



STRATA
Identity Orchestration

3RD ANNUAL

STATE OF MULTI-CLOUD IDENTITY REPORT 2023

Complexity is the enemy of securing identity

How an identity fabric simplifies and
strengthens identity management
across the enterprise

Contents

Glossary	3
Important definitions	3
Executive summary	4
What you will learn from this report.....	4
About this report.....	4
Key findings	5
Identity fragmentation is a growing cybersecurity threat.....	5
Identity modernization and compliance are still the name of the game for identity investments.....	5
Hiring more identity pros is not the magic bullet for identity fragmentation.....	5
Acceptance of new distributed approaches, like an identity fabric and identity orchestration, to combat multi-cloud identity fragmentation is growing	5
Situation: The multi-cloud movement is accelerating, and identity is in the crosshairs	6
Everything, everywhere, all the clouds	6
Incomplete visibility, inconsistent identities, and manual efforts characterize legacy identity.....	7
Identity access policy management lags in the race to the cloud.....	8
Report card on identity management best practices: Needs improvement.....	9
Show me the money! Spending plans focus on identity	10
Challenges: Identity complicated by cloud migration and business performance.....	11
Cloud migration and innovation are hampered by fragmented identity	11
Geopolitical disruptions and digital transformation trends mean ignoring identity modernization is not an option.....	12
Outages hurt business performance and customer loyalty (ouch!)	13
Organizations can't hire their way out of the identity quagmire	14
Hiring challenges delay key identity projects and undermine business performance.....	15
Solutions and recommendations: Build your identity fabric through Identity Orchestration	16
Unified identity management: The promise of an identity fabric.....	16
The multi-cloud identity requirements	17
Constructing your identity fabric through Identity Orchestration: Benefits and possibilities	18
Conclusion: Harnessing the power of Identity Orchestration in creating a robust identity fabric	19
Methodology	20
Demographics of survey respondents.....	20
About Strata Identity	21

Glossary and definitions

Glossary

AD	Active Directory
AI	Artificial intelligence
AWS	Amazon Web Services
GCP	Google Cloud Platform
IAM	Identity and access management
IDP	Identity Provider
MFA	Multi-factor authentication
ML	Machine learning
SSO	Single sign-on

Important definitions

Multi-cloud means using multiple cloud platforms to host an organization's applications. For example, rather than being hosted on a single cloud platform, enterprise applications reside across any combination of public clouds like AWS, Azure, and GCP - as well as on-premises hybrid private clouds, along with dozens of second-tier specialized platforms. Cloud platforms bundle an identity system and specify how access policies — the rules detailing which specific identities gain defined permissions to any given resource — are created, maintained, and enforced. Each cloud platform takes a different approach to how organizations manage their identity and access policies.

Identity Orchestration is a distributed abstraction layer that integrates multi-cloud and hybrid identity infrastructure and allows automated fine-grained enforcement of consistent identity and access policies.

An **identity fabric** integrates your existing identity providers and identity services like MFA and Passwordless so that they all work together seamlessly. The result is a fully-composable identity environment where the individual pieces can be changed or replaced at any time without affecting the entire system or the end user experience.

We encourage the reuse of data, charts, and text published in this report under the terms of this Creative Commons Attribution 4.0 International License. You are free to share and make commercial use of this work as long as you attribute the Strata 2023 State of Multi-Cloud Identity Report as stipulated in the terms of the license.

Executive summary

Change is inevitable, as the saying goes. And, nowhere are the effects of rapid change more apparent than in today's multi-cloud computing environments.

Organizations are constantly adopting new tools and technologies, including multiple cloud platforms, to stay competitive, agile, and secure. The findings of this year's State of Multi-Cloud Identity Report build on the reports from 2021 and 2022 to show how organizations are thinking about identity services and technologies is shifting in response to external and internal forces.

What hasn't wavered in the past three years is the increasing prevalence of multi-cloud in the enterprise and the resulting identity fragmentation that leads to security and operational risk.

Identity is a fundamental component of enterprise security. It relies on uniquely differentiating one user from another, granting the correct level of access for policies for each employee, customer, and partner. Getting identity and access policies wrong can result in the costly loss of customer confidence, data breaches, and regulatory compliance issues.

However, getting identity and access policies right is not easy. Many organizations face challenges in driving identity modernization — often tied to attempts to hire unicorn identity professionals who can handle the complexity and diversity of multiple identity platforms and services. But finding such talent is difficult, if not impossible. The skills or talent gap has delayed identity modernization projects, undermined internal capabilities, and driven away customers and revenue.

The solution to these challenges lies in the orchestration of an identity fabric. By harmonizing identity and access policies, Identity Orchestration enables organizations to manage multiple identity providers to dynamically secure applications across multiple cloud platforms and integrate new identity services seamlessly.

The benefits of an orchestrated identity fabric are manifold. It facilitates organizational digital transformations, and the modernization of on-premises applications with modern authentication capabilities while ensuring the decommissioning of legacy identity infrastructure does not compromise critical business processes or undermine security.

What you will learn from this report

- How multiple cloud and identity platforms impact identity and access policy management and the security and operational problems that come as a result.
- How the talent gap in identity professionals prevents organizations from addressing their identity fragmentation, technical debt, and modernization needs.
- How an identity fabric can help organizations achieve seamless and secure identity management across multiple clouds by unifying and orchestrating identity and access policies.

About this report

Osterman Research conducted a survey for this research and prepared this report under commission from Strata Identity. Information about Strata Identity is provided at the end of the report.

The increasing prevalence of multi-cloud in the enterprise and the resulting identity fragmentation that leads to security and operational risk has been a continual theme over the past three years.

Key findings

Identity fragmentation is a growing cybersecurity threat

More identity systems are being used to manage users, and organizations are losing visibility and control over their identities and access policies. Since the 2022 State of Multi-Cloud Identity Report, the number of organizations using two or more IDPs has increased, while the ability to discover and enforce existing access policies has decreased. Improvements in identity infrastructure intended to drive an improvement in an enterprise's cybersecurity posture have caused the opposite effect leading to complexity overload.

