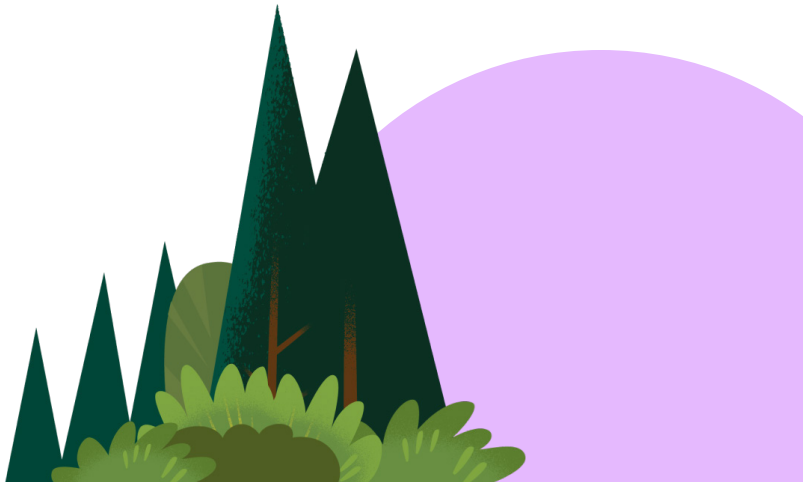
Salesforce Government Cloud Plus

Scale and secure apps on a FedRAMP High-authorized government cloud.

Content



Overview

At Salesforce, we understand the importance of adopting industry-leading security practices and technology needed to protect customers' data. Our security practices are embedded across all of our technology, programs, and processes. Our customers rely on us to deliver high levels of data integrity, confidentiality, and availability. For more than two decades, we have partnered with organizations in highly regulated industries, such as government, financial services, healthcare, and utilities - each customer willing to trust Salesforce with securing their data.

In this paper, we provide an overview of our commitment to securing data and privacy for our U.S. federal, state, local government customers and government contractors using **Salesforce Government Cloud Plus.** Built on AWS GovCloud (US), Government Cloud Plus has security and privacy controls to support FedRAMP High, DoD IL4 and additional compliance frameworks, such as: IRS 1075, NIST SP 800-171, and DoD Privacy Overlays.[1]

[1]This paper is written primarily in the context of the 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 knowledge paper. Please note that this is not an exhaustive mapping and is intended to be illustrative for the purposes of this knowledge paper. A detailed mapping of Salesforce's control requirements is available in our Control Implementation Summary (CIS) document. Please work with a Salesforce representative to request access to our CIS document.

0.1

Our Values Guide Our Business

At Salesforce, our corporate values - Trust, Customer Success, Innovation, Equality, and Sustainability - guide our business and how we work with customers and partners.

Trust

Trust is our customers' ability to depend on Salesforce's security, performance, and transparency of our systems and services. It means having a trusted relationship with our customers, and to communicate openly with them about performance and availability of our services. As part of fostering transparent communications with our customers, we offer information on the performance, security, and compliance of our applications and infrastructure visible on the trust.salesforce.com website.

Customer Success

Our people, programs, and products are focused on making our customers successful. We understand that secure innovations help drive success for our customers, which in turn drives success for Salesforce.

Innovation

We embed security requirements into all stages of the software development lifecycle to enable multiple security releases rapidly throughout the year, allowing customers the opportunity to innovate and stay ahead in their industries.

Equality

Our commitment to strengthening everyone's security posture extends to our collaboration in the industry. We value equality and actively participate in industry events and associations to improve representation in security leadership roles. In collaboration with World Economic Forum partners, Salesforce also leads an effort around reskilling and upskilling workers using the Cybersecurity Learning Hub on Trailhead, a free learning platform to help close the cybersecurity skills gap.

