WHITE PAPER • SEPTEMBER 2018

ca technologies

Choosing the Right API Management Solution for the Enterprise User

The API Opportunity

The application programming interface (API) may be an old concept, but it's one that's undergoing a transformation. More organizations, driven by mobile and cloud requirements, are opening their information assets to external developers. By exposing data through APIs to their developers, companies like eBay, Expedia and Salesforce are successfully achieving sales in new markets. According to ProgrammableWeb.com, the number of open APIs being offered publicly over the Internet now exceeds 19,933—up from just 32 in 2005.[1]

Opening APIs up to outside developers enables many technology startups to become platforms by fostering developer communities tied to their core data or application resources. This translates into new reach (think Twitter's rapid growth), revenue (think Salesforce.com's AppExchange) or end-user retention (think Facebook).

Using APIs to share information and functionality with outside developers isn't limited to technology startups. More enterprises, driven by cloud, mobile and partner integration initiatives, are using APIs to put themselves at the center of a developer ecosystem and—in so doing—drive new reach, revenue and retention possibilities around their information assets. However, unlike many startups, enterprises must approach API publishing with great caution because they have a good deal on the line, including reputation, regulation and the simultaneous needs of customers, partners, employees and shareholders.

The Enterprise API Management Challenge

Publishing APIs to an external developer community, be it partner or public, introduces a number of challenges and risks for the enterprise. How do you protect the information assets you're exposing from abuse or attack? How do you deliver your APIs as reliable services with no downtime that would impact your API users? How do you govern access and usage of your APIs in a consistent, policy-driven way? How do you make money from your APIs? How do you help developers discover your APIs and self-manage their access? Relevant to startups and enterprises alike, these questions are more acute and urgent for enterprise IT organizations. Not only because enterprises can't afford the reputation damage that may result from a rushed API management strategy, but because there are deliberate IT processes and safeguards that need to be upheld.

But no matter what type of API an enterprise wants to expose, it will need an API management solution that can address some basic functional areas:

- **API security**—Enterprises cannot afford misuse or abuse of their information or of any application resources exposed by an API.
- **API lifecycle management**—Enterprises need a way to ensure that API updates don't break when upgraded/versioned or moved between environments, geographies, data centers and the cloud.
- **API governance**—Through policy characteristics like metering, SLAs, availability and performance, enterprises need a way to control and track the broader operational character of how APIs get exposed to different partners and developers.
- **Deployment flexibility**—API management solutions should integrate with the enterprise's existing infrastructure.
- **Developer enablement and community building**—Enterprises need a way to bring developers on board, manage them and assist them in making the most of the exposed APIs.
- **API monetization**—For some enterprises, publishing APIs isn't enough. APIs also represent a new revenue opportunity, and different API management solutions enable monetization to different degrees.

For enterprises, addressing these functional requirements is non-negotiable. However, along with these functional requirements, an enterprise will expect its API management solution to deliver certain operational characteristics that are relevant to its unique IT experience.

- **Solution security**—Since API management solutions get deployed in the "demilitarized zone (DMZ)," enterprises will also need robust IT-class API solutions that can meet a range of security requirements, from penetration protection to PCI compliance to FIPS to HSM support for API key security.
- **Solution manageability**—Enterprises have development, test and production environments that span geographies, data centers and clouds, which means an API management solution must fit their specific development styles and processes.
- **Solution reliability**—Enterprises publishing APIs commercially expect five nines of uptime, if not greater, and can't afford outages.

What are the characteristics of a robust and available solution?

This white paper examines these different functional and operational requirements to give IT managers, Web managers and enterprise architects key information for selecting an API management solution.

API Management Solution Functional Requirements

API security

For prospective buyers seeking an API Management solution, security features are often top of mind—especially when the buyer is an enterprise looking to protect vital information exposed through an API independent of standards like simple object access protocol (SOAP), representational state transfer (REST) or Javascript® Object Notification (JSON). API security concerns begin with access control. For externally facing APIs, this means having the ability to:

- Accept different kinds of credentials for authentication
- Issue different kinds of credentials to developers
- Support different resource authorization schemes including federated ones like OAuth, OpenID Connect and SAML

For enterprises, this challenge is compounded by the need to integrate with existing identity infrastructure. Therefore, the overarching goal is to achieve flexibility and integration. In policy, there should be an ability to support different kinds of access tokens, and even move from one kind of developer API key to another, without touching code. The solution should be able to support a wide range of OAuth schemes, given that these are the standards for mobile security and APIs, but also handle a variety of OAuth styles like a keyed-hash message authentication code (HMAC) and combinations with enterprise standards like Security Assertion Markup Language (SAML). Of course, the API management solution also needs to work with pre-existing identity investments from companies like CA, IBM, Oracle and RSA.

