentication single sign-on** using Security Assertion Markup Language (SAML) allows a session to send authentication and authorization data between affiliated but unrelated Web services.
- **Delegated authentication single sign-on** enables an organization to integrate Force.com cloud applications with an authentication method of choice, such as an LDAP (Lightweight Directory Access Protocol) service or authentication using a token instead of a password.

Force.com also offers several features to further confirm the identity of a connection request. For example, when a user requests a connection for the first time using a new computer-browser-IP address combination, the platform notices this fact, sends an email to the user, and requests that the user confirm his/her identity by clicking on the activation link in the email. The user's browser then maintains an encrypted cookie to expedite future connection requests.

User authentication and identity confirmation determines who can log in, and network-based security features limit where users can log in from and when. Force.com includes the ability to restrict the hours during which users can connect and the range of IP addresses from which they can connect. When an organization imposes IP address restrictions and a connection request originates from an unknown address, Force.com denies the connection request, thus helping to protect data from unauthorized access and "phishing" attacks.

To protect established sessions, Force.com monitors and terminates idle sessions after a configurable period of time. Force.com's session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting.

Login profiles give organizations an efficient way to manage system and application access for sets of similar users. First, an administrator creates a profile that controls access to entire applications, specific application tabs (pages), administrative and general user permissions, and object permissions (CRUD), along with other settings. Then, the administrator assigns each user a login profile. If the common requirements for a set of users change, all that's necessary is an update to the login profile for that group of users (not each individual user).

To enable users to do their jobs without exposing data they don't need to see, Force.com provides a flexible, layered sharing design that lets an organization expose specific application components and data sets to different sets of users.

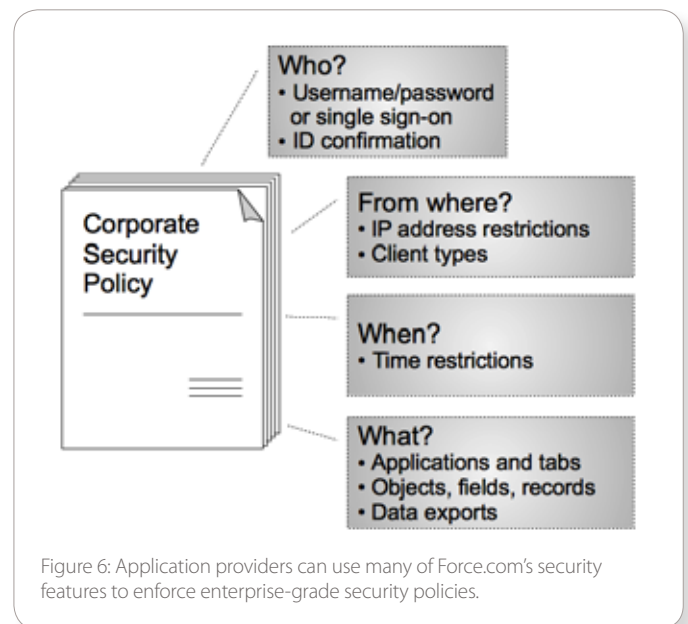


Figure 6: Application providers can use many of Force.com's security features to enforce enterprise-grade security policies.

- **User profiles** – An organization can control the access its users have to objects by customizing profiles. Within objects, organizations can then control the access users have to fields using field-level security. Sharing settings allow for further data access control at the record level.
- **Sharing settings** – Organization-wide default sharing settings provide a baseline level of access for each object and let the organization extend that level of access using hierarchies or sharing rules. For example, an organization can set the default access for an object to Private when users should only be able to view and edit the records they own, and then create sharing rules to extend access of the object to particular users or groups.
- **Sharing rules** – Sharing rules allow for exceptions to organization-wide default settings that give additional users access to records they don't own. Sharing rules can be based on the record owner or on field values in the record.
- **Manual sharing** – When individual users have specific access requirements, owners can manually share records. Although manual sharing is not automatic like organization-wide defaults, role hierarchies, or sharing rules, it lets record owners share particular records with particular users, as necessary.

