FinancialForce Security Whitepaper

Introduction

FinancialForce.com provides enterprise cloud applications including Financial Management, Professional Services Automation (PSA), and Human Capital Management (HCM) (collectively referred to FinancialForce Applications). FinancialForce applications are built on the Force.com platform, a cloud computing platform provided by Salesforce. FinancialForce serves its clients (or “user entities”) from headquarters in San Francisco, California, USA, with EMEA headquarters in Harrogate, UK (also covers the Asia Pacific region). Founded in 2009 and headquartered in San Francisco, FinancialForce is backed by Salesforce, Technology Crossover Ventures, Unit4 and Advent International.

Customer Base

Our customers are in a wide range of verticals, some with stringent security requirements, including financial services, healthcare, technology, energy and government.

Security Overview

FinancialForce applications were designed from the ground up using core information security principles:

- Confidentiality: Prevent the disclosure of information to unauthorized individuals or systems.
- Integrity: Maintain and assure the accuracy and consistency of data over its entire lifecycle.
- Availability: Ensure the information is available when needed.

FinancialForce is committed to achieving and maintaining these principles and the trust of our customers. Integral to this is providing a robust security and privacy program that carefully considers security and data protection across our services, including data submitted by customers to our services (“customer data”).

Information Security Program

FinancialForce has a dedicated Security and Trust function that coordinates security policy, program and verification efforts, to ensure that customer and company information assets are adequately protected. Our Information Security Program includes identifying, evaluating and reporting on security risks, compliance with security and privacy regulations and commitments, threat and vulnerability management, and security incident management and response. FinancialForce has an Information Security Policy and Standards framework based on ISO 27001/27002 that describe standards, best-practice guidelines and approaches required to protect customer data and corporate assets (including people, information and infrastructure).

Commitment to Security

At FinancialForce, we understand that security, availability and application processing integrity are critical for our customers. FinancialForce is dedicated to providing industry-leading security for our customers' data assets through our Security and Trust program.

People

Everyone at FinancialForce, from the research and development staff to the executive team, is committed to security excellence. The company's Chief Information Security Officer (CISO) coordinates a cross-functional team of experts focused on security-related activities. FinancialForce also has a Senior Vice President and General Counsel with responsibility for compliance with global privacy laws. All employees receive regular information security awareness training that covers key security threats and risks and employee obligations to protect the security, confidentiality and privacy of customer and company data.

Processes

All key FinancialForce business processes, including development, support, operations, consulting, and monitoring processes, consider the security of our customer data.

Technology

We leverage industry-leading and proven secure platforms for our products and services. Each component of our technology infrastructure undergoes intensive scrutiny by multiple teams of security professionals.

Customers

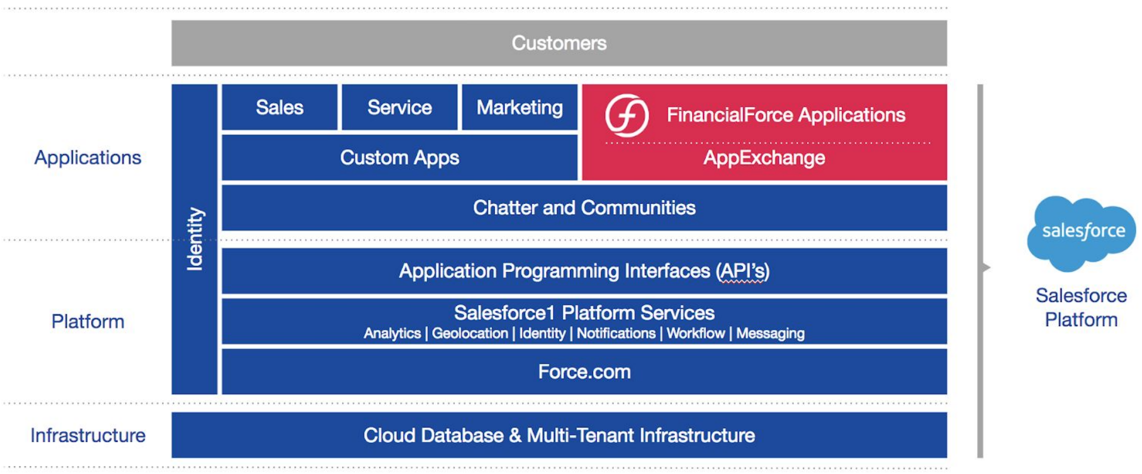
We consider our customers, partners, developers and internal users that interact with our systems to be within our security scope. Our security program is designed both to provide them a high degree of security assurance and to protect ourselves from threats they might present.

