White Paper

Identity as a Service on the Journey to the Cloud

Sponsored by: Oracle

Christian A. Christiansen Laura Stuart
May 2016

IDC OPINION

From large organizations to small organizations, a journey to using more cloud-based, and particularly software-as-a-service (SaaS), applications is under way. Whether relying on cloud-based infrastructure, platforms, or applications, customers find that the cloud offers new flexibility and efficiency they can't ignore. The ongoing digital transformation in most industries is predicated on using the cloud services that businesses increasingly need to stay competitive.

But expanded SaaS use, including from mobile devices, is among the many dynamics making companies more vulnerable to cyberattacks. It is no longer sufficient for organizations to simply wall off their corporate networks from malware and external attackers. They must recognize and adapt to employees and other users accessing cloud applications from mobile devices around the globe.

In this environment, the ability to correctly identify and control the access and actions of users becomes central to IT security. Ensuring that users have just the access permissions they need for just the necessary amount of time (e.g., as soon as, but not after, they are employees) becomes fundamental. In regulated industries, it is a compliance requirement.

The heterogeneous nature of SaaS applications is a troublesome reality in virtually all organizations today, and it makes control difficult. This is because the SaaS application might be owned and managed by IT, owned and managed by business units (without IT's knowledge), and/or owned by individual employees. Typically based in the cloud, these apps might be resident on corporate- or employee-owned PC and mobile devices.

As organizations look to meet these challenges, two aspects of IT security are gaining importance:

- Identity and access management (IAM) is central to overall security overall.
- SaaS application efficiency and security management rely heavily on IAM.

When these two trends are combined, it results in a need for identity as a service, or IDaaS. This white paper looks at how various types of organizations — from large enterprises to small and medium-sized businesses (SMBs) and start-ups — can use IDaaS as a critical element in securing their own particular paths to the cloud.

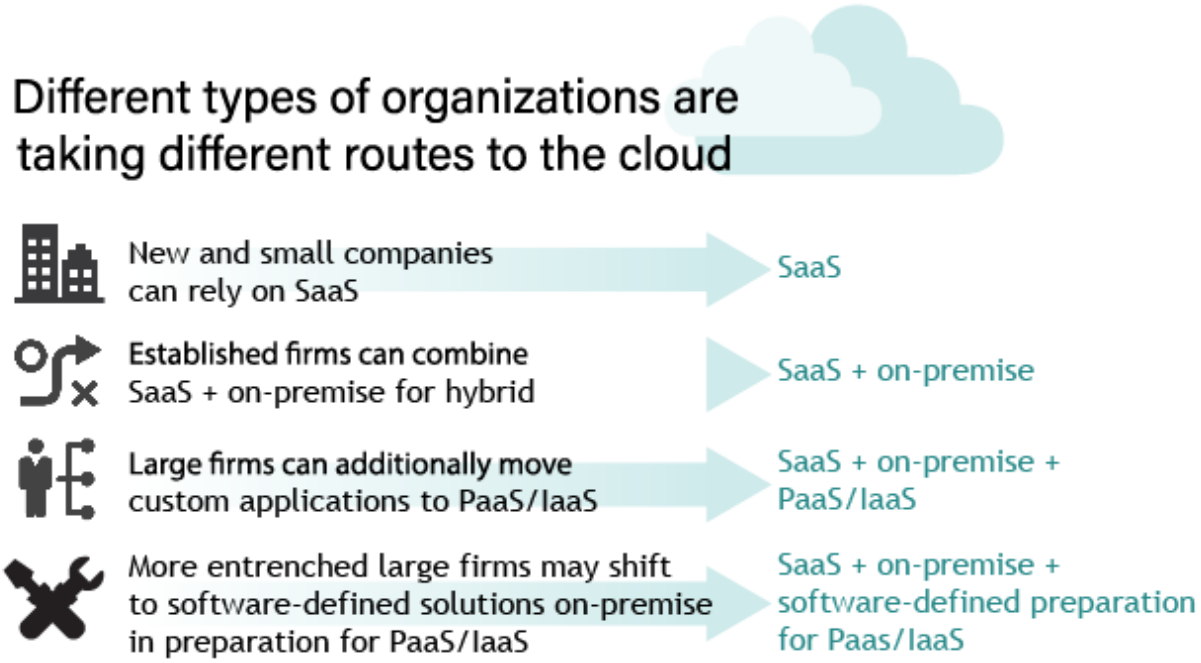
SITUATION OVERVIEW

Organizations come in all shapes and sizes, and they take a broad range of approaches in moving to the cloud. However, most will find themselves in one of four common scenarios (see Figure 1):

