



WHITE PAPER

Security overview

Anaplan was built from the ground up using the core principles of information security, also known as AIC.



Anaplan is committed to achieving and maintaining these principles and the trust of our customers.

Security overview

Security is a priority at Anaplan. Anaplan was built from the ground up using the core principles of information security, also known as the AIC triad:

Availability

Ensure the information is available when needed. Anaplan is committed to achieving and maintaining these principles and the trust of our customers. Integral to this is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services (customer data). This also includes maintaining a business continuity program.

Integrity

Maintain and assure the accuracy and consistency of data over its entire lifecycle.

Confidentiality

Prevent the disclosure of information to unauthorized individuals or systems.

Company

To support these principles, Anaplan was deliberately crafted as a highly distributed global company that allows for significant resiliency against threats and disasters. All functions within Anaplan are geographically distributed across the globe, reducing risks associated with regional events.

The U.S. offices host most of the sales, marketing, and support activities. Staff in the U.K., Japan, and Singapore offices provide regional coverage, in addition to backup support.

The U.K. and US offices provide core product development. The source code repository is hosted at an offsite data center. All staff are able to operate remotely over secure, two-factor VPN connections and provide ongoing development and technical support in the event that the main offices become unavailable.

Anaplan has a number of processes to ensure that any invocation of our disaster recovery plan leads to a quick and efficient restoration of services in the event of a major disaster.

Onsite and offsite backups, resiliency and redundancy in the infrastructure, availability of secondary data centers, and the use of geographically distributed infrastructure and support staff enable disaster recovery plans to be executed quickly and efficiently in the event of a major disaster.

Architecture

The Anaplan Service operates from third party facilities. In colocation data centers, the data center host provides physical security, power, cooling, and environmental protection (fire suppression, temperature/humidity control, etc.). Anaplan owns and operates the infrastructure. In public cloud, the cloud provider delivers all of the physical elements as well as manages the hardware. Anaplan manages the Service.

Colocation data centers

- The Anaplan data centers are based in Virginia and California in the U.S., Amsterdam and Frankfurt in the EU. These locations were chosen based on their low-risk environments for earthquakes, flooding, and other large-scale natural disasters.
- Prior to selection, each facility was subjected to a stringent assessment for the presence, implementation, and ongoing administration of physical security controls.
- Each facility is fully protected 24x7x365 by security guards, high-security perimeter protection, and video cameras. All access and activity is logged, recorded, and stored for no less than 30 days.
- Entry to each facility requires prior authorization and a process of identification validation and biometric confirmation.
- Facilities have an annual audit by industry leading firms for ISO 27001 and SSAE 18 Type II compliance. Anaplan performs its own annual data center audits.
- Technology providers are Cisco, Dell, Pure Storage, Hewlett Packard Enterprise, Palo Alto Networks and Okta.

The following security and privacy-related frameworks, audits, and certifications apply to Anaplan:

- ISO 27002 and 27018: Anaplan has adopted the ISO 27k framework as the basis for information security and privacy policies. Anaplan has scoped and tailored this standard to meet our business requirements.
- Service Organization Control (SOC) reports: Anaplan undergoes SOC 1 and SOC 2 audits every six months.

Anaplan has obtained TRUSTe Enterprise Certification to demonstrate our compliance with a number of globally recognized privacy frameworks.

Anaplan is EU-US and Swiss-US Privacy Shield certified.

Public cloud option

Anaplan's clients have the option to run their models in the public cloud. The public cloud offering has all of the security features of the colocation data centers. In addition, public cloud offerings run on servers that are custom-designed by the cloud provider. These providers have also earned additional ISO certifications, including ISO 27017 (security for cloud providers), and/or ISO 27701 (privacy of personal information), and are NIST 800-53 compliant.

With each public cloud deployment, the infrastructure is spread across multiple zones within the same region, bringing greater reliability and a reduction of planned downtime for infrastructure components. Anaplan will leverage the public cloud provider's internet point of presence, which will help ensure operational uptime.

Redundant infrastructure

Anaplan's infrastructure utilizes a redundant "active/passive" design to enable full operational failover. A failure of any single component should not lead to a disruption in customer service or a loss of customer data. In the event of a primary failure, the redundant architecture will allow for full failover to the secondary system(s).

