Can You Securely Accelerate Your Mobile Business?

agility
made possible™

ca technologies

CA Technologies allows you to accelerate mobile innovation for customers and employees without risking your enterprise data or applications.

Executive Summary

Challenge

As consumers expect a better mobile engagement experience, teams look to improve employee productivity, and BYOD takes hold within the enterprise, the business must deal with a consistent dilemma, accelerating business initiatives while mitigating risk. No longer is a device only security solution adequate, often compromising the privacy of users. But, of course, lack of visibility and control on the mobile device is no solution at all. Organizations need to take an app and data centric approach to mobile security—a solution that balances business enablement with protection while maintaining the privacy of the users and convenience of using the mobile device.

Opportunity

CA Technologies enables organizations to securely deliver mobile initiatives faster while solving the security and privacy implications of BYOD—all without compromising convenience. By taking a mobile app and data focused approach to mobile security, CA Technologies delivers mobile security solutions across four (4) pillars of capabilities:

- Mobile Development Acceleration

- Mobile App Security

- Mobile Data Protection

- Mobile IAM Apps

Benefits

CA Technologies delivers a mobile security solution that enables enterprises to securely deliver new mobile services for consumers and employees alike. Organizations are able to securely accelerate mobile app development and market reach, reduce fraud to enterprise and third-party mobile apps and enable employee collaboration improving business productivity. This end-to-end approach to mobile security enables organizations to unlock the value of their business through the mobile channel while mitigating enterprise security and compliance risks.

Section 1: Challenge

Balancing the Mobile Business with Mobile Protection

As organizations look to accelerate mobile innovation and business initiatives to drive business forward, IT and security can no longer afford to be an inhibitor to the overall goals of the business. Mobility offers tremendous opportunity to the business and an opportunity for IT and security to contribute to business success. No longer is blocking and preventing access acceptable. Instead IT and security must balance growing the business with protecting the business as cost efficiently as possible.

Extending web investments for new mobile initiatives

To deliver new mobile apps and services, organizations will need a way to open up enterprise data and applications to both mobile developers and apps. For most organizations this represents conceptually a similar undertaking to previous efforts to open up data and applications to end users via the web. But a combination of existing and legacy web application infrastructures, mobile development resource constraints and mobile security risks prevent them from meeting their mobile business goals.

Quite often is the case that existing web application environments don't seamlessly integrate with mobile applications such as REST-style architectures. This often requires organizations to develop new or rip and replace existing web environments to engage with their mobile customers resulting in significant cost implications, and duplication of efforts. And as organizations discover ways to expose services and data to mobile channels through APIs the threat of critical business services being compromised is a real risk.

It's not the mobile device it's the mobile app

As customers demand access to products and services via the mobile platform and employees require the usage of their personal device to access enterprise applications anywhere and anytime mobile security solutions must evolve. No longer is protection at the device level sufficient given consumer and employee privacy and legal implications. When protecting the device the business can often have inappropriate control over a broad set of mobile technology features giving them access to personal employee apps and data. Liability issues can arise if personal data is viewed or removed from the device.

Instead organizations must evolve their device-centric security approach to an application and data-centric approach. This will provide organizations proper control, help maintain privacy of the user and mitigate corporate liability risk.

Supporting IT consumerization without compromising security

As employees adopt cloud and mobile services, organizations can realize tremendous business productivity gains but at the potential cost of information leakage. As sensitive information is shared outside the organization across cloud services and public mobile apps businesses are put at risk of data compromise and regulatory non-compliance. Organizations are put in a difficult situation. Do they completely block access to mitigate risk but inhibit business or open up access to enable business but incur risk? Businesses need a way to improve collaboration but in a secure manner. CA Technologies provides the security tools to support IT consumerization trends without compromising security.

Section 2: Opportunity
Mobile Security Solutions

CA Technologies provides organizations the right balance of mobile business enablement and business protection. CA Technologies leverages APIs and identity to accelerate mobile app development and delivery, secure mobile apps, protect mobile data and empower mobile users.