- New and small companies may rely primarily or solely on modern SaaS applications.
- Established firms can combine SaaS use with on-premise systems for hybrid solutions.
- Large firms are building new, and moving some existing, custom applications to platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS) cloud use.
- More regulated large firms may "virtualize" some of their custom, in-house applications (rewriting their apps so they can run on different platforms) but are still running them in their own datacenters (aka private cloud) in preparation for an eventual move to an external or a "public" cloud.

FIGURE 1

Oracle IDaaS Routes



Source: IDC, 2016

Different Stages of IAM Implementation

Likewise, companies may be at various stages of implementing an IAM solution:

- They may have no integrated IAM solution and rely on internal staff to provision and deprovision users for enterprise applications.
- Companies may not even have significant authentication capabilities installed whereby they can verify the identity of users accessing company applications and data.

- They may or may not have a "single sign-on" (SSO) capability implemented whereby users can sign on to multiple, often SaaS, enterprise applications with a single user name and password.
- They may have manual, spreadsheet-driven compliance processes for access certification and approval flows, including detailed segregation of duties (SOD) checks, or maybe no process at all.
- Often companies may not have specialized capabilities to ensure the identity and control of "privileged" users, such as company administrators and IT workers who need to have a higher level of access to IT systems and data.
- Some may have installed a more or less comprehensive on-premise or SaaS-based (IDaaS) IAM solution.

The larger the enterprise and the more regulated the industry, the more likely it is that the company will have an existing, on-premise IAM system. In summary, enterprise customers are at different stages of both cloud adoption and IAM implementation. Many have on-premise systems and software, together with some popular SaaS offerings, with some using PaaS or IaaS as well. Some have made significant investments in on-premise IAM, connecting with partners and customers in B2B and B2C scenarios. Others have a pure SaaS environment, looking to add strong authentication, SSO, and data protection, including an extension of the business to social identities.

Common Needs

All of these organizations also have common needs, however, with requirements to:

- Secure and support multichannel access to systems via laptops, smartphones, wearables, or other devices.
- Continually emphasize the important concept of unified management across on-premise, hybrid, and cloud applications and data.
- Trust and verify all identities, with the ability to grant permissions and track and control user actions for governance, risk, and compliance (GRC) obligations.
- Minimize in-house, specialized IT and administrative staffing requirements.
- Minimize time to value and capital layout for new implementations.
- Scale identity management solutions vertically and horizontally with speed and flexibility.
- Expand and modify systems over time.

An Increasingly Common Solution

Because IAM, like other aspects of IT security, is becoming viable via SaaS delivery, IDaaS can increasingly meet the needs of organizations looking to implement or augment IAM solutions. Smaller and simpler organizations are more likely to implement IDaaS as a new, companywide IAM solution. Bigger and more complex organizations are likely to augment their current on-premise system with an IDaaS solution that adds modern capabilities for modern applications, particularly as they support hybrid on-premise and cloud application environments.

A Gradual Rollout

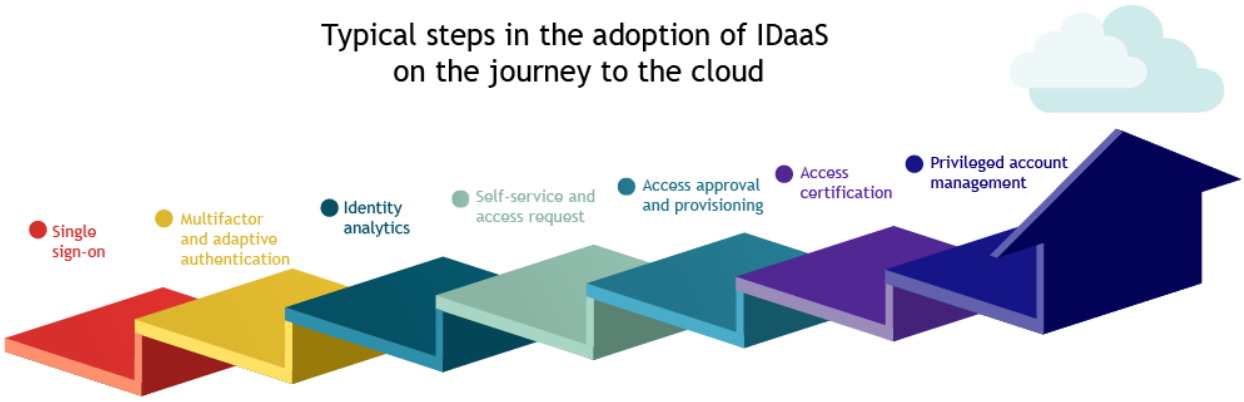
IDC finds that however IDaaS is deployed, it tends to be rolled out gradually, from initial to more extensive use of IDaaS capabilities over time. For example, many organizations first use IDaaS to provide SSO, and perhaps federated identity, whereby the system provides trust to an alternate identity provider. (For example, a Facebook ID may be used to log in to Flickr or other applications.)

