RSA

WHITE PAPER

Why Enterprises Need Cloud Identity and Access Management

Identity has evolved, so now is the time to move to cloud

Executive summary

For enterprises, implementing identity and access management (IAM) has traditionally been a complex, expensive proposition that was prone to failure. And even for those that implement it successfully, the ongoing expenses related to IAM upgrades and platform maintenance are challenging to manage.

But the IAM industry is changing and resistance to moving IAM to the cloud has decreased. Because IAM vendors have embraced industry standards and more organizations have adopted cloud-based systems, confidence has increased in off-the-shelf solutions.

By shifting IAM implementation, maintenance, and upgrades to cloud identity solution providers, organizations can benefit from the economic, scalability and flexibility of cloud without risking security.

OWN YOUR IDENTITY.

For enterprises, dealing with IAM has never been easy. Even though it's a critical system that almost inevitably touches every department, often employees and even management resist instituting IAM polices or transforming their current IAM system because doing so would affect how people do their jobs. Systems are often complex with costs that often far exceed expectations. Lack of planning means ongoing maintenance and upgrade costs also can be an unwelcome "surprise." And managing identity gets more challenging all the time because today workers use more devices and work from more locations than ever before, which can make it more difficult for security teams to gain visibility into those issues. And no matter where users may be physically located, they need secure access to resources including cloud applications.

Prior to March 2020, many organizations were working to support remote work. But remote work was "nice-to-have." It was a perk that organizations could prioritize or defer given other organizational priorities. Pew Research found that, prior to the coronavirus outbreak, 57% of workers said they rarely or never worked from home.[1]

The COVID-19 pandemic changed organizational priorities. Almost overnight everyone had to connect from home, and many enterprises weren't ready. The inevitable result was an increase in cybercrime. According to Forrester, 67% of business-impacting cyberattacks targeted remote workers.[2] And remote work isn't going away: Gallup Workplace found that hybrid work increased in 2022, and that "long-term, fully remote work arrangements are expected to nearly triple compared to 2019 figures."[3] Nearly two years after the first coronavirus vaccines were distributed in December 2020, work from home is no longer a response to a specific pandemic. It's now part of many organizations' long-term strategy. Although organizational culture has largely adapted to hybrid work, many organizations' security policies haven't adjusted to the new reality.

Security teams have always needed to know who is accessing what, when, and how. But as networks become more dispersed, securing the entire attack surface has become a daunting prospect. Today, large enterprises might need to secure tens of thousands of users and assets, infrastructure, public and private cloud environments, and more. For many large businesses, the fastest way to close that gap is to turn to cloud IAM solutions that place identity at the core of their organization's security strategy.

The challenges of traditional IAM implementations

Historically, IAM technologies have been implemented on-premises, which involved massive capital expenditures (CapEx) for data center space, equipment such as air conditioners and generators, software, hardware, and a workforce to run and maintain everything.

IAM implementation has traditionally been a very challenging and expensive business. Successfully getting an IAM project going often required months of intensive labor. An IAM solution is complex not only because it affects so many systems and applications, but also because it needs to support the entire IAM process, including onboarding, multi-factor authentication (MFA), access policies, removal of entitlements for job changes and terminations, auditing, and management. Each of these capabilities has its own set of features, processes, and rules that need to be developed.

Even worse, the license cost is only the beginning. Many times, implementation ends up being two or three times the cost of implementation. And then the "care and feeding" of the system is even more expensive: the World Economic Forum estimated that nearly 50% of IT help desk costs go to password resets.[4] And another study estimates that each password reset costs $70.[5] If you look at implementing a complex system like identity governance, the implementation costs could be up to 10 times the purchase price.

IAM touches everything

The reason IAM is so expensive is because it touches everything in a business. An identity governance and administration (IGA) system or a system that creates and provisions access must integrate with a variety of systems. In a blog post, KuppingerCole Senior Analyst Warwick Ashford detailed how the "management of identities and permissions in digital transformation is the key to security, privacy, compliance, governance, and audit, as well as system usability and user satisfaction."[6]

Because the surface area is so vast, a majority of IAM costs result from frequent associated business processes, including onboarding somebody into the organization, setting up groups, policies, and practices, and then defining workflows and approval matrixes.

The larger the surface area, the more complex implementation becomes. A large, complex enterprise can have tens of thousands of identities and hundreds or thousands of applications in their environment, which all require connections, synchronization, and ongoing upgrades and their resulting dependencies.

Those dependencies in turn require additional investments: if an organization uses an HR application, does it need to update the associated connector? Are those updates synched with the right user groups to allow them to do their jobs? As the number of applications grows, the resulting number of connectors grows exponentially.

