WHITE PAPER | JUNE 2016

Identity and Access Management in the Application Economy

The urgent market demands and how service providers can address them

ca technologies

Table of Contents

Executive Summary

Every day, the demand for advanced identity and access management (IAM) capabilities grows more urgent and widespread, as do the challenges associated with getting it right. By helping enterprise customers address their critical IAM mandates, service providers can capitalize on a significant market opportunity. This white paper examines the IAM market's evolving challenges and requirements, reporting on an extensive survey of enterprise security executives. The paper then details some of the key implications for service providers, outlining the most compelling opportunities for delivering new or enhanced IAM services.

Security Concerns an Inhibitor in the Application Economy

Today's businesses are competing on a new playing field: the application economy. No matter the industry, market success is increasingly being dictated by an organization's applications. More than ever, businesses will need to provide innovative applications that deliver exceptional user experiences—and they'll need to bring these innovations to market with increasing rapidity. In fact, one study found 94 percent of respondents felt heightened pressure to launch new applications.[1]

"More than ever, businesses will need to provide innovative applications that deliver exceptional user experiences—and they'll need to bring these innovations to market with increasing rapidity."

While the pressure to accelerate application delivery mounts, so do the mandates for bolstering security. While cyberattacks aren't a new phenomenon, they've continued to grow increasingly sophisticated and persistent, making strong security more important and more challenging than ever before.

In most enterprises, the demands for strengthened security and accelerated application innovation represent contradictory objectives. When it comes to adopting the innovations that can help fuel faster application innovation, security teams have often raised concerns or roadblocks. For example, security teams may seek to limit their organization's adoption of cloud services in order to retain stronger control of sensitive assets. Due to security concerns, enterprises may avoid extending an internal service to external developers via APIs.

In the application economy, application agility and security can't be viewed as an either/or proposition. Security teams can't be viewed as innovation inhibitors. Instead, they need to foster a new mindset and identify ways that make security an innovation enabler. Robust, advanced IAM capabilities represent a key way for organizations to do just that.

1 CA, with Vanson Bourne, "How to Survive and Thrive in the Application Economy," September 2014, URL: **http://www.ca.com/us/~/media/Files/whitepapers/how-to-survive-and-thrive-in-the-application-economy.pdf**

Introduction to IAM: What It Is, and Why It's So Critical

At a high level, IAM refers to the process of creating, managing and using digital identities and for enforcing access policies. IAM is comprised of both processes and the infrastructure and services required to support those activities. Through advanced IAM, organizations can establish efficient, centralized control and visibility.

Why the need for IAM is growing more critical

In today's rapidly evolving business and IT landscape, fundamentally new security requirements have emerged.

Within a few years, organizations have moved from running largely on-premises, tightly controlled environments, to relying on a highly dynamic, distributed ecosystem comprised of cloud services, big data environments, mobile applications, the Internet of Things (IoT) and more. The result is that sensitive assets and systems are increasingly interconnected and exposed.

IT teams used to be able to build security systems and processes around the concept of a perimeter. Today, simply making clear distinctions between internal and external—let alone establishing foolproof security along these lines—is next to impossible.

Further, organizations are increasingly being targeted by cyberattacks, including those from nation-states and sophisticated criminal organizations. Large-scale data breaches continue to make headlines, and ransomware, spear phishing and many other threats continue to plague businesses. While combatting these threats requires a significant and ongoing dedication of budgets and resources, these investments can pale in comparison to the devastating penalties associated with data breaches—which can entail lost customers and revenues, fines and civil litigation. Further, across regions and industries, privacy regulations and compliance mandates continue to grow more rigorous, which can further exacerbate these penalties.

How advanced IAM can be a business enabler

In the application economy, strong, advanced IAM is emerging as a foundational element, an integral way to fuel enhanced application innovation, while establishing strong safeguards around sensitive assets and services. The following sections offer a look at some of the business benefits that advanced IAM can deliver.

Facilitate adoption of cloud services, while establishing required controls

In recent years, the move to the cloud has been both rapid and massive. Within organizations, the adoption of cloud services has largely been driven by business leadership, with little, if any, involvement of IT. The result is that corporate data, systems and services aren't governed by consistent policies and controls. The rise of so-called "shadow IT" leaves businesses exposed to failed compliance audits and security breaches.

Rather than looking to stifle or thwart the move to the cloud, enterprise IT teams need to facilitate this transition, while establishing the safeguards needed to address security and compliance risks.

IAM can play an integral role in meeting these objectives. Through federated identities and single sign-on (SSO) capabilities, IT teams can give end users the convenience of being able to use one login to access all their business applications, whether those applications are running in the cloud or on premises. This gives users more convenience, reducing the hassles associated with multiple logins, forgotten passwords and

resets. At the same time, these capabilities can grant security administrators significant advantages in terms of efficiency and control. Through identity federation, security teams can leverage a unified, centrally controlled process and platform for policy enforcement, governance and auditing.

Improve the customer experience, user productivity and security

In the application economy, applications continue to get more complex. For a user to complete a transaction, a complex ecosystem comprised of multiple systems and vendors may be called upon to provide intelligence, data or processing. While this complexity may continue to increase, it's vital to streamline the user experience to the greatest extent possible. In order to deliver a satisfactory experience, organizations simply can't require distinct authentication methods for each different environment that comprises a composite application.

For customer-facing applications, a complex or time-consuming authentication process can hurt customer retention, transaction volumes and revenues. For employee-facing applications, a poor user experience can either hinder productivity or increase business risk—if a process proves to be too much of a hassle, users will often try to circumvent procedures and policies.

By enabling federated identities and SSO, IAM enables more efficient control, enhanced security and an improved user experience. SSO enhances employee convenience, enabling users to gain access to all their applications with a single login. Federated identities means that administrators can leverage a centrally controlled mechanism for managing identities and access policies. Advanced IAM services even enable the concept of bring your own identity, so, for example, customers can use their Facebook credentials to register or sign on to an organization's site, making it even easier for them to engage and transact with the organization.

Strengthen business and application agility

In their drive to deliver the compelling, innovative applications that their markets require, enterprises are increasingly employing APIs, outsourced development and DevOps approaches.

To address the demand for faster delivery of secure applications, it is increasingly critical to manage consistent policies across the lifecycle, not just in production, but across development, test, backup and disaster recovery environments.

Through advanced IAM capabilities, organizations can tailor policies and safeguards to specific applications, while retaining centralized visibility and control. Through strong IAM, organizations can more effectively manage external relationships, such as interacting with software development organizations, so they can maximize collaboration, while safeguarding access.