Built on Salesforce Platform

To support these principles, FinancialForce applications were developed on Force.com, an industry-leading and mature platform for cloud applications provided by Salesforce. FinancialForce applications are listed on AppExchange (Salesforce cloud applications marketplace) and use the Force.com cloud platform as the underlying technology, which includes tools for development, reporting, workflow authorizations, dashboards, social media (Chatter) and integration. All AppExchange applications go through a qualitative and quantitative review process to ensure applications meet a set of security standards and best practices.

By leveraging an industry-leading cloud platform for business applications, FinancialForce applications and our customers' data benefit from a variety of security features and controls in such areas as user management, access control, disaster recovery, backups, physical and network security. As a result, FinancialForce applications satisfy our customers' most stringent data security requirements, and comply with major security, privacy and data protection laws and standards globally.

FinancialForce Application & Salesforce Platform Architecture


Customers
Applications
Sales
Service
Marketing
FinancialForce Applications
AppExchange
Custom Apps
Chatter and Communities
Identity
Platform
Application Programming Interfaces (API's)
Salesforce1 Platform Services
Analytics | Geolocation | Identity | Notifications | Workflow | Messaging
Force.com
Infrastructure
Cloud Database & Multi-Tenant Infrastructure
salesforce
Salesforce Platform

For more information on Force.com, Salesforce compliance certifications and other security guidance please see the Salesforce Security Section below.

Shared Security Responsibility Model

Moving business processes and applications to the cloud creates a shared responsibility model between our customers, FinancialForce and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security.

FinancialForce

FinancialForce manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the FinancialForce applications.

Salesforce

Salesforce operates, manages and controls the components from the API level down to the host operating system, underlying databases and physical security of data centers in which the services operate. For details on Salesforce security, see trust.salesforce.com and search “security” on help.salesforce.com.

Heroku

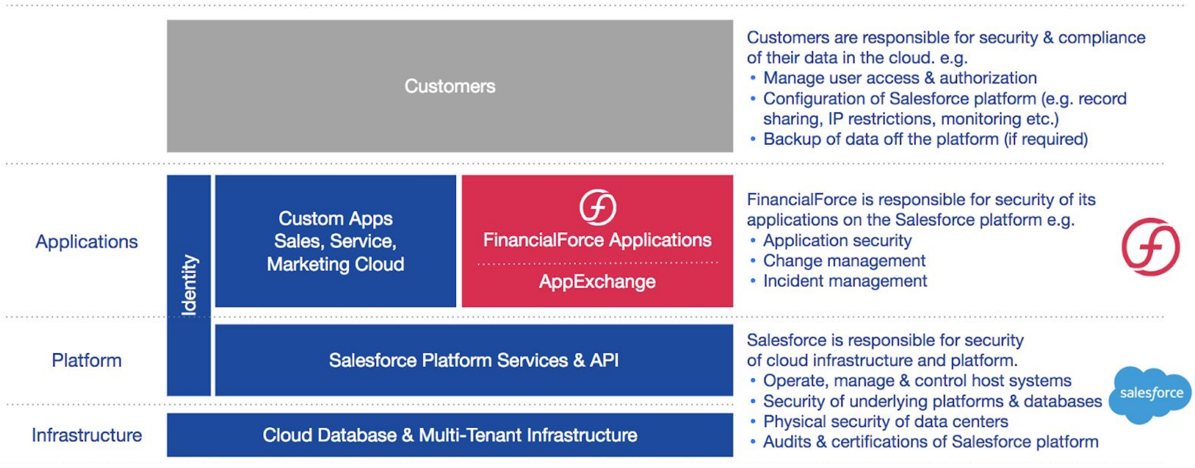
Certain FinancialForce products also use the Heroku platform, which is provided by Salesforce, to run computing operations in order to improve the performance and efficiency of background jobs. Customer data is not stored or logged in Heroku, and all customer data transferred between FinancialForce products and Heroku is encrypted-in-transit using a 256-bit TLS Certificate and 2048-bit RSA public key. We have implemented additional security enhancements to augment the security of the Heroku platform for our customers, including IP whitelisting, Web Application Firewall (WAF), multi-layer DDoS protection, and access logging and auditing.

