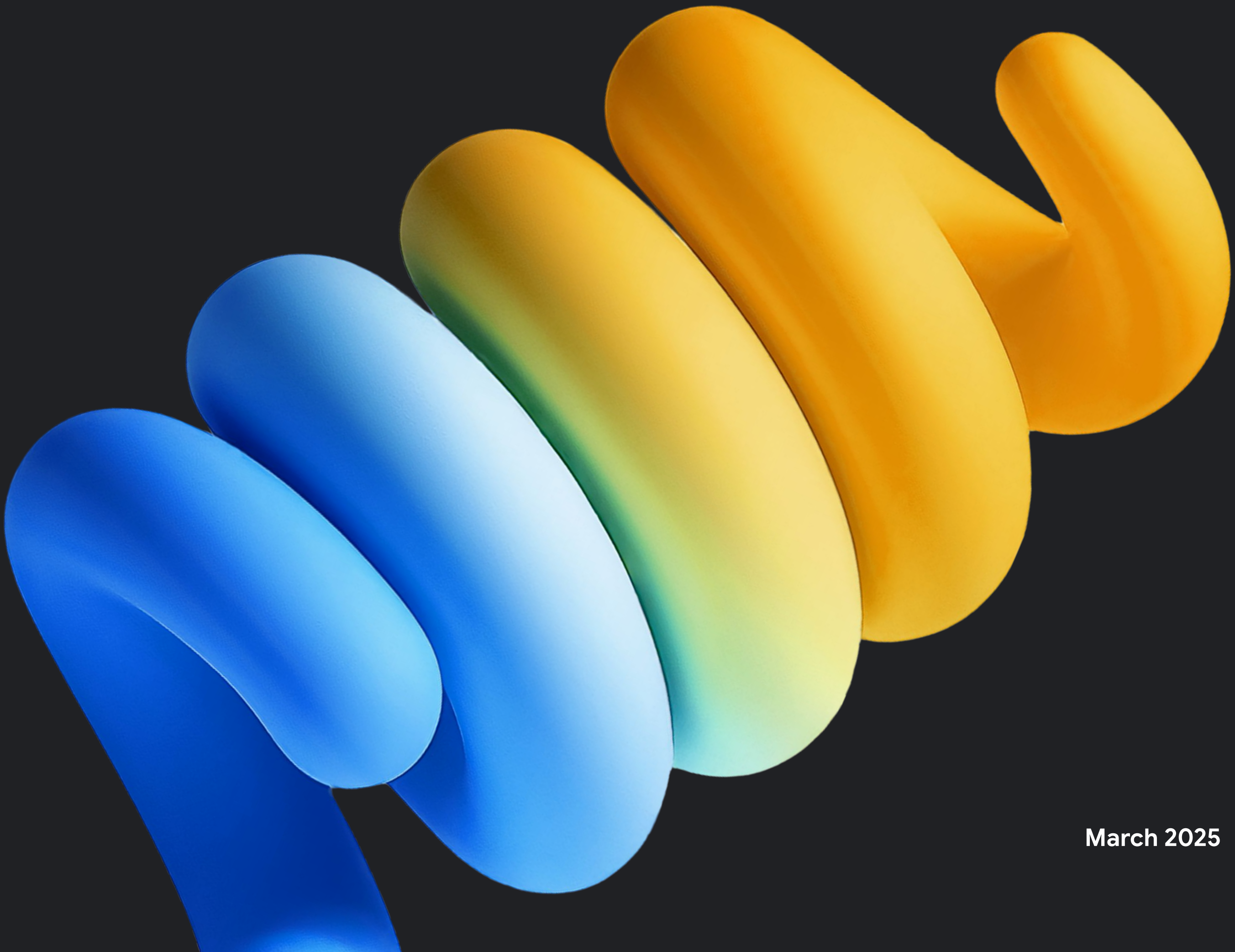
Google Cloud

Zero Trust Strategy

Google Distributed Cloud air-gapped



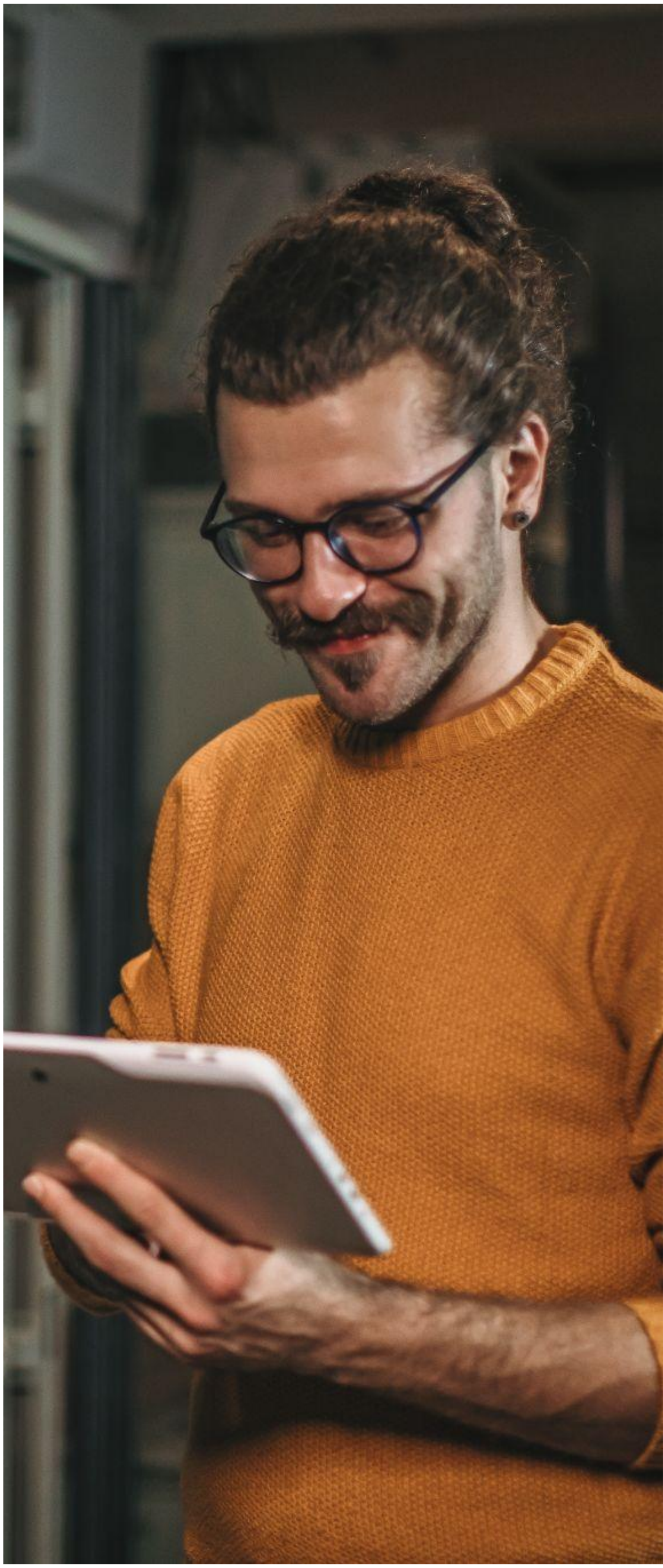
March 2025

Zero Trust Approach

Helping secure your sovereignty and accelerate results: A guide to Zero Trust with Google Distributed Cloud air-gapped

Security is a prerequisite for sovereignty, as an organization's ability to protect itself from threats is essential to maintain its independence and autonomy. Google Distributed Cloud air-gapped reinforces this concept by providing a secure and sovereign infrastructure for organizations to store and process data within their own borders, while maintaining control over their critical workloads. As cyberattacks become increasingly relentless and sophisticated, traditional security approaches fall short.[1] The *2023 Verizon Data Breach Investigations Report* finds that 74% of all breaches include the human element involving negligence, privilege misuse, or stolen credentials.[2] Statista estimates the average cost of a US data breach in 2023 was $4.45 Million dollars.[3] The frequency and cost of cyber attacks requires organizations to consider a fundamental shift from traditional perimeter defense to Zero Trust models.

Zero Trust is a security framework grounded in the principle of "never trust, always verify." It protects against cyberattacks by strategically limiting trust within systems and networks, assuming all users and devices are inherently untrustworthy. Google Distributed Cloud offers the agility and scalability of public cloud, with a key distinction: it's specifically designed for highly regulated industries, including national security, regulated enterprises, and those with sovereignty needs. It provides control to deliver data, software, and operational sovereignty within your environment.



[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[2] https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/
[3] https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/#:~:text=As%20of%202023%2C%20the%20average,million%20U.S.%20dollars%20in%202023

What is Zero Trust?

In a Zero Trust model, traditional trust boundaries dissolve. Every access attempt requires authentication and authorization. A robust security posture requires both asset-based protection and continuous monitoring. The former shields known weaknesses, while the latter proactively detects and neutralizes emergent threats. This approach safeguards organizations against a vast spectrum of cyber threats.

No implicit trust

A "trust boundary" no longer applies to a modern infrastructure.

Authentication and authorization

Authentication and authorization are discrete functions that must be performed on a session basis.

Protect resources, not network segments

Network location is no longer a core component of enterprise security posture.

