WHITE PAPER | OCTOBER 2014

Engaging Your Mobile Customers While Protecting Sensitive Data

Tyson Whitten
CA Technologies, Security Management

Table of Contents

Executive Summary

Challenge

As businesses develop their strategies to capitalize on new and evolving mobile market opportunities, application and data security challenges are inhibiting companies from achieving their goals of engaging their mobile customer base. Businesses are searching for ways to seamlessly extend Web application environments to new mobile delivery models while securing sensitive data that's communicated between employee devices (corporate and personal liable) and customer owned devices. The inability to reach new markets, enable access and secure data all while maintaining usability and privacy has inhibited business from moving forward.

Opportunity

There's an opportunity for businesses to capitalize on the mobile market opportunity and improve engagement by enabling application readiness, mobile access and data protection for both mobile customers as well as employees. But attempting to solve these mobile issues on a per application or per device channel basis can be extremely painful. Instead businesses need to take a universal approach that comprehensively solves these issues across two axes: enabling customer engagement through application management and data-centric security. By following these two guidelines businesses will be able to meet their goals of supporting business and enterprise mobile applications more securely while meeting usability and privacy expectations mobile users have come to demand.

Benefits

Once businesses are able to overcome these challenges, they will achieve their mobility goals and benefit in the following ways:

- **Grow top line revenue** – Businesses will engage customers through mobile technology more effectively. Whether it's expanding shelf space through new mobile channels, enabling sales teams to reduce time to sale, improving customer service and how they engage with consumers, or developing business services that improve customer loyalty, there are direct revenue opportunities that organizations can take advantage of once complex mobile inhibitors are removed.
- **Reduce the risk of mobile data compromise** – As mobile users engage the business, sensitive information is communicated increasing risk and inhibiting business growth. Organizations able to control identities, access and the data over the mobile channel can significantly reduce business risk, enabling organizations to grow their business securely.
- **Lower cost of ownership** – Through the delivery of unified application and end-to-end data security solutions, businesses are able to centrally manage infrastructures that supports large heterogeneous environments while also enabling convenient end-user usability reducing overall cost of ownership.

Section 1: Challenge

Mobile engagement and protection challenges

New business opportunities are taking shape as consumers across the globe are adopting new mobile devices, high-speed access and innovative mobile applications. But this proliferation of mobile devices, the development of intelligent and composite applications, the number of multi-device users, and the shift to bring your own device (BYOD) has created many challenges for businesses to effectively capitalize on mobile opportunities. Essentially the innovation rate in mobile devices is accelerating faster than the enterprise can adapt. Existing Web applications don't support new mobile models preventing access to significant market opportunities. Security solutions tend to be fragmented with security management of Web applications being separate from mobile applications or data security only focusing on the mobile device versus the data across many platforms. And then usability as well as privacy often suffers given security's traditional approach to secure the device versus the data. The end result: reduced competitiveness, missed revenue opportunities and increased risk.

Mobile access implications of application growth

The mobile phenomenon has opened up a variety of new revenue generating opportunities and has provided an effective way for businesses to improve their value chain across a variety of organizational resources. Mobility is providing businesses new ways to expand shelf space and extend reach into new markets through new development channels. It has introduced novel approaches to enable sales teams to reduce time to sale. Customer service has an opportunity to become more engaged with their customers while also developing new service annuities programs. And it has provided a new way for customers to interact with the business at their moment of decision, such as making a payment to Amazon or their bank, improving business services and customer loyalty.

But the proliferation of device types has impacted standardization and has resulted in a broad heterogeneous application environment businesses must now support to reach markets quicker and enable customer and employee access. From HTML5 to custom enterprise applications to composite applications to non-traditional wireless applications, this variation has compounded existing application issues businesses are already attempting to solve. Supporting new developer communities, non-standard protocols and decentralized mobile identities have inhibited the ability to deliver a holistic application solution that enables faster time to market and easier and more convenient access.

Big and small browsers

Businesses looking to harness the power of the browser and move past developing to the individual device or operating system will often look to develop in HTML5, CSS3 and JavaScript™. If they can monetize services over the Web while leveraging existing application infrastructures and access management solutions they will usually develop in these languages. Users see the value in viewing and transacting through a Web browser and will continue to leverage the browser to access content from a mobile device if the experience is acceptable. So if the standard "big" browser is working for them, they will also use the "small" browser if usability and profitability aren't affected during the process.