Security infrastructure

Each facility is protected by a "defense-in-depth" security architecture consisting of next-generation firewalls, Network Threat Detection and Response (NTDR), anti-virus/antimalware protection, and monitoring capabilities.

Network infrastructure

The internal network infrastructure is securely segmented using firewalls, virtual networks (VLANs), and access control lists (ACLs), which limit access and communication between systems. No system or individual can reach another system unless explicitly authorized to do so.

Server infrastructure

- All servers run Linux® Operating System and are hardened according to policy based on Center for Internet Security standards.
- All hosts are subject to a regular patching and maintenance routine.
- All hosts are periodically scanned for vulnerabilities and security threats using the industry-leading Nessus®.
- All servers are controlled and managed by an automation system to ensure consistent configuration across the environment.
- All servers have an industry-leading Endpoint Detection and Response (EDR) agent and the Anaplan cyber defense team continuously monitors activity.

Security controls

Anaplan is designed with security in mind, from networks and servers, to how users access and manage data. The Anaplan platform is a unique blend of proprietary technology that securely collects and stores data, and is agile enough to interface with external systems.

Anaplan maintains an ACID-compliant software stack that guarantees data in Anaplan models is always in a known safe state.

Atomicity requires that each transaction is “all or nothing.” If any part of a transaction fails, then the entire transaction fails and the model is left unchanged.

Consistency ensures that any change will bring the model from one valid state to another.

Isolation requires that multiple transactions occurring at the same time do not impact one another’s execution.


Durability means that once a transaction has been committed, it will remain so even in the event of a crash or error.

- Core software consists of an in-memory data storage model to achieve the fastest computational results, yet maintains an active log of all changes on disk in real time.
- The full data model is persisted to storage using AES 256-bit encryption.
- User query logs are written to disk before any changes are applied in memory.
- All data is stored and accessed through the same secure interface.
- Data never crosses the Internet unencrypted.

User access, controls, and policies

Anaplan supports a variety of configurable security controls that provide customers the security of Anaplan for their own use. These controls include:

- Anaplan Administration to provide governance and control, enabling administrators to implement user changes and organize models across the business.
- Unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual.
- Controls to revoke access after several consecutive failed login attempts.
- Controls to ensure generated initial passwords must be reset on first use.
- Controls to force a user password to expire after a period of time.
- Controls to terminate a user session after a period of inactivity.
- Password complexity requirements:
 - Minimum of 8 characters
 - At least one uppercase character
 - At least one lowercase character
 - At least one numeric character
 - Must be changed every 90 days



New users are denied access to any data by default. Access must be granted by the customer-designated administrator.

With Self-Service SAML (SS SAML), administrators can provide SSO access to speed user authentication, as well as harden protection for Anaplan security domain access. SS SAML is compliant with SAML standards and interoperates with SAML 2.0 identity providers. Anaplan SS SAML is available for both desktop and mobile.

Centralized Identity Management (CIM) allows administrators to manage the users in their tenant within a unified dashboard to secure access across users, data, and the environment. Administrators can use CIM to deliver on compliance mandates, gain granular visibility across user access, and manage users across multiple workspaces.

Anaplan employee access, controls, and policies

- Employee access to production infrastructure is permitted only with two-factor authentication via secure VPN.
- Access to any data center is further protected by the mandatory use of SSH public key infrastructure (PKI) technology.
- Employees do not have access to customer data.
- All customer data is owned by the customer.
- Anaplan staff cannot see any end-user data without being granted permission by the customer through the native access control system.

- Access is based on the information security principle of “least privilege,” and “need to know,” with access strictly limited to a select number of skilled individuals.
- All access is monitored and logged.
- All employees are subject to background checks prior to employment.
- All employees are trained on documented information security and privacy procedures.
- All employees are required to sign customer data confidentiality agreements.
- All employees in the Engineering, Quality Assurance, Technical Operations, and Security teams receive additional security training.
- All access is revoked upon termination of employment.

