# Security, Privacy and Architecture

Last updated: November 18, 2019

Confidential

# Table of Contents

# 1. FinancialForce Corporate Trust Commitment

FinancialForce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ("Customer Data").

# 2. Services Covered

This documentation describes the architecture of, the security- and privacy-related audits and certifications received for, the administrative, technical and physical controls applicable to, and the personal data typically submitted to, the following services.

## 2.1 Core Services

"Core Services" include

- the FinancialForce services branded as Financial Management ("FinancialForce FM"), Professional Services Automation ("FinancialForce PSA"), and Human Capital Management ("FinancialForce HCM") (together the "FinancialForce Applications");
- the Salesforce Force.com platform functionality within the scope of the OEM Embedded platform license as described in the OEM User License Comparison (the "Force.com Platform") and resold by FinancialForce with the FinancialForce Applications; and
- the Salesforce Heroku platform functionality utilized by certain FinancialForce FM functions (the "Heroku Platform").

## 2.2 Conga Applications

"Conga Applications" include the Conga Composer, Conductor, Workflow, Contracts, Sign, and Grid applications. FinancialForce makes the Conga Applications available to its customers as an authorized reseller of AppExtremes, LLC.

## 2.3 Integration Hub Connectors

“Integration Hub Connectors” are connectors that enable sharing of data between FinancialForce and third-party applications. FinancialForce makes the Integration Hub Connectors available to its customers as an authorized reseller of Cloud Elements Inc.

# 3. Core Services

## 3.1 Data Segregation

The Core Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific tenants ("Organization IDs") and allows the use of customer and user role-based access privileges. Additional data segregation is available from FinancialForce or Salesforce in the form of separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the Infrastructure and Sub-processors documentation.

## 3.2 Hybrid Platform Architecture (FinancialForce FM Only)

FinancialForce PSA and FinancialForce HCM are built and operate exclusively on the Force.com Platform.

FinancialForce FM is built and operates primarily on the Force.com Platform. However, certain FinancialForce FM features – currently the Reporting and Payments Plus (Pilot) features within the Accounting module of FinancialForce FM – also utilize the Heroku Platform to run computing operations. These features use the Heroku Platform only for processing, not for storage, of Customer Data.

All Customer Data entered into FinancialForce Applications is stored on the Force.com Platform.

## 3.3 Control of Processing

FinancialForce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by FinancialForce and its subprocessors. FinancialForce has entered into written agreements with its subprocessors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities.

Compliance with such obligations, as well as the technical and organizational data security measures implemented by FinancialForce, is subject to regular audits. The "Infrastructure and Sub-processors" documentation describes the subprocessors and certain other entities material to FinancialForce's provision of the Core Services.

## 3.4 Audits and Certifications

### 3.4.1 FinancialForce Applications

The following security and privacy-related audits and certifications apply to the FinancialForce Applications:

- **EU-U.S. and Swiss-U.S. Privacy Shield certification:** Customer Data submitted to FinancialForce FM is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "FinancialForce."
- **Service Organization Control (SOC) 1 report:** FinancialForce's information security control environment applicable to FinancialForce FM undergoes an independent evaluation in the form of a SOC 1 (SSAE 18 / ISAE 3402) audit. FinancialForce's most recent SOC 1 (SSAE 18 / ISAE 3402) report is available upon request from your organization's FinancialForce account executive.
- **Cloud Security Alliance STAR Self-Assessment:** FinancialForce has made available a 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.

### 3.4.2 Force.com Platform

The following security and privacy-related audits and certifications apply to the Force.com Platform:

- **Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the Force.com Platform as part of the Core Services is within the scope of the Salesforce BCR for Processors (except when hosted on the Public Cloud Infrastructure). The most current version of the Salsforce BCR for Processors is available on Salesforce's website, currently located at http://www.trust.salesforce.com.