Sustainability

We are in a climate emergency and it's time for bold leadership to accelerate the world's journey to net zero, because everything rests on a stable climate. Salesforce today has net zero emissions and has been voluntarily reporting on its greenhouse gas emissions since fiscal year 2012. Since that time, we have continued to increase the scope of our climate action strategy by actively engaging policymakers, peers, partners, suppliers, and customers to accelerate toward a net zero goal.

0.2

Salesforce Builds Security into Everything We Do

We build security into our technology, programs, and processes using the defense-in-depth approach. This strategy limits the possibility of any single point of failure by utilizing multiple layers of defensive mechanisms with redundancies. We execute our security strategy based on four key pillars to support our vision of providing the most secure and compliant enterprise cloud in the market.

Build a Trust-First Culture

To deliver the most trusted infrastructure, we strive to build a trust-first culture that encourages positive security behaviors for all Salesforce employees and partners to safeguard our customers' data. We cultivate a security-minded work environment, from driving awareness of phishing emails to embedding security requirements in our software development lifecycle process.

Nail the Basics

Many security breaches can be tracked to not getting the basics right, that's why implementing basic security practices to protect customers' data always comes first at Salesforce. We execute common security measures uncommonly well. The majority of our programs, measures, and controls focus on fundamental security practices, such as patching and the adoption of multi-factor authentication (MFA) throughout our ecosystem of employees, partners, and customers.

Enable Secure Innovation

We also enable our customers to innovate and gain business agility. For example, we embed security requirements into all stages of the software development lifecycle which allows us to release new security-focused features and applications rapidly, thus allowing customers to innovate and scale to meet changing market demands.

Raise the Security Bar

We have a long-term commitment to expanding security controls across Salesforce, including our acquisitions, to help us scale and invest in emerging security technologies such as machine learning and artificial intelligence.

01

Salesforce Government Cloud Plus

Salesforce Government Cloud Plus

Salesforce 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's Covered Services.

For more detailed information on which Salesforce applications are within the authorization boundary of Salesforce Government Cloud Plus, please refer to: Government Cloud Available Products and Features.

02

Salesforce Compliance Maturity

Implementing the Best Security Standards

Salesforce undergoes System and Organization Controls (SOC) 1 examinations semi-annually, completes SOC 2 and SOC 3 for Service Organizations audits, and has achieved compliance with PCI-DSS. In May 2008, Salesforce became the first publicly traded SaaS vendor to receive the prestigious ISO/IEC 27001 Security Certification (ISO 27001), 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.

Federal Risk and Authorization Management Program (FedRAMP)

In May 2014, Salesforce achieved its first FedRAMP Authority to Operate (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.

To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance and NIST SP 800-37. Salesforce documented a System Security Plan (SSP) in accordance with NIST SP 800-18 for the Salesforce Government Cloud Plus service offering. The SSP identifies control implementations for Salesforce 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 Salesforce Government Cloud Plus. The security assessment testing determined the adequacy of the security controls used to protect the confidentiality, integrity, and availability of Salesforce 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.

[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

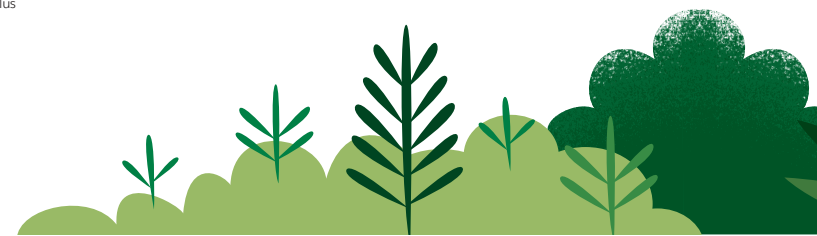
Department of Defense (DoD)

After receiving its first FedRAMP authorization in 2014, Salesforce was granted a Provisional Authorization (PA) by the Defense Information Systems Agency (DISA) in April 2017 at Impact Level 4 (IL4) for the Salesforce Government Cloud. Similarly Salesforce was granted an IL4 PA for Salesforce Government Cloud Plus in August 2021. Additionally, Salesforce Government Cloud Plus provides the following to adhere to DoD Cloud Computing cybersecurity requirements, including the DoD Secure Cloud Computing Architecture (SCCA):

