Google Cloud

Google Cloud API & Integration

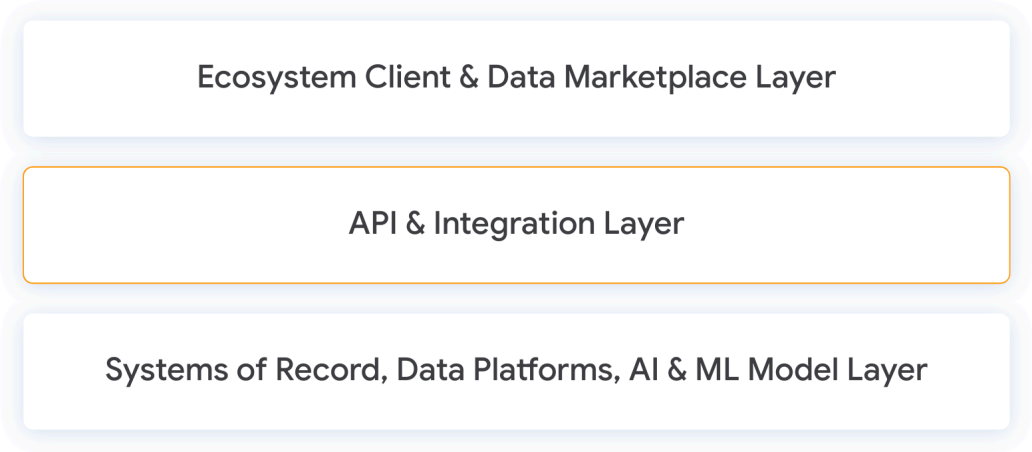
Security Architecture

Table of contents

01. Introduction

1.1 Summary

This document describes the end-to-end security architecture for a proposed API & integration architecture in Google Cloud. Most of the information can also be applied to on-premise and hybrid deployments, but unless otherwise stated the content here will focus on a cloud-first solution using cloud-native services to securely handle data processing and storage. This has the advantage that the services are hardened, verified and regularly audited to operate securely at scale for Google's internal usage, as well as for cloud customers around the world.

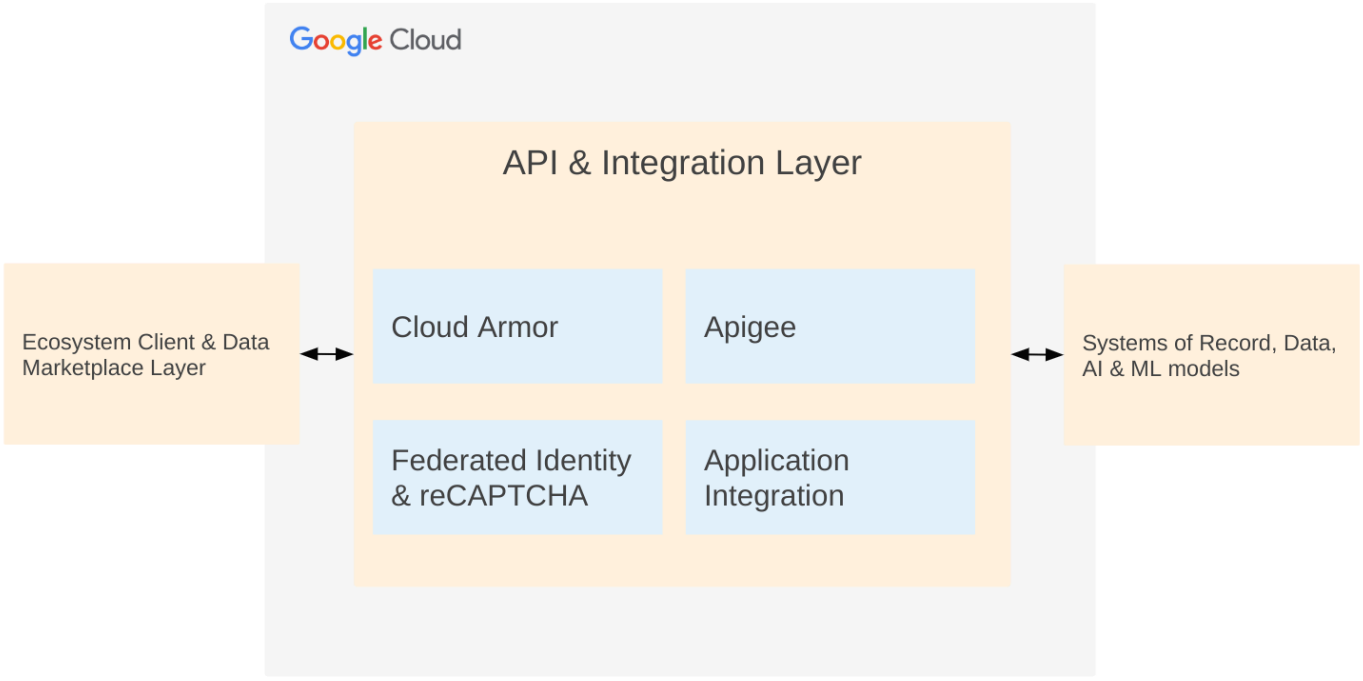


Picture 1: This document focuses on the API & Integration Layer

In the layers above the clients and data consumers (both first-party and third) connect through a verified, secured **API & Integration Layer** before reaching internal data & services in the bottom layer. This enables common, stringent and detailed security & integration policies to be applied on all traffic that is allowed to enter to the internal data layer.

1.2 API & Integration Layer components

There are multiple components used in the **API & Integration Layer**, each applying specific security capabilities to the data & service network pipeline.



Picture 2: The components used within the API & Integration Layer.

The services above are easily leveraged together in Google Cloud to bring a strong & consistent security posture through integrated security, standardized development & release lifecycles, and a unified monitoring & analytics platform. But because the services are based on secure APIs for their functionality, other solutions & services can also be easily integrated and leveraged, depending on the requirements.

Load Balancer Layer 4 / Layer 7 - Cloud Armor

- DDoS protection and WAF at Google scale
- Geo-fencing of APIs
- Mitigates OWASP Top 10 risks, custom rules engine

API Gateway Layer 7 - Apigee

- Authentication & authorization for APIs
- Rate limiting & cert management on API backends
- Custom payload signatures, injection detection (XML, JSON, SQL...)
- OWASP T10 for APIs
- Business logic attacks (scoring, abuse & anomaly detection)

Integration Layer 7 - Application Integration

- User & related data lookup, history & validation
- Structured & secure engine for processing events & data

- Code-less integrations, hardened connectors & reusable paths
- Logging & tracing of system access & validation

Identity Layer 7 - Federated Identity & reCAPTCHA

- Google Cloud Identity Platform & Firebase Auth, along with Google IAM, provide federated identity as a service to clients on the platform.
- IDPs such as Google IAM, Azure AD, ForgeRock, and any other standards-compliant system can be used to authenticate and authorize user actions through the API layer.
- reCAPTCHA enforces identity-based verification & challenge validation in addition to the IDP, resulting in the better identification of fraudulent traffic from account creation through account manipulation & theft through bots.

All together this architecture for the API & Integration layer is key to safely & securely offering packages of access to services, data & AI/ML models to both internal and external users through marketplace platforms.

1.3 Core platform principles

1.3.1 End-to-end adherence to 'zero trust' principles

Google's services are the application binaries that our developers write and run on our infrastructure. Examples of Google's services are Gmail servers, Spanner databases, Google Cloud Storage (GCS) servers, and Google Compute Engine (GCE) Virtual Machines (VMs) running customer applications. The infrastructure does not assume any trust between the services that are running on the infrastructure. This trust model is referred to as a zero trust security model, called BeyondCorp within Google. A zero trust security model means that no devices or users are trusted by default, whether they are inside or outside of the network.

At the core of a zero trust approach is the idea that implicit trust in any single component of a complex, interconnected system can create significant security risks. Instead, trust needs to be established via multiple mechanisms and continuously verified. We pioneered the foundational concepts behind zero trust architectures with our BeyondCorp and BeyondProd models. Google's proven zero trust architecture ensures that only the individual with the right identity, accessing the right machine, and authorized by the right code is accessing the right data at the right time and in the right context. Our zero trust security framework requires all users to be authenticated, authorized, and validated for security configuration and posture before being granted or keeping access to cloud-based applications and data.