The perils of project failures

Another traditional identity challenge is one people don't like to mention: failure. Many companies have struggled with identity projects and research organizations indicate that more than 50% of IAM projects fail the first time.[7] Identity is complex to begin with, and when many companies were forced to react quickly to the coronavirus and attempted to shoehorn an IAM strategy into their existing business processes, it frequently led to major problems. Resistance to changing an existing user experience or adding processes to business operations often doomed these initiatives from the start.

Because identity touches everything, any change to a company's IAM strategy needs buy-in, support, and coordination from across the entire organization. Without that mandate, many organizations struggle to implement IAM policies that meet their business goals.

Why cloud for identity?

Not surprisingly, because of the level of complexity involved in setting up and living with an in-house IAM system, more organizations are considering cloud IAM. Cloud has been the darling of the technology industry for more than a decade because it offers compelling advantages, including:

- Easy and universal access, no matter where someone is located
- Flexibility and scale, so an organization can scale the number of users up and down as needs change
- Lower total cost of ownership (TCO), particularly for updates and maintenance

Cloud lowers up-front CapEx and implementation costs and reduces ongoing maintenance costs, making expenses more predictable. Instead of committing to build an infrastructure (CapEx), organizations that use cloud IAM rely on more manageable operational expenses (OpEx) that allow them to focus more on their strategic resources and initiatives.

As infrastructure, cloud is no longer the risky new entrant disrupting the market. It's reached a level of maturity that, today, even security-first, regulated sectors such as government, finance, energy, and healthcare can deploy cloud for critical systems like IAM. According to the International Data Corporation (IDC) Worldwide Semiannual Public Cloud Services Tracker, the infrastructure as a service (IaaS) market is $91.3 billion with year-over-year growth of 35.6%.[8] Getting even more granular, the IAM market size is projected to reach USD 36.96 billion by 2030, growing at a CAGR of 14.12%.[9]

Another reason that cloud IAM is gaining more traction is the increasing cost of data breaches. According to the latest Cost of a Data Breach Report from IBM and Ponemon Institute, the average cost of a breach has climbed 12.7% from $3.86 million in the 2020 report to $4.35 million in 2022.[10] And this year, Verizon found that 82% of breaches involved the human element, which includes the use of stolen credentials.[11] But that's just this year: the same report found that passwords were one of the leading cases of all data breaches every year for the last 15 years. Identity is critical to preventing breaches, so more organizations are investing in cloud IAM to gain the modern authentication capabilities they need to secure their environments.

Making the mindset shift to cloud

The bottom line is that IAM isn't optional. The only remaining disagreement or hesitancy is the best way to deploy IAM. A decade ago, most large enterprises, governments, banks, and other security-first companies were reluctant to move to cloud because they didn't want to give up control and lacked confidence and trust in off-the-shelf cloud solutions. These organizations worried that if they relinquished control of IAM and the identity system went down, no one could log in. Today, some vendors address this concern with local failover that allows for secure access, even without an internet connection.

The challenge with cloud IAM in the early days was that it wasn't flexible. It was like the old Henry Ford quote, "You can have any color Model T, as long as it's black." But now IAM solutions are more mature with flexibility and authentication standards such as FIDO and SAML built in.

Most large enterprises would rather focus on their core business than IAM, so the idea of having a vendor do the bulk of the work of supporting and maintaining the application or the platform is compelling. Over time, enterprises have developed more trust and confidence in cloud. Many large companies such as banks are now using public cloud infrastructure.

This mindset change has led to a shift in the industry where more companies are now willing to adapt their business processes to work with an off-the shelf IAM solution. Instead of stubbornly refusing to adapt their business processes and writing millions of lines of code that they have to maintain and update, they are looking at solutions that let them write as little code as possible. They can then focus on customization instead of coding. Now rather than being faced with labor-intensive upgrades, the vendor does it automatically, maybe releasing a new feature every month or so. Enterprises can spend their time, money, and resources where it makes most sense, instead of getting bogged down in maintenance chores.

The advantages of identity in the cloud

Identity is a part of the security infrastructure that every enterprise needs. Today, virtually every organization is consuming some cloud service somewhere. So, if the organization is already using cloud-based tools from Google or Microsoft for email and word processing, for example, it's easier for a cloud IAM system to plug into that ecosystem.

The identity platform can send instructions in terms of entitlements to downstream cloud ecosystems, whether they are cloud or mainframes. With a separate identity system, a company isn't locked into a single vendor or cloud infrastructure or tasked with challenging integrations into closed ecosystems.

It's always a good idea to separate security from other systems and resources, so it is agnostic in terms of what needs to be secured. Modern cloud IAM solutions take a standards-based approach. And for enterprises moving to a zero-trust architecture, identity is a good start on the zero-trust journey because it is the foundation of everything else.