Similarly, initial IDaaS solutions, which are relatively new to the IT market, have typically been limited in functionality (e.g., offering primarily SSO capabilities to start), with more complete capabilities added over time.

IDaaS use therefore tends to evolve from the point of initial implementation — a process that is made easier with its SaaS delivery model. This also makes it easier for organizations to modify their IDaaS use as broader use of cloud technology evolves. Organizations might rely on existing, on-premise directories synchronized with cloud in initial rollouts but find use cases by which to exclusively implement cloud-based directories over time. Likewise, enterprises implementing IDaaS in a hybrid situation today may anticipate migrating to a completely cloud-based solution at some point in the future. As with all IAM, authentication methods that are initially deployed in IDaaS can likewise be revised to encompass newer technologies over time. Figure 2 depicts some of the typical steps that organizations may take in implementing modular IDaaS functionality over time.

FIGURE 2

Oracle IDaaS Steps



Source: IDC, 2016

Flexibly Configuring IDaaS

In the sections that follow, we look more closely at each of these typical IDaaS modules before considering in more depth how implementations differ for different types of organizations. There is no need to add these modules in a set order — they can be mixed and matched as the environment requires. However, organizations selecting an IDaaS today typically need to select as complete a solution as possible so that they know they will be able to broaden their use to encompass a full implementation in the future.

SSO and Cloud SSO

A general point of entry for both on-premise IAM and IDaaS in many organizations is SSO. Cloud SSO enables users to access multiple cloud resources with just a single user sign-in. This competitive market is already overlapping significantly with the enterprise SSO solutions that offer this capability as well. Often organizations will want to federate their on-premise identities. The key is for the solution to utilize open standards. This approach also allows for integration with existing SSO to preserve and extend investment (perhaps until a complete, eventual transition to the IDaaS approach is made).

When evaluating an SSO solution, organizations should look at companies that can provide both standards-based software and quality of service.

As shown in Figure 3, IDC believes that cloud SSO solutions, at a minimum, should have capabilities to:

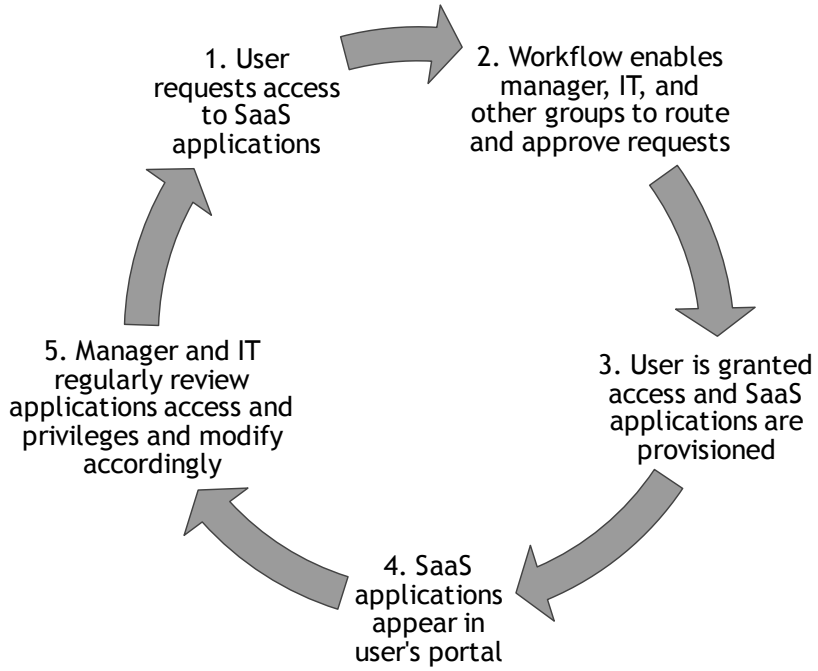
- Maintain an identity store. Track user accounts, ownership, access, and permissions that have been authorized.
- Integrate with workflow to facilitate various approvals (e.g., management, IT, human resources [HR], legal, and compliance) needed for applications access.
- Provision SaaS user account for selective devices (e.g., mobile and PC) with access to user portal containing many private and public cloud resources.
- Facilitate periodic management attestation review for compliance with regulations and current job responsibilities.

