

Google Anthos Verified Reference Architecture for PCI DSS 3.2.1

Verified Reference Architecture for PCI Compliance

COALFIRE OPINION SERIES – Ver 1.1

KERRY STEELE, PRINCIPAL CONSULTANT, CISSP, CISA, CCSP, CDPSE, ISSAP, QSA
ALLEN MAHAFFY, PRINCIPAL CONSULTANT, CISSP, CISA, QSA



Table of Contents

Executive Summary	3
Coalfire Opinion	3
Introducing the Payment Card Industry Data Security Standard 3.2.1	3
Suggestions for the Use of this VRA	4
Merchants and financial institutions	4
Service providers, designated entities, and shared PCI DSS responsibility	5
PCI DSS qualified security assessors	5
Objectives of this white paper	6
Anthos Ecosystem.....	6
Anthos Deployment Models	7
Anthos Cluster Deployment Options	8
Anthos clusters on Google Kubernetes Engine (GKE)	8
Anthos clusters on VMware (GKE On-Prem)	8
Anthos clusters on Bare Metal (ABM).....	10
Anthos clusters on AWS (GKE on AWS).....	11
Anthos clusters on Azure	12
Attached clusters	12
Anthos Features	13
Cloud Run for Anthos	13
Migrate to Containers	14
Connect Agent	14
Multi Cluster Ingress	15
Binary Authorization.....	16
Anthos Security Components.....	16
Anthos Config Management	16
Anthos Service Mesh	18
Anthos Service Mesh + Anthos Config Management	22
Scope and Approach for Review	23
Scope of Review	23
Coalfire Evaluation Methodology.....	23
Evaluation of PCI Controls and Scoring System	24
Summary of Overall PCI DSS 3.2.1 Scoring	24
Anthos Applicability to PCI DSS 3.2.1.....	26
Anthos Platform.....	26
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	26
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	27
Requirement 3: Protect stored cardholder data.....	29
Requirement 4: Encrypt transmission of cardholder data across open, public networks	29
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	30
Requirement 6: Develop and maintain secure systems and applications	30
Requirement 7: Restrict access to cardholder data by business need-to-know	32
Requirement 8: Identify and authenticate access to system components	33

Requirement 9: Restrict physical access to cardholder data 36

Requirement 10: Track and monitor all access to network resources and cardholder data 36

Requirement 11: Regularly test security systems and processes 38

Requirement 12: Maintain a policy that addresses information security for all personnel 39

Customer Responsibilities for PCI DSS Use of the Anthos Platform..... 39

Conclusion and Coalfire Opinion 40

 A Comment Regarding Regulatory Compliance 41

Legal disclaimer 41

Additional Information, Resources, and References..... 41

 Google Anthos Resources 41

 PCI Security Standards Council Data Security Standard References 42

 Coalfire References..... 42

Executive Summary

Google has engaged Coalfire, a Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent technical review of *Anthos*. This review uses a Verified Reference Architecture (VRA) methodology, which subjects this new technology to an “eyes of the assessor” simulated PCI Data Security Standard (DSS) assessment. The chosen scenario examines a payment entity’s deployment of *Anthos* in alignment with technical requirements of the Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1. This white paper details Coalfire’s methodology for simulated assessment, summarizes findings from our review of product capabilities, provides context for the possible use for these capabilities, defines parameters to form a common basis of understanding, and states an opinion as to the usefulness of *Anthos* within a program of compliance for PCI DSS 3.2.1.

Coalfire Opinion

Coalfire has determined that *Anthos* can be an effective platform when employed in PCI DSS 3.2.1 assessed environments. *Anthos* comes integrated with many security features and functions that can effectively support numerous PCI DSS technical control requirements.

Introducing the Payment Card Industry Data Security Standard 3.2.1

PCI DSS 3.2.1 is a framework that defines the baseline physical, technical, and operational security controls, known as “requirements” and “sub-requirements,” necessary for protecting payment card account data. PCI DSS 3.2.1 defines two categories of payment card account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and sensitive authentication data (SAD), which includes full track data (magnetic-stripe data or equivalent on a chip), card security code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs/PIN blocks) entered during the transaction (PCI DSS Requirements and Security Assessment Procedures, version 3.2.1, May 2018).

PCI DSS “applies to any organization that stores, processes, or transmits CHD” (PCI DSS, 2018, p. 5). These organizations include, but are not limited to, merchants, payment processors, issuers, acquirers, and service providers. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of the people, processes, and technologies that store, process, or transmit CHD or SAD (PCI Security Standards Council [SSC], LLC, 2016). PCI DSS defines twelve requirements designed to address six objectives, as shown in the high-level overview below:

Objectives	Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect CHD. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect CHD	<ol style="list-style-type: none"> 3. Protect stored CHD. 4. Encrypt transmission of CHD across open, public networks.
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to CHD by business need-to-know. 8. Identify and authenticate access to system components.

Objectives	Requirements
	9. Restrict physical access to CHD.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and CHD. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Table 1: PCI DSS High-Level Overview

The PCI DSS program is concerned with operations, not components in the abstract. Thus, the hardware and software used in a compliance program, except for POS and POI systems, are considered ineligible for component certification because of specific PCI DSS program scope (PCI DSS, 2018, p. 10).

In place of component certification, *de facto* analysis of components and ineligible systems reviewed by industry-recognized authorities (e.g., Coalfire), using guidelines and methods identical to the actual assessment and certification processes, may serve as a guide for successful use of **Anthos** in an assessment.

This Coalfire VRA documents the potential use of **Anthos** as part of an overall technical approach to PCI DSS compliance. Coalfire VRAs have been used since 2014 by various participants in the PCI community to understand how products that are ineligible for certification may be successfully used in a PCI DSS compliance program.

Suggestions for the Use of this VRA

This white paper is intended to be used by various payment card industry entities and other interested parties involved in sales, construction, operation, or infrastructure assessment who use the **Anthos** platform. This document is intended to help **Anthos** customers understand the controls built into the core infrastructure space, as well as the general availability of control options that may be implemented by the customer for the workload space.

The following sections explain how this review may be used by various entities throughout the PCI DSS life cycle. The entities include merchants and financial institutions, payment solution service providers, infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) service providers, designated entities, others who share responsibility with a payment entity, and PCI DSS-qualified security assessors (QSAs).

Merchants and financial institutions

PCI DSS requirements provide a framework of standards that, when implemented, support security for payment card transactions flowing from the merchant point-of-use, where payment and authorization transactions are initiated, to the financial institutions that provide the acquisition and settlement of a customer's purchase. **Anthos** may be used as a platform that merchants and financial industry entities use to support CDE workloads. The **Anthos** platform is designed to be turnkey and includes best practices for deploying its core infrastructure components (hardware and software), technical controls with system and network hardening methods employed to provide consistency, and a security infrastructure and services platform. This white paper is primarily intended to highlight a use case where an **Anthos** customer could implement security controls into the core infrastructure of **Anthos** and how those security controls align with PCI DSS requirements. Coalfire also references guidance for customer implementation of technical controls that occur during deployment of the **Anthos** platform on customer premises and within the customer's physical network.

Additional guidance, provided by the PCI DSS Information Supplement Guidance for PCI DSS Scoping and Network Segmentation (see references), has been integrated into this material. It calls out the following scoping categories:

- CDE systems that process, store, or transmit CHD

- Systems that support CDE systems and components through controlled access
- Out-of-scope systems that are isolated from all CDE systems and components

As it defines the CDE's scope, this material may be essential in the proper understanding of the **Anthos** software-defined network (SDN) and micro-segmentation implementation, which is a fundamental best practice of PCI DSS design. When properly implemented and tested, segmentation may be useful for reducing the scope of a PCI DSS assessment; however, PCI SSC guidance states that "implementing segmentation is no replacement for a holistic approach to securing an organization's infrastructure," (PCI SSC, 2017). Many CHD breaches have been linked to out-of-scope systems where the attacker uses the out-of-scope system to gain leverage and pivot on the payment entity's network until an access point to the CDE can be found.

Service providers, designated entities, and shared PCI DSS responsibility

PCI DSS makes provisions for payment industry entities to use service providers to store, process, or transmit CHD on behalf of the payment entity or to manage components such as routers, firewalls, databases, physical security, or servers. CHD security is impacted in the course of providing services to payment industry entities, and, therefore, such service providers are responsible for compliance with PCI DSS. This is also true of shared service providers who provide services to multiple payment entities. Requirements under section 12.8 of PCI DSS 3.2.1 are focused on managing "service providers with whom CHD is shared, or that could affect the security of CHD" (PCI DSS 3.2.1 Standard). Service provider requirements in addition to PCI DSS requirements are listed in Appendix A1 of PCI DSS 3.2.1. This white paper may be useful for service providers using or planning to use **Anthos** as a platform for delivering services where CHD is stored, processed, or transmitted.

This white paper may also be useful where a designated entity's **Anthos** instances are involved with the storage, processing, or transmission of CHD. Designated entities constitute an additional category of entity for which PCI DSS 3.2.1 is applicable. A designated entity may be any payment entity, including merchants or service providers, that a payment brand or acquirer determines requires additional supplemental validation of existing PCI DSS requirements. Examples of designated entities include those storing, processing, or transmitting large volumes of CHD; those providing aggregation points for CHD; or those who have suffered significant or repeated CHD breaches. Additional requirements for designated entities are found in Appendix A3 of PCI DSS 3.2.1.

PCI DSS qualified security assessors

This white paper and supporting materials may be useful to assist a PCI DSS QSA in evaluating an implementation of **Anthos** during assessment activities that contribute to their Report on Compliance (ROC) or their Self-Assessment Questionnaire (SAQ). In the section titled "**Anthos** Applicability to PCI DSS 3.2.1," Coalfire aligns the technical controls referenced in PCI DSS 3.2.1 with findings for how **Anthos** provides controls that can meet those requirements. Additionally, a designation of origination of control is provided with commentary on how the systems integrator would implement appropriate controls. Where applicable, Coalfire references the additional implementation steps documented in this VRA to be performed by the customer when deploying and supporting a PCI DSS compliance program. Other products have been used in conjunction with the built-in **Anthos** resources to meet the PCI DSS requirements fully, and Coalfire notes those products, such as customer edge firewalls to secure the boundary between the untrusted network (internet) and the internal, trusted networks, where applicable.

The guidance in this white paper and supporting materials are intended to provide Coalfire's opinion and are not meant to supplant or compromise the independent judgment required to perform PCI DSS assessments. The PCI SSC Code of Professional Responsibility requires QSA companies and employees to "adhere to high standards of ethical and professional conduct" (PCI Security Standards Council, LLC, 2014). Coalfire supports and upholds independent QSA judgments that might differ from this opinion.

Objectives of this white paper

This white paper's primary objective is to render an opinion on **Anthos**' suitability to assist merchants with meeting the requirements of PCI DSS 3.2.1 using a particular use case detailed below and in the subsequent sections. The following process is intended to illustrate Coalfire's findings and satisfy these objectives:

- Choose a likely and relevant use case for an **Anthos** payment card infrastructure.
- Show a possible configuration used for many likely merchant and processor scenarios.
- Analyze **Anthos**' platform and features using practices identical to an actual payment card assessment and guidance provided in QSA reactions.
- Evaluate the key features of **Anthos** per control for their ability to support the requirements.
- Make relevant observations and recommendations about each control family and the suggested implementation approaches for **Anthos** features to support meeting the objectives of these controls.
- State Coalfire's opinion.

This white paper also contains a representative overview of many aspects of the PCI DSS process and practices. This white paper's secondary objective is to inform a newcomer to PCI DSS 3.2.1 about a technical approach to using hyperconverged infrastructure to construct an infrastructure architecture able to host a compliant payment card workload.

Since the **Anthos** platform's review was not conducted on an actual payment card entity running a real-world merchant or service provider workload, Coalfire focused on the technical controls for PCI DSS 3.2.1. Coalfire did not review organizational processes, training, procedures, written supporting materials, or other non-technical controls called for in PCI DSS 3.2.1. The customer is responsible for PCI DSS processes, such as organizational, procedural, and training controls, that pertain to implementation by a real payment card entity.

Coalfire uses the term "notional" to denote the presence of such non-technical controls that may be required to support or enable the technical controls that Coalfire is evaluating. For example, PCI DSS 3.2.1 controls used to "build and maintain a secure network and systems" and "1.1 Establish and implement firewall and router configuration standards that include the following: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations..." (PCI DSS, 2018) are notional. These requirements underpin technical controls such as 1.1.1.c and 1.1.2.a.