Trust in cloud has increased

Over time, the identity industry has proven that it can work in the cloud. Yet the reality for many enterprises is that they can't move everything to the cloud yet. Some applications need to stay on-premises with hardware, networks, and applications located on site. Enterprises may be at various points along the cloud spectrum depending on their needs. Certain highly sensitive industries are never going to be comfortable relinquishing all control of IAM. But buying the server, building the server, building the rack, calling the server, and hiring staff entails more capital costs than many organizations are willing to bear. The more technology that needs to be managed in-house, the more complex and costly the proposition becomes. Conversely, the more someone else can do the work, the better the economics of cloud IAM.

Some organizations opt for hybrid deployments that can be deployed on-premises and technologies that can be accessed in the cloud with pricing models such as monthly subscriptions or pay-as-you-go options that reduce CapEx and implementation time. And of course, there's the pure cloud model with a standard user interface and application programming interfaces (APIs).

As organizations develop a strategy and research potential solutions, they need to examine their requirements versus a vendor's solution options. Many IAM vendors don't support both on-premises and cloud deployments. They support either cloud or on-premises, but not both. For various reasons, some organizations need a true hybrid deployment with both on-premises and cloud IAM. It's critical to make sure that the vendor can support these types of complex IT environments before moving forward.

Today there's a level of trust and confidence in cloud IAM solutions that simply didn't exist before. The industry has embraced standards, such as SAML, OpenID Connect, and FIDO that are supported by applications and IAM solutions out of the box. With these newer solutions, implementation moves from customization to configuration, which is vastly less complex.

Where we go from here?

Identity has finally matured to the point where enterprises can trust off-the-shelf solutions because they can solve their business problems. And they offer APIs so that if user interface changes are needed, it's not necessary to write an entirely new application. Instead, a web page can be developed that simply calls the API, which is faster, simpler, and less prone to failure.

Moving to cloud IAM opens up new possibilities as well. For example, organizations using cloud IAM have large pools of data, which makes it possible to take advantage of artificial intelligence (AI) and machine learning (ML) to gain insights into users' behavior and security vulnerabilities. With IAM in the cloud, it's possible to scale across multiple threats and data sets to expand the organization's view into what is going on and add capabilities around intelligence and risk that simply weren't feasible with an on-premises application. Cloud broadens the perspective, so tools can be applied to data at scale.

Instead of being tasked with a massive, expensive project that is prone to failure, enterprises can leave IAM to the identity experts . Because the vendor does the implementation, upgrades, and platform maintenance, the enterprise can focus on its core business. Both from an operations and a business process standpoint, the economics are why moving identity to the cloud makes so much sense.

Learn more about RSA identity and access management solutions at RSA.com

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. "COVID-19 Pandemic Continues To Reshape Work in America," Pew Research Center, February 16, 2022. https://www.pewresearch.org/social-trends/2022/02/16/covid-19-pandemic-continues-to-reshape-work-in-america/
2. "Beyond Boundaries: The Future of Cybersecurity in the New World of Work," Forrester Consulting, 2021. https://www.tenable.com/analyst-research/forrester-cyber-risk-report-2021
3. "Returning to the Office: The Current, Preferred and Future State of Remote Work," Gallup Workplace, August 31, 2022. https://www.gallup.com/workplace/397751/returning-office-current-preferred-future-state-remote-work.aspx
4. "Forgotten Your Password? Not Having One Will Make You Safer," World Economic Forum, January 20, 2020. https://www.weforum.org/press/2020/01/forgotten-your-password-not-having-one-will-make-you-safer-says-world-economic-forum/
5. "Cost of Account Unlocks, and Password Resets Add Up," Hacker News, April 22, 2022. https://thehackernews.com/2021/04/cost-of-account-unlocks-and-password.html
6. Warwick Ashford, "Identity Fabrics 2," KuppingerCole, May 31, 2022. https://www.kuppingercole.com/blog/ashford/navigator-identity-fabrics-2
7. "6 Reasons Why Identity and Access Management Projects Fail," Idenhaus, February 3, 2022. https://www.idenhaus.com/6-reasons-why-identity-and-access-management-projects-fail/
8. "Worldwide Semiannual Public Cloud Services Tracker," International Data Corporation (IDC), June 29, 2022. https://www.idc.com/getdoc.jsp?containerId=prUS49420022
9. "Identity & Access Management Market Size is projected to reach USD 36.96 billion by 2030," Straits Research, July 28, 2022. https://www.globenewswire.com/en/news-release/2022/07/28/2488249/0/en/Identity-Access-Management-Market-Size-is-projected-to-reach-USD-36-96-billion-by-2030-growing-at-a-CAGR-of-14-12-Straits-Research.html
10. "Cost of a Data Breach Report," IBM and Ponemon Institute, 2022. http://www.ibm.com/security/data-breach/
11. "Data Breach Investigations Report," Verizon, 2022. https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf