ca technologies
A Broadcom Company

A Winning API Strategy: Developing Secure Mobile Apps With a UX that Delights Customers

The Importance of a Better App Experience

The mobile app has become "the" strategic initiative for all digital organizations attempting to drive business forward. In fact, in 2014, mobile app usage surpassed desktop app usage and never looked back.1 The app has become more than a simple method of communication. It is the new critical point of engagement, the face of the organization and quite possibly the difference maker in customers staying or leaving. Getting the "user experience" (or UX) right in the eyes of the consumer is no longer a nice to have but fundamental to achieving success.

The business value of a good UX Today, the UX of an app has come to embody the characteristics of a product or service that are important to the individual. It's the recognized feeling one receives when interacting with the app, how pervasive the app becomes throughout one's life and the lasting memory the individual has after connecting with the business.

But a good UX, while ideally delivering enduring business results, must overcome obstacles to be successful. For instance, not every app type has the same user experience. Web apps, while easier to maintain and extend to the mobile device, don't always render well across different devices ultimately driving organizations to develop new native mobile apps in order to deliver the optimal user experience expected. But native apps possess their own challenges with security being a primary concern.

The implications of secure mobile app development and delivery In order to take full advantage of the app opportunity, businesses must open up their traditional boundaries and connect valuable and sensitive data to the outside mobile world. There's an increased level of risk incurred when enabling these mobile initiatives, thus security is a concern and top priority.

But security, as typically deployed, can negatively impact UX and hinder app adoption. Whether it is VPNs or browser redirect solutions, the end result can be a very poor experience. Few organizations would ask how to cost-justify a minimal investment in security, instead treating it as necessary to reduce the risk of compromised data or processes. Similarly, organizations should treat UX investment as a matter of risk mitigation.2 Leaders within large enterprises understand that security has to change. No longer is it acceptable that security takeaway from the UX and negatively impact business. Security must adapt in order for business to move forward.

Business must balance UX with security

API Management That Delivers App Security With an Optimal UX

In order to meet the demand of both the business and security there must be recognition that security cannot inhibit user experience. While the application program interface (API) provides a terrific platform to meet mobile app development needs, security cannot be an afterthought. The right API management solution will deliver a great mobile app UX while embedding the right level of security that drives app adoption and instills trust.

Developing the app from inside out Designing the right app. The development of a new native mobile app starts internally within the organization and focused on the data. Organizations need to understand the business, the value that's being delivered and what makes the organization different. Is it a credit card company that differentiates through loyalty programs? Is it a retail company offering superior quality clothing? Or is it an automobile company offering better customer service? Understanding the business and what makes it different is a key first step to opening up data to mobile apps.

Next is understanding the dynamics outside of the organization, primarily focusing on customers and competitors. Mobility has changed expectations and how consumers want to do business. The ability to engage and accomplish tasks in a minimal amount of clicks has changed the mindset from show me everything I "could" do, to show me only what I "need" to do. Today, consumers want to get into an app, perform their task and then get out. Understanding and prioritizing discreet functions that are important to each market is of critical importance in order to design an app experience consumers will adopt. These requirements will ultimately vary across markets and geographies and be dependent on the type of phone they possess or carrier plans they have.

API Types
Understanding top strategic initiatives of the business will determine API design direction and required API types: Private, Partner or Public.

And finally where does the company stack up against the competition. Do competitors already offer a dynamic mobile app with a great experience? Are they offering their content through new distribution channels and partners they never thought of engaging? Are mobile consumers leaving the business for competitors that offer a more mobile-centric experience? Answers to these questions will help prioritize mobile projects and the services that need to be offered sooner rather than later.

Ultimately by understanding the true value of the business, what customers demand and how competitors compare in the context of mobility will allow the organization to design the right data integration and access model in support of mobile initiatives.

Old systems don't die. An API will provide the foundation to enable mobile apps to connect to the data that's valuable to customers.

SOAP
SOAP defines a communication protocol spec for XML-based message exchange. When publishing a complex external API SOAP will be useful.

Businesses will always build new applications but old systems don't die. Unleashing the value of data to mobile consumers, especially when dealing with legacy architectures such as SOAP, will require some level of service adaptation. Instead of ripping and replacing existing SOAP services, some level of service translation to more modern and mobile-friendly services such as REST will be required.

In addition, it's unlikely that the only source of data for your mobile app will come from your enterprise. The most dynamic apps are an aggregation of services from inside as well as outside the enterprise. This enables the production of a composite app that delivers a more complete set of information improving the overall experience for the user. Having the ability to orchestrate services from cloud service providers, partners and the enterprise will result in a much more engaging app experience.

