ForgeRock

WHITEPAPER

Six Trends Driving the Future of Cloud

A Guide for Identity and Access Management Professionals

Executive Summary

The data shows that organizations are moving to the cloud in record numbers, with an estimated 45% of IT spending shifting to cloud by 2024.[1] But there's a deeper concern that is beginning to emerge – some cloud implementations are less than successful. In fact, 80% of CIOs admit they have not attained the desired business agility with migration to the cloud.[2]

This paper highlights the top six trends identity professionals should consider when planning their cloud strategy. For exponential growth, you need to not only stay in front of the trends, but find ways that enable you to fully implement them to achieve positive outcomes.

[1]https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/
[2]https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/unlocking-business-acceleration-in-a-hybrid-cloud-world

Six Trends Driving the Future of Cloud

A Guide for Identity and Access Management Professionals

Introduction

Cloud adoption is unstoppable. Tasked with delivering new digital initiatives ahead of competition, business and IT leaders are under pressure to take advantage of the speed, flexibility, and cost savings the cloud promises. Gartner estimates that "Seventy percent of enterprise workloads will be in the cloud by 2024, yet three out of four organizations do not have a fit-for-purpose cloud strategy." In order to succeed with your cloud implementation, you need to address the top trends driving the future of cloud.

> By 2024, more than 45% of IT spending will shift from traditional solutions to the cloud.
>
> Gartner®

Six Cloud Trends

1. Innovation and Cost Savings

Your business is moving to the cloud to save money, with a move from capital expense to operational expense. At the same time, the broad innovations occurring in the cloud are disrupting traditional ways of managing IT, which requires adaptation and change in process.

2. Multi-Cloud Strategy

You need to reduce your dependence on a single cloud vendor, while maintaining flexibility and control.

3. Hybrid Cloud

A practical cloud migration strategy requires that your business-critical applications running on premises are supported while you move to the cloud, leading to a hybrid cloud environment.

4. Cloud-Native Architectures

You can increase agility and further reduce costs by taking advantage of microservices architectures and cloud-native architecture functions.

5. Security and Privacy

You need a secure cloud, with full tenant isolation, to ensure optimal performance, reduce the risk of inadvertent or malicious snooping, and ensure regulatory compliance.

6. Identity Is the Only Security Perimeter

Increased online shopping and working from home introduces a higher level of risk, and calls for security defenses beyond the network perimeter. Protecting business-critical applications can only be done through a security strategy based on identity.

How the Six Key Cloud Trends Affect IAM

The move to the cloud places identity and access management (IAM) professionals in the middle of disruptive change that is transforming both their responsibilities and their workflows. The six recent trends related to cloud that have emerged cross industry and national boundaries. All these trends impact the way IAM professionals look at their work today and in the future.

TREND ONE

Innovation and Cost Savings

The primary drivers for cloud adoption are speed, ease of innovation, and reducing IT costs. Your development team can deploy new offerings quickly. Your portfolio of applications, products, and services can be expanded, and new features can be introduced to improve functionality and ease of use in a cloud environment. With no requirement to set up your own IT infrastructure or run, manage, or maintain your own servers, your organization reduces both capital and operating expenses.

However, on average, organizations don't prioritize 30% of their cloud spend appropriately,[3] and need to find new and better ways to optimize their cloud solutions.

Your enterprise IAM requirements exceed the capabilities provided by many cloud offerings – especially those that focus on limited use cases with unpredictable costs. A modern identity solution is the backbone to executing secure, simple, and innovative solutions in a complex environment. The ideal IAM solution has extensible integration with systems and support for application programming interfaces (APIs), microservices, and Internet of Things devices. A modern IAM solution delivers advanced capabilities to support innovation; no-code and low-code orchestration for onboarding; self-service, passwordless authentication; and advanced authorization policies. To reduce costs, look for an identity solution that offers simple and flexible subscriptions with predictable pricing.

Leveraging a modern identity and access management platform to support multi-cloud initiatives can save as much as 25% on implementation costs and increase ROI by 50%.

