BUYER'S GUIDE

Identity, Access and API Management Solutions

The Changing Role of Security

There is a confluence of forces at work that is transforming enterprises all over the world that have increased the importance and impact of enterprises having a holistic and effective IT security strategy. No longer is security the domain of just the IT department. The whole business now must be engaged on security issues because an effective security solution has the potential to significantly impact the business in many ways, such as helping expand into new markets, developing new sales channels and improving customer engagement across Web and mobile platforms.

In order to achieve this potential, the role of security needs to change—and quickly. The traditional view of identity and access management (IAM) is insufficient to meet the needs of the new reality. Provisioning, single sign-on, user authentication and federation are all essential technologies, but by themselves, they will not enable the organization to incorporate and leverage the new trends that are transforming our business and technology environment today.

This paper will highlight some of these trends and explain how they could impact your security strategy. It will also introduce an identity-centric suite of capabilities that can serve as the foundation of a strategy that can not only protect an organization from threats and attacks of many kinds, but also help enable new business opportunities to help grow the business and improve customer engagement. Most importantly, it provides a detailed analysis of the key capabilities and attributes of a security solution that are critical to success.

This document provides an overview of the critical capabilities required for an effective and comprehensive identity-centric approach to security. Very few organizations acquire a complete identity solution all at once. They generally deploy one or more components to solve an immediate challenge, then extend that to include more capabilities as their needs expand, and as the initial deployment shows significant success. So, consider this document to be a roadmap to how to achieve the benefits you desire and the capabilities required to get there.

CA Technologies is proud to be a leader in the application economy and to provide solutions that can help every organization succeed in both enabling and protecting their business.

Steve Firestone
General Manager, CA Security

What is The Application Economy?

The Changing Security Landscape

The last two years have caused huge changes in how your organization interacts with its employees, partners and customers and in what you need to do to protect it from threat and attack. The old security methods are no longer sufficient and must be enhanced with further capabilities to help keep the enterprise secure. The most significant security trends today include:

- **Rapidly increased workplace expectations** for how business apps and services are delivered and consumed. As the "face of IT" to the business, enterprise IT service delivery teams are looking for new, modern service management tools to replace outdated, inflexible systems which are hard to use, heavily customized and require more resources and budget to maintain and upgrade than they can afford.
- **Bring your own device (BYOD).** Mobility is transforming the enterprise, faster and more intensively than almost any technology before it. It is essential to manage the tsunami of devices, apps and data that are flooding into companies through channels official and otherwise, and that's a challenge unlike any enterprise IT has seen before. Mobile technologies require the extension of security capabilities out to the device, demand control of enterprise data residing on the device and increase the need for user-friendly interfaces across channels.
- **Cloud-computing.** Its promise for simplicity, ease-of-use and lower cost of ownership is here to stay, putting a premium on user experience and solutions which are personalized to the needs of its users in the context of the work they need to do. Security controls must now extend in a transparent way to cloud-based apps and data, and for maximum flexibility, identity services should be deployable in the cloud, on-premise or in a hybrid environment.
- **Increasing velocity of new apps.** A business rides on its ability to deliver new business services quickly. 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. This trend puts a premium on accelerating the deployment of secure, new apps, in order to take advantage of sudden business opportunities.
- **Bring your own Identity (BYOID).** Today's organizations need to offer a way for end-users to securely bring their own identity to their infrastructure while they put in place policies for BYOID that protect the organization.
- **Internet of Things (IoT).** New business opportunities exist for companies that can leverage the huge number of connected devices out there and provide new secure apps that interact with them.
- **Increasing amount and movement of data.** The amount of data and its geographical dispersion is increasing dramatically. As data begins to reside almost anywhere both inside and outside the enterprise boundaries, protection of it becomes a greater challenge. Security controls need to be able to operate effectively in a perimeter-less environment.
- **Increasing sophistication of attacks.** The new breed of attackers are sophisticated, dedicated, often work in tandem in their attack strategies and are motivated by financial gain. New strategies to combat them are needed.