Customers

Customers are responsible for user access and authorization, control and backup of data uploaded to the FinancialForce applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security their FinancialForce implementation and address security and compliance requirements by leveraging security features of the Force.com platform such as data encryption, IP-range restrictions, two-factor authentication, strong passwords and enforced periodic password changes.

FinancialForce recognizes that many companies are subject to regulations and standards governing security and handling of information, and therefore maintains a security program that covers policies, practices, people and technology. However, to use FinancialForce applications securely, customers must apply sound security practices to their configuration and any customization and integration of FinancialForce and the underlying Salesforce platform, including customers' design and implementation of related business processes.

Shared Security Responsibility Model


Customers
Applications
Identity
Custom Apps Sales, Service, Marketing Cloud
FinancialForce Applications
AppExchange
Platform
Salesforce Platform Services & API
Infrastructure
Cloud Database & Multi-Tenant Infrastructure
salesforce

Customers are responsible for security & compliance of their data in the cloud. e.g.

- Manage user access & authorization
- Configuration of Salesforce platform (e.g. record sharing, IP restrictions, monitoring etc.)
- Backup of data off the platform (if required)

FinancialForce is responsible for security of its applications on the Salesforce platform e.g.

- Application security
- Change management
- Incident management

Salesforce is responsible for security of cloud infrastructure and platform.

- Operate, manage & control host systems
- Security of underlying platforms & databases
- Physical security of data centers
- Audits & certifications of Salesforce platform

Example: FinancialForce provides applications and views for data entry and reporting, and the Salesforce Force.com platform provides authentication technology, but each customer must implement and monitor access and authorization controls (e.g., configuring administrators for managing privileged access, designing roles and processes for access to records, and enabling a field audit trail for monitoring user access to data).

Certifications and Attestations

FinancialForce.com Applications

Cloud Security Alliance

As part of our commitment to Trust, we have published a detailed description of our cloud security controls under the Cloud Security Alliance (CSA) STAR Level 1 - Self-Assessment program. This self-assessment uses the CSA Consensus Assessments Initiative Questionnaire to answer nearly 300 standardized questions that provide transparency into cloud vendor security practices and controls supporting their cloud service delivery and applications. You can access it here: https://cloudsecurityalliance.org/star/registry/financialforce

SSAE 16 SOC 1 Type II Report

As part of our commitment to trust and security, FinancialForce has invested in a Service Organization Control 1 (SOC 1) Type II report prepared by the global accounting firm Ernst & Young LLP. The report is prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. The purpose of the report is to provide our customers assurance that the FinancialForce Description of Services is fairly presented in all material respects, that controls put in place by FinancialForce are suitably designed to meet their control objectives, and that those controls were tested and operated effectively during the audit period.

Ernst & Young LLP created an Independent Service Auditors' Report after testing and evaluating FinancialForce applications against the following objectives:

Control Area	Description
Control Environment	Foundation for all other components of internal control, providing discipline and structure including control activities, policies and procedures that help make sure that management's directives are carried out.
Risk Assessment	Identification, analysis and management of relevant risks.
Monitoring	Processes to assess the quality of internal control performance.
Information and Communication	Systems that support the identification, capture and exchange of information that enables people to carry out their responsibilities.
IT General Controls	Defined policies, procedures and controls in place for supporting FinancialForce services.
Change Management	Controls for change initiation, prioritization and release management.
Development and Testing	Development and changes to production application systems are authorized, tested, approved and properly implemented.
Information Security Aspects	Information security policies and procedures for supporting user entities.
Incident Management	Incident monitoring, response, escalation and resolution.
Sub-Service Organizations	Usage of sub-service organizations for infrastructure support and management, physical security, environmental safeguards, and backup and recovery functions to maintain the information systems

Disaster Recovery and Business Continuity.	Disaster recovery and business continuity plan for unplanned, adverse events.

