WHITE PAPER • JANUARY 2018

Secure Mobile Access for Enterprise Employees

Simplifying Security and Management for Mobile Apps

Bill Oakes
API Management Product Marketing

Table of Contents

Executive Summary

Challenge

In recent years, mobile technology has revolutionized the corporate IT landscape. As mobile devices began to proliferate, enterprises refused many emerging mobile device features in an attempt to control their impact to the organization. But when CxOs started to visit IT demanding that their devices be enabled for email, IT caved, moving to mobile device management (MDM) to help protect liability. Very quickly, the concept of consumerization of IT emerged, forcing IT to not only embrace mobile devices but to transform their infrastructure to maximize productivity, efficiency and availability.

Opportunity

The true potential of mobile devices is in the apps they run. To get real value from mobile, enterprises are providing their employees with apps that can access corporate resources and information, even when the devices being used are not under corporate control. For many enterprises, this creates significant challenges related to security and information adaptation.

Benefits

Corporate data and application functionality can be made available to apps residing on employees' mobile devices by using APIs to expose on-premises systems and data to developers building mobile apps. Using APIs for enterprise/mobile integration generally requires a specific solution to ensure security and governance continuity. In this context, an API gateway can be optimized for mobile devices to address identity, data and application adaptation and access control across an API and/or microservices.

This white paper explores the challenges of enterprise mobility and provides practical advice on how to optimize an API gateway for mobile devices and apps. It showcases real use cases to demonstrate how enterprises benefit from providing employees with mission-critical mobile apps.

SECTION 1

Mobile Apps: Innovation Through Consumerization

Benefits of Everywhere Access

Mobile technology presents organizations with potential efficiencies that are simply too beneficial to ignore. One customer in the health insurance sector provides a great example. The customer's representatives make around 2 million house calls every year. Traditionally, member data gathered at a house call would be recorded by hand and keyed into a central database when the representative returned to the office.

It was clear that providing representatives with mobile technology would make this process quicker and more accurate. Therefore, the company created an iPad app designed to help representatives interactively assess members' needs. This application is now helping to reduce time spent on administrative tasks and increase time spent with members—leading to more efficient decision making and enhanced member services.

In this example, a large organization benefited from providing its staff with mobile devices. This case is certainly not unique—many enterprise organizations are seeing similar benefits from equipping their sales staff with mobile technology. However, in many cases, enterprises are presented with the mobile workforce as a foregone conclusion and are specifically benefitting from the fact that employees are using their own devices in the workplace.

The Mobile Movement

BYOD is old news. The reality is that, for many of us, the new desktop is the mobile device. Technological innovations are emerging directly from consumer electronics, while consumer technologies are being embraced by the business world—and IT is transforming how it works to keep up with technology.

And technology marches on. Individuals are not waiting or asking for their IT department's permission to use new devices for work—they are just doing so. And they are doing so en masse. In 2014, mobile app usage surpassed desktop, and this trend hasn't changed four years later. Enterprises must take a mobile-first approach or risk falling behind.

Smart organizations see mobile for the massive opportunity it is. The use case described earlier shows the great benefits an organization can gain from providing its employees with mobile devices. Now, imagine the additional cost savings and efficiencies that can be gained from leveraging mobile devices employees have already purchased for personal use and are already familiar with on a technical level.

Of course, as the use case also shows us, mobile devices are only half the story. Hardware (specifically the emergence of the iPad and similar tablets) has been the catalyst for a revolution in enterprise mobility, but apps are the real payoff. To truly benefit from mobile, enterprises need to build apps specifically designed to help their employees work more effectively.

SECTION 2

Mobile Integration: Using Apps to Leverage Internal Resources

Information Assets and Services

So how do you build apps to enable the mobile workforce? In the past, enterprise IT departments all too often reacted to any new technology paradigm with a "rip and replace" approach—accommodating the new technology by attempting to build new IT systems or port old processes to new packaged platforms. This approach was time- and resource-intensive, often yielding incompatible systems and limited returns. A more flexible, efficient alternative was clearly needed.

Today, more and more enterprise architects have adopted an approach driven by APIs, and now microservices, in order to make data and application functionality available across internal and third-party systems and services. These architects create services that allow them to easily consume and re-use existing IT investments while creating new business processes by composing multiple operations and configuring them together into higher-level applications.