Anthos Ecosystem

Anthos offers a comprehensive platform for customer applications development, integration, deployment, and management across multiple environments, including cloud and on-premises at the customer's data center. The **Anthos** platform consists of the following key services:

- Infrastructure management
- Container management and orchestration
- Service management
- Policy enforcement

Customers can integrate other services, as well as development and other security tools, to enable application development and deployment within the **Anthos** environment. Customers also benefit from using a centralized control plane for managing their containerized applications.

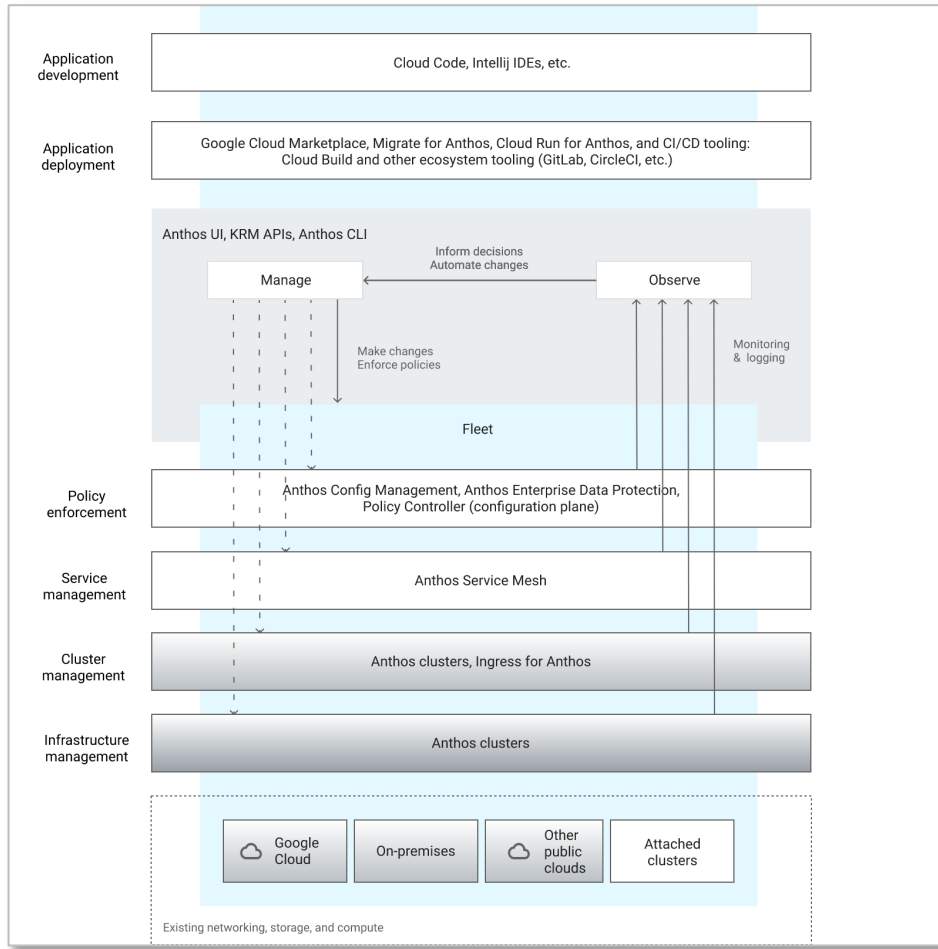


Figure 1: Anthos Ecosystem

Anthos Deployment Models

Anthos provides a multi-cloud platform for both legacy and cloud-native application deployments, offering a service-centric view of Google Cloud, on-premises, and Amazon Web Services (AWS) environments with a Kubernetes-based API with a single management interface.

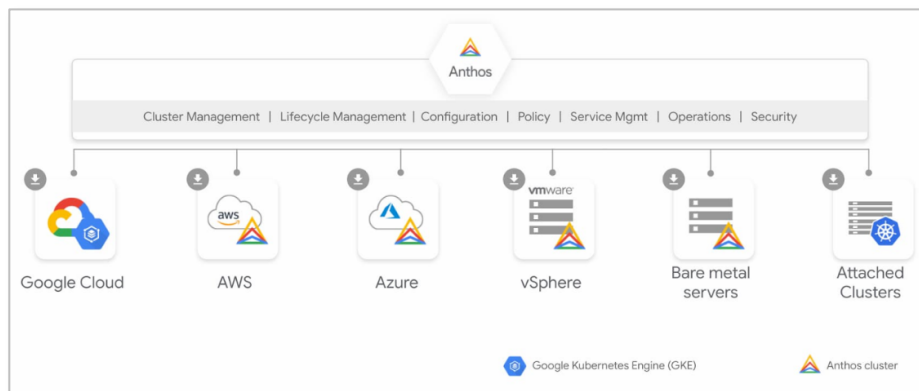


Figure 2: Anthos Deployment Models

Anthos Cluster Deployment Options

Anthos clusters can be deployed to:

- **Anthos on Google Kubernetes Engine (GKE):** Leverage the features of *Anthos* on top of fully managed GKE.
- **Anthos on VMware (GKE On-Prem):** An implementation of the GKE API running on Google Cloud VMware Engine (GCVE).
- **Anthos on bare metal systems (ABM):** An implementation of the GKE API running on the customer's own hardware.
- **Anthos clusters on AWS (GKE on AWS):** An implementation of the GKE API running in AWS.
- **Anthos clusters on Azure:** An implementation of the GKE API running in Microsoft Azure.
- **Anthos attached clusters:** Attach any conformant Kubernetes.

Anthos clusters on Google Kubernetes Engine (GKE)

Customers leveraging *Anthos* can assign, migrate, and integrate workloads running on GKE with their on-prem workloads. GKE is a fully managed service from Google Cloud Platform (GCP), and customers can rely on the GCP Attestation of Compliance (AOC) for PCI DSS compliance. Customers can build their containerized applications in GKE and can keep consistent Kubernetes versions, operating systems (OS), runtimes, and installed packages between GKE On-Prem and in GKE.

Customer workloads deployed on GKE leverage Google's Container-Optimized OS to run Kubernetes. The Container-Optimized OS implements a locked-down firewall, a read-only filesystem, and limited user accounts (with root disabled).

Anthos on GKE enables network security through leveraging software-defined networks (virtual firewall rules) that enable simple Pod-to-Pod communications within a Kubernetes cluster, and within the cluster's VPC. Customers must configure network policies to limit ingress and egress traffic to the Pods, based on business-justified and defined ports, protocols, and firewall rules.

Anthos on GKE workload security is implemented via applying default Docker AppArmor security policies to all Kubernetes pods. AppArmor is a Linux security module that protects an operating system and its applications from security threats. GKE default audit logging ensures that all administrative activity is logged and captured within GCP Stackdriver.

Anthos clusters on VMware (GKE On-Prem)

Anthos clusters on VMware (GKE On-Prem) deploys customer workloads in an on-premises environment to a customer's VMware instances, attached to the VMware clusters as nodes. GKE On-Prem leverages an optimized version of Ubuntu Linux to run the control plane and nodes within *Anthos*. Ubuntu includes a rich set of modern security features, and *Anthos* clusters on VMware implements several security-enhancing features for clusters, including:

- Images preconfigured to meet PCI DSS, NIST Baseline High, and DoD Cloud Computing SRG Impact Level 2 standards.
- Optimized package set.
- Google Cloud-tailored Linux kernel.
- Optional automatic OS security updates.
- Limited user accounts and disabled root login.

Anthos enables network security within an on-premises deployment using an “Island Mode” configuration where Pods communicate directly with each other within a cluster but cannot be accessed from outside. This configuration forms an “island” within the network that is not accessible externally.

GKE On-Prem installations include a layer 7 load balancer with an Envoy-based ingress controller that handles Ingress rules within the cluster. GKE On-Prem includes a built-in layer 4 load balancer and provides support for external F5 Networks L3/L4 load balancers. During installation of **Anthos**, a virtual IP address (VIP) is configured on the load balancer which points to the ports in the NodePort Service for the ingress controller, allowing external clients to access the service via the VIP on the load balancer.

By default, all administrative actions in **Anthos** are logged. Customers use the Connect Agent for Google Cloud to communicate to the local API server running on-premises, and each cluster should have its own set of audit logs. All actions that users perform from the UI through Connect Agent are logged by that cluster. Customers are required to ensure that all audit trails being captured are compliant with PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data controls.

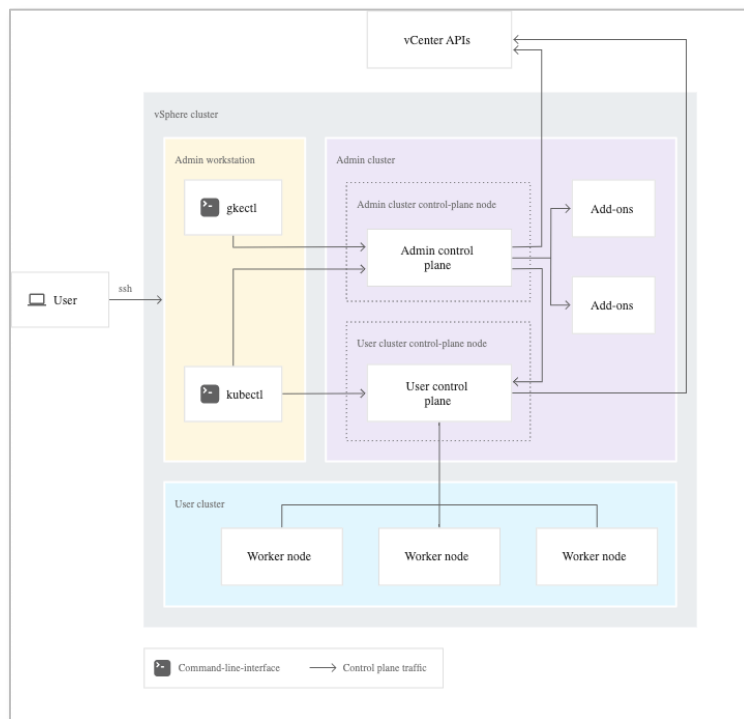


Figure 3: Anthos Clusters on VMware

Anthos clusters on VMware installation includes an admin cluster, one or more user clusters, and an admin workstation. An **Anthos** clusters on VMware cluster’s virtual machines (VMs) are all in the same vSphere cluster. **Anthos** clusters on VMware clusters can be in the same or different vSphere clusters.

Admin cluster

The *admin cluster* is the base layer of **Anthos** clusters on VMware. It runs the following **Anthos** clusters on VMware components:

- **Admin cluster control plane.** The admin cluster’s control plane includes the Kubernetes API server, the scheduler, and several controllers for the admin cluster.

- **User cluster control planes.** For each user cluster, the admin cluster has a node that runs the control plane for the user cluster. The control plane includes the Kubernetes API server, the scheduler, and several controllers for the user cluster.
- **Add-ons.** The admin cluster runs several Kubernetes add-ons, like Grafana, Prometheus, and Google Cloud's operations suite. **Anthos** clusters on VMware launches add-ons on different admin cluster nodes than other control plane components.

Note that user control planes are managed by the admin cluster. They run on nodes in the admin cluster, not in the user clusters. In addition, nodes in the admin cluster run **Anthos** clusters on VMware components. User workloads do not run in the admin cluster.

User cluster

The *user clusters* are where containerized workloads and services are deployed and run.

Anthos clusters on Bare Metal (ABM)

ABM deploys customer workloads in an on-premises environment to a customer's bare metal systems as cluster nodes.

GKE workloads deployed to ABM are deployed directly on the customer's own hardware and network infrastructure, where they have direct control over application scale, security, and network latency, as well as having the benefit of containerized applications through GKE and **Anthos** components. Because the customer manages the network requirements, the network can be optimized for low latency, crucial for performance in commercial or finance analytics, as well as other enterprise or network edge applications.

ABM runs on open-source and enterprise Linux Oss, including CentOS, Red Hat Enterprise Linux (RHEL), and Ubuntu. With ABM there is no additional VM complexity for integration with enterprise security systems, maintaining complete transparency when interacting with existing security systems.

