

Apigee SaaS vs Apigee Hybrid

Choosing the right Apigee platform for your business

By Brajesh De

Sr. Director, API Management & Integration, Blue Altair

Overview

Apigee is one of the most mature and featured API Management platforms on the market. It has ranked consecutively for several years in Gartner's leaders' quadrant for being the leading API Management platform. So, there is no doubt that Apigee reigns supreme and is the favorite choice of customers looking for an API management solution. Apigee also offers multiple product variations to help meet the needs of customers at varying stages of their API journey. So it's not surprising that with two top performing product offerings like Apigee SaaS and Apigee Hybrid, clients often ask which of Apigee's products are the best fit for their organization.

A Look Back at Apigee

To answer this question let's first take a look into the history and evolution of the Apigee API Management platform offerings. 'Apigee Edge' was the first product launched by Apigee. It provided a complete SaaS offering of the API Management platform and was completely hosted and managed earlier on AWS and then later on Google Cloud (after Apigee was acquired by Google). However, many clients wanted complete flexibility to control the API traffic and also needed to keep API analytics data within their premises for regulatory and compliance requirements. Apigee OPDK (On Premises Deployment Kit) was the solution to address the needs of such customers. With the OPDK setup, clients would completely host and manage the Apigee instances within their network. While OPDK provided the flexibility to control the deployments of the platform and the APIs, it also came with the additional overhead of installation costs and a relatively complex setup of Apigee components.

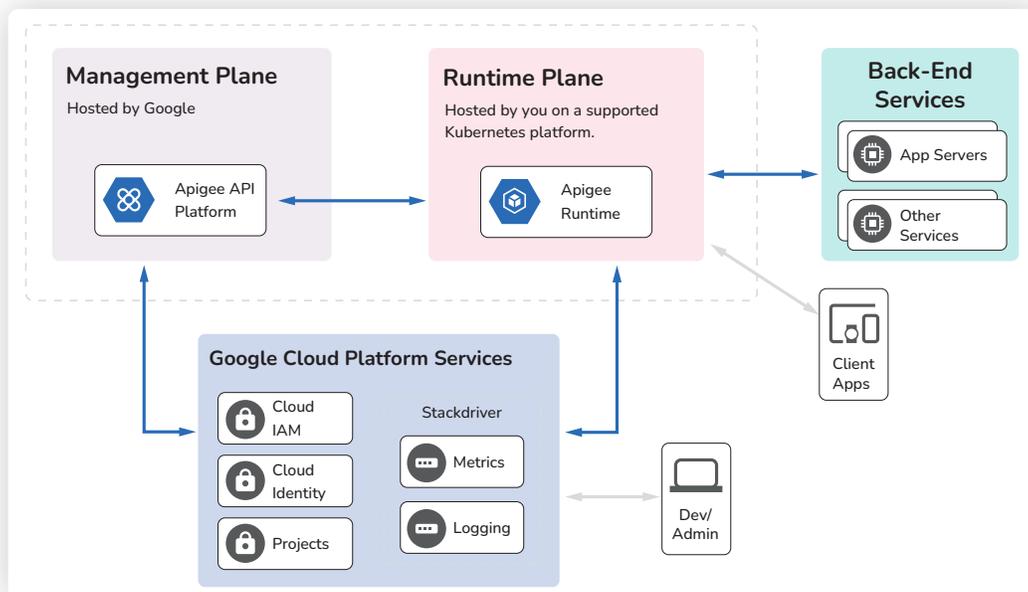
Later in February of 2021, Google launched Apigee X as a complete SaaS offering of their next-generation API management platform. This enhanced SaaS offering of Apigee provided customers with the flexibility to choose their deployment location for the runtime instances across twenty-four Google cloud regions. Customers could thus deploy APIs on Google Cloud in a runtime instance location of their choice and business needs. With caching services across more than one hundred edge locations and improved security using Google's Cloud Armor, its IAM platform along with its AI/ML based anomaly detection capability, Apigee X was an enhanced and transformed version of Apigee Edge with highly improved security posture. However, while Apigee X now provided API management capabilities as a SaaS platform, it still lacked the complete flexibility that some clients needed to setup of the runtime components in a location of their choice.

