RSA®

RSA.com

FINANCIAL
Services Need Cloud IAM

When security, usability, and flexibility are key

EBOOK | October 2022

The Case for Identity and Access Management in the Cloud

What are you waiting for?

Back in 2015, the Cloud Security Alliance released a report that showed the rate of cloud adoption in financial services organizations maxing out at about 41%.[1] Fast-forward just five years, and a follow-up report put it at 91%.[2] But wide adoption by nearly all doesn't necessarily mean all-in. A 2022 McKinsey survey revealed that only 13 percent of finserv organizations had half or more of their IT footprint in the cloud.[3] Everyone's using it, just not for everything.

How is your organization prioritizing IT workloads for cloud? More specifically, how does identity and access management (IAM) rank?

There's a compelling case to be made for prioritizing enterprise-wide cloud IAM as finserv organizations move broader IT operations to the cloud. Identity security is, after all, the aspect of IT security that touches every part of the organization. It's what makes it possible to grant authorized users access to all the resources and processes they need to do their jobs. It's also the other side of the coin: the means by which to protect against unauthorized users gaining access and using it to compromise private data, steal intellectual property, and commit other digital crimes.

Because identity is so pervasive, its impact is outsized. The infrastructure required to deploy identity is not insignificant, nor are the resources needed to maintain that infrastructure. Moving IAM to the cloud means moving from a CapEx to an OpEx model for operations, which means organizations are no longer investing resources in upgrades, patches, and other ongoing system requirements. Instead, they're free to shift focus to the business processes and other areas that identity supports, rather than focusing on the infrastructure itself.

So if you don't have IAM in the cloud yet, what's stopping you?

91%

of financial services organizations are using cloud services or planning to within 6-9 months.[2]

13%

of financial services organizations currently have half or more of their IT footprint in the cloud.[3]

Not Ready to Leave On-Premises IAM Behind?

Go at your own pace with a hybrid approach

We get it. You have one or more good reasons to wait to reap the benefits of cloud IAM. Maybe you want to avoid the potential disruption to your enterprise users. Or you have security-sensitive workloads that need to stay on-premises, at least for now, but you still want to enjoy the operational efficiency and other benefits of the cloud.

A hybrid approach to adopting cloud IAM can provide the flexibility you need.

By "hybrid," we don't just mean having two or more cloud deployments. That's the old "either/or" definition of hybrid that too many vendors provide.

Rather, we're talking about a true hybrid approach that includes on-premises *and* cloud capabilities, so you can move to the cloud at your own pace. For example, you might elect to migrate certain aspects of your IAM infrastructure now, but at the same time maintain some on-premises operations if you need to, for as long as you need to. That's far less jarring than an abrupt and complete move to everything-in-the-cloud (although if you find you're ready for that, more power to you). The point is that you should be able to make decisions based on your unique situation and strategies, and you should have a vendor that can pave a smooth path to whatever scenario will work best.

And think what you'll be gaining. A 2022 Bain & Company survey shows IT executives hope to achieve greater flexibility and scalability by implementing a cloud strategy—qualities that are essential to realizing greater operational efficiency, improved security, and other goals.[4] For example, the *New York Times* recently reported on a finserv organization being able to track fraud on a much larger scale because of machine learning capabilities in the cloud.[5]

Look for a cloud IAM vendor that will enable you to answer "yes" to the following key questions (even if—*especially* if—you're not necessarily moving all the way to cloud all at once):

- Can we integrate IAM across multiple systems?
- Do we have both cloud-based and on-premises security solutions?
- Are we partnered with an IAM vendor who can help with a seamless adoption?
- Can we gain visibility and control over who has access to what—whether on-premises or in the cloud?
- Can we scale responsibly and budget accordingly?

Concerned About Reliability and Availability?

Consider the resilience of true hybrid IAM

When a finserv organization considers moving a function as fundamental as IAM to the cloud, "always on" resilience is a critical consideration. The markets aren't going to call a timeout just because your team can't log in; customers won't overlook an outage that prevents them from connecting with account services. If there's a cloud outage or a network interruption, you need an identity platform that delivers high availability to support uninterrupted user authentication and access—always.

One of the unique advantages of a hybrid on-premises and cloud deployment is the potential for the cloud component to failover to on-premises IAM, providing an extra measure of resilience for your cloud-based IAM.

Cloud IAM that's designed to failover to on-premises IAM ensures that no matter what happens, secure authentication is always available.

Make no mistake: we don't mean that if there's a connectivity issue, users will simply be allowed in without authenticating via MFA. That can lead to threat actors exploiting the absence of MFA to gain access (see sidebar). But failover to on-premises IAM makes it possible to enforce MFA even when the MFA backend in the cloud can't be reached, so MFA will still work for all users even if they can't connect to the internet.

High availability is just one aspect of resilience; it should be part of a cloud IAM deployment that's designed for resilience in every way: capable of handling a variety of types of access requests, accommodating a diverse universe of user types, and navigating complex IT estates. Those are all hallmarks of reliable, robust IAM—whether it's in the cloud or on-premises.

