STRATA

State of Multi-Cloud Identity Report 2021

Survey Data and Insights

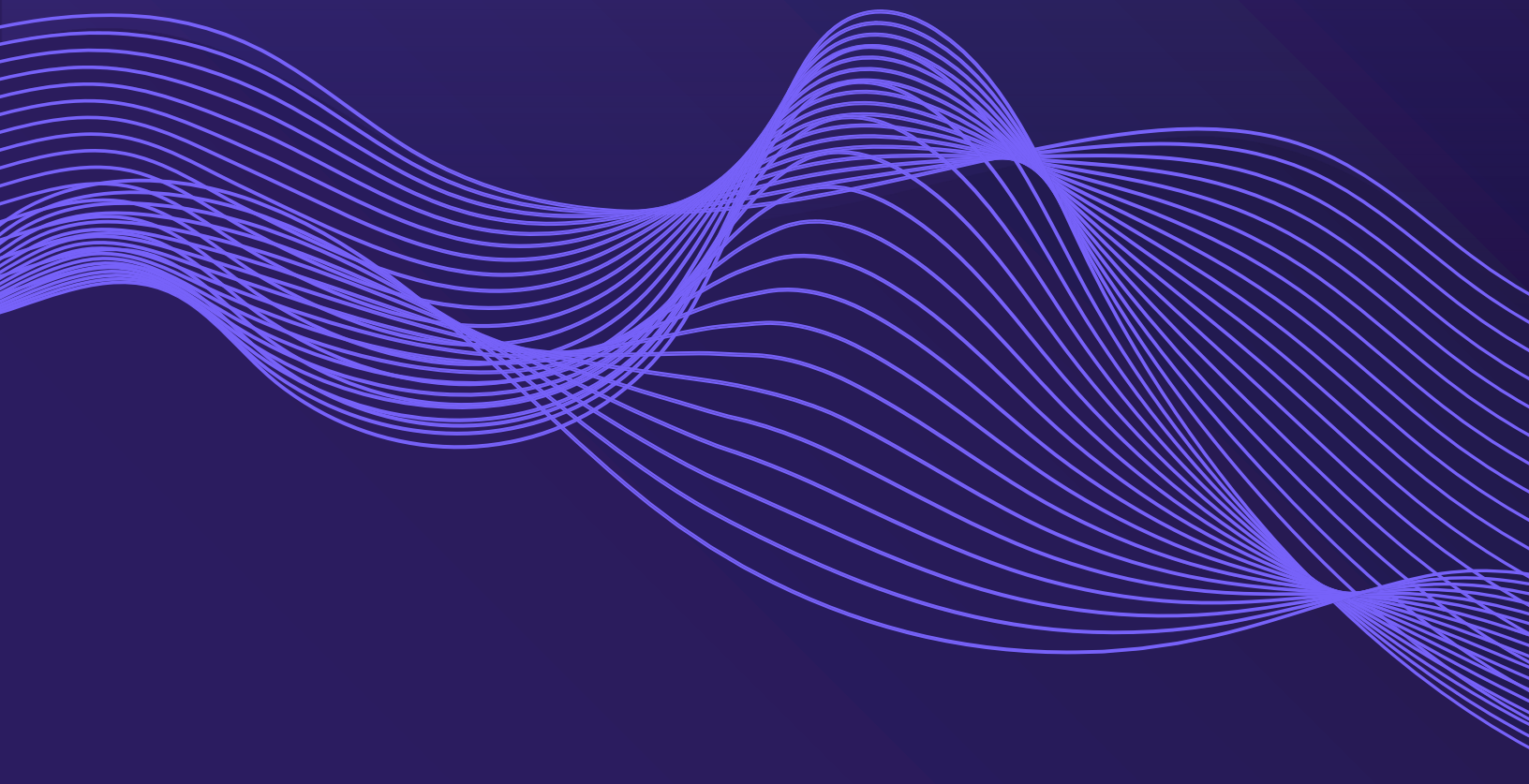
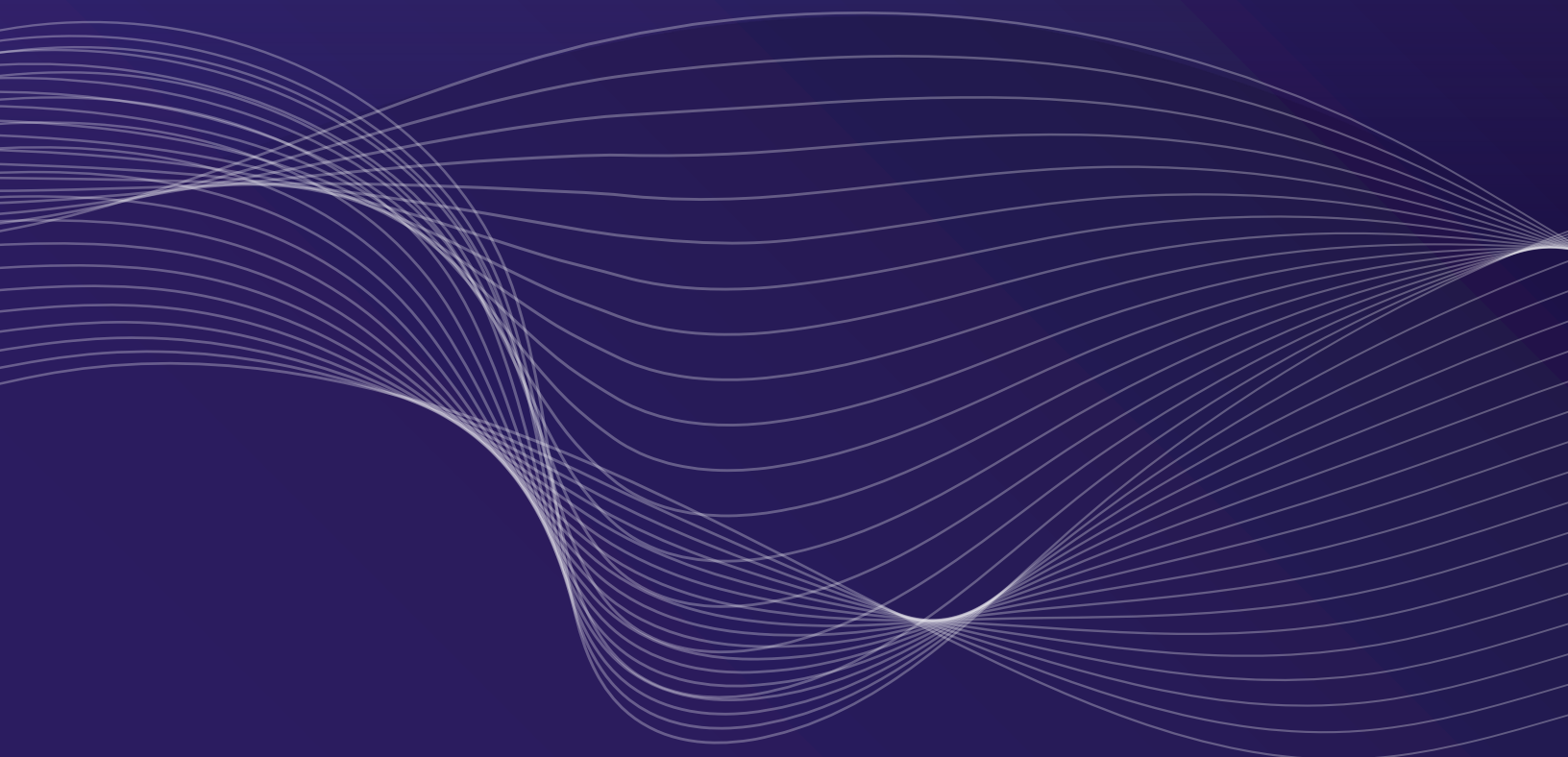


Table of Contents

01
Overview



Overview

Identity and access management (IAM) is at an inflection point. The events linked to the COVID-19 pandemic in 2020, forced cloud adoption to hit fast forward. Most enterprise organizations had already started their move to cloud computing, but project timelines had to accelerate from years to months, almost overnight. With the sudden shift to working from home, the spotlight focused on how to support workers and maintain security in this new distributed, almost entirely-remote environment.

The proliferation of applications has exploded with the increased remote work. Apps enable efficiency and help employees do their jobs better — especially when not in an office. Each app comes with its own identity system and many apps are connected to a particular cloud which also comes with its own set of identity systems. Now, it's not just "the" cloud, but multiple clouds.

At the same time, legacy, on-premises systems are still relied upon at most organizations. When operating in an environment with both private (on-premises) and public clouds, a Zero Trust security model cannot be applied. Many organizations want to migrate their apps to the cloud and modernize their systems, but it is a long, costly, and laborious process.

Navigating identity across multi-cloud or hybrid environments, while managing app and identity modernization and migration projects is deeply challenging work. Multi-cloud creates identity silos because these disparate systems don't communicate with each other.

Making legacy systems work securely with cloud apps and identities requires rewriting each app — which can take years and cost millions. Enterprises can't afford that timeline or resource focus.

Overview

We asked IAM experts and leaders across North America to share what their challenges and priorities were for identity management in 2021. Survey respondents included CIOs, CISOs, CSOs, CTOs, IAM Heads, Software Engineers, Cloud Solutions Architects, DevOps, IT Managers, Directors of Cybersecurity, and IT Compliance and Governance. All worked for Enterprise organizations with an annual revenue of at least $1 Billion (USD).

