5 Pillars of API Management

ca technologies

Introduction: Managing the new open enterprise

Realizing the Opportunities of the API Economy

Across industry sectors, the boundaries of the traditional enterprise are blurring, as organizations open up their on-premises data and application functionality to partner organizations, the Web, mobile apps, smart devices and the cloud. APIs (application programming interfaces) form the foundation of this new open enterprise, allowing enterprises to reuse their existing information assets across organizational boundaries.

Meeting the Challenges of Secure, Manageable API Publishing

APIs empower enterprises to quickly repurpose IT systems, add value to existing offerings and open new revenue streams. It should come as no surprise, though, that exposing on-premises systems via APIs also creates a range of new security and management challenges. The term “API Management” refers to a set of processes and technologies that have emerged in recent years to help enterprises meet these challenges.

API Management solutions aim to make it simple for even the most security-conscious organizations to open their information assets for use by partner organizations, third-party developers, mobile apps and cloud services, without impacting data security or the performance of backend systems. Full-featured API Management solutions also provide functionality for managing the developers who build applications that leverage enterprise APIs.

Overview: 5 Pillars of API Management

Expose Enterprise Data and Functionality in API-Friendly Formats

Convert complex on-premises application services into developer-friendly RESTful APIs.

Protect Information Assets Exposed via APIs to Prevent Misuse

Ensure that enterprise systems are protected against message-level attack and hijack.

Authorize Secure, Seamless Access for Valid Identities

Deploy strong access control, identity federation and social login functionality.

Optimize System Performance and Manage the API Lifecycle

Maintain the availability of backend systems for APIs, applications and end users.

Engage, Onboard, Educate and Manage Developers

Give developers the resources they need to create applications that deliver real value.

Expose Enterprise Data and Functionality in API-Friendly Formats

Convert complex on-premises application services into developer-friendly RESTful APIs

WHAT

Enterprise data and applications typically comprise a complex Web of standards, protocols, programming languages and file formats.

The first stage of API Management is presenting these diverse information assets in a format that developers can understand and leverage.

Commonly, this means publishing application programming interfaces that employ the REST protocol (RESTful APIs).

WHY

On-premises systems commonly rely on application services delivered in proprietary formats too verbose to work efficiently via the Web or mobile apps.

Application services associated with the common SOA (service oriented architecture) style generally employ the SOAP protocol, whereas Web/mobile devs rely on REST.

If APIs are not delivered in a format that internal and third-party developers can easily leverage, they will not facilitate the creation of any truly valuable new applications.

HOW

The most effective API Management solutions include functionality for presenting legacy enterprise services as RESTful APIs.

Typically, this will involve using a SOA or API Gateway to automatically convert data from the SOAP-based services into RESTful APIs.

To be truly effective, the Gateway should make it possible to efficiently compose RESTful APIs from “mash-ups” of multiple existing application services.

Learn More: **API Tech Talk:** Simplifying REST Adaptation.

Protect Information Assets Exposed via APIs to Prevent Misuse

Ensure that enterprise systems are protected against message-level attack and hijack

WHAT

Opening up enterprise information assets for use in new applications exposes them to many of the same security threats that plague the Web (e.g. viruses, DoS attacks).

Additionally, APIs create a range of new and unique security challenges that go beyond what enterprises are used to dealing with on the Web.

Perhaps the most essential function of API Management is the creation of a security layer to ensure that hackers are unable to access, misuse or attack exposed systems.

WHY

APIs are windows to applications and data, potentially providing hackers with a view into the inner workings of enterprise systems and a route to accessing those systems.

This creates the increased possibility that hackers will be able to steal confidential data, hijack public-facing interfaces for nefarious purposes or crash critical systems.

Conventional online security solutions designed for the Web do not cover all the potential threats created by API publishing, so specific API security must be implemented.

HOW

Arguably the key function of the type of API Gateway mentioned above is to inspect and filter all API traffic to identify then neutralize common or emerging threats.

To be effective, the Gateway should be designed and certified to tackle message-level, API-specific threats such as SQL Injection, Denial of Service attacks and viruses.

The Gateway's security functionality and threat profiles should also be easily updateable, to tackle new types of threats as they emerge.

Learn More: White Paper: Protecting Your APIs Against Attack & Hijack.

Authorize Secure, Seamless Access for Valid Identities

Deploy strong access control, identity federation and social login functionality

WHAT

Any enterprise that wants to fully secure its APIs against attack must give developers a framework for controlling how users access enterprise assets via these APIs.

This framework should balance backend security with end user experience by leveraging key identity and access management (IAM) standards such as OAuth.

