Hybrid Environments Demand Coordinated IAM For Both Security And Agility
# Table Of Contents

Executive Summary ................................................................................................................. 1
IT Is Seeing A Patchwork Of Cloud And On-Premises Deployments ............ 2
Business Owners Are Driving Moves To The Cloud, Forcing Access Governance Issues ............................................................................................... 3
Coordinate Your IAM Approach To Provide Governance To The Hybrid Environments Business Owners Love........................................................................ 5
Key Recommendations ............................................................................................................ 8
Appendix A: Methodology ...................................................................................................... 9
Appendix B: Supplemental Material ....................................................................................... 9
Appendix C: Demographics/Data .......................................................................................... 10
Appendix D: Endnotes ............................................................................................................ 11

---

**ABOUT FORRESTER CONSULTING**

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester’s Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

---

© 2014, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com. [1-NW3L93]
Executive Summary

Businesses are rushing headlong into the cloud in almost every facet of their operations — but identity and access management (IAM) is struggling to keep up. The stakes for managing identities and access entitlements in a coordinated fashion couldn’t be higher as, one by one, every category of enterprise software feels the pull of the cloud and as technology management pros find themselves and their IAM solutions trying to straddle the increasingly blurry cloud/on-premises divide.

In January 2014, Microsoft commissioned Forrester Consulting to evaluate the IAM challenges firms are facing with hybrid cloud architecture, how these are being addressed currently, and the projected evolution of these management techniques in response to continued and accelerated cloud adoption. Then, to further explore this trend, Forrester tested the assertion that centrally managed IAM is a key element to enabling technology management professionals to add governance to an environment where business owners are enthusiastically adopting cloud-based solutions.

The pace of businesses adopting hybrid cloud strategies is increasing, and a centrally coordinated identity and access management approach facilitates key associated business and security objectives.

In conducting an in-depth survey with 210 tech management professionals with security responsibilities, as well as subsequent follow-up interviews with five opt-in survey respondents, Forrester found that these companies face strongly “hybridized” environments, are sensitive to the concomitant security and business challenges, and are prioritizing IAM strategies that put them on a more streamlined, simplified footing in response.

KEY FINDINGS

Forrester’s study yielded four key findings:

› Enterprise software is unevenly distributed across cloud and on-premises environments. Today, IAM-related software is disproportionately on-premises, but 12 other categories of software show extensive moves to private and public cloud environments. In three years, the pros predict much greater cloudward moves, as well as increased collaboration between various stakeholders across several business functions. As such, the current patchwork of deployments will evolve, but not disappear.

› Moving to the cloud spurs both security fears and project complexity. We see significantly increased levels of concern about access governance in cloud environments — and we anticipate project execution challenges for cloud IAM projects, given that our survey respondents tell us that a wider variety of “moderately involved” stakeholders sit at the table.

› Simplification goals are driving next steps in IAM coordination. The technology management pros we spoke to stressed the importance of streamlining and simplification of IAM to support crucial next steps in security and business growth — and also stressed their dissatisfaction with the status quo.

› Centrally managed IAM is seen as providing key business benefits. Particularly in light of needs for extended-enterprise flexibility around application hosting, client network/device access, and population diversity, respondents expressed widespread agreement that centrally managed IAM supports key associated business goals, including, among others, enforcement of corporate enterprise security standards, risk-based authentication heuristics, and licensing cost savings.
IT Is Seeing A Patchwork Of Cloud And On-Premises Deployments

“A lot of our SaaS cloud services are connected . . . every authentication service we have is talking to the cloud.”

— Director of information services at a medium-sized US university

The shift to cloud computing is no longer a novel concept, as an ever-increasing number of firms adopt this delivery and consumption model. The pace and prioritization of what gets moved to the cloud, however, is not a linear process, as firms must decide which data is most appropriate for such a setting and how to provision access while maintaining a volatile balance between business value on the one hand, and security and risk requirements on the other. The result is a patchwork across the enterprise of on-premises, private cloud, and public cloud deployments for applications.

THE EXTENDED ENTERPRISE FACES AN INFINITE VARIETY OF IDENTITY AND ACCESS CHALLENGES

Forrester defines the extended enterprise as one for which a business function is rarely, if ever, a self-contained workflow within the infrastructure confines of the company. It presents unique IAM challenges in three dimensions simultaneously (see Figure 1). Security and risk professionals face serious challenges in managing access to sensitive resources now that application sourcing and hosting can range far from the confines of a firm’s data center. The need for some users to access these resources from unmanaged networks and devices, and the need for non-employee users to gain access to some resources, complicates matters further.

THE PATTERN OF FIRMS’ MOVES AWAY FROM ON-PREMISES DEPLOYMENT IS UNEVEN

In looking at where enterprise applications are deployed, we see a dramatically uneven pattern of the on-premises option (see Figure 2). This reality is resulting in new challenges:

Modern firms have become heavily “hybridized.” Across 16 enterprise software categories, only about one-half to two-thirds of applications in today’s enterprise are deployed on the premises today among our survey respondents. Given that cloud services must connect with those remaining on the premises, hybrid cloud architecture has emerged as a dominant model, presenting new technology management challenges. An IT director at a major software provider told us, “Data security is our biggest and most urgent initiative . . . The approach we take to move [personally identifying information] into the cloud makes us take lots of security measures.”

IAM disproportionately remains on-premises. More than any other type of enterprise software, IAM-related functions — user authentication, user repositories, access management systems, and identity management — had the highest percentage of on-premises deployment footprints. A corporation’s org chart resides in its directories and provisioning engines, and customer identity management is often sensitive and regulated, so reluctance to move from such functions into the cloud over security fears is understandable. However, it introduces tension in the form of too-tight coupling to different on-premises identity repositories. As a director of information services at a medium-sized university put it, “Our [cloud platform] is only talking to local accounts. We allow SaaS [apps] to do an LDAP [binding] behind them. We’re trying to get away from that; we’re uncomfortable about it.”

Business Owners Are Driving Moves To The Cloud, Forcing Access Governance Issues

“We are moving] everything piece by piece into the cloud.”

— IT director at a major software provider

FIGURE 2
IAM Has The Highest “On-Premises Quotient” Of Any It Element Today

“What on-premises deployments do you currently have?”

<table>
<thead>
<tr>
<th>Software that supports an industry-specific process</th>
<th>63%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance and accounting software</td>
<td>62%</td>
</tr>
<tr>
<td>Order management software</td>
<td>61%</td>
</tr>
<tr>
<td>Productivity apps</td>
<td>61%</td>
</tr>
<tr>
<td>Business intelligence software</td>
<td>59%</td>
</tr>
<tr>
<td>Enterprise resource planning (ERP) software</td>
<td>58%</td>
</tr>
<tr>
<td>Human capital management software</td>
<td>57%</td>
</tr>
<tr>
<td>Customer relationship management (CRM) software</td>
<td>55%</td>
</tr>
<tr>
<td>ePurchasing software</td>
<td>54%</td>
</tr>
<tr>
<td>Content management software</td>
<td>52%</td>
</tr>
<tr>
<td>Business process management (BPM) software</td>
<td>50%</td>
</tr>
<tr>
<td>Collaboration software</td>
<td>48%</td>
</tr>
</tbody>
</table>

Base: 210 IT professionals with security responsibilities
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2014
In the “shadow IT” phenomenon, individual employees and lines of business adopted unsanctioned — often cloud-based — applications. It has evolved into a new dynamic in which the business increasingly expects new capabilities, applications, and partnerships to be provisioned quickly and easily. The resulting proliferation of applications and consumption models has resulted in increasingly complex access governance challenges. IAM pros face a “new normal”: managing access in a way that serves the business’s needs for cloud-accelerated agility. As a result, tech management professionals are telling us loud and clear that they are dealing with real consequences for increasingly hybridized environments combined with their identity and access requirements.

Businesses are heading to the cloud in more ways than one. Both public cloud and private cloud adoption are accelerating. As economic, operational, and experiential benefits of cloud-based application and platform services come into focus after their pilot years, the pace of adoption is picking up steam for all categories of enterprise software. Forrester’s Business Technographics survey indicates that almost 70% of enterprise organizations utilize one or more public cloud services today, so there aren’t many firms immune to the trend. When asked to predict trends in deployment footprints for 16 categories of enterprise software, our survey respondents projected significant increases for both public and private cloud deployment, along with across-the-board double-digit declines for their on-premises counterparts (see Figure 3).

Cross-organizational collaboration is looking more “cloudy” as well. Collaboration with myriad external business stakeholders, such as institutional customers, partners, and SaaS suppliers, often involves integration with external apps. We asked respondents to project types of collaboration that would grow in three years. The

FIGURE 3
IT Professionals Are Predicting Every IT Element Will Shift Cloudward

“Compared to your current deployment footprints for the following IT elements, how do you anticipate these will change in three years?”

<table>
<thead>
<tr>
<th>IT Element</th>
<th>Public Cloud</th>
<th>Private Cloud</th>
<th>On-Premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance and accounting software</td>
<td>-20%</td>
<td>-6%</td>
<td>15%</td>
</tr>
<tr>
<td>Enterprise resource planning (ERP) software</td>
<td>-19%</td>
<td>-7%</td>
<td>15%</td>
</tr>
<tr>
<td>Order management software</td>
<td>-19%</td>
<td>7%</td>
<td>11%</td>
</tr>
<tr>
<td>Software that supports an industry-specific process</td>
<td>-21%</td>
<td>-7%</td>
<td>15%</td>
</tr>
<tr>
<td>Human capital management software</td>
<td>-18%</td>
<td>7%</td>
<td>16%</td>
</tr>
<tr>
<td>Business intelligence software</td>
<td>-19%</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>Content management software</td>
<td>-19%</td>
<td>2%</td>
<td>16%</td>
</tr>
<tr>
<td>ePurchasing software</td>
<td>-15%</td>
<td>4%</td>
<td>16%</td>
</tr>
<tr>
<td>Customer relationship management (CRM) software</td>
<td>-16%</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>Business process management (BPM) software</td>
<td>-16%</td>
<td>4%</td>
<td>17%</td>
</tr>
<tr>
<td>Collaboration software</td>
<td>-16%</td>
<td>4%</td>
<td>10%</td>
</tr>
<tr>
<td>Productivity apps</td>
<td>-21%</td>
<td>4%</td>
<td>15%</td>
</tr>
<tr>
<td>User authentication</td>
<td>-13%</td>
<td>4%</td>
<td>14%</td>
</tr>
<tr>
<td>Access management systems</td>
<td>-21%</td>
<td>4%</td>
<td>16%</td>
</tr>
<tr>
<td>Identity management systems</td>
<td>-24%</td>
<td>6%</td>
<td>20%</td>
</tr>
<tr>
<td>User repositories</td>
<td>-21%</td>
<td>11%</td>
<td>18%</td>
</tr>
</tbody>
</table>

Base: 210 IT professionals with security responsibilities
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2014
top two directly involve cloud interactions or share characteristics with cloud integration: 1) employee usage of software-as-a-service (SaaS) apps; and 2) institutional customer integration with digital products offered by the firm, for example, exposing web services or APIs (see Figure 4).

- **Cloud fuels access governance concerns.** When asked about their level of concern over access governance in cloud environments compared to on-premises ones, 11% more respondents to our survey rated themselves as “concerned” or “very concerned.” Given the sensitive nature of data needed for many business functions, it’s understandable that stakeholders may tread with caution. “The data we host for clients are things like names, addresses, PIN blocks, track data — anything you would want to take over a bank ID or go on a shopping spree,” the acting information security officer at a major US-based IT services firm told us. “It’s a big paranoia because the people in corporate don’t want to see our name in the paper on the bad side of things.”