Boost operational efficiency

Given their central, critical role in an organization, IAM services have to be functioning optimally at all times. IAM can require a lot of ongoing activities, putting a significant drain on budget, staff and time. In short, IAM represents an effort that's never done.

With advanced IAM capabilities, security teams can realize a number of advantages:

- **Automation and integrated workflows**. By leveraging robust IAM services, organizations can standardize and automate a lot of the daily tasks that can place a drain on users and administrators. For example, by integrating IAM with HR systems, an organization can have updates in an employee directory automatically trigger associated changes in the IAM platform.
- **Central support of multiple channels**. By leveraging extensible IAM capabilities and services, organizations can establish unified controls that encompass a number of different interaction channels, including web, mobile and API-based communications.
- **Convenient portals**. By leveraging robust IAM services, organizations can establish management and user portals. Through these portals, administrators can intuitively and efficiently manage policies and track usage and compliance. Further, by giving users self-service access to capabilities like resetting passwords and updating information, these services can enhance user satisfaction and offload significant workloads from administrative teams.

Why IAM's potential is not being realized

There's never been a greater need for advanced IAM, and the potential benefits that can be realized have never been higher. However, to date, many organizations have failed to capitalize on all the potential benefits IAM can deliver.

While virtually every organization has implemented at least some IAM capabilities, the reality is that many organizations have fallen prey to common mistakes, which can continue to plague businesses moving forward.

One of the key problems is that IAM has tended to be handled as a one-off project, or a series of isolated projects over time, rather than as a comprehensive, long-term program. When IAM is implemented in a piecemeal fashion, organizations inherently lack the potential advantages of a common, orchestrated architecture. This means internal teams lack centralized management of resources, disparate user directories have to be supported and so on. Further, because teams lack standardized, repeatable processes, the prospect of implementing integrated workflows and automation is highly unlikely.

Over time, software, ecosystems and threats continue to evolve, and internal teams face a growing struggle to keep pace. These changes necessitate different skills, programming languages, protocols, data models and so on. For internal IT teams, who have to contend with the gamut of the organization's IT infrastructure demands, it can be particularly difficult to adapt and acquire new skills and personnel at the rate required.

Because of their lack of advanced IAM capabilities, organizations contend with the following realities:

- Ongoing support of IAM is complicated and time consuming, with staff struggling to keep pace with demands for ongoing tasks like privilege assignment and revocation.
- IT can't adapt IAM capabilities quickly enough to support evolving security or business requirements.

These urgent challenges represent a significant opportunity for today's service providers. By delivering high-value, advanced IAM services, service providers can establish a strategic, long-term and profitable relationship with an expanding customer base.

Survey: Assessing the Enterprise IAM Landscape and the Service Provider Opportunities

Advanced IAM is emerging as a critical imperative for enterprises, and a compelling business opportunity for those service providers that can help customers address these requirements. To provide more insights and context into the opportunities for service providers in the IAM market, CA undertook an extensive survey of enterprise decision makers. The following sections offer a recap of the survey's findings and insights into the implications these statistics have for service providers.

Finding #1: The move to the cloud is happening—often under IT's radar

The survey found that just under half of respondents indicated that less than 10 percent of their organizations' applications were running in the cloud. These metrics appear to be much lower than many published reports around cloud service adoption.

This disparity may have something to do with the fact that the group of survey participants was predominantly comprised of IT executives and staff, who may not know the full extent of applications various individuals and business units may have running in the cloud.

Fortune magazine cited a report that underscored the wide discrepancy between IT's awareness and the realities surrounding the proliferation of the cloud in the enterprise. This report indicated that across three major industries—finance, government and health care—IT department personnel believed their organizations had about 60 cloud services on average, while the number is typically much higher. For example, the study reported that the average in financial services was approximately 1,000 applications.[2]

Percentage of business applications that are SaaS- or cloud-based

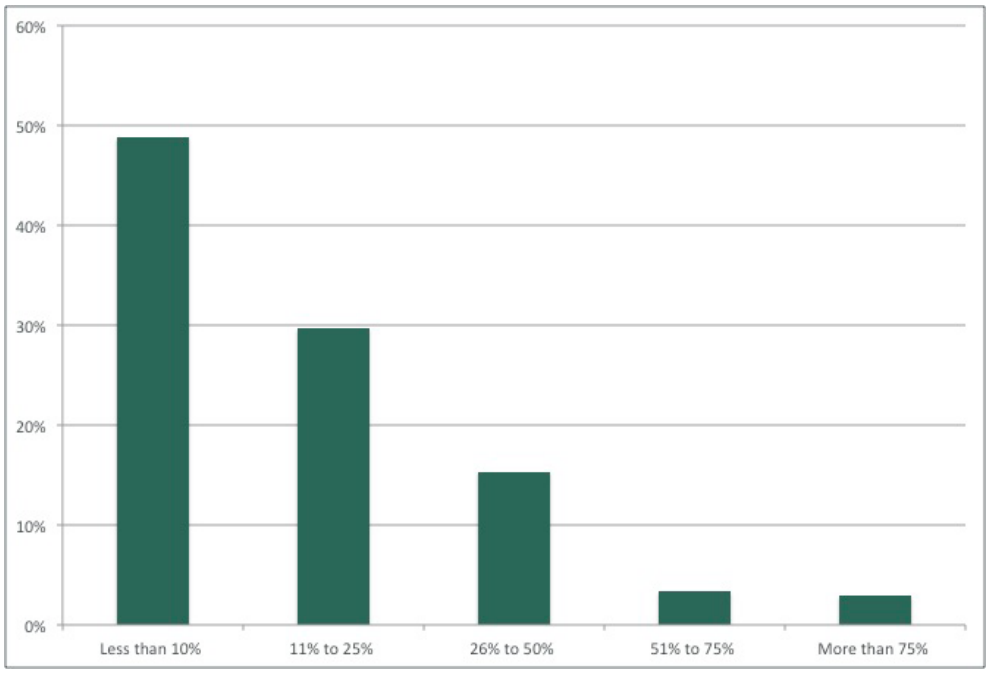


Figure A.

Organizations are running a mix of cloud and on-premises applications, with more than half running at least 11 percent of applications in the cloud.

2 Fortune, "Financial firms gravely underestimate cloud usage, report says", Robert Hackett, August 20, 2015, URL: **http://fortune.com/2015/08/20/cloud-risk-report/**

Even with that potential disparity as a backdrop, the survey still points to the fact that more than 50 percent have greater than 11 percent of applications in the cloud. More broadly, the fact remains that virtually every organization is now relying on a hybrid mix of cloud and on-premises environments.

