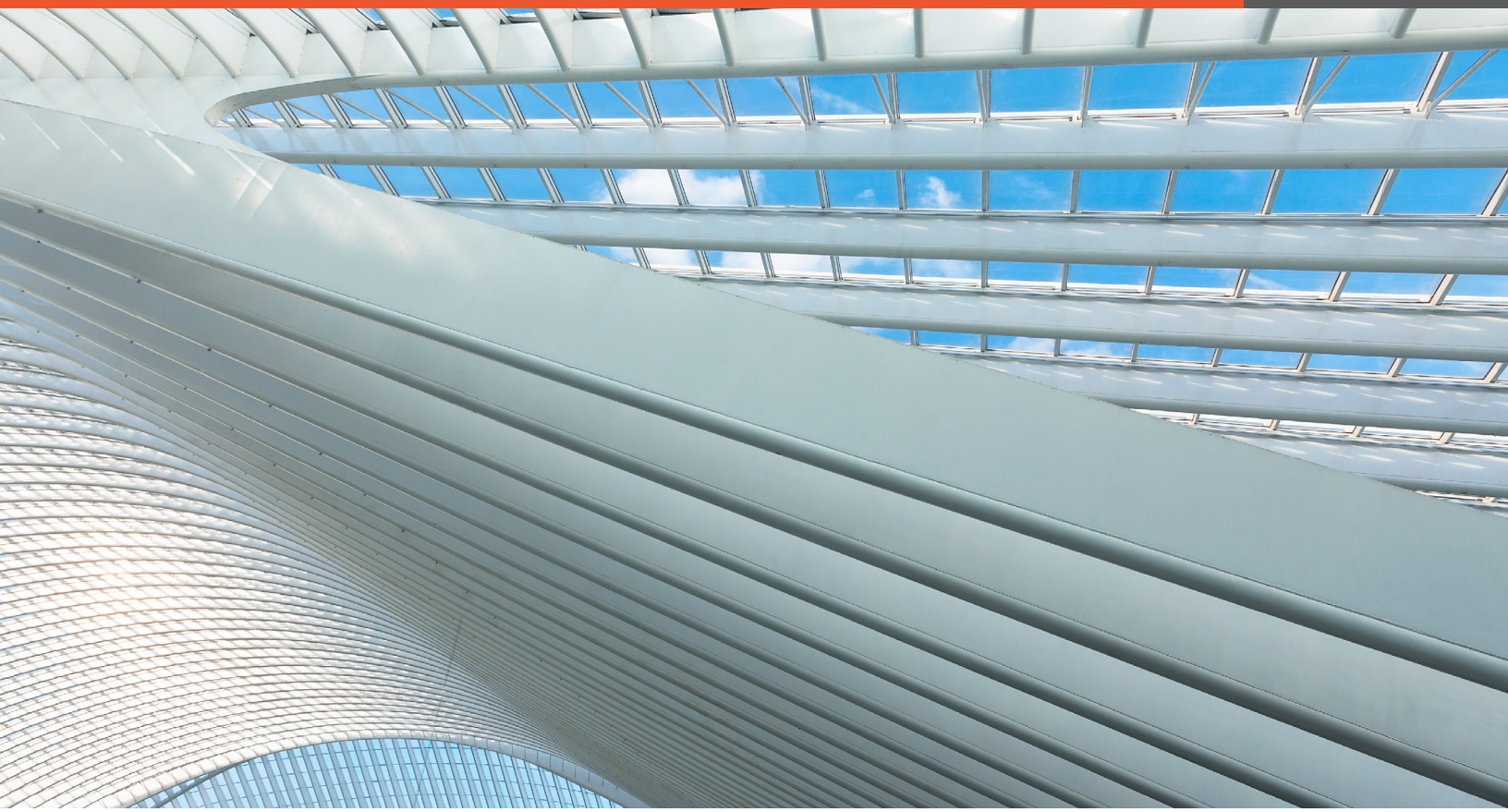
Technical Brief



A Checklist for Every API Call

Managing the Complete API Lifecycle

apigee

A Checklist for Every API Call

apigee

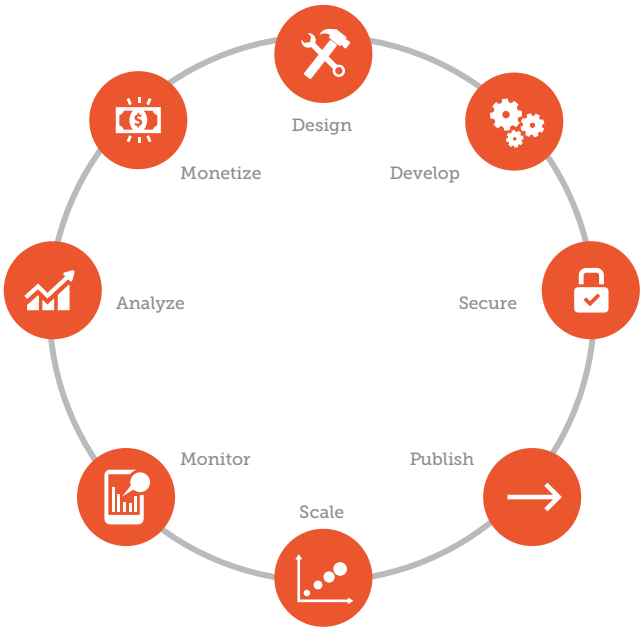
Table of Contents

Introduction: The API Lifecycle

An API gateway is the core of an API management solution. But it's not the whole solution. To learn about the components of comprehensive API management, see the eBook: The Definitive Guide to API Management.

When it comes to the API gateway, however, the most important role it serves is ensuring reliable processing of every API call.

An API gateway manages the entire API lifecycle. It is imperative that it enables the people responsible for it to effectively and securely deliver APIs that are easy to use by app developers.



People and the API Lifecycle

The following people or teams are stakeholders in the API lifecycle and therefore care about the functionality of an API an API gateway and an API management solution.

- **Security architect or CISOs**
- **Developers or enterprise architects**
- **Operations engineers**
- **API business or product owners**

While most API gateway solutions can do basic API proxying, APIs have become the fabric of the digital enterprise, so companies need functionality that addresses the concerns of all the stakeholders. The key to helping these people do their jobs? Provide an easy-to-configure tool and extensibility.

Managing the Complete API Lifecycle

Depending on their roles and responsibilities the primary stakeholders in the API lifecycle are concerned about a number of different use cases. An API management solution provides the features and capabilities that enable each stakeholder.

Security professionals

Security is paramount for companies when they expose their backend systems or proxy existing APIs. Given that customers or consumers use first-party or third-party apps on mobile devices, partners do transactions, and internal developers build apps on sensitive data, companies need to view security from the perspective of an API call: end to end.

An enterprise should assess potential risk and how to secure and mitigate those risks. The following is a list of security use cases and the API gateway features needed to address them.