Google Distributed Cloud delivers Zero Trust by design, eliminating implicit trust by requiring continuous authentication and authorization for every user, device, and workload. It extends data protection beyond creation with granular permissions, safeguarding information throughout its entire lifecycle. Google Distributed Cloud air-gapped provides two or more layers of data encryption on customer data including support for Hardware Security Modules (HSMs) and Customer Managed Keys (CMEK).

Industry-leading Mandiant detection schemas power logging and telemetry analysis, exposing threats and streamlining security operations. Automation replaces tedious manual tasks and provides immutable audit trails. Most importantly, you won't lose the cloud's advantages – Google Distributed Cloud allows you to harness cutting-edge artificial intelligence (AI), data analytics, and seamless management protected by a Zero Trust architecture. This whitepaper provides a foundation for applying Zero Trust to your Google Distributed Cloud air-gapped workloads today.

01
Benefits of Zero Trust

Air-gapped networks, while physically isolated, are not immune to threats and bad actors. Air-gapped networks shouldn’t extend trust to allow lateral movement without incremental authorization and monitoring. Zero Trust architecture recognizes this, raising the security bar even within these seemingly secure environments. Here's why organizations are embracing Zero Trust principles.

Enhanced data confidentiality and integrity

Air-gapped clouds often host highly sensitive data. Zero Trust bolsters protection through micro-segmentation, data flow monitoring, and encryption. This ensures that even a successful breach faces further barriers, safeguarding data integrity.

Defense against insider threats

Air-gapped clouds deter external attacks, but insiders remain a risk. Zero Trust combats this with granular access controls, limited privileges, and targeted monitoring to minimize the potential impact and blast radius of malicious insiders or compromised accounts.

Resilience against supply chain attacks

Air-gapped clouds depend on supplied components and software. Zero Trust treats every connection and asset as potentially compromised, demanding strict authentication and authorization to isolate threats should a software or hardware supply chain weakness emerge.

What Zero Trust is Not

Conversely, understanding what Zero Trust **is not** is key to fully appreciating its potential. It's important to remember that Zero Trust is a security framework built upon principles and policies – not a singular tool or solution. Implementing Zero Trust involves a variety of tools and technologies tailored to specific organizational needs. Zero Trust is an ongoing journey of continuous refinement, not a fixed destination. Zero Trust shouldn't be viewed as a silver bullet solution, but rather a vital component of a comprehensive security journey.

02

GDC Zero Trust principles & pillars

Secure Access

Every user and device, whether internal or external, undergoes rigorous, continuous authentication and authorization. Access is granted based on identity, device health, context, and resource sensitivity, always enforcing the principle of least privilege.