The takeaways for service providers

Many IT teams appear to be unaware of the full extent of cloud service adoption within their broader organizations, and as outlined earlier, this can ultimately leave businesses exposed to significant risks. Rather than remaining unaware of the cloud services employed or trying to restrict or halt the adoption of these services, IT organizations need to become facilitators of this move.

For service providers, this apparent disconnect between IT and the business can represent an opportunity. By delivering advanced IAM services, service providers can put IT teams in a position to centrally manage identities and access privileges across the business' entire application estate, regardless of the number or mix of applications running in the cloud and on premises.

Finding #2: IAM approaches leaving businesses ill equipped to adapt

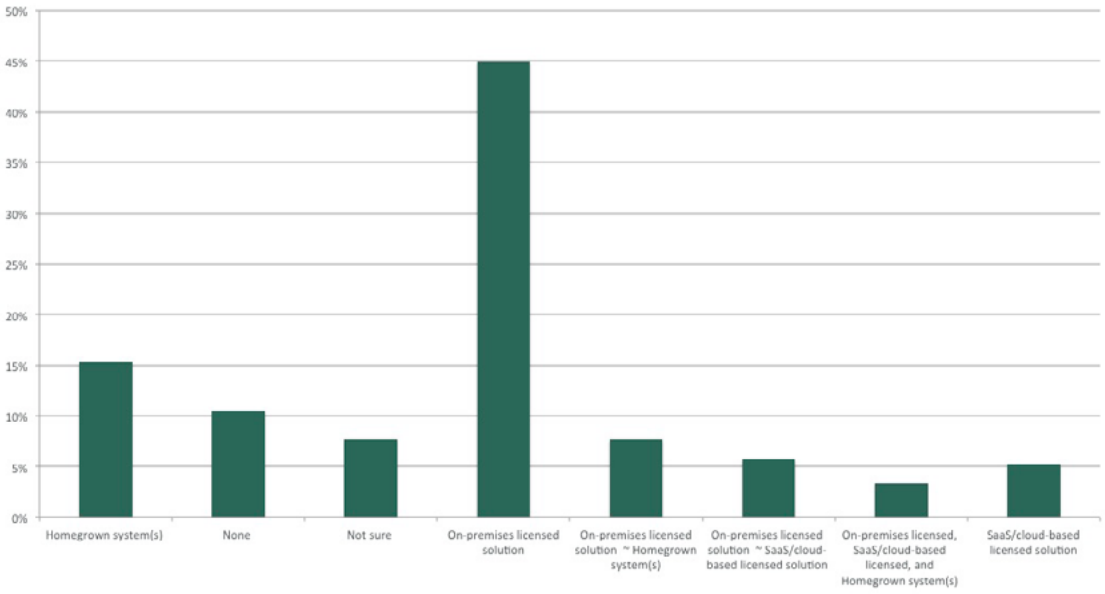
Existing toolsets inhibiting businesses

Respondents were polled on the makeup of their existing IAM tools. "On-premises licensed solution" was by far the most selected category, with a response of 45 percent. It is interesting to note that close to 20 percent stated "none" or "not sure" and that more than one-quarter of respondents are relying on homegrown systems, either solely or in tandem with other types of tools.

As outlined earlier, IT organizations will need to move away from having security acting as an inhibitor to business innovation and agility. The survey results underscore that current IAM tools and approaches are leaving many organizations ill equipped to make this move.

Figure B.

While on-premises licensed IAM solutions represented the most-often cited category, a large percentage are running home-grown systems.



The number of organizations that are without solutions or relying on homegrown systems is one of the most significant aspects: Organizations will be increasingly hard-pressed to adapt to keep pace with rapidly changing requirements when they're contending with no IAM solutions or homegrown tools, and their associated bolt-on code, scripts and so on. These organizations will urgently need to move to strong, advanced commercial IAM platforms.

In addition, organizations need a solution that's architected for today's hybrid IT environments. The reality is that homegrown systems and many commercial solutions released in prior years weren't architected for these hybrid environments. These legacy systems don't enable security teams to leverage central capabilities for managing provisioning and access controls for cloud and on-premises applications. Many solutions aren't equipped with capabilities for establishing unified directory structures. For example, because they lack support for standards like SAML and WS-Security, it's very difficult to support cross-domain interoperability.

IAM efforts time and resource intensive

The survey queried respondents on the frequency of staff's involvement in a range of IAM-related activities. The survey featured 13 potential efforts, and for at least 20 percent of respondents, each of these tasks were performed on a daily or hourly basis. Many of these tasks include tedious functions like rotating passwords and provisioning and deprovisioning users, which was cited as being conducted on a daily or hourly basis by 45 percent of respondents.

Ultimately, the breadth and scope of tasks required leave many organizations challenged with staying on top of some of the most critical efforts. For example, almost 70 percent are not doing critical efforts, like breach monitoring, on a daily or hourly basis.

How frequently does internal IT staff perform IAM functions?

(Rate 1-5, 1=Infrequent e.g. Quarterly, 5=Very frequent e.g. hourly)