Enterprise and business applications

Rich mobile applications enable users to quickly access content and transact with the business and enterprise. As businesses look to extend their presence to the mobile user through the development of mobile applications, there are advantages of starting with enterprise applications but also challenges. The business and development teams have full control over their enterprise applications. But existing application infrastructures and protocols must integrate with the new applications being built. For instance, the majority of mobile applications are developed with RESTful protocols while existing application environments are built with SOAP. This gap sometimes inhibits mobile application readiness in the marketplace but existing access management capabilities can get them started.

Intelligent and composite applications

The growth of innovative applications has expanded business opportunity and has enriched the way organizations can do business with consumers. As organizations become more advanced in their strategies to distribute content and enable transactional mobile applications, they often investigate options around intelligent or composite applications for mobile devices. These are applications that consume content from various sources, some internal and some external to the business. Protocols that must be consumed to enhance internally developed applications or protocols that distribute content to third-party partners can vary. This coupled with a lack of control over these protocols from external sources can make supporting these types of applications very difficult. The ability to integrate SOAP, REST and JSON environments together can be very challenging but ultimately very beneficial to the business.

Non-traditional applications

Not only do mobile phones and tablets provide a channel for businesses to connect with consumers but all platforms that are wirelessly connected (i.e. wireless appliances, vending machines, connected vehicles, etc) provide an opportunity to engage consumers and other key value chain resources at a more sophisticated level. Businesses need a way to create new applications for these emerging and innovative platforms. But most existing enterprise Web applications cannot support these new mobile applications. Businesses need an easier and more secure way to reach these new markets.

Sifting through the fragmentation

In summary, there is a wide range of ways mobile users can engage with the business. Each has their pros and cons based on the business use case with varying levels of support complexity. As a result, there is a high level of uncertainty surrounding standardizing on browser-based delivery or mobile applications. As reported in a recent CA Technologies survey, “50-60 percent of respondents plan to use HTML5 while 34 percent will use Rich Mobile Apps.” What this is telling us is that there will be a broad mix of both environments requiring businesses to support very heterogeneous environments.

In order to support this variety of browser and application use cases businesses will need a solution that can enable mobile engagement across a wide range of application access points. The solutions should allow businesses to reach new mobile markets and improve employee productivity by supporting developer communities to securely code to existing application environments, secure distribution and consumption of content between various mobile application channels and translate protocols to support new mobile applications. It should also enable convenient and efficient mobile user access through advanced authentication, session management and centralized authorization.

"The Rubik's Cube problem of coordinating data, access, and applications across multiple channels gets more complicated as firms pursue mobile engagement."

Source: Mobile is the New Face of Engagement, Forrester Research, Inc., Feb 13, 2012

It's not the device it's the data.

As organizations start implementing unified application security solutions they also have to take steps to ensure the data is protected.

While organizations have always lacked control of customer devices and data, enterprises are starting to lose control of employee devices as well. Organizations that traditionally have protected data at the device level are being forced to adjust. As a result of device proliferation, multi-device users, and the phenomenon more and more businesses no longer have control of employee liable devices but are challenged with still protecting company and customer data.

Device proliferation

The quantity of mobile devices in the marketplace is staggering. Forrester states, "257 million smartphones will be in use with U.S. consumers by 2016." The device volume alone is interesting, but the bigger problem impacting how data is secured is the variety of operating systems and applications. What typically was one vendor, Microsoft, owning the lion's share of the market is no longer the case. Forrester states, "Globally, one-third of devices used for work are non-Microsoft PCs or mobile devices." The world is being overrun with Apple® IOS and Google® Android™ devices. This increase in variability has changed the mindset of organizations in how they plan on securing sensitive information on the mobile endpoint. Difficult resource decisions are being made on whether to keep up with device security or instead focus on securing the data.

Multi-device users

The next trend that's having a direct impact on mobile security is the growth of multi-device users. No longer can organizations only focus on controlling one company issued device. The various use cases that spread across workstations, laptops, smartphones and tablets are resulting in users using more devices for work. Forrester states, "52 percent of all info workers use three or more devices for work." Employees are demanding and expecting a high level of usability across these device types.

