RogueWave SOFTWARE

Akana

Enterprise API management defined

WHAT YOU THINK YOU KNOW ABOUT APIS

The digital platform is the new currency, and providing access to new revenue sources is fueling innovation and change. Managing this innovation and delivering value to the business requires a holistic view of what you have, what you need, and how to get there. Part of that assessment is considering the role that APIs play in creating a comprehensive, long-term strategy to design the digital platform.

> Application programming interfaces (APIs) make digital society and digital business work. They connect people, businesses and things. They enable new digital products and business models for services, and create new business channels. APIs make digital business work.[1]

The digital platform is the new currency, and providing access to new revenue sources is fueling innovation and change. Managing this innovation and delivering value to the business requires a holistic view of what you have, what you need, and how to get there. Part of that assessment is considering the role that APIs play in creating a comprehensive, long-term strategy to design the digital platform.

APIs are fundamental to extending business logic into new arenas and quickly capitalizing on opportunities. But it's more than just creating working APIs, it's about creating a strategy to address stakeholder concerns, and creating a robust infrastructure to support the new digital platform. And while the goals may be clear, there's no shortage of confusion and proclamations of just what "API management" really is. We'll define API management and suggest the best path to quickly capitalize on new revenue channels without assuming risk along the way.

Key takeaways

Understand. APIs are the foundational element of a digital platform. And the first step in understanding API management is defining API management. Various schools of thought surround the term, and many vendor-driven definitions fall short of a comprehensive approach to drive enterprise-scale business value.

Layers matter. Each layer in the API management architecture contributes to overall success, and carries its own set of stakeholders and costs. A thorough, resilient API management approach will weather short- and long-term storms to provide access to new revenue streams and market opportunity.

Define your own. Unsurprisingly, there is no one-size-fits-all approach. And, a duct tape and baling wire approach will show signs of stress under volume and expansion expectations. Balance expectations with what exists today, and what should be built.

In this guide, we'll define API management with actionable directives, and its challenges, with consideration criteria to craft a well-crafted, executable digital strategy.

[1] Top 10 Things CIOs Need to Know about APIs and the API Economy, Gartner, January 2017.

What is API management

Like most topics, there's a wide range of perceptions of what API management is, and what it can do.

The most common definitions of API management:

- APIs support external developers and should be published and marketed like a product
- APIs enable partners and should be kept private and exposed only to select groups
- APIs are just service-oriented architecture (SOA) reinvented

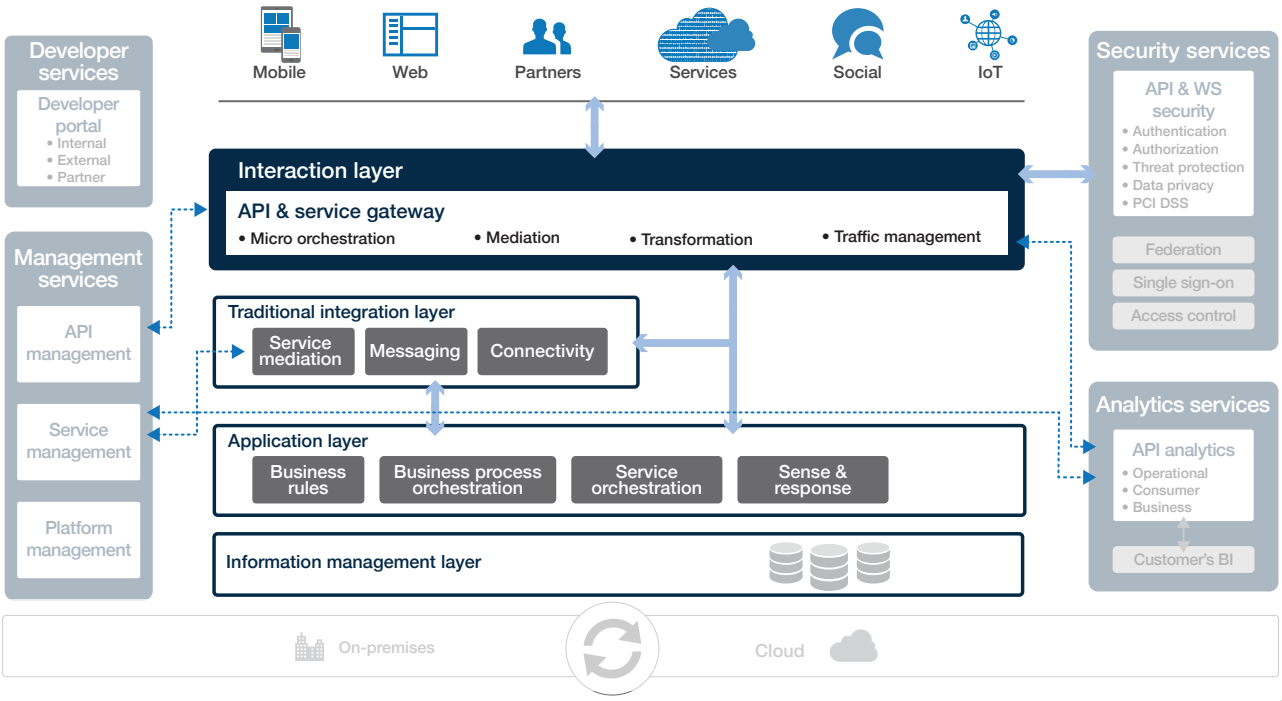
As with the many flavors of API use, there are more definitions to match. APIs can, and do, fill all these roles, forming a critical part of any digital transformation strategy. The trick is building the right infrastructure and services to enable current needs, while being flexible enough to adapt to changing needs in the future.

