SOLUTION BRIEF

CA TECHNOLOGIES IDENTITY-CENTRIC SECURITY

Identity-centric Security: The ca **Secure**center Portfolio

ca technologies

How can you leverage the benefits of cloud, mobile, and social media, while protecting your key information assets across the open enterprise? 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

Securing the Open Enterprise in a World of Cloud and Mobile

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, oh by the way… 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 – Both employees and customers want to use their own mobile device to access your apps, and organizations need to enable that. 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 develop new or 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 all serve as 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. First, very high and proven scalability to handle the potentially very large number of users and entitlements that might need to be managed. Second, flexibility of deployment options across on-premise and cloud so that you can move your identity services to the cloud as you need to, when you need to.

Increasing amount and movement of data – The amount of data, and its geographical dispersion is 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

Increasing sophistication of attacks – External attacks are far more dedicated and persistent than in the past. Advanced Persistent Threats (APTs) have emerged as a new and insidious form of IT risk. New protections are necessary to implement a true "defense in depth" approach with security controls at each level of the environment. An integrated identity platform is the most effective way of deploying this broad range of controls.

The trends described above have caused an evolution of the notion of identity and access management. Yesterday's identity management capabilities are not sufficient to meet these expanding demands. New approaches and expanded capabilities are required.

Redefining Identity and Access Management

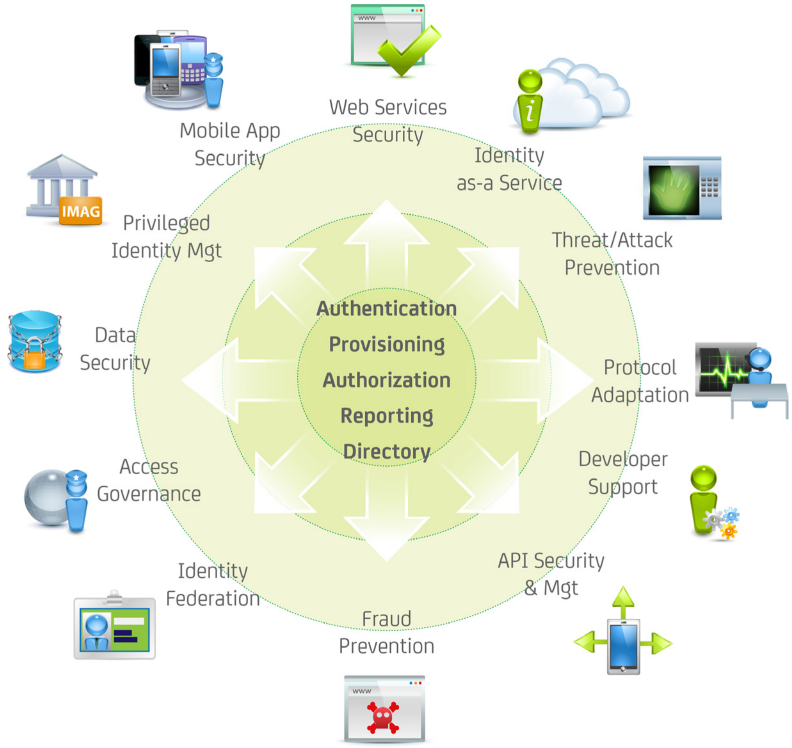
Identity and access management used to be simple – a few basic capabilities to support common use cases such as provisioning, access management, and authentication. But, these straightforward use cases have now expanded to include required capabilities that are far more than was required even a year ago. Today's organization has far more identity use cases than previously, and this expansion of requirements highlights the need for a comprehensive identity platform. The following are typical use cases that we find today in most organizations, divided into areas of *enablement, protection, and efficiency.* As noted in some examples below, many of these use cases relate heavily to more than one category.