- **EU-U.S. and Swiss-U.S. Privacy Shield certification:** Customer Data submitted to the Force.com Platform as part of the Core Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in Salesforce's Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce."
- **ISO 27001/27017/27018 certification:** Salesforce operates an information security management system (ISMS) for the Force.com Platform in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's FinancialForce account executive.
- **Service Organization Control (SOC) reports:** Salesforce's information security control environment applicable to the Force.com Platform undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available upon request from your organization's FinancialForce account executive.
- **TRUSTe certification:** Salesforce has been awarded the TRUSTe Certified seal signifying that Salesforce's Website Privacy Statement and privacy practices related to the Force.com Platform have been reviewed by TRUSTe for compliance with TRUSTe's Certification Standards.

### 3.4.3 Heroku Platform

The following security and privacy-related audits and certifications apply to the Heroku Platform:

- **EU-U.S. and Swiss-U.S. Privacy Shield certification:** Customer Data submitted to the Force.com Platform as part of the Core Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in Salesforce's Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce."
- **TRUSTe certification:** Salesforce has been awarded the TRUSTe Certified seal signifying that Salesforce's Website Privacy Statement and privacy practices related to

the Heroku Platform have been reviewed by TRUSTe for compliance with TRUSTe's Certification Standards.

- **ISO 27001/27017/27018 certification:** Salesforce operates an information security management system (ISMS) for the Heroku Platform in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party. The scope of Salesforce's ISO 27001/27017/27018 certification applicable to the Heroku Platform is available here.
- **Service Organization Control (SOC) reports:** Salesforce's information security control environment applicable to the Heroku Platform undergoes an independent evaluation in the form of a SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available by logging a support ticket via https://help.heroku.com.

As further described in the Infrastructure and Sub-processors documentation, the infrastructure used to host Customer Data submitted to the Heroku Platform is provided by AWS. Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

## 3.5 Vulnerability Assessments

The Core Services undergo infrastructure and application vulnerability assessments, including penetration testing, by internal and external personnel.

## 3.6 Security Controls

### 3.6.1 Force.com Platform

All FinancialForce applications are built and run natively on the Force.com Platform. The Force.com Platform includes a variety of configurable security controls that allow customers to tailor the security of the Force.com Platform for their own use. Information on Force.com Platform configurable security controls available as part of the FinancialForce Applications can be found in the Salesforce Security Implementation Guide.

### 3.6.2 Heroku Platform (used by FinancialForce FM for certain operations)

As described above under Hybrid Platform Architecture, FinancialForce FM performs certain computing operations on the Heroku Platform. Application code deployed to the

Heroku Platform runs within its own isolated environment that cannot be accessed by other applications or areas of the Heroku Platform. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory and the file system using Linux Containers (LXC) while host-based firewalls restrict applications from establishing local network connections. Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

FinancialForce maintains additional security controls for the Heroku Platform beyond those provided by Salesforce and AWS. These controls include an additional Web application firewall, protections against denial-of-service attacks and malicious bots, and rejection of connections to the Heroku Platform not originating from the Force.com Platform.

## 3.7 Security Policies and Procedures

### 3.7.1 All Core Services

The following security policies and procedures apply to all of the Core Services:

- Customer passwords are stored using a one-way salted hash.
- Passwords are not logged.

### 3.7.2 Force.com Platform (core platform for FinancialForce Applications)

The following security policies and procedures apply to the Force.com Platform for all FinancialForce Applications, except FinancialForce FM computing operations performed on the Heroku Platform:

- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP. If there is suspicion of inappropriate access, customers can request log entry records and/or analysis of such records to assist in forensic analysis when available. This service is available to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Certain administrative changes to the Core Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Trail" and are

available for viewing by a customer's system administrator. Customers may download and store this data locally.