Moving beyond the developer portal

Effective API management means more than providing a good developer portal, or a high-performance gateway. Because it fills a number of key functions in the modern digital enterprise, the right infrastructure is a critical consideration. As the backbone of API management, the infrastructure allows organizations to take advantage of the wide array of things that APIs can do. This infrastructure serves not only application and API developers, but also enterprise architects, and operations and security teams.

A part of any successful digital platform design is the ability to meet business demands which are either limited or enhanced by the underlying architecture. We'll walk through the key layers to define the role of each in developing and executing a comprehensive API management strategy.

The core layers



Information management layer

Here there be giants. Giant data repositories that is. Modern digital organizations run on data and need a steady diet of advanced database systems to store and manage all of it. All applications need a reliable, high-performance data layer, requiring increasingly advanced (or simplified) data storage systems.

Directive: Address the disparate systems access data in consistent, coherent manner across without re-architecting infrastructure. Don't forget you have data that resides in the mainframe.

Application layer

This speaks for itself, it's where the applications that run the organization live. And most often, this is a mix of legacy and new(er) applications. While the appetite may be to replace legacy with new, state-of-the-art alternatives, time, and direct cost often prohibit it.

Directive: Adopt a digital strategy to embrace both existing and new applications to extract business value from each.

Integration layer

This is the realm of the increasingly rare enterprise service bus (ESB), and even more rare enterprise application integration (EAI) platform. Integration architects and developers live here, elbow deep in their cauldrons working arcane magic to expose services from legacy applications and data.

Directive: Understand the landscape of both legacy and new applications and the interaction between them, and build a strategy to encompass both, quickly.

