axway

WHITE PAPER

Beware of third-party cloud service APIs

The simple way to get control, reduce risks, and lower the cost of consuming cloud services

01

INTRODUCTION

Every company today is consuming some sort of third-party cloud service – Salesforce, Marketo, Facebook, Twitter, Getty Images, Stripe, Recurly, Trello, GitHub, and many more.

Each third-party cloud service that is consumed must be integrated with a company's systems and processes. This integration is usually through APIs that, unbeknown to the company, can open them up to major costs and security risks.

How can you secure and manage these third-party cloud service APIs at least as well as you secure and manage your own APIs?

The pros and cons of third-party cloud service APIs

Leveraging cloud services enables companies to get faster business value than building or hosting the service themselves. As a result, they can focus on the core business and innovating faster to deliver new value.

However, consumption of these cloud services can be so quick, easy, and at such a low cost initially that most enterprises lose control over what cloud services they are actually subscribed to. This creates extra cost when the company has multiple subscriptions to the same service. In addition, these services are typically integrated into a company's internal and external systems, opening up a wide range of security exposures and risks, especially when a company has distributed or ad hoc integration teams. **Figure 1** below shows a company integrating directly with a third-party cloud service's APIs.

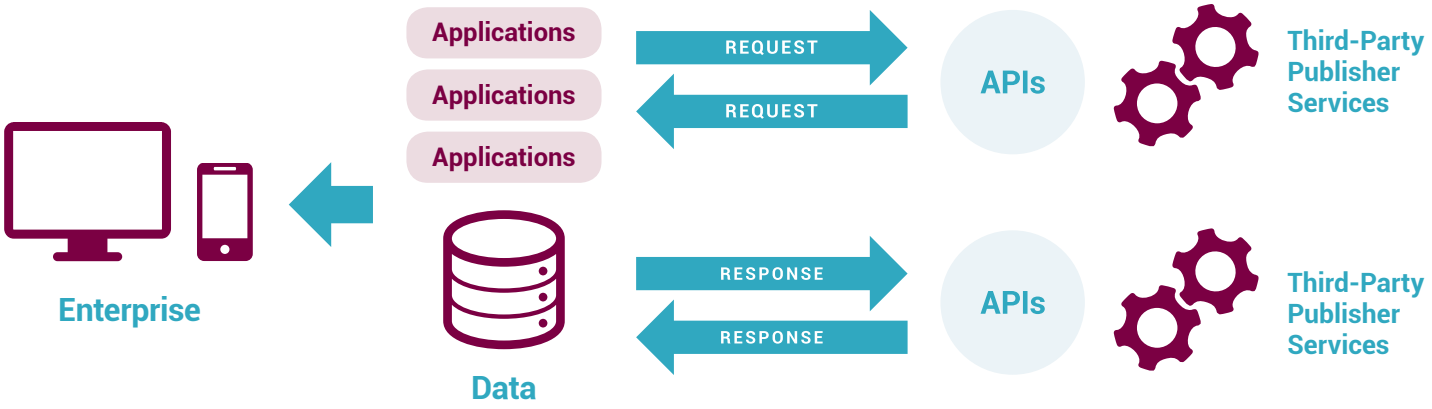

Figure 1: *Simple reference architecture for relationship between API consumer and third-party cloud service's APIs.*

Safety integrating external APIs with your internal systems

As mentioned above, it is possible to integrate third-party cloud service APIs on an ad hoc basis. Each time an application wants to connect to an API, you write the code necessary to make it happen. This is not an efficient approach, though. Nor is it consistently secure or manageable. A better practice is to use an API management platform to manage the consumption of third-party cloud service APIs.

An API management platform enables streamlined, secure integration of third-party cloud service APIs. It can also handle the monitoring of their performance. Functional specifics of these platforms vary, but they usually contain a collection of capabilities that make APIs easier and less costly to consume, including:

- **API catalog:** An API catalog offers visibility to third-party cloud services and their respective APIs being consumed in the enterprise along with their Terms of Service. The catalog makes it possible for developers anywhere in the organization to search for, find, and integrate APIs they may want for their applications. The catalog is often part of an API portal that is designed to engage API consumers and help them learn about the APIs and their use.
- **API gateway:** An API gateway gives you the ability to abstract and protect your enterprise credentials. The third-party cloud service API connects with the gateway, not the consuming application itself. It prevents employees from inadvertently exposing their enterprise credentials and putting the company at risk. The gateway can also provide monitoring and alerting. That way, if a third-party API is not performing in accordance with its ToS, the right person will be notified. **Figure 2** below shows how the API Gateway fits into the enterprise architecture of publisher and consumers.
- **API lifecycle management:** Full lifecycle management lets application owners stay on top of third-party cloud service APIs. They can keep track of API versions as they are introduced, retired, and replaced.
- **API security:** It is essential to control access to digital assets by authenticating and authorizing external third-party cloud service APIs.
- **API orchestration and integration:** To simplify and speed up integrating the cloud services with a company's system, access to no-code/low-code tools for both on-premises and cloud usage such as an iPaas is highly recommended.

