FORRESTER®

Cloud Migration Optimizes Identity And Access Management

Overcoming Infrastructural And Operational Barriers To Migration Allows IAM Organizations To Boost AI-Driven Security, Engagement, And Efficiency

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY PING IDENTITY AND FORGEROCK
NOVEMBER 2023

Cloud Sets The Stage For A More Secure IAM Solution

Identity and access management (IAM) is a critical component of the security ecosystem. To support their network of customers and employees and boost reliability and scalability, organizations are migrating their IAM solutions to the cloud. Our study found that 86% of IAM decision-makers agree that IAM technologies — including customer identity and access management (CIAM) and workforce/employee IAM — must be fully migrated to the cloud to achieve their business goals.

Infrastructural and operational complexities like a lack of integration between apps and cloud solutions, outdated technology, and organizational silos can impede the path to migration. By simplifying and centralizing these aspects of their IAM strategy, organizations can successfully migrate and, as a result, holistically improve business outcomes such as security, customer engagement, efficiency, and operational agility.

Key Findings

Global technology decision-makers view AI/ML investment and cloud migration as top near-term strategic priorities.

Eighty-two percent of respondents say that the complex nature of their current IAM environment is a barrier to innovation and agility.

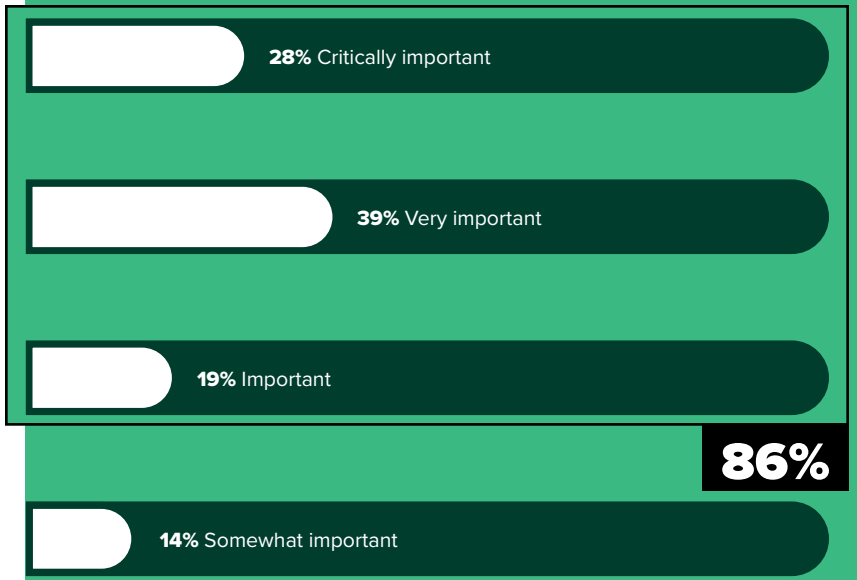
Seventy-seven percent agree/strongly agree that IAM cloud migration would allow their organization to improve its Zero Trust security posture.

Full Migration Is Critical To Success

IAM decision-makers agree that fully migrating their identity security technologies to the cloud is an important component of their success. This is even more important for organizations using both CIAM and workforce/employee IAM — 92% of whom believe migration is critical. This spotlights the greater and more positive impact of cloud migration for organizations using more than one IAM technology.

Despite this sentiment, IAM decision-makers are slow to make progress in their migration efforts. According to Forrester, only 12% of security decision-makers have fully migrated their IAM solutions to the cloud.[1] Modern IAM solutions are mostly hybrid with surveyed decision-makers' organizations hosting 37% of their security technologies in traditional on-premises environments. However, they predict this number to drop by 7% over the next two years (30%) in favor of migrating more of their security infrastructure to private cloud (40%) and public cloud (30%).

"How important to your department's success is fully migrating identity access management (IAM) technologies to the cloud?"



Orgs using both CIAM and workforce IAM place more importance on cloud migration (92%).

Base: 254 technology decision-makers from NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Near-Term Goals: Use Cloud As A Foundation To Enhance Security With AI And Zero Trust

For IAM decision-makers, improving security is a top digital priority. Within the next 12 months, they plan to invest in AI/ML and Zero Trust to enhance security. Migrating to the cloud plays a fundamental part in this.

Migration is underway from a practice-to-practice standpoint. Organizations using CIAM and/or workforce/employee IAM are in the process of migrating or planning to migrate their identity governance (69%), API security (68%), passwordless authentication (66%), and multifactor authentication (61%) to the cloud in the next 12 months.

"[To improve,] break down migration into manageable phases or stages."

— VICE PRESIDENT, HEALTHCARE, NORTH AMERICA

"Which of the following digital initiatives are likely to be your organization's most important strategic priorities during the next 12 months?"

(Showing totals from responses)

52% Increase investment in AI and ML to improve security

US orgs favor cloud migration (48%) over AI/ML investment (46%). EMEA (56%) and APAC (56%) are more focused on AI/ML.

