GOVERNMENT CLOUD PLUS SECURITY WHITEPAPER

JUNE 2020

Contents

Overview.....01

1: Salesforce Government Cloud Plus.....04

Services and Features.....05

Principles of Trust.....06

2: Salesforce Compliance Maturity.....08

Federal Risk and Authorization Management Program (FedRAMP).....09

Department of Defense (DoD).....10

3: Security and Compliance.....12

Information Security Governance.....12

Shared Security and Compliance Model.....13

Platform Security.....14

Qualified Personnel.....15

Multi-tenancy.....15

4: Controls and Database Security.....18

Physical and Environmental Controls.....18

Network Protection.....20

Logical Access Controls.....21

Configuration and Change Management.....22

Database Security.....22

Operational Monitoring.....23

Security Monitoring.....23

Incident Response.....24

Disaster Recovery and Backup.....25

Media Protection and Sanitization.....25

Platform and Application Security.....26

Logical Security.....30

5: Data Ownership and Retention.....32

Data Ownership and Retention.....32

Protecting PII and Privacy.....32

6: Additional Considerations.....36

State and Local Governments.....36

Government Contractors.....37

Conclusion.....39

Overview

Federal, state, and local government organizations, along with government contractors, trust Salesforce to deliver critical business applications, in large part because of Salesforce's commitment to security and privacy.

This white paper provides an overview of Salesforce's principles of trust and compliance specifically for Salesforce Government Cloud Plus in the context of Federal Risk and Authorization Management Program (FedRAMP) and the Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG). Subsequent sections introduce the security and privacy features inherent to Salesforce Government Cloud Plus that customers can use to build and secure their applications and customer data. The security and privacy features that help achieve compliance with required controls are derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" and are referenced in brackets throughout this white paper. Please note that this is not an exhaustive mapping and is intended to be illustrative for the purposes of this white paper. A detailed mapping of Salesforce's control requirements is available in our Control Implementation Summary (CIS) document.

01

Salesforce Government Cloud Plus

Background

Salesforce Government Cloud Plus

To support the security and compliance needs of our U.S. public sector customers, Salesforce launched Salesforce Government Cloud Plus. Government Cloud Plus is a dedicated instance of Salesforce's industry-leading Platform as a Service (PaaS) and Software as a Service (SaaS) multi-tenant public cloud infrastructure specifically isolated for use by U.S. federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host Customer Data submitted to Salesforce Government Cloud Plus Covered Services. Salesforce Government Cloud Plus is located in the Amazon Web Services (AWS) GovCloud (West) region.

Government Cloud Plus Services

Government Cloud Plus information system and authorization boundary is comprised of the following Salesforce services:

- Lightning Platform
- Sales Cloud
- Service Cloud
- Community Cloud
- Einstein Analytics Platform

Service Features

- Salesforce Files
- Ideas
- Knowledge
- Chatter / Chatter Answers
- Salesforce Mobile / mySalesforce
- Live Agent
- Salesforce Sites
- Salesforce Surveys
- Lightning Scheduler
- Salesforce Shield[1]: Platform Encryption, Event Monitoring, and Field Audit Trail
- Salesforce Industry Applications: Health Cloud and Financial Services Cloud

For more information on Salesforce Government Solutions please see:
www.salesforce.com/solutions/industries/government/overview/

[1] For additional information on Salesforce Shield, please see: https://www.salesforce.com/products/platform/products/shield/

Principles of Trust

Salesforce's vision is to be the government's trusted cloud PaaS and SaaS provider, based on the values of maintaining confidentiality, integrity, and availability of customer data. Salesforce's methods to fulfill this vision are built upon an executive commitment to maintain and continuously improve the security of Government Cloud Plus and include:

Defense-in-depth

Whenever possible, multiple controls and technologies are applied to limit the possibility of any single point of failure.

Investment

To manage, analyze, and improve security effectiveness, invest in personnel, tools, and technologies

Transparency

Trust cannot be maintained without open communications regarding service performance and reliability. Salesforce strives to be the industry leader in transparency. Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:

- Up-to-the minute information on planned maintenance
- Information on Salesforce detected Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

02

Salesforce Compliance Maturity

Salesforce Compliance Maturity

As a leading PaaS and SaaS provider, data security and compliance are paramount for Salesforce. Salesforce serves over 150,000 customers and processes over five billion transactions per day. The organizations that use Salesforce include customers in heavily regulated industries such as financial services, healthcare, insurance, and public sector that require strict adherence to security and privacy requirements. To meet the compliance needs of these customers, Salesforce continually raises the bar of security.

