ForgeRock

WHITEPAPER

Cloud Without Compromise: IAM for the Hybrid Enterprise

A Companion Guide to Forrester's "IAM for the Hybrid Enterprise" Opportunity Snapshot

Digital transformation, competitive advantage, and cost savings are factors that drive many organizations to the cloud. But for a comprehensive strategy, they also need to continue supporting business-critical applications running on premises, resulting in hybrid IT environments. ForgeRock and Google Cloud commissioned a study through Forrester Consulting to understand how identity and access management (IAM) decision makers in large organizations are handling this hybrid reality and how it impacts their IAM initiatives. Here are some of the key findings from the survey:

- Over 80% of respondents have already adopted or plan to adopt or expand their cloud-based IAM initiatives in the next two years.
- Nearly all (98%) of respondents have experienced challenges with IAM sourced from the cloud.
- Leveraging a hybrid IAM approach delivers better employee experience, customer experience, and opportunities for innovation.

This white paper reflects on the findings from the *Forrester's Opportunity Snapshot on IAM for the Hybrid Enterprise*[1] and details why ForgeRock Identity Cloud is the only IAM software as a service (SaaS) on the market today that fully supports hybrid environments that span public, private, and multi-cloud environments and supports SaaS, home-grown, and on-premises applications. Using ForgeRock, enterprises can introduce modern, identity-driven security and delightful user access journeys into their environments and address the broadest range of IAM use cases while reducing operational costs and achieving faster time to value.

Introduction

ForgeRock and Google Cloud commissioned a study by Forrester Consulting of more than 300 global IT leaders involved in IAM decisions and cloud migration efforts. The goal was to understand their current priorities and challenges for IAM adoption in the cloud. The study revealed that organizations are focused on delivering IT and security benefits by improving customer and employee experiences. The study also found that, despite a high level of interest in cloud adoption, the majority of organizations have hybrid IT environments and face serious challenges with IAM in the cloud today. To get ahead of these challenges, IAM decision makers need to prioritize a cloud IAM strategy with a hybrid approach.

Priorities for Cloud-Based IAM Adoption

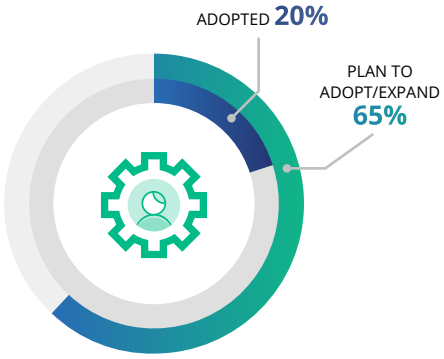
A well-implemented cloud-based IAM platform can help organizations reduce costs and improve security and business processes. Poorly implemented IAM results in lower employee productivity, wasted company resources, loss of customer satisfaction, and increased risk of loss of sales, brand loyalty, and customers.[2] IT leaders recognize this impact and plan to adopt or expand capabilities to modernize and improve user experiences by adopting commercial IAM solutions to manage employee and consumer identities in the cloud.

To provide secure and frictionless user experiences, over 80% of IT leaders are planning to adopt and expand capabilities that will give them better business insight and competitive advantage. Below are the reasons enterprises are adopting cloud IAM and our recommendations for what to look for in a platform:

Centralizing identity and gaining insights with analytics

Eliminating identity silos and centralizing identity capabilities save money by reducing the volume of identity infrastructure that has to be maintained. It is also the key first step to understanding current user access patterns.

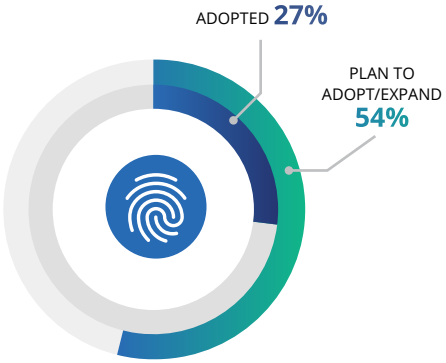
Recommendation
Choose a solution that can apply advanced artificial intelligence and analyze user access patterns. The insights gained can help enterprises understand their current security posture and blind spots, so they can take appropriate remedial actions.



Building user profiles with behavioral biometrics

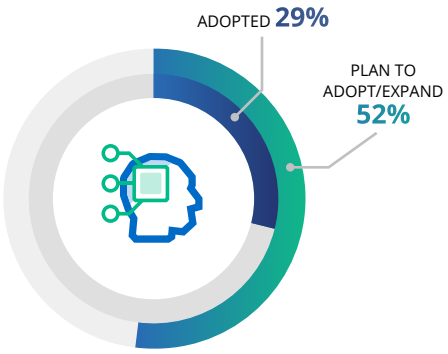
Understanding “normal behavior” is important for establishing a baseline and detecting fraud. This baseline can then be leveraged with the identity, application, and device context to determine abnormal behavior.