- **Cloud IAM projects introduce diffuse stakeholders.** Our survey shows that IAM projects have a starkly different stakeholder profile when we compare IAM projects that are deployed exclusively on-premises versus those with a cloud component (see Figure 5). IT security and IT operations roles do see a modest sharpening of their “primary decision-maker” role versus that of line-of-business owners and developers. But all four stakeholders — along with the catchall “other” stakeholder category — see a decrease in being “very involved” in favor of gains in merely being “moderately involved.” For instance, “other” stakeholders saw their role as moderate influencers skyrocket from 0% for on-premises IAM projects to 67% for cloud IAM projects. Diffuse responsibility patterns such as these can be a recipe for disaster if authority over identity data and workflows is unclear.2

### Coordinate Your IAM Approach To Provide Governance To The Hybrid Environments Business Owners Love

> **“Simplicity is my main objective.”**
> — Director of IT security at a major retailer

Clearly cloud computing is here to stay, and hybrid environments — in various guises — represent a dominant model technology managers will deal with within this era. The corresponding pressures on IAM, however, have received less attention, despite agreement among our interviewees about the challenges it poses when they attempt to synergize new and legacy technologies.

> “Every IAM implementation I’ve ever worked with has [disappointed]. When you’re trying to pair modern people, who understand iPads and how easy they are, and tell them that the mainframe with all the data they’re working with doesn’t support user names, it blows their minds . . . I see IAM as individualized platforms for which I still have to develop the routines and scripts so that fancy software can talk to the sixty year-old mainframe.”
> — Acting information security officer at a major US-based IT services firm

Along with the increasingly mobile, multidevice nature of business, hybrid environments are forcing the issue and even creating new vulnerabilities. It’s past time for forward-thinking tech management pros to abandon piecemeal approaches to access governance over disparate data
sources and software platforms. Rather, they should increasingly consider adopting a Zero Trust security posture. Zero Trust entails treating all access requests as potentially coming from “outsiders” — which may be the case more often than not when enterprise resources, users, access networks, and client devices can all reside outside your corporate infrastructure — and then performing selective trust elevation to achieve least-privilege access, using single sources of identity, authentication, and authorization truth. We see the signs in our survey:

› **Tech management pros recognize the key business benefits of centrally managed IAM.** We saw broad consensus on the validity of five business benefits, with a substantial 72% to 79% of respondents in agreement. This was true for the benefits that focus directly on security: 1) enforcing corporate standards for enterprise security architecture; 2) applying risk-based heuristics over a larger activity base; and 3) unifying access policy management. It was even true for the benefits that add efficiency and cost management to the mix: 1) getting a “single pane of glass” view of user access to resources and 2) saving on licensing costs for multiple IAM solutions (see Figure 6).

› **Strategic IAM priorities reflect the new reality.** Our respondents are prioritizing solutions that tackle all three dimensions of the extended-enterprise IAM challenge. For 39%, extending or synchronizing on-premises to cloud IAM solutions is already a priority, and 32% are making it a priority in the next year; this addresses the app sourcing and hosting dimension. And 38% of them already prioritize conditional access based on devices, while 37% will do so in the next year; this addresses the access channels dimension. Finally, a full 46% currently prioritize two-factor or other strong authentication of employees and partners, while 31% will do so in the next year, addressing the population dimension (see Figure 7).
Federated identity sourcing supports cross-organization interoperability. As one interviewee described, “We’re setting up a shared knowledge base between our campus and another. To authenticate as a member of one institution or the other, we don’t want to point to two LDAP servers. We just want it to work with [our federated identity solution] as a server provider.” This is but one example of how the new hybridized era points to the need for an increasingly holistic view of user identity across and beyond the enterprise and a shift to federated IAM interoperability.

Coordinated, simplified IAM drives the ability to win, serve, and retain customers. Whether the customers are external to the enterprise or represent internal lines of business, they benefit from tech management’s ability to provision and oversee the appropriate access to resources — wherever those resources live — without imposing unnecessary processes, costs, or delays. We heard it repeatedly: a director of information services at a medium-sized university told us, “Unification and simplification of our architecture is the most important objective for us.” The acting information security officer at a major IT services firm said, “We see an emphasis on putting risk and resiliency at the forefront. To make things easier for our customers and thus getting and holding market share and making sure we don’t lose customers, we’ve pushed hard at consolidating and streamlining.”