1.3.2 Secure data at rest and in transit

All data is encrypted at all times, including at rest, without any action required by users, using one or more encryption mechanisms. Encryption at rest is encryption that is used to help protect data that is stored on a disk (including Solid State Drives [SSDs]) or backup media. All the data that is stored by Google is encrypted at the storage layer using the Advanced Encryption Standard (AES) algorithm, AES-256. We use a common cryptographic library, Tink, which includes our Federal Information Processing Standard (FIPS) 140-2 validated module (named BoringCrypto) to implement encryption consistently across Google Cloud.

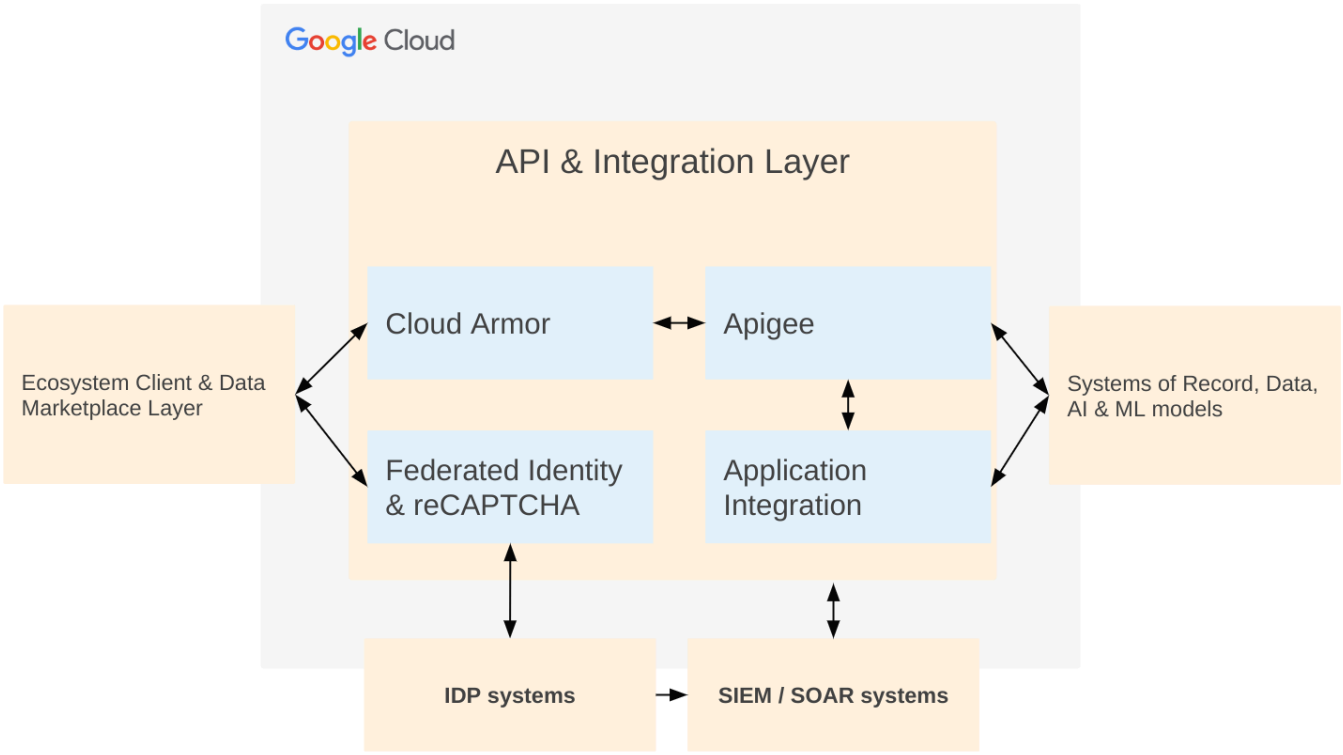
Google employs several security measures to help ensure the authenticity, integrity, and privacy of the data in transit. Google usually encrypts and authenticates the data in transit at one or more network layers when the data moves outside physical boundaries not controlled by Google or on behalf of Google. Depending on the connection that is being made, Google applies default protections to that data. For example, we secure communications between the user and the GFE (Google Frontend Load Balancer) using Transport Layer Security (TLS).

Google plans to remain the industry leader in encryption-in-transit, and thus, we dedicate resources towards the development and improvement of encryption technology, including innovations in the areas of Key Transparency and post-quantum cryptography.

1.3.3 AI/ML support

Security features throughout the stack are enhanced through the use of Google-developed and tested AI/ML models to better recognize, identify and respond to threats in real-time. Customers can even securely tune and retrain models using their own data if wanted in Apigee, reducing the number of false-positives through finer-grained recognition of the customer's own traffic patterns. AI/ML models are used at all levels, from the DDoS protection at the Cloud Armor edge to API and identity-specific models in Apigee and reCAPTCHA.

02. Security architecture



Picture 3: The security architecture for the API & Integration layer

The API & Integration layer is responsible for processing traffic and requests from clients & apps, authenticating, authorizing, & validating the requests, and finally connecting & integrating the requests to the configured backend systems, APIs, files, AI/ML models, and other destinations. The client apps will have direct contact with Cloud Armor on the API load balancer, as well as with the federated identity & reCAPTCHA systems. From Cloud Armor the requests that are not blocked are processed further to Apigee, Application Integration, and if allowed routed & transformed to the appropriate destination. Data can also flow in the other direction through events & streams, which can be processed in Application Integration and trigger updates that are broadcast, if allowed, to listeners and clients that are subscribed to receive updates. It is important that all data flows in both directions are processed in a consistent & secure pipeline, without direct and potentially insecure connectivity between backends and clients. This is provided seamlessly and automatically to everyone on the platform, for every type of API & event, making it easy and automatic for everyone to be secure.

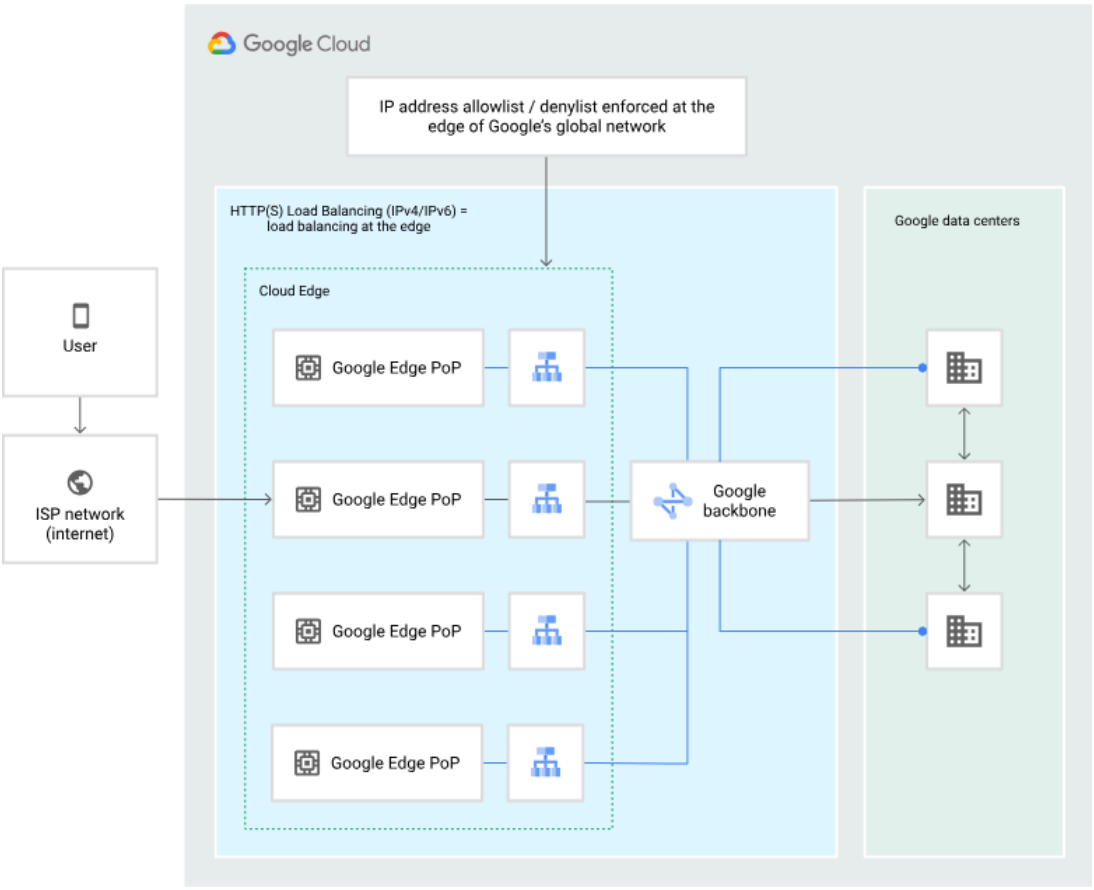
All monitoring, event & logging data is fed into the SIEM systems from the API & Integration layer, as well as from the IDPs and other systems.