Enablement	Protection	Efficiency
Partner ecosystems	User provisioning & de-provisioning	
Mobile access to enterprise apps	Centralized security policy management	
Federated SSO	Role mining and mgt	
Support for developer communities	Compliance audit reporting	
Securing APIs end to end from datacenter to mobile apps	Web access control	Self-service password reset
Multi-channel app development	Strong authentication	Access requests
Use of social media identities	Fraud detection & prevention	Delegated user admin
SaaS-based identity services	Privileged user control	Access certification
Secure access to cloud apps	Admin password mgt	
Deliver composite apps to partners and customers	Hypervisor security	
Improved customer experience	Attack detection & prevention (e.g., APTs)	
	Privacy protection for sensitive data	
	Segregation of duties violation detection	
	Email security	

But, as the scope and breadth of these use cases has increased, the requirements for an effective identity platform have expanded. No longer are basic capabilities sufficient to meet the needs of today's mobile, cloud-connected organization. Today's challenges require capabilities that don't exist in most identity products today. Figure 1 highlights the breadth of capabilities that are required in an integrated identity platform today.

Figure 1.

Redefining Identity and Access Management



The Identity Platform Approach

Some organizations are confused by the breadth of these identity capabilities that are quickly becoming essential. They might try to cherry-pick solutions, thinking that they are acquiring "best of breed" for each area, thereby giving them a "best of breed" identity platform. Unfortunately, this approach is ineffective.

A comprehensive, integrated identity platform is far more effective than multiple point solutions because it provides:

- Reduced administrative expense and effort, due to increased consistency of component interfaces
- Improved security due to a common and consistent model for roles, privileges, workflows, etc. These common models enable more mature security processes, which provide greater protection against internal and external security threats.
- Faster application development, especially when coupled with robust API security capabilities.
- Improved end-user experience, as self-service capabilities, SSO, and authentication interfaces are extended and consistent across the platform.
- Improved ROI, as the cost benefits of a platform approach become significantly better than point solutions over the three year timeframe.

In summary, given the expanded list of capabilities required for effective identity management, point solutions are a poor long-term approach to managing security across the enterprise environment.

Section 2: Solution

The ca **Secure**center Portfolio

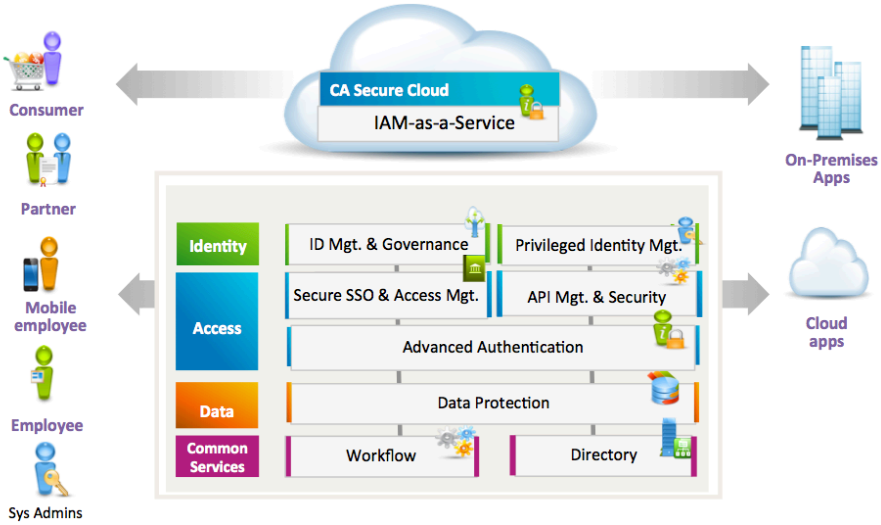
Today's business environment demands new approaches to security in order to leverage trends such as mobile, cloud, and social media. The network perimeter has been replaced by an open enterprise where users, applications and data exist almost anywhere and need access from multiple devices, including their own at any time. The old methods of security don't always secure your environment because your environment has changed.

CA Security solutions (ca **Secure**center) provide a complete identity and access management platform that enables your organization to:

- Securely deliver new online services quickly across Web, mobile and 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 2.

The CA Security Suite



The CA Technologies identity platform is an integrated set of components that provide the broad capabilities required for today's organization. For simplicity, these solutions can be viewed as focused on three areas of identity management:

Control identities—Manage and govern user identities and their roles and access, provision users to resources, and enable compliance with identity and access policies. Control actions of privileged users to protect systems and information from careless or malicious administrators.