Secure Data

Prioritizing data protection throughout its lifecycle. Sensitive data is protected with robust encryption at rest and in transit, coupled with granular access controls to ensure users and admins access only what's necessary.

Secure Apps

Move beyond network segmentation, focusing on individual apps and resources. Microsegmentation isolates applications to prevent lateral movement. Access is governed by context-aware policies factoring for user, session, and context.

Visibility & Control

Google's analytics empower comprehensive visibility within air-gapped clouds. In Google operated models, continuous monitoring provides threat detection capabilities while maintaining comprehensive audit logging.

Google's Zero Trust principles fundamentally reject the notion of a trusted internal network versus an untrusted external one. Instead, they operate under the premise that threats can exist anywhere, thus every user, device, and network flow must be authenticated and authorized – regardless of location.

This approach is essential in today's world of distributed work environments and the rising prevalence of sophisticated cyberattacks. Google's Zero Trust model enhances security posture and reduces the potential for successful breaches by continuously verifying access permissions and closely monitoring user and device behavior. This proactive approach minimizes the attack surface, helps protect sensitive data and resources, and allows organizations to adapt more securely to the ever-evolving threat landscape. Ultimately, Zero Trust enables organizations to confidently embrace the flexibility and benefits of modern cloud technologies and remote work without compromising security.[4]

Shared Responsibility Model

Google Distributed Cloud air-gapped has a shared security model for securing the complete application stack. GDC provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Google Distributed Cloud supports both Google-Operated and Partner-Operated options for infrastructure operation:

Google-Operated: Google manages the underlying infrastructure, platform, and core security of the air-gapped environment. Customers deploy, manage, and secure their applications, with shared responsibility for identity/access management and certain network security aspects.

Partner-Operated: A trusted partner manages the infrastructure, while securing the underlying infrastructure layers. Customers focus on the security of their data, workloads, and applications.

In all configurations of Google Distributed Cloud air-gapped, the customer is responsible for securing the project setup and application layer, including the application containers, base images, and dependencies. From a security perspective, the following personas operate GDC. See Security Strategy for more details.

Infrastructure Operator

Manages the day-to-day operations of the system infrastructure. This persona is the highest level administrator of the system and could be Google, acustomer-trusted third party, or the customer, depending on the nature of sovereignty restrictions.

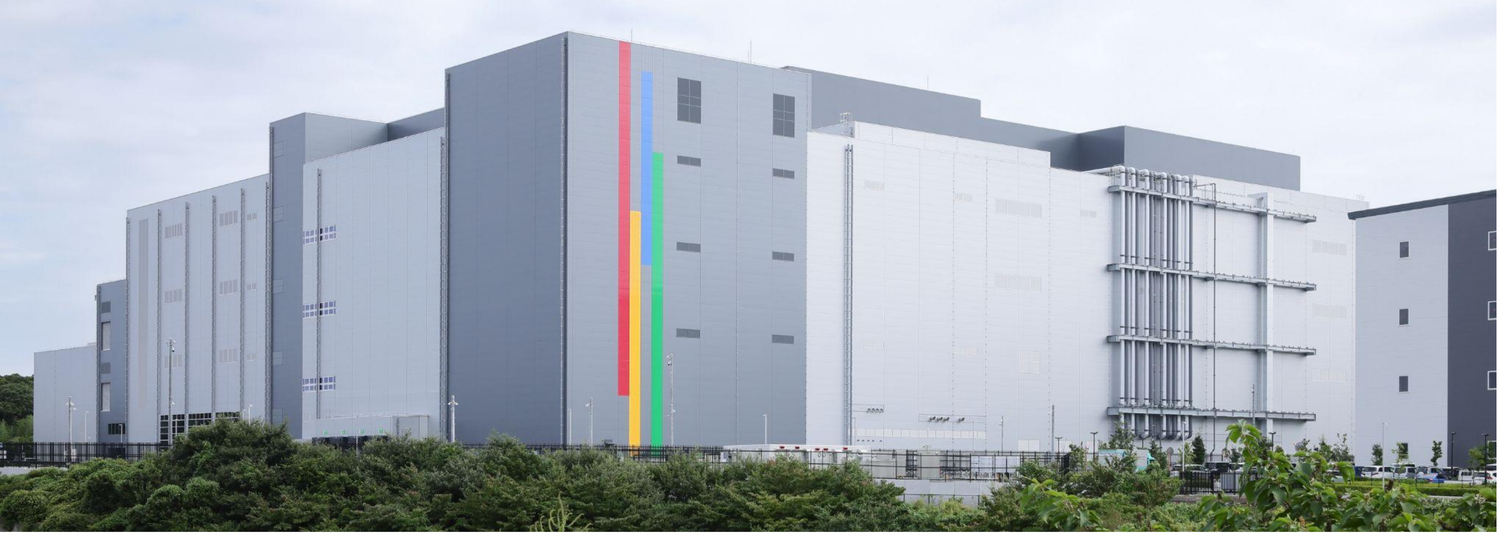
Platform Administrator

A customer end-user persona that manages resources and permissions for projects. This is the highest level of administrative privilege granted to the customer and is the only administrative level that can grant access to customer data.