2.1 What is Cloud Armor?

Google Cloud Armor helps protect services from multiple types of threats, including distributed denial-of-service (DDoS) attacks and application attacks like cross-site scripting (XSS) and SQL injection (SQLi). Google Cloud Armor features some automatic protections and some that you need to configure manually.

Google Cloud Armor security policies enable you to allow or deny access to your deployment at the Google Cloud edge, as close as possible to the source of incoming traffic. This prevents unwelcome traffic from consuming resources or entering your Virtual Private Cloud (VPC) networks.

The following diagram illustrates the location of the global external Application Load Balancers, classic Application Load Balancers, the Google network, and Google data centers.



Picture 4: Cloud Armor traffic screening at the network edge

Cloud Armor is integrated at the load balancer level to frontends, as well as with Apigee on the backend layer. Apigee extends Cloud Armor's results that do not immediately block traffic to API & identity specific threats.

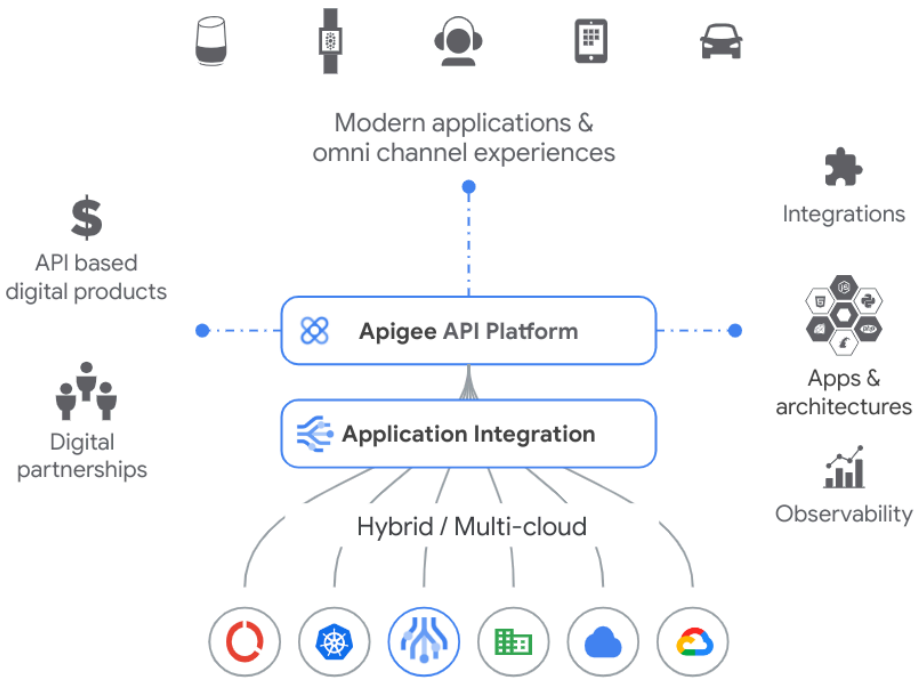
Advantages of using Cloud Armor in the security architecture:

- Benefit from DDoS protection and WAF at Google scale
- Detect and mitigate attacks against your Cloud Load Balancing workloads or VMs
- Adaptive Protection ML-based mechanism to help detect and block Layer 7 DDoS attacks
- Mitigate OWASP Top 10 risks and help protect workloads on-premises or in the cloud
- Bot management to stop fraud at the edge through native integration with reCAPTCHA Enterprise

2.2 What is Apigee?

Apigee helps companies deliver apps, data, and APIs to transform themselves into leaders in the digital world. Hundreds of digital leaders (20% of the Fortune 100, 50% of the world's most valuable retail brands, financial services institutions and banks, 9 of the top 12 telcos, many airlines, insurance providers, etc.) use Apigee to create engaging customer experiences, accelerate app and API development, drive reach and revenue, and optimize apps and APIs with contextual data analytics.

Alignment around the Apigee platform provides users with a powerful architecture for broad-reaching digital product management and an analytical model for data-driven decision making across the business. With Apigee, the platform converges on a single set of standards, an industry-leading force multiplier, and a proven partner in digital transformation use cases across industries.



Picture 5: Apigee & Application Integration overview

2.3 What is Application Integration?

Application Integration is an Integration-Platform-as-a-Service (iPaaS) solution in Google Cloud that offers a comprehensive set of core integration tools to connect and manage the multitude of applications (Google Cloud services and third-party SaaS) and data required to support various business operations.

Application Integration is serverless, auto-scales, and is fully managed by Google. This means that with simple, automated configurations, you can quickly and securely create, maintain, and scale integrations directly on top of Google's scalable infrastructure.

Application Integration helps build the security architecture by enforcing that all connectivity & integration to data & services runs on secure infrastructure & platform components, and minimizes / eliminates the need to add custom code that can introduce security vulnerabilities just to connect and integrate systems & data behind the APIs.

2.4 What is Federated Identity & reCAPTCHA?

Federated identity using Google Cloud Identity Platform & Firebase Auth enables the support of multiple IDPs to authenticate users using industry standard protocols such as SAML, OAuth 2.0, and OIDC. This makes it possible for users to securely bring their own identity, while enforcing consistent and secure pipelines for identity integration & management.

reCAPTCHA Enterprise uses advanced risk analysis techniques to distinguish between humans and bots. With reCAPTCHA Enterprise, websites and apps are protected from spam and abuse, and can detect other types of fraudulent activities on the sites, such as credential stuffing, account takeover (ATO), and automated account creation. reCAPTCHA Enterprise offers enhanced detection with more granular scores, reason codes for risky events, mobile app SDKs, password breach/leak detection, Multi-factor authentication (MFA), and the ability to tune your site-specific model to protect enterprise businesses.

reCAPTCHA works with the IDP to offer additional screening and protection of user processing flows, and identify fraudulent users faster.

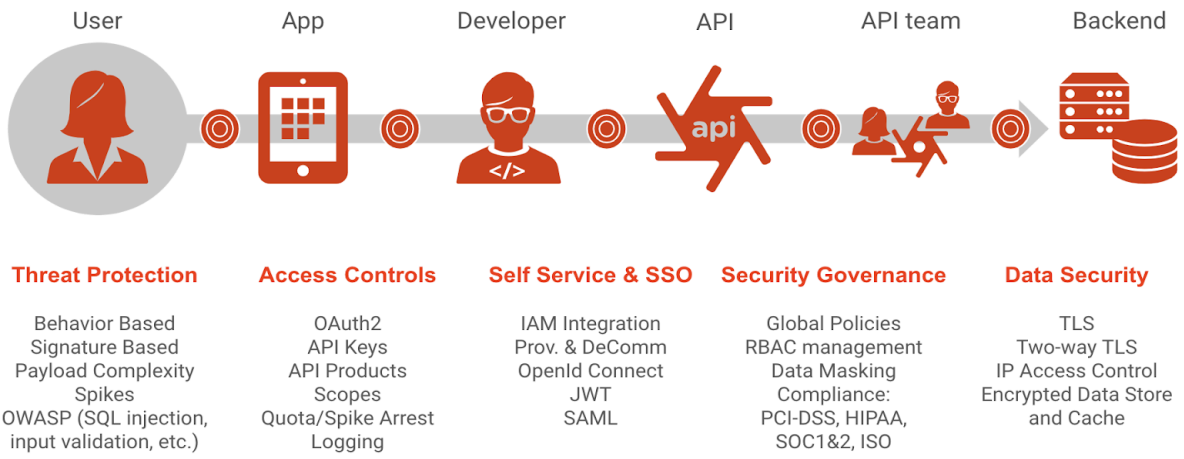
reCAPTCHA and Apigee data are used together to screen, filter & block fraudulent traffic from reaching the backend service & data layer.