Control access—Verify user identities and enforce policies relating to access to applications, systems, APIs, and key information, across Web and mobile.

Control data—Discover, classify, and prevent leakage of confidential corporate and customer information.

These three elements are essential for a comprehensive approach to IAM security. Unfortunately, most IAM vendors provide some capabilities of only the first two categories—but they don't enable you to provide control down to the data level. CA Technologies uniquely provides a comprehensive solution for securing all three critical areas.

Control Identities

Identity Management and Governance

The CA Technologies solution for identity management and governance covers management of user identities for both regular users and privileged users. The solution includes capabilities for user management, access governance, role management and mining, and user provisioning. This end-to-end approach includes the initial creation of user identities, the allocation of accounts and access entitlements, the ongoing modification of these entitlements as the user's role changes, and timely removal of these rights and accounts upon termination.

For organizations looking to leverage the benefits of a cloud-based deployment model for identity management, CA Identity Manager SaaS is a robust software-as-a-service solution for managing and provisioning user identities, as well as access request management.

It is hosted and managed by CA Technologies and also available from select CA Managed Service Provider partners, reducing the cost of ownership to your organization by reducing deployment times and accelerating your ability to leverage the cloud's elastic capabilities. Deploying identity-as-a-service gets your organization's identity management capabilities up and running faster while reducing the ongoing costs and overhead of managing related infrastructure, software or facilities.

The CA Technologies products for identity management and governance of users include:

- **CA Identity Manager** (previously CA IdentityMiinder)—Provides identity administration, provisioning/de-provisioning, user self- service, and compliance auditing and reporting. It helps you establish consistent identity security policies, simplify compliance, and automate key identity management processes.
- **CA Identity Governance** (previously CA GovernanceMinder)—leverages analytics and workflow to automate identity governance processes, including entitlements cleanup, certification, segregation of duties, and role management. By automating these processes and controls, it helps you reduce risk, improve compliance, and increase operational efficiency.
- **CA Identity Manager SaaS** (previously CA CloudMinder Identity Management)—Provides user management, provisioning, and access request management in a SaaS-based deployment model.

Privileged identity 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 Identity Manager (previously CA ControlMinder), protects systems by securing both access to privileged accounts and also what access a user has while logged in. It does this by providing highly granular entitlements for administrators which enables easier compliance through policy-based access control and enforcement that includes segregation of duties. It is a scalable solution that provides privileged user password management, fine- grained access controls, user activity reporting and UNIX authentication bridging across servers, applications and devices from a central management console.

Other CA Technologies solutions for privileged identity management include:

- **CA Privileged Identity Manager for Virtual Environments**—Brings privileged identity management and security automation to virtual environments to improve security for hypervisor environments.
- **CA Shared Account Manager** (previously CA ControlMinder Shared Account Management)—Improves security and accountability through secure, single-use password management for privileged user account identities.

Control Access

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 three important areas to consider:

- Strongly authenticating user identities
- Controlling access to Web applications
- Securely enabling access to APIs for developers (both internal and external)

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-premise 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** (previously CA AuthMinder)—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** (previously CA RiskMinder)—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.
- **CA Advanced Authentication SaaS (**previously CA CloudMinder Advanced Authentication)—Provides the capabilities described above as a cloud service.

Single sign-on and flexible 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** (previously CA SiteMinder), an industry-leading secure SSO and access management solution, provides an essential foundation for user authentication, single sign-on, authorization, 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 Single Sign-On 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.

CA Single Sign-On also includes capabilities for identity federation, to enable business growth through the expansion of complex partner ecosystems. Comprehensive security for SOA-based architectures is provided so that both Web applications and Web services can be protected in a common security infrastructure. The CA Single Sign-On solution includes:

- **CA Single Sign-On** - Provides secure single sign-on and flexible access management to applications and Web services located on-premise, in the cloud or at a partner's site.
- **CA Federation** (previously CA SiteMinder Federation)—Extends the capabilities of CA SiteMinder to federated partner relationships, which enables your organization to rapidly implement and manage partner ecosystems to help grow your business.
- **CA Single Sign-On SaaS** (previously CA CloudMinder Single Sign-On)—Provides robust cross-domain single sign-on for both identity and service providers as a SaaS service.