Recommendation
Choose a platform that incorporates behavioral signals, such as unique keystroke patterns, mouse movements, and even device telemetry, to determine the validity of the users accessing their systems. Combining these signals with user profile information and device context will enable an IAM platform to intelligently adjust access journeys to introduce the right level of friction.



Managing IoT and non-human identities

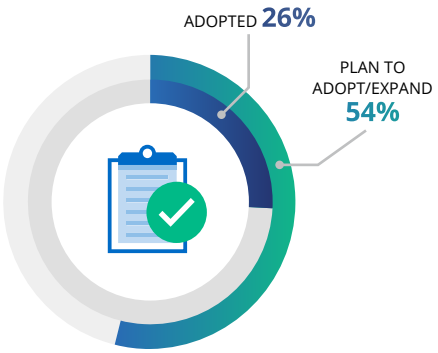
The increasing use of IoT devices is reshaping almost every industry. Combined with the growing identity needs of application programming interfaces (APIs), services, and bots in the cloud, these non-human identities are generating and accessing more information than ever.



Recommendation
Choose an IAM platform that can treat IoT devices as first-class citizens and connect them with people, systems, and data securely to enhance user experience and drive more revenue through IoT-enabled services. Extending the same platform to secure APIs, microservices, and streaming data reduces the number of point solutions that have to be supported, simplifying the architecture and reducing the costs.

Addressing growing regulatory pressures

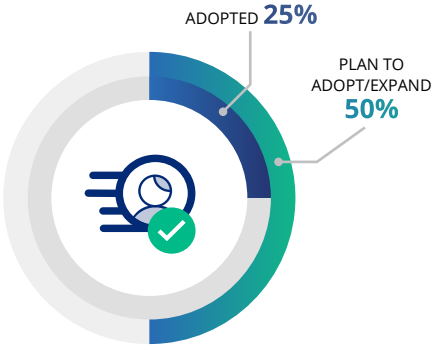
The number of industry-specific, regional, and global regulations that an organization has to satisfy is constantly growing. Addressing these regulatory challenges is an expensive proposition for any organization.



Recommendation
Choose a complete IAM platform that provides privacy and consent management options to end users so they have finer control over what data is being shared and with whom. This is a legislative requirement that also improves users' trust. Combine that with advanced artificial intelligence (AI)-based analytics to prevent entitlement creep through automated risk visibility, access review, and remediation to help achieve regulatory compliance.

Reducing friction and enabling passwordless authentication

While application owners always want to reduce user friction, security and compliance teams always want tighter security and restrictions on access. Balancing these two seemingly opposite choices always fell on the shoulders of the IAM teams.



Recommendation
Delight users *and* elevate security by providing next-generation capabilities, such as mobile biometrics and passwordless and usernameless authentication to reduce access friction and help desk costs. Eliminating passwords also reduces the likelihood of data breaches caused by phishing, password replay attacks, and username and password theft. This also improves the overall security posture of the organization.

Whether an organization is beginning this journey or is well underway to evaluating and leveraging a cloud-based IAM solution, there are three critical factors that should be considered.

- Cloud considerations and options
- The limitations of legacy IAM solutions
- The shortcomings of many SaaS solutions

Hybrid Cloud on the Rise: What to Look Out For

While cloud adoption is the priority for many organizations, the study found that the approaches they are taking to move to cloud are highly mixed. For example, while the current usage of private cloud is high, more than half of the study respondents also plan to adopt hybrid cloud and multi-cloud within the next two years.

As cloud adoption grows, hybrid enterprises continue their evolution from on-premises IT to include a mix of both private and public clouds – also known as hybrid cloud.[1]

As enterprises have evolved to a hybrid IT model over time, they are choosing the best architecture for their applications and the easiest path to delivering them to customers. TAs a result, these applications will have a variety of architectures, identity stores, and access controls. The lack of standardization results in multiple problems:

- Identity silos that support different standards and identity lifecycle management capabilities
- Access standards that differ across types of users, applications, application programming interfaces (APIs), microservices, and IoT
- Lack of governance controls to understand and mitigate high-privilege, high-risk access

As ecosystems and cloud adoption expand, security professionals are increasingly aware of siloed data environments and the blind spots of their cloud and IAM strategies.[1]

Limitations of Legacy IAM Solutions

Legacy solutions were built for an on-premises architecture and never supported capabilities and requirements for modern cloud environments. The technical debt accumulated over many years of neglect has resulted in solutions that are unscalable, unstable, and unreliable. Problems with legacy IAM solutions identified in the study include:

88% of respondents report issues with stability, scalability, or missing capabilities

66% have process issues around flexibility and adaptability to meet new business needs

50% face cost challenges related to finding the right experts to configure and manage legacy IAM solutions

Legacy IAM is also heavily customized and integrated into the current infrastructure. Unwinding those customizations can become an expensive proposition. Organizations that are still running legacy technology have to modernize to address these challenges. A modern IAM platform that supports easy coexistence with legacy infrastructure and accelerates migration to the cloud can solve the problems with legacy IAM.