The benefit of using many devices for work purposes also directly influences the expansion of work usage to personal usage. Forrester states, "60 percent of devices reported by info workers are used for both work and personal purposes." And what comes with this is an expectation of privacy of personal information, especially around personal liable devices. Organizations must now deal with the challenge of keeping information secure on devices they lack control of and users that expect a certain level of usability and privacy.

BYOD

This high rate of device growth and multi-device usage also has a direct impact on BYOD. Employees now have direct influence on the devices they use for work. Forrester states, "Many North American and European information workers report that they choose devices themselves (rather than IT choosing or the worker choosing from an IT list), ranging from 73 percent for smartphones to 53 percent for laptops, and even 22 percent for desktops." This indicates that employees are gaining control directly, impacting IT's planning for the future and how they will deal with the implications of having to support customer and employee liable devices.

But even though organizations are starting to lose control of the device when employee liable devices are allowed into the enterprise, they cannot afford to lose control of data. Businesses still must control information to mitigate the risk of losing intellectual property, impact to brand and non-compliance with PCI DSS, HIPAA or local and state data regulations. This leaves little option for the business but to transition from device-centric security to data-centric security. The data must be controlled at the source versus attempting to control it at

the container, all while maintaining the same user experience and expectation of privacy.

Section 2: Opportunity

Guide to Mobility Security Solution Selection

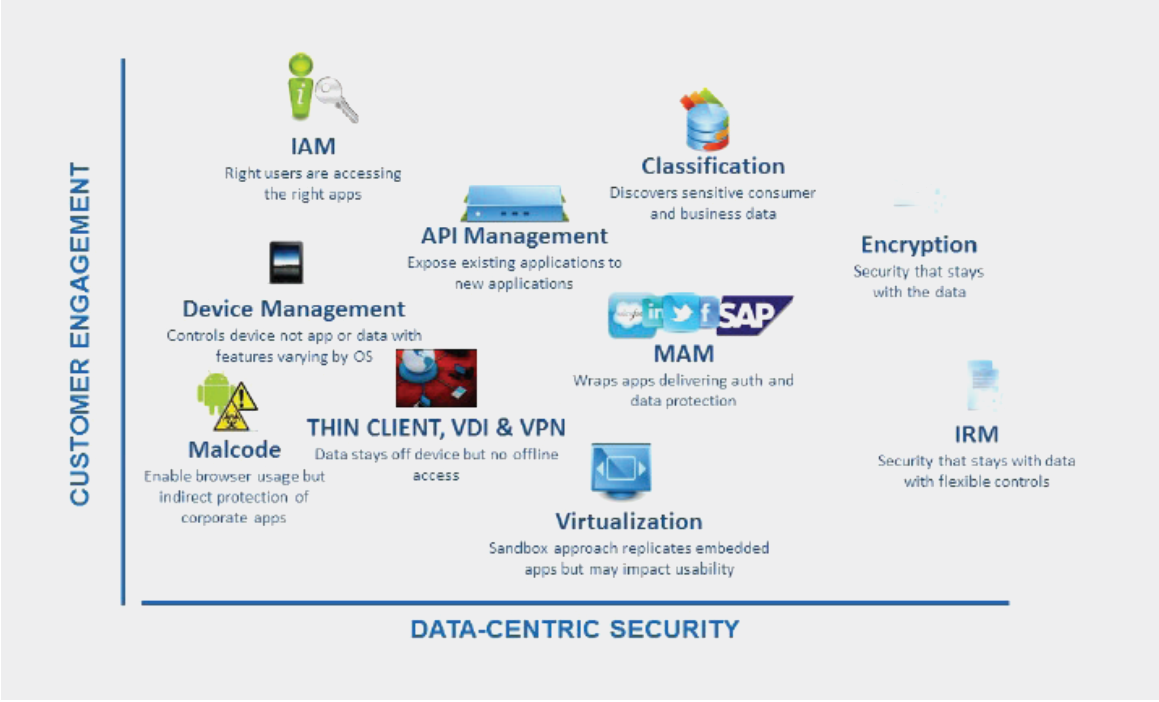
The opportunity to grow your business comes with application and data security challenges that often get in the way. A pragmatic approach should be taken to solving these challenges by simplifying the decision making process and aligning with two main decision criteria: customer engagement and data-centric security.

What mobility solutions are available?

The following solution matrix highlights the wide range of mobile security solutions currently available in the marketplace while allowing you to prioritize capabilities based on customer engagement and data-centric security. This framework provides general guidance in selecting mobile solutions but should also be measured against specific organizational goals. Business type, mobile use cases, application strategies and current solution investment would also play a part in the solution decision process and should be thought through as each solution is assessed. But if businesses want to achieve a blend of customer engagement capabilities with data-centric security, their goal should be to select solutions that are at the top and right of the matrix. Capabilities stronger in enabling better engagement to the business move from the bottom to the top while capabilities stronger to protecting the data moves from left to right. The following provides an overview of each capability area detailing pros and cons of each, additional questions you should be asking and a prescribed approach that will further help in your mobile solution selection process.

Figure A.

Mobility solution guidance matrix



Customer Engagement

The Customer Engagement axis is defined by a wide range of capabilities that enable mobile customers to better engage the business. These capabilities include authentication, authorization, single-sign on, session management, protocol translation and secure application programming interface (API) management. And data protection solutions are included as well since they also remove data security inhibitors to enabling customer engagement. All capabilities span technologies and should be selected based on specific project criteria.

Identity & Access Management capabilities enable the right users to gain access to the right applications and data. This solution would be optimal for organizations looking to extend existing access management and authorization capabilities to enterprise applications for both mobile customers and employees.

API Management solutions support organizations mature in their approach to application development. Companies creating composite applications that require the ability to consume and distribute content to and from sources they don't control need to support various protocols. This is a good solution for enabling developer communities to securely write to APIs while also translating protocols for new complex applications.

Mobile Application Management provides the ability to wrap individual applications delivering authentication capabilities as well as local data protection. This option becomes attractive when incorporating embedded and third-party party apps into an overall authentication strategy while also protecting data local to the device.

Data-centric Security

The Data-Centric Security axis covers mobility solutions that start with security solutions that indirectly protect data through various means on the left and then transitions to solutions that become much more focused on protecting the data itself as you move from left to the right.

Malcode protection and anti-virus is required to protect the enterprise when connecting to compromised applications but is indirect protection of corporate applications and data. Protection does not stay with the data.

Mobile Device Management (MDM) capabilities provide some combination of management and security but the focus is on the device and solely the mobile channel. If single channel device management and security at the device level is the objective, this solution may meet the requirements. But for organizations attempting to take an end-to-end data-centric security approach while maintaining usability and privacy, other complementary data-centric security solutions further to the right of the matrix may be required.

Virtual Desktop Infrastructure (VDI) technology keeps data secure since the data is not local to the device, but the tradeoff is network latency and no offline access. If you're attempting to enable field services, your sales teams, other mobile workers as well as your customers, and require real-time access, a VDI solution may not provide the availability required.

Virtualization and sandboxing is a segmentation approach to separate corporate applications from personal applications on the device. While information is separated providing application and data control to the business data, there are drawbacks from a usability perspective. The replication of native and embedded applications in the form the vendor chooses can often vary from the native application on the device, taking away usability the users have come to expect.

Classification is core to understanding where data is located and how sensitive it is to the business and consumer. Although classification alone does not protect the data, it is a very important enabler of IAM as well as other data-centric security controls such as encryption to selectively control sensitive information no matter where the data lives.

Data Loss Prevention (DLP) enforces data policies through the combination of classification and controls such as blocking or quarantining while data is at-access, in-use, in-motion and at-rest. It also integrates with other enforcement technologies such as encryption and Information Rights Management.

Encryption is true data-centric protection. It's not protection of the container which presents usability and support issues but the data itself, wherever the data lives. While some PKI-based encryption models pose difficulties, Identity Based Encryption (IBE) provides setup, provisioning and administration benefits for encrypting data that PKI does not offer. It is also very complementary to classification technologies.

Information Rights Management (IRM) also is true data-centric protection and a version of encryption, but it also contains inherent fine-grained policy-based controls that deliver more encryption access and handling options over the life of the data than encryption alone.

Business questions

Once you understand your solution options and how they fit into your customer engagement and data-centric security objectives they should be balanced against criteria that are specific to your business. The following are some questions to ask to help determine your next steps in selecting a mobile solution.

