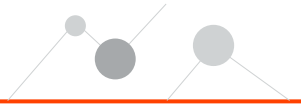
apigee



Apigee Edge: Apigee Cloud vs. Private Cloud

Evaluating deployment models for API management

Table of Contents

Introduction

APIs are the underpinnings of digital business platforms. To adopt an API-centric approach, it's critical for an enterprise to choose an API management platform that enables it to secure, scale, and manage APIs, and make them attractive to internal and external developers.

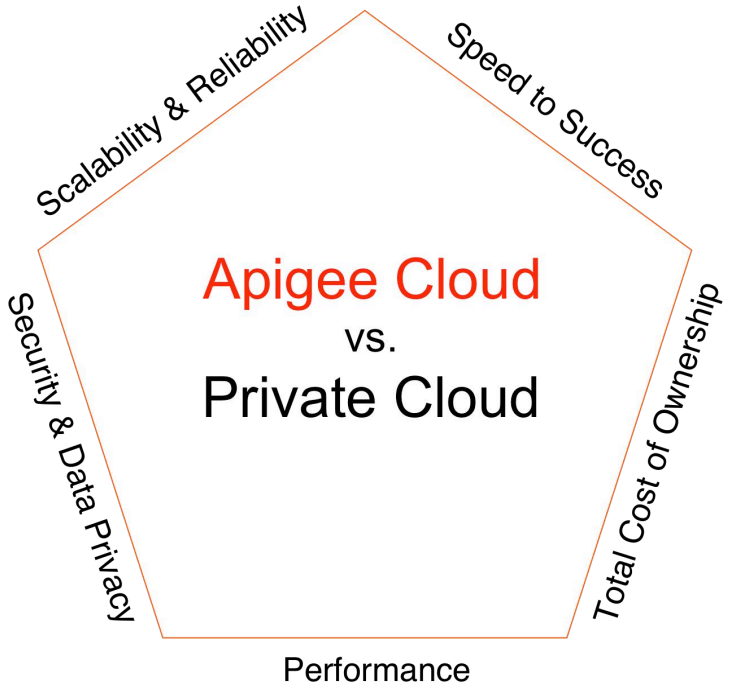
Apigee Edge, the intelligent API management platform, is the choice of hundreds of companies that are building or expanding their digital businesses. These companies can choose to deploy Apigee Edge in their private data centers or in the Apigee cloud.

Which model should you choose? It depends on your business needs—do you need to manage your APIs or control your customer data in-house?

In this brief, we examine the pros and cons of the two deployment models, and key factors to consider as you determine the deployment option for your enterprise.

When evaluating deployment alternatives, our customers consider the following dimensions:

- Time to success
- Total cost of ownership
- Security
- Performance
- Scalability and reliability



Time to success

Customers that deploy API management in the Apigee cloud typically go live with their digital initiatives much faster than those that deploy in the private cloud. The processes of acquiring, provisioning, and deploying hardware, as well as software deployment configuration, and the training required to deploy and manage API management software can all delay deployments to private clouds.

Customers that need to deliver high performance APIs to global audiences can take advantage of Apigee's global network of 24 data centers. Further, as business requirements change, a deployment in the Apigee cloud can be reconfigured to expand and adjust to a customer's needs.

Leading e-commerce and payment solutions provider First Data wanted to rapidly deliver a payment solution to enable merchants and banks to support Apple Pay in time for Apple's big launch. To ensure the delivery in less than five months, First Data chose to deploy API management in the Apigee cloud.

