Fully air-gapped: A beginner's guide to Google Distributed Cloud Hosted

Google Cloud

Table of contents

Introduction

Not all workloads can move to the public cloud due to factors such as unreliable network connectivity, data volume, or low latency requirements. Additionally, government organizations, and policy makers around the world are increasingly concerned with security, governance, and control over access to their data and provider operations. That is where distributed cloud computing comes into play.

Distributed cloud is a type of cloud computing that extends the public cloud to multiple locations. This allows organizations to run their applications and data in the most appropriate location for their needs, while still meeting strict data residency, compliance, or latency requirements for their applications.

Our distributed cloud offering - Google Distributed Cloud - brings Google Cloud's infrastructure and services to diverse physical locations, also known as distributed environments, and can run in on-premises data centers as well as Google's network edge.

Google Distributed Cloud offers three distinct solutions:

01 Google Distributed Cloud Edge (GDC Edge) brings Google Cloud infrastructure and services closer to where data is being generated and consumed.

02 Google Distributed Cloud Hosted (GDC Hosted) enables you to host, control, and manage infrastructure and services directly on your premises.

03 Google Distributed Cloud Virtual (GDC Virtual) is a software-only solution that enables you to extend a consistent development and operational experience to your existing data center environments.

The rest of this book focuses on Google Distributed Cloud Hosted.