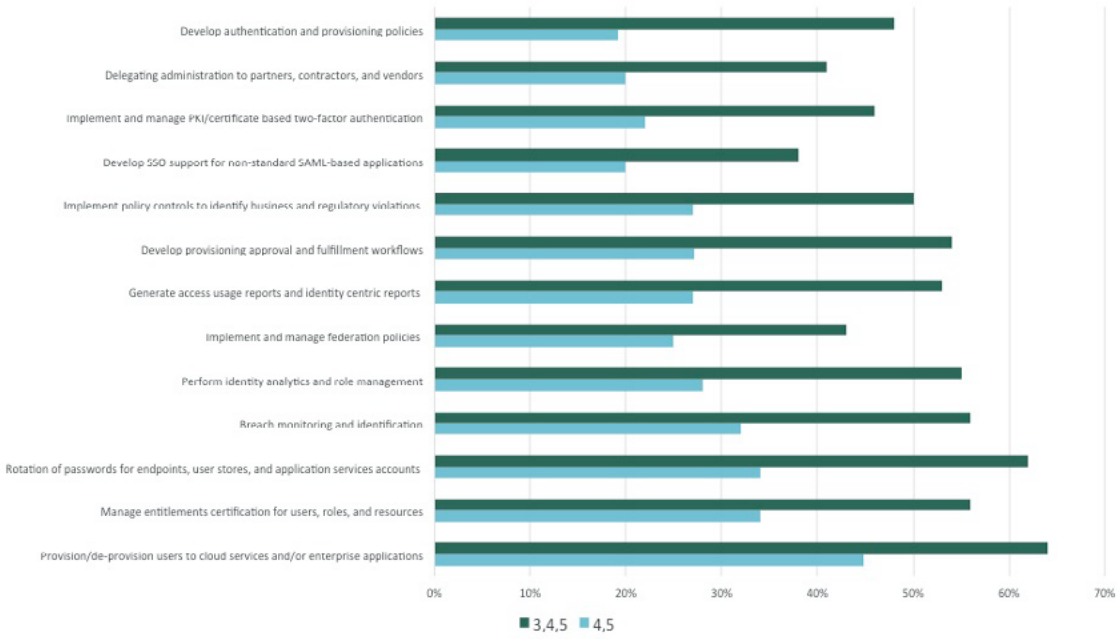


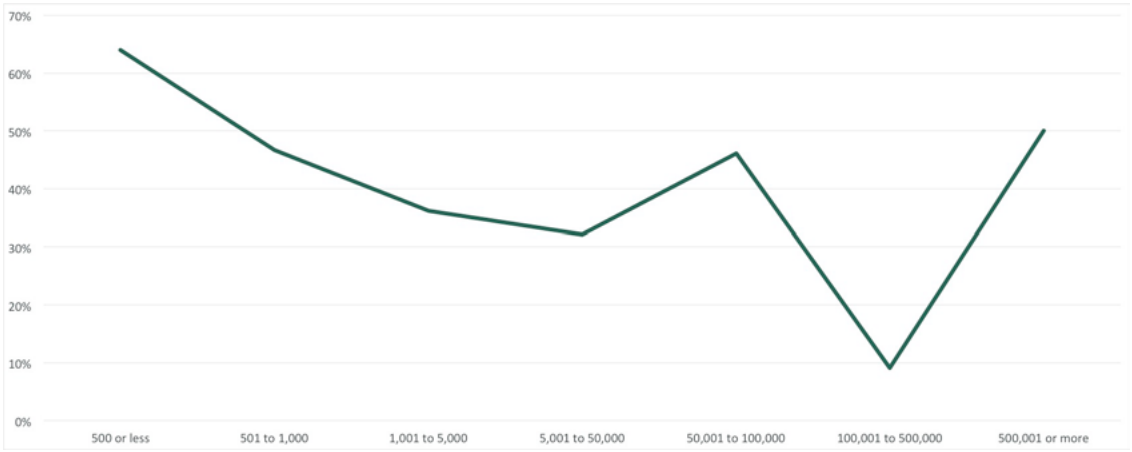
Figure C.

Managing IAM represents a significant effort, with 20 percent of respondents carrying out 13 tasks on a daily or hourly basis.

What percentage of IAM processes are manual?

Figure D.

Automation represents a critical factor in scaling IAM operations.



Automation: Key to scale, but many lacking capabilities

Respondents were also surveyed on the manual nature of their IAM processes. There's a clear disparity between organizations with a small number of identities to manage and those with high volumes of identities. For organizations with 500 or fewer identities, more than 60 percent of processes are manual. For those with 100,000 to 500,000 identities, less than 10 percent is manual.

These numbers serve to illustrate the importance of moving away from manual efforts as businesses look to scale their identities. The need to automate can grow vital—and arise very quickly, for example, if an organization suddenly needs to start managing identities of its customer base rather than just employees, or an organization goes though a merger or acquisition.

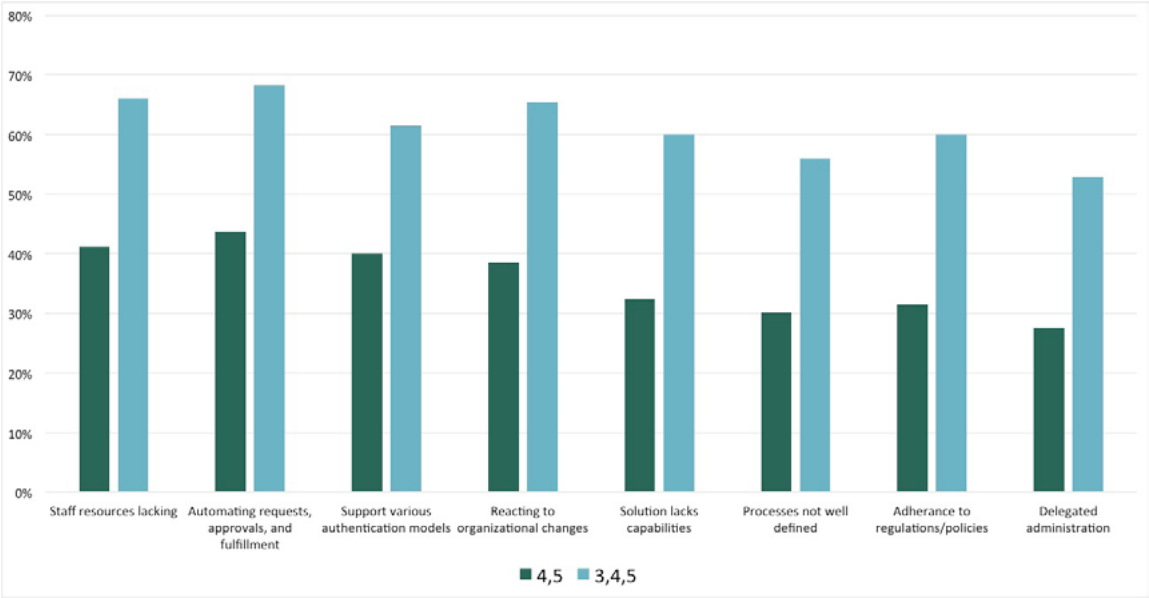
When asked about the challenges respondents are seeing with their existing IAM systems and processes, "Automating requests, approvals and fulfillment" was the option selected by more respondents than any other category.

Challenges with existing IAM systems and processes

(Rate 1–5, 1=Minor, 5=Significant)

Figure E.

Organizations face a range of IAM challenges, with automation being one of the most prevalent.