These disruptive trends will cause your role—and your security strategy—to change. And, dealing effectively with them requires a broader team of stakeholders. For example, business leaders will now take on a much more active role in your strategy.

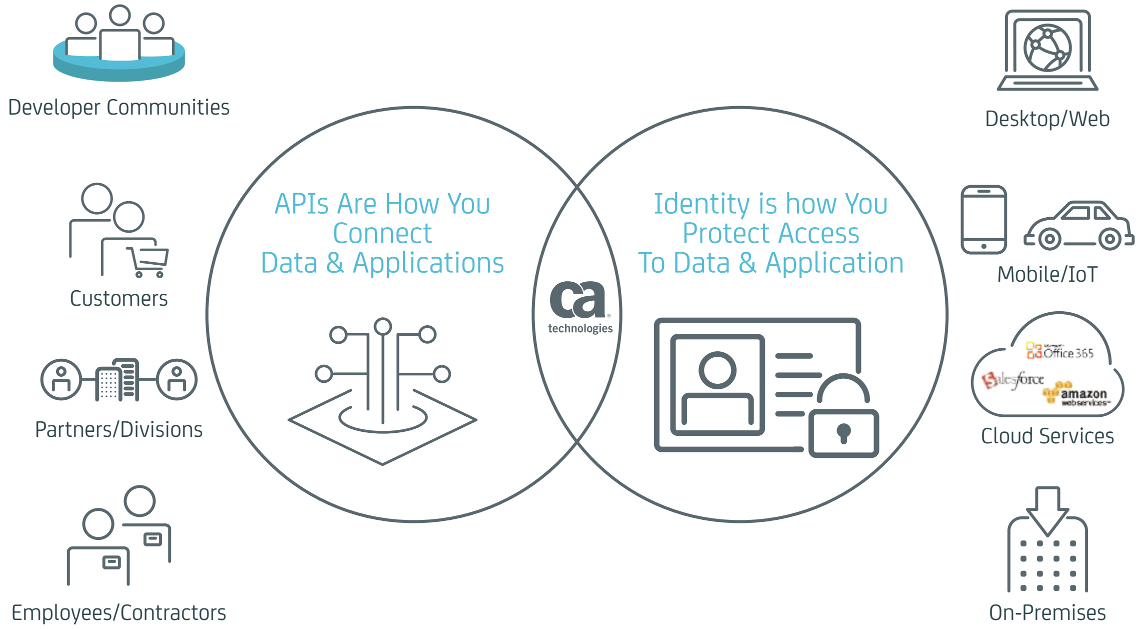
The Increasing Importance of APIs

Organizations need 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. 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. 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 and could reside on-premise, 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. Figure 1 highlights the central role of identities and APIs in the application economy today.

Figure A.

APIs and Identity are the new border and passport for Internet.



Improving Security in 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 their competitive edge, is the agile organization—the one that can quickly unlock the power of data, effectively onboard developer communities and meet the 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.

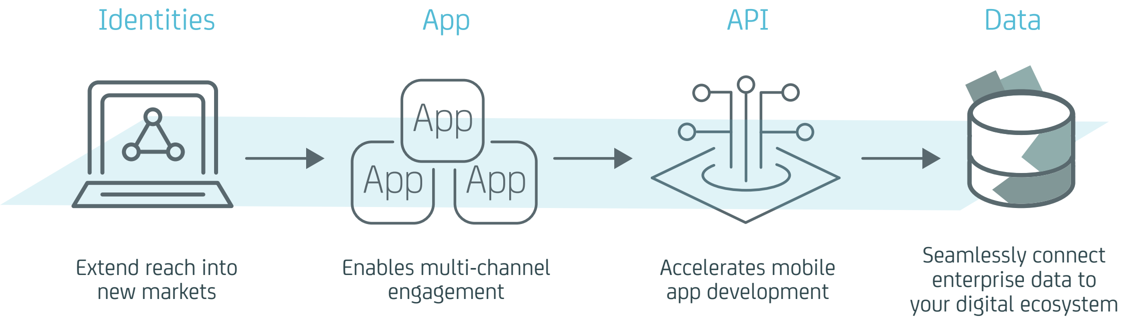
A new identity-centric app delivery platform is needed to meet the agility and security needs of the application economy. But, what would that platform provide? Such a solution would have, at a minimum, the following characteristics:

- It would leverage APIs to support app development efforts and connect the digital ecosystem.
- It would use Identity as the secure access control point that can be embedded anywhere in the app lifecycle, securing the entire channel end-to-end from the app to the backend API.
- It would support and enable significantly improved engagement with your internal and external developers, opening up the opportunity to more quickly take advantage of new business opportunities and new channels.
- It would provide a centralized, policy-based security model that simplifies security management while strengthening key security controls.

The graphic below highlights the key elements of a complete, identity-centric security approach, as well as the profound business benefits that it can provide. The right users using the device of their choice can securely access apps through APIs to get the data that they need. It's a simple model, but one that is essential to providing the flexibility as well as the security needed in today's application economy.

Figure B.

Identity-centric security in the App economy.


Identities
App
API
Data
App
App
App
Extend reach into new markets
Enables multi-channel engagement
Accelerates mobile app development
Seamlessly connect enterprise data to your digital ecosystem

A Strategy to Enable and Protect the Business

With major strategic shifts in business and IT strategy, executives have typically faced a common dilemma: Should I increase my security, or should I focus on growing my business? Just like a two-sided scale, applying more security often meant tightening controls and restrictions, which had a dampening effect on business growth and the user experience. Similarly, when the focus was on opening up new business opportunities, security suffered, which led to an increased risk of a security breach.

This trade-off is no longer tenable. Business executives must find ways to more quickly deploy secure online applications, while IT leaders must deploy security controls to prevent improper access, fraud and information misuse. The future viability of the business depends on it.

The beauty of an identity-centric solution introduced above is that it enables you to not only protect your business, but also to actually unleash it! Speed up the rollout of new apps, improve the engagement with your customers and support them across the channel of their choice (Web, mobile, APIs)—all factors that combine to actually help drive new business opportunities and improve customer loyalty. Let's see how!

In order to succeed in growing while protecting your business, there are at least four critical business drivers that you have. (There are others, of course, but these four form the core of what you need to do.):

1. **Accelerate the delivery of new apps.**
   Your business success may heavily depend on your ability to:

   a. Get new online services out to market quickly.

   b. Provide a platform where developers can easily but securely get access to your enterprise data through APIs.

   c. Reduce the complexity of developing mobile apps.

   d. Eliminate the security silos that often inhibit or delay timely deployment of new apps.

2. **Manage large numbers of distributed identities.**
   As the perimeter has disappeared, user identities are everywhere—in central directories, in the cloud, on partner sites or through social media sites. Users now want to bring their own identity to your website, and your ability to nurture these customers requires support of this capability. These identities must be managed in a cost-effective way that automates the basic provisioning processes and governs user access to help ensure that all users have the appropriate level of access. And, as the number of identities managed can often grow exponentially, scalability to many millions of identities is critical. The benefits include reduced risk of users with excessive privileges, increased employee productivity and improved visibility into who has access to what.

3. **Engage with customers through the channel of their choice.**
   Customer convenience and loyalty is a prime driver of your business growth. If you provide the services that your customers need, a convenient user experience and a reasonably consistent and intuitive interface across all channels, they will continue to return to your site instead of other sites that do not provide as simple a user interface.

4. **Reduce risk and improve compliance.**
   Protecting the business is non-negotiable. You must protect your key systems, apps and data from misuse, improper access and attack. And, to simplify compliance audits, you must be able to prove that your controls are effective. This driver is extremely broad and encompasses the traditional view of identity management, but it is nonetheless essential to truly being able to unleash the business.

These business drivers are broad, but critical to success of the business. Figure C summarizes these drivers and the individual steps that need to be taken to achieve these goals.

