HITRUST®

6175 Main Street
Suite 400
Frisco, TX 75034

July 2, 2021

Google, Inc.
803 11th Avenue
Sunnyvale, CA 94089

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® CSF Assurance Program requirements, the following platform and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.2 certification criteria:

> Google, Inc.: Apigee Edge API Management Platform.

The certification is valid for a period of two years assuming the following occurs:

- A monitoring program is in place to determine if the controls continue to operate effectively over time,
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),
- No data security breach reportable to a federal or state agency by law or regulation has occurred,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria, and
- Timely completion of the interim assessment as defined in the HITRUST CSF Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For certain HITRUST CSF control requirements that were not being met, the Organization developed a CAP that outlined its plans for meeting such requirements.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST CSF Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

A full HITRUST CSF Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST CSF Assurance Program can be found at the HITRUST website at [https://hitrustalliance.net.](https://hitrustalliance.net)

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, systematic, and regulatory risk factors.

Prepared for	Google, Inc. 803 11th Avenue Sunnyvale, CA 94089
Contact	Denis Canuel Program Manager deniscanuel@google.com
Assessment Option	HITRUST CSF Security Assessment
Company Background	Apigee is an API management platform
Number of Employees	300
Geographic Scope of Operations Considered	Off-shore (outside U.S.)
Organizational Risk Factors	
Number of Records that are currently held	Less than 10 Million Records
Systematic Risk Factors	
Is the system(s) accessible from the Internet?	Yes
Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	Yes
Does the system(s) transmit or receive data with a third party/business partner?	Yes
Is the system(s) accessible from a public location?	No - There are no publicly-facing systems within the scoped environment.
Number of interfaces to other systems	Fewer than 25

Number of users of the system(s)	Fewer than 500
Number of transactions per day	Greater than 85,000
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - There are no dial-up capabilities within the scoped environment.
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - Apigee does not utilize fax machines for any in-scope business processes.
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - Apigee employees do not travel to high risk areas.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	No - Apigee does not support a BYOD program, therefore no personal devices are permitted to connect to the in-scope environment.
Are wireless access points in place at any of the organization's in-scope facilities?	No - Wireless networks are not used to process or transmit data.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - Apigee does not conduct e-commerce transactions.
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - Apigee does not use digital signatures for any in-scope business processes.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - Apigee does not send any data via courier or mail service.
Is any aspect of the scoped environment hosted on the cloud?	Yes
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Are hardware tokens used as an authentication method within the scoped environment?	Yes

Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes

Regulatory Risk Factors

None selected

Scope of Systems in the Assessment

Organization and Industry Segment Overview

Google LLC ("Google" or "the Company") is a global technology service provider focused on improving the ways people connect with information. Google's innovations in web search and advertising have made it one of the most viewed Internet destinations and its brand among the most recognized in the world. Google maintains one of the world's largest online indexes of web sites and other content and makes this information freely available to anyone with an Internet connection. Google offers Internet-based services and tools that users can consume to communicate, collaborate, and work more efficiently.

The scope of this assessment report is limited to the Apigee Edge API Management Platform ("Apigee Edge"), which is a multi-tenant, customer-facing, web-based, self-service API development and management platform offered by Google that enables business customers to securely expose their digital assets through APIs for developers and partners who are building applications, as well as the supporting cloud hosting and infrastructure systems. Apigee Edge enables enterprise customers to measure the success of their digital initiatives with end-to-end analytics and works by fronting services with a proxy layer and providing an abstraction or facade for backend service APIs, which is used to provide environment security, rate limiting, quotas, analytics, and other related system functionality within individual customer Apigee Edge instances via an online web portal made available to Apigee Edge customers.

The core API management product includes a mediation and intelligence engine, developer services, and monitoring and reporting services and together, these services help provide a foundation for customers to leverage existing systems, shared databases, security frameworks, management infrastructure, and operational tools. Apigee Edge also includes bot detection and prevention capabilities that enable blocking or throttling of bad bot traffic based on machine intelligence configured to efficiently process and analyze information on billions of API calls.

Service(s) / Product(s) Provided

There are three services that comprise the Apigee API Management platform also known as Apigee Edge:

- Developer Ecosystems
- Monitoring and Reporting
- Mediation and Intelligence Engine

DEVELOPER ECOSYSTEMS

A developer portal is deployed by an enterprise to provide a community for developers with the resources necessary to learn about the enterprise's APIs, become a registered developer, and collaborate with both peers and the enterprise. Tools such as blogs, frequently asked questions (FAQs), and forums help developers interact with one another to present solutions. Modeling and developer management helps provide streamlined developer registration with a manual or automatic registration process.

Developer keys can be approved automatically or manually for a given API product. Interactive API documentation and modeling through Apigee's SmartDocs feature supports the design and documentation of new APIs as well as learning, testing, and evaluating existing APIs. In addition, terms of services (TOSs) and acceptance for APIs can be managed.

MONITORING AND REPORTING

This API analytics solution helps customers make better business decisions through an understanding of customer behavior and interactions, using real-time data from their APIs and from the edge of their business.

- Business metrics help provide organizations with a complete picture of their customers, including how those customers use their services with partner APIs, social networks, and other products
- Operational analytics monitors the health and performance of production APIs, enabling enterprises to plan for traffic spikes, identify slow or error-prone APIs, and to find root causes and traffic anomalies
- Application performance monitoring measures mobile application usage and performance of applications on different platforms, carriers, and devices
- Customers can segment their audience by top developers and apps, understand usage by API method to know where to invest, create custom reports on business-level information, and see long term usage trends

MEDIATION AND INTELLIGENCE ENGINE

API management enables the transformation of existing back-end services to APIs with over 40 policies designed for “configure rather than code” deployment. A unified security model is provided throughout the platform; it provides secure portal access and can support other pre-existing security programs by using pluggable authentication. Apigee enables developers with API programmability, which allows for the extension of the mediation and intelligence engine capabilities with support for Java, JavaScript, Node.js, and Python.