From the data, common patterns emerged around the evolving landscape of identity and access management. We found that **66% of enterprises $1B+ use 3 or more clouds (private and public).** The four main reasons organizations adopt a multi-cloud approach are to: **manage costs better, special capabilities, avoid vendor lock**, and **create redundancy**.

The priority initiative for organizations in the next 12 months is to implement a Zero Trust security model. Identity is enabling Zero Trust and secure hybrid access with orchestration. From the survey data, four key findings emerged:

- **Distributed architectures are becoming mainstream;**
- **Rapid multi-cloud adoption brings new identity and security challenges;**
- **Multi-cloud and hybrid driving need for app and identity migration and modernization;**
- **Identity Governance with multi-cloud is unattainable, especially for global enterprises.**

The conclusion is that **Identity Orchestration on top of an abstraction layer is the way to solve the challenges and mitigate risks** created by multi-cloud and hybrid identity silos.

This report explores how organizations are currently working towards implementing a Zero Trust security model in a multi-cloud world, the challenges they are facing, and the technologies and tools being used. The data provide a snapshot of the situation we are in right now, and a path forward through orchestration that will ease the pain, reduce costs, and increase security.

02
Key Findings

Key Findings

Rapid multi-cloud adoption brings new identity and security challenges

Zero Trust is a goal for almost every enterprise, but it's hard to reach in multi-cloud. Each cloud platform brings with it a built-in identity system; with more clouds, there are more aspects of identity to manage. It's even more difficult with a hybrid of cloud and on-premises systems. On-prem systems were built with the assumption that once a user authenticates, they are considered safe — the opposite of Zero Trust. **Running separate, non-compatible identity systems makes consistency of policy and authentication impossible**.

Distributed architectures are becoming mainstream

With the proliferation of cloud apps and the rapid adoption of remote working, **enterprise organizations are operating in a distributed environment**. Apps and identities are not centralized but live in any combination of on-premises systems, the cloud/multiple clouds, or hybrid. This reflects the reality of where the world is at: **distributed, multi-cloud**.

Multi-cloud/hybrid are driving identity and app migration and modernization

We found that **over 60% of respondents are struggling to manage identity silos** due to their distributed architectures. And, over half are still using manual efforts to manage them. Organizations using on-prem systems that are near their end-of-life (EOL) urgently need to migrate their on-prem apps to the cloud, but they must modernize them first which requires rewriting each app and can take many years, and millions of dollars.

Identity governance for multi-cloud is unattainable for global enterprises

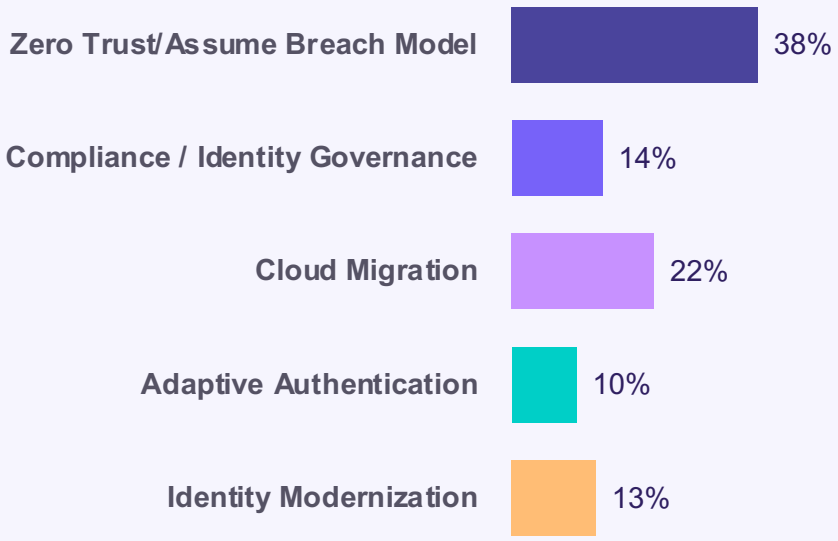
Organizations need to apply governance to their identities. Identity is the crown jewel for cybercriminals and therefore requires a hardened security posture. There is **no way to apply governance across clouds with siloed identities** and adhere to the privacy regulations in various countries.

Enterprise Priorities

Implementing a **Zero Trust/Assume Breach security model** is the top priority for organizations in the next 12 months. Other important initiatives include implementing a **compliance or identity governance policy, cloud migration, identity modernization, and adaptive authentication**.

Zero Trust is not achieved by any one piece of technology and is not a one-and-done type of project. Rather, it's a mindset that requires an overall change in how the organization approaches security.

All the priorities below are in support of Zero Trust.



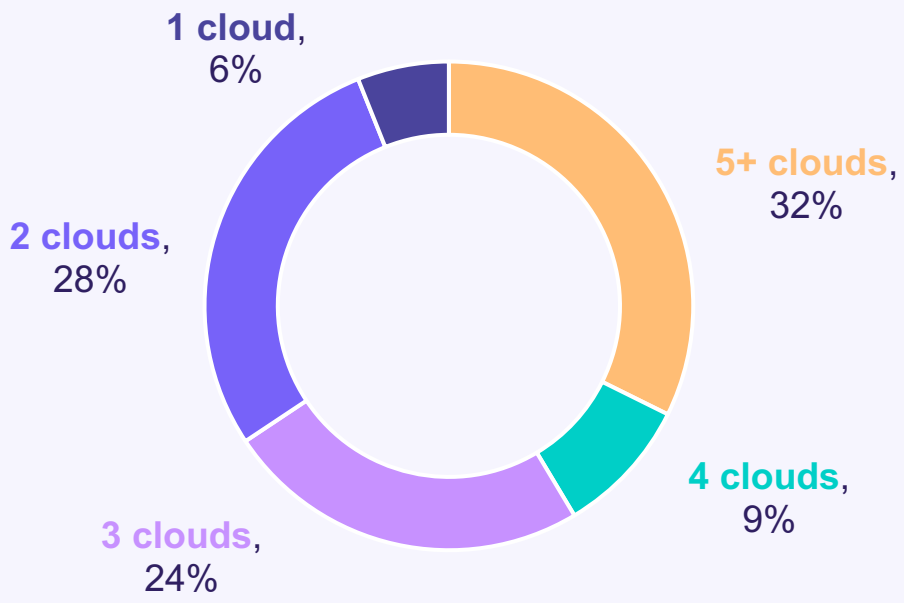
02.1

Rapid multi-cloud adoption brings new identity and security challenges

Enterprises are Using Multi-Cloud

Enterprises are not only quickly moving to the cloud, but they're also increasingly using multiple clouds. We found that **66% of respondents** at enterprise organizations with an annual revenue of over $1B **use three or more clouds (public and private)**. And an astounding **32% use five or more clouds for their business**.

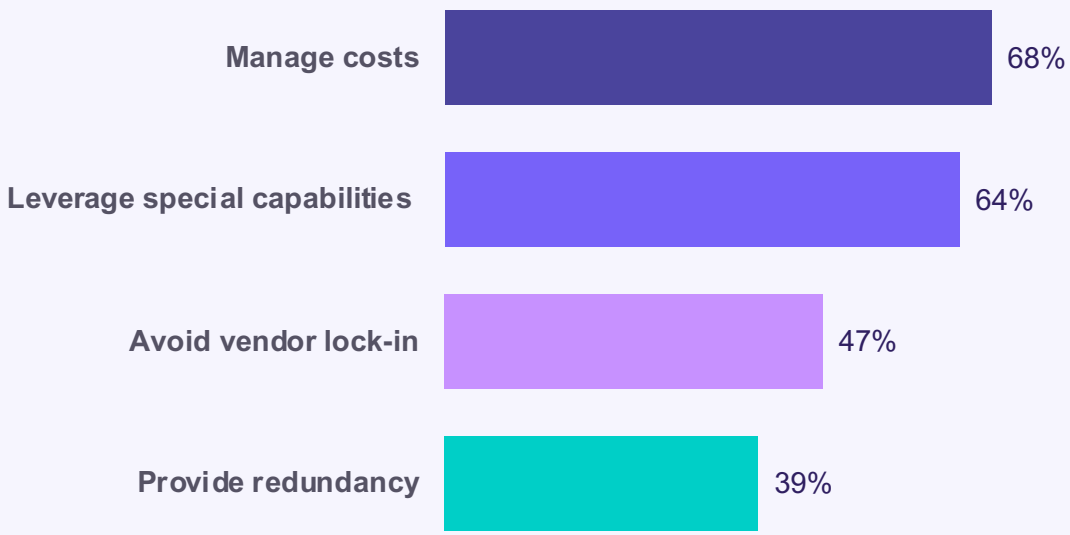
Q: How many clouds and on-premises systems do you use (public and private)**?**



Reasons for a Multi-Cloud Approach

Organizations are adopting multiple clouds for a variety of reasons including managing costs, leveraging the special capabilities of the cloud, avoiding getting locked in with a legacy vendor, and to provide redundancy in case of a breach or failover.