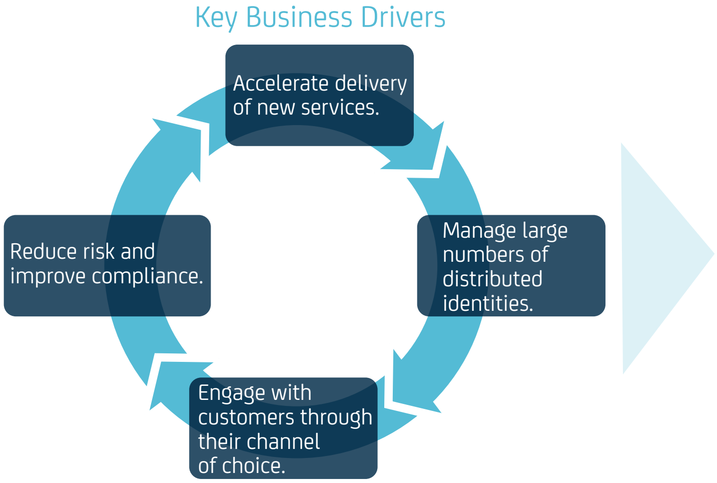

Key Business Drivers
Accelerate delivery of new services.
Manage large numbers of distributed identities.
Engage with customers through their channel of choice.
Reduce risk and improve compliance.

Figure C.

Digital platform business drivers and required steps.

Required Steps

- Seamlessly connect key apps to enterprise data
- Manage APIs and the developer lifecycle
- Manage distributed identities and entitlements
- Securely and conveniently enable multi-channel access
- Provide end-to-end security

Let's look at the specific capabilities and technologies that are helpful in implementing these steps and the benefits that they can bring to your business.

Functional Step	What You Need to Do	Identity Capabilities Required	Benefits to the Business
Seamlessly connect key apps to enterprise data.	▪ Create agile API platforms. ▪ Adapt existing services into modern APIs. ▪ Optimize large volumes of transactions	▪ API gateway ▪ Mobile API gateway ▪ API threat protection ▪ API load mgmt and balancing	▪ Differentiate business with new consumer apps. ▪ Accelerate app release cycles and time to market. ▪ Deliver the user experience consumers and employees expect.
Manage APIs and the developer lifecycle.	▪ Manage APIs like products: API design, publishing, versioning, usage and performance. ▪ Manage developers like customers: marketing, on-boarding, collaboration and testing.	▪ API gateway ▪ Mobile API gateway ▪ API developer portal	▪ Take advantage of new business opportunities and channels. ▪ Improve developer acquisition and relationship development.
Manage distributed identities and entitlements.	▪ Simplify user experience. ▪ Automate identity-related processes. ▪ Control and govern access to sensitive data.	▪ Automated provisioning ▪ Access certification ▪ User profile self-service ▪ Privileged identity management ▪ Shared account management	▪ Gain visibility into who has access to what. ▪ Mitigate risks of users with excessive privileges. ▪ Increase user productivity. ▪ Control what your privileged users can do on your systems.
Securely and conveniently enable multi-channel access.	▪ Simplify registration/login/profile mgmt. ▪ Provide a convenient, consistent experience. ▪ Enable single sign-on across apps and services.	▪ Strong, risk-based authentication ▪ Access management and single sign-on ▪ API security and management	▪ Improved customer experience/loyalty ▪ Coordinated security across Web, mobile, APIs ▪ Accelerated delivery of new apps
Provide end-to-end security.	▪ Protect data throughout entire interaction. ▪ Adopt risk-based approach to user authentication, based on context. ▪ Leverage fine-grained access control for APIs. ▪ Protect data from misuse or loss.	▪ Mobile app security ▪ Strong, risk-based authentication ▪ Access management and single sign-on ▪ API security and management ▪ Privileged identity management ▪ Data protection	▪ Improve customer confidence in privacy of their data. ▪ Increase security without inconveniencing end-users. ▪ Engage developer community to leverage new business opportunities. ▪ Control actions of privileged users. ▪ Prevent data loss and misuse.