"I wanted a flexible solution that would serve our global B2B2C market. Great customer experience is at the core of our business. To provide that, we have to understand a lot of details about the user, their identity, and the context in which they are reaching out."

Daryl Robbins
Senior Director of Global Architecture, Calabrio

TREND TWO

Multi-Cloud Strategy

Nearly 81% of organizations currently use or plan to use multiple cloud vendors in the next 12 months, up 12% prior to the global pandemic.[4] In the early days of moving to the cloud, your organization may have chosen a single cloud provider. However, like most large organizations, you need to adopt a multi-cloud strategy to overcome provider-specific limitations, vendor lock-in, and improve organizational control and flexibility over data and costs. Whether leveraging a combination of popular cloud service providers such as Microsoft Azure, Amazon Web Services (AWS), or Google Cloud Platform, the option to choose the right platform for each of your specific applications and requirements enables you to make use of each platform's unique capabilities.

When identities reside in silos, and each cloud vendor offers IAM capabilities limited to their own ecosystems, the promised agility of multi-cloud is limited. A comprehensive, integrated IAM platform capable of uniting, integrating, and securing hybrid environments can bridge the on-premises and cloud divide and enable seamless operations.

[3]https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/
[4]https://www.zdnet.com/article/research-multicloud-deployment-increases-among-enterprises/

TREND THREE

Hybrid Cloud

While a multi-cloud strategy leverages multiple cloud providers, a hybrid cloud IT architecture consists of applications, services, and systems located in private and public clouds, including on-premises environments. Hybrid cloud addresses the need to keep some data and applications on premises and under tight control while moving others to the cloud. Data sovereignty requirements may also play a role if the organization needs to ensure that specific data only resides in specific geographical regions.

A recent Forrester report showed that almost a quarter of global IT decision-makers surveyed have already adopted hybrid cloud, and 52% plan to adopt or expand their use of hybrid cloud within the next two years.[5]

An IAM solution that supports both on-premises and cloud applications and can coexist with and augment legacy and home-grown applications is critical to secure a hybrid cloud environment. You need to ensure that they can rely on an IAM service that can run, unify, and secure all digital identities in a hybrid IT environment.

> "The future isn't just cloud, it's hybrid cloud. This approach gives companies the ability to reimagine their business and modernize faster, and IAM needs to be at the center to ensure the future is both frictionless and secure."
>
> **Hamidou Dia**
> **Vice President,**
> **Global Head of Solutions Engineering,**
> **Google Cloud at Google**

TREND FOUR

Cloud-Native Architectures

You can increase agility, accelerate time-to-market, and further reduce costs by taking advantage of cloud-native capabilities like containers, dynamic orchestration, microservices, and serverless architectures. Gartner predicts that, by 2023, 70% of global organizations will be running more than two containerized applications in production – up from less than 20% in 2019. And IDC predicts that 95% of new microservices will be deployed in containers by 2021.[6]

Containers enable you to bundle an application with all of the components it needs – libraries, code, and other dependences – and deploy it as one package. You can focus on writing code without worrying about the system it will be running on, resulting in faster deployments, better security, and improved scalability.

Microservices provide a highly scalable, flexible approach to creating cloud applications because they allow an application to be broken down into individual services. Microservices make it easy for your developers to change, replace, or scale applications, with shorter testing cycles and easier collaboration so your organization can quickly react to changing demands.

Microservices and the increased use of APIs means you need to manage security and identity needs in a way that is similar to how you manage the identity needs of your users. You need a single IAM platform that can leverage the cloud native architecture to scale and run in the cloud of your choice in order to secure those APIs and microservices, along with user identities.

IAM platforms also need to be cloud-native and leverage some of these capabilities, such as containerized dynamic architecture running on Kubernetes clusters and serverless implementations to scale and support these cloud-native architectures.

[5]https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam
[6]https://www.entrepreneur.com/article/345826

Securing a cloud environment means ensuring that your organization's data is never commingled with that of other organizations. An IAM solution with full tenant isolation ensures that identities from one environment are not valid in another, making sure that any accidental or malicious access of another customer environment does not impact yours.

TREND FIVE

Regulatory compliance eats an ever-increasing share of the budget

Securing the cloud continues to be a top priority. Gartner projects cloud security spending will rise over the next year from $595 million to $841 million, an increase of 41.2%.[7] Yet many organizations also cite security challenges as a top barrier[8] for cloud adoption. When moving to the cloud, you might have assumed that your information will be secured with redundant, diversified servers managed by a third party. But just encrypting the data at rest and in transit is not enough. You need to dig a little deeper to fully understand where and how your information is being stored and how that impacts your applications as that data is retrieved.

In a multi-tenant cloud environment, you need to make sure that other tenants don't affect the performance of your business-critical functions. This issue – sometimes called the "noisy neighbor" problem – arises when a tenant monopolizes available resources, causing network performance issues for others who share the infrastructure.

[7]https://www.techrepublic.com/article/cybersecurity-spending-to-hit-150-billion-this-year/
[8]https://cloudsecurityalliance.org/press-releases/2021/03/30/cloud-security-alliance-releases-latest-survey-report-on-state-of-cloud-security-concerns-challenges-and-incidents/
[9]https://www.forrester.com/report/The+Top+Trends+Shaping+Identity+And+Access+Management+In+2021/RES166097

TREND SIX

Identity Is the Only Security Perimeter

Employees, partners, contractors, and customers all need varying levels of access to the applications running on premises and in the cloud. The shifting enterprise edge, coupled with a massive number of users, devices, and applications, create many potential points of failure. There is no longer a defined network that can be secured at the perimeter. Your network starts with users trying to access an application, whether they are working from home, at an office, or in a coffee shop. Today's world requires Zero Trust security based on user identity – and the result is that identity has become the only perimeter. A well-implemented IAM platform ensures business-critical data is protected while in the cloud and when moving laterally from one cloud service to another.

Many organizations are embracing this trend and are aware that robust security starts with leveraging native security features of the service provider – but that's just the beginning. You need to go beyond that to prevent unauthorized access and data breaches with identity-rich authentication and authorization policies. The principle of least-privilege access – ensuring that users, applications, and devices can access only the information and resources absolutely necessary for their legitimate purposes – is key to securing the new perimeter. This drives the need for comprehensive and rigorous IAM that can unify and manage identities across on-premises and cloud environments, for all users, and at all times.

"Identity-rich policies allow for much more granular and timely network access control to reduce the overall threat surface. Additionally, Zero Trust Edge (ZTE) provides much greater levels of visibility into human and machine/workload identities accessing any hybrid cloud or on-premises resources."

The Top Trends Shaping Identity and Access Management in 2021, Forrester[9]

ForgeRock Identity Cloud: Harnessing Trends to Build Trust and Deliver Great Experiences

ForgeRock Identity Cloud is a comprehensive identity and access management platform delivered as a service. Identity Cloud helps your organization:

1. Deliver superior experiences, mitigate risk, and reduce costs with a comprehensive identity platform.
2. Gain cutting-edge identity capabilities without worrying about maintenance, patching, and upgrading.
3. Increase productivity by leveraging a single platform for all identity and access needs: users, devices, things, APIs, services, and more.
4. Support business-critical applications running on premises and in the cloud for a secure hybrid enterprise.
5. Leverage a patented security architecture with data isolation that gives you total control.
6. Quickly innovate and grow the business now and into the future without costly overage charges.

With Identity Cloud, you can effectively address the six cloud trends needed to support your cloud strategy. The result: superior user experiences, uncompromised security, and reduced costs.

Summary

The six cloud trends demonstrate the dramatic, fast-paced impact of the cloud on your organization and the need for a more dynamic, secure, and efficient way to handle identities. Identity Cloud embraces IAM for the hybrid enterprise – which enables your organization to run, unify, and secure all digital identities with a single platform in a hybrid IT environment.

Next Steps

Start planning for your organization's future in the cloud and gain a competitive advantage through quick adoption of hybrid IAM. Download the ForgeRock Identity Cloud Checklist, a comprehensive list of the top ten considerations and best practices for your identity cloud strategy.