Identity modernization and compliance are still the name of the game for identity investments

Organizations are investing in modernizing legacy identity systems, driving identity governance and regulatory compliance, and adopting modern authentication approaches, such as passwordless and MFA. These investments are essential to keep up with the evolving demands of customers, employees, and partners in today's multi-cloud era.

Hiring more identity pros is not the magic bullet for identity fragmentation

It's hard to find and keep talented identity pros who can handle complex and diverse identity infrastructures. Even with more staff, rewriting old applications to play nicely with modern identity systems is expensive and slow. It stagnates important identity projects and hurts an organization's ability to innovate and compete.

Acceptance of new distributed approaches, like an identity fabric and identity orchestration, to combat multi-cloud identity fragmentation is growing

An identity fabric offers a fresh approach to identity and access management that seamlessly weaves legacy and modern identity systems. With an identity fabric, organizations can:

- Automate and orchestrate identity operations across multiple IDPs using no-code integration to secure and control users' runtime experience.
- Approach identity management through a single pane of glass and work seamlessly across multiple cloud platforms without worrying about identity and access policy gaps.
- Modernize on-premises applications with MFA and passwordless, without rewriting application code.
- Deliver business-led innovation without hiring hard-to-find unicorn engineers.
- Retire legacy identity infrastructure without breaking business processes or taking the business offline.

Identity Orchestration and an identity fabric let organizations enjoy the best of both worlds: the security and compliance of on-premises hybrid systems and the agility and innovation of cloud identity systems.

Recent investments in identity infrastructure were intended to drive an uplift in cybersecurity posture—not overwhelm it with complexity.

Situation: The multi-cloud movement is accelerating, and identity is in the crosshairs

The shift to multi-cloud is driven by organizational needs, such as having best-of-breed cloud capabilities; redundancy and high availability; IT modernization; mergers, acquisitions, and divestiture activity; and of course improved efficiency and security. To reap the benefits of a multi-cloud strategy, organizations must strategically plan for and tackle challenges around identity fragmentation.

Everything, everywhere, all the clouds

Organizations face a set of hurdles preventing the migration of applications to the cloud at the desired cadence and identity at the center. The following are the big issues keeping CISOs and identity practitioners up at night (see Figure 1):

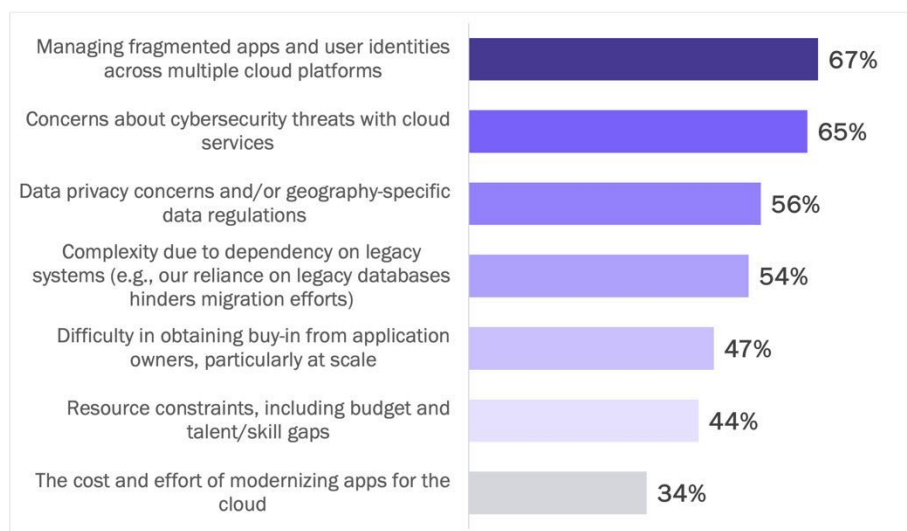
- Managing fragmented applications and user identities across multiple cloud platforms (67%)**
 The goal of a unified, resilient, and robust multi-cloud strategy is hampered by fragmentation of applications and user identities across identity silos. Fragmentation undermines the value proposition of multi-cloud, imposes ongoing costs for manual reconciliation of applications and identities, and increases the chances of unexpected data access and breach.
- Cybersecurity threats with cloud services (65%)**
 Identity attacks are a leading threat vector with cloud services, where a malicious actor uses compromised credentials for unauthorized access to applications and data. Organizations that lack visibility into access policies compounded by fragmented user identities face unknown threat vectors they cannot see.
- Data privacy concerns and/or geography-specific data regulations (56%)**
 Meeting the demands of emerging data privacy and geography-specific data regulations requires highly mature disciplines across data, applications, and identities, among others. When threat actors exploit inconsistencies in who can access what data, auditors start asking hard questions, and regulators impose expensive fines.

Identity is at the center of the roadblocks preventing organizations from migrating applications to the cloud.

Figure 1

What's getting in the way?

A lot. But these are what respondents indicated as “significant” or “extremely significant”



Source: Osterman Research (2023)

Incomplete visibility, inconsistent identities, and manual efforts characterize legacy identity

Organizations admit facing serious challenges in managing identities and applications across multiple cloud platforms and identity systems. The top challenges are:

- Limited visibility into access policies and applications (76%)**
 Three-quarters of organizations do not have complete visibility into the access policies and applications across multiple cloud platforms. They do not have a complete picture of which access policies exist, where applications are deployed, and who does and doesn't have access.
- Inconsistent attributes and duplicated user identities (56%)**
 More than half of organizations don't have a single version of the truth for identities and their associated attributes. Identity duplication with cloud-specific attributes is a consequence of multi-cloud, increasing the likelihood of unauthorized access and credential breach.
- Significant manual effort required (47%)**
 Organizations attempt to use manual efforts to cobble together multiple identity systems across clouds and on-premises systems. Manual effort increases the likelihood of error in reconciling identities and attributes. For organizations also hampered by incomplete visibility, this increases the probability of breach when identities and access are not fully and quickly revoked for employees, contractors, customers, and third-party partners.

See Figure 2.

Figure 2

📍📍 Everything, everywhere, all the clouds
 Percentage of respondents



Source: Osterman Research (2023)

Limited visibility, inconsistent and duplicated user identities, and significant manual effort are the identity nightmares ruining the cloud dream.

Identity access policy management lags in the race to the cloud

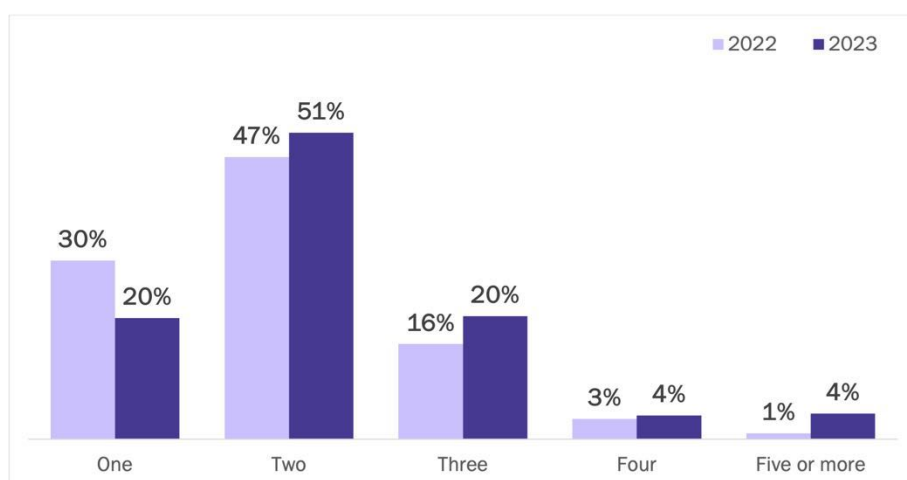
Embracing multi-cloud means managing the complexity required for identities and access policies across multiple platform-specific identity systems. Each platform's mix of user types — such as employees, customers, and partners — makes this even more complex.

The research in this year's report shows an increased number of organizations using two or more cloud or on-premises identity providers, such as Microsoft Azure AD (which is being rebranded as Microsoft Entra ID), AWS Cognito, Okta, SiteMinder, and PingFederate. The percentage of organizations using a single identity provider dropped from **30% last year to 20% this year**, while a growing percentage of organizations are using **two or more identity providers**. See Figure 3.

Figure 3

 **When one just isn't enough: Multiple IDPs and multiple types of users**

Percentage of respondents



Source: Osterman Research (2023)

While it's becoming standard operating procedure for organizations to use multiple identity systems, the ability to consistently manage identity and access policies is declining. More than half of organizations are struggling to discover and enforce access policies effectively:

- Just 40% can discover existing access policies**
 Discovering existing access policies across all cloud platforms in use means organizations know who has a given level of access permission to specific resources. Only 40% were confident in their discovery efficacy this year, down from 66% last year — a 39% year-on-year decline.
- And only 41% can enforce consistent access policies**
 Enforcing consistent access policies across all cloud platforms in use reduces identity and security risks. Only 41% were confident in their ability to do so this year, down from 55% last year — a 25% year-on-year decline.

A matter of policy

Only 7% of respondents indicate that identity access policy management is not a challenge for their organization. The vast majority say the process is challenging. Ineffective capabilities for managing identity amplify cybersecurity weaknesses, highlight tech debt's impact, and raise data privacy and protection non-compliance risks.

More IDPs and less efficacy at managing access policies — this case of “more and less” isn't a proposition for winning in the cloud.

Report card on identity management best practices: Needs improvement

Reaching the promised land of multi-cloud depends on a seamless identity experience across cloud platforms and applications; most organizations in this study know they're missing that mark. In looking at the relative importance of identity initiatives over the next 12 months (see Figure 4), key shortcomings are:

- Lack of integration between cloud identity and on-premises applications**
 Modern capabilities in cloud identity platforms are not available for use in hybrid legacy on-premises applications. Organizations want the capabilities of cloud identity platforms extended to on-premises private cloud infrastructure, too, so they can leverage modern capabilities and retire legacy identity infrastructure.
- Insecure approaches to remote access for employees and vendors**
 Work-from-home policies, hybrid and mobile workforce strategies, and integration across the supply chain rely on providing secure zero-trust remote access to organizational applications and data. Identity is a key component of zero-trust architectures.
- Reliance on manual processes for identity management**
 Organizations rely on manual processes for integrating applications with identity platforms, which requires ongoing vigilance as applications and identity services constantly change. Organizations want automated no-code and low-code solutions, and they want them now.

Organizations plan to invest in various initiatives to address these shortcomings over the next 12 months to strengthen the key identity capabilities needed to enable the continued shift to multi-cloud. See Figure 4.

Figure 4

 **Annnd action! Identity initiatives over the next 12 months**
 Percentage of respondents indicating “important” or “extremely important”



Source: Osterman Research (2023)

There's no identity genie for migration

Only with a genie offering three wishes could organizations simultaneously move all their workloads to the cloud. Until that magic lamp is found, however, organizations must face the reality that a full, immediate migration to the cloud is not realistic and that hybrid environments are here to stay.

Organizations are spending up to shore up identity initiatives to keep identity on the up-and-up.

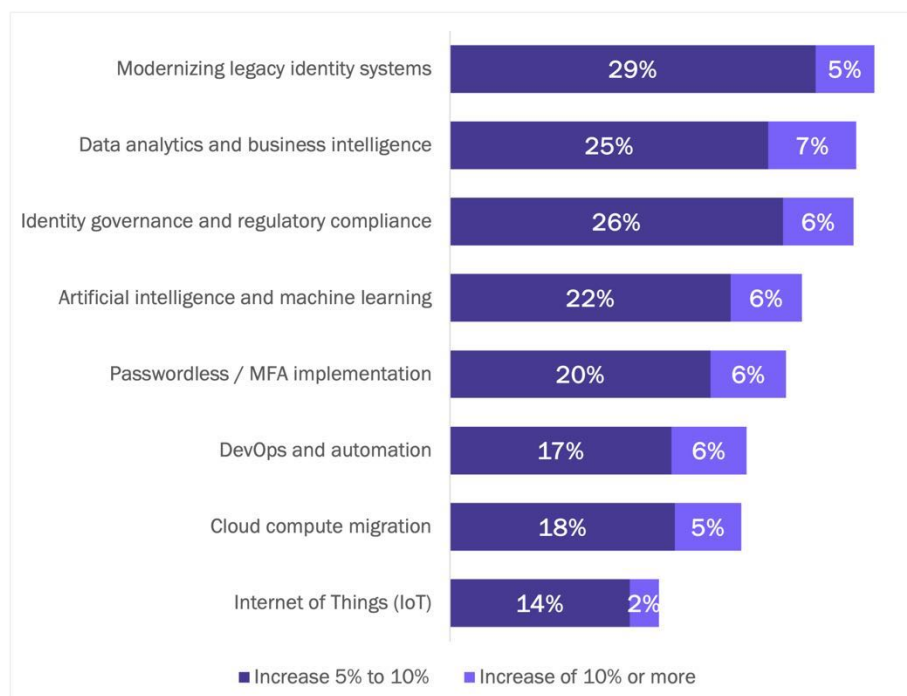
Show me the money! Spending plans focus on identity