Total cost of ownership

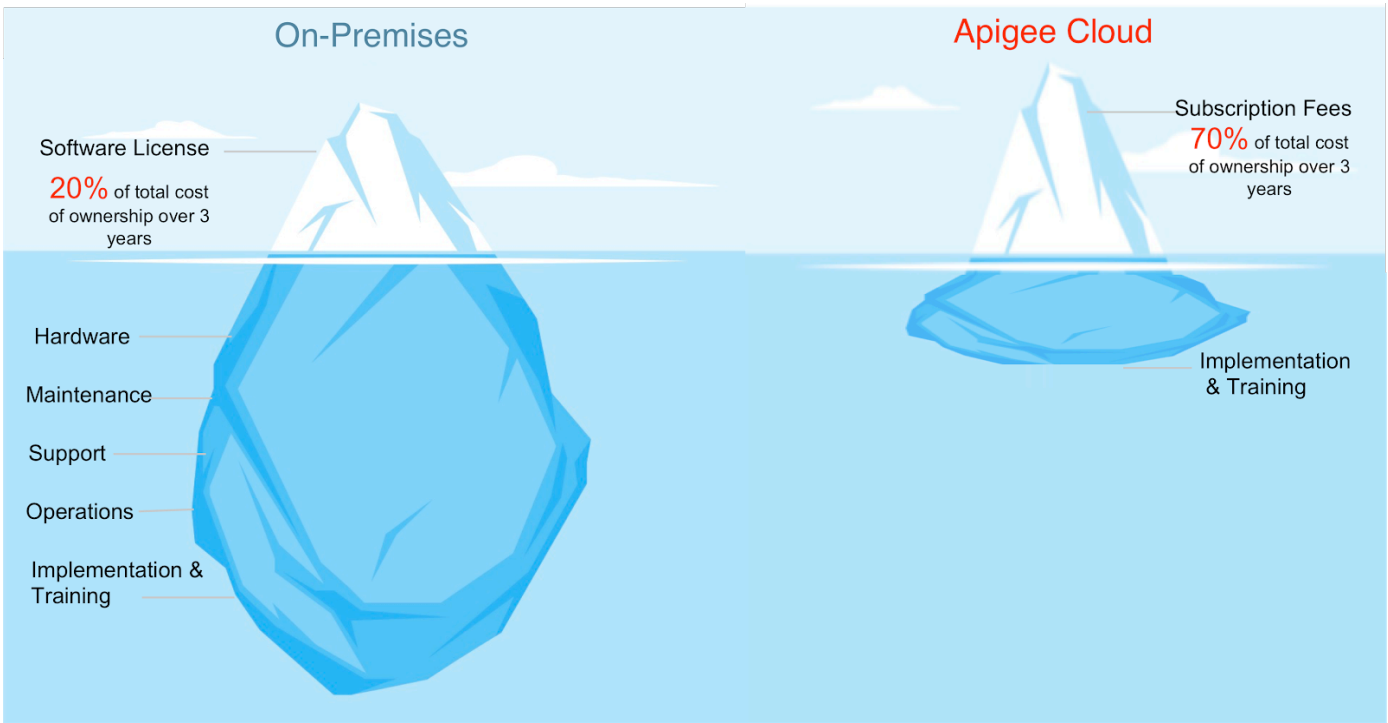
Apigee Edge API management in the Apigee cloud has a lower total cost of ownership (TCO) for our customers compared to a private cloud implementation. Private cloud costs include API management software costs, hardware infrastructure costs, hardware and software deployment and support costs, and operations and training costs.

The license cost of a private cloud deployment is less than a three-year annual subscription to the Apigee cloud. However, it is important to consider the additional costs an enterprise incurs with a private cloud implementation.

With the Apigee cloud (as with other SaaS offerings) infrastructure, operations, and support costs are distributed across Apigee's entire customer support base. Data from our customers suggest that for a single-region, medium-sized API management implementation, a private cloud deployment can cost three times as much as the Apigee cloud deployment.

A key factor for the higher TCO associated with private cloud deployments are the costs related to the people required to deploy, manage, monitor, and support the API management infrastructure 24x7.