- DoD Privacy Overlay controls, including those for Protected Health Information (PHI) and Personally Identifiable Information (PII) High, and IL4 Service Level Agreement (SLA) controls;
- Connection to the DISA Boundary Cloud Access Point (BCAP), which enables Salesforce to operate as an extension of NIPRNet with data traversing a dedicated circuit and not the public Internet;
- Support for .mil domain names and utilization of DoD IP space; and
- Integration with the DoD Enterprise Email Security Gateway (EEMSG), in accordance with CYBERCOM TASKORD 12-0920, which allows for improved email deliverability and protection for NIPRNet endpoints.

With an IL4 PA and the additional DoD-specific architectural components, DoD Mission Owners may use Salesforce Government Cloud Plus to store / process Controlled Unclassified Information (CUI), including PHI and PII, and other mission data, including data used in direct support of military or contingency operations.

[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



Internal Revenue Service Publication 1075 (IRS 1075)

IRS 1075 provides guidelines to Public Sector agencies and private companies handling Federal Tax Information (FTI). By meeting these guidelines, organizations can ensure appropriate policies, controls and safeguards protecting confidential personal information, including name, address, social security number and federal tax returns. A 3PAO has assessed Salesforce Government Cloud Plus and issued an attestation where it opined the environment is designed and operated to be in compliance with requirements for the handling of FTI. Accordingly, Salesforce customers can submit a pre-populated template form from within Salesforce Government Cloud Plus to the IRS Office of Safeguards to notify the IRS of an organization's intent to begin handling FTI within Salesforce. Once approved, customers can access critical FTI and limit reliance on inefficient paper-based systems or external databases, which can drive up operating costs, lead to synchronization errors, and serve as a security risk.

NIST SP 800-171

The Salesforce Government Cloud Plus has been issued a NIST SP 800-171 attestation by a 3PAO, which was based on Salesforce's implementation of FedRAMP High and DoD IL4 controls. NIST SP 800-171 is the basis for Level 2 of DoD's Cybersecurity Maturity Model Certification (CMMC).

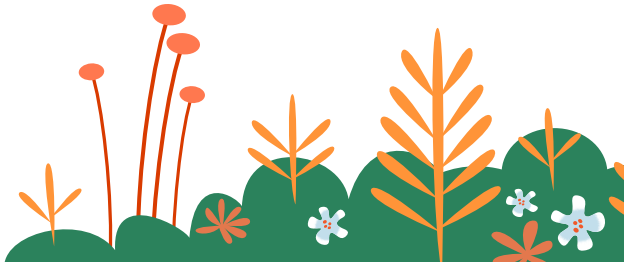
03

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, Technology / Product Counsel, 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 (e.g. SOC 2) 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, Vulnerability Management and Response Plan, Disaster Recovery Plan, etc. [IR-1, RA-1, CP-1].