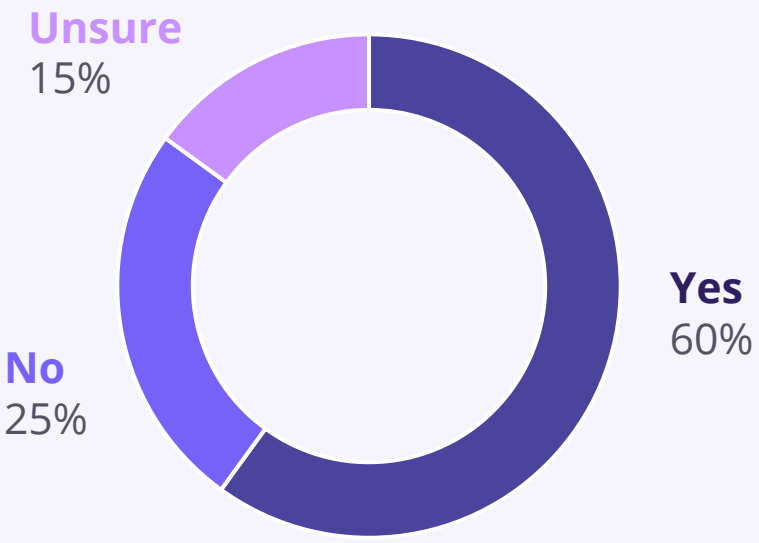
Q: What reasons exist for your organization to adopt a multi-cloud approach? (Select all that apply)



Using Multiple Clouds Causes Challenges

While there are clear benefits to being multi-cloud, it can also cause challenges. Of those respondents using multiple clouds, **60% said the use of multiple clouds has created visibility gaps of policies, apps, and users**. Identity silos emerge when identities are spread across multiple systems that cannot interoperate, thus creating gaps in visibility.

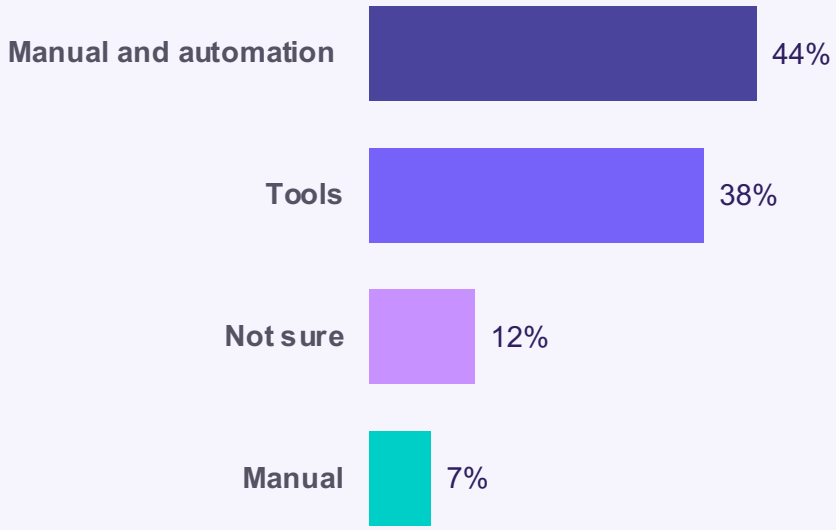
Q: Has the use of multiple clouds created visibility gaps of policies, apps, and users?



Multiple Clouds Being Managed Manually

With multi-cloud, organizations lack a consistent way to manage identity and access across clouds. Managing manually inevitably results in human error. Yet over **50% of organizations are still using some manual effort** to manage identity silos. Many are using a mix of both tools and manual which shows an understanding of the importance of automation, but the tools being used are insufficient.

Q: What approach can you take to manage the identity silos at your organization today?



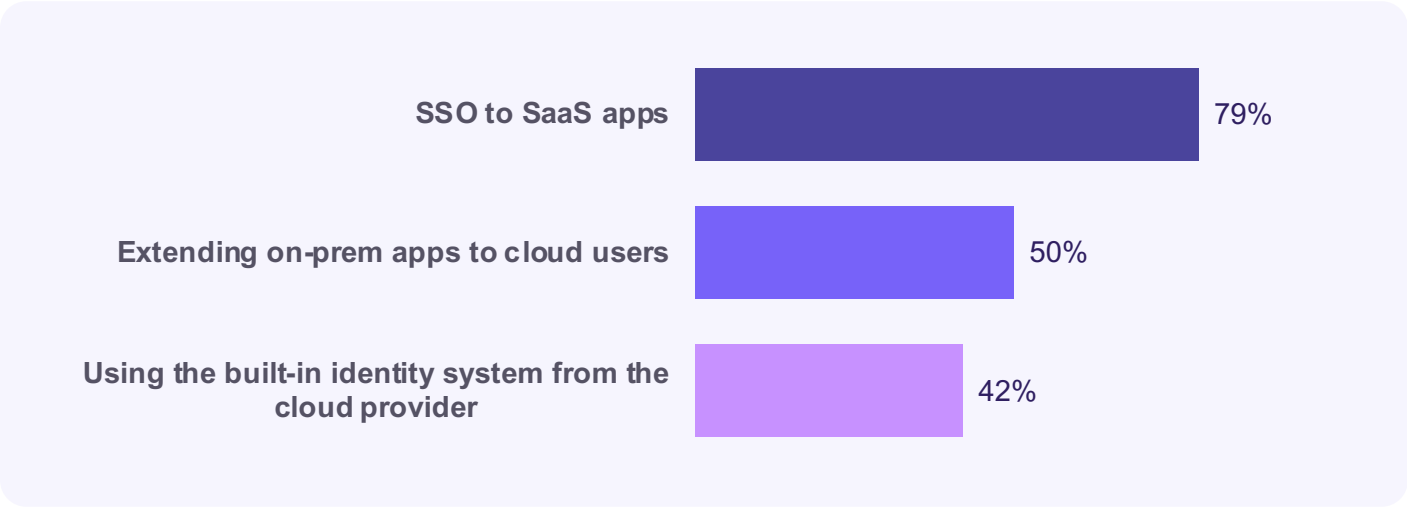
Identity Tactics Used for Multi-Cloud

Nearly **80% of organizations are using single sign-on (SSO)** as an identity tactic for their SaaS apps. SSO is still necessary in multi-cloud, but it is insufficient on its own. Using SSO for cloud apps is different than it is for SaaS. Organizations are realizing that they need to close the gaps created by these identity silos.

We found **50% of organizations are extending on-premises apps to cloud users**, but in order to extend access to these apps a new kind of software is needed for Zero Trust. Nearly half are using a built-in identity system for a cloud provider. Combined with organizations using three or more clouds, over half of enterprises must manage three identity systems plus other systems like Okta or Azure AD. Organizations need to think beyond the perimeter mindset and use Zero Trust and secure hybrid access to extend on-premises apps to the cloud.

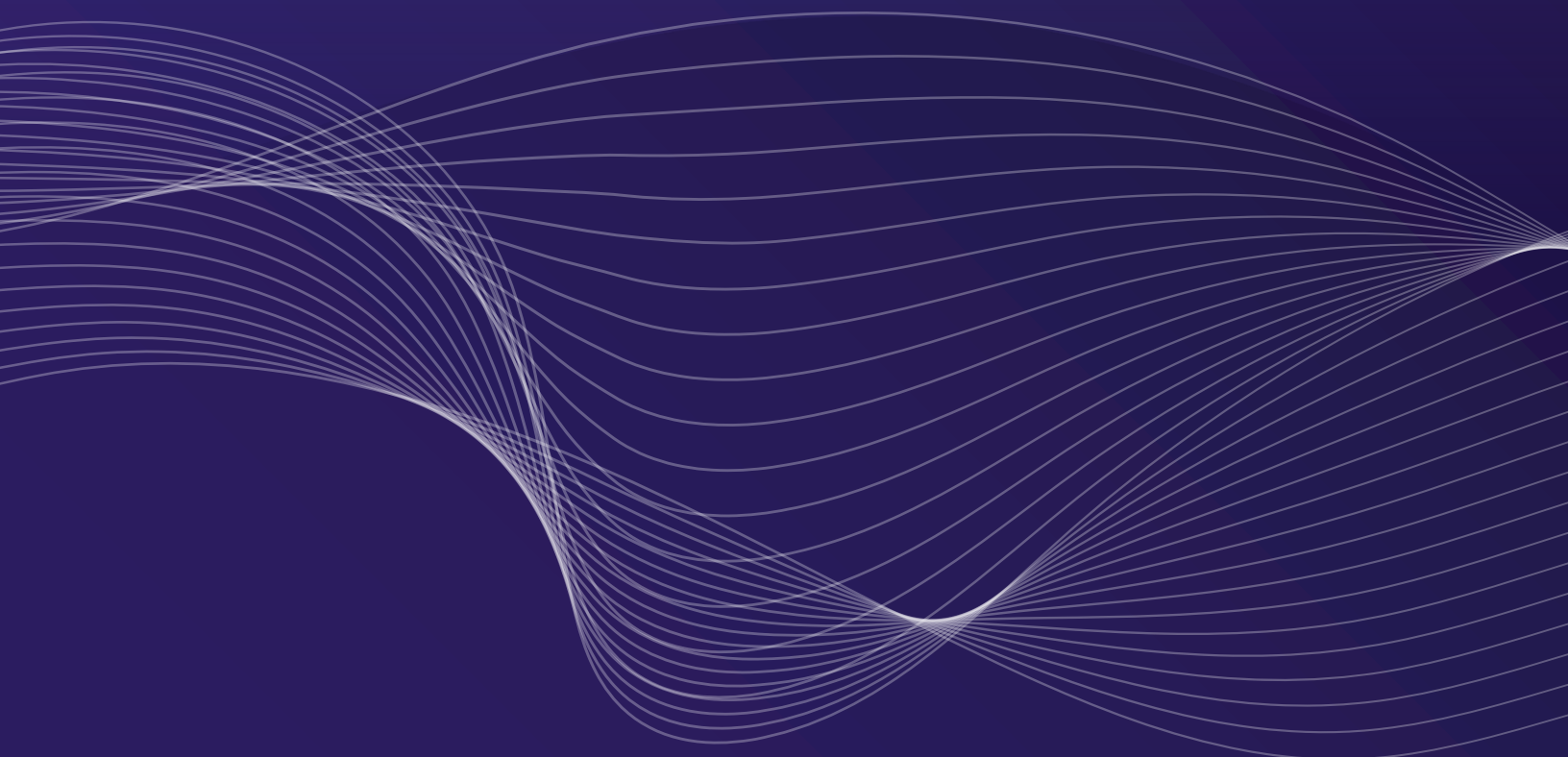
Q: Which identity tactics are you using for multi-cloud?