Identity projects are getting more investment in 2023. Three of the top five budget changes were for identity projects, with a quarter and **a third of organizations spending more in 2023 than in 2022**. Among the eight budget areas surveyed, modernizing legacy identity systems took place first. Here are the top spending plans:

- Modernizing legacy identity systems (34% spending more)**
 Migrating off legacy identity systems to modern identity providers is the area of highest growth. Legacy identity systems lack the security, resilience, and extensibility required.
- Identity governance and regulatory compliance (32% spending more)**
 Investments in identity governance (e.g., visibility into identity rights, division of duties, and analytics) and regulatory compliance are high on the list. Organizations want to avoid the headaches of identity chaos and non-compliance penalties.
- Passwordless / MFA implementation (26% spending more)**
 Finally, enabling modern authentication approaches such as Passwordless authentication and MFA is important. As discussed above, organizations face barriers to implementing modern authentication approaches for all applications (especially those on-prem applications, sometimes referred to as "unmanageable apps"), and higher budget spending to address those barriers is needed.

Nestled somewhere in the middle, data analytics and business intelligence attract the second highest overall increase in budget (at 32% of organizations), and AI/ML in fourth place (28%) — meaning that two areas of **spending on identity are more important than AI/ML** for now. See Figure 5.

Figure 5
 💰 **Investing in identity: Change in allocated budget 2022 to 2023**
 Percentage of respondents



Source: Osterman Research (2023)

When identity initiatives are a higher priority than the poster child of all things cool – here’s looking at you, AI – it’s clear we have a problem.

Challenges: Identity complicated by cloud migration and business performance

Identity fragmentation is as bad as it sounds. It inflicts high costs on organizations, slowing cloud migration and innovation, delaying the benefits sought from multi-cloud strategies, raising cybersecurity and regulatory risks, and driving customer churn.

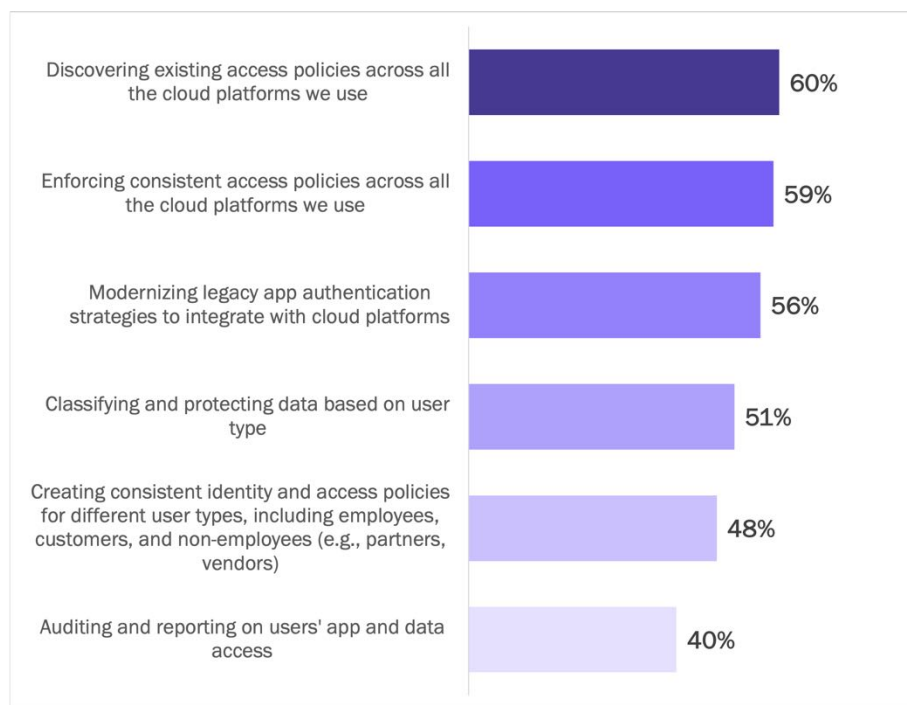
Cloud migration and innovation are hampered by fragmented identity

Less than half of organizations indicate they have effective approaches for managing identity when modernizing applications for the cloud. Organizations struggle to discover and enforce access policies across cloud platforms, modernize legacy application authentication strategies, and classify and protect data based on user type. The process with the highest efficacy (60% — the inverse of the 40% below) is the capability to audit and report on users' applications and data access — a baseline identity requirement many cannot or can only partially do. See Figure 6.

Figure 6

🙄 **But is it working? Ineffectiveness of identity and access capabilities**

Percentage of respondents indicating capabilities are not effective



Source: Osterman Research (2023)

The cost of identity fragmentation is also apparent in how few organizations have enabled modern authentication—such as MFA and Passwordless—for every application on every platform. Microsoft found that adding MFA eliminated 99.9% of credential attacks,¹ and yet **only 1% of organizations with up to 500 applications and 2% of organizations with 500 or more applications** have achieved securing every application on every platform. The entire organization is exposed to risk if just one application isn't protected.

Organizations hampered by fragmented identity can't migrate to the cloud or innovate.