What Capabilities Do I Need in The Application Economy?

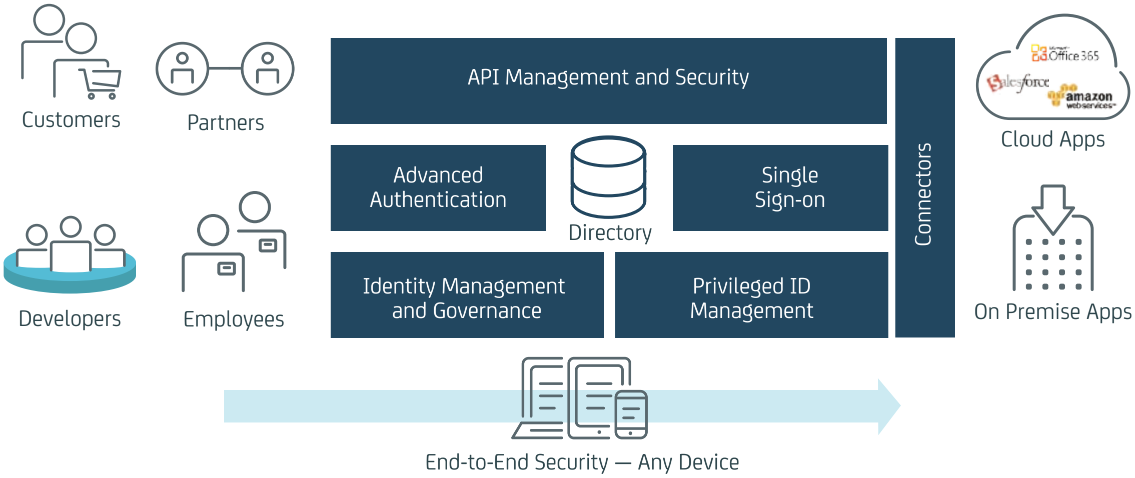
Let's look at the essential components of a comprehensive identity-centric security solution and determine how it extends the capabilities that we normally think of as identity and access management. Most importantly, let's look at how it can provide the critical capability that traditional IAM cannot—unleash the business.

Figure D highlights the key components of the approach. Some core requirements of the integrated solution are that it must:

- Control access to apps, regardless of where they reside—on-premise, cloud, etc.
- Provide flexible deployment options—on-premise, cloud or hybrid environments.
- Ensure end-to-end security—from "device to data center."
- Provide extensive onboarding capabilities for developers in order to attract value-added apps to help exploit business opportunities and channels.
- Provide consumer-level scalability to accommodate the potentially huge numbers of users that will need access to resources.

Figure D.

Identity-centric security solution.



The key component solutions of this solution, and their capabilities, include:

- Identity Management and Governance. Automated provisioning and de-provisioning, extensive connector support to key systems, user self-services, password management, role mining and management, automated access certifications
- Privileged identity management. Shared account password management, fine-grained access controls, virtualization security, Admin reporting and auditing
- Advanced Authentication. Strong, two-factor authentication (from a variety of credentials) and risk-based authentication based on device identification and geo-location, multi-channel fraud management and behavioral profiling
- Single Sign-on (and Access Management). Centralized policy-based authorization, standards-based federation, social login support, centralized session management
- API Security and Management. Developer portal for easy onboarding and support of developers, API gateways for runtime control of API access, threat protection, protocol adaptation, load balancing, etc.
- Directory. Very highly scalable standards-based directory for storage of user profile information
- Connectors. Ease-of-deployment requires extensive connector support for enterprise systems. Capabilities to easily connect with non-standard systems and applications are important also

Given that these are the critical components of an effective identity solution, how can we evaluate solutions in each of these categories? The next section provides information on key capabilities that will help distinguish a leadership solution from one with limited breadth of capability.

How Can I Evaluate Solutions?