Organizations at early stages of IAM maturity

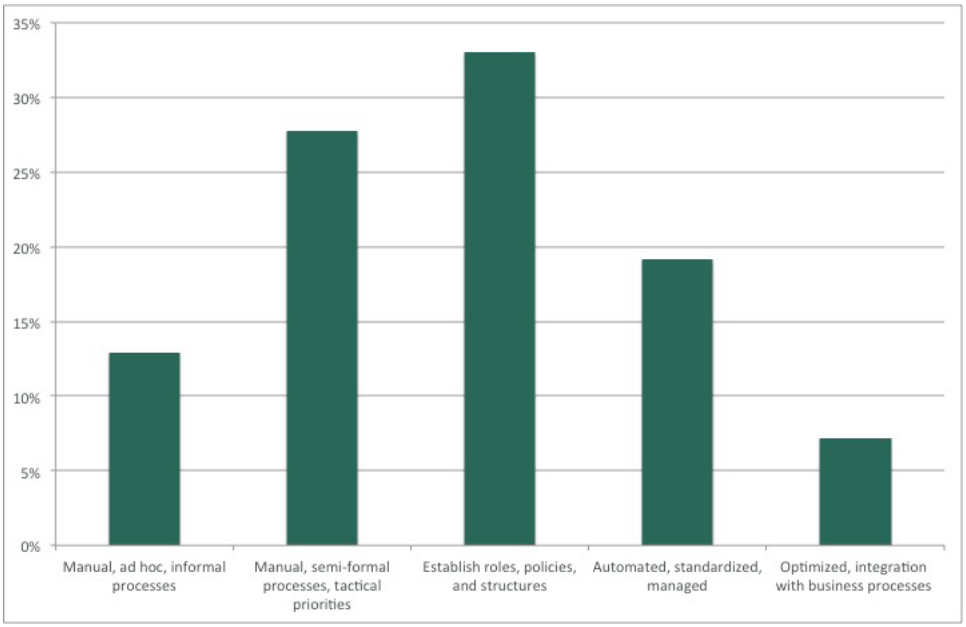
Within enterprises, IAM's advancement is a long-term journey. Particularly in smaller organizations, early IAM implementations will be characterized by manual, ad hoc processes and piecemeal tools. Over time, organizations tend to establish more formal, standardized approaches, which sets the stage for automation and optimization over time. The survey looked at where respondents were in this evolution.

Almost three-quarters (74 percent) of respondents haven't evolved their capabilities past the point in which roles, policies and structures are established in a more formal fashion. Less than 20 percent have automated, standardized processes, and just over five percent have reached the point at which they have optimized their IAM operations.

How would you assess your company's IAM maturity?

Figure F.

Almost three-quarters of respondents have not reached the point at which IAM processes and tools have been automated and standardized.



The takeaways for service providers

The survey results make clear that IAM is an arena that's ripe for optimization in the vast majority of organizations. Given the breadth and scope of activities required to support IAM in businesses, the potential gains are significant: Even slight efficiency gains can make a big difference in the business' finances and agility.

To establish the requisite capabilities, security teams will need to manage the investment and implementation of new IAM platforms. However, many internal teams lack the time and expertise needed to get maximum benefits from these tool investments. Those service providers that can help enterprise security teams with these transitions—which could include everything from tool evaluation and selection, to implementation and ongoing support and optimization—can address a significant and rapidly expanding market demand.

Service providers can deliver significant value when they help advance customers' IAM maturity. By adding or expanding their focus in IAM, service providers can establish the expertise, tools and services that help customers:

- Offload a lot of manual, time-consuming efforts and free up time to focus on more strategic endeavors.
- Establish the standardization and automation that can deliver breakthroughs in security, agility and operational efficiency.
- Gain the refined tools and capabilities that enable optimized services.

Finding #3: Customers are dissatisfied with current approaches

The survey polled respondents on their levels of satisfaction with their current approaches, and the results make clear there's a lot of dissatisfaction. Across all organization sizes, only 15 percent say their current systems fully meet their needs. Thirty-eight percent say their systems don't meet their needs or need substantial improvement. Combined, almost 70 percent say their systems don't meet their needs, need substantial improvement, or leave some room for improvement. Further, that figure rises to over 90 percent in some organizational categories.

Not surprisingly, the survey responses also point to a clear correlation between dissatisfaction and IAM maturity. When looking at survey respondents that indicated they are at the lowest end of IAM maturity (those who indicated they had manual, ad hoc processes) more than 35 percent say their systems don't meet their needs and about 45 percent say they need substantial improvement.

The takeaways for service providers

The high level of dissatisfaction among many respondents underscores the urgency of the need for effective IAM: IT executives are clearly aware of the issues and the need to address them quickly. By delivering IAM services, service providers can alleviate pain points that IT leaders are acutely aware of and so address a significant market demand.

How satisfied are you with current IAM systems and processes?

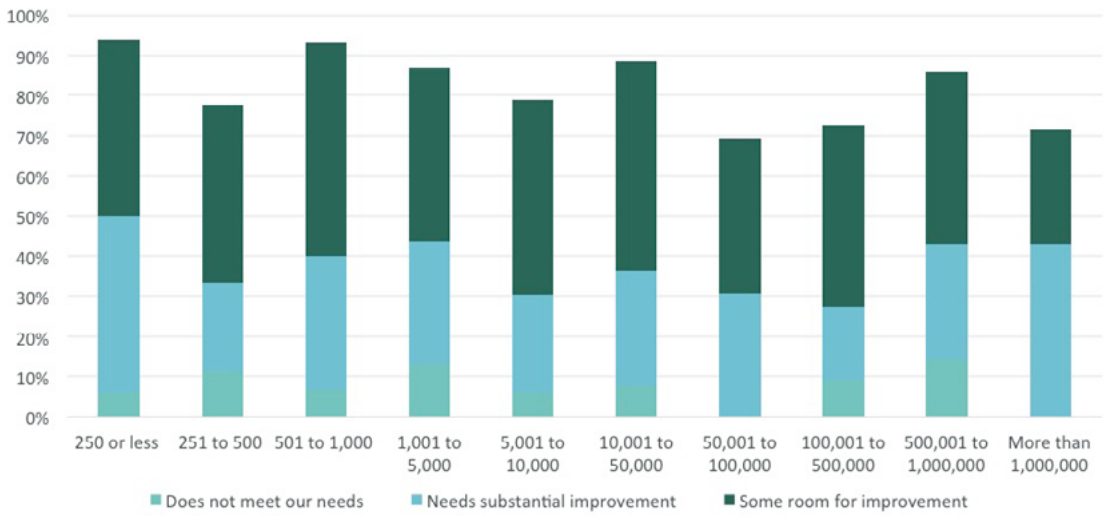


Figure G.

Across all organization sizes, only 15 percent indicate current systems fully meet their needs.