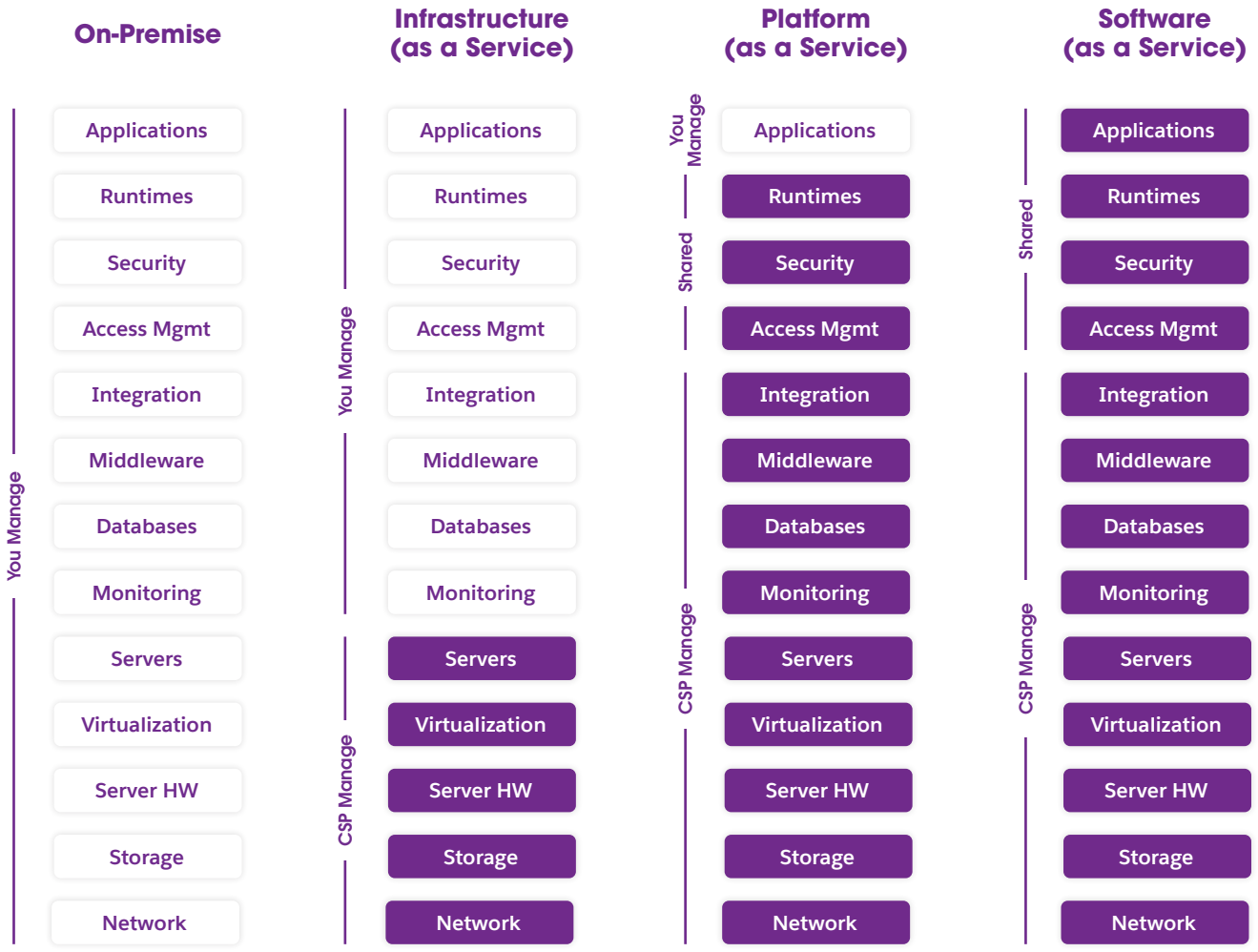
In particular, Salesforce incorporates security into its development processes at all stages through the Salesforce Secure Development Lifecycle. Further, Salesforce has integrated a Product Security team in all stages of the secure development lifecycle. From initial architecture considerations to post-release, 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 tested 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 below, when using 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. Although 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.