Salesforce undergoes System and Organization Controls (SOC) 1 examinations semi-annually and also completes SOC 2 and SOC 3 for Service Organizations audits. In May 2008, Salesforce became the first publicly traded SaaS vendor to receive the prestigious ISO/IEC 27001 Security Certification (ISO 27001) company-wide and service-wide, addressing applicable controls including our data centers and major offices worldwide. Since then, Salesforce has obtained ISO 27017 and 27018 certifications. As the only internationally accepted security standard, ISO 27001 ensures security best practices and a managed approach to business information protection, and helps Salesforce provide a consistent, reliable and secure operating environment to its customers worldwide. In May 2014, Salesforce achieved its first FedRAMP Provisional Authority to Operate (P-ATO) at the moderate impact level issued by the Department of Health and Human Services (HHS) for the Salesforce Government Cloud[2]. In May 2020, Salesforce received a Provisional Authority to Operate (P-ATO) at the High impact level issued by the FedRAMP Joint Authorization Board (JAB)[3] for the Salesforce Government Cloud Plus.

[2] See the FedRAMP Marketplace at: https://marketplace.fedramp.gov/#/product/salesforce-government-cloud

[3] See the FedRAMP Marketplace at: https://marketplace.fedramp.gov/#/product/salesforce-government-cloud-plus

Federal Risk and Authorization Management Program (FedRAMP)

Salesforce's information security program for Government Cloud Plus is aligned with the FedRAMP requirements at the High impact level.

To obtain compliance with FedRAMP, Salesforce is conducting security assessment and authorization activities in accordance with FedRAMP guidance and NIST SP 800-37h. Salesforce documented a System Security Plan (SSP) in accordance with NIST SP 800-18 for Government Cloud Plus service offering. The SSP identifies control implementations for Government Cloud Plus and in-scope customer-facing products according to the FedRAMP High baseline. In accordance with NIST SP 800-53A and FedRAMP High requirements, a third-party assessment organization (3PAO) conducted a security assessment of Government Cloud Plus. The security assessment testing determined the adequacy of the security controls used to protect the confidentiality, integrity, and availability of Government Cloud Plus and the customer data it stores, transmits, and processes.

To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring, which includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and annual independent assessments of all security controls.

Department of Defense (DoD)

Based on the Defense Information Systems Agency (DISA) decision[4] to streamline cloud authorizations and grant DoD Impact Level 2 (IL2) reciprocity to Cloud Service Offerings (CSOs) authorized at the FedRAMP Moderate baseline or higher, customers may use Government Cloud Plus for IL2 use cases. This includes storing / processing low sensitivity Personally Identifiable Information (PII) within Government Cloud Plus as approved by DISA's CC SRG interim guidance regarding PII[5].

[4] See https://www.disa.mil/NewsandEvents/2019/cloud-authorizations

[5] See https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/CC_SRG-PII-PHI_in_the_Cloud_and_PII_at_Level_2_v1.1.zip

03

Security and Compliance

Security and Compliance

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. Salesforce's approach to information security governance is structured around the ISO 27001/27002 framework and consistent with the requirements identified in NIST SP 800-53, and includes many components:

- **Employees** – Employees receive annual information security training. Employees in positions with logical access receive additional role-based training specific to their roles [AT-2, AT-3].
- **Security Staff** – Salesforce has dedicated security staff and teams supporting the system [PM-2].
- **Counsel** – Salesforce has a team of Privacy Counsel, Compliance, and Government Contracts Attorneys who are responsible for ensuring compliance with global privacy laws, international regulatory regimes, and federal procurement regulations.
- **Assessments** – Salesforce regularly conducts both internal vulnerability assessments (for example, architecture reviews by security professionals, vulnerability scans) as well as external third-party audits and external vulnerability assessments [RA-5, SI-2]. Beyond what FedRAMP requires, Salesforce conducts full scope audits every year, which gives us better assurance that the controls are implemented and operating effectively.
- **Policies and Procedures** – Detailed internal Salesforce Security Standards dictate how Salesforce handles various aspects of the security and compliance governance. Examples include: Security Incident Response Plan, Salesforce: Access Management Standard, Configuration Management Plan, etc. [IR-1, AC-1, CM-1]

In particular, Salesforce incorporates security into its development processes at all stages through the Salesforce Secure Development Lifecycle. Further, Salesforce has integrated a Product Security team in all stages of the secure development lifecycle. From initial architecture considerations to post-release, all aspects of software development incorporate security. The following describes some of the standard practices Salesforce employs, which help make it the trusted provider that it is today.

