SOLUTION BRIEF
CA TECHNOLOGIES IDENTITY-CENTRIC SECURITY

How Can I Both Enable and Protect My Organization in the New Application Economy?

ca technologies

CA Security solutions can help you enable and protect your business through identity-centric security capabilities.

Executive Summary

Challenge

Business is being impacted by many important trends—cloud adoption, increased mobility, the rise of social media and the increasing flow of information across the extended enterprise. The old network perimeter is no longer relevant. Today's IT must deal with highly distributed identities across the entire business environment that come from many sources—applications, systems, social media, etc. In addition, mobile employees and customers are changing the face of business and redefining the challenge of delivering secure applications quickly to the changing user population. Users need to be able to access information anywhere, anytime and from a range of different devices. These factors cause a dramatic shift in the role of security and how user identities should be managed. The old way of managing users and access won't suffice in the new world order.

Opportunity

Merely protecting critical assets and data is no longer the primary focus for IT security. Identity management can be an effective way to deliver new services more quickly, to improve engagement with your customers and to help open up new business opportunities with your partners. But, fully leveraging identity management requires a comprehensive, integrated identity platform that provides capabilities to support consistent security across Web, mobile and API channels. CA Technologies provides an identity management platform that can enable you to leverage new business opportunities such as mobile and cloud, while helping to ensure the security and privacy of critical IT applications and information.

Benefits

The benefits of leveraging identities as the central model for your security infrastructure are significant. Improved business agility, enablement of new business channels and improved customer loyalty can help grow your business, and identities can help you achieve these benefits. Increased productivity and overall efficiency can help to push downward on your IT security management costs. And, last but certainly not least, improved security and privacy over critical information help you avoid loss of business, the potential of paying fines or damages and the huge negative reputational damage of a data breach or attack.

Section 1: Challenge

Unleashing and protecting business in the application economy

Your organization faces significant challenges in today's world, where protecting vital business data can be a daunting proposition. Today, you must proactively protect your critical applications and information from unauthorized access you must comply with governmental and industry regulations and you must quickly deploy new business services to help grow the business. And, you must do this all while maintaining budgets and improving efficiencies.

But, today's security landscape has changed dramatically, fueled by major forces such as:

Rise of mobile – Organizations need to enable both employees and customers who want to use their own mobile devices to access enterprise apps. But, delivering mobile apps and securing the data they access, is difficult due to the differences in the app development models for Web and mobile. Existing Web application environments don't seamlessly integrate with mobile applications such as REST-style architectures. This often requires organizations to rip and replace existing Web environments to engage with their mobile customers, resulting in significant cost implications and duplication of efforts. Any capability that can help you reach your mobile customers more easily is a major business driver.

Increasing velocity of new apps – A business rides on its ability to deliver new business services quickly. Revenue growth depends on the ability to reduce friction in app development and deployment across all channels. The best way to do this is to expose your APIs—securely—to internal and external developers and to deploy capabilities to help them use those APIs. But, many challenges serve to prevent this. Conversions to mobile APIs and managing the security and performance of APIs are inhibitors to speedy and effective rollout of both Web and mobile apps. But, companies that fail to realize the importance of engaging effectively with their potential developers (both internal and external) will be left behind in the app deployment battle.

Movement to cloud services – Organizations need to be able to transparently provision to and from a variety of cloud applications. Many organizations are also moving their identity services to the cloud and gaining significant benefits in doing so. But deploying identity-as-a-service demands two characteristics from your identity provider:

- Very high and proven scalability to handle the potentially very large number of users that might need to be managed
- Flexibility of deployment options across on-premises and cloud so that you can move your identity services to the cloud as, and when, you need to

Increasing amount and movement of data – The amount of data, and its geographical dispersion, are increasing dramatically. As data begins to reside almost anywhere, protection of it becomes a greater challenge. The ability to discover, classify and protect this data, regardless of its velocity or location, is critical.