How Can I Evaluate Solutions?

This section explores some requirements of the solution as a whole, then explores specific capabilities within each security technology area that are important. There are other basic capabilities that aren't included because they are "table stakes" and almost all credible solutions will offer them. These evaluation matrices focus on areas that will separate an outstanding solution from an average one.

Overall Solution Considerations

Unified Access. Delivers users secure, convenient, and seamless access across apps, devices, and machines, including both mobile and APIs.

End-to-end security. As more transactions are done via mobile devices, it is critical that the entire transaction—from the device to the datacenter—is protected. Starting with device security, strong authentication, transmission encryption, access management, and data protection—the entire end-to-end interaction must be surrounded by strong, seamless controls.

Integration and modularity. An integrated solution reduces costs, eases deployment and administration, accommodates and correlates multiple identity directories and helps ensure cohesive auditing of all identity- and access-related activities.

Internet-level scalability. Both the number of users and the number of applications and systems are expanding rapidly—often exponentially. To support this growth, any solution must support both small and very large numbers of identities (>100M in some cases). Global implementation must be easily accomplished. Identity and access activity never ceases, so a solution must provide nonstop operation, failover and load-balancing capabilities.

Support the devices your users will want to use. Your customers will want to access your apps and data using the device and access channel of their choice. Core authentication and authorization capabilities must be available across Web, mobile and APIs. Mobile users need to have a convenient, mobile-centric experience.

Deployment flexibility. As more organizations begin to move their identity capabilities to the cloud, flexibility of deployment options becomes more important. Services should be deployable on-premise or in the cloud, and the location of the apps being protected (on-premise, cloud, hybrid) should be transparent to the user.

Best in class. Recognized leadership in ratings published by leading industry analysts.

Widespread successful adoption at a variety of enterprises. Look for solutions that have a very strong deployment track record among leading companies across many verticals.

Solution-Level Considerations

Does the solution…	**Yes**	**No**
Provides unified, consistent, and convenient access across Web, mobile, and APIs.		
Provide true end-to-end security (from device to data center)? Can it protect the entire mobile transaction and the data being transmitted?		
Enable flexibility of component adoption, while still providing strong integration across components?		
Scale to support the largest consumer-scale environments (100 million user identities, 1000s of APIs, etc) with high performance and availability? Does the vendor have a proven track record of successful deployments across large, global enterprise?		
Accommodate user devices of choice, and provide security controls across Web, mobile and APIs?		
Support deployment in on-premise, cloud or hybrid environment? Control access to resources that are either on-premise or cloud-based?		
Receive high ratings for the total suite from industry-leading analysts?		
Have a history of deployment at a wide variety of leading companies, across many verticals?		

Advanced Authentication

Does the solution…	**Yes**	**No**
Offer a wide range of credentials—from passwords and knowledge-based authentication (KBA) methods to multi-factor software tokens?		
Leverage user behavioral profiling, transaction values and a calculated risk score to enable step-up authentication as necessary?		
Work in real-time to identify risk, recommend action and provide alerts for case management?		
Provide a customizable risk engine that evaluates risk based on device identification, geo-location, IP address or user behavior?		
Support password authentication without requiring that passwords be transmitted or stored on the server?		
Help meet compliance requirements such as FFIEC, HIPAA, PCI and SOX?		
Integrate tightly with CA Single Sign-On and other Web access management systems?		

