axway

10 ways to modernize your API strategy

How to master the planning, protection, and performance of APIs to speed digital transformation and time to value

WHITE PAPER

APIs: the bridge to continuous modernization and innovation

APIs are a simple concept: they connect data to create new digital experiences. If we look at the IT modernization trends driving digital transformation, APIs play a critical role in all of them. Cloud projects use APIs. Software that interacts with IoT sensors uses APIs. Contextual mobile apps use APIs. And getting big data into systems to be ingested and analyzed is the task of the humble API. So they aren't a fad; they are the key technology that makes new business models, product offerings, insights, and many other IT changes possible, and they are increasingly seen as a critical part of the successful digital transformation of any organization.

Regardless of how you use APIs, it's critical to take a strategic, rather than tactical, view of how you plan, design, secure, and manage them. A strategic view will enable you to address the tactical needs of today while providing the flexibility clearly needed to modernize and thrive in the digital world.

These 10 best practices can help you modernize your IT infrastructure with an API strategy that supports continuous innovation while also optimizing cost, flexibility, and security:

01
Plan for positive ROI

02
Build governance as you need it

03
Use a common API layer to ground the cloud

04
Coordinate business and technical monitoring

05
Ensure a positive user experience and satisfy SLAs

06
Conduct regular audits

07
Make security a feature, not a barrier

08
Know your identity

09
Make policies separate from APIs

10
Use throttling and quota management

Change is never-ending — the new style of enterprise IT

The digital innovators of today have demonstrated the value of a more agile approach to IT. A modern, multispeed IT architecture separates slower systems of record development from the faster cycles for systems of engagement that manage interactions with customers, partners, developer communities, and employees.

It is these engagement systems that need to support continuous change and innovation. APIs, and the ways you manage them, enable both speeds to proceed at the optimal pace.

01

Plan for positive ROI

When it comes to a modern IT infrastructure, it is no longer viable to simply invest in sufficient capacity to cover the current project. You need to think about creating a broad pool of resources, sufficiently generic that they can be applied to different projects. Reusing capacity improves efficiency and effectiveness, all the while reducing costs and increasing the potential return from projects.

But with a variety of different projects, and a pool of generic resources, where should you start? The key here is to pick “low hanging fruit” — projects that create the biggest benefit in the least amount of time. Not only will these projects deliver a quick win and help improve the performance of the organization, but they also subsidize the infrastructure that can then be deployed elsewhere and on other projects.

The other critical task is to bring budget-holding executives on board. All too often, decision makers see your expenditure requests as simply, “IT wants money for some shiny new objects.” To change their perception, it is important to help them understand the fundamental changes that are occurring — both on a macro level and for the business itself — so they can appreciate the potential value your proposed projects can offer.

When you find the right executive champions, you won’t get stuck arguing over which divisions pay what percentage of the project. You will just get it done.

Make resources as generic as possible, so they can deliver quick wins and be deployed across multiple problem areas.

Think about governance not for its own sake, but as a core part of streamlining every project from end to end.

Benefits of an API catalog and self-service portal:

- An API portal contains reusable components that can help you scale from one successful project or team to many across the enterprise, reducing the cost and time parameters of subsequent products and projects.
- By implementing a broad API catalog, you can apportion the cost of governance across multiple projects, thereby reducing the cost for each individual project.

02

Build governance as you need it

Governance is a balancing act. While it is clearly important to have oversight for projects, roles, and budgets, it's hard to wrap distinct parameters around projects when the organization is in such a state of flux. The fine line is to have enough governance process in place to ensure control, but not so much that the entire process of creating products or services is slowed down.

A solution like Axway AMPLIFY™ API Management ensures lightweight, yet robust, governance by enabling you to build a broad API catalog and make it accessible via a self-service API portal. While the initial project may seem to have no critical need for a portal, by thinking about it from the outset, you can address governance in totality — aspects like the approvals process for an API can be considered in the context of the broader API strategy.

Over time, you can use the portal to securely share best practices, code samples, and resources with a growing number of internal API teams, partners, and developer communities. It is actually a small investment to ensure your platform is, as much as possible, future-proof.

03

Use a common API layer to ground the cloud

While many people think APIs mean moving everything to the cloud, or at least to new architectures, the reality is different. On-premise is not going away for many good reasons. But cloud applications don't just magically work with on-premise applications.

To bridge the gap, you will need to wrap on-premise applications in a common API layer that enables them to readily talk to the outside world while still running on traditional infrastructure and architectures. This idea of a buffer layer also extends to infrastructure elements, communication channels, mobile devices, application components, and sensor inputs that require interplay between on-premise resources and the outside world.