The rise of the application economy

The application economy has transformed the way we do business. And it's the app, present in all digital forms, that has become the critical point of engagement, optimizing experiences and providing a direct and constant connection from the business to the end user. But the organization that will win, the one that will maintain its competitive edge, is the agile organization, the one that can quickly unlock the power of data, effectively onboard developer communities and meet changing consumer demands through faster app release cycles. At the same time, they must mitigate the exposures that threaten their new open enterprise, risk the compromise of data and impact the bottom line.

In order to succeed in the app economy, organizations need to establish new business channels and to create and nurture effective partner ecosystems. Therefore, they are opening their data and applications to partners, developers, mobile apps and cloud services. APIs provide a standardized way to open up information assets across the Web, mobile devices, Service Oriented Architecture (SOA) and the cloud. The ability to use APIs to create a consistent experience across Web and mobile apps increases an organization's ability to get new apps to market quicker and to use them to improve engagement with its mobile users. In fact, APIs are critical in the application economy because they can provide the capabilities to enable internal and external developers to more easily and securely access your enterprise data. They are the connection point between apps and data.

In the new, highly distributed "Open Enterprise", user access originates from a variety of locations and devices, and the target apps might be Web or mobile, which could reside on-premises, in the cloud or in a hybrid environment. The network perimeter can no longer provide a control mechanism for this access. Identities now constitute the new perimeter and are the single unifying control point across all apps, devices, data and users. They are how you protect access to apps and data. As such, identities and APIs serve as the foundations of the application economy because they enable easier deployment of secure apps and help simplify control of access to those apps.

Organizations today require an identity-centric app delivery framework that can quickly unlock the power of data, effectively onboard developer communities and meet changing consumer demands through faster app release cycles, all while mitigating the exposures that threaten the new open enterprise and risk the compromise of data.

Section 2: Solution

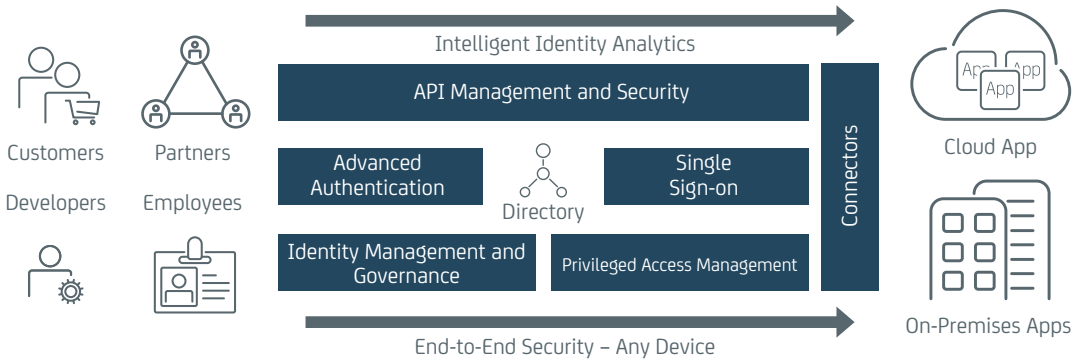
The CA Identity-Centric Security Suite

CA Technologies security solutions provide a comprehensive identity, access and API management platform that can help you succeed in the app economy because it enables your organization to:

- Accelerate the delivery of new online services.
- Improve customer engagement using the channel of their choice (Web, mobile, APIs).
- Enable secure collaboration among employees and partners.
- Protect key assets from insider threats and external attacks.
- Reduce the cost of security and compliance management.

Figure A.

CA Identity-Centric Security Suite



Identity Management

Identity management and governance

The emergence of the Application Economy has spurred a change in the role of users. Identity management processes today, including the requesting of new access, are far more user-centric than in the past. Users request access when they need it and can now perform many of the functions that were previously done only by a central IT group. As identity processes become accessible to a wider variety of business users, *user experience becomes critical* to the success of any deployment. Interfaces and available capabilities can no longer be oriented towards the IT-savvy user only. They must instead be simple and intuitive for the business user and must provide consistent experiences across the device of their choice without compromising the IT needs.