Use case	Definition	Required feature
Mutual authentication SSL, VPN, IP whitelisting	Authentication of endpoint from which API call originates	Endpoint authentication
API key validation	Authentication of process from which API call originates	API caller authentication
API key authorization	Authorization of process from which API call originates	API caller authorization
API key & request/response logging	Attributing API calls to right callers	API caller auditing
OAuth access token validation	Authentication of end user involved in API call	API user authentication
OAuth scopes check	Authorization of end user involved in API call	API user authorization
User & request/response logging	Attributing API calls to correct end users	API user auditing

Managing the Complete API Lifecycle

Security professionals (Continued)

Use case	Definition	Required feature
Bots, SQL injection, virus, compromised user, compromised API key	Screen requests for malicious intent	Threat protection
Confidential data screening, PII data screening, data masking	Ensure sensitive data is not accidentally or intentionally leaked	Leakage prevention (compliance)
SSL, storage encryption	Encrypted transmission and storage of data	Data encryption

API developers

Productivity is key for API developers. They want to use familiar tools and languages and configure things easily, and they care deeply about the experience of those who'll build on the API. API developers have to ensure that the API behaves as intended and they need to provide quick and precise debugging and optimize the backend resources that serve the API requests. Here's a list of the use cases and features that are important for API developers.

Use case	Definition	Feature needed
Service callouts	Implement APIs using multiple calls to other APIs and aggregate/ transform data between the calls	Extensibility (Java/Javascript) including support for Node.js
XML to/from JSON, SOAP to REST	Implement transformation between popular formats	Request/response transformation
Path validation, parameter validation, header validation	Validate requests	Request validation
Warnings, error logs, debug logs, info logs	Log intermediate status/data during request/response processing	Logging

Managing the Complete API Lifecycle

apigee

API developers (continued)