Higher rates of dissatisfaction for those with manual approaches

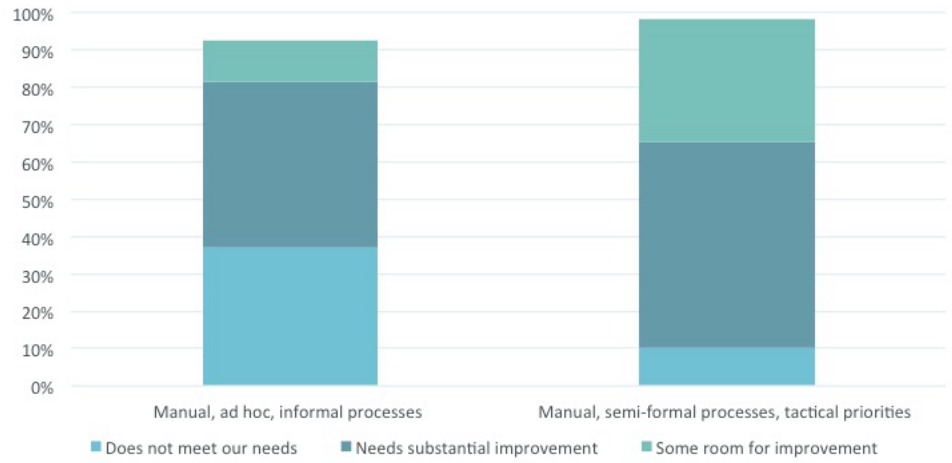


Figure H.

Survey responses show a clear correlation between immature IAM processes and high dissatisfaction.

Finding #4: Customers' challenges and requirements are significant

In today's organizations, there's a broad swath of areas in which businesses need to improve. As outlined in figure E above, following are the top four IAM challenges cited by respondents:

- Automating requests, approvals and fulfillment
- Lack of staff resources
- Supporting various authentication methods
- Reacting to organizational changes

As outlined earlier, many organizations continue to be saddled with ad hoc processes and manual efforts. These challenges present significant hits to the business:

- It takes too long to get new hires the access they need so they can start being productive.
- Sales and marketing efforts are stifled because it takes too much time and effort for potential customers to interact with the business.
- Businesses can't adapt as quickly as needed to changing opportunities and challenges.

The survey looked at the number of IDs managed by respondent organizations, and responses ranged from less than 250 to more than one million. However, critical mass was found between 1,000 and 50,000 IDs; approximately 63 percent of respondents fell within this range. Approximately 20 percent of organizations have greater than 50,000 IDs.

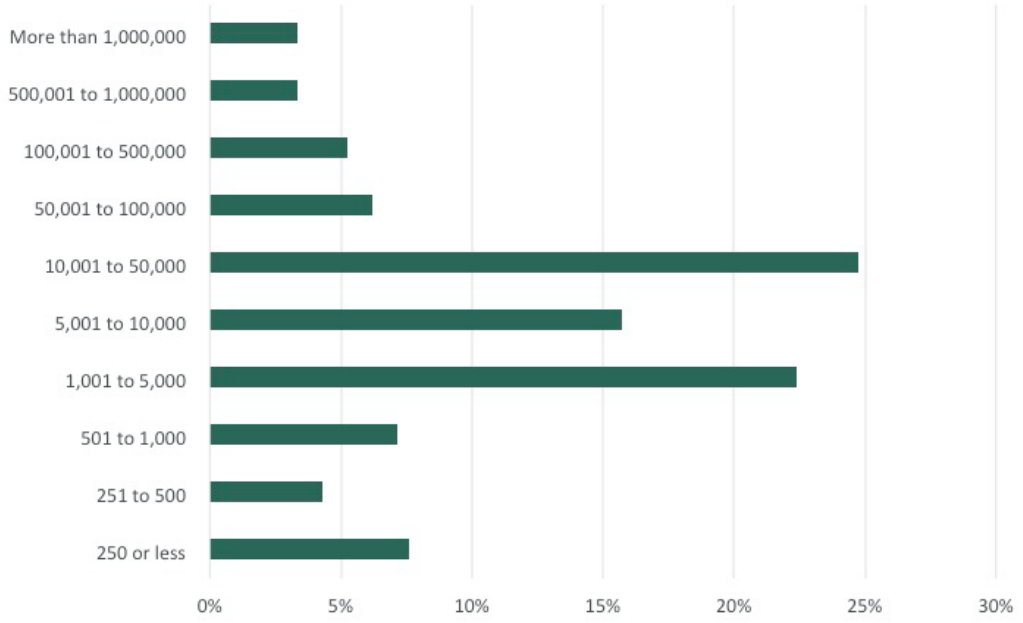
In assessing these numbers, it is important to recognize that IDs managed doesn't necessarily have a direct correlation to the number of employees. In a number of industries, including health care and online retail in particular, smaller organizations may have to manage IDs for massive customer bases.

The survey also looked at organizations' annual IAM expenditures, and the numbers show IAM doesn't just place an administrative burden on internal staff, but a significant strain on IT budgets. Approximately 40 percent of respondent organizations spend more than USD$100,000 a year.

How many user IDs are being managed currently?

Figure I.

The number of identities managed ranges widely, but almost two-thirds of respondents have between 1,000 and 50,000 identities to manage.



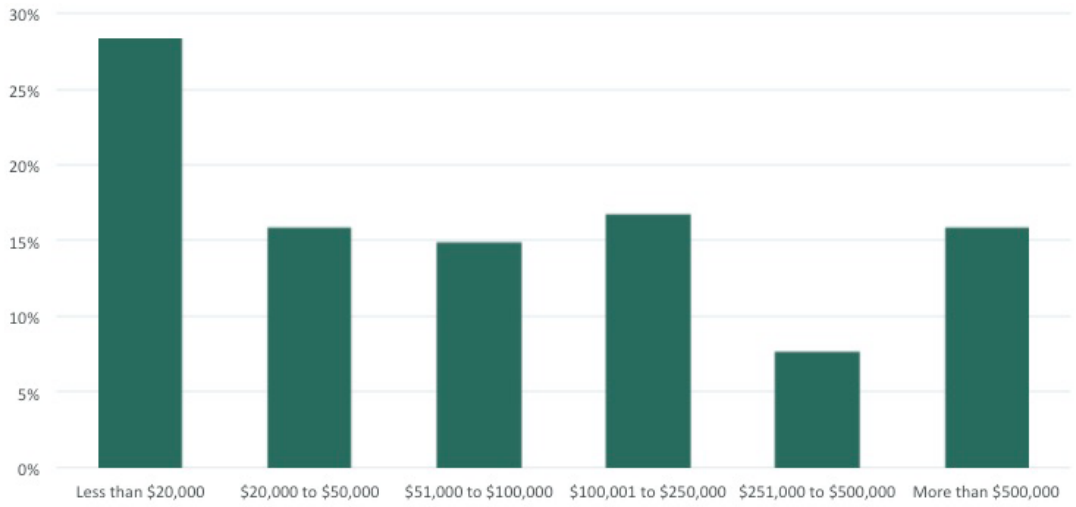
The takeaways for service providers

While the IAM market isn't by any means new, it is a healthy place for service providers to be doing business. As the numbers above show, the IAM market represents one that can yield large deal sizes; and the market is expected to grow. One research firm estimates that by 2020, the IAM market will be worth USD$12.78 billion, up from 7.2 billion in 2015.[3] By delivering advanced IAM services, service providers will be able to address large-scale demands, command large deal sizes and position themselves in a market set to see significant growth.