Geopolitical disruptions and digital transformation trends mean ignoring identity modernization is not an option

High profile cybersecurity attacks; escalating regulatory demands for cybersecurity and data privacy; and growing use of digital channels for engagement with customers, employees, and partners are the three most impactful external trends and challenges driving the urgency of identity modernization. Navigating these trends and the other challenges in Figure 7 requires enhancing identity and access practices fundamental to security. The two most significant trends are:

- High profile cybersecurity attacks on other organizations (35%)**
 Organizations want to avoid being the next victim of a breach caused by an identity or access weakness — stuck with the lasting reputation damage of a ransomware attack.
- Escalating regulatory demands for cybersecurity and data privacy (31%)**
 Nor do executives want to violate changing regulatory standards, resulting in fines and reputational damage. New data privacy regulations (e.g., GDPR in Europe and state-level regulations in California, Virginia, and Colorado, among others) also impose identity obligations on organizations, such as accurately identifying customers requesting data rights irrespective of cloud or application.

The declining economic outlook and challenging geopolitical risks are very or extremely impactful for 65% of organizations. These two trends threaten budget allocations, elevate the risk of catastrophic cyberattacks, and represent areas of significant unknowns.

Figure 7

Modernize or else! Impact of trends and challenges on identity projects in 2023
 Percentage of respondents indicating “extremely impactful” or “very impactful,” with the list sorted by the “extremely impactful” responses



Source: Osterman Research (2023)

Modernizing identity is so much more than a good sounding ideal; it's critical to embracing the opportunities and avoiding the catastrophes of modern digital business.

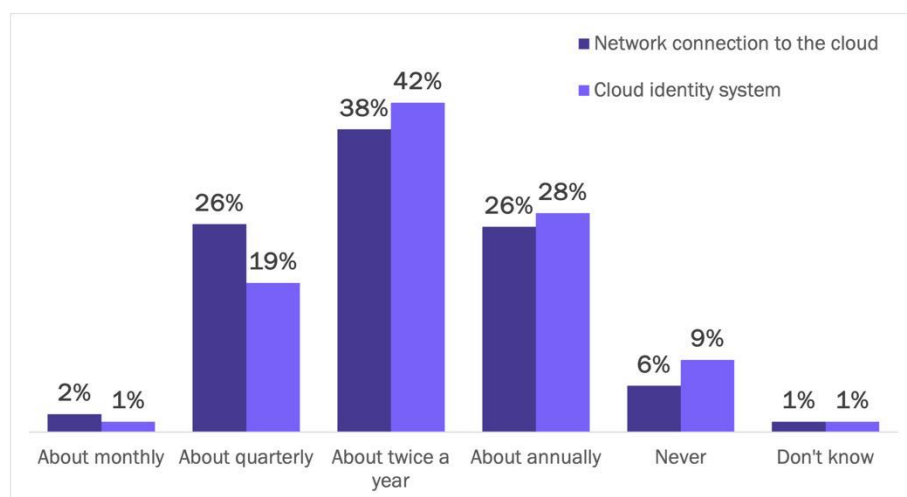
Outages hurt business performance and customer loyalty (ouch!) 🤔

Organizations can't rely on a single cloud identity solution since an outage cripples business operations and drives away customers. Headline-grabbing outages of major cloud identity systems warn organizations of these risks and lack of identity resilience.

Most organizations in this research report outages impacting their cloud identity system occurring several times yearly. For two-thirds of organizations, network and cloud identity system outages happen monthly, quarterly, or twice a year. Only 6% of organizations say they've never experienced an outage caused by a network connection failure, and 9% say they've never experienced an outage of their cloud identity system. See Figure 8.

Figure 8

🤔Houston, we have a problem. Frequency of outages of cloud identity systems
Percentage of respondents



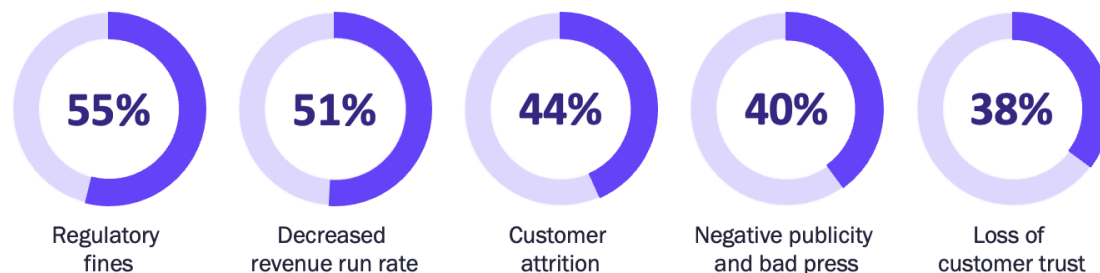
Source: Osterman Research (2023)

Virtually all organizations experience identity outages every year, resulting in regulatory fines and lost customers.

When cloud identity systems are unavailable, organizations bear the cost. The most frequently experienced cost is regulatory fines (significant at 55% of organizations), followed by decreased revenue (51%) and customer attrition (43%) due to customers taking their business elsewhere. See Figure 9.

Figure 9

🔨Hitting where it hurts. Business costs of cloud identity system outages
Percentage of respondents indicating "significant" or "extremely significant"



Source: Osterman Research (2023)

Organizations can't hire their way out of the identity quagmire

When faced with fragmented applications and user identities, most organizations try to hire more people to fix the problem. This sounds easier than it is:

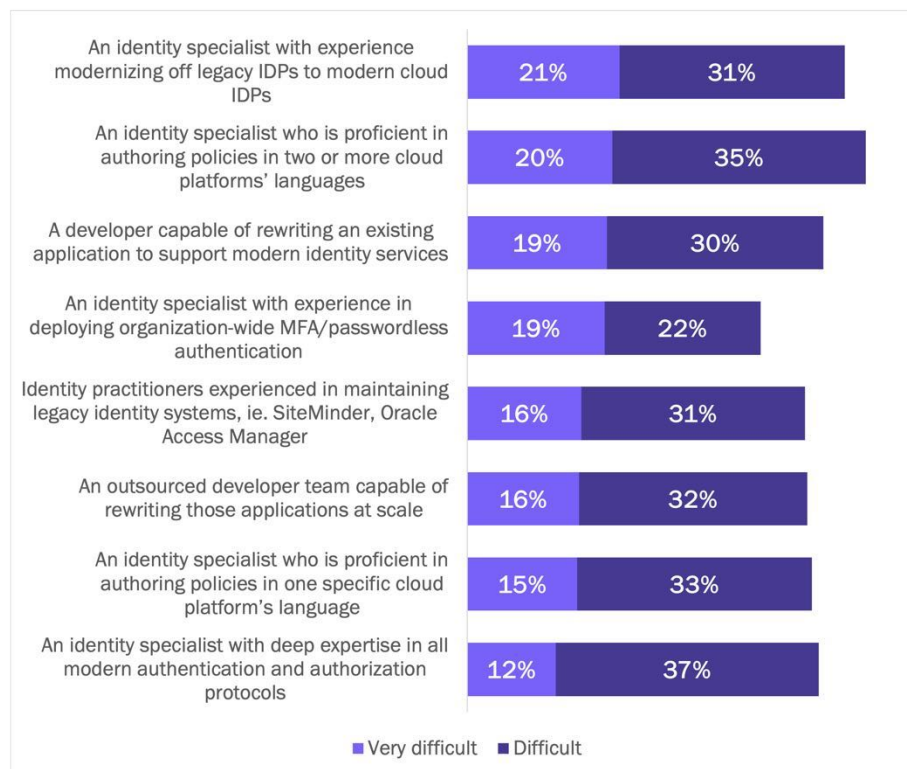
- Half of organizations can't find the right people**
 Identity professionals with experience in modernizing applications off legacy identity systems are the most challenging roles to hire (52% say this is "difficult" or "very difficult"). Other key roles are just as hard—for example, an identity specialist proficient in authoring policies in two or more languages and a developer able to rewrite applications to support modern identity services. From what we've already looked at, however, these are the roles organizations need the most. See Figure 10.
- 60% of organizations do not have the resources or time to rewrite old, outdated applications**
 A lack of resources and time to rewrite applications is an insurmountable barrier to modernization initiatives for most organizations in this research.
- 78% of organizations struggle with other barriers to identity modernization**
 Only 22% of organizations have access to the source code for their applications, judge the deployment risk as manageable, and have available resources and time for implementing modern authentication for all applications.

The vast majority are blocked by one or more of these critical barriers. And yet, as the world moves on and employees, customers, and partners demand higher identity security from the organizations they work for and with, **organizations can't afford the do-nothing approach.**

60% of organizations do not have the resources or time to rewrite old, outdated applications.

Figure 10

🦄 Looking for a unicorn in a herd of zebras? Difficulty of hiring identity professionals
 Percentage of respondents indicating "difficult" or "very difficult"



Source: Osterman Research (2023)

Hiring challenges delay key identity projects and undermine business performance

Organizations that experience hiring difficulties for IAM roles experience downstream problems. Failure to address the talent gap for identity professionals has resulted in the following negative effects (see Figure 11):

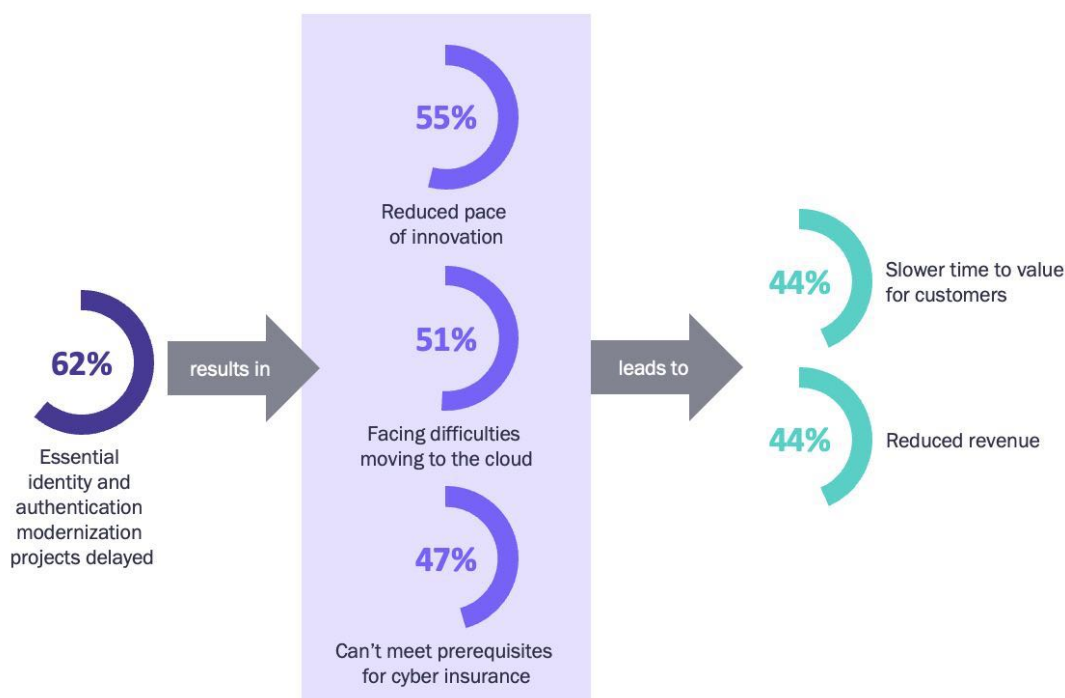
- Projects essential for modernizing identity and authentication have been postponed (“high” or “extreme” impact at 62% of organizations)**
 Without the right talent available, organizations have been unable to migrate off legacy identity systems to modern authentication approaches. Despite the widespread recommendation to move to modern authentication, organizations are stopped in their tracks by legacy technical debt.
- Lack of modernization slows down the pace of innovation (55%), hampers cloud migration (51%), and threatens cyber insurance coverage (47%)**
 Investments in addressing technical debt reduce budget for customer-facing innovation and being tied to legacy identity providers hampers modernization of applications to the cloud. Organizations unable to hire the talent required for modernization also struggle to meet elevated standards for cyber insurance coverage, pushing up premium prices and/or reducing the extent of coverage.
- Reduced innovation decreases value for customers (44%), so they go elsewhere, resulting in reduced revenue (44%)**
 Customers not seeing the innovation they care about in online services and identity controls sever ties with the organization, looking elsewhere for the capabilities and features that are important to them, e.g., modern authentication to safeguard their data, privacy, and digital identity. By implication, the organization’s revenue declines because they’ve failed to invest in competitive differentiation.