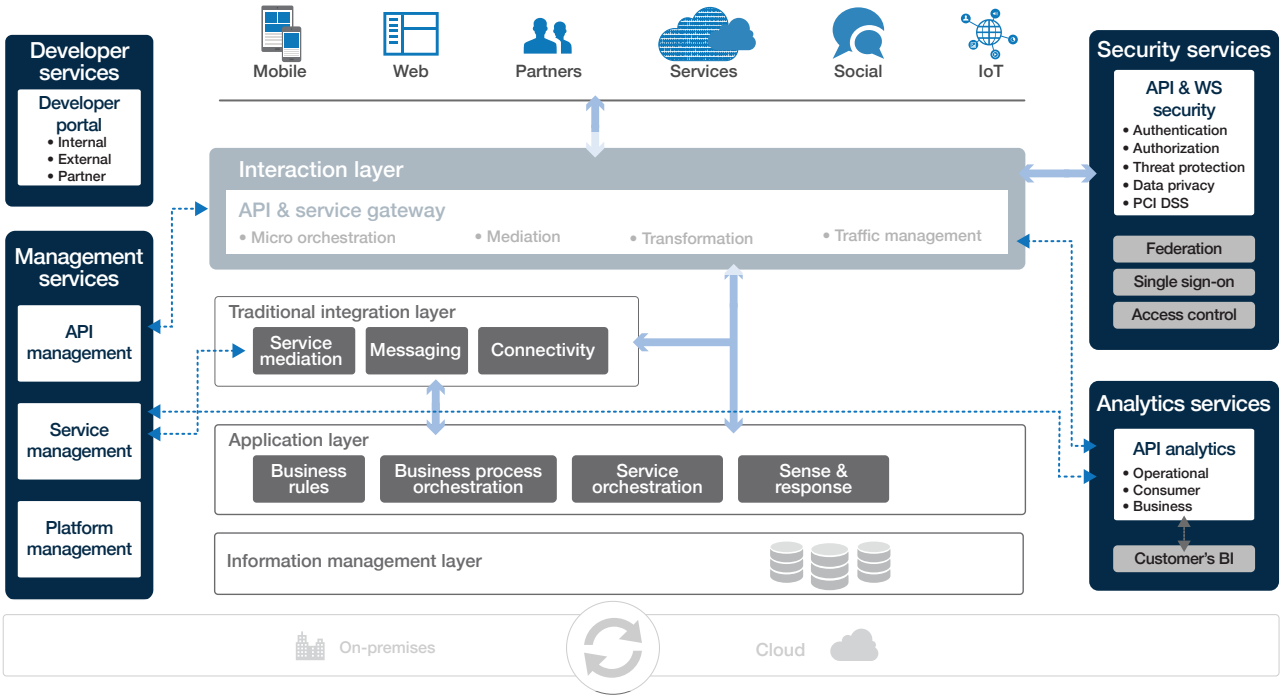
Interaction layer

This is where the applications and services used by customers, partners, and employees interact with business applications and data. Applications are no longer monolithic, inaccessible entities. Increasingly, these applications expose core functions and data via services that an API gateway can consume and aggregate with other services and capabilities to create APIs. The core of the interaction layer is the API management solution's gateway.

Directive: Ensure the API gateway provides moderated, secure, and well-defined access. Are the right people accessing what they need? And, are you measuring what matters to the business?

Services

In addition to the core layers, the diagram illustrates the surrounding services and how they support the core with value-added functionality. the solution should filter out defects introduced by other developers so only those defects introduced by a specific code change are returned to the developer.



Management services

All the technology that supports the digital business needs to be managed and monitored. This is where your centralized API management platform lives, controlling the gateway instances residing in the interaction layer. Provide configuration management and auditing, and operational monitoring across the organization. This layer includes core API management features ranging from design and definition, through monitoring and traffic shaping.

Directive: Assess stakeholder and application requirements to create an enterprise policy for management services.

Security services

This is the crux of the risk/reward scenario. Exposing data and applications creates a level of risk, but also provides new growth and revenue opportunities. Becoming a digital business forces the balance between providing APIs and protecting your customers and systems. Security services provide an underlying set of capabilities for user and application authentication and authorization, data privacy, auditing, and more. APIs are increasingly the key interaction point between applications and data, and with customers, partners, and employees, the API management solution needs to both provide and consume a range of security services.

Effective API management integrates with identity management systems to provide API and web services security, federation, and single-sign-on capabilities. It provides key management and cryptographic services for data privacy, and monitoring and auditing for API traffic and administrative activities.

Directive: Consider longer-term use for APIs when developing your security services. What may start as a simple security decision quickly becomes complex with myriad stakeholders and uses. Flexibility is key here, to avoid re-work and re-architecting while still moving fast to initial implementation.

Developer services

Where SOA and web services were all about the service provider, APIs are all about the consumer. One key to providing a good consumer experience is an intuitive developer portal allowing API developers to design, build, and document well-constructed APIs, and help app developers find and consume these APIs with minimal friction.

API management provides this social developer experience for both API and application developers, many of whom fill both roles, forming the foundation of a grass roots digital transformation initiative.

Directive: A well-crafted developer portal facilitates creating new APIs and promotes reuse of existing APIs through tagging and search.

Analytics services

A digital initiative is only as good as its measures of success. Establishing benchmarks and setting expectations relies on the ability to gather meaningful analytics. Analytics services provide dashboards built from information collected by the API platform and from other data feeds.

API management will likely not be the primary business intelligence (BI) system, but it will play a major role in delivering information, and in many cases, may provide all the data and reporting necessary to manage and optimize a digital strategy.

Directive: Establish early and dynamic measures for both the technology and the business outcomes. This year's goals are next year's benchmarks.

Architecture matters

A hybrid infrastructure supports the digital platform. Some applications will be on-premises, while others will be distributed across various cloud platforms and services. Regardless of the deployment, these distributed components need to be securely and reliably connected, with all the plumbing via APIs.

Developing and executing a well-considered digital strategy is the first step towards true transformation. Without it, there is risk of creating a piecemeal approach that may break or require ongoing upkeep. With a comprehensive strategy, the right tools, educated input across stakeholders, and an eyes wide open approach to the infrastructure, the API economy is accessible, secure, measured, and becomes part of your organizational DNA.

Enterprise API challenges

API management encompasses a broad suite of functionality and purposes. Enterprise API management extends beyond building and accessing APIs, into integration, mediation, security, analytics, and lifecycle and traffic management.

Creating a comprehensive, scaled, viable API strategy considers all of these aspects at the outset, and addresses each up front. Doing so will reduce friction from change, encourage stakeholder buy-in, and assure the business a comprehensive and well-executed digital transformation initiative.