This development process is much more efficient, while allowing for a high degree of integration and customization—and it eliminates the need to "rip and replace," as APIs and microservices can be continuously updated and configured by developers as enterprise needs evolve.

This approach can be leveraged in the enterprise mobile context. Key data and applications can be extended and delivered as services, via APIs, to mobile apps.

More specifically, services can be quickly adapted into mobile-friendly APIs that securely expose internal enterprise information assets to mobile developers and the apps they build, using formats and security models that mobile devices can easily consume.

The mission-critical and changing nature of enterprise APIs and microservices dictates that they be managed and secured—typically via an API gateway that offers a centralized location for this security and governance.

Using APIs to Enable Enterprise Mobility

The services associated with an API gateway may be exposed internally or externally. Opening APIs to internal and external developers simplifies the creation of applications able to integrate with the enterprise's information assets to benefit a range of stakeholders, from employees to partners to customers. These applications may reside within the enterprise, at partner organizations, on the Web, in the cloud or on mobile devices.

For the sake of this white paper, we are primarily concerned with the creation of mobile apps by internal developers for use by employees (and partners) across the extended enterprise. A use case from another customer demonstrates how effective this strategy can be. The customer, one of the largest U.S.-based airlines, launched an ambitious API publishing program targeted at both internal and external developers: employees and customers.

Internally, these APIs allowed the company's developers to create a range of apps designed to enable the mobile workforce. For example, they created an app designed to help ground crews expedite the loading and unloading of baggage from flights, decreasing baggage handling times to maximize customer satisfaction. Externally, apps were developed that gave customers fuller itinerary management capabilities by combining the airline's schedule and ticket information with value-added information provided by outside sources.

Our role was to help the company address the challenges of publishing, integrating and securing these APIs, thereby enhancing key business processes without stifling innovation or compromising enterprise data.

SECTION 3

Addressing the Challenges of Enterprise/Mobile Integration

APIs provide the technical components internal developers need to integrate on-premises information assets with the apps they build for employee mobile devices. However, for this approach to work, four challenges must be met:

1. Adapting internal information assets for mobile consumption
2. Optimizing app performance when accessing enterprise resources
3. Securing mobile access to enterprise APIs
4. Making APIs discoverable and consumable for developers

1. Adapting internal information assets for mobile consumption

There are a number of challenges associated with making internal information assets usable by a mobile app. First, information assets in legacy formats need to be reworked as RESTful APIs that can be accessed as XML or—increasingly—JSON data messaging formats. This requires an efficient system for translating any back end information asset into a RESTful API that communicates over HTTP/S using JSON messaging.

It may also require a reconstitution or "re-composition" of internal information assets into new APIs customized to specific devices or apps. As the number of connected devices in the enterprise grows exponentially, "mobile" no longer refers only to smartphones. Devices and applications connected by the Internet of Things (IoT) now communicate and share data over a range of unique protocols and transport mechanisms that must be centrally integrated, managed and secured. For legacy systems and new connected devices to interact, enterprise applications and services must be configured to be compatible with data sources stemming from a range of supported device types and users.

This kind of data translation and API re-composition is ideally suited to API gateways, as they can be used to integrate applications translating data formats, orchestrating service interactions, virtualizing APIs and bridging different protocols and transports. Connecting a mobile app to an enterprise application is therefore rendered as just another integration problem. Some API gateways can similarly handle this kind of integration challenge.

2. Optimizing app performance when accessing enterprise resources

When integrating enterprise applications with mobile apps, performance is always a key consideration. An enterprise that is publishing mobile APIs will need ways to accelerate the delivery of data while reducing data traffic volumes because:

- The data will be traveling on relatively low-bandwidth mobile networks.
- Mobile usage can scale geometrically as the enterprise opens applications first to employees and then consumers, placing a heavy burden on these applications.

Again, an API gateway will almost certainly help the enterprise address these challenges. This is because some API gateways deliver a wide range of functionality for managing and optimizing data traffic loads, including:

- Throttling requests that exceed a certain threshold or shaping traffic based on considerations like location, time of day or subscriber level, thus selectively limiting performance-sapping load on back-end applications.
- Using sophisticated caching capabilities in order to (a) minimize the number of requests that get passed to back-end applications and (b) improve latency response times.