For the best balance, the framework should be able to use existing IAM infrastructure and allow end users to gain access via enterprise single sign-on (SSO) or social logins.

WHY

Access control is the cornerstone of API security—the key is to prevent unauthorized users from gaining inappropriate levels of access to enterprise assets.

OAuth is especially useful as it allows publishers to flexibly implement appropriate levels of security and federate identities from existing IAM systems and social accounts.

Leveraging existing IAM infrastructure also cuts costs, reduces setup time and maximizes long-term manageability by preventing the creation of identity silos.

HOW

An API Gateway should feature out-of-the-box functionality for building an API-centric access control infrastructure using key standards and existing resources.

The Gateway should be able to integrate seamlessly with leading IAM systems like CA Single Sign-On (CA SSO), Oracle Access Manager, Microsoft Active Directory® and IBM Tivoli®.

It should also include configurable templates for implementing access control, SSO and social login in typical use cases, based on OAuth and other key standards.

Learn More: EBook: 5 OAuth Essentials for API Access Control.

Optimize System Performance and Manage the API Lifecycle

Maintain the availability of backend systems for APIs, applications and end users

WHAT

API traffic must be dealt with efficiently to ensure applications built against APIs work consistently and the performance of backend systems is not compromised.

Data from backend systems must be delivered in lightweight formats, optimized for usage patterns and filtered appropriately.

For long-term application viability, it is also necessary to carefully manage the lifecycle of APIs as they move through development, testing and production.

WHY

The introduction of Web and mobile apps that leverage backend systems can lead to sudden growth in IT traffic that can result in crashes and consequent unavailability.

It is vital to optimize the flow of API traffic, to ensure a satisfying and consistent user experience for developers, users of API-dependent apps and internal users alike.

Managing the API lifecycle, meanwhile, is crucial to ensuring existing applications do not break when APIs, clients and operating systems are updated.

HOW

An API Gateway used to compose and secure APIs is also ideally placed to control the flow of API traffic and manage the API lifecycle, to ensure availability and performance.

For performance management, the Gateway should have functionality for easy-to-scale routing, service mediation, message caching, call aggregation and traffic compression.

For lifecycle management, it should have features for dependency resolution and re-mapping plus automatic versioning, including roll-back to any previous version.

Engage, Onboard, Educate and Manage Developers

Give developers the resources they need to create applications that deliver real value

WHAT

Much of the true value of an organization's APIs comes from the developers who build Web and mobile applications or new enterprise systems against these APIs.

It is essential to target developers with the tools and materials they need in order to discover, learn about, try out and build apps against the organization's APIs.

These developers may be internal employees, partners, contractors or independent "long-tail" devs. Each group will require a particular set of resources targeted at its needs.

WHY

Developers are the lifeblood of any API publishing strategy. API publishers need devs to create apps that employees, partners and customers can actually use and benefit from.

To get developers creating truly valuable applications, the publisher must be able to attract talented developers and provide them with the tools needed to leverage the APIs.