What is your organization's yearly IAM spend?

Figure J.

IAM represents a significant investment, with 40 percent of organizations spending at least USD$100,000 a year (values in US dollars).



ca technologies

3 MarketsandMarkets, "Identity and Access Management Market by Component (Provisioning, Directory Services, Password Management, SSO, & Audit, Compliance, and Governance), by Organization Size, by Deployment, by Vertical, and by Region - Global Forecast to 2020", March 2016, URL: **http://www.marketsandmarkets.com/PressReleases/identity-access-management-iam.asp**

Figure K.

Several factors are inhibiting further IAM investment, with organizational immaturity representing the most common.

Finding #5: Customers are turning to service providers

The survey examined current obstacles to IAM investment. Results indicate that many organizations are stuck in evolving their IAM capabilities. What prevents organizations from investing in IAM, and advancing their capabilities? Organizational immaturity, unpredictable costs and lack of internal competence were each cited by significant percentages of respondents—and each of these areas are ones in which service providers can change the customers' paradigm and help them get moving in the right direction. Organizational maturity was the most common response, cited by almost 40 percent of those surveyed.

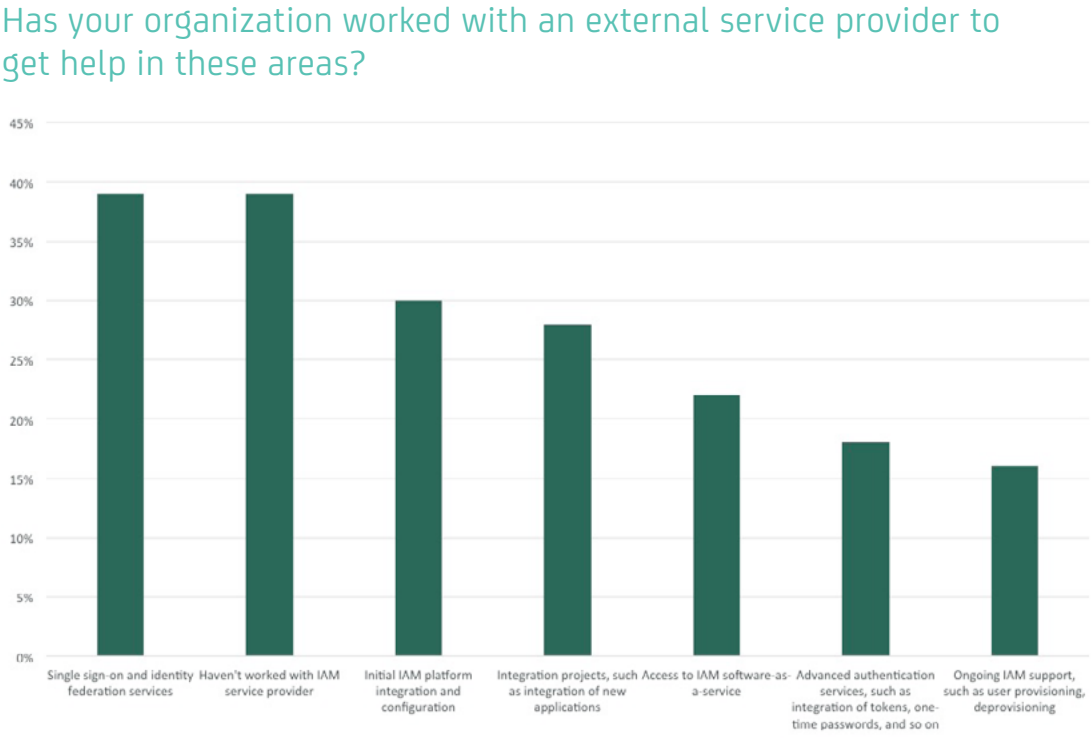


Figure L.

While almost 40 percent of organizations haven't worked with IAM service providers, many have leveraged a range of service offerings.

Enterprise executives open to working with service providers; long-term engagements represent untapped potential

Almost 40 percent haven't worked with a service provider in the IAM area. Those who have worked with service providers have most commonly worked with them for initial IAM platform configuration and integration projects. Longer-term services, including IAM as a service and ongoing IAM support, were the least-commonly selected categories.

The takeaways for service providers

For the most part, a large percentage of respondents surveyed appear open to enlisting service providers to help with their IAM efforts. Fewer than 20 percent indicated they would not adopt IAM managed services. On the other hand, the following four justifications for employing a service provider received at least a 40 percent response:

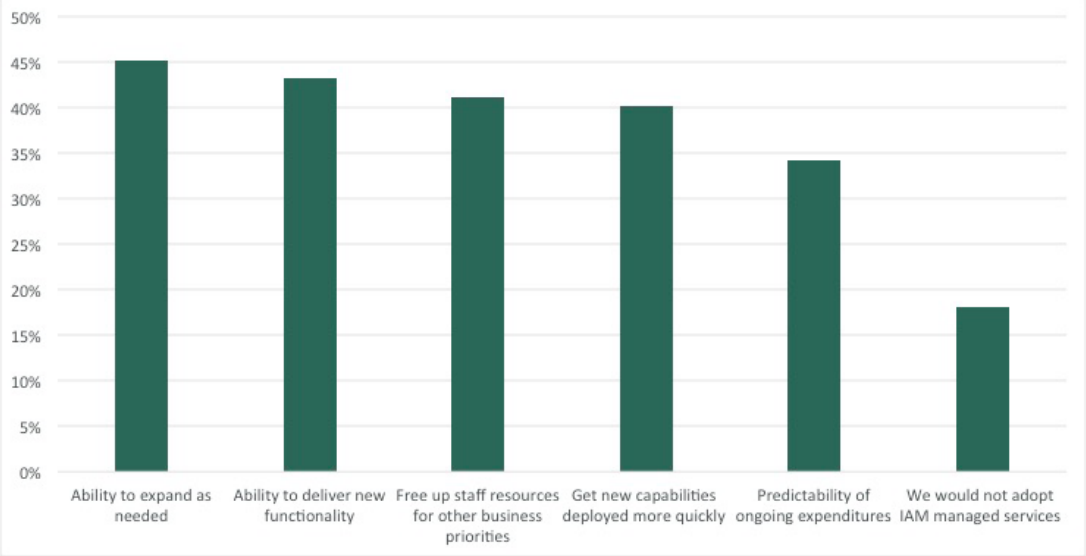
- Ability to expand as needed
- Ability to deliver new functionality
- Freeing up staff resources for other business priorities
- Getting new capabilities deployed more quickly

Therefore, respondents appear to have a good understanding of some of the key ways service providers can help their businesses.