Firms must embrace legacy infrastructure as part of their reality. Adopting a hybrid approach can bridge that gap.

Shortcomings of Many SaaS Solutions

Many early cloud-only IAM solutions focused primarily on simplicity at the expense of functionality and configurability. This narrow focus allowed them to quickly gain market share within a narrow band of organizations that had those simple needs. However, nearly all (98%) of the early adopters of cloud-only IAM solutions cited challenges that include:

- The failure to integrate with existing business processes
- The inability to manage identities across current applications and systems
- Lack of visibility into on-premises systems, and an incomplete security picture

Today's large enterprises are demanding more capabilities – including enterprise-grade security and configurability – than these simple cloud-only IAM solutions can deliver.

Bridge Hybrid IT With a True Hybrid IAM Platform

These issues can only be addressed by an IAM platform that understands this hybrid reality well and solves for all use cases. Purpose-built with hybrid IT and hybrid cloud in mind, hybrid IAM eliminates identity silos across mixed environments, which is critical for security and positive user experiences.

> The most consistent hurdle respondents face is the inability to map or integrate to existing processes or legacy solutions.

Just as hybrid IT bridges the gap between the support of business critical applications running on-premises and the new capabilities offered by cloud, hybrid IAM unifies and secures all digital identities within the hybrid IT environment.

Forrester defines hybrid IAM as an IAM platform capable of running, unifying, and securing all digital identities in a hybrid IT environment.[1]

The study found that over 70% of the respondents expect benefits from investments to secure IAM in hybrid cloud. A majority of them agreed that leveraging a hybrid IAM approach would enable them to focus on improved user experiences and security.

Benefits of Hybrid IAM

85%

Improved Customer Experience[1]

Delivering great customer experiences and protecting customers allows organizations to acquire customers faster, accelerates conversion rates, and increases retention rates.

84%

IT and Security Benefits[1]

Accelerating legacy modernization and protecting your organization mitigates risks, reduces costs, and enables greater confidence in achieving regulatory compliance.

78%

Improved Employee Experience[1]

Reducing IAM complexity and improving access automation reduces access proliferation, empowers an efficient workforce and increases opportunities for innovation.

ForgeRock Identity Cloud: The Logical Choice for Hybrid IAM

ForgeRock offers the only comprehensive IAM SaaS platform capable of being implemented within any environment with common outcomes, regardless of consumption or implementation choice. It can easily secure any hybrid IT environment spanning millions of identities in just minutes.

A scalable platform for any identity type: consumers, workforce, and things

Within a hybrid IT environment, everyone and everything has a digital identity. Adding microservices and APIs to the mix, these identities can quickly grow from a few thousand to millions for any organization. As the number of people, devices, services, and things continues to grow exponentially, it is critical to manage their complete identity lifecycle and ensure that the right access is granted only to the right person, device, or thing. This requires a scalable digital identity platform designed to support any identity type with exceptional experiences.

Some cloud IAM providers throttle traffic rates across the board to ensure stability of their offering, and prevent one noisy customer's performance from impacting multiple customers.

ForgeRock's patented tenant isolation in a multi-tenant cloud architecture allows each customer to maximize performance without impacting or being impacted by others. ForgeRock is the only IAM platform on the market that is purpose-built for consumers, workforce, and things and is designed to connect everyone and deliver digital experiences at scale.

Cloud without compromise on capabilities

Business processes and identity integrations vary widely across homegrown, on-premises, cloud, and SaaS applications. Each supports different standards and protocols, which introduces complexity for any solution that does not support them or does not offer flexibility and extensibility to adapt to business needs. The majority of the survey respondents identified these missing capabilities as an important concern.

Some IAM solutions simplify the offering by removing the extensibility needed by many large organizations. This results in a solution that cannot integrate seamlessly with legacy and modern applications or adapt to the business processes of large organizations. Organizations, therefore, have to implement multiple disjointed IAM solutions that result in poor user experiences.

ForgeRock Identity Cloud offers cloud IAM without compromise. With one subscription, organizations get complete freedom to fulfill all their hybrid needs. ForgeRock is the only IAM vendor that offers the same common outcomes across all platform consumption and implementation choices: on premises, any cloud, or as a service. Organizations get the same level of flexibility to address their business processes when implementing ForgeRock platform as a self-managed offering in a cloud of their choice, and when consuming ForgeRock Identity cloud as a service.