The report includes the Apigee API Management Platform as described above. The accompanying description includes only policies, procedures, and control activities at Google and does not include policies, procedures, and control activities at any subservice organizations (see below for further discussion of subservice organizations).

Primary System(s)

The Apigee API Management platform:

- Apigee API manager (Apigee Edge) (Dually-hosted at GCP and at AWS)
- Infrastructure Support

Google utilizes the following to manage the Apigee Edge system:

- Jump Server
- Puppet Master
- Monitoring
- Zookeeper
- Cassandra
- Collection Service
- Cloud Storage
- Preprocessing
- Spark
- Redshift
- Postgres
- Message Processor
- Router

Service(s) Outsourced

Apigee Edge is a cloud-based, multi-tenant web tool that utilizes cloud services provided by Amazon Web Services (AWS) and Google's Cloud Platform (GCP).

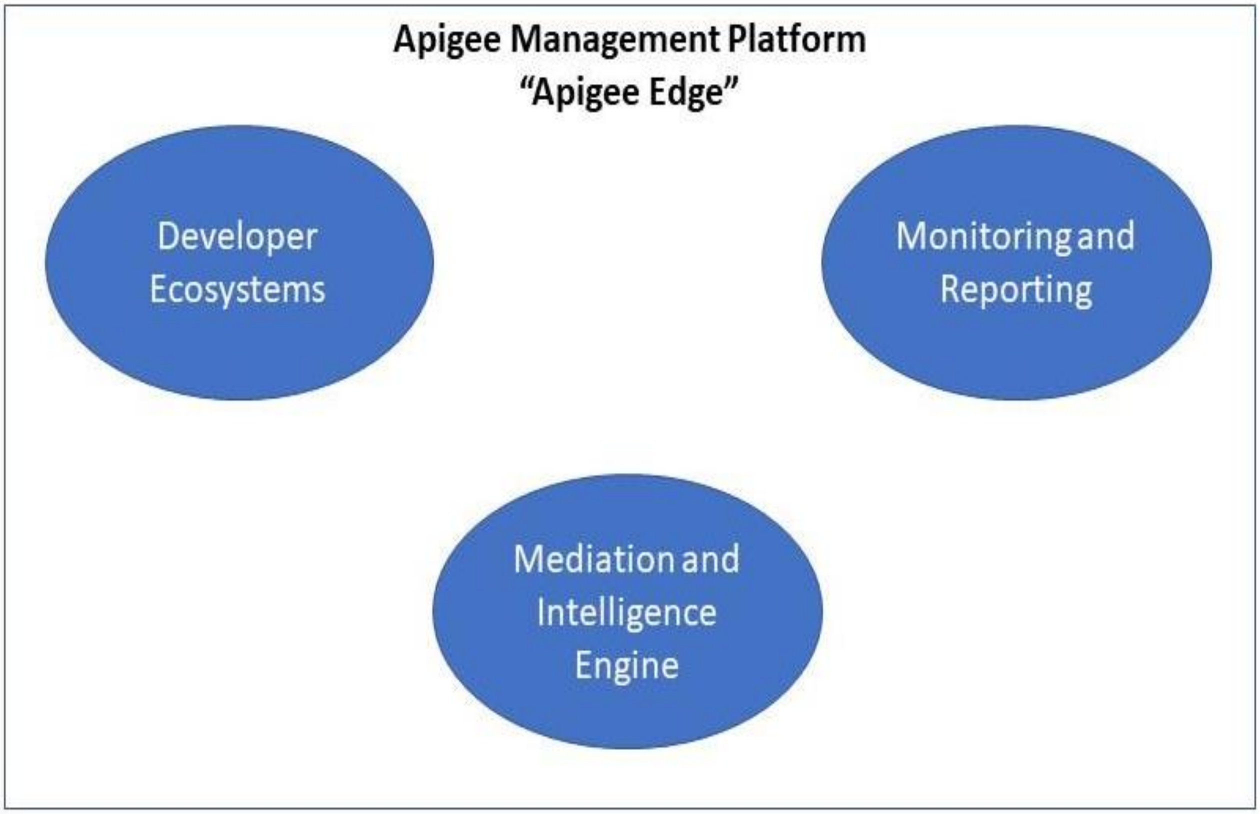
Scope Overview

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
Apigee Edge	• Jump Server • Puppet Master • Monitoring • Zookeeper • Cassandra • Collection Service • Cloud Storage • Preprocessing • Spark • Redshift • Postgres • Message Processor • Router	Developer Ecosystems	X			
		Monitoring and Reporting	X			
		Mediation and Intelligence Engine	X			

Scope Description

The scope for this assessment report is limited to the Apigee Edge API Management Platform, which includes the Developer Ecosystems, Monitoring and Reporting, and Mediation and Intelligence Engine services within Apigee Edge, as well as the supporting cloud hosting and infrastructure systems. Numerous internal and Google-developed support systems and tools are utilized, as well as cloud hosting services provided by GCP and AWS cloud service providers. Covered information is never stored locally on Google devices and Google employees do not maintain persistent access to customer data. Customer data resides strictly at cloud storage locations within individual instances of Apigee Edge customer environments.

Scope Diagram


Apigee Management Platform
"Apigee Edge"
Developer Ecosystems
Monitoring and Reporting
Mediation and Intelligence Engine