- **Design phase** – Guiding security principles and security training help ensure Salesforce engineers make the best security decisions possible. Security representatives are present during sprint reviews and help define security requirements. Threat assessments on high-risk features help to identify potential security issues early in the development lifecycle [SA-3, SA-8].
- **Development phase** – Defined security requirements for high-risk features are incorporated in feature development. Salesforce addresses standard vulnerability types through the use of secure coding patterns and anti-patterns, and uses static code analysis tools to identify security flaws [SA-10]. Secure code development during design, development, and release is controlled through a secure code repository.
- **Testing phase** – Internal Salesforce staff and independent security consultants use scanners and proprietary tools along with manual security testing to identify potential security issues. Further, releases and changes are analyzed in a dedicated test environment [SA-11].
- **Prior to release** – Salesforce Security leadership provides sign-off for each release once all security bugs are either closed or have an approved exception. New functionality is verified to ensure security requirements have been met. Code is tested and approved prior to release. Post-release, Salesforce uses independent security service providers to analyze and monitor the product for potential security issues. Reports on these findings are made available to prospects and customers under a non-disclosure agreement [SA-11].

Shared Security and Compliance Model

With Salesforce PaaS and SaaS, data security and compliance are a shared responsibility with customers. While Salesforce provides secure and compliant services to protect customer data and applications, customers are ultimately responsible for properly configuring and operating those services as required by their organization.

As depicted in the figure that follows, with legacy on-premise systems, organizations have sole responsibility for maintaining the security and compliance of the entire IT stack. This can drain resources and prevent ongoing IT modernization. It can also introduce risk and impact compliance. While Infrastructure as a Service (IaaS) may alleviate some burden, organizations still need to upgrade and patch software, worry about dependencies within the stack, and independently implement many security controls.

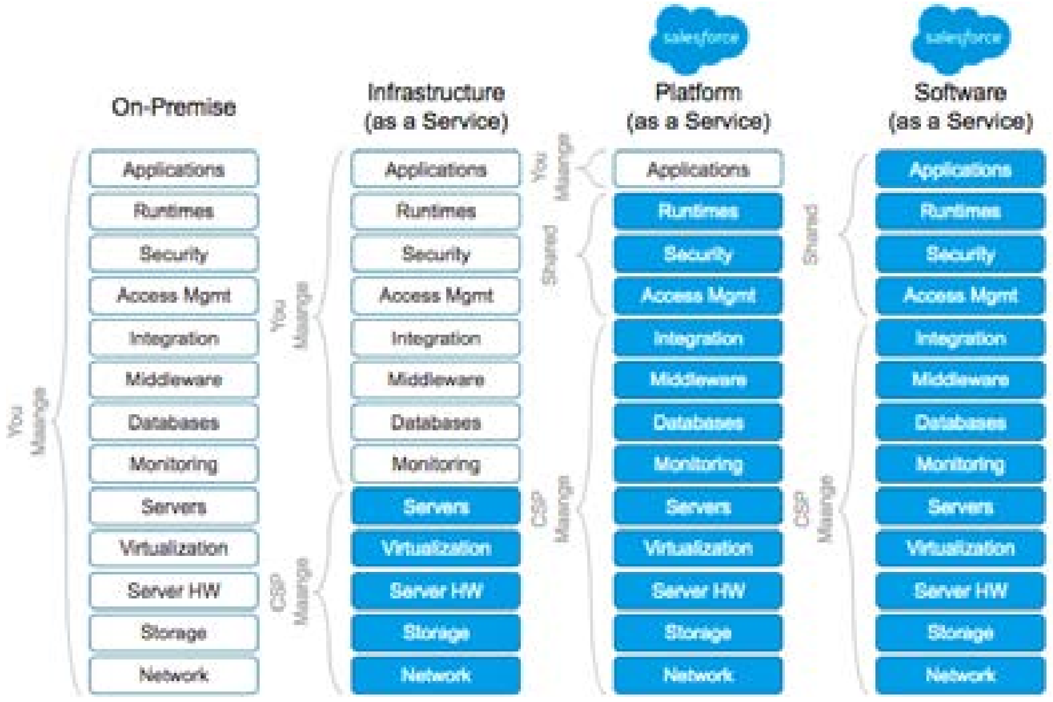


Figure: Delivery Models

With Salesforce, customers inherit the majority of security controls from Salesforce and AWS. While customers do bear some responsibility for ensuring security and compliance, Salesforce provides numerous enablement resources, including training and implementation guides. Specifically, for customers seeking compliance with FedRAMP High or DoD IL2, Salesforce provides a Customer Configuration Guide tailored to those requirements. This shared responsibility model greatly reduces both risk and burden for customers, allowing them to place more focus on their business and mission.

Platform Security

The figure below illustrates the many layers of defense Government Cloud Plus uses to resist various types of threats and achieve compliance with security frameworks such as DoD IL2, FedRAMP High, SOC 1, SOC 2, SOC 3, and ISO 27001 – all without sacrificing application performance.