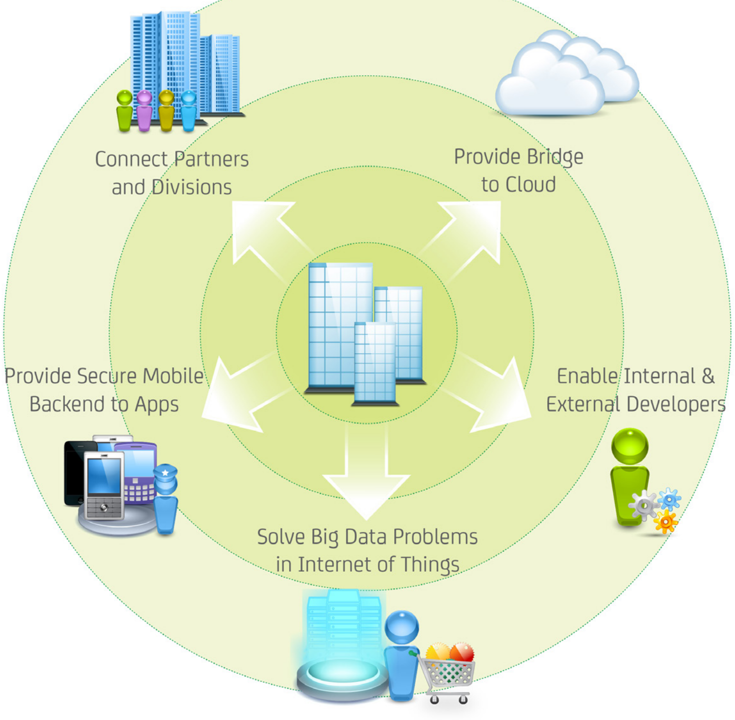
86.5%
Of Organizations will have an API Program in Place Within 5 Years

API security and management

Organizations need to be looking for ways to establish new business channels, and to create and nurture effective partner ecosystems. In order to do this, they are opening their data and applications to partners, developers, mobile apps and cloud services. In fact, as you can see from the sidebar, a huge percentage of all organizations report that they will have an API program in place within 5 years! 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 their mobile users. However, to make API information sharing safe, reliable and cost-effective, enterprises must deal with critical security, performance, and management challenges.

Figure 3.

API Enablement


Connect Partners and Divisions
Provide Bridge to Cloud
Provide Secure Mobile Backend to Apps
Enable Internal & External Developers
Solve Big Data Problems in Internet of Things

The CA API Security & Management solution 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 primary solutions:

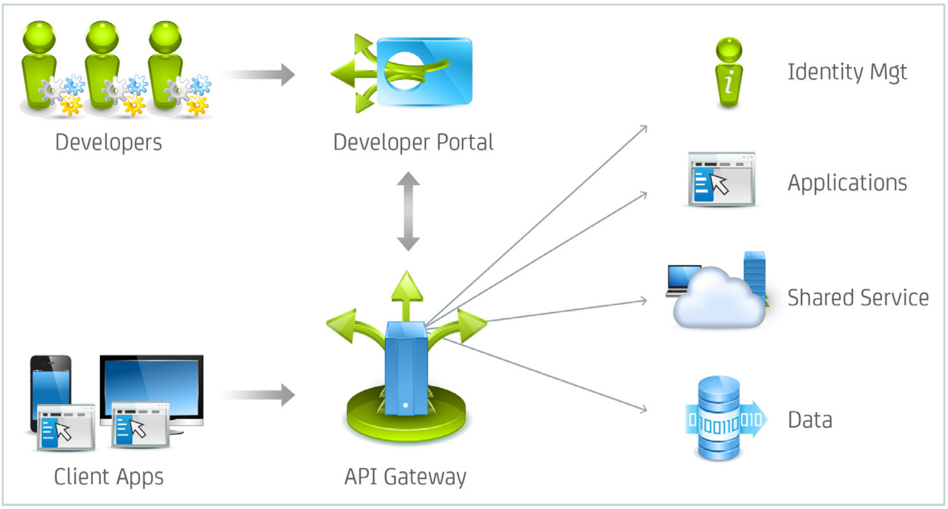
- **CA API Gateway** – A suite of solutions that offers unmatched flexibility, performance and security, these gateways are available as hardware appliances or virtual machines, for deployment on-premise or in the cloud.
- **CA API Developer Portal** (previously CA Layer 7 API Portal) – Engage, onboard and educate internal and third-party developers via a branded online interface, to facilitate the creation of applications that leverage enterprise APIs.

