Identity and access in the cloud: The future of the secure enterprise

A guide for evaluating the pros and cons of cloud-based identity solutions

Rethinking traditional approaches to managing digital identities

The continued growth of cloud-based services is prompting many organizations to rethink traditional approaches to managing their digital identities. Although on-premises identity services are effective at controlling access to systems and data, hosting and maintenance have always been difficult and costly.

These on-premises systems are becoming less relevant with data and IT services spread across data centers, cloud infrastructures, mobile devices and the expanding internet of things (IoT). As organizations move business applications to the cloud, they have to manage access into and within cloud providers. Where identity services are hosted is also becoming less relevant as many organizations drive toward Zero Trust security principles with ID verification and network context controls.

Identity services providers are responding by offering new services in the cloud. Some vendors have developed new solutions in-house, while others have expanded their services through acquisitions of smaller vendors. Many vendors are now offering dual-platform options, although the functions available on premises and in the cloud often don't match.

The move to provide identity services in the cloud, which mirrors the cloud-first strategies of other application and service providers, is expected grow dramatically by 2022 (**Figure 1**).

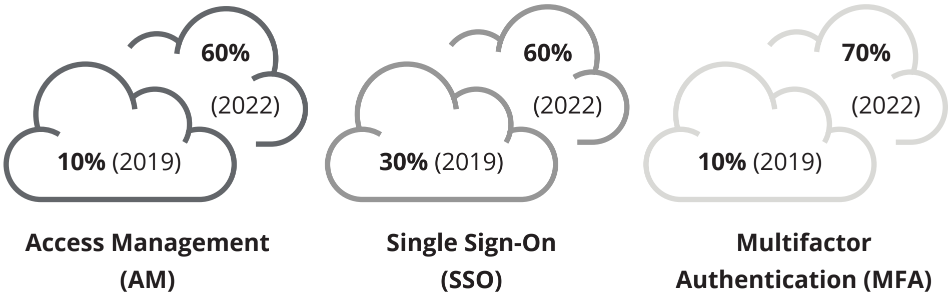


Figure 1. Nearly two-thirds of identity services are expected to be delivered in the cloud by 2022.

Source: DXC Technology research

As organizations move business applications to the cloud, they have to manage access into and within cloud providers.

Vendors are taking two major approaches to digital identity management in the cloud:

- **Cloud-native identity services providers** deliver infrastructure-as-a-service (IaaS) identity services from cloud service providers.
- **Cloud-based identity-as-a-service (IDaaS) providers** offer dedicated identity suites based on software-as-a-service (SaaS) models.

This paper examines the challenges and benefits of each approach and explores examples of how they can be implemented to provide a foundation for identity management in the future enterprise.

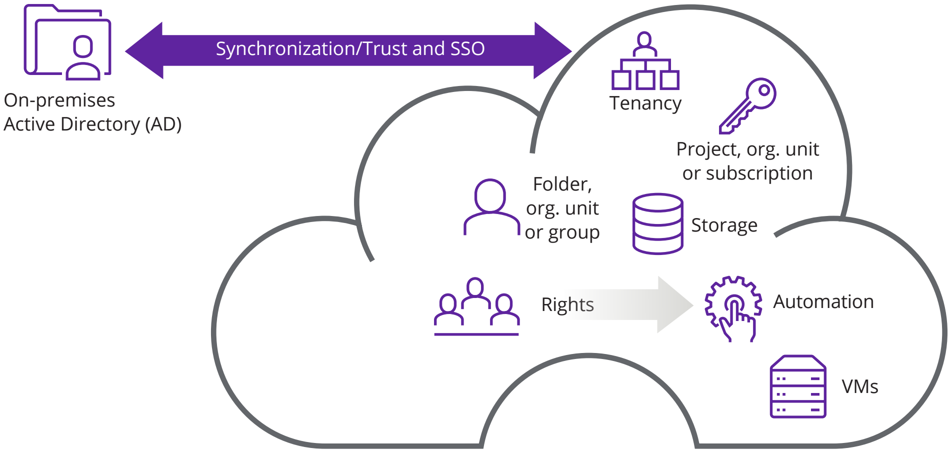
Cloud-native identity services

Cloud infrastructure providers such as AWS, Microsoft Azure and Google Cloud deliver identity management services through necessity. External-facing applications running on hosted cloud infrastructures need the provider's full support for the OpenID Connect (OIDC) framework to underpin cloud services with a rich consumer experience. Cloud-native identity services have two fundamental functions: internal and external.