(Select all that apply)



02.2

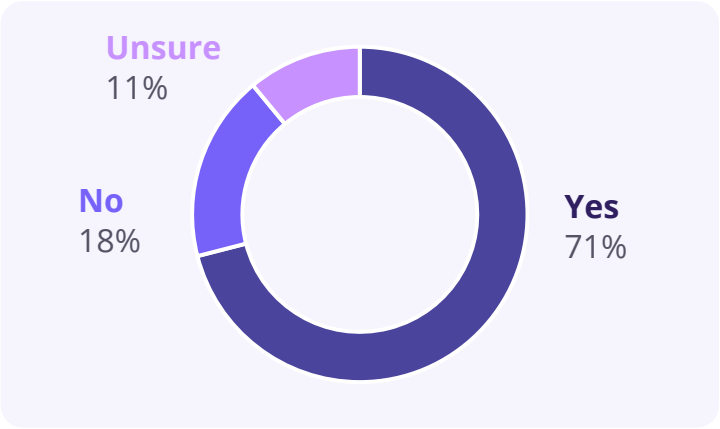
Distributed architectures are becoming mainstream



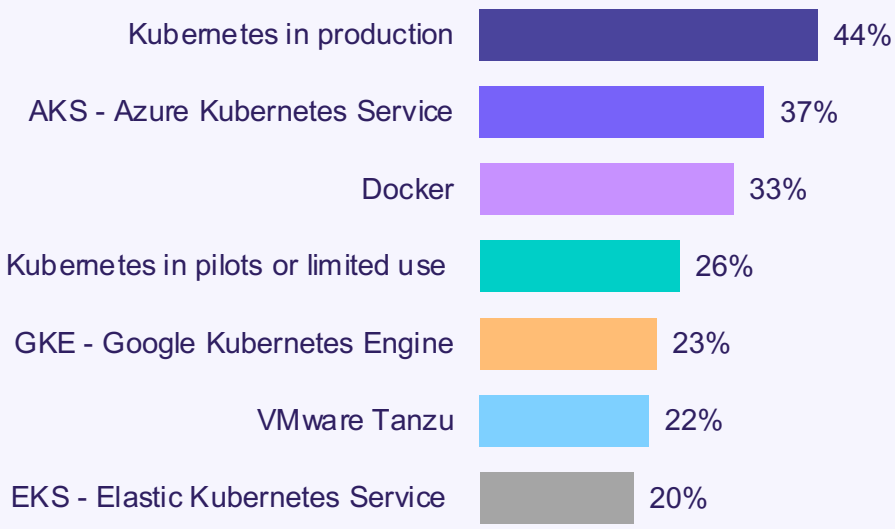
Distributed Architectures for Compute on the Rise

Everything is becoming distributed. Over **70% of organizations use distributed architectures or data**. The move toward distributed is driven by the growing awareness that multi-cloud can save money, provide organizations with the best-of-breed technologies, redundancy in case of a security incident, and more. In the same way that **compute and data have become distributed, so must identity.**

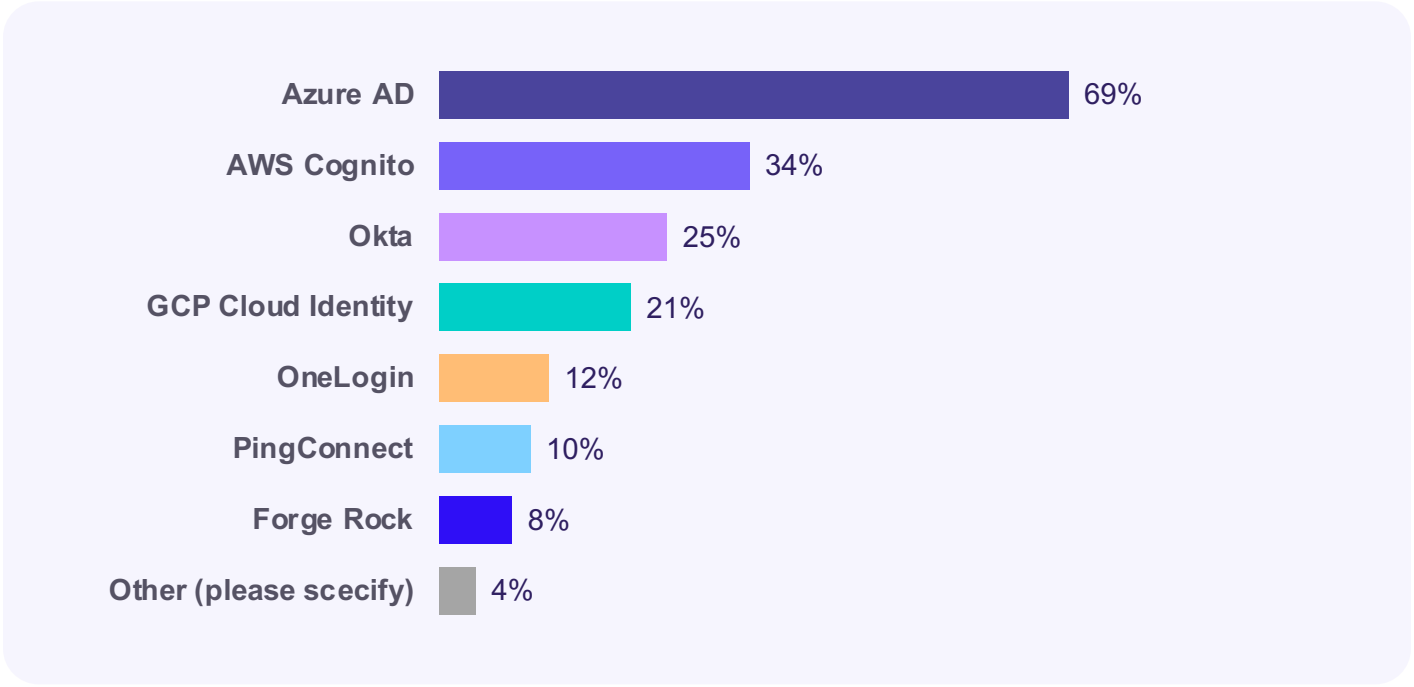
Q: Does your organization use distributed architectures for compute (Kubernetes) or data (e.g., Cohesity, Rubrik, etc.)?



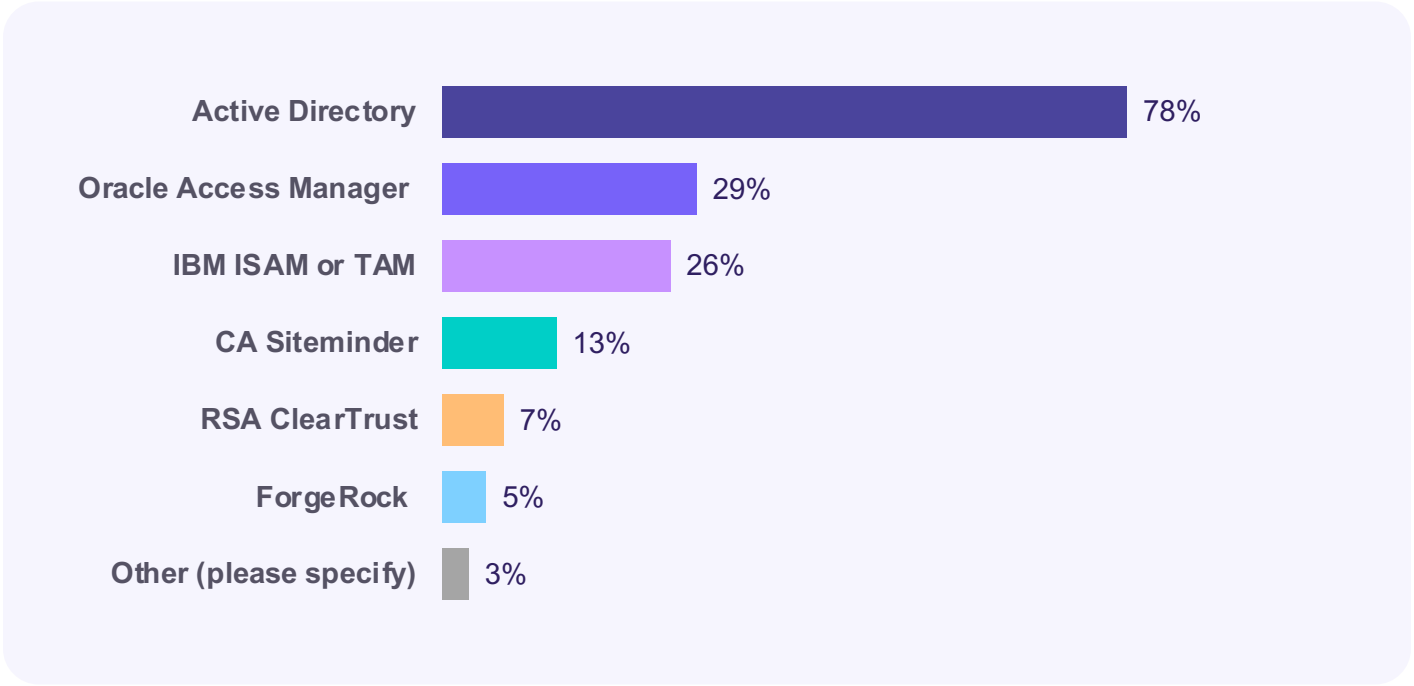
Q: Which IaaS Platforms Does Your Organization Use?