API Security and Management

Does the solution...	Yes	No
Enable you to manage all your enterprise initiatives from a single solution, including: partner access to APIs, support for mobile initiatives (including BYOD), a platform for secure cloud integration, as well as SOAP services and REST APIs?		
Support a variety of form factors—Hardware appliance, virtual appliance, on-premise software and cloud-based service?		
Provide a comprehensive Developer Portal to enable developer onboarding, API plan management and API usage and performance tracking?		
Provide API Threat Protection to protect against accidental and deliberate system compromise?		
Provide comprehensive API Management, including API versioning and rollback, API composition, API orchestration and automated API migration across environments and geographies?		
Provide capabilities for partner, developer, mobile and cloud access?		
Ensure reliability, scalability and a single point of administration through features, such as cluster-wide threat protection (for replay attacks), integrated clustering for automated replication of information, cluster-wide rate limiting (for enforcing contractual limits) and automated failover?		
Help meet government and industry regulations, such as PCI-DSS, Common Criteria, EAL4+, VMware-Ready?		
Support both external and internal (key for mobile app development) developer groups?		
Provide enhanced mobile features, such as support for geo-fencing, Web sockets, and application SSO?		
Provide military-grade security? Has it passed federal and military certifications which are important for verticals such as federal government and banking?		
Provide protocol adaptation to simplify the conversion of existing apps to mobile-friendly RESTful APIs, to great simplify mobile app development?		
Provide centralized access control policies to corporate data and applications to accelerate development?		
Convert between popular API types/formats: SOAP to REST, REST to SOAP, XML to JSON, JSON to XML?		
Automatically generate developer tools, including interactive API documentation and code samples in a wide variety of popular programming languages?		
Allow API monetization through the creation of a revenue plan that can be applied to your billing engine with a single click?		
Expose JDBC-enabled databases as APIs with just a few clicks?		

Single Sign-on and Access Management

Does the solution…	**Yes**	**No**
Support multiple methods for strong or advanced authentication, including password, one-time password (OTP) options, X.509 certificates, smart cards, biometric devices, combination and custom methods, Security Assertion Markup Language (SAML) and WS-Federation/ADFS?		
Support enterprise manageability through such capabilities as unattended installs, centralized management of components, scripting interfaces and operational monitoring?		
Support the migration of access policies from one environment (development, staging, production) to another?		
Support different authentication mechanisms for groups of applications?		
Provide deployment architecture option of using distributed Web agents, Web proxy servers, or a combination of both, with policy servers?		
Provide access control to mobile devices accessing Web resources?		
Prevent session and application hijacking via means such as man-in-the-middle/man-in-the-browser attacks, cookie theft, cross-site scripting, cross-site request forgery and spoofing?		
Enable out-of-the-box secure SSO integration with ERP/CRM systems (e.g., Siebel, Oracle, SAP, PeopleSoft)?		
Provide broad auditing capabilities, including activity, intrusion, administrative and time series reports?		
Deliver proven real-life scalability to 100 million users and above?		
Provide a federation platform that can be uniquely configured with each federation partner without requiring custom development?		
Support a multitude of authentication technologies (UIDs/passwords, OTP, smartcards, etc.) to be used by the Identity Provider for authentication, before initiating the federated single sign-on?		
Support multiple options for federated provisioning/identity administration, such as support for SPML, delegated administration and XML/Web service APIs for initiating user account creation?		

Identity Management and Governance

Does the solution…	Yes	No
Include an easy-to-use, business oriented interface that enables easy administration of user identities for admins and managers?		
Enforce segregation of duties based on the user's job roles and other aspects of their relationship to an organization?		
Include a robust yet simple-to-use access request process with a shopping cart-like experience?		
Provide a simple mobile app for password self-service and workflows approvals that any business user can use to interact with the solution from a mobile device?		
Provide advanced identity analytics to synthesize high volumes of end-user entitlements to identify users with excessive privileges and potential patterns or risk?		
Provide out-of-the-box connectivity to a wide range of systems from mainframe to Web and SaaS?		
Deliver proven real-life scalability to 100 million users and above?		
Include simple (wizard) tools to simplify connections to custom applications using standard interface protocols such as LDAP, ODBC and Web services?		
Support deployment on-premise or in the cloud?		
Allow certification, access requests and profile updates to be performed on both a portal application and a mobile device?		
Provide an entitlements catalog to hide technical details from business users while presenting them with terminology they understand and can relate to?		
Enable consistent enforcement of access policies (at the time of requests) using SAP GRC's rule set to simplify cross-system controls?		
Proactively identify potential access risks of new or changed access rights and provide option to warn or prevent the access from being approved?		