The director of information services at a medium-sized university painted this picture of the possibilities it faces with coordinated IAM: “The real wins will be when we can do things that we can’t do with our existing stuff, like connecting to other campuses.”

![FIGURE 6](image-url) Wide Consensus Exists Around The Value Of Centrally Managed IAM

<table>
<thead>
<tr>
<th>“Please indicate how strongly you agree that the following are key business benefits of centrally managed IAM.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly</td>
</tr>
<tr>
<td>Ability to enforce corporate standards for enterprise security architecture</td>
</tr>
<tr>
<td>Ability to apply risk-based authentication heuristics over a larger base of activity</td>
</tr>
<tr>
<td>Save on licensing costs for multiple IAM solutions</td>
</tr>
<tr>
<td>“Single pane of glass” view of user access to resources</td>
</tr>
<tr>
<td>Unified access policy management</td>
</tr>
</tbody>
</table>

Base: 210 IT professionals with security responsibilities
Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2014
Key Recommendations

Forrester’s in-depth surveys and interviews with technology management professionals yielded three important recommendations:

› **Adopt a Zero Trust posture to enable your IAM systems to withstand extreme heterogeneity.** Adopting Zero Trust for identity and access requires a strategic shift: Think of your organization as a “cloud provider” of authentication, provisioning, and even authorization services to internal and external applications as required, and require applications to use these services where possible.

› **Put a premium on federated IAM interoperability.** Whether cloud-based or remaining firmly on the premises, user repository data must traverse Internet boundaries more frequently, whether to be synchronized with external parties such as SaaS vendors or — ideally — at runtime when users use single sign-on (SSO) to access SaaS apps. Interoperability standards help you achieve more universal success.

› **Ensure that your enterprise presents a clean identity “source of truth.”** It’s all too easy to work on the edges of the coordinated IAM problem without addressing long-standing issues such as inconsistent user data in multiple poorly managed repositories. Access governance starts with governance over the universe of credentials for which your organization should be the ultimate authority. Getting your story straight here enables more sophisticated coordination, such as centralized access policy and SSO-powered B2B collaboration.
Appendix A: Methodology

In this study, Forrester interviewed five and conducted an online survey 210 IT security professionals to evaluate their firms’ plans as they pertain to identity and access management (IAM) in the context of hybrid cloud adoption. Survey participants included decision-makers in enterprises from a variety of industries with over 1,000 employees in the United States and over 500 employees in France, Germany, and the United Kingdom. Participants were asked questions regarding their on-premises and cloud deployment plans, governance and identity and access management challenges, strategic priorities, and organizational involvement. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in January 2014 and was completed in March 2014.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH


FIGURE 8
Location, Company Size, And Seniority Of Survey Respondents

“In which country is your organization headquartered?”

- United States: 50%
- France: 16%
- Germany: 15%
- United Kingdom: 19%

“How many employees work for your organization worldwide?”

- 250 to 500 employees (Medium): 3%
- 2,000 or more employees (Global): 19%
- 5,000 to 19,999 employees (Very large): 22%
- 1,000 to 4,999 employees (Large): 37%

“Which title best describes your position at your organization?”

- Manager (manage a team of functional practitioners): 16%
- C-level executive (e.g., CEO, CMO): 26%
- Director (manage a team of managers and high-level contributors): 38%
- Vice president (in charge of one/several large departments): 20%

Base: 210 IT professionals with security responsibilities

Source: A commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2014
Appendix D: Endnotes

1 Source: Forrsights Software Survey, 2013, Forrester Research, Inc.

2 Whenever an organization can’t firmly answer “Who owns this data?” new IAM projects become paralyzed. In some cases, IT security and HR have overlapping responsibility for employee identity, marketing owns consumer identity, and risk governance owns authentication strategy. To succeed, first clarify lines of authority and then fix overlaps. Source: “Identify And Influence Identity Stakeholders,” Forrester Research, Inc., July 16, 2012.