Resilience & Security: A Cautionary Tale

In 2022, the FBI and CISA issued an alert warning of state-sponsored cyber actors gaining network access by exploiting a "fail open" policy that allowed users to login without MFA if they were unable to connect to the internet.[6] To deactivate MFA, all the threat actors had to do was turn off the internet connection. It's a great illustration of what makes on-premises/offline failover more secure: instead of defaulting to no MFA at all, it goes to on-premises MFA.

Where Does Governance Fit in Cloud IAM?

Authentication is the first step—but it's not the last.

A lot of conversations about IAM in the cloud focus on authentication. Will authenticating be as secure in the cloud as it is on-premises? Will the user experience change? What happens if a user can't authenticate in the cloud? Those are all important questions. But they only address the "identity" half of "identity and access management." The access management half is all about governance: understanding who has access to what and what they're doing with that access. Historically, it has never commanded near the attention or market share that authentication has, but that may be changing.

As organizations shift to cloud IAM, expect concerns about visibility into access to grow—and interest in governance along with them.

If you're thinking about pursuing a governance solution, whether in the cloud or on-premises, an important consideration is how it's delivered. Can you get governance capabilities from the same source as you get authentication? Or do you need two different vendors? Even if you only need one, will the governance solution be on the same platform as the authentication solution? Or is it a completely separate implementation? If you already have a governance solution on-premises, how much of a lift will it require to move to cloud? A converged platform for authentication and governance, both on-premises and in the cloud, will speed deployment, streamline costs, and simplify vendor management, as well as make it possible to coordinate effectively across these two essential areas.

$14.7 billion

Authentication solution market, 2022[7]

$6.7 billion

Identity governance and administration (IGA) market, 2022[8]

Recap: Key Considerations for Cloud IAM

7 Essentials for the Journey

1 **Hybrid IAM.** As cloud adoption expands the attack surface and increases the impact of breaches, finserv organizations can securely move IAM to the cloud using a hybrid deployment that includes both on-premises and cloud IAM.

2 **High Availability.** Failover to on-premises MFA is critical to maintain seamless authentication in the event of a cloud outage or network connectivity failure. Failover is the secure alternative to fail-open approaches that default to no MFA.

3 **Offline Authentication.** It's not just in times of network failure that users need offline authentication; in today's work-anywhere world, they need MFA-secured access regardless of where they're working or whether there's an online connection.

4 **Security First.** Security-first shouldn't mean the user experience comes last. You can make authentication in the cloud as convenient as it is secure: elevate the experience by providing a range of authentication methods and offering always-available self-service.

5 **Identity Governance.** Authentication tells you whether people seeking access are who they say they are, but you need identity governance to get a complete picture of a user's access privileges and how they're being used.

6 **Converged Platform.** Simplify IAM security by choosing one vendor who can offer authentication and identity governance, and deliver both on-premises and in the cloud. This will both streamline solution management and simplify procurement.

7 **Continuous Innovation.** Future-proof your IAM with a solution that enables next-generation capabilities while eliminating time-consuming, multi-step, serial upgrades.

RSA has always been at the forefront of IAM security. Our cloud-based IAM solutions are built on a legacy of identity innovation that we began building decades ago. Today, we offer best-in-class identity solutions on-premises and in the cloud. That means you can rely on a single trusted vendor for all your identity needs, wherever you are on your cloud journey.

RSA®

Hybrid IAM. *Finally.*

Experience ID Plus, the next-gen cloud and hybrid identity platform that integrates security, flexibility, and convenience—without sacrificing access protection or resiliency. ID Plus offers three levels of cloud solutions, tailored to fit every identity and access management requirement. All can be flexibly deployed in the cloud, on-premises, or hybrid with an open, extensible identity platform. And all can be easily adjusted to the pace and evolution of your modernization.

About RSA

RSA provides trusted identity and access management for 12,000 organizations around the world, managing 25 million enterprise identities and providing secure, convenient access to millions of users. RSA empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, RSA connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to RSA.com

1. "How Cloud Is Being Used in the Financial Sector." March 2015. Cloud Security Alliance. https://downloads.cloudsecurityalliance.org/initiatives/surveys/financial-services/Cloud_Adoption_In_The_Financial_Services_Sector_Survey_March2015_FINAL.pdf

2. "Cloud Usage in the Financial Services Sector." February 2020. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/cloud-usage-in-the-financial-services-sector/

3. "Three big moves that can decide a financial institution's future in the cloud." McKinsey. August 3, 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-big-moves-that-can-decide-a-financial-institutions-future-in-the-cloud

4. "Countering the Myths That Hinder Cloud Adoption in Financial Services." Bain & Company. https://www.bain.com/insights/countering-the-myths-that-hinder-cloud-adoption-in-financial-services

5. "Why Banks Are Slow to Embrace Cloud Computing." New York Times. https://www.nytimes.com/2022/01/03/business/wall-street-cloud-computing.html

6. Alert (AA22-074A). Cybersecurity and Infrastructure Security Agency (CISA). March 15, 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

7. Authentication Solution Market Report. Future Market Insights. https://www.futuremarketinsights.com/reports/authentication-solution-market

8. Identity Governance and Administration Market Outlook. Solution Market report. Future Market Insights. https://www.futuremarketinsights.com/reports/identity-governance-and-administration-market

OWN YOUR
IDENTITY.