Mobile business objectives

- Is mobility transformational and strategic to driving business forward?
- Will enabling all customers all the time to better engage the business be your primary objective?
- Is mobility an enabler of employees to make them more productive?
- What types of employees will you enable and how often will they need access through mobile devices?

Strategic application objectives

- What types of applications are you planning on deploying to enable customers and employees?
- Do you plan on starting with current enterprise applications or more advanced applications such as composite or non-traditional apps?
- Is supporting embedded or third-party apps important to your application goals?

Data security objectives

- How is multi-device usage and BYOD impacting your deployment of security policy and controls?
- Will you only need to control data on corporate liable devices?
- Will you need to control data on employee liable devices as well as other devices outside of your control?

Current mobile investment

- What application or data security solutions have you deployed to date?
- Can you leverage existing solutions in order to prevent fragmentation?
- Is a unified mobile security solution important to your organization?

The answers to the questions above will help guide your selection decision process based on specific use cases related to your business. Not all technologies and capabilities are appropriate for all use cases and should be balanced based on your specific customer engagement and data protection challenges. A combination of a few may be the end result.

"The advent of the extended enterprise and the ease of accessing corporate information anytime, anywhere, and on any device will create new pressures on security teams to encrypt data. Mobile devices are easy to lose and easy to steal. Enterprise-level encryption is the best hope for securing data on these devices."

Source: Killing Data, John Kindervag, Forrester Research, Inc., Jan 30, 2012

A prescribed approach

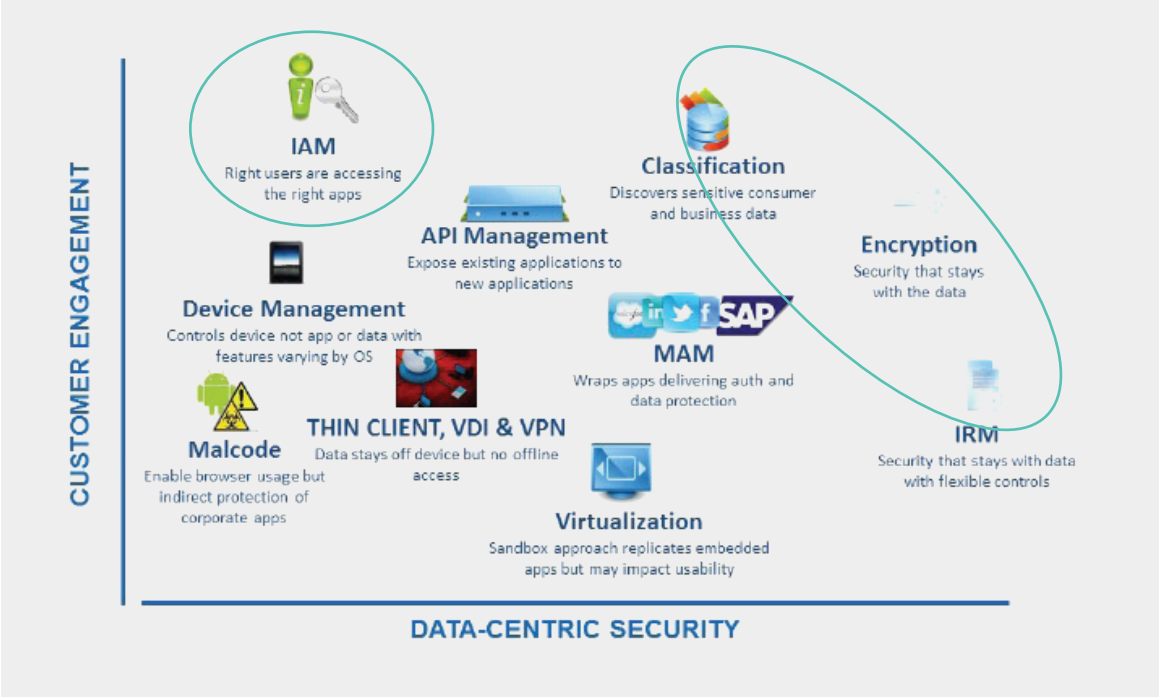
So where should you start? There are some common approaches that can be taken to achieve one's mobility goals.