Application Operator

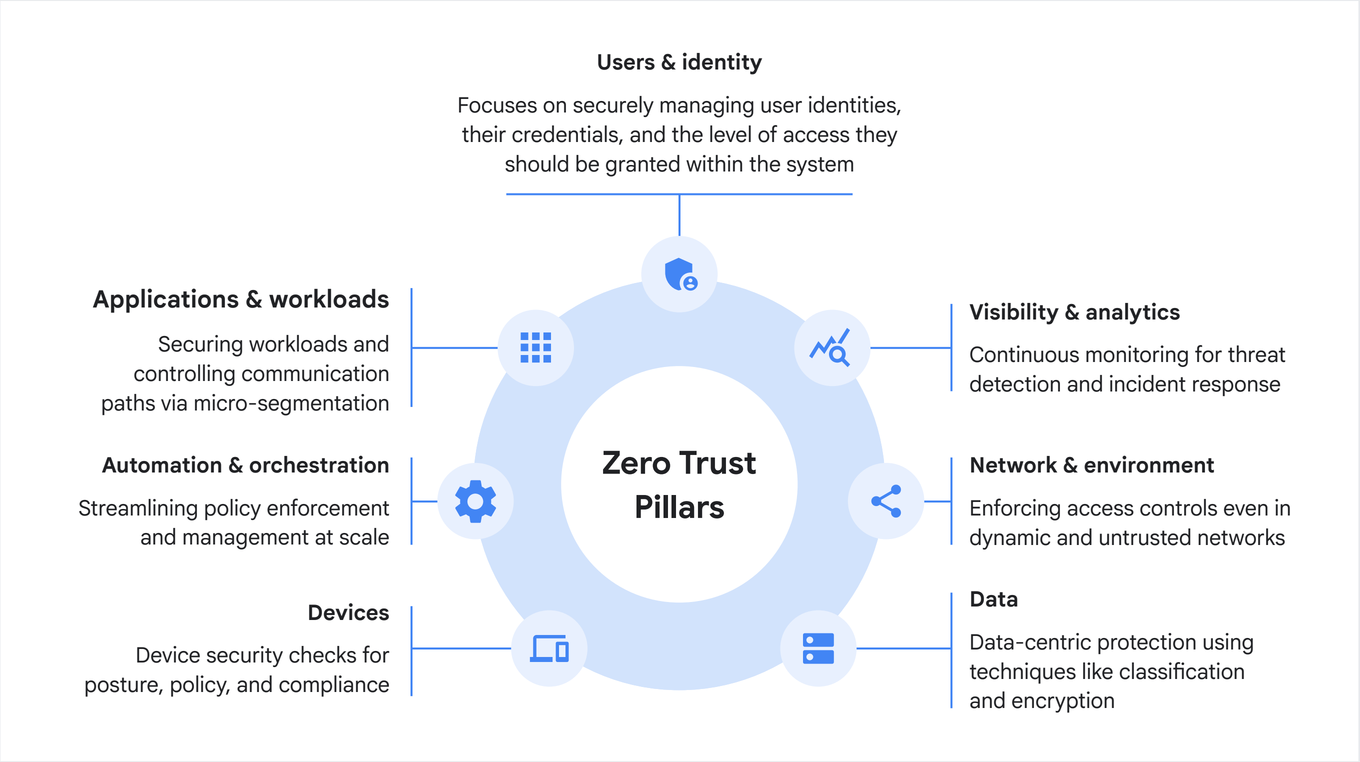
A customer end-user persona that develops, deploys, and services. This persona works within policies established by the Platform Administrator (PA) to ensure their systems align with the customer's security and compliance requirements.

[4] https://cloud.google.com/learn/what-is-zero-trust



Zero Trust Pillars

Google Distributed Cloud leverages the following Zero Trust pillars to enforce these principles — by enforcing strict controls, contextual awareness, and a focus on asset-level protection, the Zero Trust framework reduces the attack surface and the potential impact of attacks.



Users & identity

Focuses on securely managing user identities, their credentials, and the level of access they should be granted within the system

Applications & workloads

Securing workloads and controlling communication paths via micro-segmentation

Visibility & analytics

Continuous monitoring for threat detection and incident response

Automation & orchestration

Streamlining policy enforcement and management at scale

Network & environment

Enforcing access controls even in dynamic and untrusted networks

Devices

Device security checks for posture, policy, and compliance

Data

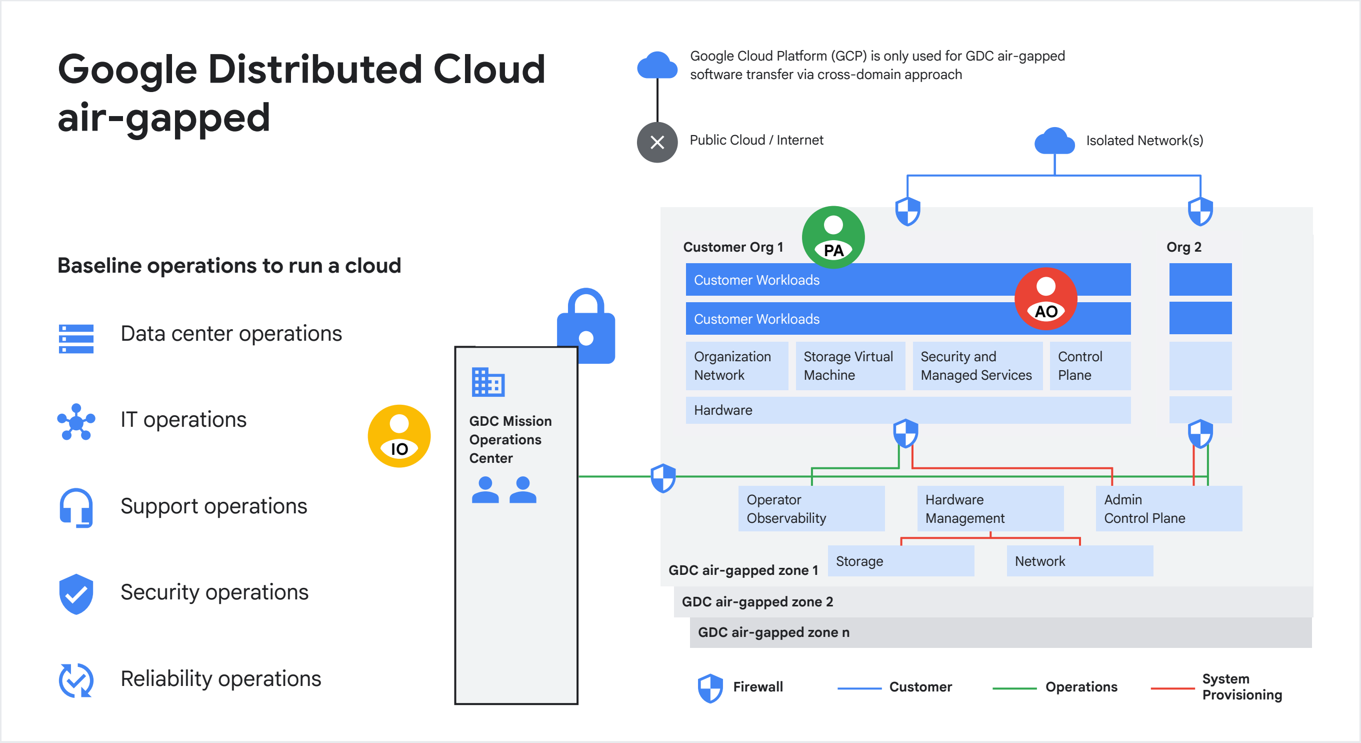
Data-centric protection using techniques like classification and encryption

