SERVICES DESCRIPTION

CA Identity and Access Management MSO

At a Glance

For your clients today, identities represent the new security perimeter—the only way to deliver timely access to resources while safeguarding sensitive assets. While IT organizations need to support identity and access management (IAM) for an increasing number of cloud-based services, applications and users, they lack the time, tools and expertise required to do so. With the CA Identity and Access Management Managed Service Offering (MSO), you can deliver robust IAM services that address this urgent market demand. This pre-packaged offering equips you with the sophisticated platform and resources you need to deliver advanced IAM services to market—with minimal up-front investment and risk.

The Market

As organizations grow increasingly reliant on a mix of internally sourced and cloud-based services—while security threats continue to escalate—the demand for strong IAM capabilities grows more urgent and widespread.

The Need

Security teams are being tasked with delivering IAM services and applications that have to support more users, use cases and environments. To do so, they need advanced IAM capabilities that provide strong security while streamlining administration.

The Opportunity

Tap into a rapidly expanding market by delivering cost-effective, pay-as-you-go IAM services that scale with your clients' business and security demands. Boost your market share while you help your customers strengthen security, respond more quickly to changing demands and deliver a better user experience.

The Increasingly Urgent Demand for IAM

Whether they're government agencies or enterprises of virtually any size, your clients have to contend with increasingly persistent and sophisticated adversaries and attacks. These organizations also have to manage the efforts required to comply with increasingly stringent regulatory mandates, or face escalating fines when they fall short of these requirements. Given these realities, relying on static user names and passwords is an approach that is increasingly proving to be a weak link in an organization's defenses.

This weakness is being exacerbated by the shifting business and technological environment your clients operate in today. As these organizations continue their move to the cloud and other externally hosted environments, the dynamics of managing security also change substantially. These changing environments serve to intensify the need for strong authentication and access controls. In fact, IAM represents one of the top concerns executives have when moving to the cloud.

IAM: Customer Implementation Challenges

Whereas in the past, security teams could solely focus efforts on a well-defined, static perimeter, they now also have to focus on securing data and identities. IAM is both more critical and more challenging than ever. In effect, identity represents the new perimeter—the only way for security teams to control, track and report on how corporate assets are accessed, when and by whom. As a result, investments in IAM capabilities are expected to increase substantially in the coming years. However, managing IAM is increasingly complex, especially given the hybrid, dynamic nature of infrastructures and business applications in use today.

These issues are compounding many ongoing challenges organizations contend with in managing IAM efforts internally:

- **Manual efforts**. Too often, administrators are saddled with manual processes associated with such efforts as setting up new users, changing users' permissions, following up on lost passwords and so on. For example, when administrators have to provision new users,

they need to manually look up associated groups and roles to determine privileges. These manual efforts are error prone and impose a significant administrative burden and cost on the IT organization.

- **Poor visibility**. Often, IT and security teams don't have any central way to track and manage access requests, which makes compliance efforts and security audits more time consuming and prone to errors.
- **Inconvenient services**. When users want to sign up to change their privileges, they have to hassle with paper-based forms and processes that are slow and inefficient. Ultimately, these delays hurt productivity because it takes so long for users to get the access they need.
- **Inadequate scalability**. When organizations need to support more applications, users and authentication processes, all the above issues significantly hinder the IT organization's ability to meet this demand.

Monetizing IAM Services: The Customer Requirements and Value

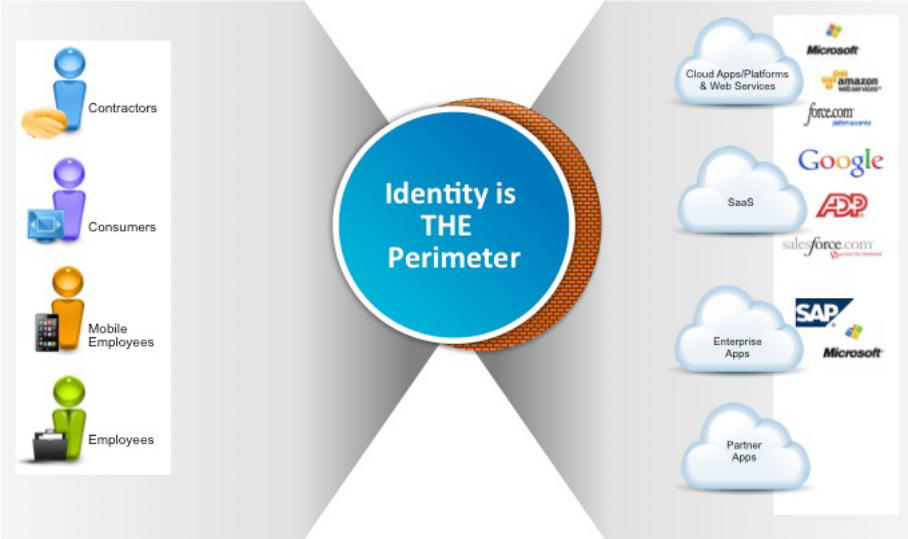
Given the changing dynamics taking place, a significant opportunity is opening up for service providers. Those organizations that can deliver cost-effective services that help customers address their IAM requirements moving forward will be well positioned to capitalize on the market's growth in the coming years. The following sections provide a look at the requirements for capitalizing on this opportunity and the value service providers can deliver as a result.