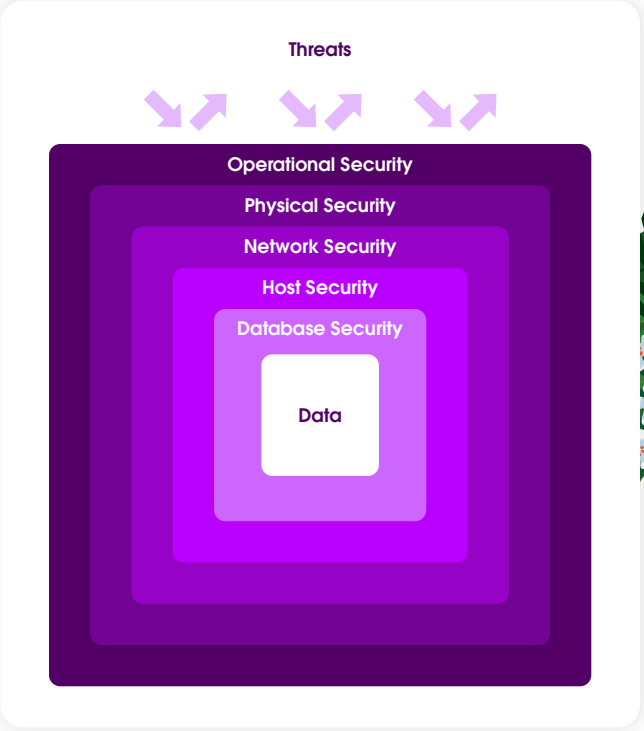


With Salesforce, customers inherit the majority of security controls from Salesforce and AWS. While customers do bear some responsibility for ensuring security and compliance, Salesforce provides numerous enablement resources, including training and implementation guides. Specifically, for customers seeking compliance with FedRAMP High or DoD IL4, Salesforce provides a Customer Configuration Guide tailored to those requirements. This shared responsibility model significantly reduces both risk and burden for customers, allowing them to place more focus on their business and mission.

Defense in Depth

The figure at the bottom of the page illustrates the many layers of defense Salesforce Government Cloud Plus uses to resist various types of threats and achieve compliance with security frameworks such as DoD IL4, FedRAMP High, SOC 1, SOC 2, SOC 3, and ISO 27001 – all without sacrificing application performance.

Salesforce strictly manages access to Salesforce 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, 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 by AWS to host Customer Data submitted to Salesforce Government Cloud Plus Covered Services.



Qualified Personnel

Salesforce enforces usage conditions for all personnel with access to Salesforce Government Cloud Plus. Specifically, all personnel must successfully undergo a Salesforce background investigation, be U.S. citizens, and are required to access Salesforce Government Cloud Plus from U.S. soil. Further, in order to obtain production access to Salesforce 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 Salesforce Government Cloud Plus access [IA-2, PS-2].

Multi-tenancy

Salesforce's innovative multi-tenant database architecture delivers operational and cost efficiencies for cloud-based applications without compromising the security of each organization's data. This 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, with Salesforce Government Cloud Plus only supporting qualified U.S. Government customers. Salesforce uses this 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 securely designed and undergoes robust testing through an ongoing process by both Salesforce and its customers [AC-2, SC-4].

- 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].

04

Controls and Database Security

Physical and Environmental Controls

Salesforce uses infrastructure provided by a third party, AWS, to host Customer Data submitted to Salesforce 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.

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 data center controls, to learn more.

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 Salesforce Government Cloud Plus authorization boundary. Network devices enforce traffic flow policies in Salesforce 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 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 Salesforce 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:

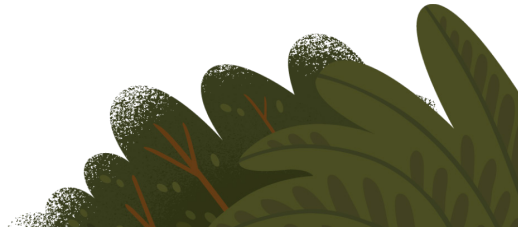
- The Site Reliability (SR) team monitors the service and has Subject Matter Experts (SMEs) in various disciplines. The SR handles first-and second-tier support, with technical engineers providing escalation support.
- Overall system monitoring is provided by a variety of tools and alerts are aggregated.
- Monitoring tools are automated and route issues, warnings, and problems to the SR 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 Salesforce's 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

Salesforce Government Cloud Plus 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].

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. Security controls available for configuration are detailed in Salesforce's Security Implementation Guide.