AMPLIFY API Management is an example of a sensible early investment that can be deployed in the cloud, on-premise, or a hybrid of the two, and used to create a common, reusable API layer that can traverse cloud to ground. Again, reusing elements in subsequent projects will reduce long-term costs and help you achieve a more compelling ROI story that should, in turn, build your case for future projects.

Create an integration layer that connects solutions within the firewall and on the outside and takes care of API impedance mismatches and error handling.

04

Coordinate business and technical monitoring

The modern face of IT is one of rapid iteration and a plethora of smaller projects. Each individual project or application is often made up of a vast distributed group of components, and developers can pick and choose the ones that best fit the specific use case. This paradigm makes it even more critical to ensure good monitoring is in place — both business-centric and technical.

In the past, technical monitoring (uptime, performance, etc.) was discrete from business monitoring (costs, ROI, etc.). Today, the two are much more closely linked. There are two critical things to think about here:

1. You will need to feed extracted business and technical performance data into other systems of record. For example, your financial application shouldn't be blind to the business data coming out of a technical platform — it is key to constructing meaningful links between systems and demonstrating the value of the API initiative.
2. You will need to integrate the data coming out of the business and technical monitoring aspects of the API management solution with other data — from both inside and outside the organization. End-to-end business metrics and visibility are key here, and it is only through integration of multiple data sources that you will gain a clear view.

AMPLIFY API Management includes comprehensive business and technical metrics that provide visibility into where and how your API program is or isn't succeeding. Mobile metrics gauge the last mile of performance. Baseline trends help predict when abnormal situations may be arising. Analytics dashboards can be customized for a specific business purpose and metrics can be exported and combined with external data to enable even deeper understanding.

Make sure you have real-time operational visibility to monitor API performance, as well as adoption and usage metrics to gauge API program business success.

05

Ensure a positive user experience and satisfy SLAs

Best Practice 04 suggested that it's critical to give everyone within the organization visibility into the business and technical performance of the API platform. Beyond simply justifying the existence of the platform, or what is built upon it, this visibility is critical to ensuring that user expectations and formal SLAs are met.

Missed SLAs can have serious repercussions. For example, studies have shown that even a small increase in page load times for an app or service can have a big impact on conversion rates. If you have an API-driven experience made up of many different components, each communicating via different APIs, there is a significant risk of service degradation or even service outages. When this happens, you face unhappy users and potential SLA penalties.

To provide a positive user experience and satisfy your formal SLAs, you need a clear picture of the expected service levels for different parts of the platform. Metrics and predictive analytics like those available through AMPLIFY API Management will let you measure what matters, and give business and technical users the ability to monitor, predict, and proactively act on changes in performance.

Determine the appropriate SLAs for different parts of your API platform and for each app or service. This way, they become a useful tool tied directly to business value.

Use audit data as a rich source of information that can be further mined to gain insights that become more valuable over time.

06

Conduct regular audits

Audit. It's probably one of the most dreaded activities in your IT department, but it also has an upside. By conducting audits on a regular basis, whether for internal security or external regulatory requirements, or even a one-time investigation of suspicious activity, you can ensure services are used in the right way, by the right people, and for the right purposes.

Regardless of whether you see auditing as an opportunity or a burden, it is generally a core, non-negotiable requirement for your API platform. So, make sure to adopt a solution such as AMPLIFY API Management that can capture and archive audit trails to streamline the process.

07

Make security a feature, not a barrier

In the old days of IT, a security architect could draw a boundary around the enterprise infrastructure. Everything outside the boundary was in the “red zone” and everything inside was in the “green zone.” A network firewall was the point of demarcation between the zones, and provided a somewhat false sense of security that everything in the green zone was safe from harm.

Today, there is no red or green zone. Thanks to APIs, enterprise IT extends beyond on-premise infrastructure and the firewall to the cloud, mobile devices, IoT, and various internal and external user communities. These connections must be secured, but you can’t do it with an old-fashioned firewall because there is no logical perimeter. Instead, security must be built in at the infrastructure level using an API gateway to control access and protect data as it flows to and from different systems, applications, and people.

A word of caution: It might be tempting to allow developers to build their own API security using a mix of security logic and business logic. This is not a manageable approach. A solution like AMPLIFY API Management enables you to build security into your API infrastructure and manage it centrally, putting control of crucial components such as API keys and user credentials firmly in the hands of operations and security staff, where it belongs.

Secure the data itself, so you can meet high-level protection and privacy requirements across a modern architecture that spans on-premise, cloud, mobile, and IoT.

08

Know your identity

One of the great benefits of APIs is their ease of use and reuse. It is relatively simple for developers to use APIs in a mobile app, or to call a cloud API from SalesForce.com or Amazon Web Services. The ease-of-use benefit also applies to end users, who now have much richer and more convenient experiences at their fingertips.