Modernizing identity and authentication is being delayed by difficulties in hiring for IAM roles, causing a cascade of internal and external problems.

Figure 11

You can't buy time. Impact of IAM hiring challenges

Percentage of respondents who say hiring challenges have had a “high” or “extreme” impact on modernization projects, internal constraints, and customers



Source: Osterman Research (2023)

Solutions and recommendations: Build your identity fabric through Identity Orchestration

The proliferation of identity-centric security over the past decade shows the connection of identity to security on the one hand and the unaddressed organizational challenges on the other. The common thread in solving many aspects of the identity challenge — identity and access management, identity security, identity governance and administration, and privileged access management — is actually the orchestration of services across an integrated fabric: **an identity fabric**. In this section, we look at what it takes to use Identity Orchestration to construct an identity fabric, addressing the previously discussed identity and access policy challenges and vulnerabilities.


Unified identity management: The promise of an identity fabric

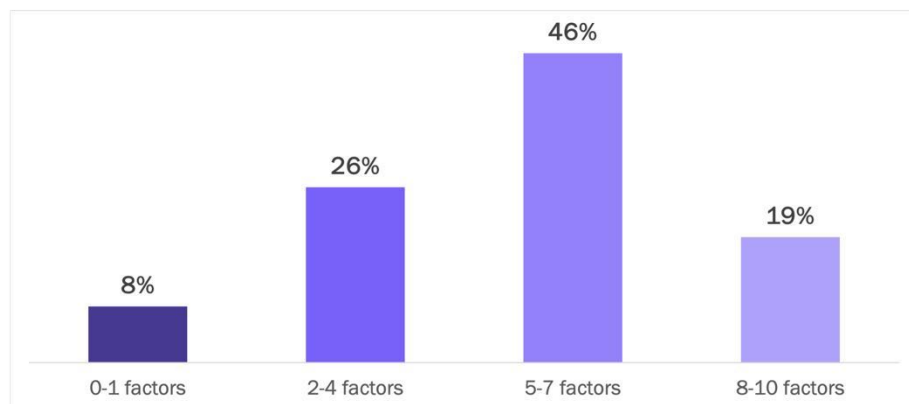
The unintended consequences of managing disparate identities are manifold for organizations. The complexity of legacy systems, market competition, identity vendor services proliferation, M&A activity, and the rapid shift to multi-cloud environments amplifies the challenge.

An identity fabric emerges as a concept that coalesces distributed identity services. This fabric is a unified approach to Identity and Access Management (IAM) that consolidates scattered IAM systems, tools, and processes into a single, cohesive, and flexible architecture. An identity fabric provides a common framework for managing and governing identity and access across various platforms, applications, and devices—on-premises, private, and public clouds.

In the survey, respondents rated the importance of ten factors in building an identity fabric. A significant two-thirds rated five or more factors as highly crucial. See Figure 12. The ten factors are listed in Figure 13.

Figure 12

 **The goods.** How many factors of an identity fabric resonate with identity leaders
Percentage of respondents indicating “important” or “extremely important”

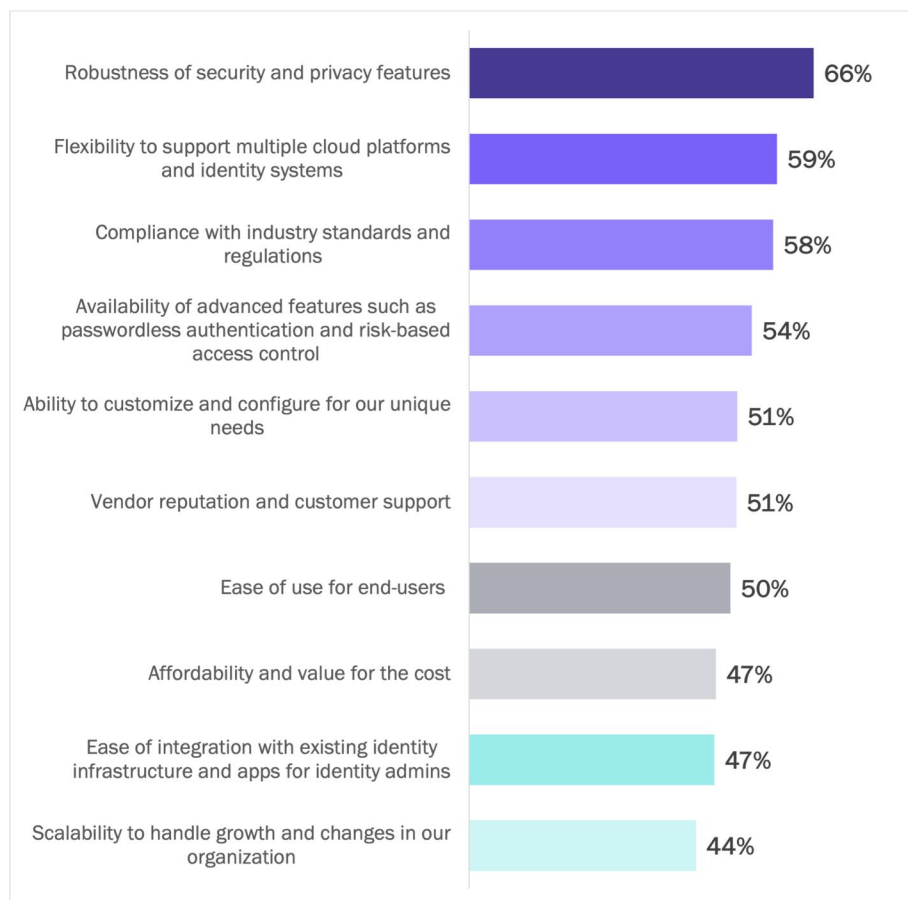


Source: Osterman Research (2023)

The thread that ties together various components of the identity challenge is actually a fabric – an identity fabric which is part of Identity Orchestration.