- FinancialForce personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

### 3.7.3 Heroku Platform (used by FinancialForce FM for certain operations)

The following security policies and procedures apply to computing operations performed by FinancialForce FM on the Heroku Platform:

- User access log entries will be maintained, containing date, time, user ID, resource accessed, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP. If there is suspicion of inappropriate access, customers can request log entry records and/or analysis of such records to assist in forensic analysis when available. This service is available to customers on a time and materials basis.
- Salesforce personnel will not set a defined password for a user. If a user requests a password reset, Salesforce will deliver a temporarily valid, secret URL to the requesting user via email. A new password is set by visiting this URL.

## 3.8 Intrusion Detection

The Core Services are monitored for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. FinancialForce and Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the services function properly.

## 3.9 Security Logs

Systems used in the provision of the Core Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

## 3.10 Incident Management

FinancialForce maintains security incident management policies and procedures. FinancialForce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by FinancialForce or its sub-processors of which FinancialForce becomes aware to the extent permitted by law. Salesforce publishes system status information for the Force.com Platform and Heroku Platform on the Salesforce Trust and Heroku websites, respectively.

## 3.11 User Authentication

Access to Core Services requires authentication via one of the supported mechanisms as described in the Salesforce Security Implementation Guide, including user ID/password, SAML based Federation, Oauth, Social Login, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

## 3.12 Physical Security

Production data centers have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

## 3.13 Reliability and Backup

### 3.13.1 Force.com Platform (core platform for FinancialForce Applications)

All networking components, network accelerators, load balancers, Web servers and application servers are in a redundant configuration. All Customer Data submitted to the Core Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the Core Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Core Services, up to the last committed

transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis. Any backups are verified for integrity and stored in the same data centers as their instance. The foregoing replication and backups may not be available to the extent any of the FinancialForce Application managed packages is uninstalled from Customer's Salesforce instance, or "org," during the subscription term because doing so may delete Customer Data submitted to such services without any possibility of recovery.

### 3.13.2 Heroku Platform (used by FinancialForce FM for certain operations)

FinancialForce FM components and configurations deployed on the Heroku Platform, up to the last committed transaction, are automatically replicated on a near real-time basis at the database layer and are backed up as part of the deployment process on secure, access controlled, and redundant storage. Customer Data is not stored, and is therefore not backed up on, the Heroku Platform.

## 3.14 Disaster Recovery

### 3.14.1 All Core Services

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The Core Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event FinancialForce production facilities at the primary data centers were to be rendered unavailable. Disaster recovery plans are in place and are tested at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

### 3.14.2 Force.com Platform (does not apply to FinancialForce FM processes that run on Heroku Platform)

The disaster recovery plans covering the Force.com Platform currently have the following target recovery objectives: (a) restoration of the Covered Service (recovery time objective) within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments, such as the Sandbox service.

## 3.15 Malware

FinancialForce and Salesforce implement practices and software to limit the risk of exposure to malware. The Core Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Core Services by a customer. Uploaded attachments, however, are not executed in the Core Services and therefore will not damage or compromise the Core Services by virtue of containing a virus.

## 3.16 Data Encryption

### 3.16.1 Encryption in Transit

The Core Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Core Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum. Additionally, Customer Data is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

### 3.16.2 Encryption at Rest

For customers that have purchased Salesforce Platform Encryption, encryption at rest is available for the following fields:

| FinancialForce Application | Fields Encryptable at Rest |
|---|---|
| FinancialForce FM | |
| Accounting Module | All Salesforce standard object fields except Opportunity object fields |
| Revenue Management Module | All Salesforce standard object and FinancialForce object fields |
| Billing Central Module | All Salesforce standard object fields except Opportunity object fields |
| Reporting Module | All Salesforce standard object fields except Opportunity object fields |
| FinancialForce PSA | Contact Name and Account Name fields |

Salesforce Platform Encryption uses AES-256 bit encryption.

## 3.17 Return of Customer Data

Customers may export their Customer Data weekly using the Force.com Platform Weekly Export Service feature.