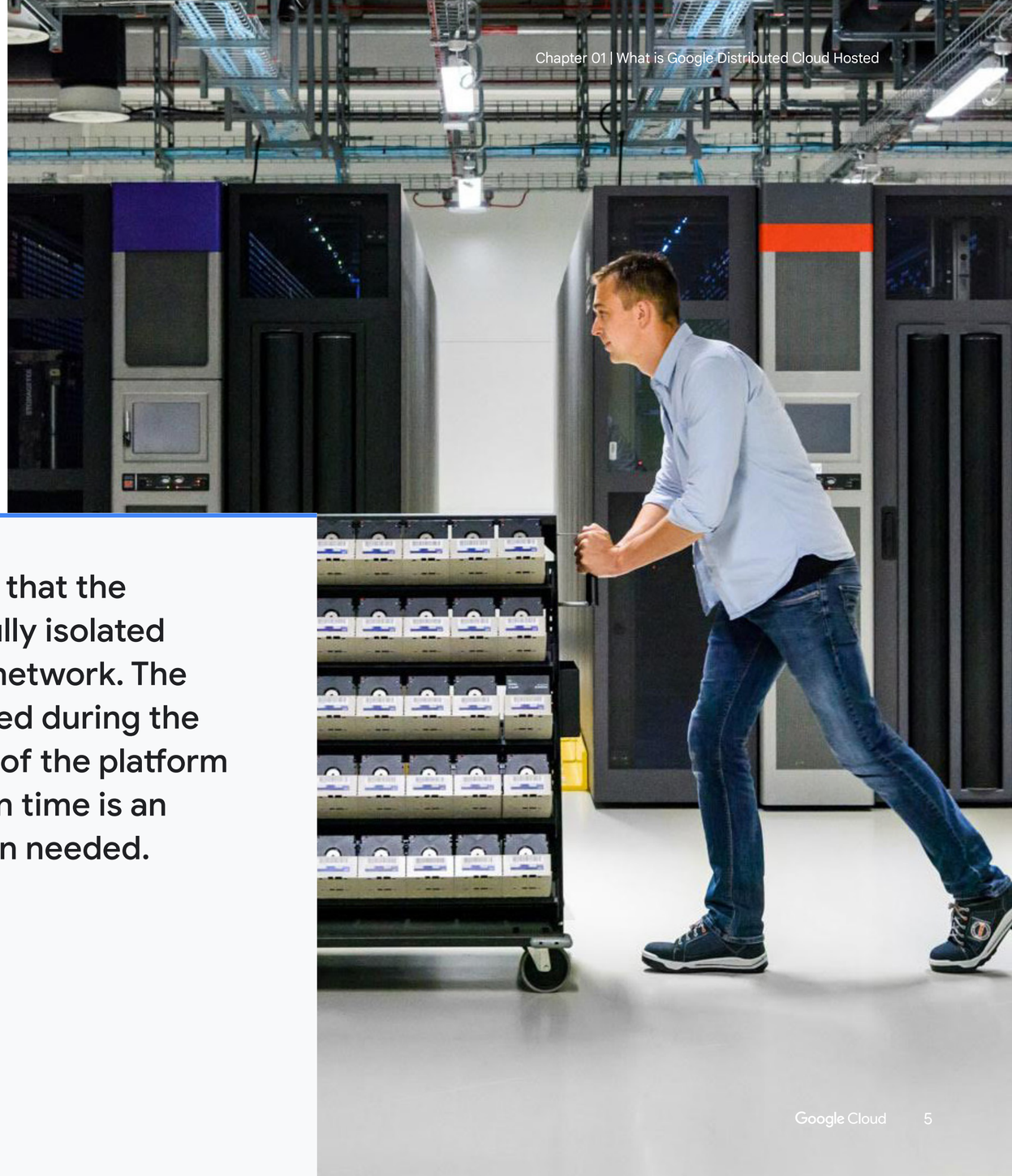
Chapter 01

What is Google Distributed Cloud Hosted?

GDC Hosted is a full stack, air-gapped private cloud solution purpose-built to meet sovereign requirements of customers with the most stringent security and compliance requirements, including classified, restricted, and top secret data.

It includes the hardware, software, local control plane, and operational tooling necessary to deploy, operate, scale, and secure a complete private managed cloud.

GDC Hosted delivers a fully managed cloud experience - even in highly regulated environments, without requiring a connection to Google Cloud or the Internet at any point in time. This opens up a new capability for customers with these challenges - enabling them to innovate, modernize, and migrate workloads in these environments in the same way they would with public cloud.



Air-gapped means that the platform can run fully isolated from any external network. The isolation can be used during the complete lifecycle of the platform hence at no point in time is an external connection needed.

Use cases

GDC Hosted is focused on customers who face the most stringent sovereignty, regulatory, or accreditation standards.

Public sector

Governments around the world benefit from GDC Hosted in the following ways:

- Analyze and translate sensitive documents containing personal identifiable information (PII) using Vertex AI optical character recognition (OCR) service.
- Use pre-trained AI/ML services to optimize natural disaster response, analyze infectious diseases, or detect fraud.
- Train machine learning models on sensitive economic datasets.

Financial services

GDC Hosted provides a flexible option for financial services firms to meet regional regulatory requirements while protecting sensitive financial information and trade secrets. A fully disconnected solution allows them to build resilience against any interruption in the public cloud, run closer to legacy computing systems like mainframes to reduce latency, and process data that cannot be put in a public cloud environment.

The IT landscape at financial institutions is particularly varied, with 40-year-old applications running alongside more modern systems.

Source

Healthcare

GDC Hosted provides a platform to improve latency for the local operation of medical equipment, and to enable the development and protection of sensitive clinical trial data. Healthcare providers also require secure storage capabilities to process sensitive data, including patient and disease registries for chronic conditions. GDC Hosted also provides a consistent deployment platform where data and applications need to be isolated to a region, country, or use case.

95% of patients are concerned about a potential data breach or leak of their medical records.

Source

Manufacturing

Modern manufacturing is a digital business, and GDC Hosted provides a solution that allows manufacturers a solution that allows manufacturers to ensure operations do not go offline or get disrupted. In cases where organizations such as auto manufacturers want to run AI against proprietary or patented data, and are unwilling to move to the public cloud or need low latency to process data tied to industrial devices in their facility, GDC Hosted is a great option.

Utilities

In the energy sector, GDC Hosted can help secure systems running critical, national infrastructure, and support remote environments such as offshore wind energy farms that have needs for computing resources but no access to the public cloud.

In Europe, Proximus selected GDC Hosted in a multi-year agreement to deliver sovereign cloud services for governments, regulated enterprises, and international organizations in Belgium and Luxembourg.

In the United States, the Department of Defense recently selected Google Cloud as an approved vendor in the Joint Warfighting Cloud Capability contract vehicle. This partnership will enable U.S. defense and intelligence communities to have greater flexibility in their cloud technologies, using solutions like GDC Hosted.

In Singapore, The Centre for Strategic Infocomm Technologies (CSIT) and Google Cloud announced they will be piloting the use of Google Distributed Cloud Hosted (GDC Hosted) to support CSIT's effort to harness AI in tackling Singapore's defense and security challenges.