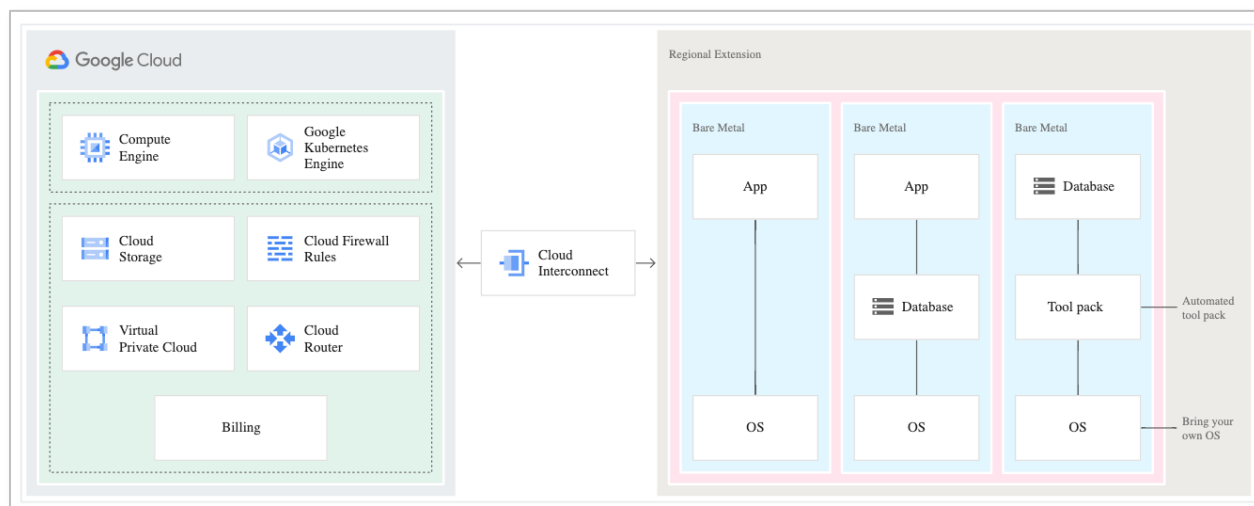


Figure 4: ABM Overview

ABM uses an “Island Mode” configuration where Pods communicate directly with each other within a cluster but cannot be accessed from outside. This configuration forms an “island” within the network that is not accessible externally.

ABM includes a layer 7 load balancer with an Envoy-based ingress controller that handles ingress rules within the cluster. ABM also includes a built-in layer 4 load balancer, as well as provides support for external F5 Networks L3/L4 load

balancers. During installation, a VIP is configured on the load balancer that points to the NodePort Service for the ingress controller. The Connect Agent is used with **Anthos** to communicate to the local API server running on-premises for monitoring, logging, and analysis of clusters and workloads.

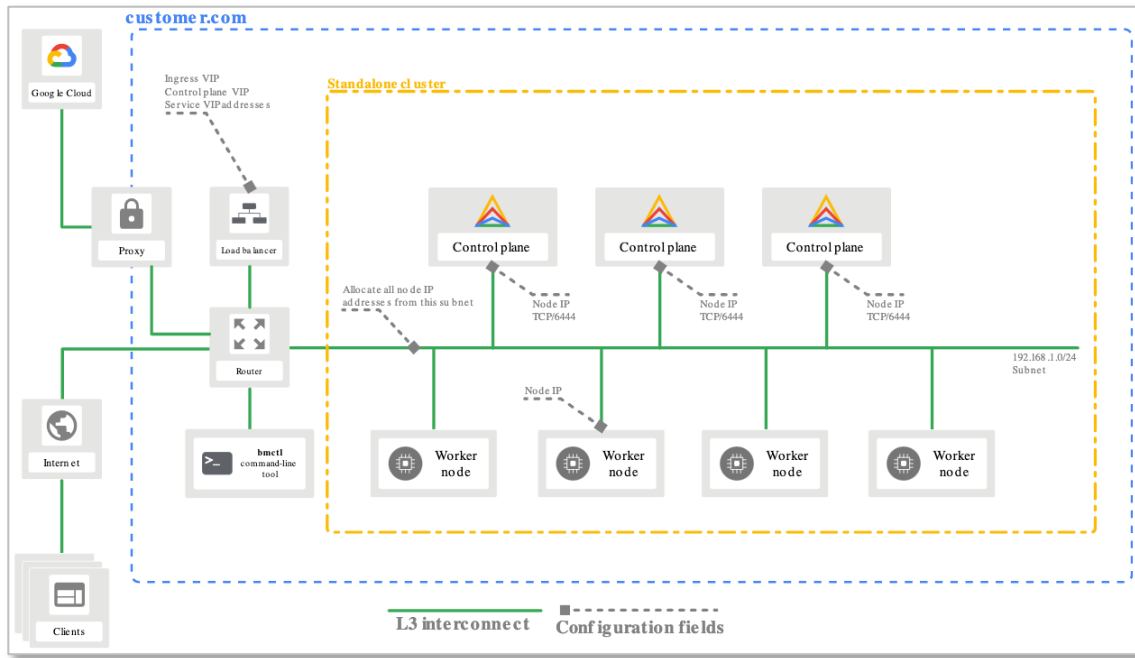


Figure 5: ABM Networking

Anthos clusters on AWS (GKE on AWS)

Anthos clusters on AWS (GKE on AWS) is deployed with a common environment including gcloud, Terraform, and kubectl to perform multi-cloud cluster orchestration with GKE on AWS leveraging the **Anthos** Multi-Cloud and Connect APIs for AWS.

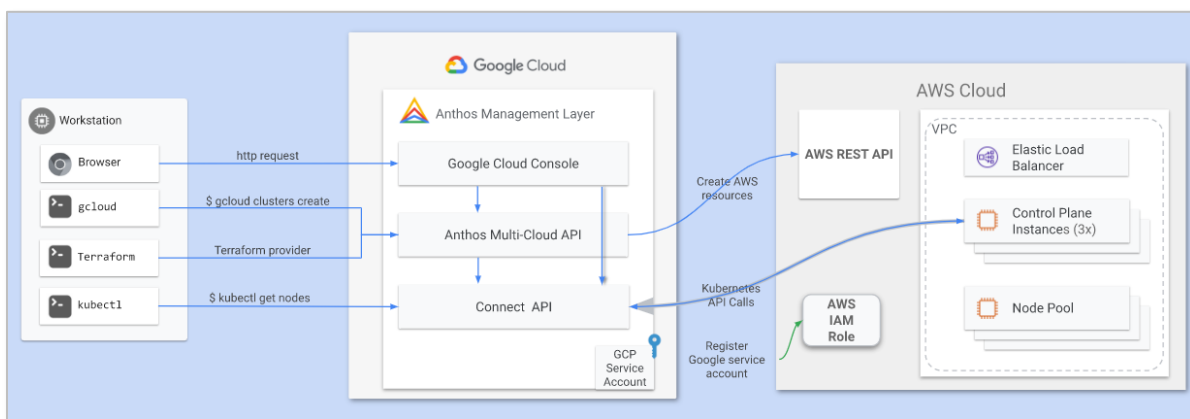


Figure 6: Anthos Cluster Management on AWS

Anthos clusters on Azure

Anthos clusters on Azure is deployed with a common environment including gcloud, Terraform, and kubectl to perform multi-cloud cluster orchestration with **Anthos** clusters on Azure leveraging the **Anthos** Multi-Cloud and Connect APIs for Azure.

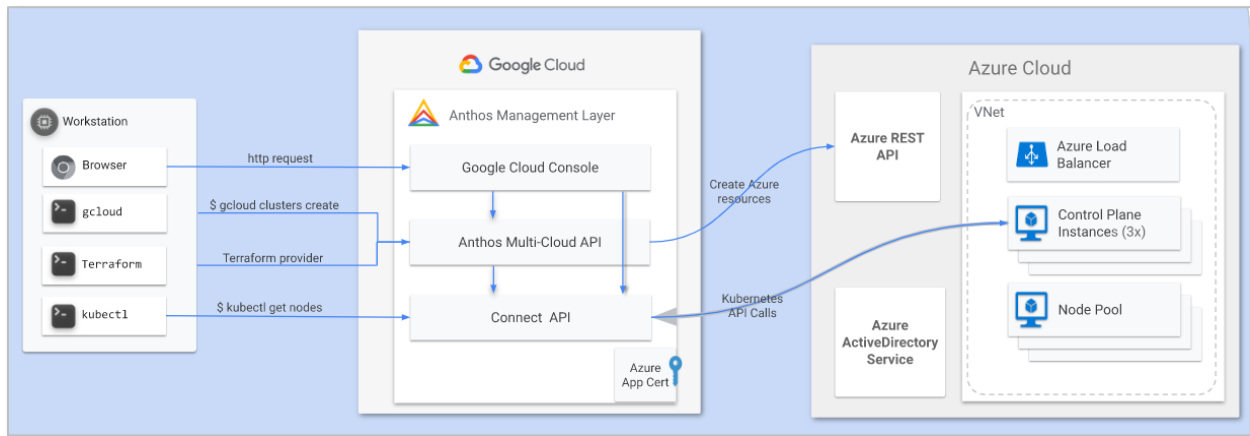


Figure 7: Anthos Cluster Management on Azure

Attached clusters

Attached clusters allow for any conformant Kubernetes cluster to be attached, including:

- Amazon Elastic Kubernetes Service (Amazon EKS)
- Microsoft Azure Kubernetes Service (Microsoft AKS)
- Red Hat OpenShift Kubernetes Engine (OKE) 4.6, 4.7, 4.8, 4.9
- Red Hat OpenShift Container Platform (OCP) 4.6, 4.7, 4.8, 4.9
- Rancher Kubernetes Engine (RKE) 1.2.6, 1.3, 1.3.6
- KIND 0.10, 0.11
- K3s 1.20
- K3d 4.4.3

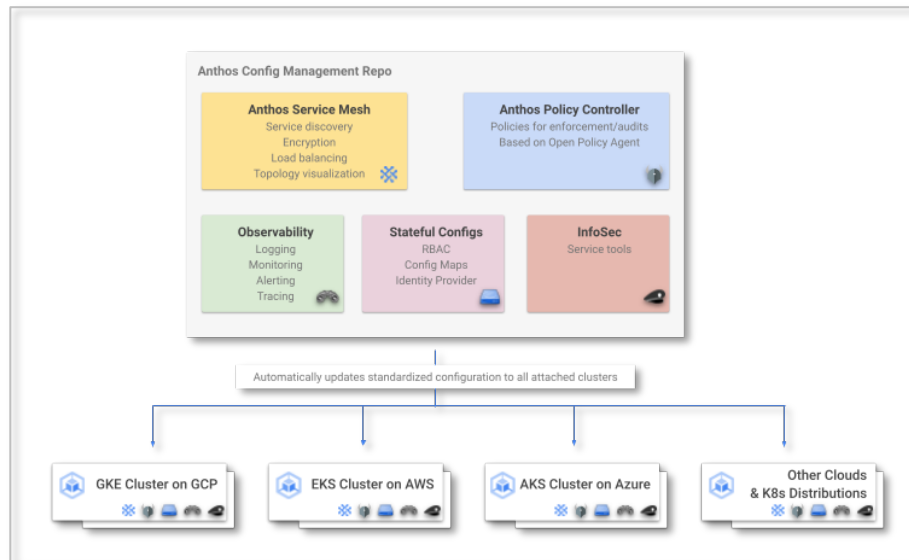


Figure 8: Anthos Attached Clusters

Anthos Features

Anthos features include:

- **Cloud Run for Anthos:** Deploy serverless workloads across hybrid and multi-cloud environments with *Anthos*.
- **Migrate to Containers:** Convert VM-based workloads into containers that run on GKE or *Anthos* clusters from VMs that run on VMware, AWS, Azure, or Compute Engine.
- **Connect Agent:** Register clusters outside Google Cloud to a fleet.
- **Multi Cluster Ingress:** Deploy shared load balancing resources across clusters and across regions.
- **Binary Authorization:** Enforce software supply-chain security for container-based applications with a policy that the service enforces when an attempt is made to deploy a container image on one of the supported container-based platforms.

Cloud Run for Anthos

Cloud Run for *Anthos* is a fully managed and completely serverless product, while Cloud Run for *Anthos* offers a serverless developer experience on a shared responsibility *Anthos* platform. If a customer is already using *Anthos*, Cloud Run for *Anthos* can easily deploy their workloads across hybrid and multi-cloud environments, all with the same consistent experience.

Cloud Run for *Anthos* abstracts away the complexity of Kubernetes, making it easy to build and deploy apps across hybrid and multi-cloud environments. Cloud Run for *Anthos* is Google's managed and fully supported Knative offering, an open-source project that enables serverless workloads on Kubernetes.

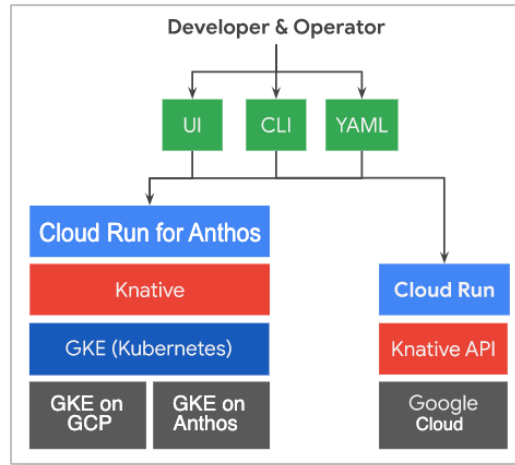


Figure 9: Cloud Run for Anthos

Migrate to Containers

Migrate to Containers is used to convert VM-based workloads into containers that run on GKE or **Anthos** clusters. Customers can migrate workloads from VMs that run on VMware, AWS, Azure, or Compute Engine, giving the flexibility to easily containerize existing workloads.

