Enterprise On The Go: 5 Essentials For BYOD & Mobile Enablement

Introduction: The Opportunities & Challenges of Enterprise Mobility

Apps & the Enterprise

The existence of smartphones and tablets able to run lightweight apps has created a quantum leap in the potential of mobile devices in the workplace. Apps present enterprises with clear benefits in terms of maximizing employee connectivity, availability, flexibility and productivity.

Many enterprises have begun investigating how they can realize these benefits. Meanwhile, employees have independently started using their personal devices for work – launching the BYOD ("bring-your-own-device") movement.

Example 1: Mobile Field Enablement for Health Insurance
A leading health insurance provider gave field operatives Apple iPads with a custom app that made it possible to enter customer data into a central database when making house calls. This allowed operatives to spend more time on customer service and less on administrative tasks, while increasing the accuracy of data collected.

Example 2: Baggage Handling App
A major US airline created an app that allowed its baggage handlers to access critical flight information via their mobile phones. The app allowed ground crews to better expedite the loading and unloading of baggage from flights, decreasing baggage handling times and therefore increasing customer satisfaction.

Introduction: The Opportunities & Challenges of Enterprise Mobility

The Challenges of Enterprise Mobility

Enterprises are finding that, to get true, measurable benefits from employee mobility and BYOD, they need ways to:

- Deploy apps, like those described above, which give employees mobile access to missioncritical data and functionality from on-premise applications

- Ensure these apps provide seamless access to the necessary data and functionality without compromising the security of on-premise systems

So, how do enterprises approach these challenges? For many organizations, dipping a toe into the onrushing torrent of mobile innovation can seem daunting. However, if viewed historically, the challenges of enterprise mobility start to seem much more approachable.

Mobile & the Open Enterprise

Since the dawn of the World Wide Web, boundaries surrounding enterprises' information assets have become far less rigid. More recently, Web-like IT concepts such as Service Oriented Architecture (SOA) have become central to how enterprises provide access to these assets.

In these Web-like architectures, enterprises use application programming interfaces (APIs) to open their on-premise data and application functionality for reuse in new on-premise systems and partner applications, as well as online tools open to customers or even the general public.

Clearly, opening on-premise systems in this way creates serious security and management challenges for enterprises. To help organizations address these challenges, new technology paradigms and product categories have emerged – notably API Management.

In this eBook, we describe five key ways enterprises can securely and manageably leverage their existing information assets – not just SOA services but any legacy systems – in order to give their employees "anywhere access" to key data and application functionality.

Overview: 5 Essentials for BYOD & Mobile Enablement

Expose Internal Applications as APIs

Publish APIs to expose on-premise applications as reusable services

Optimize APIs for Mobile

Efficiently deliver legacy application functionality via mobile ready APIs

Secure & Manage Data Exposed via Mobile APIs

Control the flow of data to protect APIs against attack and to ensure availability

Institute Identity & Access Control Systems

Secure enterprise systems against unauthorized use while ensuring seamless Mobile Access

Enable & Educate App Developers

Give your developers access to the resources they need to create really useful apps

CHAPTER 1:

Expose Internal Applications as APIs

Publish APIs to expose on-premise applications as reusable services

WHAT

In SOA, enterprise architects maximize IT efficiency by making application data and functionality available for reuse in other applications.

This is achieved via programming interfaces that deliver applications as reusable “services”. Increasingly, APIs are used to make these services available outside enterprise boundaries.

Even for organizations that do not have existing SOA systems, the API approach can be leveraged relatively easily to reuse legacy data and applications in mobile apps.

WHY

This focus on reuse emerged so that enterprise architects could adapt to the emergence of powerful new technology paradigms without having to start from scratch each time.

The mobile app represents exactly the type of paradigm the API-based approach to enterprise architecture was designed to prepare enterprises for.

So, for many enterprises, the key to responding to the app paradigm and BYOD will be repurposing existing interfaces – or designing new APIs, when necessary.

HOW

In most cases, the new APIs will be designed specifically to enable in-house or contracted developers to build apps that leverage internal information assets.

Interfaces should be designed specifically for mobile. For example, it may be necessary to translate application data from the SOAP protocol to enable REST-style interactions.

As the APIs will expose enterprise information assets to apps via public mobile networks, strong data security and access control measures must be put in place.

LEARN MORE | White Paper: Secure Mobile Access for Enterprise Employees
Simplify security and management for enterprise-level apps and BYOD

CHAPTER 2:

Optimize APIs for Mobile

Efficiently deliver legacy application functionality via mobile ready APIs

WHAT

Existing enterprise APIs are often unsuitable for exposing services to app developers. Therefore, a mobile strategy will require the creation of new mobile ready interfaces.

Typically, this will involve enabling translation from SOAP (or other legacy protocols) to REST and using filtering, caching and compression to deliver data in lighter formats.

It may also involve delivering functionality for streaming protocols and services that are particularly useful in mobile apps e.g. WebSocket, XMPP, Apple Push Notifications.

WHY

Enterprise data must be delivered via mobilefriendly interaction styles and protocols (REST, JSON etc.) to enable the creation of apps that effectively leverage the data.

Also, data must be delivered in appropriately lightweight formats in order for apps to run stably, efficiently and reliably enough for employees to get true value from them.

By leveraging new mobile-friendly protocols and mobile-specific services, developers can create apps that add new, interactive value to existing application functionality.

HOW

The process of optimizing APIs for mobile apps can be greatly simplified by deploying an API Gateway, either as a physical networking appliance or as a virtual machine.

To be effective for mobile, an API Gateway should be able automate the process of translating legacy services to mobile-friendly protocols and lightweight data formats.

API Gateways designed specifically with mobile in mind should also deliver out-of-the-box functionality for common streaming protocols and notification systems.

CHAPTER 3:

Secure & Manage Data Exposed via Mobile APIs

Control the flow of data to protect APIs against attack and to ensure availability

WHAT

Security is always an issue when an enterprise exposes its information assets via APIs, particularly when these assets will be accessed outside the company firewall.

Therefore, in any API-based scenario, security measures must be taken to protect the APIs against denial of service, SQL injection and other types of attack or misuse.

Additionally, data throughput should be throttled to make sure services remain consistently available, maintaining compliance with service level agreements (SLAs).

WHY

Clearly, enterprises have a strong interest in ensuring the security of their mission-critical systems, if only to meet data privacy standards and regulatory requirements.

Concerns over API security are amplified in mobile scenarios, where data travels over consumerfocused wireless communications networks.

These concerns are only made more severe by BYOD because enterprises cannot lock down personal mobile devices the way they might with corporate hardware.

HOW

As well as optimizing the performance of mobile APIs, an API Gateway can significantly simplify the process of securing APIs against attack and misuse.

A full-functioned API Gateway should have features for preventing all common attacks and should be easy to update, ensuring the latest threats are always covered.

An API Gateway should ideally be certified to meet the widest possible range of security standards. FIPS and PCI-DSS provide particularly notable examples.

CHAPTER 4:

Institute Identity & Access Control Systems

Secure enterprise systems against unauthorized use while ensuring seamless Mobile Access

WHAT

Access is central to enterprise mobile app effectiveness. For apps to work, employees must be able to seamlessly access on-premise data beyond the enterprise perimeter.

At the same time, data should only be exposed on a temporary basis and access to the data should be strictly limited to authorized users.

To ensure this balance between effectiveness and data security, apps must be able to leverage strong identity and access management (IAM) functionality.

WHY

Exposing on-premise systems to mobile devices via public wireless networks creates a significant risk of unauthorized parties accessing sensitive enterprise data.

However, the value of mobile technology comes from the flexibility, seamless convenience and level of personal control it provides – access control should not impact this.

This security/openness balance can only be achieved via the type of authentication and authorization functionality already used by common enterprise IAM systems.

HOW

Mobile device management (MDM) solutions are popular but they usually take a somewhat inflexible, BYOD-unfriendly approach to access control.

A more constructive approach is to use a Gateway to flexibly enforce API access policies based on user, group, attributes and even geo-location (rather than by device).

For truly seamless access, the Gateway must also be able to integrate with on-premise IAM systems and leverage API-friendly standards like OAuth and OpenID Connect.

CHAPTER 5:

Enable & Educate App Developers

Give your developers access to the resources they need to create really useful apps

WHAT

Many consumer-focused apps result from organizations opening their APIs to the “long tail” of lone hackers, working to their own specifications and schedules.

Employee-focused enterprise apps are more likely to result from APIs published privately to internal resources or devs contracted to deliver specific corporate requirements.

In either case, it is essential to provide developers with the tools and materials they need in order to access, learn about, try out and build apps against your mobile APIs.

WHY

Developers are the lifeblood of any mobile app strategy. To get real results, you need developers to create apps your employees can actually use and benefit from.

To get developers creating apps your employees can use, you need to provide them with well-designed mobile APIs and any tools necessary to effectively leverage these APIs.

The better the APIs you design and the more tools you provide to enable and educate your developers, the more useful the apps these developers deliver will be.

HOW

An organization targeting long-tail developers will commonly deliver APIs via an online portal where devs can register for, learn about and test the APIs.

In fact, building an API Portal of this kind is also an extremely effective way of enabling internal and contracted mobile app developers to leverage private APIs.

A full-featured API Portal should provide access to interactive documentation, code examples, sample apps, testing tools and discussion forums.

Conclusion: Deploying a Mobile Access Gateway

Responding to the opportunities presented by employee mobility and the challenges created by BYOD does not have to be as complex as you might think. Deploying an API Gateway – or using an API/SOA Gateway that is already in place – can greatly simplify the process of securely opening up on-premise data and application functionality to custom-made mobile apps.

However, most Gateways on the market do not currently have the full set of functionality necessary for a genuinely secure and effective mobile enablement strategy. That is why CA Technologies has expanded the functionality of its API Gateway products to create a Mobile Access Gateway.

The CA Mobile API Gateway includes all the functionality of CA Technologies' API Proxy and SOA Gateway products and it adds a range of mobile-specific features, including support for OAuth, WebSocket, XMPP, data filtering and more. Combined with the CA API Developer Portal, the CA Mobile API Gateway delivers a complete enterprise mobile enablement solution.

Visit ca.com/api for more information

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**.

This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages. The information and results illustrated here are based upon the speaker's experiences with the referenced software product in a variety of environments, which may include production and nonproduction environments. Past performance of the software products in such environments is not necessarily indicative of the future performance of such software products in identical, similar or different environments.

ca® technologies