- Compressing data on the fly to minimize traffic sent to and from a mobile app. Some API gateways can load balance across multiple back-end application instances, ensuring more evenly distributed load across APIs and simplifying scale-out of back-end applications.
- Prioritizing API calls to ensure that paid subscribers or key users receive a consistent quality of service, with guaranteed access to enterprise resources. This function can also be used to reserve API access capacity based on a specific traffic type.

When deployed in the cloud, some API gateways can also help auto-scale back-end services and even dynamically add gateway nodes to a cluster in order to process more traffic.

3. Securing mobile access to enterprise APIs

The mobile device is, well, mobile. And unlike a desktop (or, to a lesser degree, a laptop), it's not unusual for mobile devices to be frequently lost or stolen. So while security is a major concern whenever an application outside the DMZ needs to access information inside the enterprise, it's even more important for mobile devices. But implementing security without negatively impacting the user experience can be challenging.

APIs have to be protected against attack or misuse. The data transmitted to and from the API needs to be secured (through encryption, tokenization or redaction) and its integrity verified. And access to the information resources exposed via the APIs will need to be controlled at a granular level, based on the identity or role of the requestor.

Control of access to information exposed through an API is an even thornier issue. A user may use different apps on different devices to access a piece of data or functionality exposed through the same enterprise API. Those apps can be built by different groups or designed as mash-ups of different information assets.

Each app may use a different user ID, complicating the identification of the user. Furthermore, users dislike retyping app-specific identities on mobile devices and would prefer to delegate that authentication to a pre-existing trusted app.

To address the dilemmas created by the need to provide flexible yet secure access control for APIs in these more complicated mobile (and similar Web-based) scenarios, a new standard—OAuth—has emerged.

OAuth is the protocol that makes it possible to identify a user, and the resources that user is interested in accessing, via an intermediate app, without necessarily requiring the user to enter a username and password combination specific to the app.

The OAuth specification allows enterprises to grant authorization rights to an app based on (a) the user's pre-existing credentials within the organization and (b) a trust relationship between the enterprise and the intermediate app. This kind of transitive trust and rights passing happens in the background—the user only needs to establish trust for the intermediate app once.

While OAuth solves prickly access problems particular to mobile app dynamics, it remains complicated for enterprises to set up. In particular, there are challenges around integrating OAuth with an enterprise's existing identity infrastructure. To address these challenges, an API gateway may come with an OAuth Token Server, which will simplify the process of deploying and maintaining an OAuth access infrastructure on top of an API.

OpenID Connect has recently emerged as a standard mobile security protocol. OpenID Connect is a simple identity layer that leverages the OAuth protocol and lets developers authenticate their users across websites and apps without having to own and manage password files. Again, an API gateway may also provide a toolkit to implement OpenID Connect for mobile apps.

Identity and access are covered with these two protocols, but access control is normally just the beginning of the security challenges facing an enterprise—and these challenges are exacerbated in a mobile scenario, where the enterprise cannot lock down remote mobile and IoT devices the way it could with desktop computers. Key challenges include:

- Protecting against denial of service, cross-site scripting, SQL injection and URL tampering attacks
- Preventing accidental damage caused by poorly written apps
- Deploying a scalable system for preserving data security in communication to and from APIs in order to meet data privacy standards like FIPS, PCI-DSS and HIPAA

Again, some API gateways help enterprises address these challenges by providing a range of API, data and URL security policies.

4. Making APIs discoverable and consumable for developers

A critical element in enabling integration between mobile apps and enterprise services occurs before the first byte of data is exchanged. In order to build mobile apps based on enterprise APIs, developers and developer teams need certain information on the APIs they can call. This may include information on the functionality an API exposes, the data it returns and best practices for its use.

Enterprises therefore need systems for developer on-boarding (i.e., registering developers to use an API) and management. This can be achieved by deploying an API portal—a secured central location where developers go to get documentation on an API, test its behavior, sign up for usage, track API health and collaborate with other developers. Many API gateway vendors provide integrated API portals to ease the governance of APIs and the developers that use them.

Simplifying Secure Enterprise Mobility With an API Gateway Optimized for Mobile Access

As we have seen, the type of infrastructure that has emerged over the last decade or so to enable secure access to APIs can be applied to mobile app integration. A DMZ-deployed API gateway with an integrated OAuth Token Server and API portal provides the basic requirements for mobile, addressing the specific data adaptation, performance optimization, security and developer management challenges associated with exposing internal information assets to mobile developers and apps.