2.5 Security requirements

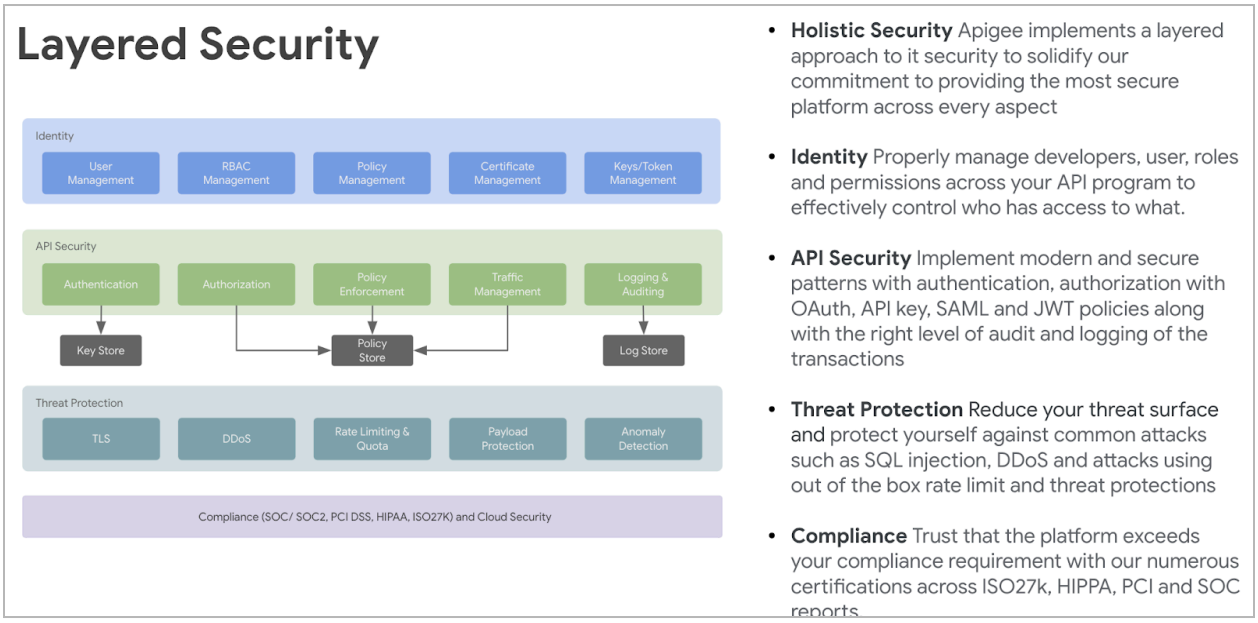
Google's zero-trust security model is an end-to-end process designed to provide security throughout the information processing life cycle. Our best-in-class security infrastructure provides a secure deployment of services, protected storage for business-critical assets, secure communications between services, and a safe and private communication with customers over the internet.

2.5.1 API security

Apigee provides industry-leading security functionality at all points of engagement along the digital value-chain and is easily integrated with existing corporate security standards and systems.



Picture 6: **Security functionalities of Apigee along the digital value chain**

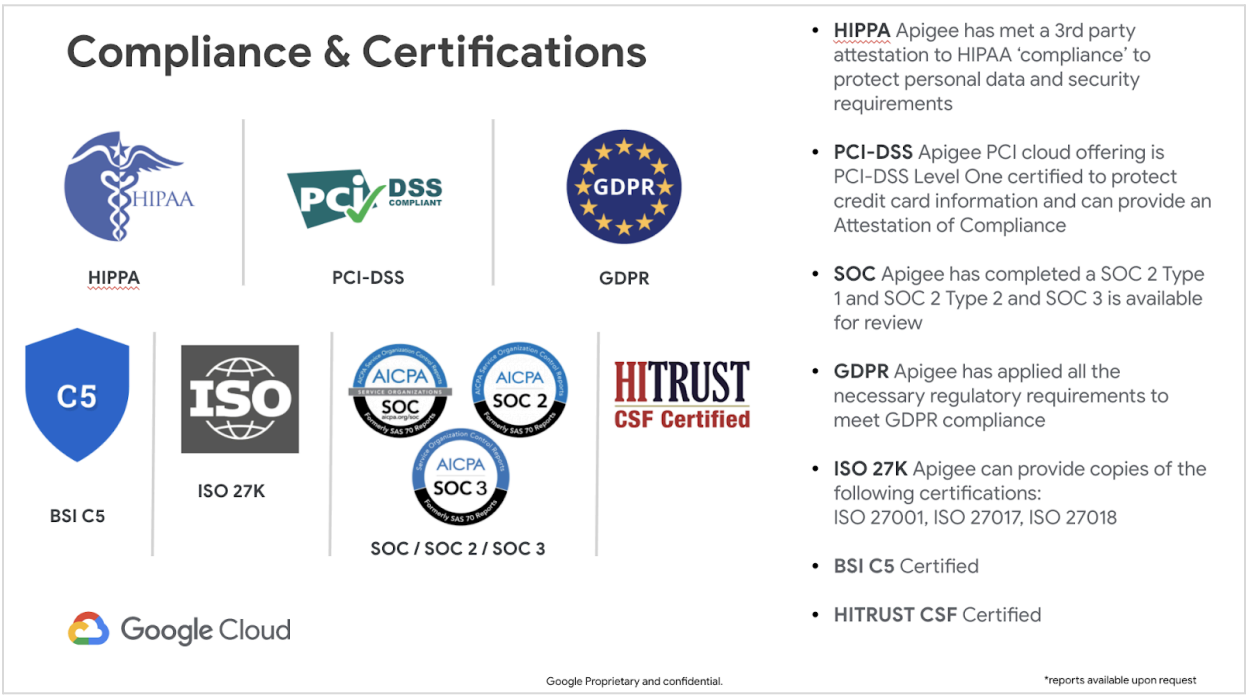


Picture 7: **Layered security**

From an **admin perspective**, Apigee has implemented RBAC to restrict API lifecycle management tasks on the platform, to users with the appropriate privileges based on the roles the user is assigned. Apigee also supports the definition of custom platform user roles.

From a **consumption perspective**, Apigee has OOTB support for API keys, OAuth v1 and v2, SAML, and JWT. We typically encourage the use of three-legged OAuth with authorization code grant type to authenticate the end user and validate that the developer/app with an appropriate API key for accessing the API. We also support the concept of security mediation, where we may be using OAuth on the frontside (app client to Apigee) and some other security mechanism (customer specific or integrated with other security provider, such as Ping, Okta, etc.) on the backside (Apigee to backend service). Apigee also supports the integration to external Identity providers (for example, Okta, Firebase, etc.) for client app user (resource owner) identity validation. At the transport level, Apigee supports Secure Sockets Layer/Transport Layer Security (SSL/TLS) on the inbound request from the app to Apigee and on the outbound request from Apigee to the backend service. The GCP Global HTTPS Load Balancer support for northbound mTLS is currently in private preview and planned for GA later this year. Northbound mTLS can also be done using Envoy and other types of load balancers in the meantime.

In addition, the Apigee platform is industry-certified for **PCI, SOC/SOC2/SOC3, HIPAA, BSI C5, ISO, and GDPR compliance**. These certificates are only applicable to our cloud. So only X applies, or in case of hybrid, only the control plane is taken into account. Please find the listed certificates in the [compliance and certification page](#).



Picture 8: **Compliance & security**

Apigee supports the following API security mechanisms:

- OAuth 2.0 (two-legged and three-legged authentication)
- Support for authentication via OAuth is provided easily by OOTB configurable policies. Apigee could act as an authorization server (generate token, refresh token, and verify, etc.) as well as to credential mediation. Flows supported are - client credentials, authorization code, implicit, and resource owner password flow
- Support for SAML and WS-*

- The management API also facilitates inspection and static analysis of all the assets within an organization. For example, a company may periodically run a governance check to insure that:
  - Cached data is correctly managed
  - Secrets are stored properly and retrieved correctly
  - Naming standards for fields and URL paths are applied correctly
  - APIs adhere the the corporate standards for error message formats
  - Documentation is correctly published and formatted
  - Log messages are being sent to the correct destination
  - TLS certificates are in compliance with corporate requirements: supports SAML 1.1 and 2.0 tokens (sender-vouches and holder-of-key) for identity and authorization policies
- Support for LDAP/Active Directory (AD)
  - Any of the authentication mechanisms can also be enabled to authenticate against an external LDAP user store or any user store exposed over a web service
- Support for API keys
  - Apigee offers API key management OOTB and supports any existing external API key management systems
- Support for TLS/SSL
  - Apigee supports SSL/TLS at the Transport Layer from the client app to Apigee and from Apigee to the backend service. We support both mutual SSL/TLS and one-way SSL/TLS by using the TrustStore and KeyStore to identify the SSL/TLS participants
- Support for token-based authentication include:
  - HTTP basic authentication token
  - Bearer (for example, OAuth, OpenID Connect)
  - SAML
  - X509 token
  - SAML token
  - Any custom token
- Support for other mechanisms, including:
  - WSSE X509 signature (certificate)-based authentication
  - File-based authentication
  - XML decryption/encryption and verification
  - IP-based authorization
  - Credential mediation between tokens (for example, SAML-to-OAuth)
  - Flexible pluggable framework for integration with other authentication mechanisms

- Apart from the support to the standard authentication standards, Apigee supports custom algorithms by making web service callouts to external and internal systems

More information can be found for Identity providers and options for configuring TLS.

