Security, Privacy and Architecture for Non-GA Services offered under the Unified Pilot Research Agreement ('Covered Services')

Published: April 4, 2022

Salesforce's Corporate Trust Commitment

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

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via a customer-specific unique identifier and, depending on the Covered Service, may allow the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions.

Security Policies, Procedures and Controls

The Covered Services are operated in accordance with policies and procedures to enhance security and may include a variety of configurable security controls that allow customers to tailor the security of the Covered Services for their own use. Where applicable, please see additional information on such controls in the Salesforce Security Guide.

Salesforce uses infrastructure provided by third parties to host Customer Data submitted to certain Covered Services. Depending upon the Covered Service, Salesforce may use infrastructure provided by Amazon Web Services, Inc. ("AWS"), Google, LLC ("GCP"), and Microsoft Corporation ("Azure") to host Customer Data. Further information about security provided by AWS, GCP, and Azure is available from the AWS Security website, including AWS's overview of security processes, the Google Security website, and the Azure Security website.

Intrusion Detection

With the exception of Einstein Vision and Language, Salesforce, or an authorized third party, will monitor the Covered Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plugins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, and to ensure that the Covered Services function properly.

Security Logs

All systems used in the provision of the Covered Services, including firewalls, routers, network switches and operating systems, may log information to their respective system log facility, AWS's CloudTrail system (for agentless AWS services), or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

User Authentication

Access to the Covered Services requires authentication via one of the supported mechanisms as described in the applicable Documentation, which may include user ID/password; API key/secret; SSO Authentication; SAML-based Federation; OpenID Connect; OAuth; Social Login; or Delegated Authentication, which is determined and controlled by the customer.

Physical Security

Production data centers used to provide the Covered Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by guards and access screening, and are also supported by onsite back-up generators in the event of a power failure.

Further information about security provided by AWS, GCP, and Azure is available from the AWS Security website, including AWS's overview of security processes, the Google Security website, and the Azure Security website.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are designed to be highly redundant and reliable.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance.

Data Encryption

The Covered Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services, including and depending on the Covered Service through Transport Layer Encryption (TLS) leveraging TLS 1.x, 256-bit TLS certificates, 128 SSL certificates, 256-bit AES encryption or 1024-bit RSA public keys or 2048-bit RSA server certificates and 128 bit symmetric encryption keys.