In addition to these initial SSO functions, providers are differentiating their offerings with broader IDaaS features that include:

- Cloud account provisioning, managing account life cycle in cloud apps
- More robust multifactor authentication (MFA) integration
- Extensive mobile security capabilities
- Dynamic authentication options

FIGURE 3

Cloud SSO Solutions



Source: IDC, 2016

Authentication Technology

Adaptive authentication and multifactor authentication technologies are evolving and are part of an inclusive IDaaS deployment. For some time, passwords and challenge questions have been seen as being inadequate and susceptible to common attacks such as phishing. Most business entities today are looking at some form of multifactor authentication to reduce risk. To be successfully deployed, however, solutions must be easily provisioned, maintained, and understood by the end user. It is proven time and again that end users will resist anything that interferes with their digital experience. Companies are looking for ways to securely incorporate bring your own device (BYOD), social identities, remote users, customers, and contractors while making MFA an almost transparent component of a seamless user access experience. Within an MFA deployment, industry standards, such as OAuth and OpenID Connect, are essential to ensure integration of existing multifactor solutions and the incorporation of newer, adaptive authentication technology.

IDC defines dynamic (or adaptive) authentication as the evaluation of available information (i.e., IP address, location, time of day, and biometrics) to prove an identity after a user session has been initiated. The key to dynamic authentication is to use additional methods for a user to verify his/her identity in circumstances that are potentially higher risk — and fewer methods in lower-risk environments. The goal is to be more secure while providing a productive environment for users. Dynamic authentication has been used in high-risk industries such as financial services for some time and is now being extended into other verticals.

Advanced authentication for security and identity is at a turning point today in the industry. Newer software-based solutions, typically offered on smartphones, are becoming the de facto standard for strong authentication (as opposed to traditionally deployed hardware tokens). As biometrics are incorporated into mobile devices, MFA enhances the user experience by reducing the need for tedious passwords and PINs while improving risk by more thoroughly authenticating the user, device, and application access.

The replacement of specialized biometric capture/input devices across many industries with mobile devices is also reducing the cost and complexity of systems integration. These newer technologies are providing more secure, multifactor authentication with potentially lower disruption for the end user. With the appropriate standards (e.g., OATH and FIDO) integration and extensible identity management framework, MFA solutions can be adopted, upgraded, and integrated easily within an IT organization as part of an end-to-end secure IAM deployment.

When considering MFA and adaptive policies, organizations must implement consistent policies across on-premise and cloud resources, which in a hybrid IDaaS and on-premise IAM environment requires integration between systems.

User Provisioning and Access Certification

The fundamental function of an IAM solution is to enable and support the entire user provisioning life cycle. This includes providing users with the applications access appropriate for their identity and role within the organization, certifying that they have the correct ongoing access permissions (e.g., as their role or the tasks or applications used within their role change over time), and promptly deprovisioning them as their departure from the organization may require. This is important not only for meeting various compliance requirements but also because inappropriate insider access is a major source of security breaches and attacks.

An automated user provisioning capability within an IDaaS solution can be important not only in its own right but also as part of a hybrid IAM solution whereby IDaaS provisioning may provide greater flexibility than an on-premise solution for transitions as a company downsizes, upsizes, merges, or looks to integrate existing systems with IaaS/PaaS/SaaS environments. An IDaaS approach can save time and effort in one-off upgrades and ensure appropriate integration among necessary departments, divisions, and systems. The need to scale this technology often sneaks up on corporations, and the ability to deliver a scalable IDaaS capability immediately across the enterprise can provide benefits in flexibility, cost, and control.