Key features

01

Full isolation

GDC Hosted is air-gapped and does not require connectivity to Google Cloud or the public internet at any time to manage the infrastructure, services, APIs, or tooling. It is built to remain disconnected in perpetuity. Google designed GDC Hosted to explicitly meet the most stringent accreditation requirements.

02

Integrated cloud services

GDC Hosted delivers advanced Google Cloud services, including many of our industry-leading data and artificial intelligence (AI) technologies. Customers can use built-in AI solutions, such as Translation, Speech-to-Text, or optical character recognition (OCR)—all features of our Vertex AI platform.

03

Open ecosystem

GDC Hosted is built on Kubernetes, and uses leading open source components in its platform and managed services. Open software accelerates developer adoption by leveraging existing expertise and does not require customers to learn new, proprietary systems. GDC Hosted is also built to be extensible, and enables a growing ecosystem of independent software vendors (ISVs) to integrate through our marketplace for disconnected solutions.

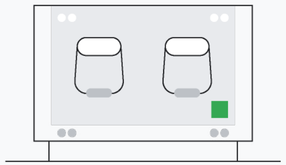
04

Flexible hardware options

GDC Hosted provides customers industry-leading flexibility for hardware including general purpose compute and GPUs. Customers can start small with as few as four racks and grow to hundreds as their needs scale.

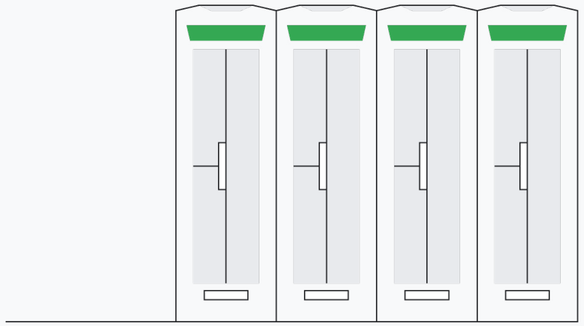
Flexible deployment options with a variety of form factors

Appliance



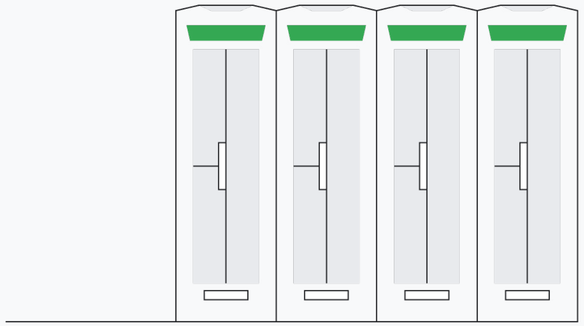
Human-Portable Rugged Appliance
Operated by customer in field

Modular Data Center



Full GDC Hosted cloud deployment
Trained operational staff

Data Center



Full GDC Hosted cloud deployment
Starts at 4 racks and scales as needed
Trained operational staff

Chapter 02

How it works

GDC Hosted is designed to deliver fully managed cloud services to customers who can’t take advantage of regular public cloud offerings for regulatory, compliance, or technical reasons.

It is therefore designed so users get the same benefits of the public cloud - a fully converged hardware and software stack, integrated and optimization operational tooling enabling operators to deliver public cloud like service levels, and a full suite of multi-tenant managed services.

This chapter looks into the platform architecture, hardware platform, tenancy model, and operational models that GDC Hosted can deliver to help customers solve their modernization or innovation challenges.

01

Multi-tenancy

GDC Hosted is a multi-tenant managed cloud platform just like Google Cloud. Its architecture is designed to deliver strong isolation between tenants, providing a strong layer of protection between users of the cloud, and allowing users to meet stringent workload accreditation standards.

02

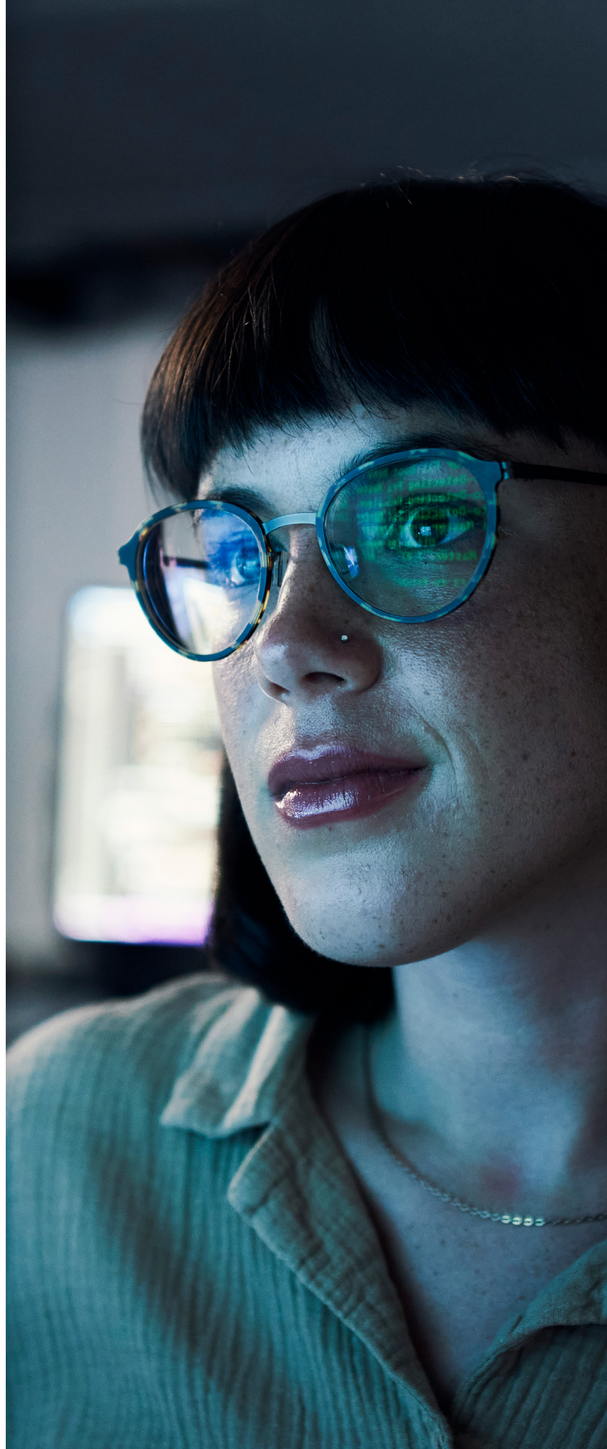
Deployment options

GDC Hosted provides flexibility in deployment architecture, enabling users to meet your technical and compliance requirements. A typical GDC Hosted deployment has at least three zones, in two locations, with at least one operations center. GDC Hosted can be self-operated, partner-operated, or Google-operated.

03

Networking options

GDC Hosted is designed to be air-gapped from the Google Cloud control plane. This is possible through the use of an operations center directly connected to GDC Hosted, enabling operators to manage it without using Google facilities or systems. Customers access the system usually through a wide-area network (WAN) or a dedicated private network.



04

Hardware options

GDC Hosted is designed to be a turnkey, fully integrated private cloud solution. This includes all the infrastructure (Compute, Storage, Networking, and Security) needed to operate the platform.

We recently announced next-generation machines with increased performance, flexibility, and modular scaling options. The new Google Distributed Cloud hardware stack features the 4th Gen Intel® Xeon® Scalable Processors and high-performance network fabrics with up to 400 Gbps throughput. The new machines also come with improved vCPU performance, DDR5 high bandwidth memory, Gen5 PCIe I/O performance, 400G/100G network links, and specialized GPUs for AI workloads with NVIDIA A100 chips to power AI and data processing applications in an air-gapped cloud environment.

Minimum deployment unit

GDC Hosted provides a minimum deployment model that requires 3 racks of space and one additional rack for operational tooling. This includes the control plane, initial compute capacity, security services, block, file, and object storage systems. This initial system is scaled by adding incremental compute, object, or block file storage racks. GDC Hosted can scale to support hundreds of racks per region.

Secure supply chain

Google Cloud and our partners provide options to enable customers to follow their secure supply chain requirements. Our vendors already meet or exceed requirements in all regions we support, and offer services like cleared personnel for hardware support or maintenance, support for drive or device destruction, and requirements like certification or origin, and secure shipment.

05 User experience

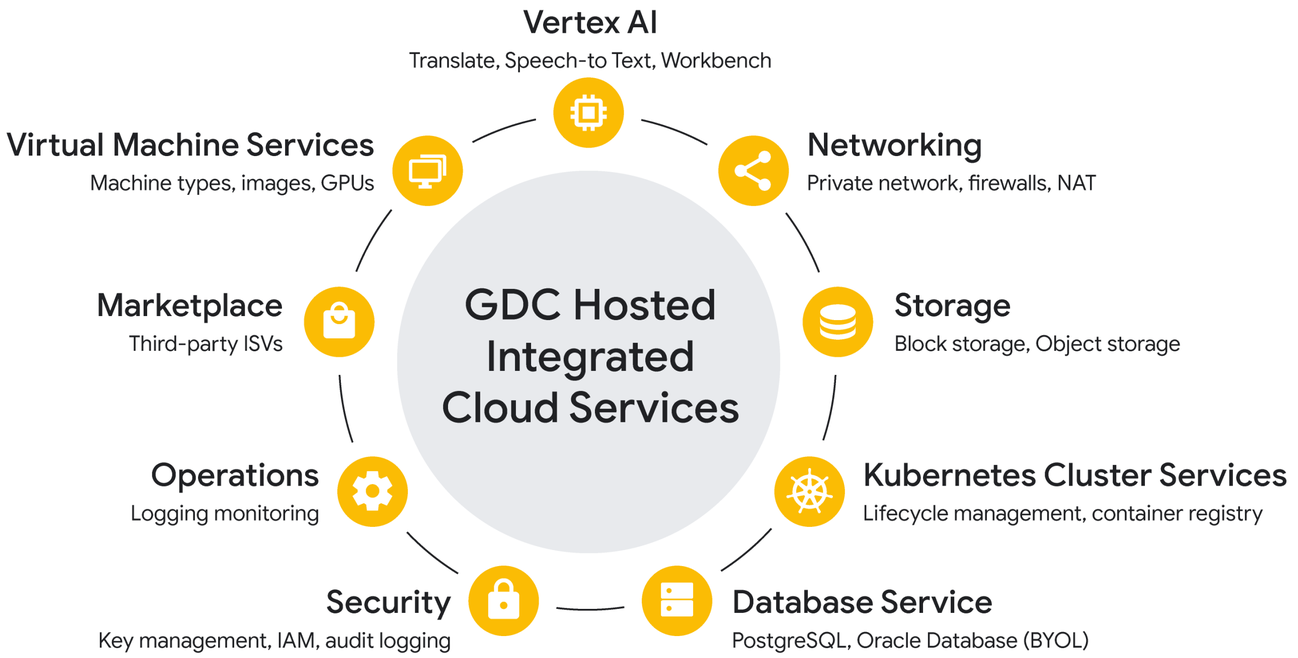
The overall user experience has been kept as similar to Google Cloud as possible. The user experience starts with a web-based user interface and extends to a command-line interface and API surface designed to enable scale and automation. GDC Hosted was built following the Web Content Accessibility Guidelines (WCAG) and conforms to the US Government's federal standards (US Section 508) and EU's (EN 301 549) standards for accessibility.

Chapter 03

Services

GDC Hosted delivers services ranging from standard VMs, containers, and storage, to advanced services like managed databases and AI/ML services. This section explores the various services available today on GDC Hosted.

GDC Hosted integrated cloud services



Compute

VM service

GDC Hosted provides the capability to run and manage your virtual machines instances. The VM service lets you deploy, manage, and secure workloads running in virtual machines instances on GDC Hosted, providing unified management, security policy, and observability across VMs and containers.

Cluster & container service

GDC Hosted offers a best of breed Google Kubernetes Engine (GKE) provided by the team that brought you Kubernetes. The Anthos GKE Clusters are fully managed and provide easy lifecycle operations. GKE provides a managed environment for deploying, managing, and scaling containerized applications.

Storage

GDC Hosted's storage offerings include block storage available to VM and Container workloads executed on GDC Hosted. High-performance object storage provided via an S3-compatible interface natively integrated with GDC Hosted. A workload backup service solution designed to allow users of the system to schedule backups and restores of their VM, and container-based workloads along with attached block and file volumes to local or remote storage solutions.

Artificial intelligence and machine learning

Our portfolio of artificial intelligence machine learning, and database products enable customers to quickly deploy services with out-of-the-box simplicity. GDC Hosted offers the best of Vertex AI's pretrained models, such as optical character recognition, translation, and speech APIs.

