Anaplan

WHITE PAPER

IT operational resilience

Objective

The objective of this white paper is to provide information on Anaplan's business continuity and disaster recovery measures, so the reader will understand how Anaplan will provide continuity of service to its customers in the event of a disaster.

Offices

Anaplan operates as a highly distributed global company, to minimize the risk of any single point of failure. We have staff operating from 20 offices spanning four continents and multiple time zones.

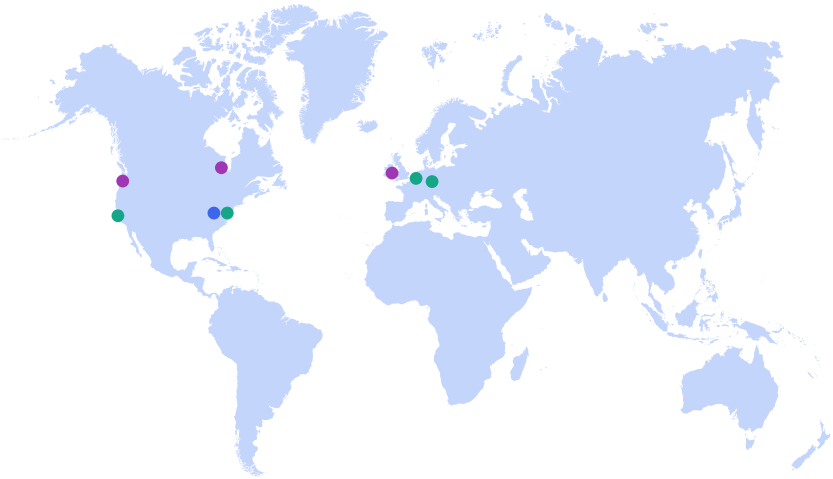
Global headquarters is in San Francisco, California. Core product development and technical support are run out of offices in the U.S., U.K., Japan, Israel, and Singapore. In the event of any one office being offline, all development, test and support staff are able to operate remotely (from home or a temporary office) over secure VPN connections, providing ongoing development and technical support.

Each office's development team can backup each other. Responsibilities are spread across each team and there are shared skills within every team, in addition to wide geographic distribution to provide backup as described above. Infrastructure Engineering and Customer Care team members operate from six offices around the world. Anaplan's business continuity and disaster recovery program is aligned with ISO 22301, the business continuity standard.

Colocation facilities

The Anaplan infrastructure is hosted out of globally respected Equinix International Business Exchange (IBX) data centers, based in Virginia and California in the US, Amsterdam and Frankfurt in the EU, with 24x7x365 support. These Equinix data center facilities are ISO 27001 certified and SOC audited with a proven >99.999% uptime record.

Anaplan owns and operates all infrastructure supporting the service, and controls physical access to this equipment. The Anaplan application and all customer data are stored within the data center, which means there is no customer data or production application code stored or processed on computers issued to personnel. In the public cloud offering, Anaplan operates the servers and services, and the cloud provider does not have access to client data.



AMERICAS

- Primary:
  - Virginia
  - California
- Disaster recovery:
  - Oregon
  - Ohio
- Public cloud:
  - Virginia

EMEA

- Primary:
  - Amsterdam
  - Frankfurt
- Disaster recovery:
  - Dublin

In line with data regionalization requirements, backups of all customer Workspaces and Models are maintained both within the primary data center and/or at the relevant cloud facility. Data is persisted to encrypted storage and streamed in near realtime to the respective cloud facility, depending on location of the primary data.

Data center

Anaplan has created a fully self-managed infrastructure to provide in-region data hosting. The facilities were designed and built to high availability standards. Redundancy extends throughout from multiple Internet Service Providers, Uninterruptible Power Supply systems with N+1 or greater redundancy levels, multiple auxiliary power generators and fuel, and guaranteed fuel delivery contracts with both in-region and out-of-region providers.

Anaplan's application infrastructure is built with high availability features as well. Each compute resource has redundant network cards and power supplies. All data is held on redundant encrypted storage. Additional availability controls are tested in the SOC 2 audits.

Backup and disaster recovery for facilities are enabled to provide for full data redundancy for each geographic region, with streaming file replication for all models and transaction logs, so that in the event of a major disaster, a secondary infrastructure could be activated and customer redirection invoked with minimal disruption and downtime.

As Anaplan continues to grow, we will continue to invest and support our customer base throughout the globe.

Public cloud platform

Customers who choose to run their models in the public cloud can rest assured that Anaplan's public cloud data centers meet and exceed all the industry standard measures for redundancy. For 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. Customers who select the public cloud will have their data backed up within that public cloud provider's infrastructure.

Anaplan will leverage the public cloud internet point of presence to ensure operational uptime and business continuity.

Disaster recovery

Minor incidents such as the failure of a core application server will be handled without any data loss through the redundancy in the compute infrastructure, and resilience built into the Anaplan architecture.

In the event of a major disaster, the service will be recovered in another region of the same country wherever possible. Our disaster recovery efforts are coordinated and managed by a multi-disciplinary team of appropriately authorized and qualified Anaplan individuals. The disaster recovery plan is tested at least annually.

Cyber and physical defenses

Substantial defenses are in place to protect our services against the ever-increasing array of cyber threats. Firewalls block unwanted connections. All customer access to the application is via secure encrypted HTTPS / TLS connections. Anaplan administrative access is via a combined mandatory two-factor and SSH PKI authentication system and limited to senior technical staff. (See the Security Overview white paper for further information).

Regular vulnerability scans and penetration tests are performed to ensure that the infrastructure is securely configured.

Physical access to the production environment is restricted to facility staff (for remote hands-on management of the physical hardware if needed), together with a select number of trusted Anaplan infrastructure engineering employees.

The facilities feature state-of-the-art physical security, including round-the-clock staffing and CCTV monitoring, two- and three-factor authentication at entry points, mantraps, and biometric scanners. Visitors must be pre-authorized, have their identity verified and be escorted through the facility. Facility staff are subject to the operating procedures required for SOC 1 Type II, SOC 2 Type II, and ISO 27001 compliance.

Summary

Anaplan operates in a decentralized way that gives significant resilience against threats and disasters. Near real-time backups, resilience and redundancy in the infrastructure, availability of secondary facilities, and the use of geographically distributed infrastructure support staff will enable disaster recovery plans to be implemented quickly and efficiently in the event of a major disaster.

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

Anaplan