Figure A.

Accelerate app development, secure apps, protect data and empower IAM users
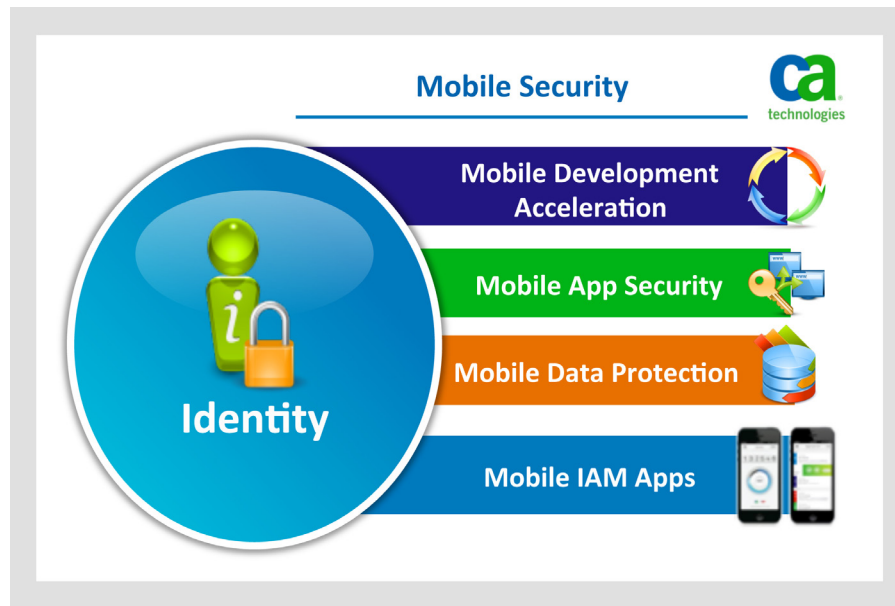
Mobile Development Acceleration

CA Technologies allows organizations to grow their mobile business through accelerated app release cycles, securely externalized business services and the externalization of valuable data to third-party developer networks.

CA Technologies provides the means to open data up to mobile developers and apps through an approach that leverages prior investments in web access management and translates to a modern API format enabling efficient and secure mobile app development.

APIs are how native, hybrid and HTML5 mobile apps consume enterprise data. Web assets along with legacy applications and enterprises data stores can be outfitted with an API to make the underlying resource consumable by a mobile developer or app. CA Technologies can help adapt existing data and applications to be API ready while ensuring consistent control across both web and APIs.

Mobile protocol adaptation

Allowing mobile app developers to develop to existing application environments can be difficult and expensive. Connecting existing SOAP application environments to new RESTful style mobile environments can be a difficult proposition. The CA Layer 7 Mobile Access API Gateway accelerates

mobile app development by allowing organizations to leverage existing application investment such as SOAP through the adaptation of web application protocols into modern mobile RESTful APIs. Enterprise data stores and applications are then securely externalized for developers to quickly create mobile apps. Security is also abstracted out of the development process, centralizing at the gateway, allowing developers to focus on the value of what's being developed and speeding up the entire process.

Mobile API developer portal

Not every mobile API can be treated the same. There's a learning curve that directly impacts the development process. The CA Layer 7 API Developer Portal provides organizations a central place to present data and application APIs to internal developers and optionally external communities of developers. The API Portal simplifies the publication of APIs to developer communities while managing how developers discover information about the APIs, register for access and gain insights into API usage and best practices.

Mobile backend security

A layered security model is suggested in any security program. Especially in the world of BYOD with a lack of device control, protecting inappropriate access to the enterprise at the gateway is extremely important. The CA Layer 7 Mobile Access API Gateway protects the organization from malicious or accidental mobile app connectivity to the backend. It delivers a secure pathway for mobile apps to access corporate data. Access is centrally managed to the API, protecting data and resources exposed from attacks and misuse. It also provides a centralized way to control SLAs, availability and performance parameters for the APIs. The business constraints necessary for secure mobile access can be accomplished by an IT administrator without having to engage with their mobile app developers.