Industry regulation and audit requirements are the primary drivers for access certification, but there are overriding security issues. Access certification continually audits individual permissions to ensure that users have access to only what they need. Overprivileged users are the source of many high-profile data breaches.

Many targeted attacks start with highly tailored and socially engineered phishing attacks. The goal of attackers is to capture specific individuals' account names, passwords, and other credentials. The next step is to escalate privilege to an administrative level. This becomes dangerously easy for the attackers if they can capture a seemingly ordinary user that is "overprivileged." In a typical scenario, an employee is granted additional privileges (i.e., "privilege creep") over the years as her/his job changes. Companies that are lightly regulated generally lack an "attestation" process that requires managers to regularly audit their employees' privileges (e.g., access to networks, servers, applications, and data). This attestation process, while not always successful, helps halt or slow the privilege creep that results in overprivileged accounts. IDC strongly believes that this regularly conducted (at least once a year) attestation process is critical to the IDaaS process as privilege creep proliferates across on-premise systems to private and public clouds.

With mergers and acquisitions, the need for these tools and services increases exponentially as users multiply. Some may be on SaaS systems, some may be on-premise, many span different departments, and some are being deprovisioned or reallocated. The move to cloud can further confuse this situation. Things can quickly escalate beyond existing, often manually managed, certification methods. While role-based access controls and SOD methods have been in use for several years, the ability to automate these functions and apply sophisticated analytics to user profiles, access history, provisioning/deprovisioning, and fine-grained entitlements is becoming increasingly available beyond the Fortune 1000.

Identity Analytics

The ability to integrate identity analytics with the IAM engine for comprehensive certification and attestation can be critical to securing an organization's risk profile. Properly deployed identity analytics can demand total internal policy enforcement — often an unsung hero in corporate security. Identity analytics that provide a unified, single management view across cloud and on-premise are much needed in a proactive GRC enterprise environment and aid in providing a closed-loop process for reducing risk and meeting compliance regulations. Ideally, identity analytics should be easily customizable by the client to accommodate specific industry demands and government regulations for reports and analysis required by managers, executives, and auditors.

Self-Service and Access Request

Self-service and access request technology is a great way to improve the experience and efficiency of the end user and to reduce costs from help desk calls. While a number of companies deploy on-premise self-service access request for their employees, many have not extended these systems adequately outside the formal corporate walls. Beyond employee use, a positive digital customer experience increases business credibility and ultimately contributes to revenue increase. Companies not only save on customer help desk calls and costs but also improve customer satisfaction. In an IDaaS environment that is based on open standards, these systems should seamlessly integrate with existing access control software and multifactor authentication mechanisms when necessary. The SaaS delivery model saves time and effort formerly devoted to systems upgrades and maintenance, freeing professional IT staff to focus on more core business applications.

Privileged Account Management

Every organization, whether using SaaS, PaaS, IaaS, or on-premise applications, is vulnerable to unauthorized privileged account abuse. Traditionally, this concerned insiders with superuser access credentials, usually system administrators. Today, this concern extends to executives, HR officers, contractors, systems integrators, and other personnel with elevated entitlements and access. Moreover, outside threats typically first breach a low-level user account to eventually reach and exploit privileged user access controls within the enterprise system. Privileged account management (PAM) is designed to prevent such unauthorized insider account use. The main component of a PAM solution is the password vault. This vault may be delivered in various ways — as software to be installed on an enterprise server, as a virtual appliance also on an enterprise server, as a packaged hardware/software appliance, or even as part of a cloud service. The management functionality is typically installed on this server as well. Historically, PAM has been defined as the logical incarnation of a physical safe used to store passwords kept in an envelope and changed periodically, with a manifest for signing them in and out. Today's solutions are multifaceted, allowing not only for a password checkout but also setting time limits, forcing periodic changes, automatically tracking checkout, and reporting on all activities. Perhaps most importantly, these solutions typically provide a way to connect directly through to a requested resource without the user ever knowing the password. This capability also paves the way for session management and additional functionality.