Organizations attempting to extend current business and enterprise application access to mobile device users can get off the ground through existing access management investments. IAM technologies can quickly provide the ability to incorporate new mobile users into existing application access management solutions delivering a convenient user experience and centralized application management. Adaptive authentication can also be applied to help ensure the right user is accessing mobile resources based on contextual attributes of the mobile phone such as location. And while this enables access to new mobile markets and employees to be more productive there are data risks that must also be mitigated.

Since mobility work usage varies more times than not, a solution that allows for real-time data access while protecting information even when outside of the mobile channel should be the goal. While some organizations have attempted to control information at the device level through technologies such as MDM, this approach is not end-to-end and does not protect information after it leaves the device. VDI is another solution that protects data but doesn't support the real-time use cases workers come to expect especially if they're mobile, on the road or often find themselves on planes. And it doesn't enable business processes to continue since it's unlikely VDI would be deployed to customer devices. To avoid these issues customers ideally need to implement data-centric security solutions that protect information throughout its life. And they often want to do this selectively. A combination of classification and encryption would enable organizations to meet this requirement. As depicted in the following diagram a combination of capabilities that span the top to the right of the matrix is a good guide for solution selection.

Figure A.

Mobility solution guidance matrix



Section 3: Benefits

Benefits of Unified Application and Data-Centric Security Solutions

The benefits of selecting a unified solution that meets your application and data requirements will enable you to capitalize on new mobile market opportunities, reduce the risk of data compromise and non-compliance and reduce overall cost of ownership.

Grow top line revenue.

The benefits of a mobility solution that will enable mobile users and employees to better access products, services and enterprise resources via new browser and rich mobile application technologies will allow businesses to capitalize on new mobile market opportunities. Whether it's reaching new mobile markets through new developer networks, enabling sales teams through enterprise applications, improving service based annuity programs or enhancing business service innovation, mobility can help organizations grow their business.

Reduce the risk of mobile data compromise.

Device, OS and application fragmentation, multi-device users and BYOD are all impacting the organization's ability to control data as they always have – at the container. The lack of device control and the privacy and usability expectations from users are requiring businesses to deliver data protection solutions that protect the data itself. But data-centric solutions are able to control more than just the mobile channel. The ability to control information end-to-end delivers a holistic solution that helps reduce the risk of data compromise over the life of the data while avoiding the device, usability and privacy issues that come with device-centric security.

Reduce total cost of ownership.

The mobile channel has introduced significant application and data challenges to the enterprise. The combination of browser-based and client/server access models within mobile devices has created a level of fragmentation very difficult to manage. Unified security solutions are able to centralize security management and expand user convenience to the mobile device with reduced overall cost of administration and management.

The same holds true for data protection. Device proliferation and personal liable devices have forced organizations away from attempting to control a wide range of mobile devices. Instead, the value of controlling the data versus the device end-to-end not only helps reduce the risk of data compromise but also reduces the cost of administration and management due to centralized and scalable infrastructures.

Section 4:

Conclusions

The opportunity to capitalize on the mobile marketplace is there for the taking, but inhibitors must be overcome if businesses are going to have a high likelihood of success. New mobile application delivery models and a lack of device control have impacted the direction businesses are taking to achieve their objectives.

There are many solution options businesses can choose from to assist in reaching their goals. And many factors will play in the decision making process. It's in the best interest of the business to select a unified solution that enables customer engagement while taking a data-centric approach to data protection. CA Technologies provides two axes to help in selecting one's mobile solution to drive business forward: Customer Engagement and Data-Centric Security. Varying mobility objectives, use models and business profiles will ultimately help determine the solution of choice, but CA Technologies recommends specific capabilities to help organizations improve the probability of capitalizing on new mobile market opportunities quickly while reducing the risk of data compromise at a lower overall cost of ownership.

Section 5:

About the Author

Tyson Whitten is a CISSP with 15+ years of IT and security experience managing application, network and risk based products and services. In his current role he has responsibility for API Management and Mobile Security solutions at CA Technologies. Prior to CA Tyson held positions at SecureWorks, VeriSign, Guardent and Genuity. Tyson has a BS in Finance and Information Systems and a MBA in Product Management from Boston College.

Connect with CA Technologies at ca.com

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**.

CS200-94857_1014