With Migrate to Containers, VMs can be migrated from supported source platforms to the following:

- GKE and Autopilot clusters
- **Anthos**
- **Anthos** clusters on VMware
- **Anthos** clusters on AWS
- ABM
- Cloud Run

Connect Agent

When a customer registers a cluster outside Google Cloud to its fleet, Google Cloud uses a Deployment called the Connect Agent to establish a connection between the cluster and the customer's Google Cloud project and to handle Kubernetes requests. This enables access to cluster and to workload management features in Google Cloud, including a unified user interface, Cloud console, to interact with the cluster.

If a customer's network is configured to allow outbound requests, the customer can configure the Connect Agent to traverse NATs, egress proxies, and firewalls to establish a long-lived, encrypted connection between their cluster's Kubernetes API server and their Google Cloud project. Once this connection is enabled, the customer can use their own credentials to log back into their clusters and access details about their Kubernetes resources. This effectively replicates the UI experience that is otherwise only available to GKE clusters.

After the connection is established, the Connect Agent software can exchange the account credentials, technical details, and metadata about connected infrastructure and workloads necessary to manage them with Google Cloud, including the details of resources, applications, and hardware.

This cluster service data is associated with the customer's Google Cloud project and account. Google uses this data to maintain a control plane between the customer's cluster and Google Cloud, to provide the customer with any Google Cloud services and features they request, including facilitating support, billing, and providing updates, and to measure and improve the reliability, quality, capacity, and functionality of Connect and Google Cloud services available through Connect.

The customer remains in control of what data is sent through Connect: their Kubernetes API server performs authentication, authorization, and audit logging on all requests via Connect. Google and users can access data or APIs via Connect after they have been authorized by the cluster administrator (for example, via RBAC); the cluster administrator can revoke that authorization.

Multi Cluster Ingress

Multi Cluster Ingress is a cloud-hosted controller for GKE clusters. It's a Google-hosted service that supports deploying shared load balancing resources across clusters and across regions.

Multi Cluster Ingress builds on the architecture of the global external HTTP(S) load balancer. The global external HTTP(S) load balancer is a globally distributed load balancer with proxies deployed at 100+ Google points of presence (PoPs) around the world. These proxies, called Google Front Ends (GFEs), sit at the edge of Google's network, positioned close to clients. Multi Cluster Ingress creates external HTTP(S) load balancers in the Premium Tier. These load balancers use global external IP addresses advertised using anycast. Requests are served by GFEs and the cluster that is closest to the client. Internet traffic goes to the closest Google PoP and uses the Google backbone to get to a GKE cluster. This load balancing configuration results in lower latency from the client to the GFE. The client can also reduce latency between serving GKE clusters and GFEs by running their GKE clusters in regions that are closest to their own clients.

Terminating HTTP and HTTPS connections at the edge allows the Google load balancer to decide where to route traffic by determining backend availability before traffic enters a data center or region. This gives traffic the most efficient path from the client to the backend while considering the backend's health and capacity.

Multi Cluster Ingress is an ingress controller that programs the external HTTP(S) load balancer using network endpoint groups (NEGs). When a MultiClusterIngress resource is created, GKE deploys Compute Engine load balancer resources and configures the appropriate Pods across clusters as backends. The NEGs are used to track Pod endpoints dynamically, so the Google load balancer has the right set of healthy backends.

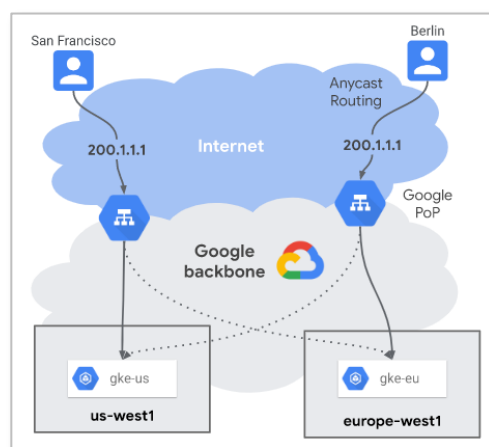


Figure 10: Multi Cluster Ingress

Binary Authorization

Binary Authorization is a service on Google Cloud that provides software supply-chain security for container-based applications. It enables customers to configure a policy that the service enforces when an attempt is made to deploy a container image on one of the supported container-based platforms.

Binary Authorization supports the following platforms:

- **GKE:** Runs images in clusters that are hosted on Google Cloud.
- **Cloud Run (Preview):** Runs containerized applications on a fully managed serverless platform.
- **Anthos Service Mesh (Preview):** Manages a reliable service mesh on-premises or on Google Cloud.
- **Anthos clusters on VMware (Preview):** Runs the images in clusters that are hosted in on-premises data centers.

Binary Authorization is part of a deployment architecture that includes the following related products:

- Artifact Registry, Container Registry and other registries that store the images to be deployed.
- Container Analysis provides vulnerability information that can be used with Binary Authorization to control deployment. Separately, Container Analysis stores trusted metadata that is used in the authorization process.
- Security monitoring is a dashboard that can be used to assess application security posture across interdependent Google Cloud products, including Binary Authorization.
- Google Cloud Deploy is a managed continuous-delivery service, which automates delivery of applications to a series of target environments in a defined sequence.

Binary Authorization allows or blocks deployment of images based on configured policy.

Anthos Security Components

Anthos Config Management (ACM) and **Anthos Service Mesh (ASM)** provide important capabilities to secure workloads deployed on **Anthos**.

- **ACM:** A service which abstracts configuration of the Kubernetes workloads, enabling centralized configuration management across **Anthos** clusters
- **ASM:** A version of Istio that allows establishing and managing a service mesh ensuring end-to-end mutual TLS (mTLS) across workloads, regardless of where they are running

Anthos Config Management

ACM provides platform, service, and security operations for managing **Anthos** workloads using a multi-cluster management approach for both on-premises and cloud environments. ACM allows customers to design and implement common configurations and policies across all **Anthos** clusters.

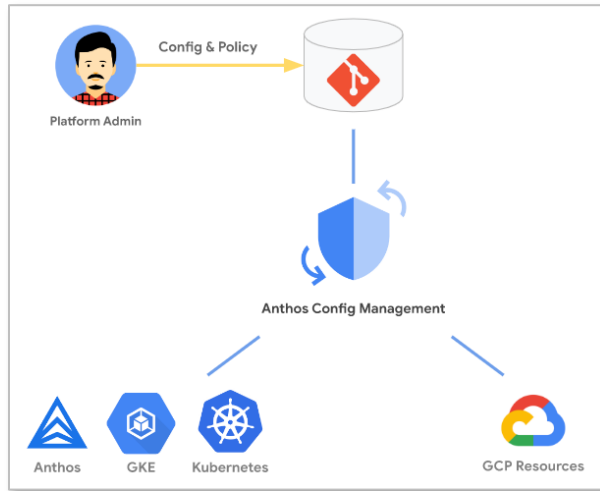


Figure 11: Anthos Config Management Overview

Leveraging ACM, customers access their own central Git repository hosting a common configuration. ACM then evaluates each commit to the Git repository and applies the configuration changes to all clusters. ACM includes a built-in validator that checks for misconfigurations compared to the hosted common configuration and will prevent the pushing of bad configurations if too much drift occurs. ACM is deployed as an operator within GCP or deployed on-premises in the customers environment.

The ACM operator facilitates the importing from the central Git repository, synchronizes and updates the configuration information for **Anthos** GKEs, and monitors for changes between the active configurations of the **Anthos** GKE clusters and the stored configurations. ACM has a policy controller where customers can implement customer policies based on environment or business need and can aid in the support of PCI DSS compliance.

Based on ACM policy implementation, the customer can wholly reject changes that do not comply with the policy implemented or audit changes that violate the policy. Customers define their policy rules within their **Anthos** GKE cluster-scoped template, and the policy will be applied to a particular GKE namespace and/or specific GKE object type. Customers can also leverage the policy engine for their own compliance. ACM can also be integrated with ASM, for management of service mesh policies and configurations.

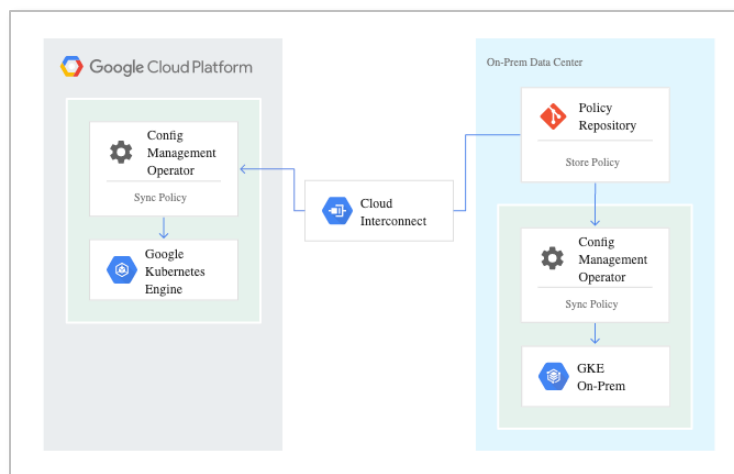


Figure 12: Anthos Config Management Operator

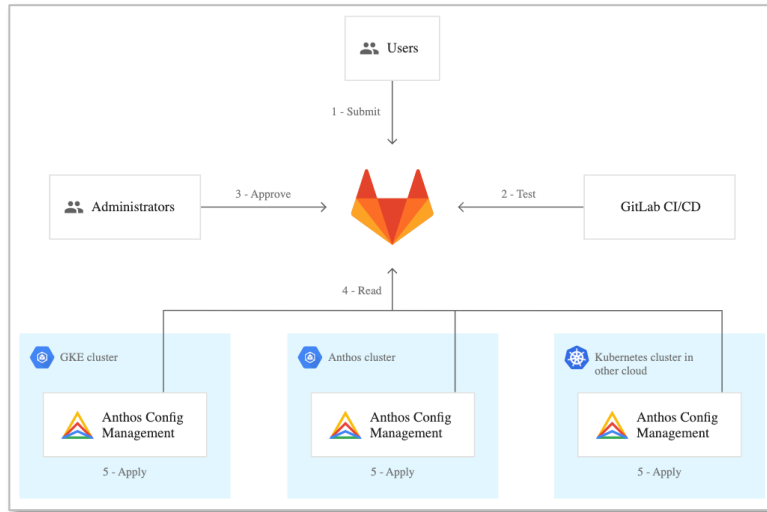


Figure 13: Anthos Config Management Policy Management

ACM helps prevent the deployment of vulnerable container images using defense-in-depth. GCP provides managed base images that a customer can utilize to build container images. Managed base images are built reproducibly and are patched automatically by GCP when patches are available upstream.

Anthos Service Mesh

A service mesh is an architecture that enables managed, observable, and secure communication across services, letting customers create robust enterprise applications made up of many microservices on their chosen infrastructure. Service meshes factor out all the common concerns of running a service, such as monitoring, networking, and security, with consistent, powerful tools, making it easier for service developers and operators to focus on creating and managing great applications for their users.

ASM is powered by Istio, a highly configurable and powerful open-source service mesh platform, with tools and features that enable industry best practices. ASM is deployed as a uniform layer across the entire customer infrastructure. Service developers and operators can use its rich feature set without making changes to application code.

Architecturally, a service mesh consists of one or more control planes and a data plane. The service mesh monitors all traffic through a proxy. On Kubernetes, the proxy is deployed by a sidecar pattern to the microservices in the mesh. On VMs, the proxy is installed on the VM. This pattern decouples application or business logic from network functions and enables developers to focus on the features that the business needs. Service meshes also let operations teams and development teams decouple their work from one another.

ASM provides management of disparate workloads in heterogeneous, multi-cloud environments and on-premises data centers. For organizations that do not already have Istio deployed, ASM will be critical to ensure to secure end-to-end mTLS.



Figure 14: Anthos Service Mesh

Traffic management

ASM controls the flow of traffic between services, into the mesh (ingress), and to outside services (egress). Customers configure and deploy Istio-compatible custom resources to manage this traffic at the application (L7) layer. For example, with the custom resources, customers can:

- Create canary and blue-green deployments.
- Provide fine-grained control over specific routes for services.
- Configure load balancing between services.
- Set up circuit breakers.