2.5.2 Threat protection

Apigee supports policies on XML threat protection, JSON threat protection, and regular expression threat protection. The XML threat protection policy addresses the XML vulnerabilities and minimizes attacks by detecting XML payload attacks based on the configured limits. The same applies to the JSON threat protection policy.

The regular expression policy allows the API publisher team to scan inbound URLs, headers, or payloads for content that matches a particular regular expression.

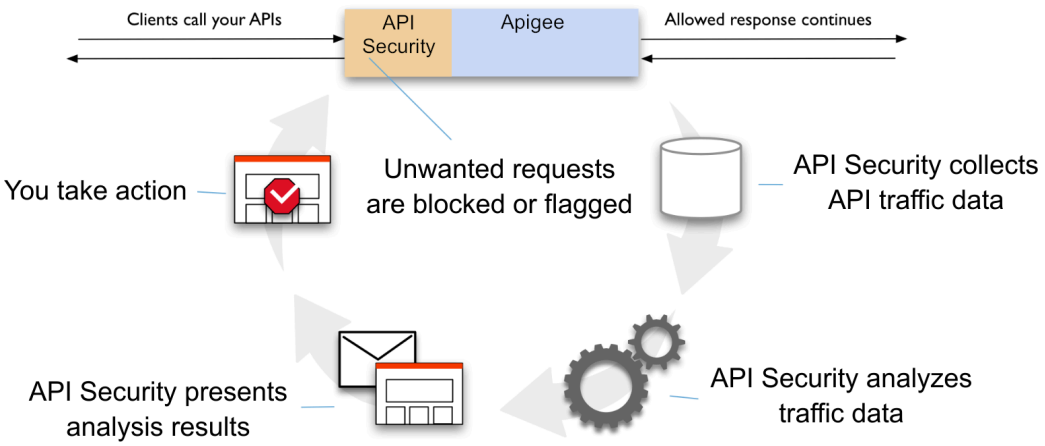
Apigee supports multiple different protections in a single API proxy. Once a threat is detected, the API proxy can reject the call with a 400 Error or can invoke an external webhook to log the detection or any configurable action.

Additional information can be found in the JSON threat protection policy.

2.5.3 Bot detection

Apigee X & Hybrid leverage Apigee Advanced API Security and Cloud Armor that analyzes multiple factors, including time and frequency, payload content, and IP origin to detect bot threats.

Apigee API Security uses adaptive algorithms that are tuned with data from across multiple datasets. As a result, it is able to distinguish legitimate traffic more effectively than would be possible from a single source of data. Adaptive algorithms automate the identification and tracking process. As a result, you only need to decide how to deal with suspicious traffic from an IP address.



Picture 9: **Apigee API Security: functional components**

Apigee API Security is made up of four components:

- A **collection engine,** which collects a large number of relevant signals as traffic passes through Apigee Edge. Apigee Sense collects typical metadata about the source and target for the API call, as well as the metadata relating to both request content and response status. It also collects timing and latency information
- The **analysis engine,** which assembles all the collected data into a summary data structure. Apigee Sense does a deeper analysis on this structure, examining how each request source behaves. Apigee Sense then makes judgments on whether the source has a suspicious signature
- Through the **curation engine**, Apigee Sense presents analysis results to the users. With these results, you can specify the action to take for each identified suspicious client
- Finally, there is an **action engine,** which identifies the requests as originating from suspicious clients in real time and takes the appropriate action required on such traffic

Cloud Armor puts additional security on top for cloud environments by providing the following features:

- **Pre-defined Web Application Firewall (WAF) rules to mitigate the OWASP Top 10 risks:** OOTB rules based on industry standards to mitigate against common web application vulnerabilities and help provide protection from the OWASP Top 10
- **Bot management:** Provide automated protection for your applications from bots and help stop fraud inline and at the edge through native integration with reCAPTCHA enterprise
- **Rich rules language for WAF:** Create custom rules using any combination of L3–L7 parameters and geolocation to help protect your deployment with a flexible rules language
- **Visibility and monitoring:** Easily monitor all the metrics associated with your security policies in the Cloud Monitoring dashboard. You can also view suspicious application traffic patterns from Cloud Armor directly in the Security Command Center (SCC) dashboard
- **Logging:** Get visibility into Cloud Armor decisions as well as the implicated policies and rules on a per request basis via Cloud Logging
- **Preview mode:** Deploy Cloud Armor rules in preview mode to understand rule efficacy and the impact on production traffic before enabling active enforcement
- **Policy framework with rules:** Configure one or more security policies with a hierarchy of rules. Apply a policy at varying levels of granularity to one or many workloads
- **IP and geo-based access control:** Filter your incoming traffic based on IPv4 and IPv6 addresses or Classless Inter-Domain Routing (CIDRs). Identify and enforce access control based on the geographic location of incoming traffic
- **Support for hybrid and multi-cloud deployments:** Help defend applications from DDoS or web attacks and enforce Layer 7 security policies whether your application is deployed on Google Cloud or in a hybrid or multi-cloud architecture
- **Named IP lists:** Allow or deny traffic through a Cloud Armor security policy based on a curated Named IP list

2.5.4 Shared policy enforcement

Apigee provides a capability known as 'shared flows', which allows configuration and packaging of reusable functionality that can then be applied to all of the APIs within an organization. By capturing this functionality in a central place, a shared flow helps ensure consistency, shorten development time, and manage code more easily. This can be useful to enforce standards within an Apigee organization for common functionality like centralized security validation, logging requests to the corporate standard logging service, or for any other reason. From a governance perspective, this means the central team responsible for enforcing these standards and best practices, can implement their controls once and be assured that any APIs exposed through Apigee will be bound by those controls.

- Multiple shared policies can be defined
- Multiple shared policies can be used in an API proxy
- Usage of desired policies in API proxies can be verified and centrally enforced
- API providers cannot modify or remove enforced policies

2.5.5 Vulnerability documentation and processes

Google's vulnerability management program and vulnerability priority guidelines define how to track vulnerabilities, including identification and remediation updates with the responsible teams.

We believe that vulnerability disclosure is a two-way street. Both vendors and researchers must act responsibly. This is why Google adheres to a 90-day disclosure deadline. We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix.

This page outlines how Google handles security vulnerabilities.

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than many traditional on-prem solutions. Although we make security a priority to protect our own operations, but because Google runs on the same infrastructure that we make available to our customers, your organization can directly benefit from these protections. That is why we focus on security; and the protection of data is among our primary design criteria. Security drives our organizational structure, training priorities, and hiring processes. It shapes our data centers and the technology they house. It is central to our everyday operations and disaster planning, including how we address threats. It is prioritized in the way we handle customer data, and is the cornerstone of our account controls, our compliance audits, and the certifications we offer to our customers.

Google's approach to security and compliance for Google Cloud outlines our suite of public cloud products and services. This whitepaper focuses on security, including details on organizational and technical controls.

Customers will be informed about vulnerabilities within Mandatory Service Announcements (MSA). An MSA is a communication that is necessary to the continued use of a product or service, or that is considered an essential legal update. An MSA falls within one of the following three categories:

- **Legal:** Terms of Service (ToS) changes, privacy changes, etc.
- **Security:** Major security communications are sent in bulk, such as notifications informing customers about a security breach.
- **Product:** Communications about changes that will break—not just improve—usage of a product. The break would happen even without the user logging in.

2.5.6 Dealing with vulnerabilities

Google monitors various well known public channels for vulnerability disclosures. Google security team's security incident response process ensures that such reports are tracked, investigated, and followed up upon. We also provide libraries that prevent developers from introducing certain classes of security bugs. For example, we have libraries and frameworks that eliminate Cross-site Scripting (XSS) vulnerabilities in web applications. We also have automated tools for automatically detecting security bugs, including fuzzers, static analysis tools, and web security scanners.

As a final check, we use manual security reviews that range from quick triages for less risky features to in-depth design and implementation reviews for the most risky ones. These reviews are conducted by a team that includes experts

across web security, cryptography, and operating system security. The reviews can also result in new security library features and new fuzzers that can then be applied to other future products.