Salesforce strictly manages access to Government Cloud Plus. Before being granted access, employees must pass a thorough Salesforce background check [PS-3]. After a person is authorized for logical access,

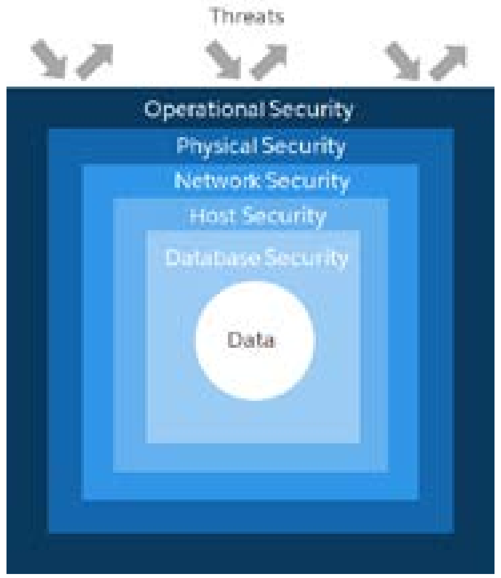


Figure: Salesforce incorporates security at multiple layers to protect against threats they can access the production network using secure methods, such as private networks, stringent segregation of duties, and least privilege [AC-2, AC-5, AC-6, IA-2]. With respect to physical security, Salesforce uses infrastructure provided Amazon Web Services, Inc. ("AWS"), to host Customer Data submitted to Government Cloud Plus Covered Services.

Qualified Personnel

Salesforce enforces usage conditions for all personnel with access to Government Cloud Plus. Specifically, all personnel must successfully undergo a Salesforce background investigation, be U.S. citizens (sole citizenship only), and are required to access Government Cloud Plus from U.S. soil. Further, in order to obtain production access to the Government Cloud Plus, all personnel must go through an enrollment and identity proofing process in accordance with NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing Requirements. Proofing is performed at Identity Assurance Level 3 (IAL3) prior to activation of user authenticators for Government Cloud Plus access [IA-2, PS-2].

Multi-Tenancy

The Salesforce service is delivered using a multi-tenant model. The multi-tenant architecture and secure logical controls address separation of customer data.

The Salesforce infrastructure is divided into a modular architecture based on "instances." Each instance is capable of supporting multiple customers in a secure and efficient manner. Salesforce uses the instance architecture to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's implementation of Salesforce from being compromised. This functionality has been designed and undergoes robust testing through an ongoing process by both Salesforce and its customers [AC-2, SC-4].

04

Controls and Database Security

Controls and Database Security

Physical and Environmental Controls

Salesforce uses infrastructure provided by a third party, Amazon Web Services, Inc. (“AWS”), to host Customer Data submitted to the Government Cloud Plus Covered Services. Each customer's instance is hosted from a primary and secondary site, with near real-time replication occurring between the two sites. There are currently two sites supporting the Services delivered on AWS public cloud infrastructure.

Salesforce inherits all physical and environmental controls from the pre-existing AWS GovCloud FedRAMP JAB P-ATO. AWS GovCloud (US), has been granted a JAB P-ATO for the high impact level. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at high baseline security categorization can be found within AWS Services in Scope by Compliance Program **(https://marketplace.fedramp.gov/#/product/aws-govcloud?sort=productName&productNameSearch=AWS)**.

Data centers are monitored using AWS global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

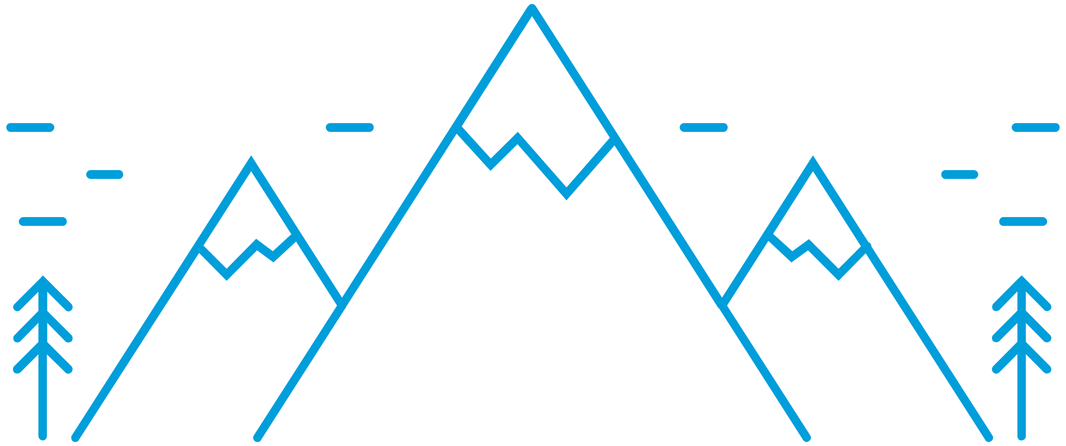
Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage. For further information, visit: **aws.amazon.com/compliance/data-center/controls/.**



Network Protection

Salesforce secures its network on many different fronts; for example:

- **Transport Layer Security (TLS)** cryptographic protocols encrypt network data transmissions between the customer to Salesforce, with a preference for TLS 1.2. HTTP Strict Transport Security (HSTS) is enabled by default on all Salesforce and Visualforce pages, and can be enabled by Customer administrators on Communities and Salesforce Sites [SC-8(1)].
- **Network gateways and firewalls** at the external network boundary are configured by default to deny all traffic and allow by exception, filtering unwanted network traffic. If necessary, they apply traffic rate limits. Filter events are logged and monitored for anomalies. [CM-7, SC-7, SC-7(3)].
- **AWS Security Groups** act as virtual firewalls that restrict and control communication boundaries and prevent unauthorized traffic between services. [SC-7].
- **Stateful packet inspection (SPI)** firewalls inspect all network packets and prevent unauthorized connections [SC-7].
- **Secure routing and traffic flow policies** ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140 compliant and are located inside of the Government Cloud Plus authorization boundary. Network devices enforce traffic flow policies in Government Cloud Plus [SC-4, SC-5, SC-7, SC-7(3), SC-7(4), SC-8, SC-8(1)].
- **Denial-of-Service (DoS) protections** are provided by AWS. At the network hardware level, AWS provides industry leading network DoS and DDoS protections on a 24/7 basis to detect, and react to any perceived attacks. Further, Salesforce also monitors for DoS at the PaaS and SaaS layer to guard against resource exhaustion and capacity attacks [SC-5].

Logical Access Controls

Salesforce has implemented strong logical access controls for the production network, including:

- **Authorized users** are granted production access after manager approval and based on business justification. All personnel with logical access must must go through an enrollment and identity proofing process in accordance with NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing Requirements. Terminated users are removed in a timely manner [AC-2] [IA-5].
- **Two-factor authentication processes** verify the authentication of access requests to internal systems. Further, authentication is NIST SP 800-63B AAL3 compliant utilizing FIPS 140 compliant authenticators [IA-2(1)].
- **Virtual Desktop Infrastructure (VDI) and Bastion Hosts** act as hardened barriers between the authentication perimeter and core servers [AC-2, IA-2, IA-2(1)].
- **Segregation of duties and least privilege** is enforced to ensure that employees are granted only the necessary level of access to the production network to perform their assigned job functions based on role [AC-5, AC-6].
- **Infrastructure and AWS logging** is enabled to capture system activity and logs are forwarded to a central logging system that is located within the authorization boundary [AU-2].

Configuration and Change Management

Salesforce implements industry-accepted best practices to harden underlying systems that support the various software layers of the service [CM-2, CM-6]. For instance, hosts are configured with non-default software configurations and minimal processes, user accounts, and network protocols. Hosts log their activity in a remote, central location for safekeeping. Salesforce has performed a review of device configurations against industry best practices and required standards for government markets [e.g., DISA Security Technical Implementation Guides (STIGs) or Center for Internet Security (CIS) Benchmarks (where available) to ensure devices are configured securely [CM-6, CM-6(1)].

Change Management processes dictate that system changes and maintenance are documented in Salesforce's internal ticketing system. Changes require approval, testing, and security impact analysis prior to deployment [CM-3, CM-4]. In addition, any changes that constitute a significant change, per FedRAMP's Significant Change policies and procedures, require analysis and a thorough impact assessment to determine the impact to the Government Cloud Plus environment [CA-6].

Database Security

The underlying database layer plays a significant role in platform security. Salesforce enforces strict control of database administrator access to only authorized individuals with a business justification for access [AC-2, IA-2(8), IA-5, IA-5(1), IA-5(6), IA-5(7)]. Databases are configured in accordance with security benchmarks provided by industry best practices and required standards for government markets (i.e., the CIS Benchmarks, DISA STIGs) [CM-6].

Operational Monitoring

The Salesforce application and website are monitored on a 24x7 basis for reliability and performance. This includes:

- The Site Reliability (SR) team monitors the service and has Subject Matter Experts (SMEs) in various disciplines. The SR handles first-and second-tier support, with technical engineers providing escalation support.
- Overall system monitoring is provided by a variety of tools and alerts are aggregated.
- Monitoring tools are automated and route issues, warnings, and problems to the Site Reliability teams.
- Alerts of significant events are routed to on-call personnel as well as to the engineering teams.