Figure B.
Accelerate, secure and expand mobile opportunities
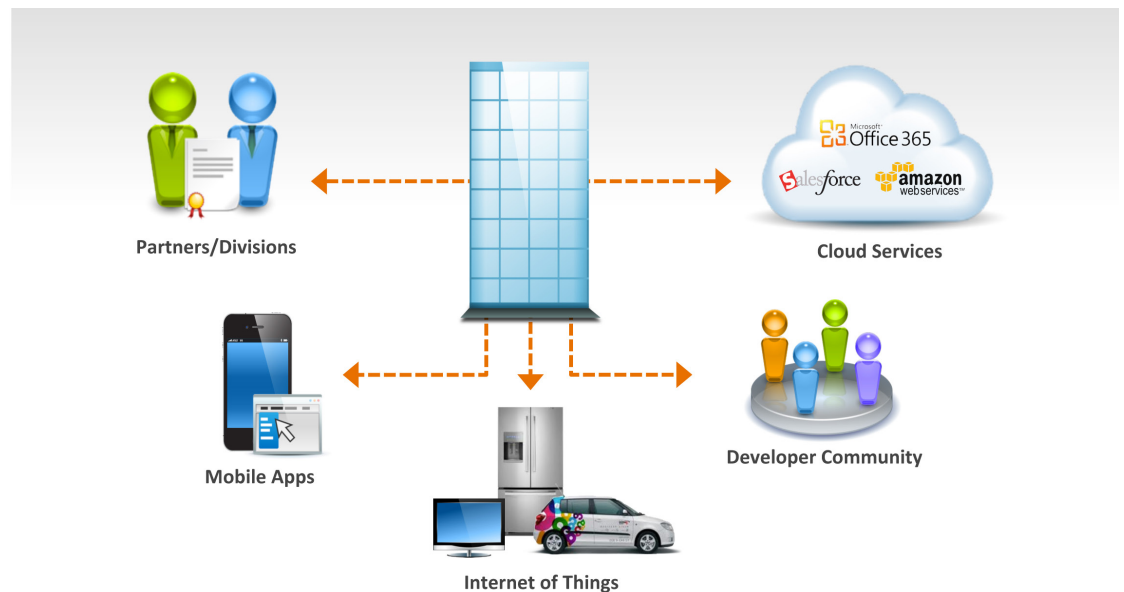
Mobile App Security

As new mobile apps are released to the market they must be protected to reduce organizational risk. CA Technologies centers on the identity of the user allowing for a convenient yet private experience while protecting business data.

Depending on your business scenario, customer lifecycle or employee enablement plan, your organization will no doubt adopt different mobile app strategies. Whether your plan is to develop mobile business apps to deliver to customers or partner with third-party SaaS providers like SalesForce and leverage their mobile apps for employees you'll need different mobile app security solutions.

Two options: SDK and wrapping

CA Technologies offers two mobile app security options delivered as a SDK or in the form of wrapping. Organizations focused on developing new mobile apps may require a security tool kit in order to apply security capabilities directly into their own apps as part of the development process. But if the organization is utilizing third-party mobile apps, applying security into those app development processes is not an option. Security must be applied in a different form. CA Technologies offers organizations the ability to wrap third-party apps with security policies post development. CA Technologies offers the following capabilities as both a SDK or in the form of a wrapper.

Mobile single sign-on (mSSO)

As consumers access business services through the mobile platform maintaining a convenient experience is extremely important. The ability to remember multiple usernames and passwords has proven to be a significant challenge for users that also results in a loss of productivity and business service engagement. The mobile form factor, also makes the entry of multiple user credentials difficult and error-prone. CA Technologies removes these inhibitors by enabling a convenient mobile application experience through mobile single sign-on. The ability to deliver a convenient and seamless experience when working between mobile apps is extremely valuable. Users no longer have to remember a unique username and password for each mobile app. Instead standards-based protocols such as OAuth are utilized to deliver a convenient mobile app single sign-on experience improving mobile usage productivity and business engagement.