Q: Which Cloud IAM Providers Does Your Organization Use?
(select all that apply)

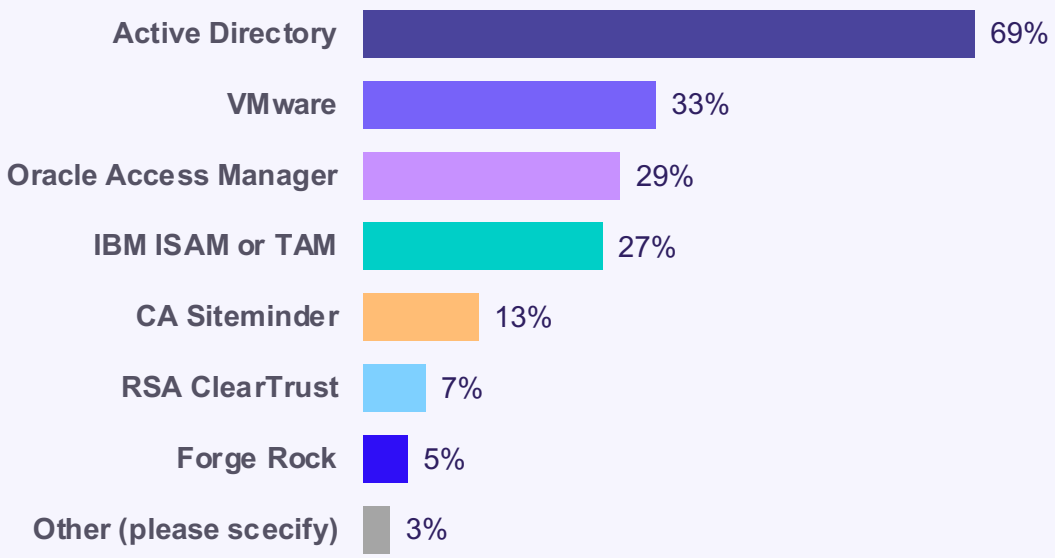


Q: Which On-Premises IAM Systems Does Your Organization Use?
(select all that apply)



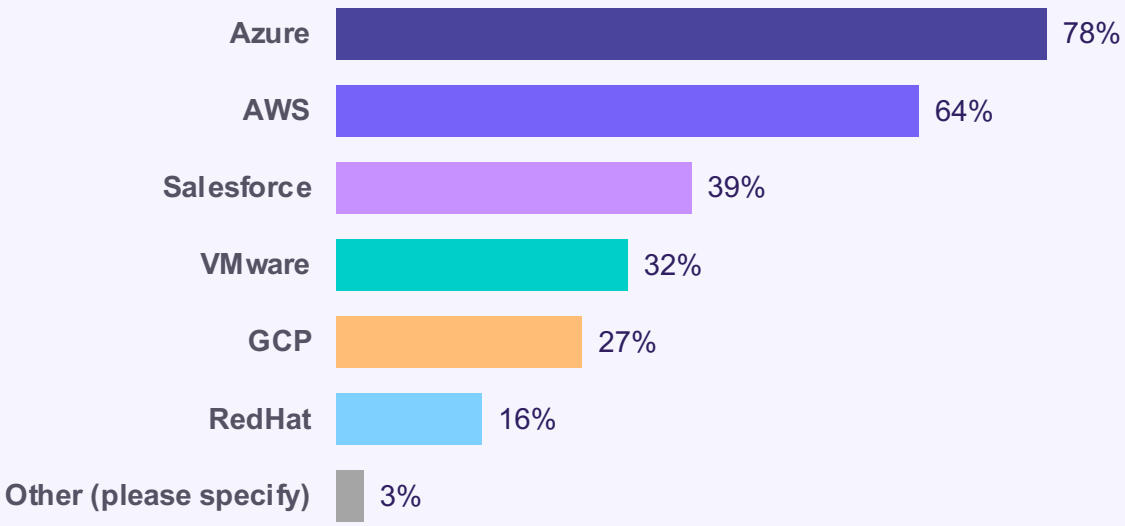
Q: Which On-Premises Systems Does Your Organization Use?

(select all that apply)



Q: Which Cloud Infrastructure Providers Do You Use?

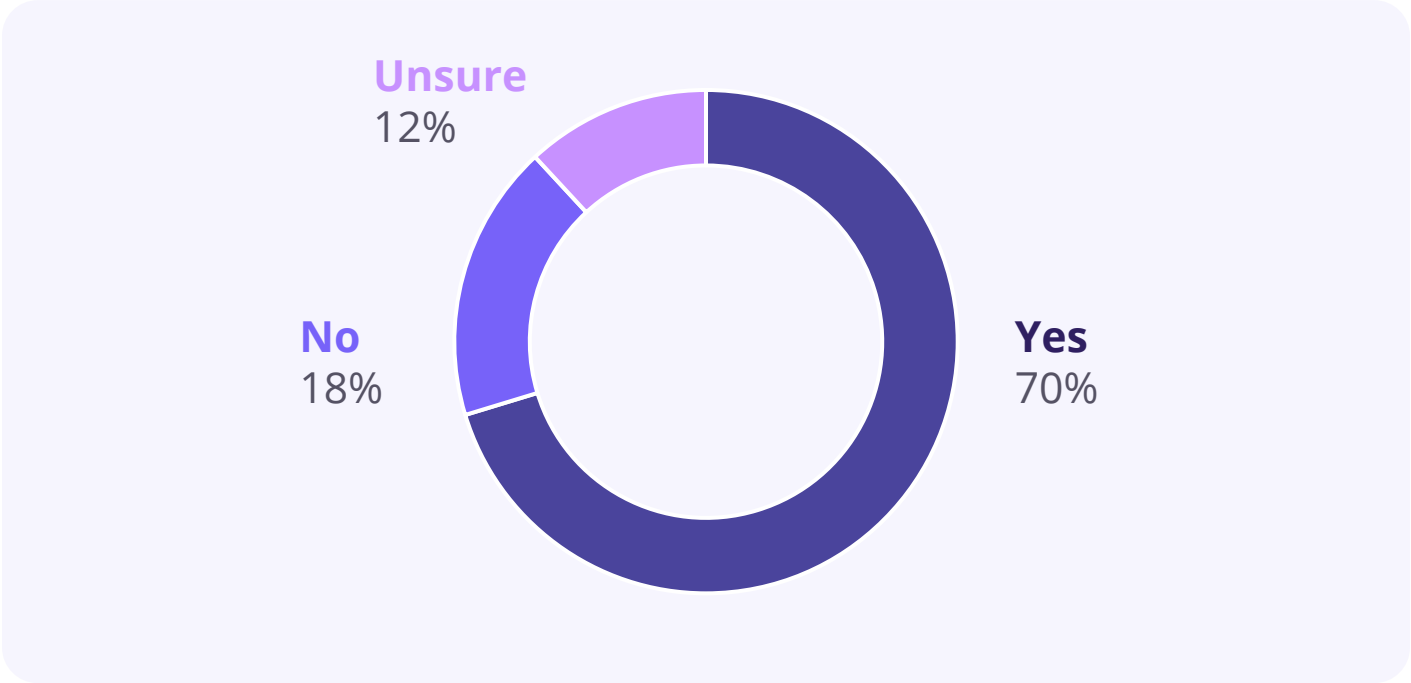
(select all that apply)



