STRATA

TOP CHALLENGES AND SOLUTIONS FOR MULTI-CLOUD IAM ENTERPRISES

The acceleration of digital transformation triggered by recent volatile global events has left businesses grappling with increased security in the face of mounting technical debt and resource shortages.

To explore this, Forrester Consulting surveyed 221 North American IT leaders and decision-makers to learn what influences the transition to the cloud and what is getting in the way of successful digital transformations. This infographic is a snapshot of the resulting study: Distributed Multicloud Ecosystems Require a New Approach to Identity and Access Management.

Multi-Cloud Creates Complexity Beyond The Capabilities Of Current IAM Solutions.

Multi-Cloud Complexity Makes Achieving Zero Trust Challenging

Low-Code IAM: Increases Scalability, Unlocks Innovation, Improves Agility

Multi-cloud acceleration creates complexity

Cloud migration is accelerating, expanding multi-cloud ecosystems and increasing IAM complexity.

Many organizations are now using multiple clouds and IT and cloud security teams are challenged to manage distributed identities

67%

use three or more clouds today (and expect that number to double in two years)

71%

say managing many identities across a distributed environment is challenging/very challenging

The need to increase security & data protection as primary drivers

Cloud migration helps streamline operations by reducing technical debt, increasing systems' reliability, and modernizing IT departments by adding new capabilities. However, the top reason for cloud migration is to increase security and data protection.

2/3

migrate to the cloud to increase security and data protection

Remote workers create IAM challenges

Supporting remote and hybrid workforces creates inherently complex IAM challenges. Over half of IT decision-makers responded that they struggle to enforce consistent user policies and comply with changing regulations.

78%

Have difficulty managing identities in apps across multiple clouds

66%

Lack the time and money to properly enforce consistent user policies

62%

Lack the skilled workforce to support complex, cloud-based IAM

> **If budgets are tight and teams lack the proper skills to build appropriate security postures, the consequences could be devastating.**

The complexity of multi-cloud creates threat exposures

When combining the complexity and challenges of IAM in multi-cloud ecosystems, IT teams are under-resourced leaving systems at risk and potentially exposed to threats.

- 3/4 struggle to manage identities between clouds
- 64% say having to rewrite apps impedes cloud migrations
- 62% can't deploy modern passwordless/multi-factor authentication
- 2/3 can't integrate legacy on-premises systems and apps

A new low-code solution is needed to automate IAM

85%

agree that having a low-code/no-code solution for IAM would allow easier adoption of a Zero Trust posture

55%

say they need a solution that automates IAM for apps in multiple clouds with a reported lack of skills to support complex IAM

Firms are ready to invest in IAM with their multi-cloud deployments in order to:

- Improve **Efficiency**
- Achieve better **Integration**
- Increase **Security**
- Enable **Automation**

Creating a new IAM structure covering multi-cloud workloads is a significant challenge. Firms today must carefully plan application modernization and cloud migration. See how this can be achieved.

Download study

STRATA