Most cloud services utilize APIs and administrative interfaces, which provide opportunities for infiltrators to circumvent security. These holes must be accounted for in existing PAM practices. The move to the cloud presents new challenges for PAM. Many SMBs now administer their own SaaS systems (e.g., Office 365). Larger companies increasingly have individual business units spinning up their own SaaS and IaaS services. These customers find themselves with PAM capabilities within the IDaaS solution or from their IaaS/PaaS provider but with little experience in handling this responsibility. Moreover, in some cases, many different geographically dispersed business units are trying to segregate administrative responsibilities for the same SaaS applications.

IDC believes that customers in these situations may want to link existing PAM into the overall identity framework and move toward greater security and compliance with the assurance of scaling to cloud load requirements as business needs dictate.

Different IDaaS Implementations for Different Cloud Scenarios

IDaaS thus may be consumed in its entirety or in functional components as business and security needs dictate. With that flexibility, an optimal IDaaS offering can be implemented successfully by almost any organization at any point along its overall cloud journey.

The path to the cloud is unique to each organization, but just as we find that most businesses are represented in one of the four types of cloud adoption discussed previously, there are some common tendencies and needs for companies implementing IDaaS within those four scenarios:

- **Newer, small companies using all SaaS for IT.** These companies, while successful at using a variety of SaaS apps (such as Google Apps and Box), are perhaps the most vulnerable to identity-related security breaches and violation of industry standards. Without an integrated, structured identity management framework, it is difficult to maintain an overall, centralized view of who is accessing what and when and whether users should have such access. These companies deal heavily in B2B and B2C transactions, and the ability to trust and verify with confidence is critical to ongoing fiscal health.
- **Mix and match of on-premise software and SaaS applications**. This spans companies of all sizes. Most organizations have purchased third-party software for their office applications, payroll, HR, and so forth, but have moved to SaaS providers for certain applications (i.e., Google for email and Dropbox for collaboration). With the proliferation of BYOD and bring your own apps (BYOA), these companies must have the capability to establish and enforce policy for access control, provisioning, and, in some cases, regulatory compliance. These companies may already have an IAM solution onsite, but the capabilities must be integrated and extended to an elastic cloud environment.
- **Custom apps on PaaS/IaaS.** Large, established multinational organizations are the most likely to be using platform and infrastructure services to host their business-critical applications. Experienced and specialized IT staff are becoming more difficult to maintain, and the scarcity of these employees is endangering IT-dependent growth, especially security expertise. Customers look to the benefits of SaaS use and are now looking to offload more generally established IT practices to a reliable service. These companies were early adopters of IAM solutions and are looking for ways to grow identity management functionality within a cloud deployment. Integration is important, compliance is mandatory, and security is paramount.
- **Custom apps in software-defined datacenter (SDDC) in preparation for lift/shift.** Some companies are not quite ready to transition their custom apps to the cloud today. However, they are preparing their datacenters to lift/shift at an appropriate time in the future by "virtualizing" their applications in an SDDC, which may take the form of an on-premise, "private cloud." IDaaS can readily create the necessary levels of trust for these applications in both their initial and ultimate deployments, thus easing the transition. The adoption of IDaaS also allows in-house developers to focus on the purpose-built features and functionality of their custom apps without the added burden of creating cloud-ready security and identity capabilities.

Benefits of IDaaS

Adopting an IDaaS approach involves lower deployment and operational costs than traditional on-premise security solutions. This is immediately appealing to many enterprises, but IDaaS offers many more particular advantages on the road to lowering overall risk while achieving greater governance benefits.

Identity and access management solutions support the validation, provisioning, and management of user accounts across many different platforms as well as those supporting the authentication and access rights of users during sessions. New distributed architectures along with existing standards make it easier to tie together technical components such as strong authentication, single sign-on, and user provisioning. Since IDaaS offers these capabilities in a service model, they are implemented quickly and easily in stages, and businesses can realize ROI in deployment flexibility, quick provisioning, scalability, process automation, permissions controls, analytics, and consistent user experience. All of these offer greater security.

IDaaS as a Solution — What Pieces Do I Need, and When Do I Need Them?

As the world moves rapidly to adapt to digital innovations, enterprise IT must lead, not lag behind. BYOD and BYOA have become the norm, along with ever-increasing digital business capabilities. Consumers, contractors, and employees are now requiring access via social identities, on-premise apps, and cloud apps or through other third parties. Within all this activity, governance, access analytics, and certification are integral to establishing a proactive, risk-averse identity framework. Transformative digital business greatly increases the capacity for achieving greater business benefits – *providing that the correct security controls and services are in place* (see Figure 4).