Identity & Access Management

User Authentication

User authentication and identity confirmation determine who can log in. The default user mechanism for Salesforce Government Cloud Plus requests the user provide a username and password ("credentials") to establish a connection.

Many organizations use a single sign-on (SSO) mechanism 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 SSO options:

- **Federated authentication** using Security Assertion Markup Language (SAML), which allows a session to send authentication and authorization data between affiliated but unrelated Web services.
- **Delegated authentication,** which 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.

To increase protection for user accounts against common threats like "phishing", credential stuffing, and account takeovers, customers can implement multi-factor authentication (MFA) by integrating with one of Salesforce's SSO capabilities [IA-2(1)]. MFA adds another layer of security to your login process by requiring users to enter two or more pieces of evidence – or factors – to prove they're who they say they are. One factor is something the user knows, such as their username and password combination. Other factors are verification methods that the user has in their possession, such as an authenticator app or security key.

Specifically, customers who require user authentication via Government-issued smart cards, such as the Common Access Card (CAC) or Personal Identity Verification (PIV) card, can implement federated authentication. Alternatively, Salesforce also offers a native certificate-based authentication capability that enables CAC- and PIV-based user authentication.

Network Based Security

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 IP address, the connection is denied, helping protect data from unauthorized access and “phishing” attacks [SC-(3), SC-7(4)].

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 their identity by clicking the activation link in the email [IA-2(1)].

To protect established sessions, Salesforce 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 their computer unattended without first disconnecting [AC-11].

Access Management

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]. This includes:

- **Organization-wide sharing:** Default settings that provide a baseline level of access for each object. 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 object access to particular users or groups.
- **Sharing rules:** Exception rules to organization-wide sharing settings that give additional users access to records they don’t own. Sharing rules can be based on the record owner or on the field values in the record.
- **User profiles:** Efficient way to manage system and application access for groups of similar users. If the common requirements for a defined group of users changes, the administrator simply updates the profile for the group, instead of applying updates to every individual user.
- **Manual sharing:** When individual users have specific access requirements, owners can manually share records.

Encryption of Data-at-Rest

By default, all customer data at rest is encrypted at the volume level using AWS Elastic Block Storage (EBS) and AES 256-bit encryption. Additionally, Salesforce provides the ability to encrypt data at the field and file level. To achieve this, 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 [SC-28]. Encrypted fields utilize AES-128-bit keys for Classic Encryption and AES-256-bit keys for Platform Encryption. While both features allow customers to manage the encryption key lifecycle, only Platform Encryption provides customers Bring Your Own Key (BYOK) options to import key material from third party services.

The encryption libraries for both Classic Encryption and Platform Encryption are FIPS 140-2 validated [SC-13, SC-13(1)].

Monitoring & Auditing

To help diagnose potential or real security issues, Salesforce Government Cloud Plus offers history tracking and auditing features that provide information about the use of an organization's applications and data [AU-2, AU-6, AU-7, AU-11]. Features include:

- **Event Monitoring (additional subscription option):** A granular log of user activity. Event logs and streams can be retrieved via API or analyzed in the Event Monitoring Analytics App to help administrators view individual event details or monitor trends to identify abnormal behavior and safeguard data [AU-2, AU-6, AU-7].
- **Field Audit Trail (additional subscription option):** Organizations can retain field history data for up to 18 months, in addition to defining object-level policies to retain archived field history data for up to 10 years from the date of archive.
- **Field History Tracking:** Organizations can enable auditing for individual fields, which can track any changes in the values of selected fields and retain the data for 18 months. Auditing is available for all custom objects. Only some standard objects allow field-level auditing.
- **Identity Verification History:** A history of users' identity verification attempts, such as when using a time-based single use password for MFA in the past six (6) months. This audit trail can be downloaded or exported via API and stored locally to meet longer audit log retention requirements [AU-11].
- **Login History:** A list of successful and failed login attempts to an organization for the past six (6) months. This audit trail can be downloaded or exported via API and stored locally to meet longer audit log retention requirements [AU-11].
- **Record Modification Fields:** All objects include fields to store the name of the user who created the record and who last modified the record.
- **Setup Audit Trail:** A log of modifications to an organization's configuration in the past six (6) months. This audit trail can be downloaded or exported via API and stored locally to meet longer audit log retention requirements [AU-11].
- **Security Health Check:** A single view to help customers identify and fix potential security risks and vulnerabilities within their organization. This view assesses security settings against an established baseline and calculates a summary score. With Government Cloud Plus, Salesforce provides two baselines; a standard baseline and one aligned to a subject of FedRAMP High and DoD IL4 requirements. In addition, customers can define up to five custom baselines to perform health checks.