REST
REST describes a set of architectural principles by which data can be transmitted over HTTP. REST will be most useful when a lower learning curve, and lightweight and faster results are needed.

As data is consumed from multiple sources across a large set of distributed mobile apps, performance can become a problem. Data transactions will need to be managed for optimal performance through various throttling and caching capabilities.

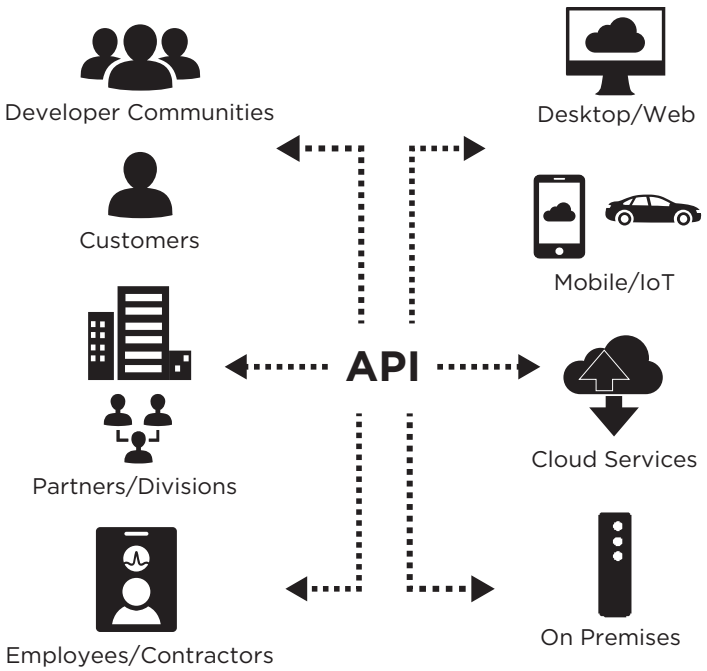

FIGURE A.

APIs are how you securely connect data and applications

Anything that collects and processes data. Today it's normal for a user to connect to the enterprise via a number of different devices, both in consumer and enterprise cases. Hence, users expect that an app will work across different platforms with a seamless UX when moving from device to device. This same expectation can be extended to the proliferation of smart devices that can collect and process data including cars, watches, televisions and utilities. This fragmented ecosystem often results in the development of custom app solutions to support device-to-device interworking scenarios. But it also often leads to a less optimal UX and a lack of trust by the user. If a smartphone is stolen the implication cannot be the owner's car being stolen, or inappropriate access being granted to the home or office. App development needs to ensure device to device connectivity while preserving security that's appropriate to the situation.

Security for the open enterprise. As the enterprise opens its traditional borders to mobile apps, cloud platforms and the Internet of Things (IoT), business is forced to make tradeoffs, taking on some risk in order to capitalize on new digital trends.

Malicious threats such as SQL injections and cross-site scripting as well as rogue or compromised apps can compromise sensitive enterprise data if not adequately protected. Organizations need to ensure, that for every API that is externalized, security is embedded across the entire API layer in order to reduce risk while reducing administrative costs.

Every user, app and machine that connects to the API should be checked against policy to ensure only the appropriate access is granted. Understanding the identity, application and device provides the right level of context to enable fine-grained access decisions that aligns with policy and reduces risk.

Embedding security in the app that delights customers and instills trust

While centralizing security at the API layer provides risk reduction benefits, the security conscious organization should not stop there. Applying security across the entire channel from the app to the backend API provides an additional layer of security necessary for mobile scenarios.

Meeting the needs of the app developer. When applying security to the mobile app, the organization must be conscious not to inhibit release cycles or the end-user experience. Especially when developing consumer focused apps, security solutions that reduce app adoption rates are no solutions at all. App adoption rates must see growth if an app project can be declared a success.

While mobile app projects are funded to drive business forward, mobile app security requirements can often be a mandate that's not well understood by developers. They either don't have the expertise or are far more focused on building engaging apps that delivers an optimum user experience.

Mobile app security that delivers the right level of security while meeting the user experience and time-tomarket needs of the business is an achievable goal. The usage of a software development kit (SDK) allows mobile app developers to apply a standard security model to a large volume of apps, avoids having to train app developers on secure coding practices and allows them to focus on what's important, the business logic and experience the app delivers.

Multi-Device Universe
SSO delivers a convenient mobile experience when moving between apps. The new multidevice world has changed consumer expectations. Moving beyond app SSO to cross-device SSO (tablet, car, door) breaks down barriers and drives better interactions.