Google Distributed Cloud

Enterprises, government organizations, and policy makers around the world want to partner with hyperscale cloud providers that deliver cloud on their terms — ones that meet their requirements for digital sovereignty while still delivering the innovation, functionality, flexibility, and scale of cloud services. Google Distributed Cloud provides a full stack offering that does exactly this. GDC air-gapped is a disconnected private cloud solution purpose-built to meet sovereign requirements. This enables customers with the most stringent security and compliance requirements, including classified, restricted and top secret data.

Google Distributed Cloud is a direct result of Google Cloud's commitment, made in 2020, when we introduced our digital sovereignty vision that included three distinct pillars: data sovereignty, operational sovereignty, and software sovereignty. We then built upon this vision with a portfolio of sovereign solutions delivered by Google Cloud and partners. GDC includes the hardware, software, local control plane, and operational tooling necessary to deploy, operate, scale, and secure a complete managed cloud. Additionally, GDC natively integrates with commonly used third party systems including:

- Hardware security modules which add extra layers of protection
- Security Operations and Observability tools for monitoring
- DevSecOps tools to enhance developer, security and operator productivity



Google Distributed Cloud air-gapped

Baseline operations to run a cloud

- Data center operations
- IT operations
- Support operations
- Security operations
- Reliability operations

03

Google’s Zero Trust Journey

Google's Zero Trust journey began as a response to the sophisticated Operation Aurora cyberattack in 2010, which exposed the vulnerabilities of traditional perimeter security models.[5] Google developed BeyondCorp, an internal implementation of Zero Trust that focuses on device and user-based authentication and authorization, regardless of network location.[6] Google’s commitment to Zero Trust is evident in community contributions, open-source tools, and industry collaborations. The $10 billion cybersecurity pledge in 2022 and acquisition of Mandiant reinforce Google's focus on advancing Zero Trust technologies and incident response capabilities. Today, Zero Trust is a cornerstone of Google's security strategy, integrated into its products and guiding its ongoing innovation within the cybersecurity landscape.

Operation Aurora A series of cyber attacks called Operation Aurora target 20+ tech companies	2009
First Zero Trust paper is written The new theoretical publication of a zero trust model is introduced	2010
Google implements internally Google's Zero Trust implementation proves to be successful	2015
Got rid of VPNs Google achieves 100% cloud and full multi-factor authentication	2016
BeyondCorp Enterprise Commercializes BeyondCorp for organizations to benefit from Google's learnings	2019
Cyber Executive Order Google attends a White House Cybersecurity meeting	2021
Google Cyber Commitment Google pledges to provide tech training to 100,000 Americans and invest $10B to advance cybersecurity	2022

[5] https://blog.google/outreach-initiatives/public-policy/transparency-in-the-shadowy-world-of-cyberattacks/
[6] https://research.google/pubs/pub43231/

Traditional Perimeter Model

The traditional perimeter security model operated like a piece of candy with a hard outer shell and a soft, trusting center. This assumed a clear divide between "trusted" inside users and "untrusted" outside threats.[7] Sadly, the rise of cloud technologies, mobile devices, and sophisticated attacks has proven this model squishy and outdated. Bad actors can exploit internal weaknesses or compromised credentials, breaching the outer shell with ease. This flawed internal trust becomes a serious vulnerability. Zero Trust changes the paradigm with a "never trust, always verify". Continuously authenticating and authorizing every user and device, regardless of location, creates a far more robust and adaptable security posture in today's complex threat landscape.

[7] https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf

Zero Trust Guidance

Google Distributed Cloud’s Zero Trust Architecture is informed by a comprehensive blend of industry-leading guidance documents, lessons learned and product offerings to provide robust security for air-gapped environments including the below. Disclaimer that “informed/influenced” does not imply compliance with or for respective standards:

Google BeyondCorp Enterprise[8]

Air-gapped environments often host highly sensitive data. Protection is bolstered through micro-segmentation, data flow monitoring, and encryption. This ensures that even a successful breach faces further barriers. Learn more

NIST SP 800-207

This foundational publication by the National Institute of Standards and Technology outlines the key principles and logical components of a Zero Trust Architecture (ZTA).[9]

National Security Memorandum 8

National Security Memorandum on Improving the Cybersecurity of National Security Systems, NSM-8 mandates a Zero Trust approach for critical government systems.[10]

Trusted Internet Connections 3.0

The Trusted Internet Connections (TIC) program provides guidance for federal agencies, including a strong focus on evolving to Zero Trust principles.[11]

CISA Zero Trust Model

The Cybersecurity and Infrastructure Security Agency (CISA) model provides a practical roadmap and maturity model for organizations transitioning to Zero Trust.[12]

DoD Zero Trust Model

The Department of Defense Zero Trust Reference Architecture outlines a detailed implementation strategy for Zero Trust within DoD environments.[13]

[8] Google BeyondCorp Enterprise isn’t currently available for Google Distributed Cloud air-gapped