But API security doesn't stop at access control. APIs provide the programmatic window into your data, which is why an enterprise-class API management solution will need to give the enterprise architect or security administrator fine-grained control over what data get exposed, how this information is kept confidential and how its transmission can be guaranteed against interception or tampering.

Moreover, API security rests on the integrity of both the API and the data/functionality it exposes, which necessitates an ability to ensure that APIs aren't compromised by attack, denial of service or misuse. A good API management solution will equip its operator with a wealth of threat-protection controls that will assure the availability and fidelity of the API and the communications it enables.

API lifecycle management

APIs aren't built in a vacuum. Like any application functionality, APIs demand their own development lifecycle, from design to coding to testing to deployment. This requires an ability to track changes to an API across that development lifecycle, whether the development process follows a waterfall or agile approach. That's why any API management solution needs to have fully functional workflows for:

- Planning and designing APIs using industry standards
- Integrating and securing APIs from end to end
- Testing, deploying and accommodating versioning and rollbacks
- Managing and monitoring API utilization, including reports and analytics

A fully functional API management solution should also be able to accommodate multiple versions in production simultaneously, either to accommodate older clients or different access technologies like SOAP, REST and JSON. A lifecycle management framework that can only accommodate localized development won't meet the needs of most modern enterprises. The cloud, both public and private, is growing in importance. Which means enterprises need an API management solution that can span testing and production in the cloud, as well as the ability to isolate API developers from the vagaries of network idiosyncrasies and topology.

API governance

Governance is a broad term often used to capture a wide range of management, process and visibility requirements, and defines the terms and conditions under which an API is exposed to one or more consumers. While governance encompasses security and lifecycle concepts, it also articulates various SLA, monitoring and reporting requirements. Furthermore, in the case of API management solutions, governance is relevant to the broader imperative of enabling differentiated terms and conditions for sharing API data and functionality to different consumers based on their identity, capability, subscription level or other transactional context that can be defined in policy.

Effective API governance is all about flexibility. The technology to control how APIs get shared should follow the preferences and processes of the enterprise and not the other way around. This means that an API management solution should be configurable around any SLA, security, log or other control using policy. Policy is at the heart of flexibility and ensures consistency from one implementation to the next. API management solutions that constrain administrators to course-grained controls without a full policy IDE limit what can be governed and how it can be controlled.

Deployment flexibility

Most enterprises have an existing infrastructure designed to complement the way they do business. As the enterprise moves toward an API management solution, it should evaluate solutions that plug into its existing environment. Architecture teams should be able to manage this solution as an extension of their infrastructure rather than as a separate environment. For more information on this level of integration, read the solution brief, "An Architect's Guide for Extending Your ESB/SOA Environment to Mobile, Cloud and IoT."

Developer enablement and community building

Governing an API ensures consistent control for the publisher, but if that API can't be easily discovered and consumed by external developers, the publisher risks that it will go unused. For that reason, most modern API Management solutions go beyond control features like security, lifecycle and governance to provide functionality that helps publishers expose information about their APIs to outside developers—often via developer portals. Providing a single point of interaction, a developer portal lets a developer register for an account, request an API access key, discover what APIs are available and see example code.

An API developer portal focused on enterprise usage should:

- Provide easily consumable mobile APIs (including for OAuth and OpenID Connect)
- Provide reporting and analytics for operators
- Easily enable business relationship management

Because different enterprises will come to API publishing with different experiences and priorities, a one-size-fits-all API portal approach will be no more attractive than a one-size-fits-all API security, lifecycle and governance framework. Which is why many enterprises will want to consider a decomposable API portal. This could mean a white-label portal that can be customized to suit a particular developer engagement strategy, or an API portal that can be consumed as discrete components by a pre-existing enterprise developer portal. Again, flexibility is the watchword.