ASM maintains a service registry of all services in the mesh by name and by their respective endpoints. It maintains the registry to manage the flow of traffic (for example, Kubernetes Pod IP addresses). By using this service registry, and by running the proxies side-by-side with the services, the mesh can direct traffic to the appropriate endpoint.

Observability insights

ASM provides the following insights into the customer's service mesh in the Google Cloud console:

- Service metrics and logs for HTTP traffic within the mesh's GKE cluster are automatically ingested to Google Cloud.
- Preconfigured service dashboards give the information needed to for customers to understand their services.
- In-depth telemetry—powered by Cloud Monitoring, Cloud Logging, and Cloud Trace—lets customers dig deep into their service metrics and logs and to filter and slice data on a wide variety of attributes.

- Service-to-service relationships immediately help customers understand who connects to each service and the services that each service depends on.
- The ability for customers to quickly see the communication security posture not only of their service, but its relationships to other services.
- Service-level objectives (SLOs) insight into the health of services. Customers can easily define an SLO and alert on their own standards of service health.

Security benefits

ASM has the following security benefits:

- Mitigates risk of replay or impersonation attacks that use stolen credentials. ASM relies on mTLS certificates to authenticate peers, rather than bearer tokens such as JSON Web Tokens (JWT).
- Ensures encryption in transit. Using mTLS for authentication also ensures that all TCP communications are encrypted in transit.
- Ensures that only authorized clients can access a service with sensitive data, irrespective of the network location of the client and the application-level credentials.
- Mitigates the risk of user data breach within a production network by ensuring that insiders can only access sensitive data through authorized clients.
- Identifies which clients accessed a service with sensitive data. ASM access logging captures the mTLS identity of the client in addition to the IP address.
- Provides strong encryption for all in-cluster control plane components and proxies with FIPS 140-2 validated encryption modules.

Deployment options

ASM 10.3 and later has the following deployment options:

- In-cluster control plane.
- Managed **Anthos** Service Mesh.
- Now supports adding Compute Engine VMs in the service mesh.

In-cluster control plane

The following diagram shows the ASM components and features for the in-cluster control plane and sidecar proxies.

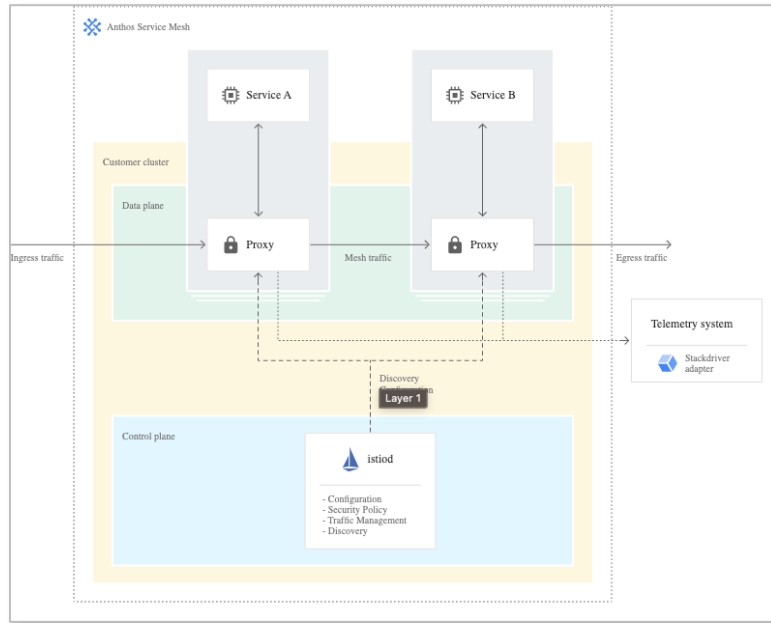


Figure 15: Anthos Service Mesh: In-cluster Control Plane and Sidecar Proxies

Managed **Anthos** Service Mesh

Managed **Anthos** Service Mesh consists of the Google-managed control plane and, in ASM 1.10.4 and later, the optionally enabled Google-managed data plane. With managed **Anthos** Service Mesh, Google handles upgrades, scaling, and security for the customer, minimizing manual user maintenance. When the Google-managed data plane is enabled, an annotation to namespaces is added which installs an in-cluster controller that automatically manages the sidecar proxies. The following diagram shows the ASM components and features for managed **Anthos** Service Mesh:

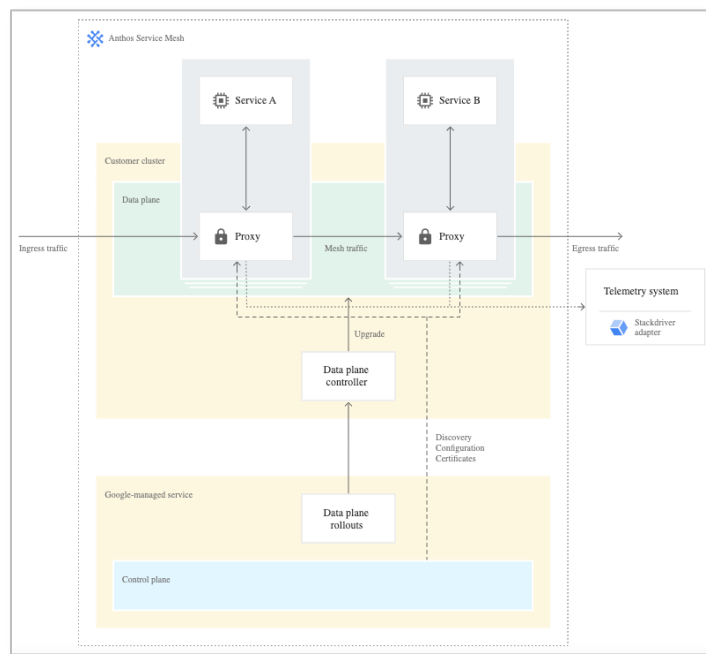


Figure 16: Managed Anthos Service Mesh

Anthos Service Mesh for Compute Engine VMs

Anthos Service Mesh for Compute Engine VMs is available as a preview feature. Customers can manage, observe, and secure services running on both Compute Engine Managed Instance Groups (MIGs) and GKE on Google Cloud clusters in the same mesh. Customers can mix and choose the best environment to run their services while enjoying the benefits of ASM. The following diagram shows a MIG in the same service mesh as a GKE cluster:

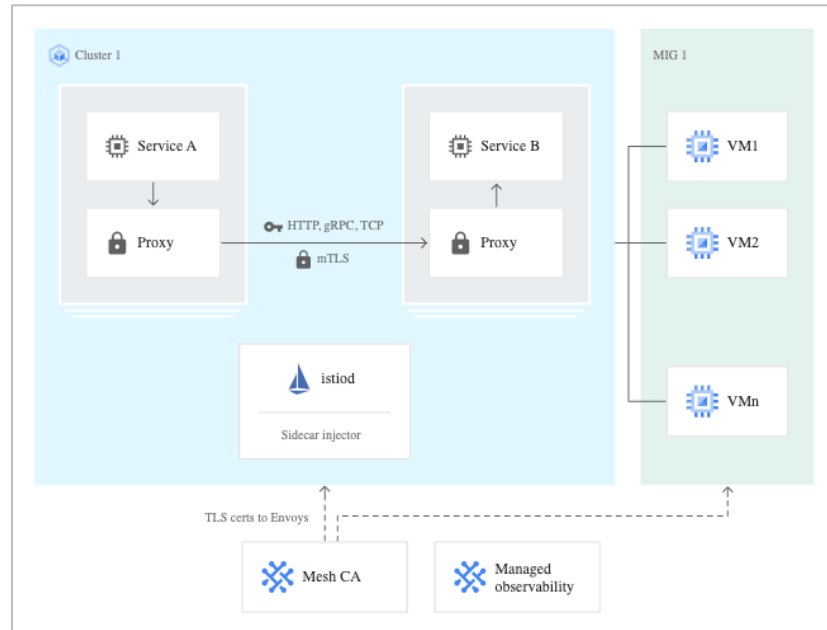


Figure 17: Anthos Service Mesh for Compute Engine VMs

Anthos Service Mesh + Anthos Config Management

Anthos customers can prevent misconfigurations and automatically validate ASM policies by using guardrails with Anthos Config Management's Policy Controller and Config Sync. Policy Controller enables the enforcement of fully programmable policies for clusters. Policy Controller comes with a library of constraint templates for use with the Anthos Service Mesh security bundle to audit the compliance of ASM security vulnerabilities and best practices. Config Sync continuously reconciles the state of clusters with a central set of Kubernetes declarative configuration files. Using Policy Controller and Config Sync together enables the capability to continuously enforce constraints on ASM policy configurations.

The following diagram shows an overview of how Anthos Service Mesh, Policy Controller, and Config Sync work together.

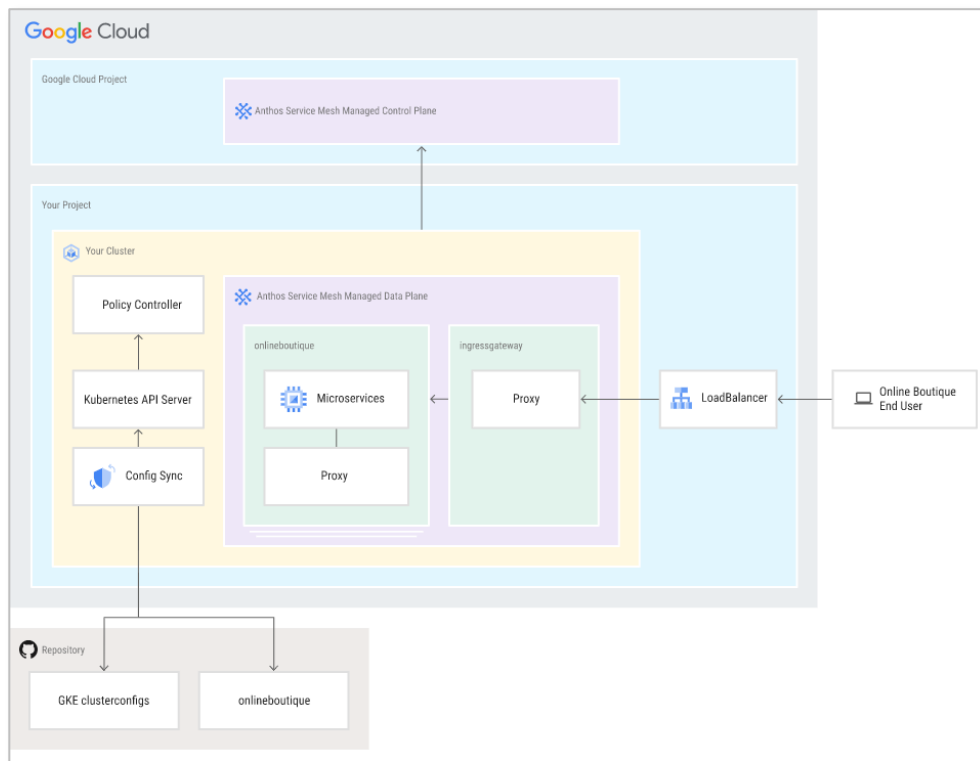


Figure 18: Anthos Service Mesh with Anthos Config Management

Scope and Approach for Review

Anthos may be used in a variety of likely PCI DSS scenarios. Coalfire Opinion Series VRAs benefit from the careful selection of possible and impactful use cases, highlighting critical areas within a product to evaluate potential for PCI compliance.

Scope of Review

While **Anthos** can be deployed within any cloud service provider (e.g., GCP, AWS, Azure), this assessment included on-premises deployments with **Anthos** on VMware (GKE On-Prem) running on GCVE and ABM systems. ACM and ASM were not included in the scope of review, however ACM and ASM (or an equivalent solution) are recommended for production deployments.

As noted in this white paper, Anthos deployments come in many flavors. Customer environments may differ, however most recommendations in this white paper still apply. Anthos customers should consult their security team or a QSA for recommendations specific to their implementation.

Coalfire Evaluation Methodology

Coalfire began by examining the PCI DSS 3.2.1 requirements and identifying them as either organizational (non-technical) or technical. A requirement was determined as either procedural or technical based on a review of the requirement's narrative, testing procedures, and guidance.

Organizational requirements include documented policies, procedures, and standards that were not considered directly applicable to the technical solution. Examples of these non-technical requirements include maintaining facility visitor logs, verifying an individual's identity before granting physical or logical access, performing periodic physical asset inventories, generating network drawings of CHD flow diagrams, and other elements that **Anthos** cannot satisfy.