The **CA Identity Suite** meets this challenge by providing comprehensive identity management and governance capabilities with a simple, intuitive user experience. This user experience can dramatically simplify processes such as user access requests and access certifications, resulting in improved productivity and user satisfaction. In addition, the Identity Suite performs risk analysis and certification and enables remediation actions in real-time during the access provisioning steps, thereby improving audit performance and risk posture with preventive policy enforcement.

While providing this outstanding user experience, the CA Identity Suite also delivers core identity management and governance capabilities, including broad provisioning support for on-premise and cloud apps, extensibility and flexibility to integrate with other identity management/security solutions, other IT systems and consumer-grade scale. The CA Identity Suite provides organizations with deep functionality, high scalability, and most importantly, an outstanding user experience.

Privileged access management

One of the most important areas of IT risk relates to privileged users. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and on the overall security and privacy of corporate assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that are essential for their role—enabling "least privileged access" for reduced risk.

The CA Technologies solution for privileged identity management, **CA Privileged Access Manager (CA PAM)**, provides a network-based solution spanning the entire enterprise—delivering comprehensive protection for traditional physical data center resources, software-defined data centers and networks, and cloud-based infrastructure and service providers. Delivered as a hardened physical or virtual appliance, the system deploys rapidly and provides a complete, self-contained solution that eliminates the requirement for expensive hardware and software components that drive up costs. CA Privileged Access Manager is particularly well suited for organizations relying on cloud and virtualized technology—a backbone of the application economy—given tight integration with those platforms. CA Privileged Access Manager provides:

- Strong authentication of privileged users, including support for a variety of multi-factor authentication technologies
- Least-privilege, role-based access controls over all kinds of resources
- Robust password and credential lifecycle management
- Privileged user single sign on
- Secure, agent-less command filtering and fine-grained controls over administrative actions
- Detailed session recording, with DVR-like playback highlighting events of interest and attempted policy violations
- Application-to-application credential management
- Protection of cloud and virtual management consoles and APIs
- Full support for IT infrastructure across the modern enterprise

Access Management

Controlling access to critical enterprise IT resources is required not only for effective compliance, but also to protect shareholder value, customer information and intellectual property. Without effective user authentication and access policy enforcement, improper access can have disastrous effects. There are two important areas to consider:

- Strongly authenticating user identities
- Controlling access to Web applications

Advanced authentication

Concern about identity theft, data breaches and fraud is increasing, but at the same time organizations are feeling pressure to enable employees, partners and customers to access more sensitive information from anywhere and any device. These market dynamics make multi-factor authentication and fraud prevention critical parts of any organization's security strategy.

CA Advanced Authentication is a flexible and scalable solution that incorporates both risk-based authentication methods like device identification, geolocation and user activity, as well as a wide variety of multi-factor, strong authentication credentials. This solution helps an organization provide the appropriate authentication process for each application or transaction, delivered as on-premises software or as a cloud service. It helps to protect application access from a wide range of endpoints which include all of the popular mobile devices.

The products in the CA Advanced Authentication Suite include:

- **CA Strong Authentication** – A versatile authentication server that allows you to deploy and enforce a wide range of strong authentication methods in an efficient and centralized manner. It provides multi-factor strong authentication for both internal and cloud-based applications. It includes mobile authentication applications and software development toolkits (SDKs), as well as several forms of out-of-band (OOB) authentication.
- **CA Risk Authentication** – Provides multi-factor authentication that can detect and block fraud in real-time, without any interaction with the user. It integrates with any online application and analyzes the risk of online access attempts and transactions. Utilizing contextual factors such as device ID, geolocation, IP address and user activity information, it can calculate a risk score and recommend the appropriate action.

Single sign-on and Web access management

In order to deliver—securely—the new applications that can drive the business, organizations need a centralized way of controlling access to these services across an often huge number of users.

CA Single Sign-On, an industry-leading secure SSO and access management solution, provides an essential foundation for user authentication, single sign-on, authorization, session management and reporting. It enables you to create granular access policies that can control access to critical applications based on a flexible set of static or dynamic criteria. In addition, CA SSO (formerly called CA SiteMinder) has been successfully deployed in some of the largest and most complex IT environments in the world, scaling to millions of users with very high performance and reliability.