Two-factor authentication

The mobile device is now viewed as a significant threat vector to any business or organization. Either organizations have no control and lack visibility into the device or control the entire device impacting user data privacy and potentially legally exposing the business. CA Technologies enables BYOD by protecting the corporate app through two-factor authentication. Additional security is delivered with the storage of credentials in a local, persistent format to avoid inadvertent removal. This format improves security and the user experience while reducing IT administrative burdens. The software credential can also be locked to the device in order to prevent the reuse of a stolen credential by another device. In addition, the mobile device may be used to verify transaction details, such as a financial transaction amount or payee, as part of an out-of-band authentication process, to reduce the risk of fraud in online transactions.

Risk-based authentication

The scenario in which a mobile user accesses information can often change resulting in elevated risk levels to the user and organization. In order to mitigate this risk CA Technologies delivers risk-based mobile authentication taking into account various contextual factors such as user identity, geography and device type to determine if access should be granted. This may be applied across multiple channels and identities delivering a consistent and centralized security policy. All rule-building and editing is done from a single web interface, improving risk evaluations and fraud detection performance.

Figure C.

Secure the mobile app while leveraging the convenience of the device

Mobile Data Protection

As organizations attempt to improve productivity through on-premise, cloud and mobile forms of collaboration sensitive information is often shared putting the business at risk of data compromise and non-compliance. CA Technologies intelligently controls the dissemination of sensitive information shared and communicated over email or through files whether on-premise, in the cloud or through the mobile platform.

Secure mobile message control

Email remains the most used mode of communication in the workplace and a critical tool for organizations when communicating with customers. But quite often is the case that sensitive customer or company information is purposely, mistakenly or maliciously sent out of the organization over email with little to no control. CA Technologies, with partnerships through encryption vendors such as Voltage Security, are able to intelligently classify sensitive content and then control the email

all based on the content and identity of the user. As an employee attempts to send an email to a mobile device the content is classified and then controlled in the form of a warning, block or encryption. This enables organizations to not solely rely on the policy knowledge of employees but instead automatically classify and control content reducing the risk of error and non-compliance. It also enables organizations and employees to communicate sensitive information that needs to be communicated in order to keep business moving.

Secure mobile file sync and sharing control

The advent of cloud models, such as Dropbox, box and SkyDrive, that enable the sharing and collaboration of files have had a significant impact on consumers and enterprises. As consumers uncover the value of using the cloud to share personal content to their mobile device they immediately attempt to apply the same model to work environments as the opportunity arises. But organizations, as a matter of policy, either block access completely, limiting productivity, or allow access and sharing without control exposing the business to enormous risk. It is a continuing battle, users finding ways to share their files, and IT trying to manage the risk to the enterprise. CA Technologies solves this problem by applying intelligent control to the sharing of sensitive content in files. As a user attempts to copy or move a file to their Dropbox folder the data is classified and controlled, either warning the user that the action is against policy, blocking the content from being shared or encrypting the file so that it's protected whether in transit, stored in the cloud or sync'd to the mobile device.

Figure D.

Intelligent data-centric security of files and emails

Mobile IAM Apps

As mobile users drive demand for anywhere/anytime access and a more convenient software usage experience in the workplace the enterprise is pressured to respond. CA Technologies enables a more productive Identity and Access Management experience with its software through the delivery of IAM software in the form of mobile apps. Each IAM app is developed with the premise of improving daily work activities for IAM users through a better user interface and workflow process via the mobile phone.