OAuth
An open standard to authorization. OAuth provides client applications "secure delegated access" to server resources on behalf of a resource owner.

OpenID Connect
OpenID Connect is a simple identity layer on top of the OAuth protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server.

Mobile toolkit that drives app adoption. It's important that the SDK chosen contains the security features sufficient to protect sensitive information while achieving the adoption goals targeted.

Security should be as transparent to the user as possible without sacrificing protection or consumer trust. There are many mobile security solutions that require a number of intrusive steps when first opening and provisioning a secure mobile app. Secure app provisioning steps, device registration and secure storage of key materials and tokens should be as frictionless to the user as possible.

Once the app has been provisioned the user should be provided with app security features that are also convenient. Social login features which integrates with social networks such as Facebook and LinkedIn is a frictionless way for prospects to avoid frustrating user profile form fields. And single sign-on (SSO) enables users to login once and gain access to many apps. The enterprise should not stop there. Providing convenient access for the app is important but extending that same experience across multiple devices is game changing. The multi-device universe is here. Users constantly move between laptop to mobile phone to tablet. Providing a secure and convenient access experience across devices should be part of any access and SDK solution selected.

Giving users control over apps without involving administrator intervention also delivers security while promoting trust. Standards such as OAuth, OpenID Connect and JSON WebToken (JWT) provide security that delivers user control. The attributes collected through these standards are also used to provide additional policy context. The ability to collect user, app and device information can deliver fine-grained policy control allowing for more flexible policies in support of a particular business scenario.

Finally mobile SDKs should be supported by all relevant mobile development platforms such as Adobe Cordova, Android and iOS.

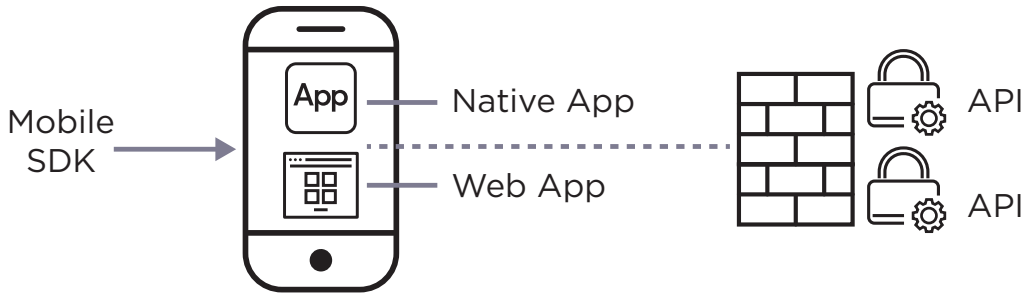

FIGURE B.

Secure mobile channel end-to-end with client SDK

Organizing apps for employees. While lines of business are refocusing resources to win with the mobile app, employees need the same attention if productivity is to improve.

One of the biggest issues employees deal with when attempting to access enterprise applications is understanding what apps are available to them on the mobile device. Make it easy for your employees by providing them an app that organizes all apps, whether Web, native, hybrid or third party, in a single place while only requiring them to login once. SSO should be a requirement across all mobile app types to ensure employees receive the experience expected. This should support existing IAM infrastructures as well.

JSON WebToken (JWT)
JSON Web Token (JWT) is a means of representing claims to be transferred between two parties.

The Right UX and Security Drives Business Forward

The right API management solution will give mobile app developers the tools to accelerate mobile app development, the security to mitigate risk across the entire mobile channel and the UX that will power app adoption to compete in the application economy.

Accelerate development

The API provides deeper benefits than only connecting to data. The API externalizes data to developers in very consumable chunks that have inherent UX benefits. With the right API design and management mobile app developers will be able to access APIs very quickly, develop apps that access the right data that's important to the user and embed standardized security once, accelerating app release cycles.

Instill trust with end-to-end security

Implementing security at the API layer is not enough. In order to adequately secure the entire mobile channel end-to-end the mobile app must be protected. Security that protects the app to the backend API instills trust that improves loyalty.

Improve secure app adoption with a great UX

Implementing app security that inhibits usability and creates friction is security at the expense of the business. Organizations that can find the right level of control while delivering a convenient and engaging app experience will ultimately meet the business and adoption goals they are pursuing.

About Broadcom
Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom's category-leading product portfolio serves critical markets including data center, networking, enterprise software, broadband, wireless, storage and industrial. Our solutions include data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation. For more information, go to www.broadcom.com.

0719