Once identified, technical requirements were then assessed to determine applicability to **Anthos** for the selected use case. If the achievement of the required objectives was more likely to be met using an external and non-adjacent mechanism, the requirement was determined to be notional to the **Anthos** platform and excluded from the use case. Examples of PCI DSS-related components that Coalfire considered notional and not natively supplied by **Anthos** included external encryption key management solutions, wireless networking, technical or physical access controls, anti-malware solutions, file integrity monitoring (FIM), external firewalls, network switches, network intrusion detection and prevention systems (IDS/IPS).

Coalfire used kube-bench to evaluate **Anthos**' security posture as compared to best-practice recommendations in the current (at the time of writing) Center for Internet Security (CIS) Kubernetes Benchmark, v1.20. Additionally, Coalfire Labs performed an internal penetration test of the mock environment running GKE On-Prem and ABM.

Evaluation of PCI Controls and Scoring System

Coalfire evaluated PCI DSS 3.2.1 requirements and classified them as either organizational or technical. Procedural or technical requirements were based on requirement narratives, testing procedures, and guidance.

Where the requirement was determined as applicable, Coalfire assessed the capability of **Anthos** to address the requirement. In keeping with the desire to present the information compactly, Coalfire used Harvey Balls (https://en.wikipedia.org/wiki/Harvey_Balls) to assign each applicable requirement a qualitative category of capability, including the implementation effort for the **Anthos** adopter implementing the solution.

The table below is a key for the scoring given to each requirement in the scoring tables below:

Symbol	Description	Definition
●	Solid	Fully Supported
◐	Three-fourths	Supported; Minor Implementation Effort for Adopter
◑	Half	Supported; Moderate Implementation Effort for Adopter
◒	One-quarter	Supported; Significant Implementation Effort for Adopter
	Blank	Not Applicable (N/A)
⌋	n-bar	Notional Control

Table 2: Key for Score and Other Symbols

Summary of Overall PCI DSS 3.2.1 Scoring

The information presented in this section (Table 3) represents an aggregate score of the **Anthos** platform based on a composite of the scores provided in the individual requirement scoring tables included in the sections that follow. Coalfire's scoring system summarizes Coalfire's findings for PCI DSS control applicability by representing the number of technical controls and notional controls met for the PCI DSS requirement. The column marked Controls (TC, #, ⌋) reflects the total number of controls (TC) for that requirement, the technical control count (#) potentially applicable to **Anthos** support, and the notional controls (⌋) that would be required and supplied by a system outside of **Anthos** (and therefore be entirely

the customer's responsibility). Any customer responsibilities for the elements of the platform are detailed in their respective section.

In this overall scoring representation, Coalfire has included all requirements, including a non-applicable control, Requirement 9, which pertains to physical access. Requirement 9 comprises customer and non- **Anthos** responsibilities for housing the **Anthos** systems in secure and monitored facilities and for ensuring that the staff supporting those systems have undergone background checks, are trained, and have designated roles.

In subsequent scoring tables, any non-applicable requirements, such as Requirement 9, are omitted for clarity.

PCI Req	PCI DSS Requirements and Security	controls (TC, #, η)	Score
	Build and Maintain a Secure Network and Systems		
1	Install and maintain a firewall configuration to protect cardholder data.	19, 8, 11 η	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	12, 7, 5 η	
	Protect Cardholder Data		
3	Protect stored cardholder data.	21, 0, 21 η	η
4	Encrypt transmission of cardholder data across open, public networks.	4, 1, 3 η	
	Maintain a Vulnerability Management Program		
5	Protect all systems against malware and regularly update antivirus software or programs.	6, 0, 6 η	η
6	Develop and maintain secure systems and applications.	28, 9, 19 η	
	Implement Strong Access Control Measures		
7	Restrict access to cardholder data by business need-to-know.	8, 5, 3 η	
8	Identify and authenticate access to system components.	23, 18, 5 η	
9	Restrict physical access to cardholder data.	22, 0, 22 η	η
	Regularly Monitor and Test Networks		
10	Track and monitor all access to network resources and cardholder data.	29, 28, 1 η	
11	Regularly test security systems and processes.	17, 1, 16 η	
	Maintain an Information Security Policy		
12	Maintain a policy that addresses information security for all personnel.	41, 0, 41 η	η

Table 3: PCI DSS 3.2.1 Overall **Anthos** Scoring

Anthos Applicability to PCI DSS 3.2.1

This section details Coalfire's compliance findings and the corresponding customer requirements and responsibilities for the **Anthos** platform elements, as reviewed in Coalfire's analysis of the suggested use case.

It is essential to understand that platforms and technologies do not themselves provide a CDE application base (software that performs the storage, processing, or transmission of CHD), but can support CDE application software as the term platform implies. Coalfire's review of **Anthos** applicability to PCI DSS is based on the platform's capacity to either provide compliance with the specific PCI DSS control or directly support the actual application code via technical means and other necessary elements of architecture for payment card processing.

Anthos Platform




Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls control the computer traffic that is allowed into and out of a company's network and monitor traffic destined for more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet specified security criteria.

All systems must be protected from unauthorized Internet access, whether through e-commerce requests or employees using desktop browsers or email. Often seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls provide a critical protection mechanism for any computer network.

GCP protects the underlying infrastructure, including hardware, firmware, kernel, OS, storage, network, and more. This includes encrypting data at rest by default, providing additional customer-managed disk encryption, encrypting data in transit, using custom-designed hardware, and laying private network cables. GKE's native Container Network Interface plugin and Calico for NetworkPolicy can be leveraged for fine-grained L7 application layer load balancing.

For all **Anthos** Services (GCP, GKE On-Prem, ABM, ACM, ASM): All virtual firewall rules, network policies, Istio, and load balancing needs to be limited to business justified ports, protocols, and services for both inbound and outbound traffic. Proper configuration of namespaces and Istio is required for limiting defined ports, protocols, and addresses inbound and outbound. It is important to note that the validity of any segmentation must be validated by technical review and penetration testing to meet PCI DSS compliance.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
1	Install and maintain a firewall configuration to protect cardholder data.		
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	<u>GCP</u> : Virtual firewall rules need to be configured on GKE network policy enforcement and applied within the GKE clusters and between nodes, including configuring a DMZ and externally exposing any clusters. These should be limited to defined ports, protocols, and addresses, inbound and outbound, while denying all other traffic.	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Firewall rules should be applied at each Internet connection and between the DMZ and private networks.	
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide	These should be limited to systems components only providing authorized publicly accessible services, ports, and protocols. Limit outbound traffic from the internal	

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
	authorized publicly accessible services, protocols, and ports.	network to only authorized traffic. Additionally, a Cloud NAT instance or gateway can be created for internal nodes to reach out to the Internet.	
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	<p><u>GKE On-Prem and ABM</u>: Load balancer rules and VIPs for services, control plane, and ingress should be applied within the clusters and between nodes. These should be limited to defined ports, protocols, and addresses, inbound and outbound. Firewall rules should be applied at each Internet connection and between the DMZ and private networks. This includes configuring a DMZ and externally exposing any clusters. These should be limited to systems components only providing authorized publicly accessible services, ports, and protocols. This includes limiting outbound traffic from the internal network to only authorized traffic. All egress traffic from the Node to targets outside the cluster is NAT'd by the node IP. Additionally, a Cloud NAT instance or gateway can be created for internal nodes to reach out to the Internet.</p> <p><u>ACM</u>: Proper configuration of connector to the control plane and ingress should be applied within the GKE clusters and between nodes. Proper configuration of namespaces and network constraints with Policy Controller to limit traffic in ACM is required. These should be limited to defined ports, protocols, and addresses, inbound and outbound. Firewall rules should be applied at each Internet connection and between the DMZ and private networks. Proper configuration of namespaces and network constraints with Policy Controller is required to enforced guardrails for network traffic. These should be limited to defined ports, protocols, and addresses inbound and outbound.</p> <p><u>ASM</u>: Proper configuration of Istio is required for limiting namespaces, defined ports, protocols, and addresses, inbound and outbound. Policy Controller is required to enforced guardrails for network traffic. Proper configuration of network constraints with Policy Controller is required to enforce guardrails for outbound network traffic. Proper configuration of Istio is required for proper alias CIDR ranges.</p>	
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.		
1.3.5	Permit only "established" connections into the network.		
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		
1.3.7	<p>Do not disclose private IP addresses and routing information to unauthorized parties.</p> <p>Note: Methods to obscure IP addressing may include, but are not limited to:</p> <ul style="list-style-type: none"> • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses. 		

Table 4: Anthos Platform PCI DSS 3.2.1 Scoring

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Customers are responsible for documenting, developing, and implementing configuration standards for the container node images that are within the CDE. **Anthos** customers using GKE should select a Container-Optimized OS with containers employed with GKE for **Anthos**. Container-Optimized OS by default does not contain any accessible user accounts. The SSH daemon is configured to disallow password-based authentication, and no root logins are allowed. However, each

GKE node does come provisioned with the default Compute Engine service account. Customers must manually configure and remove this default account. GCP protects the underlying infrastructure, including hardware, firmware, kernel, OS, storage, network, and more.

For all **Anthos** Services, GCP maintains TLS 1.2 or greater to support customer's PCI workloads. Customers are responsible for initiating TLS connections that use TLS 1.2 or greater to meet their PCI compliance requirements.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
2	Do not use vendor-supplied defaults for system passwords and other security parameters.		
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Anthos supports industry-accepted standards by supporting tools including Aqua's Kube-Bench, which tests clusters against CIS benchmarks to identify and remediate configuration drift.	●
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: <ul style="list-style-type: none"> Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST) 	<u>GCP</u> : Customers are responsible for ensuring secure communication for administrative access to the cluster nodes by enforcing SSH v2 or above with appropriate SSH keys. <u>GKE On-Prem</u> : Customers are responsible for documenting, developing, and implementing configuration standards for the container node images that are within the CDE. Anthos clusters are deployed with an Ubuntu OS image that has root login disabled. Anthos nodes are configured with Anthos node images whereby SSH root login is disabled. Customers are responsible for ensuring secure communication for administrative access to the cluster nodes by enforcing SSH v2 or above with appropriate SSH keys. <u>ABM</u> : Customers are responsible for documenting, developing, and implementing configuration standards for the container node images that are within the CDE. Customers are responsible for documenting, developing, and implementing configuration standards for the open-source and enterprise Linux OSs, including CentOS, Red Hat Enterprise Linux (RHEL), and Ubuntu. Customers are responsible for ensuring secure communication for administrative access to the cluster nodes by enforcing SSH v2 or above with appropriate SSH keys.	●
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	<u>ABM</u> : Customers are responsible for documenting, developing, and implementing configuration standards for the open-source and enterprise Linux OSs, including CentOS, Red Hat Enterprise Linux (RHEL), and Ubuntu. Customers are responsible for ensuring secure communication for administrative access to the cluster nodes by enforcing SSH v2 or above with appropriate SSH keys.	●
2.2.4	Configure system security parameters to prevent misuse.	<u>ACM</u> : Customers are responsible for documenting, developing, and implementing configuration standards for ACM components, enabling Config Sync, and configuration of Policy Controller with applicable policies that support PCI compliance. ACM does not come configured with any default accounts. Anthos customers must configure defined roles and permissions to be able to administer and install ACM itself, as well as components for Config Sync, Hierarchy Controller, Config Connector, Binary Authorization, and Policy Controller. Customers are responsible for documenting, developing, and implementing configuration standards for the Git repository used by ACM. Customers are responsible for ensuring secure communication is used	●
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		●
2.3	Encrypt all non-console administrative access using strong cryptography.		●


PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
		for access to the Git repository used by ACM via SSH deploy keys or HTTPS deploy tokens. <u>ASM</u> : Customers are responsible for documenting, developing, and implementing configuration standards for ASM, including Istio configurations and namespaces, and for configuring mTLS STRICT mode for all services. ASM does not come configured with any default accounts. Anthos customers must configure defined roles and permissions to be able to administer and install ASM. Customers are responsible for ensuring secure communication for administrative access.	
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Google Cloud console, monitoring dashboard, and CLI support maintenance of an inventory of system components in scope.	

Table 5 *Anthos Platform PCI DSS 3.2.1 Scoring*

Requirement 3: Protect stored cardholder data


Protection methods such as encryption, truncation, masking, and hashing are critical components of CHD protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential opportunities for risk mitigation. For example, methods for minimizing risk include not storing CHD unless necessary, truncating CHD if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

For all **Anthos** services, customers are responsible for maintaining appropriate data retention policies and procedures, encryption technologies, and cryptographic key management processes for maintaining stored CHD, including SAD.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to CDEs.