API monetization

The concept of monetization is related to the idea of developer enablement. While many enterprises will want to foster adoption by allowing free access to their Web and mobile APIs, others will want to offer pay-per-use options for higher tiers of access. Again, there is no single right way of approaching the monetization problem. Some options are:

- A freemium model where usage is free below a certain threshold of data transmission or client requests
- Charging for specific levels of service guarantee or for priority over free users
- Offering premium information or functionality unavailable to non-paying customers

Regardless of the selected approach, the API management solution should be sophisticated enough to give an enterprise flexibility in how it sets up its revenue criteria. The solution should be able to:

- Capture a range of usage statistics to create a basis for measuring consumption
- Provide advanced SLA and class of service capabilities, allowing for traffic prioritization
- Compose virtual pay-only APIs that could be isolated for paying customers, without coding

API Management Solution Operational Requirements

Solution security

Because an API Management solution will often be the only piece of technology separating enterprise APIs from the outside world, the level of security the solution can confer on APIs will only be as strong as the security of the solution itself. If the solution is compromised, any security rendered onto the APIs will be similarly compromised. Therefore, enterprises examining API management solutions should make the solution's security an absolutely critical consideration.

These solutions will be interposed as intermediaries between the outside world and internal APIs, which means the first quality often evaluated is whether the solution itself can be compromised. This will depend on what kind of penetration testing the solution has undergone, how constrained access to the solution is and whether it has met key vulnerability assessments. Consideration should be given to Security Technical Implementation Guide (STIG) tested solutions, Payment Card Industry Data Security Standard (PCI DSS) certification for solutions that will pass credit card information, Federal Information Processing Standard (FIPS) compliance and Common Criteria certification for solutions that need to meet higher government security standards.

For most practical purposes, enterprises will often look at API management solutions that are proxy based for handling the intermediation of outside requests to an internal API. Intermediary-based API gateways offer the advantage of clear inline points of control and isolation, simplifying security certification and administration (just like with network firewalls). Some may also offer onboard hardware security module (HSM) support for encrypting API keys. And in many scenarios, API keys are the main line of authentication defense against abuse, so protecting those keys from theft through encryption is a prudent strategy.

Solution manageability

Unlike a typical startup, which may run its entire production website from a single Amazon instance or small hosted provider, an enterprise will typically have varied development and production environments, such as:

- Geographically distributed developer teams
- Production environments that span global data centers
- Cloud-based disaster recovery systems

Therefore, manageability will be central to any selection decision. Considerations like how you manage clusters of API gateways, how you load balance geographically, how you operate in a lights-out data center environment and how you handle peak loads will take priority over other features. Again, not all API management solutions are designed to cater to the specific needs of the enterprise, so before embarking on a particular path, you should take care to evaluate how various solutions support cluster management, failover, load bursting, disaster recovery and other operational management factors.

Solution reliability

Once an enterprise decides to embark on an API publishing program, it will effectively become a service provider to its API consumers who will come to rely on the enterprise and expect continuous uptime. In this context, an enterprise will inevitably place a considerable premium on reliability when selecting its API management solution. The enterprise will look for solutions where redundancy is built in and risk of downtime has been extremely minimized or eliminated. Enterprises looking at API management solutions may want to consider ones that can:

- Be deployed on premises, in the cloud or via a hybrid solution (API gateway on-premises, developer portal in the cloud)
- Provide complete redundancy, regardless of deployment model
- Integrate into your existing infrastructure
- Meet security mandates

Conclusions

Because no two enterprises have exactly the same needs or environment, there will never be a one-size-fits-all API management solution. However, all enterprises share a common need for excellence in functional capability and operation. For most organizations endeavoring to start publishing APIs externally, this will translate into a desire for a flexible, policy-driven API management solution that can meet the production rigor of a dial-tone-class service provider. Functionally, it will require an API management solution that can meet a variety of security prerequisites, accommodate common development lifecycles, be governable through policy, enable developer onboarding, foster developer engagement and support the option of monetization. Operationally, the API management solution should be secure, manageable and reliable.

Use independent research to help you choose an API management solution

Several of the top analyst firms cover API management technology and publish reports that compare vendors to help enterprises choose the best solutions for their digital strategies. IT review sites such as IT Central Station can also be an excellent information source for vendor comparisons and customer reviews.

To get complimentary copies of the top analyst vendor comparison reports and see what customers are saying about CA API Management, visit: ca.com/us/products/api-management/why-ca-api-management.html.

We welcome your questions, comments and general feedback.

To learn more, visit **ca.com/api**

Connect with CA Technologies

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit ca.com/customer-success. For more information about CA Technologies go to ca.com.

1 ProgrammableWeb API Directory, September 2018, www.programmableweb.com/apis/directory

ca technologies

CS200-366260_0618