In addition, we run a Vulnerability Rewards Program, where we pay anyone who is able to discover and inform us of bugs in our infrastructure or applications. We have paid several million dollars as rewards in this program.

Google also invests a large amount of effort in finding zero-day exploits and other security issues in all the open-source software that we use, as well as upstreaming these issues. For example, the OpenSSL Heartbleed bug was found at Google and we are the largest submitter of Common Vulnerabilities and Exposures (CVEs) and security bug fixes for the Linux Key Value Map (KVM) hypervisor.

Based on the severity of the vulnerabilities, Google attaches an internal priority code to it. This defines if all other work should be stopped immediately or if there is time to fix that issue within the next year. Within customer communication, this severity is communicated. The time taken to fix an issue depends on the incident itself.

2.5.8 Security documentation

Google is a pioneer in the area of security. We take care of all necessary steps to ensure a secure and reliable environment. This includes internal systems and processes as well as externally provided product documentation, best practices, and security guidelines. The security features and functions of the solution as well as its security architecture is available and continuously maintained. You can find relevant documentation on our websites:

- Design fundamentals
- Infrastructure security design
- Security whitepaper
- OWASP Top 10 mitigations

2.5.9 Authentication and role/group-based authorization management

OIDC is a supported authentication mechanism for the administrative users and API developers in Google Cloud and Apigee X (SaaS & hybrid), but not currently for the private cloud Apigee OPDK version. All three are able to use OIDC within the context of API traffic.

Apigee supports SAML authentication with the identity provider of your choice. By using SAML with Apigee, you can support Single Sign-On (SSO) for the Apigee UI. When users leave your organization and are deprovisioned centrally, they are automatically denied access to Apigee.

- Control how users authenticate to access Apigee: Select different roles and access levels for your Apigee organizations and environments
- Control authentication policies: Your SAML provider may support authentication policies that are more in line with your enterprise standards to control access to Apigee

- Full control: Apply governance to your API program and maintain control of which organizations and environments developers have access
- Built-in roles: Leverage one of the six built-in roles that are provided to you for the common user access scenarios, such as read-only, monitoring/support, business personnel, and more
- Custom roles: Create access to individual developers by defining custom roles and assigning permissions
- API permissions: Roles not only apply to the Apigee UI but also to any of the management APIs your developers may be consuming

More information on IDP (for example with Azure AD) federation available here.

2.5.10 Strong authentication

The Apigee management and developer portal supports Universal 2nd Factor (U2F)/Two-Factor Authentications (TFA) with SAML or OpenID Connect (OIDC).

2.5.11 Cryptography regulations/Encrypted storage of sensitive data

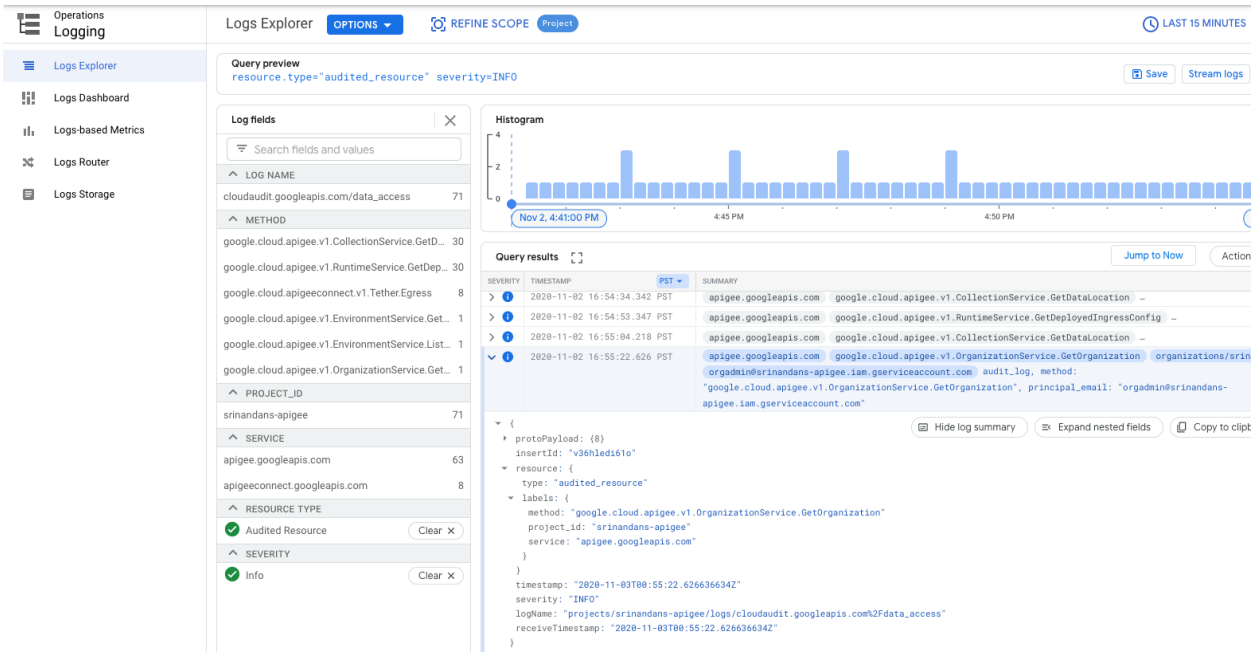
Google supports the following procedures and technology:

- The customer can be the owner of their own encryption keys (CMEK). In Apigee X, the customer can use the Google KMS service, see documentation here. For Apigee hybrid and OPDK the customer can define the encryption keys.
- Google employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit. We plan to remain the industry leader of encryption in transit. To this end, we dedicate resources toward the development and improvement of encryption technology. Our work in this area includes innovations in key transparency and post-quantum cryptography
- Google Cloud encrypts all customer content stored at rest without any action required from the customer, using one or more encryption mechanisms
- Data for storage is split into chunks and each chunk is encrypted with a unique Data Encryption Key (DEK). DEKs are stored with the data, encrypted with (or 'wrapped' by) Key Encryption Keys (KEKs) that are exclusively stored and used inside Google's central KMS, which is redundant and globally distributed
- The steps in this document explain how to enable the KEK feature, which allows Apigee to encrypt the secret keys used to encrypt developer application consumer secrets when they are stored at rest in the Cassandra database
- All data stored in Google Cloud is encrypted at the storage level using AES256, with the exception of a small number of Persistent Disks (PDs) created before 2015 that use AES128
- Google uses a common cryptographic library, Tink, which incorporates our Federal Information Processing Standards (FIPS) 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. Consistent use of a common library means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code

- Apigee Hybrid and private cloud includes a secure store for storing secrets that can be used at runtime by the API proxies

2.5.12 Audit logging

Apigee X and Hybrid provides an audit feature that is helpful in tracking changes, troubleshooting problems, as well as security incidents.



Picture 10: **Example audit logs**

2.6 Development standards

The Apigee solution supports and adheres to the industry's best practices. The different components of Apigee can be deployed on several cloud platforms as well as on-prem to avoid vendor lock-in. The API definitions used will be based on open standards (for example, OpenAPI).

2.6.1 API gateway/runtime

Apigee runtime processes requests and responses to and from backend services securely, including transformations and traffic distribution, provides traffic management, and asynchronously pushes valuable API execution data to Apigee for consumption by the Apigee analytics system.

- Convert messages between formats, such as from XML to JSON
- Set variable values from message content and create messages from variable values

- Use procedural code, such as JavaScript, Java, and Python, to handle messages and data in more complex ways
- Guarding against malicious message content, accessing and masking sensitive encrypted data at runtime, protecting your backend services against direct access, and other important safeguards

Apigee Hybrid supports two kinds of updates. The first is an in-place update where you apply a configuration change and hybrid begins a Kubernetes rolling update. In Kubernetes, rolling updates allow deployment updates to take place with zero downtime by incrementally updating pod instances with new ones.

Apigee Hybrid also supports a canary or AB-style update. In an AB update, the new revision is deployed, however, at first a small percentage of traffic is directed to it. Over time, this percentage increases until all of the traffic goes to the revision. For more information, please visit the Apigee page.

2.6.2 Optional third-party developer portals/portal integration layers

Apigee can integrate external portal solutions via API (for example, Drupal and Liferay) to build custom developer portals.