46% Migrate more of our security solutions into the cloud

43% Improve security posture within cloud environments

39% Implement a Zero Trust security strategy

Base: 254 technology decision-makers from NA, EMEA, and APAC
Note: Showing top 4 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Workforce Support, Reliability, And Scalability Drive Migration

Organizations that use IAM as a core element of their security infrastructure have many reasons to migrate to the cloud. Respondents noted primary motivators like better support for an evolving workforce ecosystem, improved reliability, and better management of legacy technology.

Surveyed IAM decision-makers see cloud-based IAM as an environment that will allow them to scale for customer growth, a key motivator that connects to the user experience benefits of a successful cloud migration. Another driving factor for IAM cloud migration is improvements in security, which is also the top business outcome of cloud migration.

> "When selecting … IAM solutions, ensure that they are fully scalable and resilient enough to adapt to the growth and change of the organization."
>
> **— VICE PRESIDENT, FINANCIAL SERVICES, APAC**

Base: 254 technology decision-makers from NA, EMEA, and APAC
Note: Showing top 6 responses; total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Internal And External Silos Form Barriers To Migration

Despite a broad range of reasons to migrate IAM to the cloud, less than half of surveyed decision-makers have the support to do it. Organizational barriers like silos inhibit centralized communication and top-down support of business outcomes. Three in four surveyed IAM decision-makers define their department as functionally siloed — an issue even more significant in externally focused organizations with CIAM solutions (80%). CIAM users have siloed user groups as well (60%), complicating their external network. These internal and external silos form communication barriers and can impact migration support.

Silos aren't the only barrier to migration. Respondents note that security and IT teams contend with outdated technology that requires constant maintenance (62%), a lack of bandwidth for skilled workers (56%), poor password hygiene (49%), and the inability to enforce consistent user access (41%).

44%

receive the support they need from leadership to migrate to the cloud.

75%

say they are functionally siloed/very siloed within their own department (i.e., security, IT).

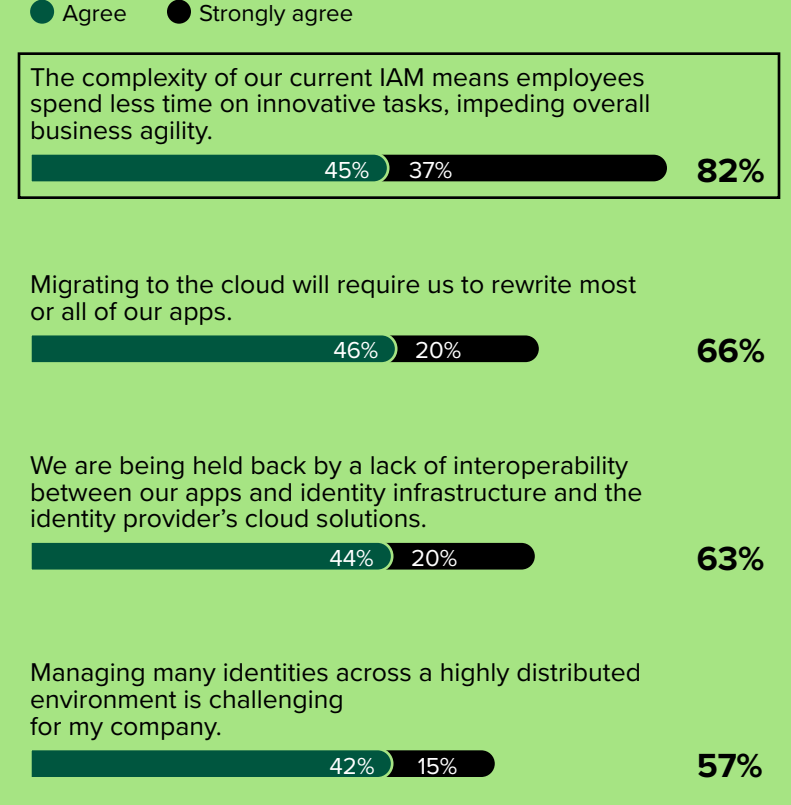
Base: 254 technology decision-makers from NA, EMEA, and APAC
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Complexity Is The Primary Gating Factor Of Evolution And Innovation

Successful IAM cloud migration requires organizations to assess the infrastructure, apps, and identities that make up the identity ecosystem. This process, including the potential rewriting of apps and management of identities in a highly distributed environment, is a pivotal point in the journey to optimizing IAM, and a key challenge that is exacerbated by legacy IAM solution complexity.

Eight in 10 surveyed IAM decision-makers are plagued by the complexity of their current solution. Managing this complexity takes valuable time away from employees who would otherwise be focused on security and innovation. In addition, this complexity can lead to misalignment of internal infrastructure, apps, and third-party cloud solutions, making the journey to cloud even tougher. Before migration can be possible, organizations need to assess and realign their internal technology to alleviate friction.