A comparison of the TCO of private cloud API management and an Apigee cloud implementation



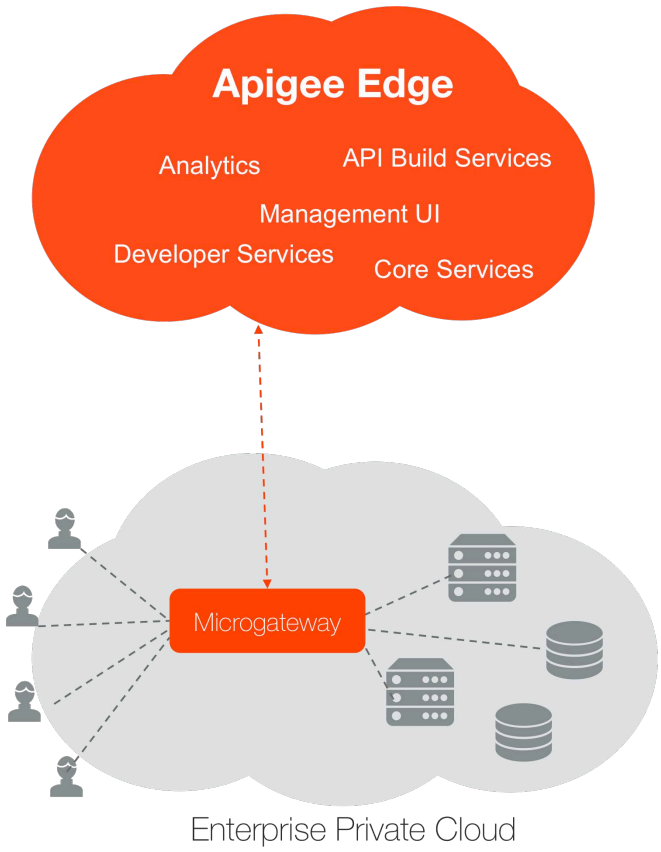
A private cloud deployment can be the right choice for customers who want to recognize their investment (via a one-time perpetual license purchase) as a capital expenditure instead of as an operational cost (a subscription license).

For customers with significant private cloud investments and spare bandwidth in their cloud operations team, the incremental operational costs are minimal, and the economics of a private cloud implementation are similar to that of the Apigee cloud.

Performance

The choice of API management deployment model can impact API performance in a couple of scenarios: for internal use cases, and when reaching geographically distributed audiences.

In internal use cases, where both the target backends and the API consumers are in a private cloud, API management in the Apigee cloud can introduce additional round-trip latency to API calls. However, Apigee Edge Microgateway—a hybrid cloud solution—solves this problem. Edge Microgateway enables customers to maintain their API run-time infrastructure in their private cloud, while keeping the rest of API management in the Apigee cloud.



Because Apigee runs the API management platform in 24 globally dispersed data centers, the Apigee cloud can deliver superior performance to global audiences.

Many of our global customers deploy in the Apigee cloud across multiple regional data centers (Virginia, Oregon, Ireland, Singapore, Tokyo, and Sydney, for example). Customers not only benefit from the reduced latency of API requests, but also enjoy improved overall reliability and disaster recovery in the event of a catastrophic data center failure.

Security

Apigee adopts industry standards, deploys numerous security offerings and processes, and employs third parties to enhance the security of the Apigee cloud.

Industry standards	The Apigee Platform is third-party audited, compliant, and certified for PCI DSS, HIPAA, SOC1, and SOC2. These and other certifications are available to customers and each of these standards is audited annually.
Security frameworks	Apigee uses multiple frameworks to define and manage security controls, including Cloud Security Alliance (CSA) and ISO.
Information security	Apigee has a formal information security policy and team. The team addresses the following domains: • Cloud security • Application security • Corporate security (IT, HR, network, privacy, and physical security) • Incident management • Business continuity and disaster recovery
SLAs and redundancy	Service level agreements are met through the use of redundant services in each region and redundant regions.
Application testing	Apigee cloud is a multi-tenant, self-service, SaaS platform that is penetration tested annually by multiple third parties. This annual report is available to customers. Apigee Edge software is also tested annually by a third party with expertise in application testing. Apigee also conducts its own internal application testing.
SDLC	Apigee follows a secure, formally documented software development lifecycle. This lifecycle includes static code analysis and dynamic code analysis tools, as well as peer code reviews and code release testing and approval processes.
Risk Analysis	An independent third party conducts an annual formal risk analysis for Apigee Corp, including all software and services. This analysis identifies areas of risk to be addressed and an annual update allows for changing threats, risks, and environments.
Incident management	Apigee has a formal incident response process that is carefully documented, tested at least once a year. It is updated and reviewed by third parties annually.
Background checks	Apigee conducts background checks on all employees prior to their employment. Financial checks are also performed on key finance employees. Repeat checks for key positions are performed after five years of employment.