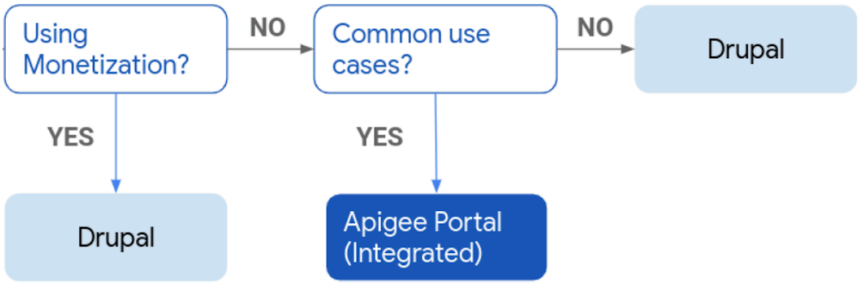
Apigee supports several developer portal solutions, as summarized in the following table, ranging from simple turn-key to fully customizable and extensible. When choosing a solution, you need to balance your customization requirements against the time and knowledge required to implement your portal.

The following solutions are available:

Apigee solution	Features	Hosted by Apigee?	Support (Requires licensed subscription)
Apigee integrated portal	Simple self-service portal development.	Yes	Apigee 24/7 support
Drupal 9 modules	Fully customizable option, based on a powerful, open source CMS integrated with Apigee using modules.	No	Apigee 24/7 support for break-fix issues
Do-it-yourself (DIY)	Fully customizable portal development using Apigee APIs.	No	Apigee 24/7 support for Apigee APIs only

Choose your developer portal solution

To help you decide which developer portal solution to choose, consider the following decision tree and review the Comparison of developer portal features.



Consider building an Apigee integrated portal if you plan to support common use cases for portal development, such as standard registration and app creation flows, and more stylistic than functional changes.

Picture 11: Developer portal solutions

2.7 Integration requirements

Apigee will be integrated into the IAM system of the customer. The Apigee integration extends the Apigee API management platform to include core integration features. These consist of connectors, an integration engine, and data transformation tools. Apigee integration offers business organizations of all sizes the tools needed to connect and manage the multitude of software applications required to support business operations in a digital world.

2.7.1 Integration of organization data

Custom properties are supported at multiple levels in Apigee, from API products to applications and alerts based on faults raised by proxies. This especially includes the documentation and reference of organization data, with regard to:

- API products

- API proxies
- Alerts generated by the platform
- Attributes in organizational master data
- Custom attributes in client applications that subscribe to API products
- Custom attributes evaluated at runtime

2.7.2 Integration of IAM (roles and rights)

Apigee can be integrated into the IAM and will allow the integration of user data and roles via SAML/OIDC federation.

When enabling the integration via SAML or federation, the already existing roles or users can be mapped to roles or users in Apigee. Additionally, the sync of roles is supported from an already existing LDAP server.

2.7.3 Disabling functionalities

Some components of Apigee can be disabled if not needed or wanted. Additionally, with the IAM deny policies, you can define deny rules that prevent certain principals from using certain permissions, regardless of the roles that they are granted. This policy could be used in order to manage restrictions on features or packages. See complete documentation for Apigee permissions here.

2.7.4 Transparent integration of third-party API gateways

Apigee supports the integration of third-party API gateways by leveraging the following features:

- Apigee can do API calls to third-party services and backends
- Services behind third-party API gateways can be exposed via API proxy
- Apigee supports the following mechanisms for authenticating API calls:
  - OAuth 2.0 (two-legged and three-legged authentication)
  - Apigee can do this with large numbers of tokens, clients, and at very high concurrency
  - Whether using two or three-legged flows, Apigee can alternatively delegate authentication of the client (the application) to a third-party system, such as Ping or Okta
  - SAML and WS-*: Apigee supports SAML 1.1 and 2.0 tokens (sender vouches and holder-of-key) for identity and authorization policies
- Support for AD/Okta/Auth0, etc.: Any of the authentication mechanisms can also be enabled to authenticate against any user store exposed over a web service
- API key: Apigee includes API key management OOTB and supports any existing external API key management systems
- Proxy chaining
  - Enables the user to easily chain multiple proxies without incurring network costs

    - Might be desirable in order to support separation of organizations in the server or to reuse specific proxy functionality on the server across multiple endpoints
- Transformation of authentication information is supported: Using a ServiceCallout to obtain authorization information is a very common pattern among Apigee customers

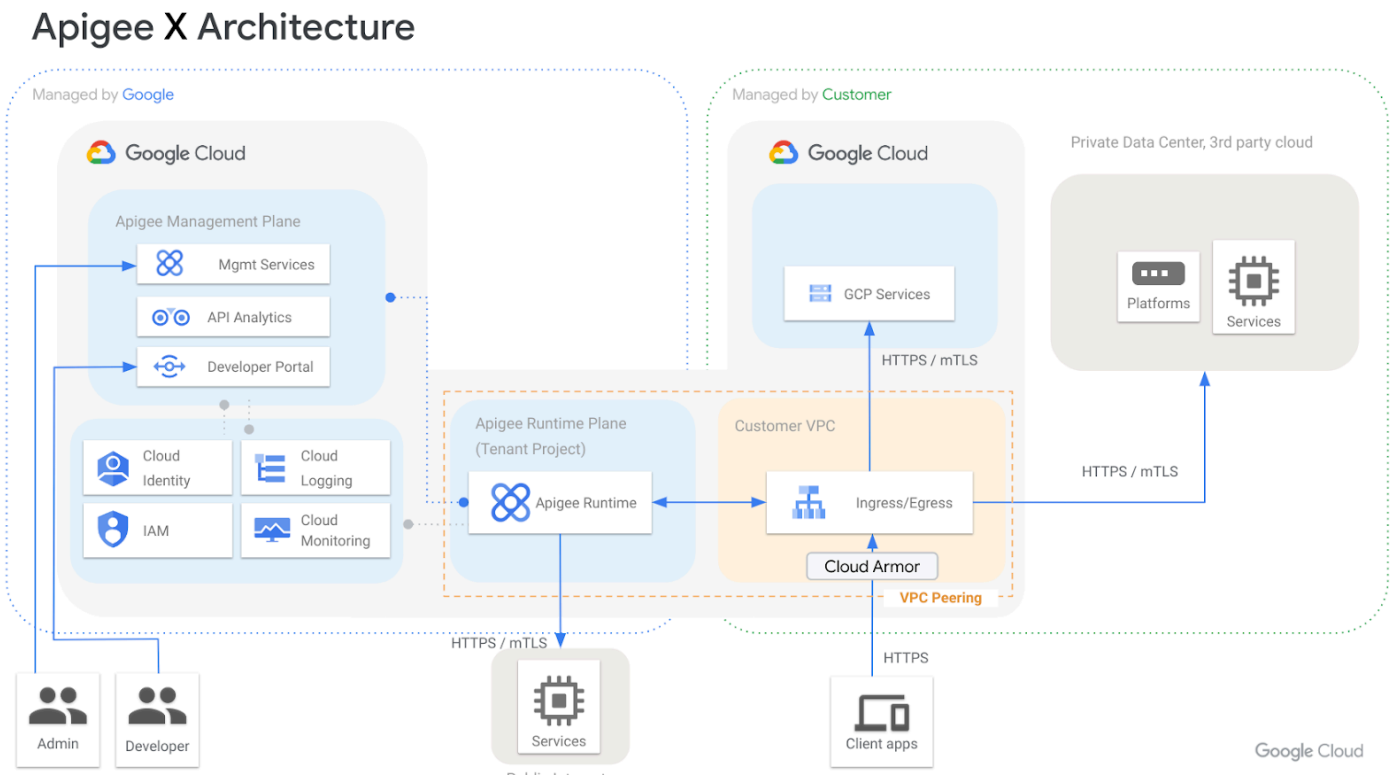
2.7.5 Deployment overview

Apigee X, a hosted SaaS version in which Apigee maintains the environment. Apigee SaaS is available in the public cloud in most Google Cloud regions and AZs.