To meet the growing demand for location flexibility, Apigee Hybrid was launched as an additional entitlement of Apigee. With Apigee Hybrid, the management plane is hosted and maintained by Google, while the customer owns the responsibility of installing and managing the runtime components either on premises or in a supported cloud of their choice. With Apigee runtime instances deployed geographically close to the backend services, it reduced the overall round-trip latency of the APIs and also allowed clients to meet regulatory compliance requirements for data residency. Apigee Hybrid reduced some of the management overheads, but its installation and management of the runtime components is non-trivial.

Exploring the Architecture of Apigee

Now that we have covered the evolution of Apigee and differentiated between the various API management platforms available through Apigee, let's take a closer look at the architecture of Apigee.

Understanding the architecture for each of Apigee's platforms is key when making the right choice between Apigee's SaaS and Hybrid offering for your organization. Apigee as a product has two main logical components – the management plane and the runtime plane.



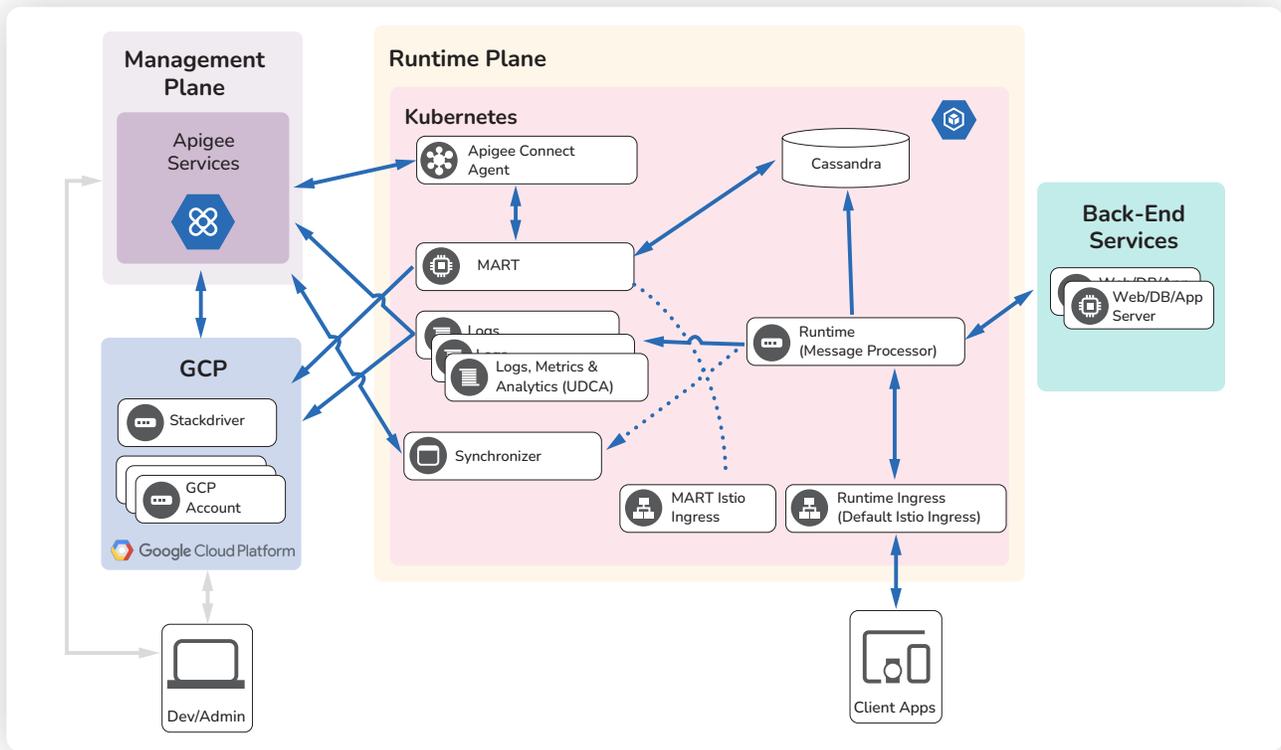
The management plane controls the Role Based Access Control (RBAC) using Google Cloud Platform Cloud Identity Services and consists of the following components:

- **Apigee UI:** Provides the UI console for Apigee configuration and management
- **Management APIs:** Provides a set of management APIs to control and configure Apigee components
- **API Analytics:** Provides analytics information for API traffic

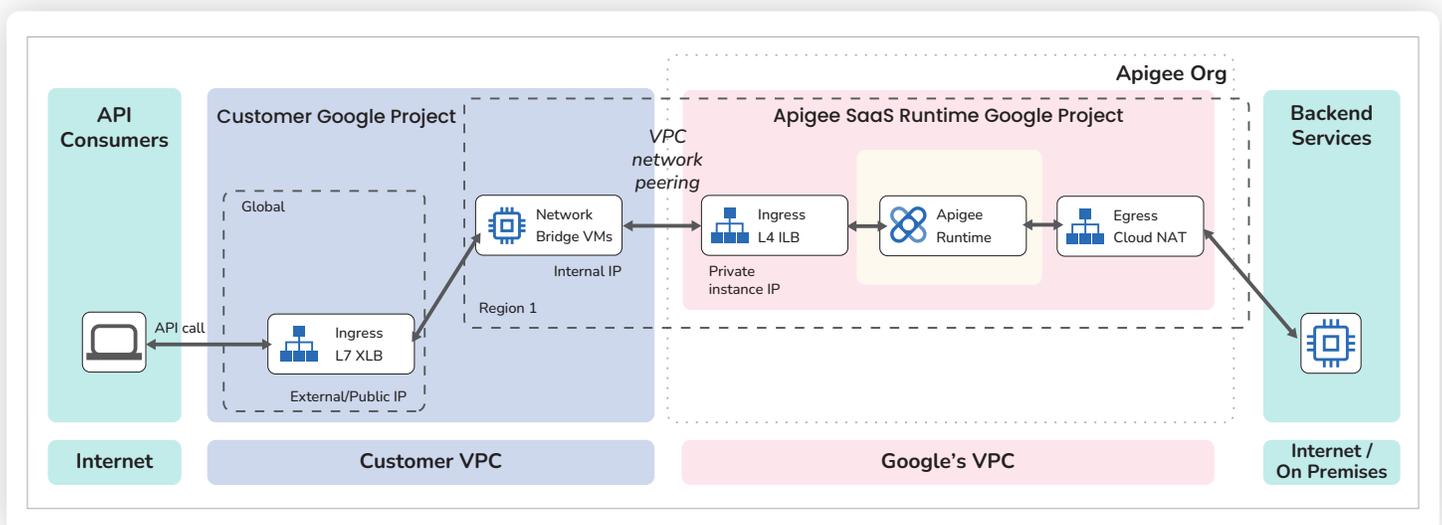
The runtime plane provides the enterprise API gateway capabilities to secure, route, and manage API traffic. It consists of the following components that are deployed on a Kubernetes platform:

- **Message Processor:** Provides API Message processing and policy execution capabilities
- **Synchronizer:** Fetches configuration data about an API environment from the management plane and propagates it across the runtime plane
- **Cassandra Datastore:** Provides data persistence for the runtime plane and is deployed as a StatefulSet node-pool on the Kubernetes cluster
- **Management API for Runtime Data (MART):** Provides APIs to access runtime data stored in Cassandra viz. App configuration, KMS, Cache, KVMs, API Products, Developer Apps
- **Universal Data Collector Agent (UDCA):** Functions as a service running within the data collection pod in the Runtime plane that extracts analytics, debug, and deployment status data and sends it to the Unified Analytics Platform (UAP)

In an Apigee Hybrid setup, all the runtime components are installed and managed by the customer on a supported Kubernetes platform of their choice – either on-premises or on a cloud. The management plane components are set up and managed by Google Apigee on Google Cloud.