Apigee works with our customer's information security team to further ensure that Apigee cloud meets the specific security requirements of the business.

Data privacy

The customer manages all data processed through or stored in Apigee cloud. Apigee does not need access to any end-user data for operation of the platform. The customer has the ability to decide what data to send through Apigee and what data, if

any, to store in the Apigee cloud (either in the API BaaS or in a cache). When a customer sends sensitive data through the Apigee cloud, Apigee operations does not see the payload in normal operations.

A customer can give Apigee support access to run a “trace/debug” session and, in that case, Apigee support may get access to customer data. If the Apigee customer does not want Apigee to have access to end-user data, this authorization can be withheld from all users of the Apigee platform, or from specific users.

Apigee does manage the platform and holds the master keys. But our access to customer environments is done the same way customers use the management UI. If an Apigee employee were to be given advanced access—the kind required to run a trace/debug—the enablement of this account, along with their actions, would be tracked in both the customer space and in the Apigee infrastructure logs.

Apigee prohibits this access by policy unless a customer requests it during a troubleshooting session. The customer can use analytics to identify any users with this type of access and remove those users at any time.

A private cloud deployment is a good choice in cases where industry or company regulations require that all your data, including API definitions and keys, need to reside on-premises.

Scalability and reliability

The Apigee cloud is managed by a talented operations team with hundreds of years of aggregate experience managing API management software in the cloud. Beyond the people expertise benefit, there are additional benefits of Apigee cloud compared to private cloud deployment.

Scale	The Apigee cloud processes over 300 billion API calls per year for customers across a variety of industries that have rigorous compliance requirements (including financial services, healthcare, and telecommunications). During Black Friday last year, peak API traffic in the Apigee cloud exceeded 50,000 requests per second. The Apigee cloud provides the additional benefit of dynamically scaling based on changing business needs.
Reliability	We delivered 99.999% availability to our customers in the Apigee cloud in 2015 and we continue to improve availability. The Apigee cloud’s distributed global network of 24 data centers and strong traffic management capabilities ensure that the system is well-protected from system outages and traffic bursts.
Ease of operations	Apigee has built a variety of tools to streamline the operations of the Apigee cloud, making upgrading software, debugging failures, and ensuring high uptime smoother. Apigee does, however, provide all the necessary training to enable customers to manage Apigee in their private cloud, as it takes additional operations resources and knowledge to become completely operational. A private cloud implementation is a good choice if you require complete control over the deployment of API management, including version upgrades and scaling.

Summary

API management is a key enabler of your digital business strategy. Making the right deployment decision will help you accelerate your digital initiatives. In most cases, deploying in the Apigee cloud is the better option compared to private cloud.

However, for pure internal use cases and for company-specific security policy reasons, a private cloud deployment can be the right choice. Even for pure internal use cases, we recommend the Apigee cloud option with the hybrid Edge Microgateway to minimize run-time latencies.

We encourage your security team to conduct an audit of our security policies to determine if the Apigee cloud meets your company's specific requirements.

Whether in the Apigee cloud or a private cloud, the Apigee Edge API management platform is built from the same Apigee codebase, so you always have the unique flexibility to start with the Apigee cloud option and then, if needed, move to a private cloud deployment.

About Apigee

Apigee® (NASDAQ: APIC) provides an intelligent API platform for digital business. Many of the world's largest organizations select Apigee to enable their digital business, including 30 percent of the Fortune 100, five of the top six Global 2000 retail companies, and five of the top 10 global telecommunications companies. Apigee customers include global enterprises such as Walgreens, Burberry, Morningstar, and First Data. Apigee is headquartered in San Jose, California and has over 400 employees worldwide. To learn more, see apigee.com.