[9] https://csrc.nist.gov/pubs/sp/800/207/final

[10] https://cloud.google.com/gov/cybersecurity

[11] https://www.cisa.gov/tic

[12] https://www.cisa.gov/zero-trust-maturity-model

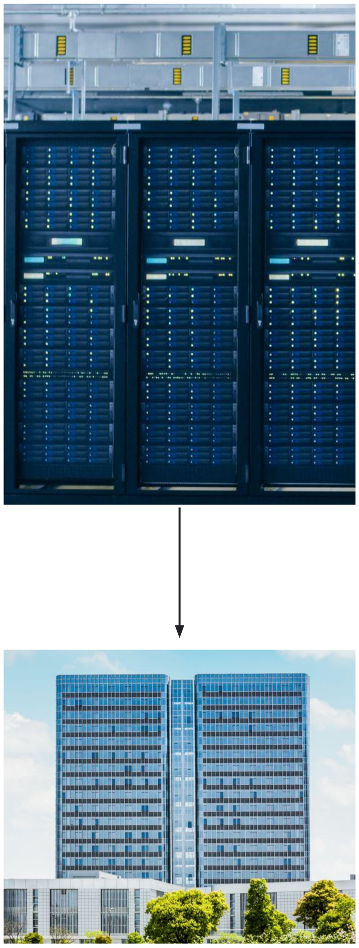
[13] https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Building upon the principles of Industry Zero Trust Frameworks, Google Distributed Cloud offers a powerful, multi-layered security stack designed for the most critical environments. It transcends best practices by physically isolating hardware and integrating them with Google's cutting-edge security technologies.

This unique approach safeguards infrastructure, applications, and data at every level. Strict tenant isolation keeps your workloads separate, relentless monitoring ensures constant vigilance, and robust encryption protects your data at rest and in transit. All of this is deployed within a customer-controlled environment, empowering you to tailor security to your specific needs. Google Distributed Cloud goes beyond theoretical best practices and delivers tangible security outcomes.

Google Distributed Cloud security best practices

GDC air-gapped



Identity & Access Control

Manage digital identities, use multi-factor authentication, federated identity providers, and granular controls to prevent unauthorized system access.

Audit Logging

Set a minimum standard of what is logged and monitored for security. This should be a default feature that helps detect and investigate attacks.

Encryption

Customer-managed keys, centralized certificate authority, FIPS 140-2 level 3 HSMs, mandatory data encryption, secure boot, integrity tools.

Security Monitoring

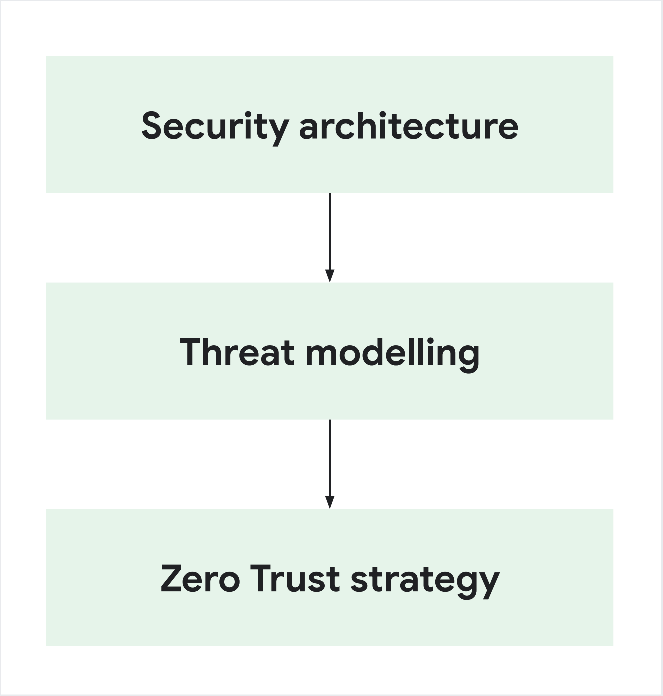
24/7 monitoring, vulnerability management, endpoint security, and Mandiant powered threat intelligence.

Software & Hardware Supply Chain

Mitigate supply chain risks with comprehensive security measures including source build verification, binary authorization malware detection, trusted vendors, and chain of record tracking for both hardware and software.

We’re just getting started

These are just a few of the features and capabilities that organizations in a variety of industries can use with Google Distributed Cloud air-gapped to build Zero Trust workloads — while enjoying state-of-the-art infrastructure and operational features, giving you your cloud, your way. If you’re interested in bringing the power of Google Cloud to the edge of your data center using Google Distributed Cloud reach out to us to schedule a security engagement and check out our resources.



Security architecture

Threat modelling

Zero Trust strategy

Google Distributed Cloud - Security Strategy

Google NEXT 2024 Keynote Announcement

Run Data & AI Anywhere with New Google Distributed Cloud Services

Zero Trust Implementation Guide

Pillar	Feature	Guide
User & Identities	**User Inventory & Credentialing** External IdP (Identity provider). It uses Anthos Identity Service (AIS) - an authentication service that lets users bring their existing identity solutions for authentication and supports both SAML 2.0 and OIDC (OpenID Connect) for IdP federation.	Connect to an identity provider Grant & revoke access Identity & Access Management
	Conditional User Access Anthos Identity Service (AIS) to authenticate users. The system supports both SAML 2.0 and OIDC (OpenID Connect) for IdP federation. Access is based on rules of least privilege. Role Based Access Control (RBAC) is used to authorize all control planes and data access. Open Policy Agent (OPA) Gatekeeper is used for customer-defined policies.	Grant and revoke access Predefined role descriptions Role definitions
	Multi-Factor Authentication GDC requires MFA for privileged users in the operations center using hardware tokens. GDC supports BYO-IdP and syncs to customer's organization via SAML/OIDC protocols. MFA is dependent on the capability of the customer's IdP. If BYO-IdP supports MFA, GDC meets the requirement for privileged access via MFA.	Connect to an identity provider Sign in
	Privileged Access Management Enforced via Infrastructure as Code (IaC) and Anthos Config Management (ACM) for reconciliation. Any privileged/elevated access required, for example, to repair the system during exceptional events, requires multi-party authorization, two-person integrity, temporary elevation, activity audit, and an account reset upon completion.	Administrative Overview Security Strategy Identity & Access Management Break glass access IaC