- **CA Mobile API Gateway** – provides a centralized way to control security and management policies for information assets exposed, via APIs, to mobile developers and apps.

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 their own competitive position. The airline deployed the CA API Gateway to secure, orchestrate and regulate mobile app access to their diverse backend systems (see graphic below). The API Gateway enabled them to quickly deploy composite mobile apps, and to control use and performance of their APIs – acting as the hub of aggregating and presenting data from multiple sources, internal and customer data of the airline, and external data from partners such as Sabre. The 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 4.

API Security use case



Control Data

Enforcement of access controls over sensitive information is only the first step in a comprehensive approach to information security. Once users have gained legitimate access to this data, many organizations have little or no control over what those users can do with it. An employee might email a sensitive document to their home account, or copy it to a USB device, or a number of other policy violations. These organizations often are not fully aware of all the places their sensitive information is stored, and have no protection against this information being exposed or disclosed to unauthorized people, either internally or externally.

CA Technologies solutions for data security help you get control of your massive amount of information, and most importantly, protect sensitive data from inappropriate disclosure or misuse.

It protects data-in-motion on the network, data-in-use at the endpoint, and data-at-rest on servers and repositories. It enables you to define policies for which type of data should be monitored, and the action to be taken if inappropriate activity is detected. It can significantly reduce information security risk and makes it easier to prove compliance with certain security-related regulations and best practices.

CA Technologies solutions for data security include:

- **CA Data Protection** (previously CA DataMinder)—Reduces risk by automatically classifying data as to its type, and then controlling what users can do with the data—in use, in motion, or at rest.
- **CA Email Supervision** (previously CA Email Control for the Enterprise)—Prevents unauthorized use of your sensitive data with centralized email security policy enforcement.

The value of integration

Breadth of a security solution is important. But, without component integration, a broad suite becomes just a series of independent point products. The suite of products from CA Technologies is integrated at the component level to provide organizations with easier management, decreased costs, and reduced risk. For example, CA Advanced Authentication has been integrated with other relevant components, providing a consistent model for risk-based authentication across the suite. CA Risk Authentication has been integrated with CA Single Sign-On so that user authentications can be assigned a risk score, and high risk attempts can require additional authentication information, resulting in reduced fraud threat. In addition, CA Identity Manager and CA Identity Governance are integrated to provide a single, consistent solution for identity management and governance. The integrated solution provides “smart provisioning”, which means that before a user is provisioned for access to a resource, SOD (segregation of duties) checks are automatically done to help ensure that access should be granted. This results in reduced risk, and less time spent later in manual SOD checks and compliance reporting. Finally, the classification capabilities of CA Data Protection are accessible through CA Single Sign-On, enabling it to make access decisions based not only on the identity of the user, but also on the content of the data. This content-aware IAM capability is unique to CA Technologies, and provides additional security against the misuse or improper access of sensitive information.

These are just simple examples of the integration of CA Security solutions. But, as you expand your business to mobile and cloud environments, and your user population grows ever larger and more distributed and diverse, these integrated capabilities can be important to enabling you to meet your growing requirements.

Section 4: Benefits

Securely Enable Your Open Enterprise

Leveraging the business potential of trends like cloud and mobile challenge 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. The developer portal greatly simplifies app development, and helps support new apps and services to help expand your offering.
- **Reduced security risk** - Improper access, insider threat, 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 5:

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 & 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.

Leadership products – Each component of the CA Technologies identity platform has been rated as being a “leader” in their area by the leading analyst firms, such as Gartner, Forrester, and KuppingerCole. Whether you deploy one, or several of our solutions, you can benefit from using a solution that is rated as being best-of-breed.

Flexible deployment options - CA Security solutions can be deployed on-premise, 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.

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**.