"How much do you agree or disagree with the following statements?"



Base: 254 technology decision-makers from NA, EMEA, and APAC
Note: Showing top 4 responses; total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Cloud-Based IAM Is Optimized With AI, Integration, And Zero Trust Capabilities

Increasing investment in AI/ML is a top near-term strategy of IAM decision-makers, more than half of whom see cloud-based IAM as the platform to optimize their use of automation. Security and efficiency are critical benefits of cloud-based IAM, and organizations view AI/ML-driven threat protection and identity analytics as the ideal means to achieve them. Organizations also seek support for a Zero Trust architecture as a critical layer of protection within cloud-hosted environments.

Identity silos are an obstacle to migration, so naturally the integration of these silos across cloud and on-premises environments is a key capability of the ideal cloud-based IAM platform. Streamlining the cloud ecosystem of identity and access is essential to achieving business outcomes like operational efficiency and agility.

"Which of the following capabilities are most important to have in the ideal cloud-based IAM platform?"

(Showing totals from responses)

56%
AI/ML-driven automation (i.e., automated threat protection, AI-driven identity analytics, etc.)

50%
Integrated silos of identity and access across different cloud platforms and on-premises systems

44%
Support for a Zero Trust, least-privileged ID perimeter architecture

33%
Identity governance

Base: 254 technology decision-makers from NA, EMEA, and APAC
Note: Showing top 4 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Successful Migration Boosts Password Security, Engagement, And Efficiency

For IAM decision-makers, successful cloud migration unlocks a range of positive business outcomes for their organization — the most important of which are rooted in security. Improved password security is a critical benefit for IAM organizations and favored by those respondents using workforce/employee IAM (66%). Improvements to Zero Trust posture is another security benefit that 77% of decision-makers agree is enabled by cloud migration.

Enhanced internal/external UX is a broad benefit of cloud-hosted IAM, but customer-facing benefits are most critical. Scaled customer adoption is an important motivator for migration, and 72% of respondents say that improved customer experience is a key outcome.

At the operational level, cloud-based IAM introduces more agility and efficiency via bandwidth, allowing organizations to free up more resources for innovation, versus governance and maintenance.

"Which of the following are the most important benefits your organization would gain as a result of successfully migrating IAM technologies to the cloud?"

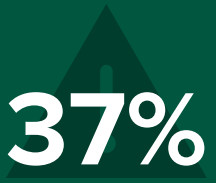
(Showing totals from responses)

61%

Improved password hygiene and security

50%

Improved internal/external user experience within our applications



37%

More agility to quickly comply with regulations

32%

People resources freed up

Base: 254 technology decision-makers from NA, EMEA, and APAC
Note: Showing four top-ranked choices
Source: A commissioned study conducted by Forrester Consulting on behalf of Ping Identity and ForgeRock, August 2023

Conclusion

Keep the following in mind as your organization explores cloud-based IAM:

Simplify IAM and app infrastructure. Migrating a complex IAM ecosystem to the cloud can be difficult. Evaluate your infrastructure and ensure that internal apps externalize IAM functions (e.g., authentication), then consolidate user stores and centralize efforts to rewrite apps much as possible.

Create shared goals across security and business teams. Centralizing communications and objectives ensures that migration is collaborative, not siloed. Adding business users' objectives to IAM's goals strengthens support for migration.

Automate legacy operations. Select a solution that uses AI-driven identity analytics and automatic remediation to identify user access and defend against IAM threats. This will increase bandwidth for IAM practitioners, allowing them more time to innovate.

Endnotes

[1] Source: "Identity and Access Management Market Insights, 2022", Forrester Research, Inc., January 12, 2023.

Resources

Related Forrester Research:

"Passwordless Authentication In Customer Identity And Access Management," Forrester Research, Inc., September 25, 2023.

"The Security Best Practices Of Cloud Migration," Forrester Research, Inc., September 20, 2021.

Related Webinar

December 15, 2022, "The State Of Customer Identity And Access Management," Webinar.

Project Team:

John Lloyd,
Market Impact Consultant

Lillie Sinprasong,
Associate Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

Methodology

This Opportunity Snapshot was commissioned by Ping Identity and ForgeRock. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of security decision-makers responsible for their organizations' identity and access management platform technology. The custom survey began and was completed in August 2023.

Demographics

REGION	
NA	**40%**
EMEA	**40%**
APAC	**20%**

EMPLOYEES	
20,000+	**4%**
15,000 to 19,999	**5%**
10,000 to 14,999	**25%**
5,000 to 9,999	**65%**

INDUSTRY (TOP 4)	
Healthcare	**13%**
Tech/tech services	**11%**
Finserv/insurance	**10%**
Retail	**10%**

DEPARTMENT	
IT	**51%**
Security (info/cyber)	**49%**

Note: Percentages may not total 100 due to rounding.

FORRESTER®