CA IdentityMinder™ mobile app

The CA IdentityMinder mobile app is the first CA Technologies IAM app to be supported. This mobile app includes identity management functionality such as the ability to update profiles, reset passwords, change passwords, and approve requests. The app will also support on-premise as well as CA CloudMinder™ deployments. Organizations will benefit from improved user productivity to perform identity management tasks wherever they are and through a streamlined workflow process.

Figure E.
Improve productivity
with mobile IAM apps
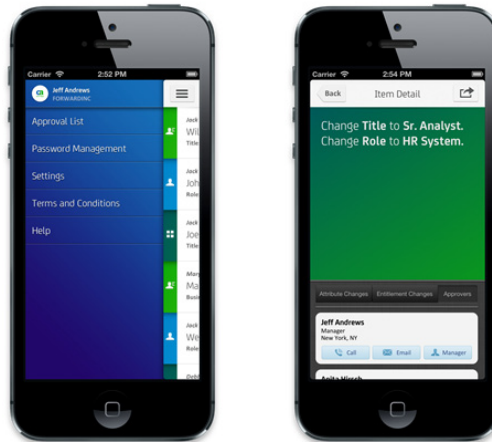
Section 3: Benefits
Securely Grow Mobile Business and Improve Employee Productivity

CA Technologies enables organizations to leverage the mobile platform to securely grow their business and improve employee productivity.

Grow and Innovate Business

The mobile app is fast becoming the strategic initiative to drive business forward. The emphasis of organizations to identify solutions that enable business growth and innovation could not be greater. With CA Technologies organizations will be able to improve customer engagement, accelerate app delivery and externalize the business unleashing the power of data.

Securely accelerate app delivery

As organizations investigate the mobile business opportunity there are often barriers preventing them from reaching their markets in a timely fashion. CA Technologies securely accelerates the delivery of mobile apps enabling organizations to reach their markets faster. Organizations are able to adapt existing web environments to mobile architectures avoiding having to rip and replace, deliver tools to mobile app developers improving the development and testing of apps, and then secure and govern all mobile transactions at the perimeter avoiding having to build security into the development process. The result is a faster, higher quality and more secure process of releasing mobile apps.

Securely improve user engagement

Customers want to engage the business through the channel that suits them best whether it's through the web or a mobile app. CA Technologies allows organizations to engage their customers through their channel of choice delivering a convenient experience while mitigating risk to the application and business.

Improve Mobile Employee Productivity

The mobile device has quickly become the communication of choice to enable better employee and partner collaboration. But the uncontrolled sharing of sensitive content has inhibited organizations from realizing the full potential of the mobile platform. CA Technologies enables enterprises to securely collaborate through the mobile platform while also allowing users to access IAM software anytime/anyplace.

Enable secure collaboration

Whether it's SharePoint, Dropbox or email, users often share dynamic forms of content unknown to the business. CA Technologies allows organizations to continue sharing sensitive information, but in a controlled manner that mitigates risk to the business. Through intelligent data-centric security, organizations are able to balance business enablement with business protection.

Empower CA Technologies users

CA Technologies enables IAM software users to improve their productivity through the usage of CA IAM software on the mobile platform. The convenience of the mobile platform and workflow usability of the mobile app improves the productivity of IAM administrators and other functional groups that work within the IAM workflow process on a daily basis.

Section 4:
The CA Technologies Advantage

CA Technologies allows organizations to balance enabling the mobile business with securing the mobile business. CA leverages identity to securely accelerate mobile app delivery, improve engagement through secure mobile apps, protect mobile data through intelligent data-centric security and empower mobile IAM users.

CA Technologies mobile security solution is core to any mobility initiative. As organizations evaluate mobility management and service offerings, security should be considered a core component to an overall and comprehensive solution.

CA Technologies has been a leader in IT management for over 30 years, has over 1000 security customers, and is committed to continuing to bring innovative management and security capabilities to the marketplace. We have a large and dedicated group of security experts who know how to make security deployments successful, and to help our customers achieve accelerated time-to-value.

Agility Made Possible: The CA Technologies Advantage

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.