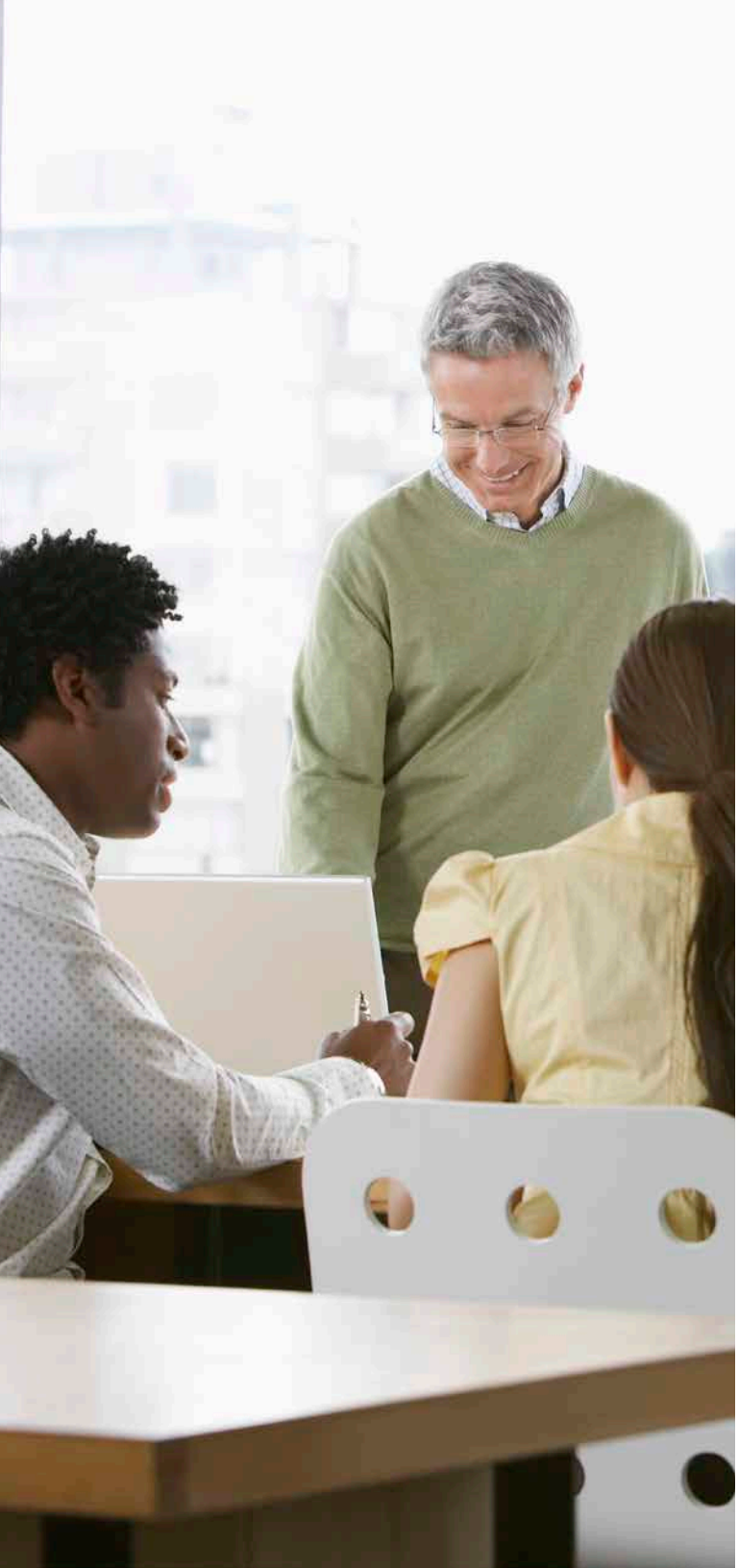
The more engaging and interactive the tools provided by the API publisher to enable and educate developers, the more useful the applications these developers deliver will be.

HOW

For internal and external developers alike, the most effective way to engage and educate developers is through a branded, interactive online portal.

This portal should make it simple for developers to register for APIs and access interactive documentation, sample apps, code examples, testing tools and discussion forums.

Effective API Management solutions include functionality that makes it simple to build a full-featured developer portal, pre-integrated into the API Gateway.



Conclusion: Deploying a Complete Solution for API Management

With Web, mobile and cloud technologies becoming increasingly essential to how the world does business, the API is emerging a key enabler for smart enterprises. To realize the value of APIs and avoid the pitfalls of exposing enterprise systems, it is vital to deploy technology that enables and simplifies key API Management processes related to service composition, security, performance optimization, lifecycle management and developer engagement.

The CA API Management Suite provides all the components required for effective, enterprise-level API Management, including a range of API Gateways designed to simplify all key API security and management processes. The CA API Management Suite also includes an API Portal for developer engagement and management and an OAuth Toolkit for ensuring secure, standards-based access management for enterprise APIs.

Additionally, the CA API Management Suite offers:

- A choice of on-premises, cloud or hybrid deployments
- Military-grade data and application security
- Analytics on API usage
- Operations management that can span distributed datacenters and clouds
- Application adaptation and interface management with advanced SOA connectivity

About CA API Management

The API economy is exploding, mobile devices are proliferating across the workplace and large organizations are moving critical IT infrastructure to the cloud. This is creating the need for technology able to securely connect with external developers, mobile apps and cloud services. CA Technologies is at the cutting edge of this red-hot market.

The CA Technologies industry-leading Gateway products make it simple for enterprises to share data with customers, mobile apps and cloud services. Delivered as hardware networking appliances, virtual appliances or as software, our products are helping large organizations open up to the Web, mobile networks and the cloud, without jeopardizing security or performance.

In September 2014, CA API Gateway was recognized as a Leader in the API Management space by top analyst firm Forrester Research, in its The Forrester Wave: API Management Platforms Q3 2014 report.[1] CA API Management is a key component of the solutions that CA Technologies provides for enterprises that need to secure and manage complex IT environments to support agile business processes.

Learn more at ca.com/api.

[1] Forrester Research, Inc., The Forrester Wave: API Management Platforms, Q3 2014, September 29, 2014

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-132272_0615

ca technologies