05

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, 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

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 IL4 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.[4] Salesforce recommends that federal agencies relying on our FedRAMP P-ATO and DoD PA determine the Security Categorization of their data to ensure the data stored in Salesforce does not exceed the High impact level [PL-5].

Privacy

At Salesforce, 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 by providing a world-class privacy program, secure infrastructure, and flexible tools that help enable our customers comply with global privacy and data protection regulation

Privacy Statement

06

Other Customer Considerations

Other Customer 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 ATO. While both the Salesforce commercial cloud and Salesforce Government Cloud Plus implement similar security controls, 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 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 IL4 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 and requirements, including FedRAMP, CMMC, and International Traffic in Arms Regulations (ITAR), may be relevant.

As the DoD seeks to bolster security of the Defense supply chain, Contractors:

- Using an external cloud service provider for internal business purposes to store, process, or transmit CUI must require and ensure the CSO meets security requirements equivalent to those established by the FedRAMP Moderate baseline (DFARS 252.204-7012) and post summary level scores of a current NIST SP 800-171 DoD Assessment to the Supplier Performance Risk System (SPRS) for relevant systems (DFARS 252.204-7019);
- Operating a cloud-based system on behalf of the Government in performance of a DoD contract must adhere to the DoD CC SRG (DFARS 252.239-7010); and
- Must restrict ITAR-controlled data access to U.S. persons.

With a FedRAMP High P-ATO, DoD IL4 PA, NIST SP 800-171 attestation, and enforcement of U.S. citizenship for access to Salesforce Government Cloud Plus, Salesforce can help Government contractors address these compliance requirements.

07 Conclusion

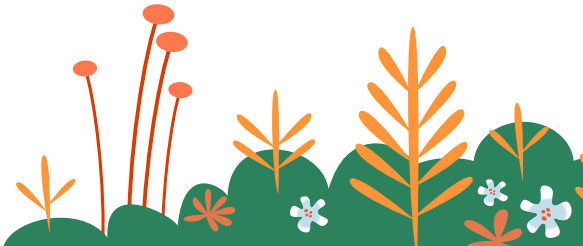
Conclusion: U.S. Government Organizations and Contractors Trust Salesforce