What factors are most important in deciding to adopt managed IAM services?

Figure M.

Respondents identified a number of factors that would motivate them to work with an IAM service provider.



Key Approaches to Capitalizing on IAM Managed Services Opportunities

Service providers that have the expertise needed to work with customers and define the strategies and tactics that can help them advance their IAM maturity, will deliver significant value and be well positioned in a growing market. Following are some key considerations that service provider executives should factor in as they look to capitalize on the IAM opportunity:

- **Define optimal sales targets**. As outlined above, many organizations are at the earlier stages of the IAM maturity evolution. However, a prospect with manual, ad hoc processes isn't necessarily a good fit for every service provider. For example, if a service provider is focused on implementing and optimizing IAM tools, it's important to recognize that a company with no formally defined processes will need significant consulting services to establish those processes, before it is time to implement any tools. It is important to ensure early on that the prospects being targeted are a good fit for the service provider's offerings and skill sets.
- **Start with business drivers**. As outlined earlier, respondents understand that there are some strategic reasons for leveraging managed IAM services. It is critical to start with an understanding of the prospect's business drivers for adopting services, and align value propositions, pricing, packaging and other efforts with those drivers.
- **Align with maturity levels**. Once objectives are clearly understood, it will be important to gain a clear understanding of where the business is in its IAM evolution—and ensure services and solutions are aligned with where the customer is, and how to get them to the next phase.
- **Maximize standardization and automation**. Both for the service provider's internal operations and for any client services being delivered, it is critical to maximize automation wherever possible. Without automation, standardization and operational efficiency, service providers will be hard-pressed to gain the agility required to compete in the application economy—and will be fundamentally challenged in helping customers do so.

Conclusion

The survey results detailed throughout this paper offer a strong case for service providers to build or expand their IAM practices. The results make clear that many enterprises have an urgent need to optimize their IAM efforts and implementations—and that many IT teams will need to partner with expert service providers to make this happen. For service provider executives, here are a few of the most significant takeaways from the survey:

- Organizations have grown increasingly reliant on cloud services, with little awareness or involvement of IT organizations. Shadow IT can expose businesses to significant risk. Advanced IAM represents a key strategy for addressing this risk.
- Many enterprises are in the early stages of IAM maturation.
- Enterprise customers are dissatisfied with current IAM approaches, and open to working with service providers to address their challenges.
- Many have worked or are currently working with service providers, but a lot of opportunities remain to establish longer-term, higher-value service engagements that help customers enhance IAM maturity.

About the Survey

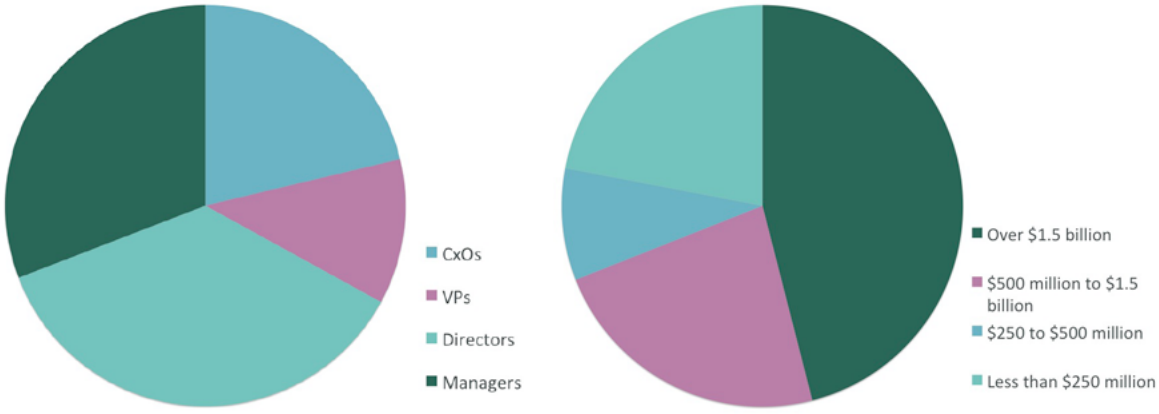
This report draws from a survey of security executives conducted by CA in 2016. 210 respondents participated, and individuals came from a range of levels within their respective organizations: 20 percent were C-level executives, 11 percent were vice presidents and 34 percent were at the director level. Almost half of respondents worked for Fortune 1000 companies with revenues over $1.5 billion, while 31 percent came from small and mid-market companies.

Respondents also represented companies from a wide range of industries, including financial services, manufacturing, high tech, telecommunications and more. In addition, while almost three-quarters of respondents were based in the U.S., a total of 24 countries were represented.

Respondent breakdown by title, company revenue

Figure N.

Survey respondents were comprised of security executives from a range of levels in the organization and from the spectrum of business sizes.



About CA IAM Solutions

CA offers service providers advanced IAM solutions with comprehensive capabilities. Service providers can effectively leverage these solutions to deliver profitable, high-value IAM services to their customers.

CA solutions offer advanced capabilities in the following areas:

- **Identity management**. CA solutions offer complete capabilities for managing identities across their lifecycle. These solutions also offer governance, self-service onboarding, access request workflows and risk analytics.
- **SSO**. With CA solutions, organizations can establish SSO capabilities for all their employees' applications—whether they're web or non-web based. These solutions offer session security, which helps strengthen safeguards around sensitive systems and services.
- **Advanced authentication**. CA solutions offer support for a broad range of strong, multifactor authentication mechanisms, so service providers can address a broad range of customer environments. CA solutions support one-time passwords, software tokens and hardware tokens. CA also offers solutions that can dynamically factor in contextual risk, for example, adapting authentication requirements based on where users are, what devices they're using, their online behavior and more.

- **Privileged access management**. CA delivers capabilities for establishing advanced controls around the access of privileged users. Solutions feature capabilities like password vaulting, central authentication for Linux® and Microsoft® Windows® servers, session recording for auditing purposes and kernel level controls. These capabilities can be instituted in both customer and service provider environments to establish robust, multilayer security.

For more information, visit the **CA identity management page**.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-209458_0616