Within 30 days after contract termination, a customers may request return of their Customer Data submitted to the Core Services (to the extent such data has not been deleted by Customer). FinancialForce shall cause such Customer Data to be provided via a downloadable file in comma separated value (.csv) format and attachments in their native format. Note that Customer Data submitted by Customer to Core Service features utilizing Einstein Analytics for analysis is derived from other data to which Customer has access, for example, data stored by Customer using FinancialForce Financial Management or PSA, or Salesforce Sales Cloud or Service Cloud. The foregoing return of Customer Data for managed packages may not be available if the packages were removed prior to contract termination.

Please note that if a customer's contract with FinancialForce Applications terminates but the customer maintains an ongoing contract with Salesforce, then ***Customer Data held in FinancialForce Application objects will be immediately and permanently deleted if the corresponding FinancialForce managed package is uninstalled***. Therefore, if a customer's contract with FinancialForce Applications terminates and the customer maintains an ongoing contract with Salesforce, and the customer desires a return of its Customer Data, the customer should request such return within 30 days after termination of its FinancialForce contract and should not uninstall any FinancialForce managed packages until the Customer Data has been returned to the customer.

## 3.18 Deletion of Customer Data

### 3.18.1 If FinancialForce Subscriptions Terminate and Customer Has No Continuing Salesforce Subscriptions

If all of a customer's FinancialForce Application subscriptions terminate, and the customer does *not* have an existing Salesforce subscription that continues after termination of its FinancialForce subscriptions, then after such termination, Customer Data submitted to the Core Services is retained in inactive status within the Core Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days.

Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Salesforce uses to host Customer Data unless the media is at

the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

| Day 0, subscription terminates | Day 0 - 30 | Day 30 - 120 | Day 121 - 211 | Day 121 - 301 |
|---|---|---|---|---|
| | Data available for return to customer | Data inactive and no longer available | Data deleted or overwritten from production | Data deleted or overwritten from backups |

Without limiting the ability for customers to request return of their Customer Data submitted to the Core Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. FinancialForce will update this Security, Privacy and Architecture Documentation in the event of such a change.

### 3.18.2 If FinancialForce Subscriptions Terminate and Customer Has Continuing Salesforce Subscriptions

If all of a customer's FinancialForce Application subscriptions terminate, and the customer *has* an existing Salesforce subscription that continues after termination of its FinancialForce subscriptions, then after such FinancialForce subscription termination, Customer may obtain an export of the Customer Data by submitting a request to FinancialForce for such an export within 30 days after the subscription termination date. Thereafter, Customer Data stored in FinancialForce Application objects will remain securely and inaccessibly stored in the Salesforce Platform until the corresponding FinancialForce Application packages are removed from that Salesforce instance. Removal of the FinancialForce Application packages will result in immediate deletion from Force.com Platform servers. The customer may engage FinancialForce to assist with such package removal pursuant to a signed statement of work. Termination of the customer's FinancialForce Application subscriptions will not trigger deletion of Customer Data stored in Salesforce standard objects if the customer has a continuing Salesforce subscription. All Customer Data associated with the customer's Salesforce instance, whether stored in FinancialForce Application objects or Salesforce standard objects, will be deleted following termination or expiration of all FinancialForce, Salesforce and other third party subscriptions associated with the Salesforce instance, in accordance with timetable in Section 3.18.1 above.

Without limiting the ability for customers to request return of their Customer Data submitted to the Core Services, FinancialForce reserves the right to reduce the number of days it retains such data after contract termination. FinancialForce will update this Security, Privacy and Architecture Documentation in the event of such a change.

## 3.19 Sensitive Data

Customers may not submit payment card data, payment card authentication data, credit or debit card numbers, or any security codes or passwords to the Core Services (other than submission of security codes and/or passwords as part of the user login process).