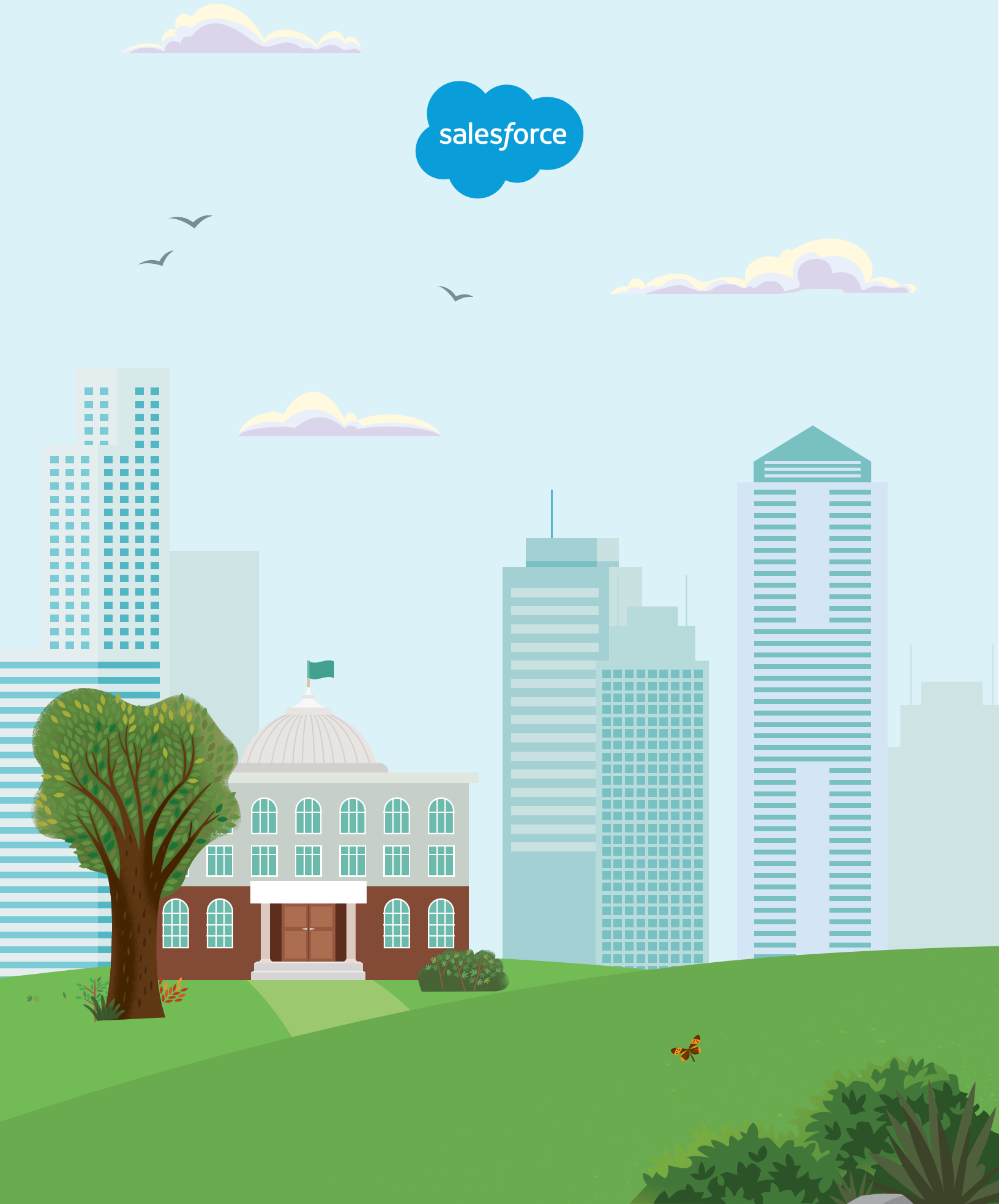
U.S. government and government contractors are faced with unique challenges. They are tasked with handling and protecting sensitive data in the face of increasing cybersecurity threats while also meeting compliance mandates in an evolving regulatory landscape. To meet these needs, Salesforce recognizes 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 it is possible to drive mission success using cloud-first IT innovation, while maintaining security and adhering to mandated compliance regulations. For more detailed information on Salesforce's security for Salesforce Government Cloud Plus, please contact your Salesforce Account Executive.

Document Disclaimer

Disclaimer: The information provided in this document is strictly for the convenience of our customers and is for general informational purposes only. Salesforce does not warrant the accuracy or completeness of any information, text, graphics, links or other items contained within this document. It may be advisable for you to consult with a professional such as a lawyer, accountant, architect, business advisor, or professional engineer to get specific advice that applies to your specific situation. This document is subject to change at any time without notice. The rights and responsibilities of the parties with regard to use of Salesforce's online 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 information is subject to Salesforce's Forward-Looking Statements.




salesforce