Security team

Anaplan has more than 20 full-time employees around the world focused on governance, risk, audit, and compliance in the areas of security and privacy. Team members have years of industry experience and well-known industry certifications, including OSCP, OSCE, CISSP, CISM, CISA, CIPT, CCSP, CRISC, CIPP/US, and CIPP/E.

Vulnerability and malware management

Malware and viruses

Anaplan will never introduce any virus or malware to a customer's systems. Scans are performed for viruses and malware that could be included in attachments or other customer data uploaded by customers.

Web application vulnerability management

The Anaplan application is subjected to a regular web application scanning (WAS) process carried out using market-leading security and compliance providers, Nessus® and Burp Scanner®.

Anaplan's Information Security team has employees around the world focused on governance, risk, audit, and compliance in the areas of security and privacy.

Anaplan uses industry-standard encryption products to protect customer data and communications during transmissions between a customer's network and Anaplan.

Security procedures, policies, and logging

All services are monitored both internally and from an external system. Anaplan is operated in accordance with the following procedures to enhance security:

Security logs

- All systems (for example, firewalls, routers, network switches, and operating systems) used in the provision of Anaplan will log information to their respective system log facility and to a centralized syslog server.
- All data access by customer and staff is monitored and logged.
- All data changes by customer and staff are monitored and logged.
- Logs are kept for a minimum of 365 days.
- Logs are kept in a secure area to prevent tampering.

Audit logs include the following:

- Date, time, and time zone of the event.
- URL executed or entity ID operated on.
- Identity of the system and the component.
- Type of event and operation performed (viewed, edited, etc.).
- Success or failure.
- User ID.
- Client IP address. Note that this data is not available if Network Address Translation (NAT) or Port Address Translation (PAT) is used by a customer or its ISP.
- Passwords are not logged under any circumstances.

Data encryption

Anaplan uses industry-standard encryption products to protect customer data and communications during transmissions between a customer's network and Anaplan.

- All data in transit between client and server is encrypted via HTTPS using TLS 1.2. Key exchange is done via the browser using 2048-bit certificates. Session key length is negotiated by the end-user browser using the strongest available encryption.
- Data at rest within the system is stored in a unique binary format and subject to full-disk AES-256 encryption.
- Anaplan's BYOK service allows customers to define and manage unique encryption keys for their Anaplan workspaces.

Disaster recovery

Disaster recovery plans are in place and tested at least once per year.

Anaplan utilizes disaster recovery facilities that are geographically remote from primary data centers. In the event that production capabilities at the primary data centers become unavailable, the disaster recovery facilities would be enabled and brought online. Since customer data is already streamed and held at these facilities, recovery time is greatly decreased.

System maintenance

Maintenance is carried out during non-business hours, typically Saturday afternoon from 1:00 p.m. to 5:00 p.m., Pacific Time. Maintenance is most commonly used for a new version release, which typically occurs every four to six weeks.

Change management

- Anaplan follows fully documented change management procedures for all tiers of the service covering application, operating system, server, and network layers.
- All configuration changes are tracked and managed through a written ticketing system.

Customer data

Deletion of customer data

Upon contract termination, customer data submitted to Anaplan is retained in inactive status within Anaplan for 30 days and a transition period of up to an additional 30 days, after which it is overwritten or deleted. Anaplan reserves the right to reduce the number of days it retains such data after contract termination. This process is subject to applicable legal and/or contract requirements.