Customers may not submit Protected Health Information, as defined under the U.S. Health Insurance Portability and Accountability Act, to FinancialForce FM, or to the Salesforce Public Cloud Infrastructure.

For clarity, the foregoing restrictions do not apply to financial information provided to FinancialForce for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by FinancialForce's website Privacy Statement.

## 3.20 Analytics

FinancialForce and Salesforce may track and analyze the usage of the Core Services for purposes of assisting customers, security, and improving the Core Services and the user experience in using the Core Services. For example, FinancialForce and Salesforce may use this information to help customers derive more value from their purchase of the Core Services, to understand and analyze trends, or to track which features are used most often in order to improve the Core Services. FinancialForce and Salesforce may share anonymous usage data with their service providers for the purpose of helping FinancialForce and Salesforce in such tracking, analysis and improvements. Additionally, FinancialForce and Salesforce may share such anonymous usage data on an aggregate basis in the normal course of operating their business; for example, FinancialForce and Salesforce may share information publicly to show trends about the general use of their services.

## 3.21 Personal Data Processed in FinancialForce Applications

FinancialForce customers choose what data to submit to FinancialForce Applications. The types of personal data typically submitted to each of the applications are listed below.

### 3.21.1 FinancialForce FM

Types of personal data typically submitted to FinancialForce FM include:

- name,
- title,

- address,
- phone number, and
- email address.

In addition, the Contacts object on the Account for customer/vendor/partner/investor/any party includes “sentiment” information for individual contacts (adversary, advocate, or neutral).

### 3.21.2 FinancialForce PSA

Types of personal data typically submitted to PSA include:

- name,
- email address,
- telephone number,
- business travel and expense information,
- professional certifications/qualifications,
- utilization information, and
- skills ratings.

In addition, the Contacts object on the Account for customer/vendor/partner/investor/any party includes “sentiment” information for individual contacts (adversary, advocate, or neutral).

### 3.21.3 FinancialForce HCM

FinancialForce HCM requires first and last name for each employee. All other personal data is optional through configuration of HCM, including the following categories:

- address and address history,
- phone numbers and phone history,
- ethnicity*,
- date of birth,
- blood type*,
- disability status*,
- emergency contacts full name, address, and phone,
- certifications and related identification numbers,
- email addresses (work and personal),

- national identification numbers (US SSN, Canada SIN, etc.),
- dependent / beneficiaries first name, last name, national ID, date of birth,
- benefits enrollment information,
- pension contribution information,
- bank account information,
- Twitter, Facebook, LinkedIn identifications,
- proof of citizenship documents for US Form I-9,
- tax withholding information related to US Form W-4,
- absence history,
- information related to extended leave, such as notes from doctors*,
- candidate information, including full name, address, education and work history, email address and disability status,
- job/position history,
- salary history,
- bonus history,
- equity history
- allowance history,
- performance reviews (including competencies and ratings as part of performance reviews),
- ad hoc feedback provided by managers or fellow employees, and
- professional / personal goals either part of performance review or standalone.

* May be considered sensitive personal data under EU General Data Protection Regulation.

# 4. Conga Applications

Conga Applications are provided by AppExtremes, LLC (“Conga”) and resold by FinancialForce. Conga’s security documentation is available here.

Conga Composer and Sign process data outside the Salesforce platform. Conga Composer extracts data from the customer’s Salesforce org, processes the data and Conga Composer templates in memory on Amazon Web Service (“AWS”) servers, and returns the merged data to Conga Composer in the customer’s Salesforce org. Conga Composer does not store the processed data on the AWS server. Conga Sign is a composite application on the Salesforce platform, with processing managed on AWS.

# 5. Integration Hub Connectors

Integration Hub Connectors are provided by Cloud Elements Inc. (“Cloud Elements”) and resold by FinancialForce. Cloud Elements’ security documentation is available here.

Integration Hub Connectors process and store data on AWS, and transmit data to and from the third-party applications to which they are designed to connect.