Use case	Definition	Feature needed
Thread pools, exception counts, object counts	Collect metrics specific to API implementation	Metrics collection
Round robin, least loaded, retries	Load-balance calls made to other API implementations from a given API implementation	Target load balancing
Fallbacks, back pressure, multiple implementations	Route around issues when making calls to other API implementations from a given API implementation	Target routing
Caching	Cache data used in API implementations	Data caching
Encryption, masking	Encrypt data used in API implementations	Data encryption
Custom usage tracking	Track usage of specific data or logic resources within API implementations	Usage tracking
Custom usage records, custom limit enforcement	Track subscriptions or limits specific to API implementations	Subscription & limit checks
Custom caller journey, custom user journey	Track journey specific to API implementations	Journey tracking
API access keys, database credentials, certificate keys	Store credentials required to access data or another API implementations from a given API implementation	Credential store
Key value map, document store, graph, relational store	Persist the data required by the API implementations	Data persistence

Managing the Complete API Lifecycle

Operations engineers

Operations teams are accountable for the reliability of the service, both internally and externally. Managing the service level agreements (SLAs) for the APIs is a priority. Operations teams also need tools that enable them to provide the best service for developers without major increases to infrastructure costs.

Use case	Definition	Feature needed
Caching	Caching of responses to avoid reprocessing requests	Response caching
Access logging, custom logging	Logging of requests and responses	Request/response logging
Latencies, status codes	Collecting metrics related to requests and responses	Metrics collection
Rate limits, spike arrests, concurrency limits, quotas	Implementing quality-of-service management through traffic shaping	Traffic management
Round robin, least-loaded, retries	Supporting clustered API implementations	Load balancing
Retries, fallbacks, back pressure, multiple implementations	Routing around faults or latencies based on context	Request routing
Progressive rollout, experimentation	Splitting traffic between two different implementations	Traffic splitting

Managing the Complete API Lifecycle

API product or business owners

For the API product or business owner, it's crucial to relate the APIs to the business imperatives and results in a meaningful way and therefore to instrument APIs to capture the right metrics and measure the impact. More advanced needs include the ability to have rate cards and charge developers who consume the APIs.

Use case	Definition	Feature needed
Per-caller tracking, per-user tracking, per-API tracking	Track usage of API calls	Usage tracking
Subscription validation, limit enforcement	Validate subscriptions to APIs and ensure limits have not been reached	Subscription & limit checks
Caller journey, user journey	Track journey through API calls	Journey tracking

Managing the Complete API Lifecycle

apigee

Apigee Edge

Whether you're a security architect, developer, operations engineer, or API product owner—or you require different combinations of the features required for these roles—Apigee Edge has you covered. With more than 30 preconfigured policies, the ability to use common languages like Java, JavaScript, Python, and Node.js, and built-in metrics collection and reporting, Edge offers the powerful extensibility needed to build and manage every aspect of an API program.

USE CASES TO MANAGE THE API LIFECYCLE			
API developer	**Security professional**	**Operations engineer**	**API product owner**
• Service callouts • XML to/from JSON, • SOAP to REST • Path validation, parameter validation, header validation • Warnings, error logs, debug logs, info logs • Thread pools, exception counts, object counts • Round robin, least loaded, retries • Fallbacks, back pressure, multiple implementations • Caching • Encryption, masking • Custom usage tracking • Custom usage records, custom limit enforcement • Custom caller journey, custom user journey • API access keys, database credentials, certificate keys • Key value map, document store, graph, relational store	• Mutual authentication SSL, VPN, IP whitelisting • API key validation • API key authorization • API key & request/response logging • OAuth access token validation • OAuth scopes check • User & request/response logging • Bots, SOL injection, virus, compromised user, compromised APIkey • Confidential data screening, PII data screening, data masking • SSL, storage encryption	• Caching • Access logging, custom logging • Latencies, status codes • Rate limits, spike arrests, concurrency limits, quotas • Round robin, least-loaded, retries • Retries, fallbacks, back pressure, multiple implementations • Progressive rollout, experimentation	• Per-caller tracking, per-user tracking, per-API tracking • Subscription validation, limit enforcement • Caller journey, user journey

apigee

About Apigee

Apigee delivers an intelligent API platform to accelerate the pace of digital business. We help companies – from disruptive start-ups to the Fortune 100 – use their enterprise data and services to create connected digital experiences for customers, partners, and employees. This is digital business.

For more information, visit apigee.com.

Where to go from here

For more on the anatomy of a sophisticated API management solution, best practices for API security, getting insights from API analytics, extending your basic APIs via BaaS, and more, download the eBook, "The Definitive Guide to API Management".

The Apigee Edge product helps developers and companies of every size manage, secure, scale, and analyze their APIs. Get started with the right Apigee Edge for your size business.

For additional resources, visit apigee.com/about/resources/

Share this eBook