Networking

Virtual Private Cloud (VPC) provides logically isolated network functionality from other tenants. All project networks are subnets of this network and are by default isolated from other projects via denying all inbound traffic rules. Load Balancing internal and external provides the ability to expose workloads through load balancers, both internally to other workloads on GDC Hosted, and externally to systems outside of GDC Hosted.

Databases

The GDC Hosted database service supports PostgreSQL and Oracle database engines. We recently added support for AlloyDB Omni as a new managed database engine. AlloyDB Omni is more than 2x faster than standard PostgreSQL for transactional workloads, and delivers up to 100x faster analytical queries than standard PostgreSQL.

Observability

The GDC Hosted Observability Service collects and tracks relevant telemetry data, for example, metrics, operational logs, audit logs, to provide visibility into the health and performance of the GDC Hosted system and user workloads to the users of the system. The Observability Platform consists of 2 core services - a monitoring service and a logging service.

Marketplace

The GDC Hosted Marketplace lets users easily access and deploy solutions from popular independent software vendors (ISV) in their own environments. Currently, the marketplace supports a bring-your-own-license (BYOL) model for ISVs, allowing customers who already have licenses to use them and receive support directly from the ISV.

Identity and access management (IAM)

IAM manages the access to sensitive resources to keep them secure from unauthorized use and to help support rigorous compliance requirements. GDC Hosted's authorization model manages access control policies and defines permissions, roles, and role bindings. IAM is unique per organization.

Migration

Customers with virtual machines can run Fit Assessment Tools on their existing environment to establish a baseline. This tool collects data from sources in fully disconnected & controlled mode, allows them to execute reports with aggregated information and provides prescriptive guidance and a curated strategy based on over 300 rules. GDC Hosted also offers migration options for containers, databases, and storage.

Chapter 04

Operations & platform security

Operations suite

The GDC Hosted comes with an Operations Suite that contains the necessary hardware, software, tooling, specifications and facility guidelines to successfully operate an instance of GDC Hosted. It includes an extensible operating model - a comprehensive library of operational processes, workflows, and guidance for operating partners to use when deploying and managing GDC Hosted.

Billing

Customers interact with billing through features such as cost dashboards, resource usage labels, spend threshold alerts, pricing calculator, invoice data export API. Billing on GDC Hosted is computed in an air-gapped environment that is not connected to Google Cloud - no individual customer's consumption is visible in the Google Cloud console.

Platform updates & upgrades

Software upgrades to the air-gapped private data centers cover the entire stack, including applicable device drivers, firmware, operating systems, core platform software, and services.

Upgrades and patches are a shared responsibility between the GDC Hosted operator and the users of the system. The core platform capability allows automated software delivery and upgrade processes for GDC Hosted components, services, and user resource.

Platform security

GDC Hosted takes a security-first approach with multiple layers of security to deliver maximum control while maintaining compliance with statutory regulations and safeguarding confidential data. It is designed to run on dedicated and secured hardware in a local data center to provide strict tenant isolation.

Secure software development life cycle (SDLC)

To protect against software supply chain attacks, all GDC Hosted software is developed in accordance with the SLSA (Supply chain Levels for Software Artifacts) security framework developed by Google in partnership with organizations including the CNCF and the Linux Foundation.

Conclusion

As you conclude your exploration of Google Distributed Cloud Hosted, let's recap the key takeaways that will empower you to navigate the world of distributed cloud computing with confidence.

Recap of key takeaways

01

Unleash the power of a fully disconnected cloud

GDC Hosted provides a secure and isolated cloud environment, enabling you to run sensitive workloads without compromising data privacy or regulatory compliance.

02

Empower modernization and innovation

GDC Hosted empowers you to modernize even your most sensitive workloads, leveraging Google Cloud's advanced technologies and services to drive innovation and enhance business outcomes

03

Tailored to regulated industries

GDC Hosted is specifically designed for organizations in regulated industries, such as government, financial services, healthcare, and manufacturing, ensuring compliance with strict data residency, security, and privacy requirements.

04

Unlock flexibility and scalability

GDC Hosted offers flexible hardware options and a fully redundant, high-availability architecture, allowing you to tailor your cloud infrastructure to meet your specific needs and scale seamlessly as your business grows.

Hit the ground running.

To further your learning and delve deeper into the world of GDC Hosted, explore our documentation pages

→ Learn more

Google Cloud