As Forrester's Randy Heffner says,

> "APIs are critical for digital business. They create agility within an organization's solution architecture, which in turn enables faster delivery of business change. Even more important, APIs enable new angles into business strategy. But executing on an API strategy is hard work, complicated by the fact that organizations must create many APIs of many different types."[2]

In this section, we'll walk through the fundamentals of a well-crafted digital platform, built for scale and the long view. As part of that, we'll also offer guidance on best practices as well as considerations for designing a well-rounded, complete API strategy.

API design

The success of any API effort depends on the quality of the APIs it produces. At its core, an API platform needs to provide API developers with tools to design, test, and document APIs. It must also support the import and export of a wide range of API description languages (Swagger, RAML, WSDL, WADL) to ease exchange of API definitions between application and API developers working across different languages and environments.

Consideration criteria: Flexibility is key, with the ability to support multiple description languages, built-in testing, and methods to document APIs.

API security

APIs offer significant value to the enterprise, but can also introduce new risks and potential attack vectors. With constant and intense cyber-attacks, APIs offer a tempting pathway to data. Responsible API management requires:

- Protection of the information and capabilities exposed by the API from disclosure and misuse
- Restrictions on access to data and capabilities without incurring application overhead
- Limit access to APIs themselves to prevent attacks and misuse

Consideration criteria: A comprehensive API management plan including authentication, authorization, and ongoing diligence to secure key organizational assets.

[2] Keep API strategy on track with an API taxonomy, Randy Heffner, Forrester Research, May 2017.

Mediation and integration

APIs represent a new way of accessing core business data and capabilities, in both existing and new applications. Applications and data systems increasingly expose services, but these services are often poorly structured, or do not comply with industry or enterprise standards. Addressing existing applications requires more than simply creating an API call. Accessing legacy applications via a one-off API can be a quick fix, but will create overhead in the long-haul.

Consideration criteria: An enterprise-wide platform to mediate and integrate existing granular technical services to provide a faster pathway to digital transformation.

Traffic management

APIs drive new revenue sources and tap into a larger ecosystem. That's the good part. Challenges exist in managing the API traffic, especially across geographies and systems. Adopting a holistic approach will sidestep scale, technical debt, and SLA problems.

Consideration criteria: An effective traffic management solution to scale while retaining performance and maintainability, including enforcing quotas and global DNS.

Developer portal

Unlike their SOA predecessors, APIs are consumer-centric. APIs should be designed and constructed to meet developer needs, with user experience at the forefront. This means providing good documentation, tools for testing the API and its functional operation, the ability to see API traffic, discussion forums, and more. And, this all needs to be packaged to be easily searchable and accessible.

Consideration criteria: Flexibility to create a customized, branded developer portal to serve as both a platform to market APIs, and to meet the needs of the developer community.

API analytics

One of the key challenges lies in integrating business and operational analytics to extract meaningful insights from API data. API analytics also serve to make the APIs themselves better through intelligent monitoring and optimization. Advanced practitioners expand the measures beyond how the APIs are performing into how they are being used.

Consideration criteria: An extensible and configurable platform to perform complex custom analytics, or integrate with an existing BI platform to reduce infrastructure redundancy.

Lifecycle management

The API landscape is rapidly changing, with new protocols and access points arriving daily. APIs cross multiple functional units in an organization, requiring collaboration between lines of business, developers, and IT operations, assuring all requirements are clear, understood and implemented. Managing APIs throughout their lifecycle drives a faster return on investment, while making sure they are built to plan and to priority.

Consideration criteria: Comprehensive API lifecycle management, including visualizing interactions and dependencies, DevOps integration, and customizable workflows.

Deployment options

Organizations find themselves somewhere along a spectrum of transition to the cloud. Decisions about what, when, and how to deploy to the cloud are highly dependent on several internal factors, like application criticality, ability to install and manage software, cost management, and overall strategy. The same holds true for API management, where choice is critical. Cloud, on-premises, and hybrid deployments each offer their own advantages. With the hybrid model, vendors manage complex centralized components leaving the organizations free to run their own on-premises gateways to meet enterprise or regulatory requirements. Choice is key: The right decision today may be the wrong decision tomorrow.

Consideration criteria: API management solutions allowing for flexibility in deployment options to address internal and external mandates and regulations. Look for on-premises, SaaS and hybrid API management deployment.

Summary

APIs offer a powerful way to extend current operations and gain currency in complex and broad ecosystems. The price tag here is a possible oversimplification of the opportunity and the path to success. Seasoned practitioners build a complete, scalable API management strategy addressing the various elements for today, and into the future.

See how Rogue Wave Akana can help your team implement a successful API strategy and drive business innovation at roguewave.com.