Event management

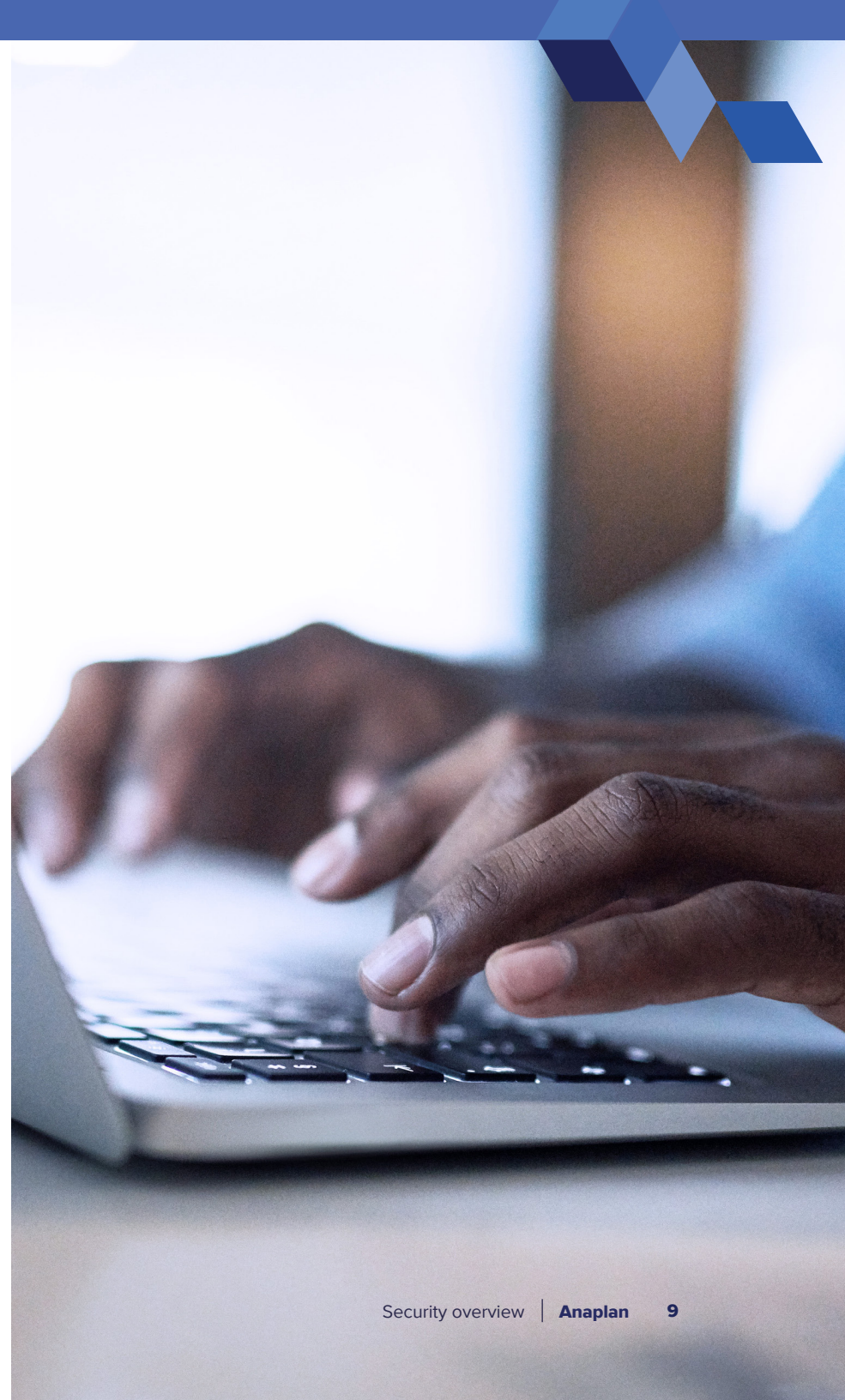
Anaplan maintains event management policies and procedures.

Backups

- All data is held on a redundant disk encrypted storage using industry-standard AES-256 encryption technology.
- Data is streamed in near-real time to backup and disaster recovery storage.
- Model changes are easily reversible and can be returned to previous versions within seconds.
- End users can archive models within their workspace at will.
- All user changes are reviewable and easily reversible.
- Data is stored in more than one area, with each model store being replicated to a secondary unit that will assume responsibility in the event of a primary failure.

Recovery procedure

In the event that data needs to be restored and application history is not available, the backups would be the next point of recovery. Restoration time will vary depending on the volume of data to be recovered, but a single server restore would take no more than a few hours.



About Anaplan

Anaplan, Inc. (NYSE: PLAN) is a cloud-native enterprise SaaS company helping global enterprises orchestrate business performance. Leaders across industries rely on our platform—powered by our proprietary Hyperblock® technology—to connect teams, systems, and insights from across their organizations to continuously adapt to change, transform how they operate, and reinvent value creation. Based in San Francisco, Anaplan has over 20 offices globally, 175 partners and approximately 1,600 customers worldwide.

To learn more, visit anaplan.com