Privileged Identity Management

Does the solution…	Yes	No
Provide fine-grained control over access to sensitive server-based resources, programs files and processes?		
Enforce segregation of duties based on the user's job role to enable appropriate levels of server access?		
Support creation of access policies include date and time, login method, network attributes and access program?		
Trace actions made using Superuser account privileges back to the original user identity?		
Protect virtualization platforms, such as VMware?		
Support access policies that can be deployed in a hierarchy to enable automated policy distribution, updates and reuse?		
Generate granular audit trails of all user actions to whatever level is needed?		
Allow administrators to securely delegate temporary access rights to other users?		
Restrict users to perform sensitive operations only through approved applications?		
Maintain the integrity of audit logs through self-protection and limited auditor access?		
Manage and control passwords to shared privileged accounts via a password safe?		
Enable UNIX and Linux authentication and SSO via Kerberos from Active Directory?		
Provide workflow-enabled emergency access and access requests for the password safe?		
The password safe supports interactive/administrative check out and check in, as well as programmatic check out and check in?		
Capture video records of admin sessions for improved forensic analysis?		
Integration with Identity Management and Governance solutions?		

Note: for a comprehensive Buyer's Guide for Privileged Identity Management, please consult:
https://www.ca.com/us/register/forms/collateral/buyers-guide-for-privileged-identity-management.aspx

What are the next steps?

Deploying a comprehensive identity-centric security suite is not quick and easy. It requires planning, communication and working effectively across organizational boundaries within the enterprise. Often, it requires rethinking existing security strategies and approaches, and this can be challenging in many organizations that are not agile enough to adapt to the changing needs of the application economy. But, the benefits can be profound, and can help you drive your business and improve your competition position.

Start small. Don't bite off more than your organization can chew initially. Focus on the critical needs first, because this will increase the commitment level and therefore the likelihood of success. Show some early success, measure it and communicate it, and your path will be much smoother as you extend your strategy to include more comprehensive capabilities.

Develop a long-term architecture. But, don't try to fund it all at once. Pick a single app, or a few important ones, and focus on identity-enabling those apps to show some early success. This will help support funding decisions for the rest of your architecture.

Go to the Business now. Engage with them and understand their needs for business enablement. Have a conversation about what the Business needs—automation, cloud services, mobile access to data, social sign-in to capture more info on their customers, etc. They will want to protect their data, but their needs are far broader than this—and a comprehensive identity solution can help meet those needs. It will also help the security organization to be seen not as a blocking function, but as one that can help enable a stronger and more agile business. It can help you gain a more prominent seat at the planning table.

Develop a strategy for "identity as a dial-tone." Identity and API management can provide a service to the entire enterprise, rather than just serve as a back-office function. Consider having this vision as the foundation of your strategy, since it will help underscore the impact and benefits that this approach can provide. A ubiquitous identity service can help simplify mobile app development, centralize policy management, improve efficiencies and help support the growth of customer initiatives.

Make sure you have the capability to protect your key data. The impacts of a data breach are well-known, especially to those companies that have suffered through one. Your data is likely being attacked right now as you read this document. There is no single "silver bullet" to help prevent these attacks, but there are some technologies that can significantly improve your chances of preventing a successful breach. Implement data classification and protection, privileged identity management and strong, risk-based authentication to provide an effective barrier to data loss through either internal misuse, or external attacks. Breaches will happen! But, you can detect them earlier and prevent many or most of them with careful deployment of these types of technologies.

The CA Advantage

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

A comprehensive identity-centric security 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 no other suite vendor provides—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.

Best of breed products. Each solution within CA Securecenter has been rated as being a "Leader" 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, market-tested 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.

Architected to fit/integrate into your existing environment. The components of the CA Security Suite are designed to fit easily into complex existing environments. From a wide variety of connectors to enterprise applications, to support for standards-based interaction with existing components (including competitive solutions), the CA security solutions are designed to make integration and deployment as easy as possible.

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.