SECTION 4

Advanced Tools for Enhanced Mobile Security

While following the above tactics will provide the basic platform necessary for enabling mobile devices and apps in the enterprise, some API gateway vendors provide advanced functionality:

1. Hardened security for regulated industries and public sector
2. Software development kits (SDKs) for integration with single sign-on (SSO)
3. SDKs for dynamic secured collaboration
4. Integration with hardware security functionality
5. Integration with back-end systems for predictive analytics

1. Hardened security for regulated industries and public sector

Some API gateways provide the security required by regulated industries, including public sector agencies such as the United States Department of Defense, Victoria Police Service and United States Customs. These gateways are likely FIPS 140-2 certified (a government security standard for cryptography). Policies should be available to protect against Web-based threats, ensure proper authentication and authorization (and logging) and require VPN for secured communications. Many agencies additionally require that the API gateway meet protection profiles as identified by the National Information Assurance Partnership (NIAP). A third-party product evaluator approved by the United States, NIAP tests solutions to ensure that they meet the hardened requirements of some government agencies. Failure to complete the test or exclusion from the approved list can prevent an API gateway implementation, regardless of any other consideration.

2. SDKs for integration with single sign-on (SSO)

SSO is a key component of the security mandates for many enterprises. Some API gateways include SDKs that allow developers to easily integrate authentication calls into mobile applications—both removing the burden of security from the developer and providing a seamless integration into the enterprise's identity and access management system—allowing the development team to focus on customer experience.

3. SDKs for dynamic secured collaboration

Many enterprises have corporate intellectual property (IP) that they don't want exposed on a mobile device. The ability to flag such files as confidential and to dynamically create/delete secured storage on mobile devices can dramatically reduce the risk of lost IP. Likewise, messaging: Corporate executives often need to communicate securely, and the industry standard, Short Message Services (SMS), fails in that regard. The ability to integrate secured messaging into an enterprise application again reduces corporate risk of IP loss.

4. Integration with hardware security functionality

Another benefit mobile SDKs can provide is integration with mobile device hardware such as TouchID or FaceID on Apple mobile products, or supported biometrics on devices running Android 6.0 (Marshmallow). For regulated industries such as financial services and healthcare, the ability to require multi-factor authentication dramatically reduces both enterprise and customer risk of lost PII or financial information.

5. Integration with back-end systems for predictive analytics

Risk analytics engines ensure that a mobile device is in the hands of the right customer. Such engines, often used by financial institutions, may note that a transaction falls outside of normal usage of that customer and require additional validation (such as a one-time password) in order to complete that transaction. Integrating such calls via a mobile SDK both reduces risk and decreases time-to-market for such apps.

One systems integrator summed up the value of mobile SDKs when building mobile applications by stating, "SDKs dramatically decrease our overhead and time to market. High-risk, complex and time-consuming features like authentication, security, messaging and groups are built in, allowing our team to focus on the customer experience and delivering the best product."

SECTION 5

Conclusions

As mobile utilization continues to proliferate and enterprises move to support it, API gateways are an excellent solution for addressing the challenges of enterprise/mobile integration and can also be used to enhance mobile security to integrate mobile devices, apps and users with enterprise identity and access management systems; provide secure collaboration; integrate with advanced authorization techniques for risk management; and meet the requirements of regulated industries.

To learn more about how CA Technologies provides solutions that solve the challenges described in this white paper, please visit www.ca.com/api.

SECTION 6

About the Author

Bill Oakes, CISSP, is director for product marketing for API management at CA Technologies. He joined CA with more than 15 years of experience in security and mobility marketing. In his role, he is responsible for messaging, positioning and evangelism of the best API management solution on the market today.

Prior to joining CA, Bill was responsible for product marketing for the developer platform at Good Technologies—a secure mobile email company—rolling out the initial positioning, messaging and strategy of Good's foray into developer/ISV markets. Prior to Good, Bill held product/solutions marketing positions at Blue Coat Systems, a Web security company with real-time defense against malware and Web-based threats.

Weekends will almost certainly find Bill riding with his Harley club—or possibly teaching people how to teach people to blow bubbles underwater.

For more information, please visit **ca.com/api**