Salesforce has built extensive monitoring and instrumentation into the application itself so that the application can accurately report its health and performance to on-call support staff and engineers [IR-2, PM-6].

Security Monitoring

A variety of tools, third-party resources, and a dedicated Computer Security Incident Response Team (CSIRT) provide comprehensive monitoring of the Salesforce production environment. These include:

- **Intrusion Detection Systems (IDS)** – IDS monitor the production network for potentially malicious network traffic [AC-4, SC-7, SI-4].
- **Logging and Alerting System** – Activity logs from production devices and servers are sent to a logging and alerting system within the authorization boundary that reports and alerts on events [AC-2(4), AU-2, AU-6, SI-4].
- **Threat Monitoring** – The Salesforce security team receives and reviews threat alerts from a variety of sources including SANS, United States Computer Emergency Readiness Team (US-CERT), and Open Web Application Security Project (OWASP). Threats that

are deemed critical are escalated to the appropriate resource to respond [SI-5].

- **Vulnerability and Configuration Scanning** – Vulnerability scans are performed at least monthly to check all operating systems, databases and applications for known vulnerabilities. Salesforce also performs operating system and database configuration baseline compliance scanning. Vulnerabilities and misconfigurations are remediated in accordance with established remediation timeframes [RA-5].
- **Security Incident Monitoring** – The CSIRT monitors for security incidents. Identified security incidents are handled in accordance with the Incident Response Plan [IR-4].

Incident Response

Salesforce maintains an Incident Response Plan and has an established Security Incident Response process. Salesforce will notify customers promptly in the event that Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of customer data. Notification may be made by any of the following methods: phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and/or public posting on trust.salesforce.com [IR-4, IR-6, IR-8].

Salesforce Government Cloud Plus customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com and via calling (212) 634-6630. Salesforce will respond in accordance with the incident response process.

Disaster Recovery and Backup

The Salesforce service is replicated at 100% capacity between the primary and secondary data centers.The secondary site is geographically separated from the primary site by nature of it being located within a separate Availability Zone within the AWS GovCloud region. Data is transmitted between the primary and secondary data centers across encrypted links. Our continuous site switching program verifies the projected recovery times, as well as the data replication between primary and secondary data centers. Additionally, back-ups of data are designed to be highly available and reliable through the use of Amazon Elastic Block Storage (EBS) volumes [CP-4, CP-6, CP-7, CP-9, MP-5].

Media Protection and Sanitization

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST SP 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned [MP-4, MP-6].

Platform and Application Security

Salesforce Government Cloud Plus provides extensive features and tools that provide security for the data generated by customers. Customers can use many of these features to implement security policies governing exactly who, what, from where, when, and how users can access specific IT applications and data, and meet related auditing requirements.

The default user authentication mechanism for Government Cloud Plus requests that a user provide a username and password (credentials) to establish a connection. Government Cloud Plus does not use cookies to store confidential user and session information [AC-2, IA-2].

Many organizations use single sign-on mechanisms to simplify and standardize user authentication across a portfolio of applications [IA-2(1), IA-5, IA-5(1)]. Salesforce Government Cloud Plus supports two single sign-on (SSO) options:

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

Customers can implement multi-factor authentication by integrating with one of Salesforce's SSO capabilities [IA-2(1)]. Specifically, customers who require user authentication via Government-issued smart cards, such as a Common Access Card (CAC) or Personal Identity Verification (PIV) card, can implement federated authentication to authenticate users via a SAML assertion generated by their identity provider (IdP).

Salesforce Government Cloud Plus 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, Salesforce notices this request, sends an email to the user, and requests that the user confirm his/her identity by clicking the activation link in the email [IA- 2(1)].

User authentication and identity confirmation determine who can log in, and network-based security features limit the time and location from where users can log in. When an organization imposes IP address restrictions and a connection request originates from an unknown address, the connection is denied, helping protect data from unauthorized access and "phishing" attacks [SC-7(3), SC-7(4)].

To protect established sessions, Government Cloud Plus monitors and terminates idle sessions after a configurable period of time. Session security limits help defend system access when a user leaves his/her computer unattended without first disconnecting [AC- 11].

Login profiles provide 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 (create, read, update, delete)], along with other settings. Then, the administrator assigns each user a login profile. If the common requirements for a set of users change, the administrator simply updates the login profile for that group of users, instead of applying updates to every individual user [AC-2, AC-5, AC-6].

Salesforce Government Cloud Plus provides a flexible, layered sharing design that lets an organization expose specific application components and data sets to different sets of users [AC-2, AC-5, AC-6, SC-2]:

- **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.

Salesforce Government Cloud Plus has a multitude of history tracking and auditing features that provide valuable information about the use of an organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues [AU-2, AU-6, AU-7, AU-11].