For all **Anthos** services, customers are responsible for strong cryptography and security protocols for any connections transmitting CHD and for ensuring the data is encrypted in transit. This includes encrypting data at rest by default, providing additional customer-managed disk encryption, encrypting data in transit

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
4	Encrypt transmission of cardholder data across open, public networks		
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks	<u>GCP</u> : Customers are responsible for configuring nodes with appropriate certificates and strong cryptography and security protocols to protect CHD in transit. Customers can use Google-managed SSL certificates or customer-managed certificates. <u>GKE On-Prem and ABM</u> : Customers are responsible for configuring load balancer rules and VIPs, control plane,	

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
		<p>and ingress applied within the clusters and between nodes with appropriate certificates and strong cryptography and security protocols to protect CHD in transit. Customers can use Google-managed SSL certificates or customer-managed certificates.</p> <p><u>ACM</u>: ACM's Policy Controller constraints can be used to enforce TLS and host restrictions for open, public networks.</p> <p><u>ASM</u>: Proper configuration of Istio is required, as is configuring the Service Mesh to use the Certificate Authority (CA) service.</p>	

Table 6 *Anthos Platform PCI DSS 3.2.1 Scoring*

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware” (such as viruses, worms, and Trojans), enters the network during many business-approved activities, including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

For all *Anthos* services, customers are responsible for managing anti-virus to PCI requirements for any node images determined to be commonly affected by malware.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of CHD by malicious individuals and malicious software.

For all *Anthos* services, customers are responsible for managing the security patches of their cluster node images and for ensuring compliance with requirement 6. Customers are responsible for maintaining software development standards, change control, and vulnerability management programs in alignment with PCI requirements for applications deployed.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
6	Develop and maintain secure systems and applications.		
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	<p><u>Customers are responsible for managing the security patches of their cluster node images and ensuring compliance w/ PCI 6.1 requirements.</u></p> <p><u>Customers are responsible for reviewing all Google Security Bulletins and applicable vendor security alerts and ensuring that any recommendations that are</u></p>	

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
6.2	<p>Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.</p> <p>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</p>	<u>applicable to the customer's environment are reviewed and implemented as necessary.</u>	
6.3	<p>Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:</p> <ul style="list-style-type: none"> • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle 	<p><u>All Anthos Services:</u> Customers are responsible for any custom configurations that may be created using development criteria that are allowed by the APIs. This development should use the same processes as other applications that are developed by the customer and be compliant with the PCI requirements for development standards.</p> <p><u>ACM:</u> Customers can implement a pipeline with Cloud Build, Config Sync and/or Policy Controller leveraging GateKeeper policy constraints to enforce their SDLC policy and testing.</p>	
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	<u>ACM:</u> Customers can implement a pipeline with Cloud Build, Config Sync and/or Policy Controller leveraging GateKeeper policy constraints that could include blacklisting/whitelisting rules to prevent test accounts, user IDs, or credentials are from migrating into production.	
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes)	<u>ACM:</u> Customers can implement a pipeline with Cloud Build, Config Sync and/or Policy Controller leveraging GateKeeper policy constraints that could include blacklisting/whitelisting rules for successful code promotion and testing use cases.	
6.4	Follow change control processes and procedures for all changes to system components.	<u>ACM:</u> Customers can implement a pipeline with Cloud Build, Config Sync and/r Policy Controller leveraging GateKeeper policy constraints that could include blacklisting/whitelisting rules for successful code promotion and testing use cases that support at least part of this requirement.	
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	<p><u>ACM:</u> Customers can implement a pipeline with Cloud Build, Config Sync and/r Policy Controller leveraging GateKeeper policy constraints that could include blacklisting/whitelisting rules for successful code promotion and testing use cases that support at least part of this requirement.</p> <p><u>ASM:</u> Proper configuration of Istio is required for limiting namespaces, defined ports, protocols, and addresses inbound and outbound.</p>	

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
6.4.2	Separation of duties between development/test and production environments	<u>ACM</u> : Customers can implement a pipeline with Cloud Build, Config Sync and/r Policy Controller leveraging GateKeeper policy constraints for Namespaces, RoleBindings, PSP, and other constraints to enforce access restrictions. <u>ASM</u> : Proper configuration of Istio is required for limiting namespaces, defined ports, protocols, and addresses inbound and outbound.	●
6.4.4	Removal of test data and accounts from system components before the system becomes active / goes into production.	<u>ACM</u> : Customers can implement a pipeline with Cloud Build, Config Sync and/r Policy Controller leveraging GateKeeper policy constraints for Namespaces, RoleBindings, PSP, and other constraints to enforce access restrictions.	●

Table 7 Anthos Platform PCI DSS 3.2.1 Scoring

Requirement 7: Restrict access to cardholder data by business need-to-know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need-to-know and according to job responsibilities. “Need-to-know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.

For all **Anthos** services, customers are responsible for managing access to all **Anthos** services that are included in their CDE. GCP provides various mechanisms for controlling access to the services, including IAM for integration with corporate directories and granular access controls to the GCP Management Console.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
7	Restrict access to cardholder data by business need-to-know.		
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	<u>GCP, GKE On-Prem, and ABM</u> : Customers can configure IAM or Kubernetes RBAC to manage access to clusters, nodes, and objects.	●
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	<u>ACM</u> : Customers can implement a pipeline with Cloud Build, Config Sync, and/or Policy Controller by leveraging GateKeeper policy constraints for NameSpaces, RoleBindings, PSP, and other constraints to enforce access restrictions. Proper configuration of ClusterRoles and ClusterRoleBindings allow customers to control permissions within a cluster. Additionally, enforcing SSH with keys or tokens to the Git repository is necessary. Customers can federate Google Cloud to their chosen IdP or use Google as their IdP using the Google OAuth 2.0 OmniAuth Provider or Secure LDAP.	●
7.2	Establish an access control system(s) for systems components that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed. This access control system(s) must include the following:	<u>ASM</u> : Customers can grant access to Service Mesh within the Google Console, as well as set up the necessary roles required to install and manage ASM via IAM.	●
7.2.1	<ul style="list-style-type: none"> Coverage of all system components 		●
7.2.3	<ul style="list-style-type: none"> Default “deny-all” setting. 		●

Table 8 Anthos Platform PCI DSS 3.2.1 Scoring

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification to each person with access ensures that everyone is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system, particularly how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

For all **Anthos** services, customers are responsible for managing access to all **Anthos** services that are included in their CDE. GCP provides various mechanisms for controlling access to the services, including IAM for integration with corporate directories and granular access controls to the GCP Management Console.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
8	Identify and authenticate access to system components.		
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	<u>GCP, GKE On-Prem, and ABM</u> : Customers can configure IAM or Kubernetes RBAC to manage access to clusters, nodes, and objects.	
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	<u>ACM</u> : Proper configuration of ClusterRoles and ClusterRoleBindings allow customers to control permissions within a cluster. Additionally, enforcing SSH with keys or tokens to the Git repository is necessary. Customer can federate Google Cloud to their chosen IdP or use Google as their IdP using the Google OAuth 2.0 OmniAuth Provider or Secure LDAP.	
8.1.3	Immediately revoke access for any terminated users.		
8.1.4	Remove/disable inactive user accounts within 90 days.	<u>ASM</u> : Customers can grant access to ASM within the Google Console, as well as set up the necessary roles required to install and manage ASM via IAM.	
8.1.5	Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: <ul style="list-style-type: none"> Enabled only during the time period needed and disabled when not in use. Monitored when in use. 		
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Customer must enforce account lockout to no more than 6 attempts.	
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Customer must enforce account lockout for a minimum of 30 minutes or until an admin unlocks the account.	
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Customer must enforce session timeout after no more than 15 minutes.	
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on	<u>GCP, GKE On-Prem, and ABM</u> : Customers can configure IAM or Kubernetes RBAC to manage access to clusters, nodes, and objects.	

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
	<p>all system components by employing at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric 	<p><u>ACM</u>: Proper configuration of ClusterRoles and ClusterRoleBindings allow customers to control permissions within a cluster. Additionally, enforcing SSH with keys or tokens to the Git repository is necessary. Customer can federate Google Cloud to their chosen IdP or use Google as their IdP using the Google OAuth 2.0 OmniAuth Provider or Secure LDAP.</p> <p><u>ASM</u>: Customers can grant access to ASM within the Google Console, as well as set up the necessary roles required to install and manage ASM via IAM.</p>	
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	<p><u>All Anthos Services</u>: Customers are responsible for managing user accounts using the various authentication mechanisms within IAM. For accounts managed directly in IAM, passwords are rendered unreadable in storage and transmission fully managed by GCP. For customers connecting IAM to the corporate directory, customers are responsible for ensuring that the corporate directory configuration stores credentials in an unreadable and protected format as well as in transit for authentication.</p> <p><u>GCP, GKE On-Prem, and ABM</u>: Customers are responsible for managing user accounts and access controls using the various authentication mechanisms offered by GCP. This includes access controls to all Anthos Products included in scope as well as to the cluster nodes and applications that customers may be hosting. Customers are responsible for ensuring proper configuration of the authentication mechanisms to ensure that passwords are unreadable in storage and transmission.</p>	●
8.2.3	<p>Passwords/passphrases must meet the following:</p> <ul style="list-style-type: none"> • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. • Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above. 	<p><u>All Anthos Services</u>: Customers are responsible for managing user accounts. IAM features include password management options for user and service accounts such as password length and complexity requirements. Additional password management controls can be provided by connecting IAM to a corporate directory service.</p>	●
8.2.4	Change user passwords/passphrases at least once every 90 days.	<p><u>All Anthos Services</u>: IAM features include password management options for user and service accounts such as password rotation every 90 days. Additional password management controls can be provided by connecting IAM to a corporate directory service.</p>	●
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	<p><u>All Anthos Services</u>: IAM features include password management options for user and service accounts such as password history and remembrance. Additional password management controls can be</p>	●

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
		provided connecting IAM to a corporate directory service.	
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.	<u>All Anthos Services:</u> IAM features include password management options for user and service accounts such as password change enforcement. Additional password management controls can be provided by connecting IAM to a corporate directory service.	
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	<u>All Anthos Services:</u> Customers are responsible for managing access to all Anthos services in the CDE. GCP provides various mechanisms for controlling access services including IAM for integration with corporate directories and granular access controls to the GCP Management Console. Customers can integrate with Google Authenticator MFA or leverage their desired MFA solution according to PCI requirements.	
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator and including third-party access for support or maintenance) originating from outside the entity's network.		
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: <ul style="list-style-type: none"> • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. 	<u>All Anthos Services:</u> Customers are responsible for managing access to all Anthos services in the CDE. GCP provides various mechanisms for controlling access to the services including IAM for integration with corporate directories and granular access controls to the GCP Management Console. Customers can integrate with Google Authenticator MFA or leverage their desired MFA solution according to PCI requirements.	
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: <ul style="list-style-type: none"> • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). 	<u>All Anthos Services:</u> Customers are responsible for managing user accounts and access controls to applications installed by the customer running on Anthos cluster nodes, including databases.	

Table 9 Anthos Platform PCI DSS 3.2.1 Scoring

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house CHD provides the opportunity for individuals to access devices or data and to remove systems or hard copies and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service worker, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing CHD.

For all **Anthos** services, GCP maintains the physical security and media handling controls for Google data centers and colocations supporting the **Anthos** services running on GCP.