Internal identity management

For employees to be able to create, modify, access and delete cloud resources, a basic level of access control must be established. **Figure 2** depicts an on-premises identity store that has a trust relationship with the cloud provider, allowing employees to access resources in a compliant, secure way.

Figure 2. Cloud-native identity management (internal use case)


On-premises
Active Directory (AD)
Synchronization/Trust and SSO
Tenancy
Project, org. unit or subscription
Folder, org. unit or group
Storage
Rights
Automation
VMs

Cloud service providers offer tenant infrastructure provisioning capability via a management portal. Public key infrastructure (PKI) and single sign-on (SSO) provide controls for basic tenant access security.

Enforcing an enterprise cloud access policy requires a central user repository for authorizing, granting and revoking access to infrastructure such as compute and storage. A root, or main, account subscription manages the administration of the policy. There are some semantics about the naming of core containers for user management, which varies between providers — for example, folders, organizational units or groups — but perhaps more vital is the user management model. There are two ways to manage relationships with on-premises Active Directory services: User accounts can be synchronized, or trust relationships can be used to provide user/group management between on-premises and cloud-based domains. There may also be other deployment considerations; for example, a multicloud strategy may call for a mix and match of both.

For easier management of access controls, cloud service directories arrange user accounts in a hierarchy of organizational units, folders or groups. These directories often support synchronization with enterprise Active Directory environments to give the on-premises user base access to the cloud platform. The level of synchronization between the two environments may vary between providers — some offer higher levels of granularity, while others deliver domain trust without synchronizing users, groups and credentials.

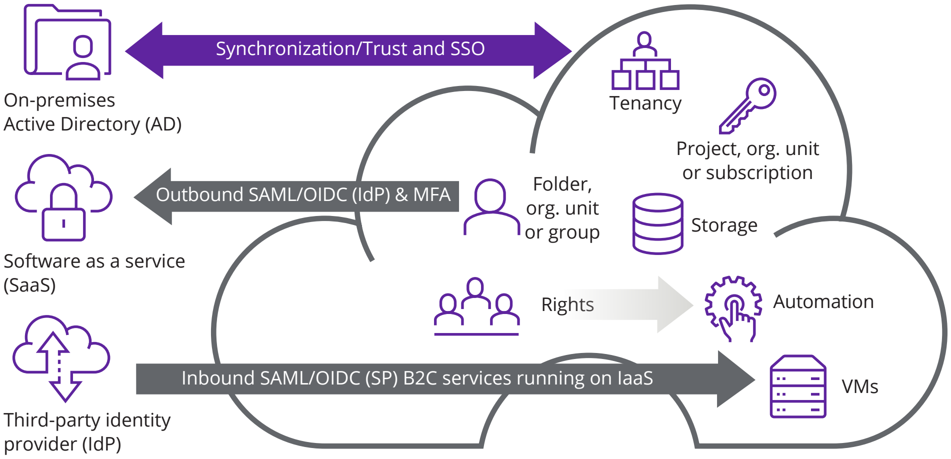
External identity management

A cloud provider serves as an identity consumer or provider through federated trust relationships, using open standards and protocols to set up relationships with partners to enable:

- Consumption of business services hosted on the cloud-native platform in a service provider mode
- Orchestrated authentication for customer accounts held directly in a cloud repository or on premises to consume identity services from external parties and service providers

Native support of the OIDC framework allows organizations to establish authentication and access tokens required to support modern consumer-facing services. The OIDC protocol wraps the open authorization version 2 (Oauth2.0) protocol used to capture additional user consent or authorization that a business-to-consumer (B2C) service may request. All major cloud platforms with full B2C support will adhere to the OIDC standard for application hosting (**Figure 3**).

Figure 3. Cloud-native identity management (external use case)


On-premises Active Directory (AD)
Synchronization/Trust and SSO
Software as a service (SaaS)
Outbound SAML/OIDC (IdP) & MFA
Third-party identity provider (IdP)
Inbound SAML/OIDC (SP) B2C services running on IaaS
Tenancy
Project, org. unit or subscription
Folder, org. unit or group
Storage
Rights
Automation
VMs

Multifactor authentication (MFA), which applies multiple independent channels to verify positive authentication, is commonly used to improve authentication assurance for both internal and external services.

Cloud-native providers use a deployment portal to manage IaaS infrastructures that includes both SSO and MFA services to enable access to the portal.

Benefits of cloud-native identity services

A cloud provider's native services offer some advantages. Secure communications with the existing cloud provider tenant and instance are already in place, along with the associated trust established via exchange of PKI key pairs. For many organizations, this is a sensible starting point that should be considered before initiating a business case for additional services.