Pillar	Feature	Guide
User & Identities *Continued*	**Behavioral & Contextual Identification** External IdP (Identity provider) synchronization for RBAC and ABAC access control; User and entity behavior (UEBA) data is captured using custom monitoring analytics to detect anomalous and malicious activities. This includes monitoring and detecting abusive or excessive privilege access requests or sessions.	Request threat protection Security Operations Marketplace overview
	Least Privileged Access Granular RBAC and ABAC for access control, and access is based on principles of least privilege. Configuration changes are done using Infrastructure as Code, which requires multi-party authorization. The platform is designed with "No Implicit Trust" or Autonomous capabilities. All privileged access and API activity is promptly audit logged and monitored.	Connect to an identity provider Sign in Identity & Access Management
	Continuous Authentication Sessions are time-bound for inactivity and 15+ minutes triggers logout, while active sessions last a maximum of 12 hours. Privileged access adheres to Just-in-Time (JIT) and Just-Enough-Access (JEA) principles, with customizable expiration based on the task. This allows granular control, like longer access for observability versus short access for sensitive operations. There are concurrent session limits for both users and administrators, further enhancing authentication monitoring.	Grant & revoke access Authenticate with service identities Identity & Access Management
	Integrated ICAM Platform Authentication leveraged in a BYO-IdP model including centralized Private Key Infrastructure. X.509 CA management with trust distribution for the central root certificates. Each user and asset communicated in the network is authenticated (on application level).	Connect to an identity provider PKI Encryption

Pillar	Feature	Guide
Devices	**Device Inventory** GDC air-gapped collects telemetry from multiple systems and device attributes captured include hostname, vendor info, model, serial number, Mac Address, and IP Address. Separate vulnerability reports that are generated periodically highlight device inventory and potential vulnerabilities. This is also integrated with SIEM for continuous monitoring of potential rogue assets.	VMs overview Audit logs overview Security Operations Marketplace overview
	Hardware Device Security Google manages hardware security qualifications, collaborating with vendors to address issues, ensuring a secure supply chain, platform certificate verification, and secure boot, while also overseeing vulnerability and patch management.	Security Strategy Hardware Security Compliance Processes
	Device Detection & Compliance Rogue Asset detection via security monitoring capabilities. This is reinforced by security workflows in the Google Distributed Cloud Incident Response Plan and product collateral. Google Distributed Cloud also provides vulnerability management for incremental vulnerability scanning, STIG, and device compliance assessments.	Create org network policies VMs overview Audit logs overview Security Operations Marketplace overview
	Device Authorization & Inspection Google Distributed Cloud air-gapped provides several Endpoint Detection & Response (EDR) platforms for admin planes and GDC Marketplace offerings for customer planes. EDR facilitates monitoring, detection and remediation of malicious activity on endpoints. EDR tools provide Next Gen Anti-Virus, Heuristic/behavioral-based monitoring, risk assessment, PKI integration, and entity activity monitoring. There are also device controls for audit logging, configuration management and secure boot.	Security Operations Log and monitor Marketplace overview

Pillar	Feature	Guide
Applications & Workloads	**Vulnerability & Patch Management** Comprehensive vulnerability management system that uses multiple scanners to check for vulnerabilities, pull the appropriate patches, and test the patches using automated CI/CD systems. Once the patch release is certified in Google, it is made available to air-gapped deployments. After the patch is transferred to the air-gapped deployment (through a secure device), the patch application is automated.	Vulnerability Management Configure an upgrade Upgrade Gdcloud artifacts patch
	Application Inventory Comprehensive Software Bill of Materials (SBOM) in a machine-readable format (SPDX). Only accredited and approved features are provided to users in Google Distributed Cloud deployments.	Deploy container workloads Deploy applications Application Security
	Secure Software Development & Integration Google follows the Secure Software Development Framework recommendations and those laid out by the SLSA framework for secure development practices, including two-person code review. Security is ingrained into the development process with security reviews of design and code, incremental threat modeling and periodic pen-testing. Google Distributed Cloud provides several inbuilt controls for Container and pod security and provides different mechanisms for the user to specify the appropriate security context for their container. Serverless technologies are not offered in Google Distributed Cloud. Google Distributed Cloud provides continuous monitoring systems with runtime protections.	Developer Overview Application Security Compliance processes

Pillar	Feature	Guide
Applications & Workloads *Continued*	**Software Risk Management** GDC air-gapped provides a comprehensive SBOM (Software Bill of Materials), incorporates numerous checks to ensure dependencies, including open source components, are downloaded from approved and trusted sources with baked-in integrity checks (Cryptographic validations), and has a thorough vulnerability management program with multiple scanners to remediate or mitigate vulnerabilities within the FedRAMP-mandated service-level objectives (SLOs). Additionally, runtime CONMON systems, STIG controls, etc., continuously verify that the system is running with the desired configuration.	Developer Overview Application Security Compliance processes
	Resource Authorization & Integration Infrastructure as Code (IaC) enforces CI/CD pipelines and respective change management enforcement via the Anthos Configuration Management reconciler. An unauthorized system level change is automatically rolled back if not committed to IaC. For users/devices, these are monitored via change management and unauthorized entities trigger security monitoring procedures.	Infrastructure as Code Configure an upgrade Physical Network Upgrade and update system
	Continuous Monitoring Runtime continuous monitoring systems, configuration controllers, STIG controls, etc., that continuously monitor the system and check whether it is running the desired components and configuration or if there are any anomalies.	Request threat protection Security Operations Compliance processes Shared responsibility model