By request, Force.com can also require users to pass a user verification test (CAPTCHA) to export data. This simple text-entry test helps prevent malicious automated programs from accessing an organization's data.

And finally, Force.com has a multitude of history tracking and auditing features that provide valuable information about the use of an organization's virtual private cloud of applications and data, which in turn can be a critical tool in diagnosing potential or real security issues.

Force.com cloud platform privacy

Since the dawn of the Digital Revolution, information privacy has become an increasingly important concern. Although computers and networking make it easy for legitimate people and organizations to quickly communicate and share vast quantities of information, the same technologies can also endanger the privacy of their data.

Privacy refers to an individual's ability to control how his or her information is collected, used, and disclosed. Data privacy in the context of technology and information systems most often concerns personal information (such as an individual's name, email address, and Social Security or Social Insurance number) or an organization's confidential information (such as employee records, customer lists, and sales data). This paper refers to individuals about whom personal information relates as the "data subjects."

Privacy laws and frameworks vary greatly in different countries and regions, but there are some common themes:

- **Notice** – Informing data subjects about the collection and use of their personal information.
- **Choice** – Providing options to data subjects about the collection and use of their personal information.
- **Access** – Providing data subjects the ability to review and correct their personal information.
- **Security** – Protecting personal information from various threats using reasonable safeguards.

The privacy of customer data is of paramount concern to salesforce.com. For example, previous sections of this paper explain the administrative, physical, and technical safeguards salesforce.com uses to protect the security, confidentiality, and integrity of data that resides on the Force.com platform. Additionally:

- The salesforce.com full Privacy Statement details what type of personal information salesforce.com collects about Force.com subscribers and how salesforce.com uses this information. For example, when a developer fills out a contact form for technical support, salesforce.com uses the contact information only to reply and nothing else.
- Force.com subscribers always have real-time access to their personal information through Web-based user account interfaces. Anyone with concerns about the privacy of personal information and data can contact salesforce.com's privacy department using a convenient [Contact Privacy questions form](#).

- The salesforce.com Privacy Statement is certified compliant with the highest independent, international, industry-accepted privacy standards. Certifications include TRUSTe Certified Privacy Seal, EU Safe Harbor (U.S. Dept. of Commerce, TRUSTe), and JIPDC (Japan Privacy Seal) that govern personal information and cross-border transfer of customer data.

Data privacy in the context of a cloud computing platform is somewhat unique in that the platform provider must address the privacy concerns of both its direct and indirect customers. For example, the data privacy of Force.com platform subscribers that build and deploy applications is just as important as the data privacy of end users who use platform applications. In the latter context, salesforce.com generally doesn't have a relationship with indirect customers, and therefore doesn't collect personal information on behalf of direct customers or determine how service providers use their data. Furthermore, salesforce.com's customer contracts generally prohibit salesforce.com from accessing or disclosing confidential customer data except under certain narrowly defined circumstances, such as when required by law.

And lastly, salesforce.com is transparent about platform security and privacy issues. Real-time system information is available at the company's "trust site" at <http://trust.salesforce.com>. Here, anyone can find live data on system performance, current and recent phishing and malware attempts, and tips on best security practices.

Conclusion: the world's largest enterprises trust Force.com

Conclusive proof that salesforce.com's commitment to securing its cloud services and maintaining the privacy of customer data is the ever-growing number of enterprises that place their trust in Force.com.

Visit www.salesforce.com/customers/ for a list of some of salesforce.com's customers, big and small, that trust salesforce.com to run their mission-critical operations.



For More Information

Contact your account executive to learn how we can help you accelerate your CRM success.

Corporate Headquarters

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

Global Offices

Latin America	+1-415-536-4606
Japan	+81-3-5785-8201
Asia/Pacific	+65-6302-5700
EMEA	+4121-6953700