Requirements

To deliver a compelling IAM service today, service providers need the following capabilities:

- **Complete coverage of hybrid environments**. As organizations' cloud services continue to grow more widespread and vital to the business, IT teams need to have IAM capabilities that span all the environments that matter, including the traditional internal IT infrastructure as well as private and public cloud services.
- **Automation**. To meet the growing demand for IAM services, and to contend with the increasingly dynamic and complex environments in which these services are deployed, it is incumbent upon IT organizations to leverage automation wherever practical. This includes offering users self-service access to portals for requesting new services or changes as well as the automation of workflows, approvals and provisioning when those requests are submitted.
- **Robust controls**. Ultimately, it's most critical that IAM supports an organization's security objectives. Toward that end, it's vital to leverage platforms that can support a range of authentication methods and that can apply more rigorous controls when highly sensitive assets are being accessed or high-risk situations arise.
- **Streamline user experience through single sign-on**. The user experience is critical as it plays an integral role in both user productivity and security: If authentication processes are too time consuming, users will find ways around them, and policies won't be adhered to. As a result, it's critical that IAM implementations support the single sign-on (SSO) initiatives that help boost user convenience while enabling more centralized security administration.
- **Deliver maximum scalability, security and availability**. When IAM services are implemented, users count on them continuously. If these services should fail or suffer from performance issues, productivity and security can take an immediate hit. That's why it's vital to have IAM services running in environments that deliver maximum up time, that can scale to support growing usage and use cases and that have strong security mechanisms in place.

In today's increasingly cloud-based environments, identities represent the key means for safeguarding access and sensitive assets.



Value

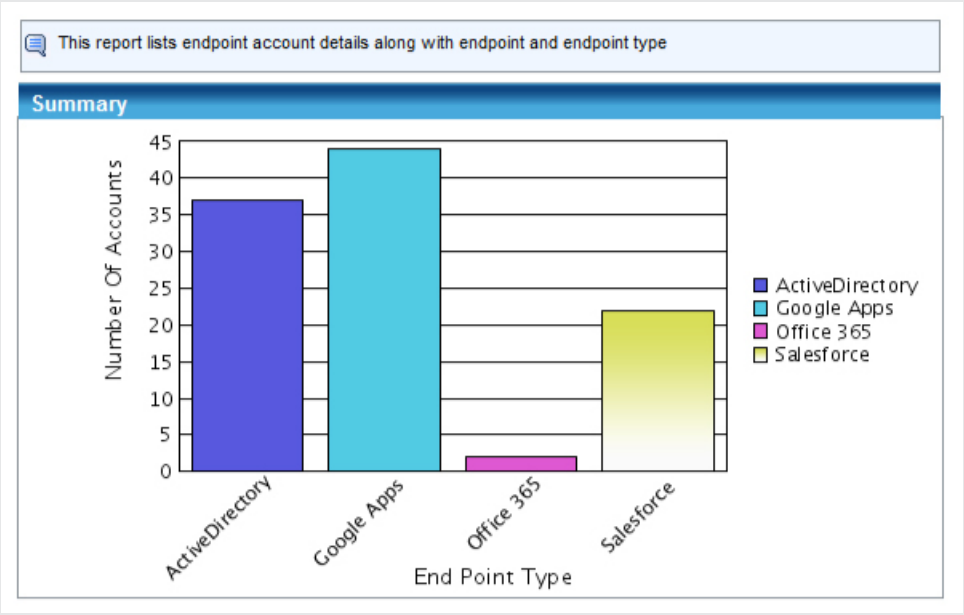
When service providers can deliver IAM services that address the requirements above, they can help their customers realize a number of benefits:

- **Improve end user experience**. By leveraging SSO implementations, users can spend more time working and less time logging in,

trying to remember passwords and following up on forgotten or lost credentials. Further, when they can gain self-service access to portals that enable them to request permission changes, reset passwords and so on, they ultimately enjoy more convenience and faster response.