The CA SSO solution also includes:

- **CA Federation** – Extends the capabilities of CA SSO to federated partner relationships and SaaS applications, which enables your organization to rapidly implement and manage partner ecosystems to help grow your business
- **CA Directory** – Provides the performance, scalability and reliability needed to support your most demanding online applications through its high performance for read and write operations and transparent distribution and replication to scale to any number of servers

API Management

Increasingly, enterprises are opening their data and applications to partners, developers, mobile apps and cloud services. APIs provide a standardized way to open up information assets across the Web, mobile devices, SOA and the cloud. However, to make API information sharing safe, reliable and cost-effective, enterprises must deal with critical security, performance management and data adaptation challenges.

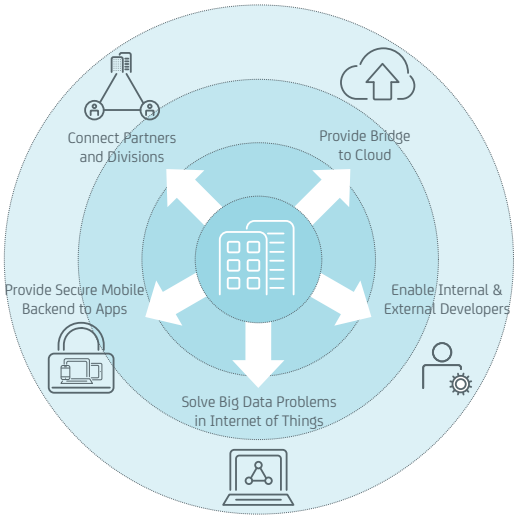


Figure B.

Business drivers for API management

The CA API Management suite makes it simple for enterprises to address these challenges. It combines advanced functionality for backend integration, mobile optimization, cloud orchestration and developer management. It is unique in its ability to address the full breadth of enterprise API management challenges.

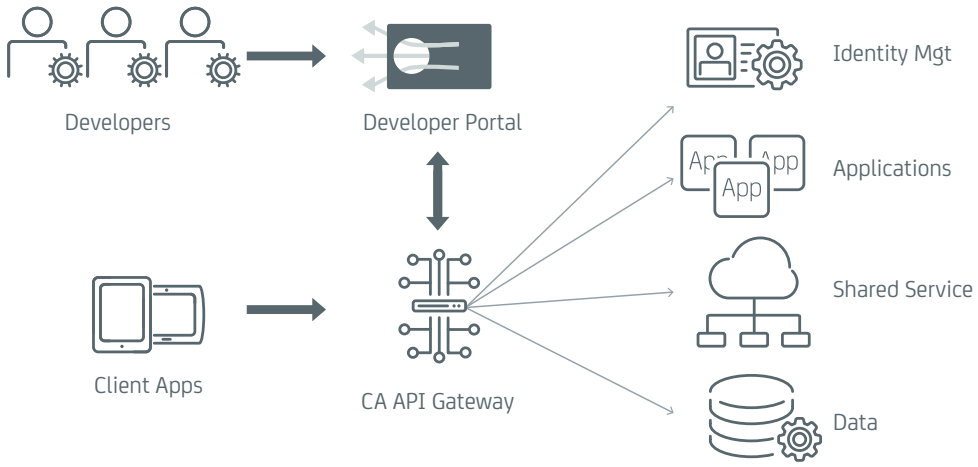
The suite includes the following solutions:

- **CA API Gateway** – CA API Gateway and CA Mobile API Gateway offer unmatched flexibility, performance and security and are available as hardware appliances or virtual machines, for deployment on-premises or in the cloud
- **CA API Developer Portal** – Engage, onboard and educate internal and third-party developers via a branded online interface, to facilitate the creation of applications that leverage enterprise APIs