The SOC 1 report provides FinancialForce customers with the additional assurance that our applications are developed and delivered in accordance with transparent standards to ensure high-quality and secure products are deployed to our customers' environments.

Salesforce Certifications

As FinancialForce applications are developed and run natively on the Force.com platform, we benefit from various security controls designed and implemented by Salesforce. Salesforce undergoes comprehensive privacy and security assessments by, and has achieved certifications from, multiple auditors and certifying bodies. These include the following security- and privacy-related audits and certifications:

Geographical Recognition

- EU / EEA Binding Corporate Rules for Processors
- EU / EEA and Switzerland Safe Harbor self-certification through the U.S. Department of Commerce
- TRUSTe Certified Privacy Seal

Global Audit Compliance

- ISO 27001
- SSAE 16/ISAE 3402 SOC-1
- SOC 2
- SOC 3
- FedRAMP
- PCI-DSS
- TÜV Rheinland Certified Cloud Service

A current list of security and privacy assessments and certifications of the Salesforce platform can be found at https://trust.salesforce.com/trust/learn/compliance.

Security Controls

Product Security

Product Security Measures

FinancialForce's software development lifecycle incorporates a number of security measures, including:

- Code reviews designed to ensure adherence to FinancialForce development standards.
- Software security testing and code scanning to identify and address security vulnerabilities.
- Release reviews and approvals designed to ensure product releases comply with internal process requirements.
- Vulnerability testing and remediation for infrastructure and tools supporting our source code management platform.
- Development and changes to production application systems are authorized, tested, approved and documented.

Salesforce AppExchange Security Review

FinancialForce applications are submitted to Salesforce as part of the AppExchange Security Review process. Salesforce provides the AppExchange Security Review program to assess the security posture of ISV applications published on the AppExchange against industry best practices for security.

Application Controls

FinancialForce provides rigorous application controls that ensure your financial transactions have been correctly validated and reviewed prior to posting, have comprehensive audit trails and cannot subsequently be modified via “back door” manipulation of object data.

These application controls include:

- Comprehensive audit trails for transactions, master data modifications and security setup changes.
- Multi-level approval processes for transactions and master file data changes
- Segregation of duties
- Highly granular control of company, object, record and field level access by role

Disaster Recovery

Because FinancialForce applications are 100% Force.com-native, all data processed by FinancialForce applications resides on the Salesforce cloud platform owned, operated and managed by Salesforce. As part of its disaster recovery planning, FinancialForce, in collaboration with Salesforce, undertakes to ensure that the systems where customer data is stored have a disaster recovery facility that is geographically remote from its primary data center, along with required hardware, software, and Internet connectivity, in the event production facilities at the primary data center were to be rendered unavailable.

Change Management

FinancialForce follows fully documented change management procedures for all aspects of its software lifecycle, including application development, release management, service management and enhancement.

Incident Management

FinancialForce maintains security incident management policies and procedures, which include prompt notification of customers in the event FinancialForce becomes aware of an actual or reasonably suspected unauthorized use or disclosure of customer data.

Data Encryption

FinancialForce relies on Salesforce platform capabilities for encryption of data in transit. Salesforce uses industry-accepted encryption products to protect customer data and communications during transmissions between a customer's network and the FinancialForce applications, including 128-bit TLS Certificates and 2048-bit RSA public keys at a minimum. Additionally, customer data is encrypted during transmission between data centers for replication purposes.

Contacts

For security related questions please email us at security@financialforce.com

Additional Resources and Links

FinancialForce Security and Trust Website

https://www.financialforce.com/trust

FinancialForce Privacy and Data Protection

http://www.financialforce.com/company/cloud-erp/legal/data-processing-addendum/

FinancialForce Privacy Statement

http://www.financialforce.com/company/cloud-erp/legal/privacy-statement/

Salesforce Security and Trust Resources

https://trust.salesforce.com/

Salesforce Administrator Security Best Practices

http://content.trust.salesforce.com/trust/en/learn/bestpractices/

Salesforce Security Implementation Guide

https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/

Salesforce Security for IT Executives

s3.amazonaws.com/dfc-wiki/en/images/3/39/Salesforce_CRM_Security_for_the_IT_Executive.PDF

Salesforce Security Data Sheet

https://help.salesforce.com/servlet/servlet.FileDownload?file=01530000003SfNCAA0