Auditing features include:

- **Record Modification Fields** – All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
- **Field History Tracking** – Customers can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields and retain the data for 18 months. Although auditing is available for all custom objects, only some standard objects allow field-level auditing.

- **Field Audit Trail (additional subscription option)** – With Field Audit Trail, customers can retain field history data for up to 18 months and define object-level policies to retain archived field history data up to 10 years from the time the data was archived. This feature helps customers comply with industry regulations related to audit capability and data retention.
- **Login History** – Customers can review a list of successful and failed login attempts to your organization for the past six months within Salesforce by accessing Login History.
- **Identity Verification History** – With Identity Verification History, administrators can review their org users' identity verification attempts, such as when using a time-based one-time password for two-factor authentication, for the past six months.
- **Setup Audit Trail** – Administrators can view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to an organization's configuration. While the Login History, Identity Verification History, and Setup Audit Trail are available for six months within Salesforce, these audit trails can be downloaded or exported via API and stored locally to meet longer audit log retention requirements [AU-11].
- **Event Monitoring (additional subscription option)** – Event monitoring provides granular level logging data, which monitors user activity within Salesforce. Event log can be retrieved via API or analyzed within the Event Monitoring Analytics App. Administrators can view information about individual events or track trends in events to identify abnormal behavior and safeguard data [AU-2, AU-6, AU-7].

Finally, Salesforce administrators can identify and fix potential security risks and vulnerabilities with their Salesforce org from a single page using Security Health Check. This feature assesses security settings against an established baseline and calculates a summary score. Salesforce provides a baseline standard, while administrators can upload up to five custom baselines. Additionally, for Government Cloud Plus, Salesforce provides a baseline aligned to a subset of FedRAMP High and DoD IL2 requirements. For more information, please see: **help.salesforce.com/articleView?id=security_health_check.htm&type=5.**

Logical Security

Salesforce Government Cloud Plus's innovative multi-tenant 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, the user is assigned a client hash value associated with the session.
- During login, the authenticated user is mapped to their org and access privileges according to the sharing model [AC-5, AC-6].
- Along with the formation and execution of each application request, the application confirms that the user context [an organization ID (orgID)] accompanies each request. It includes it in the WHERE clause of all SQL statements to ensure the request targets the correct organization's data. The application validates that every row in the return set of a database query matches the session's orgID [SC-4].
- Before the rendering of a web page that corresponds to an application request, the application confirms that the calculated client hash value matches the client hash value that was set during the login phase [SC-4].
- An error in the query process does not return any data to the client [SI-11].

05

Data Ownership and Retention

Data Ownership and Retention

Data Ownership

Salesforce will maintain customer access to customer data; however, customer data is owned by the customer. Customers can use Export Services utilities to extract their data, including: weekly export (for applicable products), data loader, APIs, EAI tools, etc.

Data Retention

Active customer data stays on disk until the customer deletes or changes it. Customer-deleted data is temporarily available (15 days) to customers online from the recycle bin. Backups are rotated every 90 days (30 days for sandboxes); therefore, changed or deleted data older than 90 days (30 days for sandboxes) is unrecoverable.

Salesforce customers are responsible for complying with their organization's data retention requirements in their use of the Salesforce services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may export their data at no charge as part of the applications' applicable Export Services utilities previously discussed, or may create a sandbox account for storage of this data. Exports of customer data are otherwise available in comma separated value (.csv) format by request via Salesforce's Customer Support department for a fee. In addition, an org administrator can manually pull many exports detailing system usage and other data.

Protecting PII and Privacy

Salesforce has conducted a Privacy Impact Assessment (PIA) for the delivery of the Salesforce service. The Salesforce service is rated as a High impact system. As such, Salesforce has implemented security controls aligned with the FedRAMP High and DoD IL2 security baselines and are assessed against both by an independent third party assessor at least annually [PL-5].

Customers are responsible for conducting their own PIA for customer data stored in Salesforce. NIST SP 800-60 provides guidance to organizations on categorizing an information system, and states that for PII, the confidentiality impact level should generally fall into the moderate range[6]. Salesforce recommends that federal agencies relying on our FedRAMP P-ATO determine the Security Categorization of their data to ensure the data stored in Salesforce does not exceed the High impact level [PL-5].

As outlined in the previous sections, Government Cloud Plus has numerous configurable security features that allow customers to customize security based on the sensitivity of the data customers store in the application, consistent with the FedRAMP requirements for High impact systems. One such security feature is encryption. The Salesforce service provides the ability to encrypt fields and files. Customers can implement Classic Encryption for selected custom fields, or, with Platform Encryption (additional subscription option), customers can encrypt a variety of widely used standard fields, many custom fields and files and attachments.