For GKE On-Prem, customers are responsible for physical security requirements for running the GKE On-Prem and ABM implementation of **Anthos**.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

For all **Anthos** services, customers are responsible for setting permissions and access controls for audit logs. IAM can be used to set permissions for accounts with access to Google Cloud Logging/Stackdriver. Customers are responsible for the review (automated or manual) of audit logs received via Google Cloud Logger/Stackdriver or via a customer-defined centralized audit log solution in alignment with PCI requirements.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
10	Track and monitor all access to network resources and cardholder data.		
10.1	Implement audit trails to link all access to system components to each individual user.	<u>GCP</u> : Customers are responsible for configuring logging parameters and enabling audited logs for cluster nodes. This includes customer enabling application specific logs, the GKE audit policy, and the Kubernetes audit policy in alignment with PCI requirements. GCP Console and all command-line use of GCP API actions are logged by GCP and may be accessed via Google Cloud Logging/Stackdriver.	●
10.2	Implement automated audit trails for all system components to reconstruct the following events:		●
10.2.1	<ul style="list-style-type: none"> All individual user accesses to cardholder data 	<u>GKE On-Prem and ABM</u> : Customers are responsible for configuring logging parameters and enabling audited logs for cluster nodes. This includes customer enabling application specific logs and the Kubernetes audit policy in alignment with PCI requirements. Customers must enable the Anthos GKE and Anthos Audit API.	●
10.2.2	<ul style="list-style-type: none"> All actions taken by any individual with root or administrative privileges 	Customers can choose to send logs to Cloud Logging (for indefinite storage) or logs can be written locally to disk at the customer premises for up to 12 GB of log data.	●
10.2.3	<ul style="list-style-type: none"> Access to all audit trails 		●
10.2.4	<ul style="list-style-type: none"> Invalid logical access attempts 	<u>ACM</u> : Customers can configure enforcement actions within the policy controller to deny or monitor (via dryrun) violations of rules without blocking. Audited violations are appended to the Constraint objects and are also written to the logs. To see violations of a given constraint, run	●
10.2.5	Use of and changes to identification and authentication mechanisms — including but not limited to creation of new accounts and elevation of privileges — and all changes,		●

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
	additions, or deletions to accounts with root or administrative privileges	<p>kubectl get constraint-kind constraint-name -o yaml. To get all Policy Controller logs, run the following command: <code>kubectl logs -n gatekeeper-system -l gatekeeper.sh/system=yes</code></p> <p><u>ASM</u>: Customers must configure audit policies specific to a workload, namespace, or the entire service mesh. These can be viewed within Google Cloud Logging in the GCP Console. ASM writes Admin Activity audit logs, which include operations that modify the configuration or metadata of a resource. ASM doesn't write Data Access audit logs, doesn't write System Event audit logs, and doesn't write Policy Denied audit logs.</p>	
10.2.6	Initialization, stopping, or pausing of the audit logs		●
10.2.7	Creation and deletion of system-level objects		●
10.3	Record at least the following audit trail entries for all system components for each event:		●
10.3.1	<ul style="list-style-type: none"> User identification 		●
10.3.2	<ul style="list-style-type: none"> Type of event 		●
10.3.3	<ul style="list-style-type: none"> Date and time 		●
10.3.4	<ul style="list-style-type: none"> Success or failure indication 		●
10.3.5	<ul style="list-style-type: none"> Origination of event 		●
10.3.6	<ul style="list-style-type: none"> Identity or name of affected data, system component, or resource. 		●
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	<p><u>GCP, GKE On-Prem, and ABM</u>: Customers are responsible for appropriately managing time service (NTP) configuration for cluster nodes on GCP and GKE On-Prem and should be configured to use centralized NTP servers. This assures that log events from customer cluster nodes will be time synchronized. GKE is pre-configured with timesyncd configured to GCP NTP time servers or customers can configure to use their own defined NTP servers and time sync solution.</p>	◐
10.4.1	Critical systems have the correct and consistent time.		◐
10.4.2	Time data is protected.		◐
10.4.3	Time settings are received from industry-accepted time sources.		◐
10.5	Secure audit trails so they cannot be altered.	<p>Customers are responsible for setting permissions and access controls for audit logs. IAM can be used to set permissions for accounts with access to Google Cloud Logging/Stackdriver. Customers are responsible for configuration of logging and monitoring their systems components and cluster nodes in alignment with PCI requirements.</p> <p><u>GKE On-Prem and ABM</u>: If customers utilize the log to disk feature, those up to 12GB of audit logs must also be</p>	◐
10.5.1	Limit viewing of audit trails to those with a job-related need.		◐
10.5.2	Protect audit trail files from unauthorized modifications		◐
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		◐

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	backed up to a centralized server or media that is difficult to alter.	●
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this requirement.	Customers are responsible for review (automated or manual) of audit logs received via Google Cloud Logger/Stackdriver or customer defined centralized audit log solution in alignment with PCI requirements.	●
10.6.1	Review the following at least daily: <ul style="list-style-type: none"> All security events Logs of all system components that store, process, or transmit CHD and/or SAD Logs of all critical system components Logs of all servers and system components that perform security functions (for example, firewalls, IDS/IPS, authentication servers, e-commerce redirection servers, etc.). 		●
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).		●

Table 10 *Anthos Platform PCI DSS 3.2.1 Scoring*

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

For all **Anthos** services, customers are responsible for all internal vulnerability scanning and rescanning efforts for GKE cluster nodes and applications. Scans should include internal, private customer IP addresses and not GCP endpoints, which are tested as part of GCP compliance vulnerability scans. Customers are responsible for all penetration testing activities, including external and internal penetration testing, application testing, and network testing to include segmentation validation every six months for GKE cluster nodes and applications. All exploitable findings must be remediated and re-tested until a passing score is obtained. Penetration testing should include externally facing and internal private customer IP addresses and not GCP endpoints, which are tested as part of GCP compliance vulnerability scans. Customers are responsible for implementing FIM capability for their GKE cluster nodes and applications.

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
11	Regularly test security systems and processes.		
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to	Customers can deploy FIM with Container Analysis and the Artifact Registry using Container-Optimized OS pods	●

PCI Req	PCI DSS Requirements and Anthos Platform	Comments	Score
	alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	<u>ACM</u> : Customers can implement a pipeline with Cloud Build, Config Sync, and/or Policy Controller leveraging GateKeeper policy constraints to enforce immutability in image repos and build policy.	

Table 11 *Anthos Platform PCI DSS 3.2.1 Scoring*

Requirement 12: Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors, and consultants who are “resident” on the entity’s site or otherwise have access to the CDE.

For all *Anthos* services, customers are responsible for maintaining information security policies, procedures, and processes applicable to their CDE to maintain PCI DSS compliance.

Customer Responsibilities for PCI DSS Use of the Anthos Platform

Summarized below are customer responsibilities for PCI DSS use of the *Anthos* Platform.

- Customers should:
 - Maintain network and data flow diagrams
 - Maintain workloads, application code, build files, container images, containers, pods, IAM, and data
 - Operate, maintain, and patch infrastructure
 - Maintain connectivity to Google Cloud
 - Minimize Google Cloud service account privileges
 - Configure OpenID Connect for user authentication
 - Use namespaces with RBAC for administrative isolation and least privilege roles and entitlements
 - Use a vSphere administrator account with minimal privileges (GKE On-Prem)
 - Set vSphere to encrypt the volumes used by *Anthos* clusters (GKE On-Prem)
 - Encrypt data at rest
 - Encrypt secrets at rest
 - Implement controls to isolate and protect the control plane networks and nodes
 - Implement network policies to control L4 traffic
 - Implement ASM or Istio to control L7 traffic and enforce strict mTLS
 - Implement *Anthos* Config Management Policy Controller or Gatekeeper
 - Restrict the ability for workloads to self-modify by applying Gatekeeper or Policy Controller constraints
 - Secure containers with SELinux (ABM)

- Use secure computing mode (seccomp) to restrict containers (ABM)
- Don't run containers as root user
- Deploy logging and monitoring agents
- Integrate logging into a SIEM solution
- Monitor security bulletins
- Upgrade **Anthos** clusters, nodes, and admin workstation as needed
- Maintain support contracts with vendors, including VMware and F5 if deployed.

Conclusion and Coalfire Opinion

Coalfire reviewed **Anthos** for its efficacy in assisting payment card entities with successful deployments resulting in a compliant SAQ or ROC for PCI DSS 3.2.1. It has the following opinion of the potential product use in the compliance program.

Anthos can be implemented as part of a CDE. When deployed with controls described in this paper, **Anthos** supports and often meets PCI DSS compliance requirements. While there are additional factors unique to a cloud solution, these factors are in no way insurmountable. In fact, many features of **Anthos** easily support compliance with PCI DSS requirements and assist organizations with a more secure and cost-effective solution.

Coalfire concludes that the reviewed **Anthos** solution can be effective in providing significant and substantial support for PCI DSS payment entities' objectives and requirements. This opinion applies to scenarios like the suggested merchant POS use case and a considerable number of other real-world payment card applications, based on the observed PCI DSS control support that is common to both the reviewed scenario and those other applications.

This opinion is also dependent on many underlying presumptions (caveats), which are expectations of an actual payment card processing environment and are listed below:

- Adherence to vendor best practices for **Anthos** and other associated vendors used in an actual deployment.
- Required ancillary services to provide CT/SI systems, including potential Microsoft AD, LDAP, DNS, NTP, and other likely services.
- Implementation of specific external firewalls, external network switches, anti-malware/anti-virus, FIM, IDPS, SIEM, and other required PCI systems.
- Use of supporting services and providers to process payments (upstream payment providers), supply continuous repair and maintenance, and other contracted and PCI DSS compliant services consumed by the entity.
- Actual organizational controls support their payment card entity roles, responsibilities, policies, procedures, baselines, and mandates.
- Physical controls to control and secure access to the facilities.
- Periodic penetration testing (internal and external), and vulnerability scans, including internal scans and external scans by a PCI DSS Approved Scan Vendor (ASV).
- Presence of IT staff to support the workload and business operations.
- Actual payment card bespoke, organization-custom POS applications, POI devices, and other POS components.

A Comment Regarding Regulatory Compliance

Coalfire disclaims the generic suitability of any product to establish regulatory compliance strictly by use of that product. Agencies and entities attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not *via* the use of a specific product. This is true for merchants and service providers subject to PCI DSS, and customers targeting compliance with other regulations.

Legal disclaimer

This white paper is provided by Coalfire Systems, Inc., or its subsidiaries (“Coalfire”) for informational purposes only. This white paper is the property of Coalfire and is protected by U.S. and international copyright laws. Unauthorized use, reproduction, or distribution of this white paper, in whole or in part, is strictly prohibited. Factual information included in this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

Additional Information, Resources, and References

This section contains a description of the links, standards, guidelines, and reports used for the materials used to identify and discuss the features, enhancements, and security capabilities of *Anthos*.

Google Anthos Resources

- *Anthos* clusters on VMware overview
<https://cloud.google.com/anthos/clusters/docs/on-prem/latest/overview>
- ABM overview
<https://cloud.google.com/anthos/clusters/docs/bare-metal/latest/concepts/about-bare-metal>
- Hardening your ABM cluster’s security
<https://cloud.google.com/anthos/clusters/docs/bare-metal/latest/how-to/hardening-your-cluster>
- Hardening your VMware (GKE On-Prem) cluster’s security
<https://cloud.google.com/anthos/clusters/docs/on-prem/latest/how-to/hardening-your-cluster>
- Security blueprint: PCI on GKE
<https://cloud.google.com/architecture/gke-pci-dss-blueprint>
- PCI DSS baseline for *Anthos* clusters on VMware (GKE On-Prem)
<https://cloud.google.com/architecture/pci-dss-baseline-for-anthos-clusters-vm>
- Security features included in *Anthos* clusters on VMware (GKE On-Prem)

<https://cloud.google.com/anthos/clusters/docs/on-prem/latest/concepts/security>

- CIS Kubernetes Benchmark compliance auditing with **Anthos** clusters on VMware (GKE On-Prem)
<https://cloud.google.com/anthos/clusters/docs/on-prem/latest/concepts/cis-benchmarks>
- CIS Kubernetes Benchmark compliance auditing with ABM:
<https://cloud.google.com/anthos/clusters/docs/bare-metal/latest/concepts/cis-benchmarks>
- **Anthos** shared responsibility
<https://cloud.google.com/anthos/docs/concepts/gke-shared-responsibility>
- **Anthos** code samples
<https://github.com/GoogleCloudPlatform/anthos-samples>
- Cloud Security Blueprints for **Anthos**
<https://github.com/GoogleCloudPlatform/anthos-security-blueprints>
- **Anthos** security bulletins:
<https://cloud.google.com/anthos/clusters/docs/security-bulletins>

PCI Security Standards Council Data Security Standard

References

- The current version of the PCI DSS is 3.2.1 as of May 2018. This white paper references the PCI DSS Standard revisions from 2014-2018. The current revision may be accessed via the following link:
https://www.pcisecuritystandards.org/document_library
- An information supplement from the PCI SSC is the guidance for PCI DSS Scoping and Network Segmentation. The guidance document may be found at the following link:
https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf
- Details of the PCI SSC Cloud Special Interest Group updates to virtualization and cloud Information Supplement, developed as PCI SSC Cloud Computing Guidelines, April 2018, are available at the following link:
https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

Coalfire References

- The Coalfire corporate payment card references and the Solutions Engineering offerings may be found at the following links:
<https://www.coalfire.com/industries/payments>
<https://www.coalfire.com/solutions/cyber-engineering>
- Coalfire corporate information is available at the following link:
<https://www.coalfire.com/about>

About the authors

Kerry Steele | *Principal Consultant, Payments & Cloud Advisory*

With over two decades of information security risk and compliance management experience, Kerry is responsible for providing guidance to business and technical leaders through adoption of new and emerging payment and cloud security solutions to address complex business challenges with business-centric cybersecurity solutions strategies.

Allen Mahaffy | *Principal Consultant, Payments & Cloud Advisory*

Allen works in the Payments & Cloud Advisory practice performing advisory and assessments for major cloud service providers and large enterprises. His other experience in cloud includes assessing and analyzing cloud micro-service architectures, container orchestration, security and compliance automation, and various emerging cloud technologies.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit [Coalfire.com](https://www.coalfire.com).

Copyright © 2022 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.