Importance of a Cloud-First Strategy Recognized

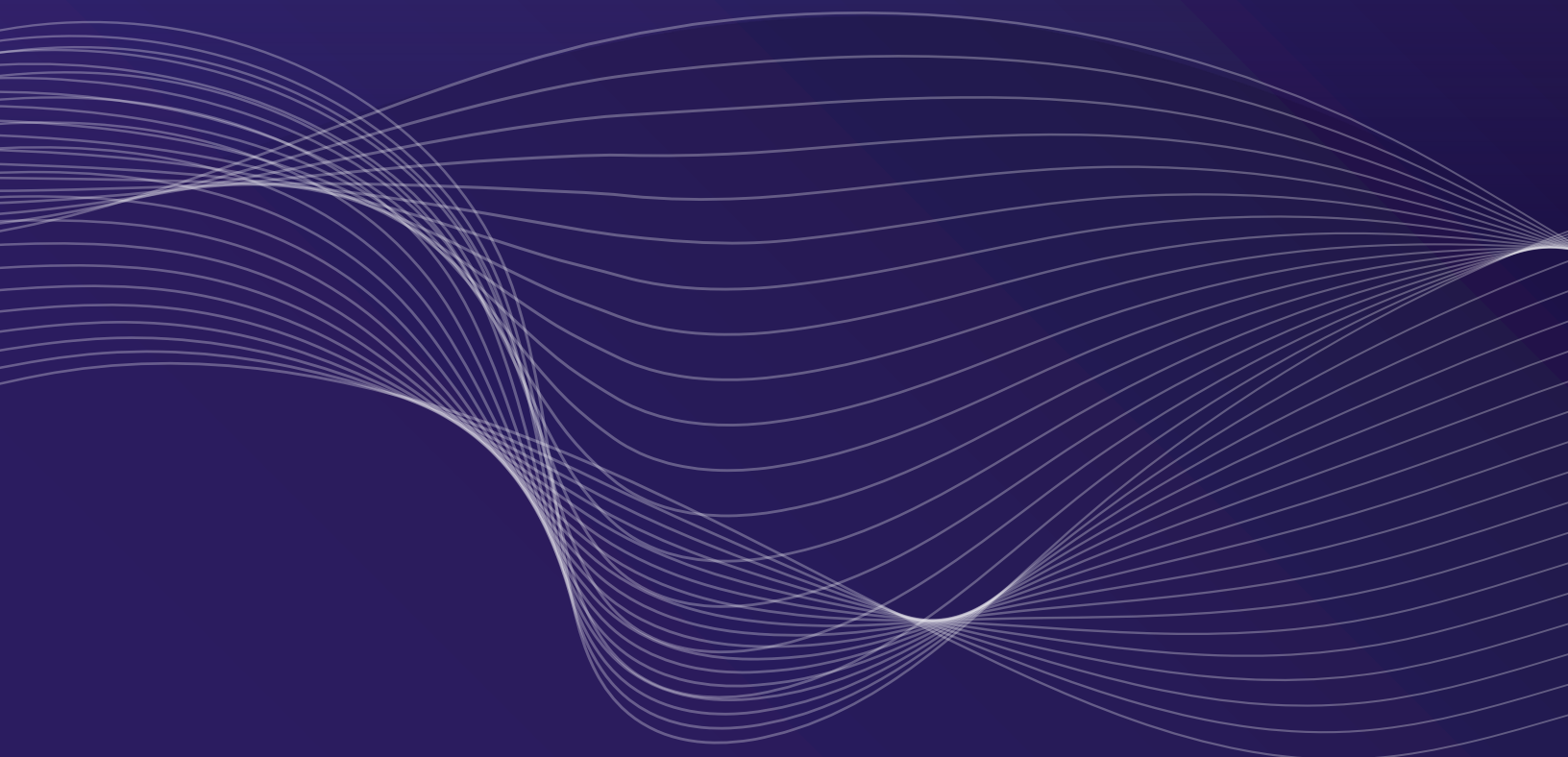
71% of organizations have a cloud-first strategy. Distributed, cloud-native architectures reflect cloud-first priorities.

Q: Does your organization have a 'cloud-first' strategy?



02.3

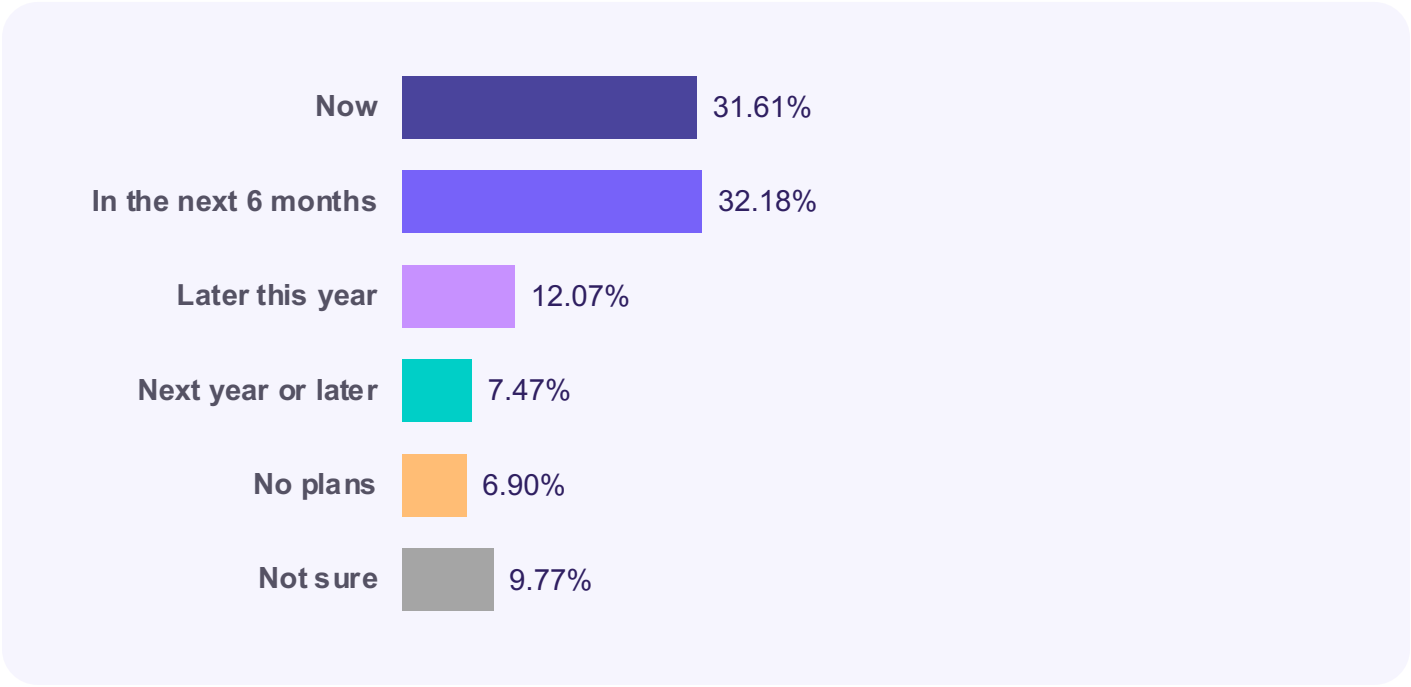
Multi-cloud and hybrid driving need for app and identity migration and modernization



Active Identity Modernization or Migration Project

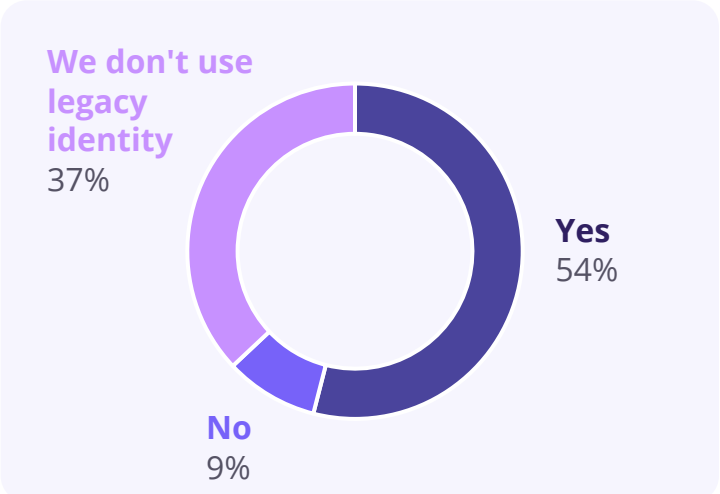
70% of enterprises have active migration/modernization projects in 2021.

Q: Do you have an active identity modernization or migration project?



Legacy End-of-Life Awareness & Planning

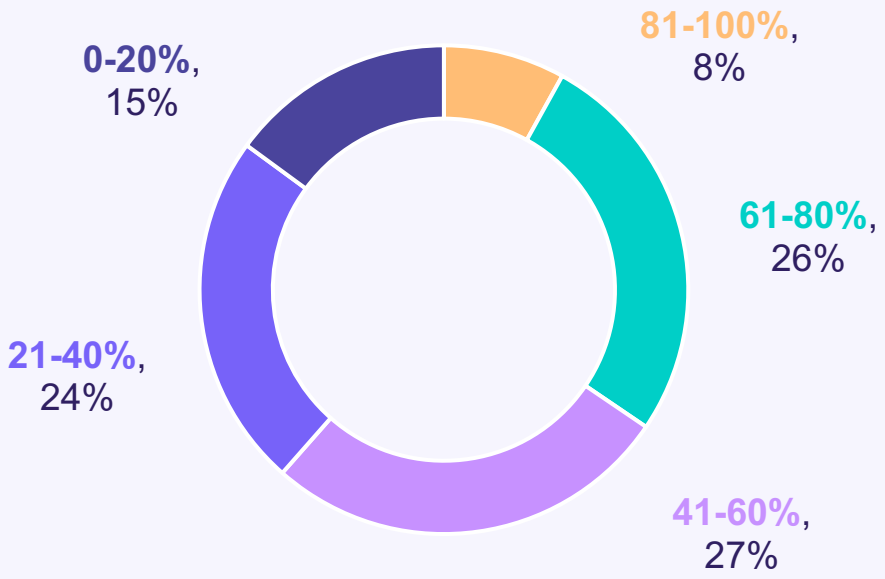
54% of respondents are aware CA SiteMinder, Oracle Access Manager, RSA ClearTrust, IBM TAM have reached End of Life (EOL) and will not be supported by 2022.