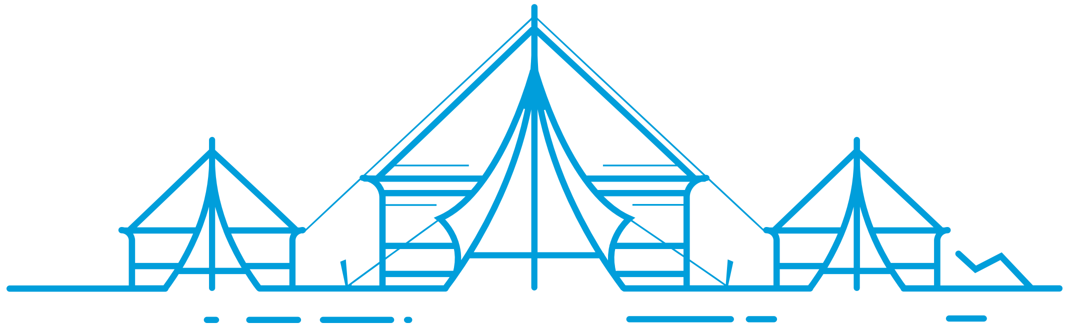
Encrypted fields utilize AES-128-bit keys for Classic Encryption and AES-256-bit keys for Platform Encryption. Platform Encryption also allows customers to manage the encryption key lifecycle. The encryption libraries for both Classic Encryption and Platform Encryption are FIPS 140 validated [SC-13, SC-13(1)]. Additional security controls are detailed in Salesforce's Security Implementation Guide: **resources.docs.salesforce.com/sfdc/pdf/salesforce_security_impl_guide.pdf.**

[6] NIST SP 800-60, Section 4.4.2.4

Privacy

At Salesforce, there is no higher priority than the privacy and security of our customers' data. We believe that protecting the privacy of our customers' data is integral to our mission of earning and maintaining the trust of each of our customers. We seek to lead the industry as a trusted repository for customer data through a world-class privacy program and provide a secure infrastructure and flexible tools that help enable our customers to comply with global privacy and data protection regulations.

Privacy Statement: **www.salesforce.com/company/privacy/.**



06

Additional Considerations

Additional Considerations

State and Local Governments

Many state and local government customers require the implementation of NIST SP 800-53 controls for a commercial CSO, while others now require a FedRAMP P-ATO. While both the Salesforce commercial cloud and Salesforce Government Cloud Plus implement similar security controls, only the Salesforce Government Cloud Plus has been assessed against the FedRAMP High baseline security controls, which are derived from NIST SP 800-53 controls, by a 3PAO and only Salesforce Government Cloud Plus maintains a FedRAMP High P-ATO. Please contact your Salesforce Account Executive to discuss other compliance frameworks or privacy regulations, including those at the state and local levels, which are not covered by the FedRAMP High baseline or DoD IL2 requirements.

Government Contractors

Government contractors may utilize commercial CSOs for a variety of use cases. Depending on the use case and the sensitivity of data managed by a commercial CSO, Government-mandated compliance frameworks may be relevant.

Per DFARS 252.204-7012, contractors using an external cloud service provider (CSP) for internal business purposes to store, process, or transmit Covered Defense Information (CDI) must require and ensure the CSO meets security requirements equivalent to those established by the FedRAMP Moderate baseline.

Per DFARS 252.239-7010, contractors must adhere to the DoD CC SRG when operating a cloud-based system on behalf of the Government in performance of a DoD contract.

Salesforce Government Cloud Plus has been assessed by a 3PAO against the FedRAMP High baseline and maintains a FedRAMP High P-ATO. This also means the Salesforce Government Cloud meets DoD IL2 requirements.

Conclusion

GOVERNMENT ORGANIZATIONS AND CONTRACTORS TRUST SALESFORCE

Salesforce recognizes and appreciates that government solutions need to address specific high-priority security requirements. We will continue to partner with governments at all levels to demonstrate that the required level of protection can be provided in the cloud environment. For more detailed information on Salesforce's security for the Salesforce Government Cloud Plus, please contact your Salesforce Account Executive.

DOCUMENT DISCLAIMER

Although Salesforce has attempted to provide accurate information and guidance in this document, Salesforce provides no warranty or assurances related to its content. The implementations, procedures, and policies of Salesforce are subject to change and may impact the information reflected in this document. The rights and responsibilities of the parties with regard to your use of Salesforce's online software services shall be set forth solely in the applicable agreement executed by Salesforce. Customers should make their purchase decisions based upon features that are currently available. This document is subject to Salesforce's Forward-Looking Statements at:

https://investor.salesforce.com/about-us/investor/forward-looking-statements/

salesforce