Pillar	Feature	Guide
Data	**Data Monitoring** Google Distributed Cloud mitigates data spillage by providing default deny firewall policies for customer workloads via macro/micro segmentation, endpoint detection & response, intrusion prevention & detection, and comprehensive security operations monitoring.	Control data exfiltration Shared responsibility model Respond to storage incidents
	Data Encryption Provides two or more layers of data encryption on customer data. Data at rest encryption with keys rooted back to FIPS 140-2 level 3 HSMs. Data in-transit encryption with TLS 1.2+, HTTPS and IPSec tunnels. Mutual TLS is applied throughout the platform. Keys are rotated periodically.	Encryption Control HSM keys Key management
	Data Access Control Google Distributed Cloud provides role based access (RBAC) and attribute based access (ABAC) for granular access control.	Grant and revoke access Data Storage overview Grant and obtain bucket access
Network & Environment	**Data Flow Mapping** Google Distributed Cloud provides an observability platform with log collection, visualization and monitoring capabilities.	Logging overview Observability audit logger Manage flow logs
	Software Defined Networking Software Defined Networking (SDN) with APIs to set up and operate. Customers can use various APIs to validate and change their settings such as overlay networking and service mesh.	Networking overview Software Defined Networking

Pillar	Feature	Guide
Network & Environment *Continued*	**Macro & Micro Segmentation** Macro Segmentation corresponds to the tenant boundaries/segmentation, Micro Segmentation is at service level - and each of these has particular properties that enforce that segmentation (k8s namespaces, VRF, VXLAN, k8s network policies). Each user and asset communicated in the network is authenticated and authorized (on application level). Firewalls have default deny posture to control and Intrusion Prevention & Detection Systems to monitor/block suspect traffic. Google Distributed Cloud provides dedicated VXLANs and VRFs for each org and firewall policies that block any traffic between orgs.	Request threat protection Physical Network Virtual Network Denial of Service Protection Networking overview
Automation & Orchestration	**Policy Decision Point** Policy Decision Points (PDPs) are the core of the authorization system. It leverages Identity and Access Management (IAM) for Role-Based Access Control (RBAC), where PDPs match a user's roles against required permissions. For finer control, Attribute-Based Access Control (ABAC) is employed, with PDPs evaluating complex policies based on user attributes, resource properties, and environmental context. Within Kubernetes, Kubernetes Resource Manager (KRM) manages authorization using RBAC and can be extended with ABAC for more sophisticated decisions. Overall, Google Distributed Cloud air-gapped offers a layered authorization approach with centralized IAM, potential for granular ABAC, and Kubernetes-specific controls.	Security Strategy Manage Kubernetes

Pillar	Feature	Guide
Automation & Orchestration *Continued*	**Security Operations Center** In Google hosted models, the Security Operations Center provides 24/7 security monitoring a blend of manual and automated procedures, ensuring swift response and mitigation of threats. Security Orchestration Automation & Response (SOAR) is applied at various levels of the logging, ticketing, and monitoring stack to achieve security monitoring requirements. The SOC operates a suite of security tools, including intrusion detection and prevention, vulnerability management, web scanning, antivirus, endpoint detection, and security incident response providing the foundation for comprehensive, 24/7 monitoring of the administrative planes.	Request threat protection Security Operations Shared responsibility model Respond to storage incidents
	Artificial Intelligence & Machine Learning *Infrastructure:* Google Distributed Cloud employs machine learning to analyze vast amounts of data, detecting subtle anomalies, suspicious behavior, and known threat patterns. This proactive and intelligent monitoring enables security teams to identify and neutralize potential threats faster, while reducing false positives for a more effective security posture. *Customer Workloads:* Google Distributed Cloud provides industry leading artificial intelligence services with Vertex AI. Vertex AI has several capabilities including Vertex AI Workbench which provides development/deployment of models for cybersecurity detection. Google Distributed Cloud provides capabilities for both Infrastructure Operators and end-customers to build data pipelines from observability platforms for risk assessment, access review, and environmental analysis of behavioral and heuristic anomalies.	Optical Character Recognition Speech to Text Translation Document Vision Service Online Predictions Vertex AI - Deploy a model Create ML notebook Security Operations

Pillar	Feature	Guide
Automation & Orchestration *Continued*	**API Standardization** Anthos Service Mesh is a managed service mesh that provides a uniform way to connect, secure, monitor, and manage platform services. It standardizes the way microservices are deployed and managed across different environments, including on-premises, hybrid, and multi-cloud. Anthos Service Mesh provides customer-facing/maintained APIs. GDC air-gapped also extends K8S API via KRMs which allows for a consistent K8S experience across environments. Lastly GDC air-gapped provides openAPI compliance.	Request threat protection Physical Network Virtual Network Denial of Service Protection Networking overview
Visibility & Analytics	**Observability** Google Distributed Cloud logging is aligned with the Maturity Model for Event Log Management (M-21-31) directive including centralized logging, including network, data, application, device, and user activity. Logs are consolidated for analysis and immutable storage, supporting various formatting options for flexibility. Observability ingests and replicates these logs, leveraging the open schemas for standardized security monitoring.	Logging overview Observability audit logger Manage flow logs
	Security Information & Event Management All security, audit, and operational logs are replicated to a Security Information & Event Management platform for enhanced security monitoring. The Security Operations Center leverages over 1,200 custom analytics, powered by Mandiant threat intelligence and updated regularly to detect the latest attacker techniques.	Security Operations Shared responsibility

Pillar	Feature	Guide
Visibility & Analytics *Continued*	**Security & Risk Analytics** Solutions for intrusion detection/prevention, vulnerability management, web application scanning, antivirus protection, and endpoint detection and response tools integrate with a centralized SIEM to enable comprehensive 24/7 SOC monitoring of the infrastructure, enhancing security visibility and incident response.	Request threat protection Shared responsibility model
	User & Entity Behavior Analytics Google Distributed Cloud leverages External IdP (Identity provider) and uses RBAC and ABAC for access control; User and entity behavior (UEBA) data is captured using custom analytics. Custom-written analytics are used to detect anomalous and malicious activities; this includes monitoring and detecting abusive or excessive privilege access requests or sessions.	Request threat protection Connect to an identity provider Security Operations

Google Cloud