Most cloud providers can offer a rich level of synchronization between the customer's on-premises authoritative directory store (primarily Active Directory) and a replica repository in the cloud via secure channels and trusted connectivity. Classic cloud attributes such as availability, reliability, scalability and security make a good case for using a cloud replica as the main user repository — the integrity of which is based on the granularity of synchronization with the on-premises directory.

Because many solutions are delivered through consumption-based SaaS models, enterprises have an advantage when their user accounts persist in a secure cloud identity provider repository. This repository significantly simplifies the SSO function for orchestrating native Active Directory (using Kerberos) or LDAP-based authentication.

When access to secure assets or services requires higher levels of trust, providers that support MFA also offer stepped-up levels of assurance to SaaS services by providing the concurring positive authorization from a second channel.

Challenges of using cloud-native identity services

The potential downside to using native cloud identity services for access is the requirement for additional subscriptions to take advantage of extended capabilities. Additional charges can be incurred when moving beyond a base service feature level. There may also be occasions when a single component feature can only be accessed as part of a broader subscription or upgrade package and the native providers may not be able offer a granular feature since they are not identity service specialists.

Out-of-the-box integrations and support for multiple protocols are areas in which SaaS-based identity providers far exceed the capability of cloud-native identity providers.

While it can be easy for admins to overprovision and generate unnecessary costs, it is vital that they receive training and certification via the cloud admin tracks in the respective providers' environments. With respect to the internal use case, the more serious challenge is to get the identity and access policy set correctly to avoid erroneous access.

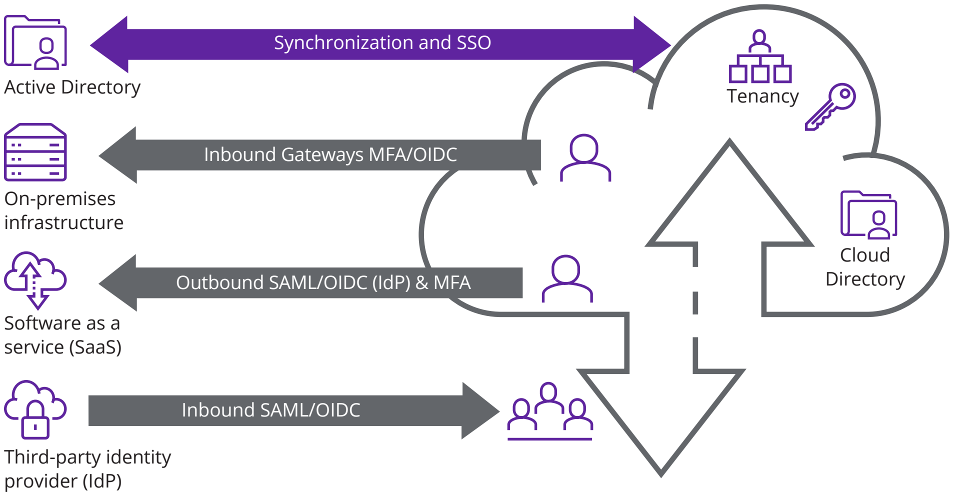
Organizations with their IT estates distributed across many providers (including other cloud service providers) are at risk of incurring unnecessary overhead to manage multiple gateways, key stores and identity providers. There may also be a business preference to having identity interactions and integrations maintained by an independent provider.

Some smaller cloud infrastructure providers offer secondary identity services, yet they do not employ specialists. As a result, new identity service capabilities may lag behind dedicated identity SaaS providers. Organizations are likely heavily invested in their hosting services, making it costly to move to a new provider. It is also common to need to fill gaps with the cloud provider's technology, either through partners or homegrown technology and skills.

Identity as a service providers

The concept of identity as a service is nothing new, and these providers typically use cloud hosting partners. The location of the centers can influence choice, especially with public sector or even defense sector engagements. In instances when regulatory compliance would prevent customers from using standard hosting regions, some providers can host services in alternate regions. Almost all identity capabilities can now be delivered through SaaS models (**Figure 4**).

Figure 4. Identity-as-a-service provider services


Active Directory
Synchronization and SSO
Tenancy
On-premises infrastructure
Inbound Gateways MFA/OIDC
Cloud Directory
Software as a service (SaaS)
Outbound SAML/OIDC (IdP) & MFA
Third-party identity provider (IdP)
Inbound SAML/OIDC

When evaluating security controls of SaaS-based identity services and choosing a service provider, organizations must examine the multi-tenancy model, specifically the security model of the underlying hosting partner. Examination should cover both physical and logical access, any access rights to its tenants and key management processes. If the underlying cloud hosting partner is compromised, the tenants (including customers of the SaaS provider) can be compromised.

When selecting a SaaS provider, organizations should also focus on differentiation. SaaS-based identity offers a full suite of access control, provisioning and even API management services. Services are well placed to cater to both the workforce and external customers, which some providers call out explicitly in their service models. This approach is a great way to segregate pools of users between differing governance dimensions by having separate tenants for each type of community being served.

Key management requires consistent discipline in any area of security; however, when sound procedures are adopted, encrypted data is more secure when persisted in a cloud rather than in a traditional on-premises environment.

The identity and access management (IAM) market has been addressing workforce use cases since its inception. As a specialized area of security, identity as a service now covers many disciplines, with controls bound to the access of network domains as an initial application. The notion that identity is the new boundary and the ethos of Zero Trust is now more widely adopted. This change in focus positions IaaS as central to access security.

Customer identity access management (CIAM) is a valid use case for cloud-based identity. As such, it has led to areas of specialization, such as how to cost-effectively manage customers while verifying that those users are genuine.

With CIAM, organizations incur the overhead of hosting an account solely to support transactions, but with the objective of building a richer relationship to encourage its customers to spend more. Migrating the burden of building and maintaining provisioning, authenticating services and managing customer consent gives organizations more time to focus on customer service, which enables them to become competitive.

Other specialist SaaS providers offer services that take charge of provisioning, registration, and verification of new customers and handle the integration with existing systems. In the cloud-based identity market, these “know your customer” service providers engage specialists who work together with both on-premises and cloud-based identity repositories.

The adoption of modern customer-focused provisioning and consent protocols such as OIDC and System for Cross-domain Identity Management (SCIM) offers significant benefits to organizations. It provides a customer consent framework that customizes experiences for improved customer retention and higher repeat business rates. Such adoption also provides an open standard that allows customers to drive integration and provisioning to a broad range of environments, thus reducing operational costs.

Benefits of identity as a service

Out-of-the-box integrations and support for multiple protocols are areas in which SaaS-based identity providers far exceed the capability of cloud-native identity providers. SaaS providers’ broad application support enables them to offer a level of maturity when underpinning organizational identity strategies as organizations evolve.

SaaS providers offer another major benefit in supporting businesses with standard onboarding processes. The user base, application integration and policy store are often accessible via a single interface, thereby reducing the complexity of such projects.

The speed of evolution and adoption of new standards supported by these identity providers enables capabilities that meet or exceed the demanding use cases of most organizations. Many SaaS service providers participate in defining industry standards with organizations like the World Wide Web Consortium (W3C) before developing a compliant offering. Through extensive adoption of secure development and deployment practices such as DevSecOps to firmly utilize the ethos of the open source community, organizations with cloud SaaS development can accelerate their time to market.

An IDaaS provider enables organizations to grant mobile workforces secure access to both on-premises and cloud-hosted business applications, independent of and more comprehensively than cloud-native identity service providers. This capability makes SaaS a more effective method when managing access for organizations with multihost IT estates, which is critical with the widespread adoption of remote working.

Challenges of identity as a service

As with all cloud service consumption models, the duty of security is shared between the provider and consumers. Corporate responsibility demands that security technology, process and governance align with or exceed corporate guidelines; therefore, it is vital that chief information security officers (CISOs) ask serious questions of proposed providers.

Organizations are likely heavily invested in their hosting services, making it costly to move to a new provider.

Key management requires consistent discipline in any area of security; however, when sound procedures are adopted, encrypted data is more secure when persisted in a cloud rather than in a traditional on-premises environment. Network security is not to be overlooked, but overall, providers use the same standard protocols and encryption. Therefore, a successful implementation and strong corporate practices are key to long-term success.

The Cloud Hopper attack, discovered in late 2019, targeted environments of managed security service providers (MSSPs) so it could gain access to these providers' customers. For a SaaS-based identity provider, the breach potential of the underlying cloud hosting partner is the same: Gain access to the hosting framework first and then laterally move through tenants.

The question of when to adopt cloud-native identity service over a dedicated IDaaS provider solution is more related to integrity and ease of management. If cloud-native services cover all use cases, why pay more for another service?

One discipline that has been slow to migrate to a cloud model is privileged access management (PAM), though not because of technical limitations, but more due to a matter of trust. A key proposition for many PAM vendors was to protect passwords in a "bastion" vault, hosting the vault close to the assets being protected to mitigate risk of exposure on the network. A renewed focus on just-in-time and Zero Trust principles and smart architectural patterns has seen the PAM-as-a-service model emerge as a valid option for development, making the hosting location of PAM services irrelevant.