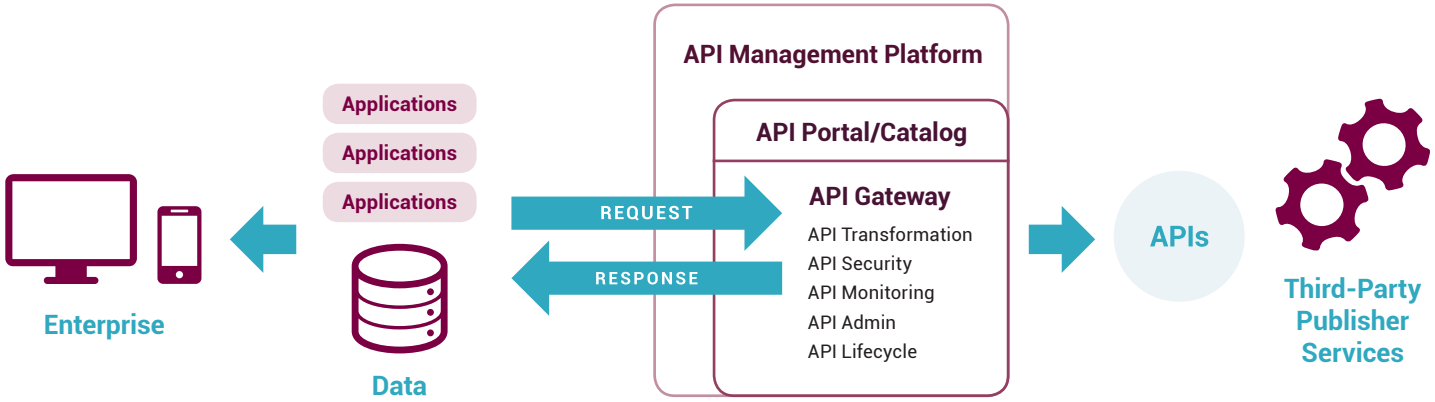

Figure 2: *The role of the API gateway: Handing API monitoring, transformation, security, admin, security, and life-cycle management*

Overcoming risks and challenges

Bringing external APIs into your enterprise introduces a number of risks and challenges. These range from inconveniences and unexpected charges to potentially serious security issues. Each risk and challenge can be addressed by people, processes, and technology.

Unnecessary charges

One issue that can arise is the misuse of the API leading to unnecessary charges. For example, a company might subscribe to an API that gives them the ability to download images. Depending on how it was set up, the API might charge repeatedly for the same image if it were downloaded more than once. To avoid situations like this, it's important to understand exactly what the API's terms of service includes.

An API gateway solves this problem. Admins can establish controls so when an image is downloaded from the API, it is 'cached' or saved to a file system. Then, if that image is requested again, the gateway will check to see if it's already on file — avoiding a repetition of the download and charge.

Sub-optimal subscription pricing

We have seen cases where multiple business units at a company each negotiate separately for subscriptions to the same API. This invariably leads them all to get a sub-optimal deal.

With the right API management platform and an API catalog, the separate API consumers can be aware of their usage and leverage that knowledge to negotiate the best possible terms. In one example, a power generating company subscribed to external weather services via API. They used the service across the company to better predict customer demand, e.g. if it were going to be hot in a given location, that might trigger a greater demand for electricity. After centralizing access to this service with API management and controlling when updates occurred, they were able to save over $1 million dollars annually.

Usage monitoring

You may also receive an API bill you can't validate. The publisher says your enterprise used the API 10,000 times, but you don't know if this is true. You can neither prove nor disprove the claim. Without effective API management, you could find yourself in this bind. On a related note, if you want to change API suppliers, you might have an issue because you don't know which of your applications is consuming the API. Not knowing which third-party cloud service APIs are being consumed in the enterprise can also expose the organization to problems related to security and compliance as well as legal liability.

Security

Security becomes an issue with third-party cloud service APIs if employees share their personal login credentials with other employees. This is a more common practice than you might think. In way, it even makes sense. If you're signing up for a cloud service and your company doesn't have a formal process and platform for doing this, you might share your cloud service credentials so that a developer in your organization can easily connect to the cloud service APIs to perform an integration.

Typically, you create an “admin" account for the cloud services and use that account to share with all the developers who integrate the services with your company's systems. The problem here is that you've just exposed the enterprise to the risk of breach. Also, if the developers are directly using the third-party cloud service's API key to access the service, the risk of unauthorized access emerges. A developer might leave the organization but retain the API key. Without an API management platform, it is difficult to keep track of key assignments like this.

Terms of service

As APIs become more critical to core business applications, it is essential to know the third-party cloud service's API terms of service and understand when they're not being met. Issues may include who

CONCLUSION

As companies work on externalizing their services via APIs, they should also pay attention to how they consume third-party cloud service APIs. Risks can arise from neglecting security and management aspects. Inadequate third-party cloud service API management also affects compliance. Performance issues can be a problem, too, as internal applications become reliant on external APIs that are not well monitored or understood.

API management platforms offer a solution to the challenges of managing third-party cloud service APIs to maximize the business benefits.

They do this by creating a catalog of APIs so everyone in the enterprise can be aware of which APIs are available along with their respective ToS.

An API gateway provides a secure, managed point of integration between internal applications and external APIs. The right tools and processes for the consumption of third-party cloud service APIs can result in significant benefits to a business while minimizing downside risks.

Discover 10 ways to modernize your API strategy for third-party cloud services

READ THE WHITE PAPER