A Slow Go From On-Premises to the Cloud

Workloads are mostly still on-premises. **Only 34% of organizations say that more than half of their workloads are in the cloud**, meaning 66% still have majority of workloads on premises. The majority of organizations are more than halfway through their workload migration.

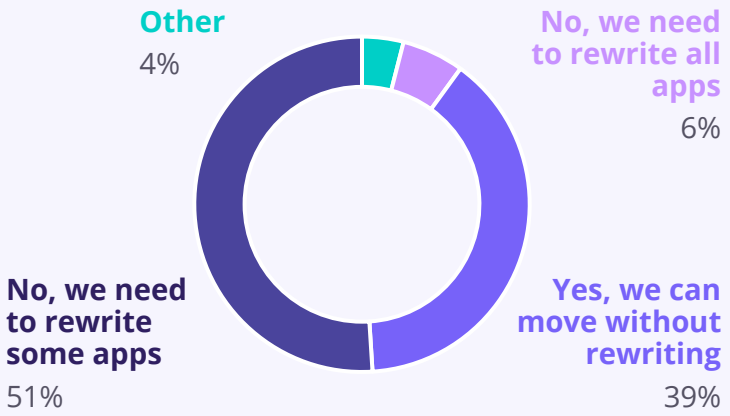
Q: What percent of app workloads has your organization moved from on-premises to the cloud?



Challenges of Moving Legacy Apps and Identity

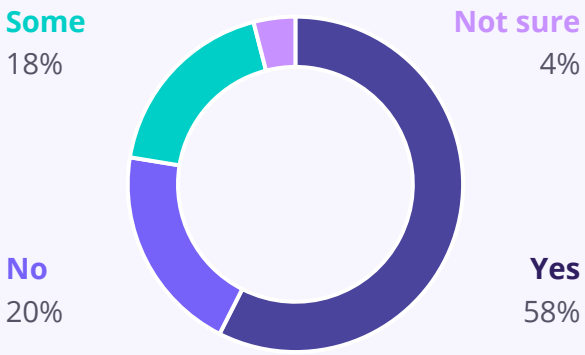
57% of enterprises need to rewrite at least some of their apps to migrate off legacy. Rewriting one app takes an average of two to three months. If an organization has hundreds or even thousands of apps, migration will take years and cost millions of dollars.

Q: Can you move your apps from legacy identity (SiteMinder, OAM, ClearTrust etc.) without rewriting them?



Manage Data Access Policy for Global Data

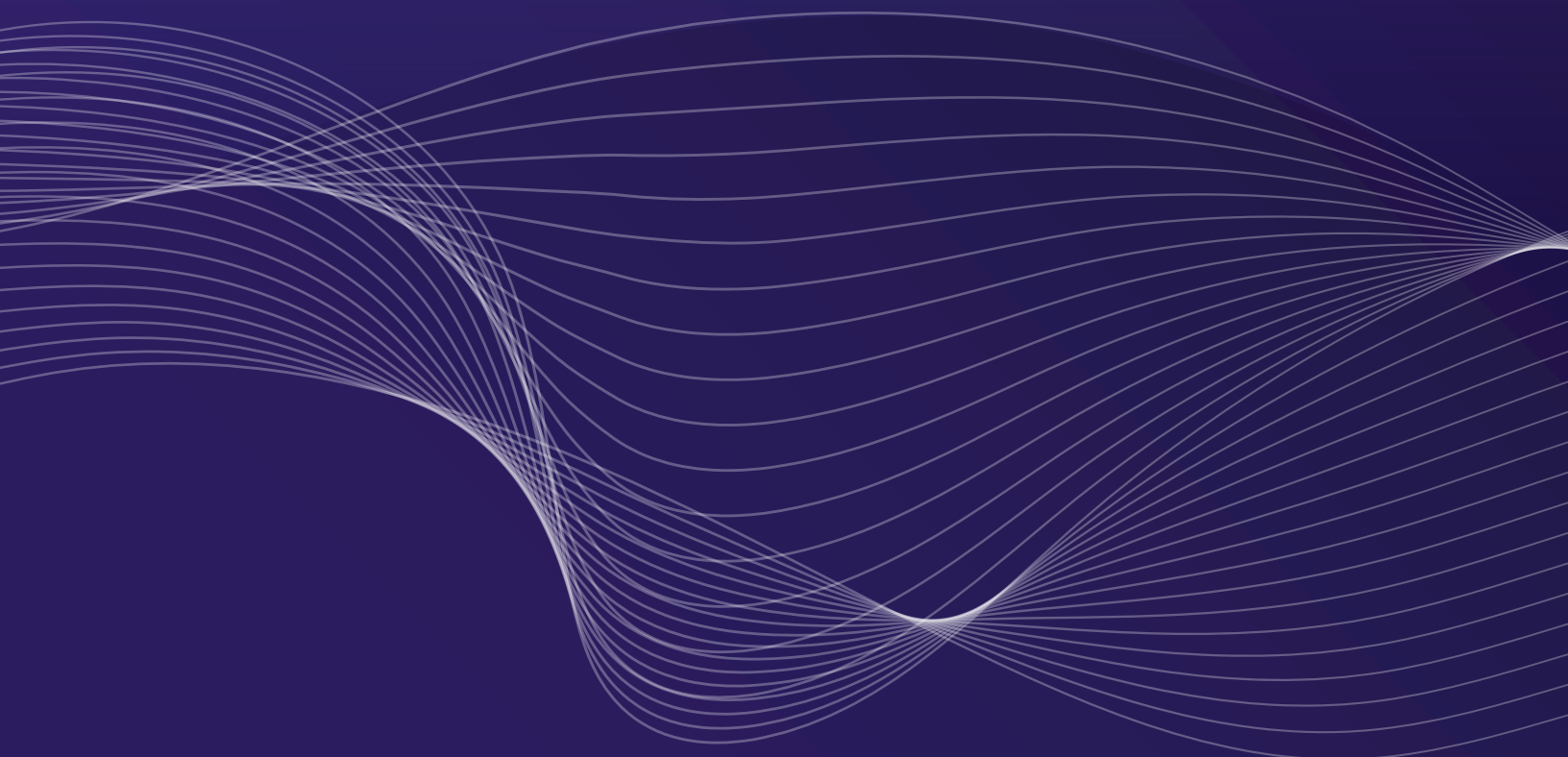
Global organizations face new challenges as a result of a diverse and evolving regulatory landscape. Over **75% of survey respondents must manage some data access policy for global data**. Organizations that lack a way to manage identity governance consistently across multiple cloud and on-premises identity providers and apps are at-risk of decreasing their security posture.



Q: Do you need to manage data access policy for global data?

02.4

Identity Governance in multi-cloud and hybrid is nearly impossible



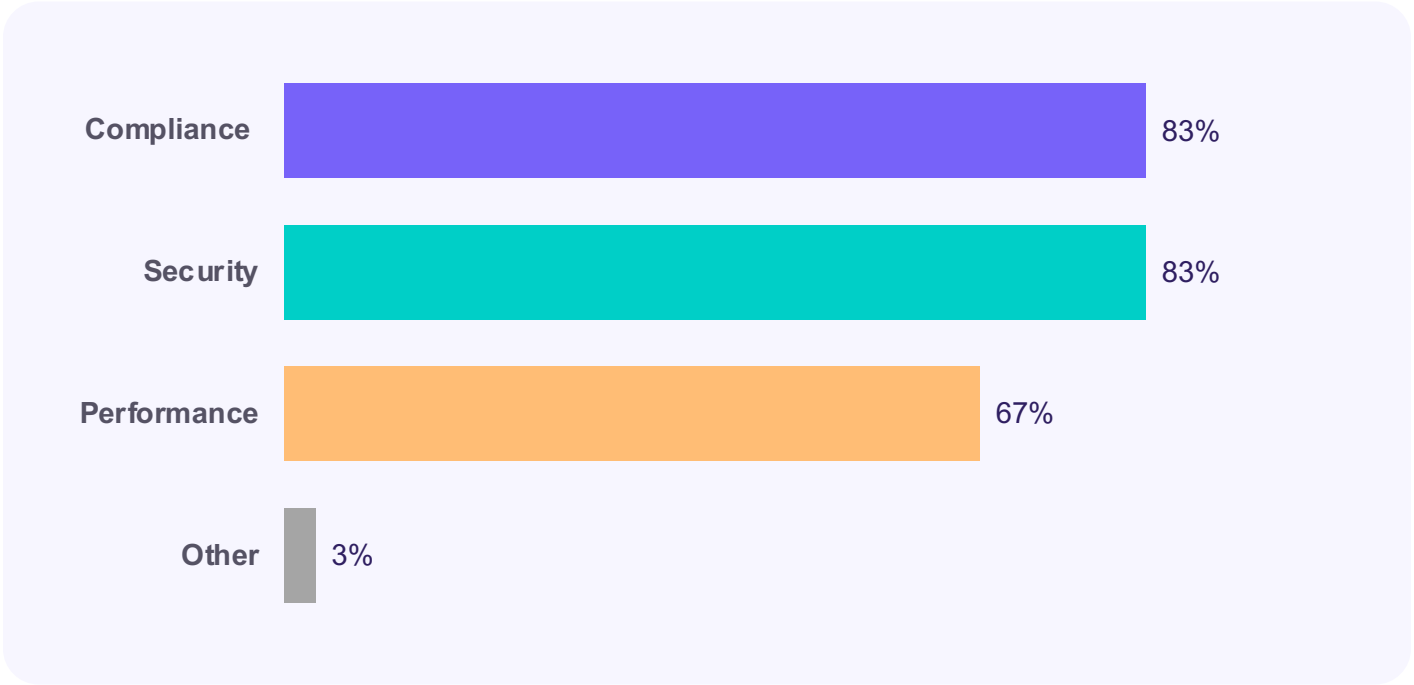
Factors that Affect Strategy for Data Storage

Where data is stored is a big consideration — especially for global enterprises where data privacy regulations differ from country to country. The **classic model of identity governance has broken down.** It doesn't work in the multi-cloud era.