Why choose cloud identity providers?

Table 1 shows the high-level differentiators of native and hosted cloud-based identity service platforms. The on-premises model is included for general comparison to the cloud platforms.

Cloud-native services cannot evolve with organizations' identity strategies at the pace of cloud infrastructure providers. Native organizations are locked in after implementation. With the loose coupling, API-driven services and use of standard protocols by cloud-based SaaS identity providers, it is fairly easy to change providers, outside of any contractual obligations.

Decentralized identity, also referred to as self-sovereign, will offer the prospect of further outsourcing with the potential to reduce both liability and cost. Those opportunities will be easier to grasp for organizations familiar with using cloud-based third-party identity providers (IdPs).

Identity services hosted and delivered via a cloud platform allow for fast and efficient onboarding of users and applications. The implicit availability of cloud-hosting ensures the bandwidth and scale to suit most use cases.

IDaaS providers support standard protocols to encrypt, authenticate and supply consent mechanisms. The support for standards represents a distinct customer advantage both commercially and technically, as it is possible to change IDaaS providers a lot easier than changing on-premises vendors.

The recent development of new solutions fostered directly in the cloud includes CIAM and "know-your-customer" (KYC) services. Organizations that become familiar with and adopt outsourced identity processes common to cloud IdPs will be well-positioned for future identity service evolution.

Table 1. Pros and cons of IAM services

Platform	Pros	Cons
Cloud-native (IaaS)	• Scalability • Resiliency • Cost	• Narrow scope • Less mature
Identity as a service (SaaS)	• Scalability • Resiliency • Rich identity features • Independence	• Additional investment
On-premises	• Use of existing resources • Maturity	• Rigid • Fragile • Limited future

Conclusion

IDaaS providers will deliver increasing benefits as enterprises consume more SaaS-based application services. It is abundantly clear that outsourcing the complexity of hosting and maintenance of identity services while still retaining management of access policy is very compelling to most organizations, especially when combined with elastic capacity.

Future use cases and cost benefits will evolve, but likely will be available only to organizations with strong cloud identity strategies using verifiable processes to trust external entities and events. Identity as a service represents the best way forward for most organizations that want to be well-positioned for the future.

About DXC in security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000 experts and a global network of security operations centers. DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in cyber defense, digital identity, secured infrastructure and data protection. Learn how DXC can help protect your enterprise in the midst of large-scale digital change.

About the authors

Martin Reilly is global strategy lead for Identity and Access Management in the Security practice at DXC Technology. With more than 25 years of experience in supporting business and technology change, he has managed large enterprise implementations and solution development to make identity an enabler for customers' digital transformations.

Aditya Varanasi has over 14 years of experience in information security, primarily in the banking and financial sectors, providing security governance, risk and compliance, and security solutions reviews. He has in-depth experience in security project implementations such as SIEM, vulnerability management, on-demand application security, and standing up managed security services. His current role includes security advisory and architect in enabling secure cloud journey for DXC.

Junyuan Han has been working in the information security domain for the past 8 years in various areas, such as vulnerability and threat management, security assessment, cryptography and security governance. His current role includes looking out for the next big thing in the industry and creation of prototypes to solve clients' cybersecurity challenges.

Juergen Jaeger has been working in the IT security industry for nearly 30 years. He started his security career in 1989, joining EDS as a data security administrator for IBM. He has held various sales positions at SYSTOR AG and SECUDE GmbH in the areas of identity management, PKI, digital signature and encryption. He later joined Unisys as security practice director for Germany, focusing on managed security services, governance, risk management and compliance (GRC), and network security in financial operations. Prior to HPE/DXC, he was a regional practice director for Wipro Technologies, advising on GRC, SIEM, identity management, infrastructure security, data privacy, industrial automation (SCADA, OTI) and physical security.

Adrian Slade has been designing, implementing and talking about Identity solutions for well over 20 years. Starting his career with a giant from the past, Novell, back in 1988. Developing solutions and controls-based on the Novell eDirectory platform, then 5 years as the Director/ Owner of a Consultant System Integrator before finally managing Identity services @ DXC. Adrian takes part in Kantara working group sessions whenever time permits and he is currently helping initiate an OASIS project to define a new authentication method.

Learn more at
dxc.com/identity

Get the insights that matter.
dxc.com/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.

© 2021 DXC Technology Company. All rights reserved. DG_1258a-22 July 2021