In an Apigee SaaS setup, all components are hosted and managed by Google Apigee. The customer controls the API traffic through a customer Virtual Private Cloud (VPC) that is setup within the customer's Google Cloud Platform project and peered with Google VPC that hosts all the runtime components of Apigee. The traffic is routed from the client through an external Load Balancer in the customer's VPC, to the Google VPC via a Managed Instance Group (MIG) as shown below:



Key Drivers When Choosing Apigee

Having this basic architectural understanding, lets look at the main business and technical drivers driving the selection between SaaS and Hybrid offering of Apigee.

Business Drivers

Features	Apigee SaaS	Apigee Hybrid
Initial Setup and Configuration Time	Time and effort for initial setup and configuration is less	Setup and configuration time is longer and an intensive exercise
Infrastructure Cost	Infrastructure setup and configuration is owned by Google/Apigee	Customer needs to bear the cost of the underlying infrastructure
Support Cost	No additional cost for supporting the Apigee infrastructure	Requires additional cost to setup in-house support team
Infrastructure Monitoring	Reduced monitoring and maintenance overheads	High monitoring and maintenance overheads
Software Upgrades	Version upgrades are managed by Google/Apigee	Apigee Software version upgrades have to be managed by the client
Infrastructure Maintenance Skills	No additional skills required for maintaining the Apigee SaaS	Needs special skills and knowledge about Apigee runtime components
Regulatory Compliance	Meeting regulatory compliance requirements may be a challenge	Meeting regulatory compliance requirements is easier
Security	Enhanced API security	Limited API security

Technical Drivers

Features	Apigee SaaS	Apigee Hybrid
Hosting	Completely hosted on Google Cloud	Hosted on Google Cloud and Customer owned private network
Management	Completely managed by Google/Apigee	Jointly managed by Google and customer
High Availability and Scalability	Extended global reach, high performance and reliability	Limited to the underlying infrastructure provided by the customer
Performance	Network latency may be high	Reduced network latency
Security	Provides a robust WAF security and DDoS protection	Lacks a robust DDoS and needs investments for enhanced security
Automation	Enhanced automation capabilities to identify anomalies and predict API traffic	Very limited automation capability to analyze API traffic and detect anomalies

In Conclusion

Choosing between Apigee Hybrid and Apigee SaaS depends on various factors such as organizational requirements, compliance needs, and preferences. Apigee SaaS is a good choice for organizations looking for a fully managed, cloud-based solution that offers scalability, reduced operational overhead, and rapid deployment. Apigee Hybrid is suitable for organizations that require a combination of on premises and cloud deployment, giving them more control over the infrastructure and the ability to meet specific compliance or security requirements.

The Blue Altair Advantage

To ease the API adoption journey for our clients, Blue Altair has developed a comprehensive comparison scoring sheet that evaluates major and popular API Management platforms based on fifteen different criteria. Our evaluation criteria cover various aspects, including platform deployment models, ease of use, API development features and developer portal, among others. Furthermore, our strong partnership with leading API Management platform vendors enables us to ensure Blue Altair provides the best and latest technologies to our clients.

Our approach with clients is one of collaboration. Right from day one, we collaborate with them to assess their requirements, develop a comparison matrix of different API Management platforms, and build a proof of concept. Based on these initial efforts, we guide our client on the API Management platform best suited to their business needs. We also help clients during the pre-sales phase, working closely with both their customers and their product teams.

About the Author

Brajesh is the Sr. Director for API Management and Integration at Blue Altair. He has 25 years of experience in technology, leadership, consulting, architecture, and design, as well as implementation of distributed, cloud native, highly scalable and secure applications using APIs, Microservices, Cloud and Big Data technologies.

Prior to joining Blue Altair, he worked with Accenture as a capability lead for APIs, Microservices and Cloud Native Technologies, where he was primarily responsible for supporting sales, delivery, thought leadership and building reusable delivery assets and accelerators.

He is AWS- and GCP-certified as a Professional Cloud Architect, and an MIT certified Application Security Architect. He is the author of a book titled "API Management" and holds two published patents for his work in API assessment and Data Intelligence.