But ease of use comes with an identity problem. Users are now accessing services that span on-premise to cloud, with a variety of interfaces including mobile and wearables. It is important that these users are not forced to sign into each service individually; it's not only inconvenient, but they will also be tempted to use the same password everywhere, which creates a serious security issue if that password is compromised.

AMPLIFY API Management supports current identity standards such as OAuth 2.0 and address this problem with a capability called identity federation. In addition to enabling single sign-on across cloud, mobile, and on-premise applications, it also provides a security benefit by delivering varying degrees of authorization based on user or provider preferences. The "Login with Google" and "Login with Facebook" buttons we see all over the Internet are examples of single sign-on powered by APIs using standards such as OAuth and OpenID.

Implement identity federation and single sign-on at the infrastructure level to centralize management, simplify the user experience, and create a more secure environment.

Free developers to specialize in business logic without being expected to also define and manage policies.

09

Make policies separate from APIs

Exposing services as APIs makes them easier to manage, but also requires policies to be separate from the APIs. This is because policy enforcement will apply independently for each API depending on who's using it, and in what context or application.

Given that policies enforce both business and technical requirements, they need to be higher-level rules that both analysts and business stakeholders can understand. They also need to be flexible enough to be driven by data, roles, API usage, and other attributes. Otherwise, policies will take too long to build and change, slowing down API deployment times.

Policies should also be reusable to save time and money and prevent mistakes. An organization that has 100 API operations may only have a few reusable policies that can be enforced everywhere, such as a policy that throttles usage according to organization. Separating policy management from APIs themselves also brings other advantages. For example, it enables policy lifecycles to be managed separately from the API lifecycles, so a change to an API does not require a change to policies.

Policy management can be complex and requires specific skills. It makes sense to enable specialized staff to define policies using a tool like AMPLIFY API Management Policy Studio, which streamlines reusability and provides over 200 prebuilt policy filters.

10

Use throttling and quota management

When you open up transactions supported by internal systems to the outside world, you can easily see a 4-5x annual growth in transaction volumes, which can overwhelm your existing infrastructure if you don't plan ahead. That's why API throttling and quota management are key to a successful API program. They enable you to apply rules for tiered levels of access to an API, such as "Only 10,000 requests per day" or "1,000 API calls per second."

Throttling belongs on the network using an API gateway, not in the application itself. This is because by the time a traffic spike hits the API backend, it is often too late to do anything about it. At the network level, usage overages can be handled by queuing up traffic or by routing it elsewhere.

AMPLIFY API Management is an example of a solution that combines comprehensive policy-based throttling and quota management with full API lifecycle support, simplifying everything from initial rollout to viral adoption, and providing the enterprise-grade reliability you need as more of your business becomes digital.

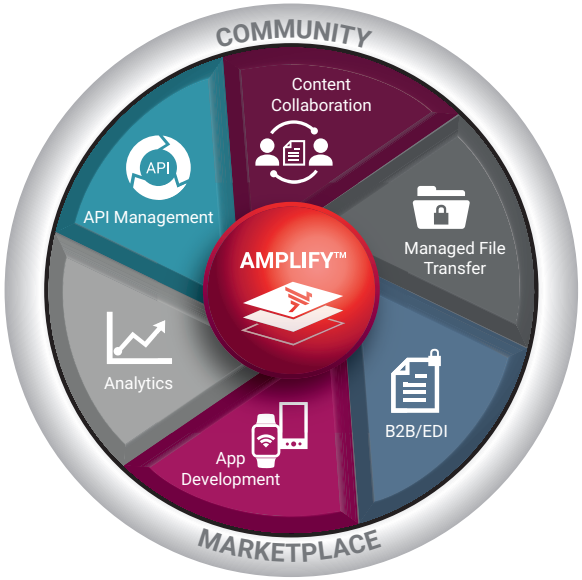
What's next?

APIs are an incredibly valuable tool for IT modernization — they unlock data, increase agility, encourage innovation, and speed time-to-value. This is why it is vitally important to take a thoughtful approach to managing the API-related tasks and cross-functional constituencies involved in bringing a product or solution from concept to delivery.

While this list isn't exhaustive by any means, it is a solid starting point for planning and implementing an API program that drives digital success. The pragmatic and strategic modernization approach defined by these time-tested best practices has been a guiding force in the development of AMPLIFY API Management, which provides a complete end-to-end set of services that simplifies access to enterprise data, integrates with full API lifecycle support, and streamlines app building to speed delivery of value to the business.

AMPLIFY API Management is part of the Axway AMPLIFY hybrid integration, engagement, and collaboration platform, which also includes Managed File Transfer, Analytics, App Development, B2B Integration, and Content Collaboration/EFSS solutions.

Enforce quotas and protect APIs from misuse with throttling based on priorities, current performance, and overall usage.



axway.com/api-management