Exceptional user experiences while delivering on Zero Trust strategy

Maintaining a competitive advantage and supporting new business initiatives when data breaches and advanced threats are at an all-time high requires a new approach to balancing security and the user experience. Traditionally, organizations either lean heavily towards usability – potentially resulting in more fraud – or lean heavily towards security, resulting in increased user friction and bad user experiences. It shouldn't come down to a choice between one or the other.

Security, fraud, and identity professionals can simultaneously elevate security and usability by leveraging modern capabilities like mobile biometrics and passwordless and adaptive authentication in combination with continuous and fine-grained authorization. Adding identity governance to ensure that there are no excessive entitlements and automating risk visibility, access review and remediation will ensure regulatory compliance and add a defense-in-depth strategy for security. This is called the Continuous Adaptive Risk and Trust Assessment (CARTA) or Zero Trust model.

ForgeRock enables a Zero Trust strategy and improves an organization's security posture by designing purpose-built user journeys with ForgeRock Intelligent Access. Authentication journeys can include user and device context so every transaction across an enterprise can be continuously authorized with no visible impact to the end user. Additionally, organizations can centralize identities to improve audits and compliance with full user lifecycle management. Balancing security with capabilities like passwordless and adaptive authentication results in lower friction for users, improving their overall access experiences.

> Many legacy IAM solutions have no useful cloud offering, and many cloud IAM solutions do not offer the flexibility to be deployed on premises. Organizations have had to choose their deployment option at the start of their IAM journey **and remain saddled with that choice forever**.

Peaceful coexistence with on-premises applications

One of the defining elements of a hybrid IT architecture for many organizations is the presence of a large number of business critical applications that are still running on premises. As organizations evolve to keep pace with cloud requirements, the prospect of modernizing and the potentially disruptive migration to a new solution can be daunting.

Some IAM vendors provide simple solutions for only part of the problem – covering either cloud or on-premises integrations, without offering the mix of both that the customer actually needs. Failure to address the complete picture will only result in a broken architecture that will eventually need to be ripped and replaced. There is no need to go through the pain, risk, and expense of regularly ripping out legacy identity solutions to gain competitive advantage.

ForgeRock has a better way. With a single subscription, ForgeRock delivers complete freedom to support any hybrid identity needs. ForgeRock includes a completely flexible and configurable cloud service along with powerful downloadable components that can be deployed on premises to integrate all applications.

Maximum deployment flexibility and ability to transition to cloud

Depending on where an organization is in their hybrid journey, they may have more on-premises or more cloud needs. Organizations may want to start with an IAM SaaS, having some components on premises to integrate legacy applications. Or, they may choose to deploy primarily as a self-managed service while also consuming parts of the SaaS. As they're modernization journey progresses, organization will eventually be ready to migrate most, if not all, to cloud.

Many legacy IAM solutions have no useful cloud offering, and many cloud IAM solutions do not offer the flexibility to be deployed on premises. Organizations have had to choose their deployment option at the start of their IAM journey and remain saddled with that choice forever.

ForgeRock is the only IAM vendor offering complete deployment flexibility as a service, from any cloud, or even on premises. This choice of deployment options allows organizations to define their own hybrid IAM strategy and consume the cloud platform with as much or as little of the platform running on premises as needed. This flexibility and the ability to transition from cloud to on premises (or vice versa) enables organizations the deployment choice that is right for them without being locked into a solution that no longer meets their needs.

Predictable pricing with overage protection

Cost reduction is a key consideration when adopting the cloud. All cloud solutions deliver a consumption-based pricing model to allow organizations to only pay for the services they consume.

However, many cloud IAM vendors charge exorbitant overage fees that penalize even the smallest incremental growth over initial estimates. On the other hand, many legacy vendors keep increasing the costs of support and maintenance and create a cycle of "legalized ransomware," effectively holding an organization hostage to their solution.

ForgeRock is the only IAM service that offers predictable pricing with a simple user-based subscription. ForgeRock does not charge for overages up to 10%, resulting in a five to 10 times reduction in IAM spend compared to other cloud vendors. Organizations can predictably project their IAM costs and use ForgeRock as a key part of their strategy to reduce capital expenses and deliver value to the business.

Summary

Managing IT and IAM infrastructures both on premises and in the cloud results in complexities that lead to migration and integration issues. The result is compromised security, poor user experiences, inefficiency, and lack of innovation.

Hybrid IAM enables organizations to seamlessly integrate, centralize, and manage identities and data across any environment. Capable of being implemented within on premises, any cloud, and as a service infrastructures, ForgeRock offers the only comprehensive hybrid IAM platform.

To learn more about how you can use ForgeRock as a single platform for all your identity and access needs across your hybrid IT environment, visit: www.forgerock.com/platform/identity-cloud

[1]Forrester, "IAM for the Hybrid Enterprise: Current challenges and strategies for global security professionals," https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam

[2]Forrester Research, "Evolve your IAM strategy For Your Digital Business," December 4, 2020