Apigee X consists of the following components:

- **Apigee services:** The APIs that you use to create, manage, and deploy your API proxies
- **Apigee runtime:** A set of containerized runtime services in a Kubernetes cluster that Google maintains. All API traffic passes through and is processed by these services
- **GCP services:** Provides identity management, logging, analytics, metrics, and project management functions
- **Backend services:** Used by your applications to provide runtime access to data for your API proxies

The following picture shows an example deployment in a Google region:



Picture 12: Apigee X deployment example for one region

2.8.2 Incident management

The initial priority of a service case is set by the customer and are described as followed

	Description
P0	Impact is critical and the service is down or unusable, only applies for production and Mission Critical Services (MCS) defined upfront
P1	Impact is critical and the service is down or unusable, only applies for production
P2	Impact is high and the service is severely impaired, that is, performance is degraded or service is available but is producing errors
P3	Impact is medium and the service is partially degraded, that is, the service is generating error messages but without any end user impact This priority can be also used for questions about features used in customer launch
P4	Impact is low and the service is still usable, that is, minor things like documentation issues or feature requests

In case of incident tickets, the following target initial response times are in place for Premium Support based on the ticket priority:

	Response Time	Resolution time
P0	5min (Premium support w/ MCS only)	*
P1	15min	*
P2	2 hours	*
P3	4 hours	*
P4	8 hours	*

*: Our SaaS components guarantee an availability of 99,99%. This equals a maximal downtime of 53 minutes per year and is used as our internal goal to fully restore services.

During the ticket handling process, it might be necessary to change the priority (up or down) due to new findings. For example, a P1 case might be prioritized down to P2, after the initial damage is fixed and the systems are running again, but a post-mortem document needs to be provided. Resolution times will shift with these adaptations based on the actual situation for the customer.

2.8.3 Problem management

In case of not resolving incidents directly, workarounds need to be implemented and followed up.Our SaaS components guarantee an availability of 99,99%. This equals a maximal downtime of 53 minutes per year and is used as our internal goal to fully restore services.

Operational Health Reviews

Operational Health Reviews help you measure your progress and proactively address blockers to your goals with Google Cloud. The reviews serve as a regular touchpoint with your TAM where you can discuss various topics related to your Customer Care experience, including:

- The efficiency of your cloud operations, including support trends.
- Analysis of trends in operational metrics.
- Incidents, case escalations, and outages.
- Tracking of open cases.
- Status reports for high-priority Cloud projects.

Event Management Service

You can use Premium Support's Event Management Service for planned peak events, such as a product launch or major sales event. With this service, Customer Care partners with your team to create a plan and provide guidance throughout the event.

With Event Management Service, your team is supported with the following tasks:

- Preparing your systems for key moments and heavy workloads.

- Running disaster tests to proactively resolve potential issues.
- Developing and implementing a faster path to resolution to reduce the impact of any issues that might occur.

After the event, your TAM works with you to review the outcomes and make recommendations for future events.

To initiate the Event Management Service for an upcoming event, contact your TAM.

2.8.4 Escalation process

If your support case has the appropriate priority, you can escalate it if the support effort or the provided solution is not meeting expectations.

When a support case is escalated, escalation is immediately assigned to a Customer Care Manager and notifies you within an hour. The Customer Care Manager owns the escalation until escalation closure. They would identify and address the escalation root cause, and report preventative actions to avoid similar escalations in the future.

The following examples demonstrate possible reasons for escalating a case:

- Customer Care misses time commitments.
- Customer Care misunderstands the impact or the nature of the issue and would not comprehend even after you have made several attempts to clarify the impact or nature of the issue.
- The case might require additional expertise to resolve the issue.
- You think that the provided solution is completely off based on the nature of the problem and Customer Care would not provide convincing explanation that would be sufficient to prove solution validity, even after you request for an explanation.
- Your case is stuck because you and Customer Care are not in sync, despite communicating several times with each other, and your case requires additional resources to analyze the issue and determine the next steps.

When requesting an escalation, quote the case number and provide a reason for the escalation. You can make the request in the following ways:

- Comment in the case.
- Click the Escalate case button which appears 30 minutes after creating the case.
- Contact Customer Care.

If you have a Premium Support offering, you can also request an escalation by contacting your Technical Account Manager.

2.9 Governance/Reporting

2.9.1 Reports

Incident and problem management report

The monthly Operational Health Report (OHR) contains a list of all open cases, including the planned and necessary action items on the customer's and/or Google's side.

Post-mortem report

A post-mortem report describes a production outage, paging event, or any event with an external negative impact, including (at minimum): a timeline, description of the user impact, root cause, and action items or lessons learned. This report will be provided after critical outages to the user..

API management platform utilization report

Apigee analytics offers various charts and metrics to analyze the API utilization, for example, the number of calls, the slowest and fastest API, or the revenue generated. More information can be found within 2.5.5.

API transaction report

The operational metrics of Apigee analytics allow to view and analyze the transaction percentiles for the systems as a whole or an individual API proxy. The data is presented via a UI. More information can be found within chapter 2.5.5.

API management availability report

The availability report is available here. This page provides status information on the services that are part of Google Cloud as well as the history of incidents up to 365 days.

2.9.2 Reviews

Google will provide periodic reviews for the customer. These reviews will be announced by the customer at least 14 days upfront.

Service review (monthly)

Google will provide the OHR on a monthly basis, which provides a view on the costs as well as tickets per month.

Transaction + invoicing review/billing review (quarterly)

Google will support issues or missing transparency according to invoices. In addition, Google will execute cost optimization workshops to check for potential optimizations and provide best practices and recommendations.

Installation/Change management review

From time to time, a review of the installation or necessary changes might be required. Google will support the customer in this review based on the demand. It is assumed that these reviews will not happen more than twice a year.

Management review

On a quarterly basis, Google will provide a Quarterly Business Review (QBR) to review the last quarter's performance as well as strategic planning for the quarter ahead with the management. The aim is to have a management discussion, aligning with the long-term goals established by the customer around the past performance and new strategic or tactical targets.

Security review

Google will support security reviews on an on-demand basis triggered by potential security incidents or severe vulnerabilities affecting the Apigee environment. To provide the necessary support and technical or organizational detail, the reviews will be aligned based on the actual situation.

Audits

Google will support audits on an on-demand basis. To provide the necessary support and technical or organizational detail, the audits will be aligned upfront.

03. Miscellaneous

3.1 Certificates

Google undergoes several, independent, third-party audits on a regular basis to provide assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure, and operations. If the customer requires one/more of these certificates, we need a written request with a contact person and email address - a personalized report will be shared with that contact person within 48 hours. Google has annual audits for the following standards:

- BSI C5
- ISAE 3402
  - SOC 1
  - SOC 2
  - SOC 3
- VDA-ISA TISAX
- EU DSGVO
- Bank/Payment
  - PCI DSS
  - BaFin
- ISO
  - Norm 27001
  - Norm 9001
  - Norm 22301
  - Norm 20000: Please see following information

Additional information on ISO norm 20000:

Please note that Google services are designed and operated substantially to address the objectives defined in the ISO 20000 Standard.

The ISO developed the ISO 20000 Standard, which establishes international requirements for service management. This framework aims to enhance the service value provided to consumers through the establishment of a service quality

management standard. Specifically, ISO 20000 provides guidance on the planning, design, transition, delivery, and improvement of services to bring value to customers and users.

Google is committed to providing quality service to our customers and maintains industry-leading processes and standards that meet compliance frameworks across industries and product areas. The design and operation of the Google services and various compliance frameworks which Google adheres to help address the service management objectives set forth in the ISO 20000 Standard:

- **Leadership and commitment:** Google Cloud has qualified leaders that support the development and delivery of Google Cloud products and services
- **Third-party certifications and compliance:** Google Cloud provides a number of third-party certifications, detailed in the compliance resource center. In addition, our compliance reports manager can be used to obtain a variety of Google's third-party certifications and reports
- **Information security:** As a cloud pioneer, Google fully understands the security implications of the cloud model. Google Cloud protects customer's data, applications, infrastructure, and customers from fraudulent activity, spam, and abuse with the same infrastructure and security services that Google uses. For more information about Google Cloud's information security management, please see the Google security whitepaper
- **Technical support services:** Google offers a variety of ways to get support, including basic billing support at no charge, paid packages, and developer communities. For more information, please see our support hub and the technical support guidelines for our Cloud products (GCP and Google Workspace)
- **SLAs and monitoring:** Google maintains SLAs for its cloud products (GCP and Google Workspace). In addition, status dashboards are also available for GCP and Google Workspace
- **Announcements, news, and communications:** Google maintains a variety of communication channels to keep our customers informed about updates and changes to our cloud products. Please follow the Google Cloud blog, release notes, and Next conference to find out about the latest news and improvements to Google Cloud

Google Cloud maintains industry-leading security, third-party audits and certifications, documentation, and legal commitments to support our customer's compliance obligations. Although our service delivery management systems are not designed around the ISO 20000 standard, our services are designed and operate in a way that significantly addresses the objectives defined in the standard. Please visit our compliance resource center for the full list of standards and regulations that Google complies with.