Anaplan Google Cloud

# Anaplan on Google Cloud

**Delivering better together security across the public cloud**

## Cloud security overview

As customers continue their journeys to the public cloud as part of their digital transformation initiatives, security and privacy are top of mind for business and IT leaders. The good news is that the public cloud can improve security for many organizations. According to Gartner, "workloads that exploit public cloud IaaS capabilities to improve security protection will suffer at least 60% fewer security incidents than those in traditional data centers."

Security is a priority at both Anaplan and Google Cloud. That is why the Anaplan on Google Cloud offering is designed to deliver security across users, data, and the environment. This brief describes the security, privacy, and trust implemented at each layer of the Anaplan and Google Cloud stack as a shared responsibility model.

## The Anaplan on Google Cloud better together approach

Anaplan on Google Cloud deploys defense in depth across the physical, hardware, software, and operational layers to deliver a highly secure infrastructure and experience.

Anaplan is designed with security in mind, from networks and servers to how users can access and manage data. The Anaplan platform is a unique blend of proprietary technology that securely collects and stores data while providing the agility to interface with external systems. Anaplan maintains an atomicity, consistency, isolation, and durability (ACID)-compliant software stack that guarantees data in Anaplan models is kept in a known safe state.

Anaplan owns and operates all the equipment within its physical data center cages and manages all layers of the cloud platform. Anaplan leverages Equinix to provide physical security, redundant power, and environmental controls, such as temperature, humidity, and fire detection and suppression.

As customers move to transformation clouds, trust is a key element to securing your workload in the cloud. Google provides a trusted cloud environment that protects the enterprise workload, including people, customers, and data, while meeting regulatory and governance requirements.

For Anaplan on Google Cloud, Google manages physical security, redundant power, and environmental controls at the Google data centers. In addition, Google also manages its own physical servers, storage, and network between data. Anaplan operates and manages everything from the server operating system and up to the application.

Google's entire hardware infrastructure stack is custom designed to precisely meet their security requirements. If a vulnerability is found, Google can take steps immediately to develop and roll out a fix. This level of control results in greatly reduced exposure for us and our customers. Once data reaches Google's infrastructure, it is encrypted at rest by default, with no extra effort. Google regularly undergoes independent third-party audits to ensure continuous accreditation.

[1] MacDonald, Neil and Croll, Tom, "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center," Gartner, October 9, 2019.

## The Anaplan on Google Cloud shared responsibility model

Customers control access to their data, user accounts, and environment across both models.

| | Anaplan | | Google Cloud Platform | |
|---|---|---|---|---|
| Application | Anaplan | • Identity & access control<br>• Account takeover protection<br>• Web application firewall<br>• Digital certificates | Anaplan | • Identity & access control<br>• Account takeover protection<br>• Web application firewall<br>• Digital certificates |
| Service | | • Data-at-rest protection<br>• Gateway & API security<br>• Token authentication | | • Data-at-rest protection<br>• Gateway & API security<br>• Token authentication |
| Image | | • OS hardening<br>• Image scanning<br>• Antivirus/anti-malware<br>• Patch management | | • OS hardening<br>• Image scanning<br>• Antivirus/anti-malware<br>• Patch management |
| Software-defined Data Center | | • Network detection & response<br>• Data security<br>• Web application firewall | Google Cloud | • Intrusion detection<br>• Denial-of-service protection<br>• User authentication |
| Hypervisor | | • Firewall<br>• Event logging<br>• Patch management<br>• Malware protection | | • Patch management<br>• Reduced attack surface |
| Infrastructure | EQUINIX | • Hardware monitoring<br>• Hardware failover<br>• Security of physical premises | | • Hardware design/provenance<br>• Secure boot stack/machine ID<br>• Security of physical premises |

## About Anaplan

Anaplan (NYSE: PLAN) is a transformative way to see, plan, and run your business. Using our proprietary HyperblockTM technology, Anaplan lets you contextualize real-time performance, and forecast future outcomes for faster, confident decisions. Because connecting strategy and plans to collaborative execution across your organization is required to move business FORWARD today. Based in San Francisco, we have 20 offices globally, 175 partners and more than 1,700 customers worldwide.

**To learn more, visit Anaplan.com**