Let's look at a customer example to highlight the power of this solution. One of the largest airlines in the world needed to improve the customer experience across Web and mobile channels, thereby improving customer loyalty as well as its own competitive position. The airline deployed CA API Gateway to secure, orchestrate and regulate mobile app access to its diverse backend systems (see graphic below). CA API Gateway enabled the organization to quickly deploy composite mobile apps and to control the use and performance of its APIs. CA API Gateway acts as the hub by aggregating and presenting data from multiple sources, internal and customer data of the airline, and external data from partners such as Sabre. CA API Developer Portal enabled developers to easily get information about the APIs, test out their apps and collaborate with other developers. Upon deployment, they were able to provide customers with a 360 degree view of their travel itinerary, and a convenient mobile experience, thereby improving customer satisfaction.

Figure C.

Sample use case



Section 3: Benefits

Enable and protect your business

Leveraging the business potential of trends like cloud and mobile challenges all IT organizations. The CA Security suite can enable you to do that, while providing these key benefits:

- **Quicker deployment of new apps** – Through such capabilities as centralized security policy management, common authentication across channels, federation and API security, CA Security solutions enable you to build and deploy services quickly, helping to take advantage of changing marketing and competitive events. Most importantly, you can deploy mobile apps much quicker by leveraging our API security capabilities.
- **Improved user engagement** – CA Security solutions enable you to more easily engage with your customers and to improve loyalty throughout their lifecycle. Self-service, federated SSO, consistent authentication, convenient UIs and social media identity support all help drive a favorable user experience.
- **Creation of new business channels** – The ability to easily and securely expose your APIs to internal and external developers can enable new business opportunities and speed the creation of complementary solutions from your partners. CA API Developer Portal greatly simplifies app development and helps support new apps and services to help expand your offerings.
- **Reduced security risk** – Improper access, insider threats and external attacks are all major challenges that can leave your data and apps exposed. CA Security solutions enable a defense-in-depth strategy in which automated, comprehensive controls can be implemented at all levels of the identity infrastructure. Reduced risk of information theft or disclosure can also drive increased customer loyalty.
- **Improved secure collaboration** – Strong security controls within the suite of solutions enable your users to share information more easily and enables you to control what they can do with your critical information.
- **Improved efficiencies** – Automated identity lifecycle management and governance reduces expensive manual processes and enables your managers to focus more on the business than on managing these processes.

Section 4:

The CA Technologies advantage

CA Technologies is uniquely positioned to help organizations solve the challenges of today's mobile, cloud-connected, open enterprise. Our identity management suite offers unique benefits and capabilities that other offerings cannot match, including:

- **Broad, comprehensive solution** – CA Security solutions are an integrated set of products that can enable you to effectively manage identities, access and data for all your user populations. The suite also includes capabilities that virtually no other suite vendor can provide—including privileged identity management, API security and management, risk-based authentication and data classification and control. The breadth of the CA Technologies solution means that we are well-positioned to meet your identity requirements both today and as they evolve.
- **End-to-end security** – CA Security solutions provide strong security from device to the data center, enabling you to improve customer confidence that personal information will not be compromised, while delivering a convenient user experience.
- **Flexible deployment options** – CA Security solutions can be deployed on-premises, in the cloud or in a hybrid environment. Given that most organizations that have existing deployments tend to move to the cloud in a phased approach, this flexibility helps ensure business agility as you gradually adopt SaaS-based identity services.
- **Proven scalability** – Your organization and its needs are very likely to grow. You need to feel comfortable that your vendor can meet these growing needs. CA Security solutions have been proven in some of the largest IT environments in the world today. Whether you have a small, large or huge environment, our solutions can scale to meet your needs.
- **Proven success in IAM deployments** – We have years of experience in IAM deployments. We have a very large and dedicated group of security experts who know how to make security deployments successful and help our customers achieve very quick time-to-value.

Learn more at **ca.com/securecenter**.

ca technologies

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.

Copyright ©2015 CA. All rights reserved. UNIX is a registered trademark of The Open Group. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. 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 non-infringement. 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.

CS200-159385_1015