Hybrid deployments extend existing investments by offering a way to keep sensitive data on-premises while allowing access to the cloud.

Q: Which factors affect strategy for where data may be stored?

(Select all that apply)



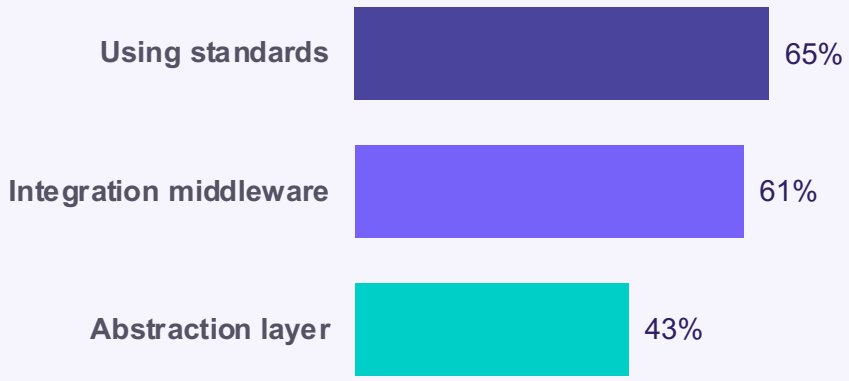
Inconsistency Managing Multi-Cloud

Managing multi-cloud environments is challenging and IT teams are using a variety of tactics to try to maintain visibility and security across multiple platforms.

- **65% of organizations are using standards (such as SAML)** and/or an integration middleware tool.
- **43% are experimenting with an abstraction** layer. This means that there is an understanding that doing an integration with one system to many systems is preferable to a one-to-one integration.

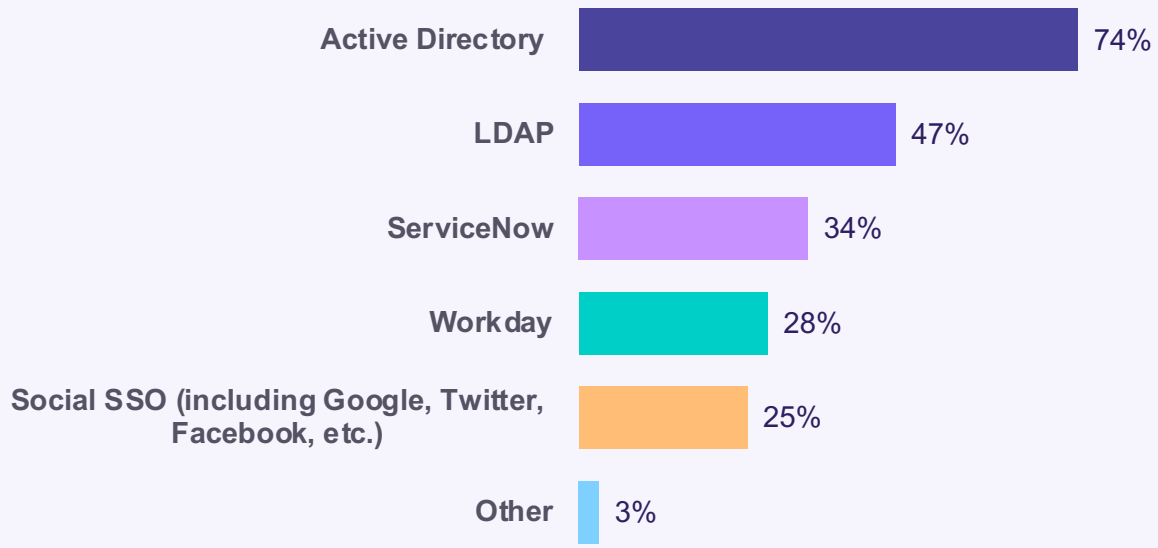
Q: What tactics have enabled you to manage multi-cloud?

(Select all that apply)



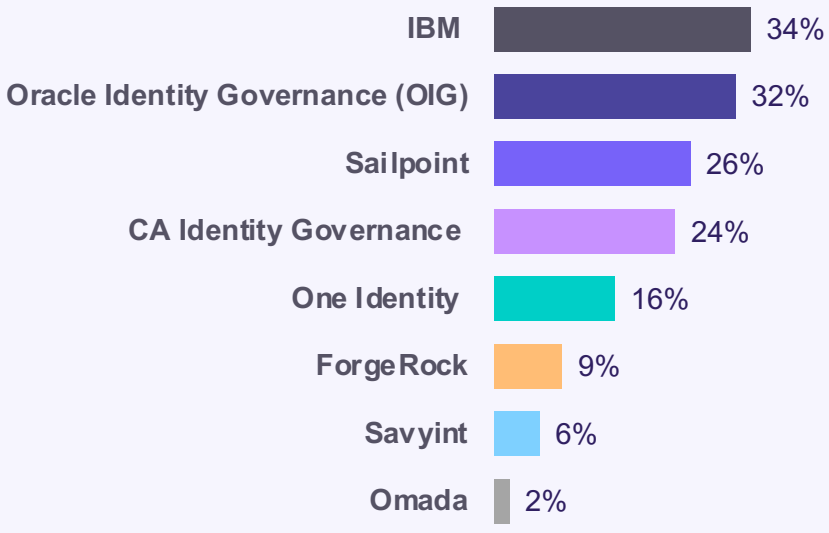
Q: Which IDPs Does Your Organization Use?

(select all that apply)



Q: Which Identity Governance Products Does Your Organization Use?

(select all that apply)



03

Conclusion:

Orchestration on top of an abstraction layer is the solution for multi-cloud identity

Identity Orchestration

Orchestration on top of an abstraction layer is the solution for managing identities for multi-cloud and distributed enterprises. Organizations need to manage identity across multiple clouds. Centralization doesn't work in distributed environments and rewriting hundreds of apps and identities isn't realistic or feasible.

Cloud adoption needs to go faster because thousands, or millions, of apps can't move to the cloud by hand. It will take too long, and enterprises will be locked out of all the benefits that the cloud brings.

Like how Kubernetes automates the deployment, management, scaling, and networking for data management, identity orchestration automates identity management for multi-cloud. It provides an abstraction layer that integrates heterogeneous identity management systems to make many policies, APIs, and sessions work as one.

Identity is enabling Zero Trust and secure hybrid access in multi-cloud with orchestration. Hybrid deployments extend existing investments. Emerging identity orchestration technology offers hope for multi-cloud organizations.

Download the

Guide to Identity Orchestration

04
Recommendations

Recommendations

Modernizing identity is a critical step to achieving Zero Trust in a hybrid or multi-cloud environment. Below are our go-to best practices to follow when embarking on your identity modernization and migration journey.

Think incrementally for your migrations

As tempting as it is to try and get migrations done quickly, “Big Bang” migrations don't work well. Organizations have been trying to do them for years and the failure rate on them is shockingly high. Instead, incremental migrations have a significantly higher success rate. It’s an agile process much better-suited for multi-cloud. It also allows for A/B testing, and if you experience a setback, simply roll back to a recoverable state with ease because you're taking things in small increments.

Modernize for a distributed, multi-cloud model

Centralization has been the traditional mindset that existing vendors would like people to believe is the right way. However, it’s not possible in multi-cloud. For example, AWS's identity system cannot take on Microsoft's identity system and vice versa. With modernization, embrace the distributed nature of existing platforms and build identity systems around that distribution.

Working with multiple clouds is not going to go away; it’s only increasing. Recognize that there will be multiple identity systems to manage and instead of trying to centralize, make each one of those things work better together.

Recommendations

Decouple apps from identity

Avoid tightly coupling your apps to your new identity system. Individual products bring their own ecosystems, like multi-factor authentication and deeper authorization.

The big reason behind many modernization efforts is to get untangled from vendor lock-in situations. So, when entering a modern identity system and a distributed model, don't couple apps tightly with identities so as not to repeat pitfalls of the past.

Instead, use an abstraction layer between apps and identity systems. This allows choice of any identity system, extends functionality to existing systems, and enables seamless switching between identity systems. An abstraction layer makes it much easier to achieve flexibility and choice when building out a distributed identity architecture.

About Strata

Strata is pioneering the concept of identity orchestration for distributed, multi-cloud identity. The Maverics Platform enables enterprises to seamlessly unify on-premises and cloud-based authentication and access systems for consistent identity management in multi-cloud environments. Strata's distributed approach to identity enables organizations to break decades-old vendor lock-in that has prevented a broader transition of enterprise workloads to public cloud infrastructures. The company's founders co-authored the SAML open standard for identity interoperability, created the first cloud identity services, delivered the first open-source identity products, and are now building the first distributed identity platform.

Visit us at Strata.io

Contact

General communication
For general queries, including partnership opportunities, please email info@strata.io

For Sales: sales@strata.io or 1-888-552-4930

Strata.io

STRATA