Figure 13

🤖 **In a perfect world: What organizations want from an identity fabric solution**
Percentage of respondents indicating “important” or “extremely important”



Source: Osterman Research (2023)

The multi-cloud identity requirements

An identity fabric's key value proposition is its ability to seamlessly integrate identity and access policies across multiple cloud platforms and identity systems. It ranks second amongst the most valued requirements by organizations. The first and third requirements bracketing this value are robust security and privacy, and compliance with industry standards and regulations — both non-negotiable prerequisites for any organization investing in an identity fabric. See Figure 13 above.

Beyond these core principles, organizations seek key features that modernize authentication capabilities and offer customization options, such as adding passwordless authentication and risk-based access controls. Followed closely by customization and configuration options to address the organization's unique needs.

The final group of requirements includes purchase-decision factors such as vendor reputation, ease of use for end-users, and affordability.

As long as security and compliance mandates are met, organizations want what identity fabric offers.

Constructing your identity fabric through Identity Orchestration: Benefits and possibilities

So, how can an identity fabric, created through Identity Orchestration, benefit your business goals and outcomes? An identity fabric enables the speedy addition of new identity services or the retirement of old ones, ensuring security and evolving authentication capabilities for on-premises applications with modern cloud identity providers.

The Identity Orchestration-enabled identity fabric empowers organizations to:

- **Work cohesively across multiple cloud platforms**
Organizations can pursue a multi-cloud strategy unencumbered by the identity and access policy shortcomings that have characterized most attempts to date. Access policies are fully visible and consistent, irrespective of cloud platform or app. The Identity Orchestration approach ensures consistent identities and access policies, reducing disruption during cloud IDP outages. It creates identity resilience by seamlessly transitioning to a backup IDP or on-premises identity store during a potentially catastrophic cloud outage.
- **Modernize on-premises applications with MFA and passwordless**
With an identity fabric in place via orchestration, on-premises applications can be updated to work with modern authentication methods like MFA, passwordless, and risk-based authentication. As "modern" evolves with new identity innovations, the identity fabric can extend any best-in-class tooling to all applications at scale. Forget needing to get app owner buy-in for long-timeline security deployments.
- **Innovate without needing scarce identity talent**
In the absence of an identity fabric, organizations have been caught in a proverbial Catch-22: to meet the business and security imperative of finding and hiring identity specialists. Without identity specialists, the Identity Orchestration solution provides a no-code identity modernization path. This approach empowers less specialized identity and security personnel to manage the process.
- **Retire legacy identity infrastructure without compromising business processes**
With Identity Orchestration and an identity fabric, organizations can retire outdated systems and redirect identity mechanisms to the new identity infrastructure without disrupting business processes.

By orchestrating your identity fabric, you can dynamically move applications across multiple cloud platforms and easily add new identity services.

Conclusion: Harnessing the power of Identity Orchestration in creating a robust identity fabric

Organizations navigating the identity challenges of a multi-cloud world should consider adopting Identity Orchestration and an identity fabric. By orchestrating disparate IAM systems, tools, and processes, Identity Orchestration creates an identity fabric that supports cloud innovation, improves security, and enhances the user experience.

The ideal solution will align with the organization's specific needs, such as integrating various identity providers, modernizing authentication methods, and retiring legacy on-premises identity infrastructures. Identity Orchestration enables an organization to bridge the talent gap, empowering identity professionals to manage distributed data, identities, and multiple identity services cohesively. Regular communication and collaboration between identity professionals and other organizational stakeholders is vital for effectively managing current and future identity tools, services, and providers.

An identity fabric unifies disconnected and disjointed IAM systems, tools, and processes—enabling organizations to address the challenges of identity in a multi-cloud world.

Methodology

This report was commissioned by Strata Identity. Osterman Research surveyed 308 IT leaders and decision-makers in North America during April 2023 on their challenges and priorities for identity management in multi-cloud environments this year. Respondents had to work at organizations with annual revenue of US\$100 million or more.

This report is the third annual State of Multi-Cloud Identity Report. For last year's report, see the [Strata website](#).

Demographics of survey respondents

Industry

Business or professional services	16%
Technology and/or technology services	14%
Financial services and/or insurance	12%
Healthcare	9%
Manufacturing and materials	7%
Energy, utilities, and/or waste management	5%
Construction	5%
Retail	4%
Consumer product goods and/or manufacturing	4%
Consumer services	4%
Transportation and logistics	3%
Chemicals and/or metals	3%
Professional services	3%
Media and/or leisure	3%
Telecommunications services	2%
Travel and hospitality	2%
Agriculture, food, and/or beverage	2%
Government	2%
Advertising and/or marketing	1.0%
Electronics	0.6%
General trading	0.6%
Legal services	0.3%

Respondent level

C-level	12%
Vice president	17%
Director	36%
Manager	26%
Full-time practitioner	9%

Company size

\$100 million to \$499 million	51%
\$500 million to \$999 million	33%
\$1 billion plus	17%

Geography

United States	83.8%
Canada	16.2%

About Strata Identity

Strata Identity is the leader in Identity Orchestration for hybrid and multi-cloud environments. The orchestration recipe-powered Mavericks platform enables organizations to integrate and control incompatible identity systems without changing the user access experience. By decoupling applications from identity, Mavericks makes it possible to implement modern authentication, like passwordless, and enforce consistent access policies without refactoring source code. The company's founders created the IDQL (Identity Query Language) standard and Hexa open-source software for multi-cloud policy orchestration and are co-authors of the SAML standard for SSO federation.

For more information, visit us on the [Web](#) and follow us on [LinkedIn](#) and [Twitter](#).



www.strata.io

[@StrataIdentity](#)

sales@strata.io

+1 888 552 4930

© 2023 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

¹ Melanie Maynes, One simple action you can take to prevent 99.9 percent of attacks on your accounts, Microsoft Security Blog, August 2019, at <https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>