- **Maximize ROI**. By leveraging a comprehensive IAM service, organizations can strengthen security while reducing costs and improving staff efficiency. Available via a predictable, pay-as-you go model, these services enable customers to eliminate the need to do IAM platform procurement, implementation and support. This means they don't need to hire or train internal IAM experts. Further, when many routine administrative tasks are automated, staff quickly become more efficient and deliver more value to the business.
- **Enhance agility**. By providing central management across cloud and internal environments, these services enable customers to respond to changing requirements faster. These externally hosted services make it much easier for customers to scale or contract their capacity as business demands dictate, and when new applications or services come online, IAM services can quickly be updated to support them.
- **Improve security**. By leveraging robust IAM capabilities that provide centralized control across both internal and cloud environments, customers can reduce risk and strengthen compliance with security policies and regulatory mandates. These IAM services enable security teams to automatically apply stronger controls for higher risk situations, and to institute robust safeguards through separation of duties, granular access management and other capabilities.

With ca **Secure**center solutions, you can provide your customers with a range of reports, including user accounts by application.



CA Identity and Access Management MSO

Now you can harness the tools and resources your organization needs to deliver high-value, differentiated and profitable IAM services to clients. CA Identity and Access Management MSO is a complete, pre-packaged bundle that provides the tools you need to deploy and run IAM services, and it offers the best-practice guidance you need to optimize these deployments. In addition, the MSO delivers the sales, marketing and business enablement resources you need to launch these services in the market.

With the CA Identity and Access Management MSO, you can deliver a comprehensive IAM solution with the following services, which can be bundled or delivered individually:

- **Identity management service**. The MSO enables you to deliver a complete identity management service, including the initial implementation of the platform and ongoing user management services. Support access requests, new user provisioning and identity synchronization. With the ca **Secure**center suite of solutions, you can deliver automated user provisioning, including capabilities for adding, modifying and deleting user accounts. In addition, you can enable users to make online requests that initiate streamlined workflows and approvals based on the policies defined.
- **SSO service**. With this offering, your clients can deliver an improved experience to users by enabling them to access applications and services through SSO. In addition, your clients can provide just-in-time provisioning when users make requests to have new services or applications added. You can federate identities for your clients' SAML-compliant applications and cloud services and deliver SSO integrations with applications that don't support SAML.
- **Advanced authentication service**. With this service, you can implement the mechanisms that strengthen your clients' authentication processes and overall security. You can provide services for implementing software tokens, one-time passwords, OAUTH tokens and more. In

addition, you can leverage robust rules and modeling engines that help your clients assess—and dynamically respond to—high-risk behaviors and incidents.

How CA Identity and Access Management MSO Benefits Your Business

Put the CA Identity and Access Management MSO to work for your business, and your organization can realize a range of benefits:

- **Gain differentiation from competition**. Be early to market with IAM offerings that address an urgent and rapidly expanding market demand.
- **Generate new revenue streams**. The CA Identity and Access Management MSO equips you with the capabilities you need to support a range of IAM services, so that you can address more customer needs and win more deals.
- **Deepen account penetration**. With the CA Identity and Access Management MSO, you can start to sell additional services in your existing accounts, so that you can expand your footprint and increase revenue per user.
- **Boost margins**. The CA Identity and Access Management MSO enables you to deliver high-value, high-margin services, so that you can minimize the need to compete in more commoditized markets. This pre-packaged offering is powered by the leading ca **Secure**center suite of solutions. These solutions deliver the automation and self-service capabilities that streamline operations. With these solutions, your organization can get new services to market with speed and cost efficiency.

CA Technologies: A Strategic Partner

The CA Identity and Access Management MSO is backed by CA Technologies, an organization that has over 30 years of experience in providing leading IT management software and solutions to organizations in over 45 countries. Today, more than 750 of the world's largest service providers rely on solutions from CA Technologies. In addition to the CA Identity and Access Management MSO, we offer MSOs for monitoring, enterprise mobility management, XenApp and XenDesktop and data center infrastructure management.

For More Information

Visit the **service providers page** on ca.com to learn more about how CA Technologies is helping its service provider partners boost business results.

The CA Service Provider Center of Excellence delivers an extensive range of enablement services, helping to ensure that you get the targeted assistance and resources you need, when you need them. The Center of Excellence team can help you more fully leverage your technologies and investments, optimize your operations, enhance your go-to-market capabilities and scale intelligently—so you can more effectively accelerate your services and your business.

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**.

Copyright © 2014 CA. All rights reserved. This document is for your informational purposes only, and does not form any type of warranty.