FIGURE 4

Customers' Digital Transformation to the Cloud Enabled by Identity as a Service

- Education and tone
- Partners and ecosystem
- Risk making and taking
- Innovative platforms
- External communications

- Identifying and protecting customers and partners
- Cloud identities
- Global privilege access management
- Antifraud
- API security for SaaS apps

- Information protection
- Cyberanalytics and cyberintelligence
- Visualization
- Information sharing for greater threat insight

- Operational technology (OT)
- Internet of Things (IoT) security
- Machine to machine (M2M)
- Monitoring and surveillance
- Vendor risk management

- Organizational realignment
- Insource/outsource security operations
- Expert advisory services
- Talent acquisition
- Enterprise training
- Background investigation

Source: IDC, 2016

Grow as You Go

A full stack offering of IDaaS can be adopted piecemeal (see the Benefits of IDaaS section) depending on an organization's needs. It should integrate smoothly and seamlessly with existing on-premise identity investments, on-premise applications (custom and commercial), existing directories, existing SaaS/PaaS/IaaS, and social identities. Multichannel support for devices is rapidly becoming a mandatory cost of doing business, and linking all these devices to the enterprise securely requires an established "trust, but verify" approach – often a combination of several technologies such as MFA, password management, SSO, and sophisticated access controls and permissioning. Any, all, and some of these technologies should be available to the customer in individual, easily assimilated pieces, to be consumed as needed to fit the customer's business, compliance, and security requirements.

Customers evaluating IDaaS as part of a hybrid IAM solution should verify that the services adhere to open standards, such as OAuth, SCIM, SAML, and OpenID Connect. They should also have a track record of scalability in large volume deployments. Most importantly, successful customers transition to the cloud gradually. Building on a good base, they already have a strong on-premise solution that unites key legacy and Web security by breaking the connection to application-specific authentication and authorization. By building a centralized application-independent IAM solution, the company and all its affiliates enjoy the benefits of SSO, rapid provisioning/deprovisioning of access rights, and unified PAM. This positions the company to gradually move to "noncore" SaaS applications in file sharing, CRM, collaboration, and office applications. The next step might be a hybrid situation where Big Data marketing applications are shifted to cloud service providers because in-house datacenters are too expensive and inflexible. The final steps involve a very careful and gradual shift of production applications to the cloud. Right now, most companies are still in the middle of this transition with a heavy reliance on on-premise for critical applications that are gradually transitioning to a hybrid state that is divided between private and public cloud.

IDC offers the following guidance for customers adopting IDaaS cloud security solutions:

- Assess the overall security architecture and determine which capabilities would best fit an IDaaS, a managed service, or a hybrid model.
- Develop a security architecture framework that enables business flexibility with reasonable and understandable constraints, being able to adopt and adapt identity services as necessary to the organization's business and security needs.
- Work with business operations in using IDaaS to quickly integrate security into new business initiatives.
- Implement IDaaS for noncore applications first, potentially moving to encompass systems of record only once the solution has been proven.

Customers adopting an IDaaS should see ROI from:

- A holistic and integrated approach to IDaaS delivery, including both SaaS and on-premise offerings that securely extend all services to remote, home, satellite, and branch workers and enable access to applications services from mobile devices
- The ability to leverage new technologies such as cloud, mobility, Big Data, and social media to develop new identity-aware solutions and flexible, secure business models and incorporate line-of-business (LOB) managers into the identity life cycle
- Ease of use and customizable capabilities around both horizontal and industry-specific opportunities
- Elimination of identity silos created by cloud
- Integrated IaaS/PaaS/SaaS
- Consistent customer experience

Oracle Solution: Oracle Identity Cloud Service

Oracle has deep experience with enterprise stack identity development and deployment. The Oracle Identity Cloud Service (IDCS) has 35,000 customers across 19 datacenters supporting over 35 million daily log-ins and has been available for over four years. Oracle's on-premise IAM product, Oracle IDM 11*g*Rx, has deep and extensive enterprise capabilities, including SSO, adaptive authentication, access management with password policy management, provisioning and analytics, and directory virtualization via Oracle's Unified Directory (OUD). IDC research shows that Oracle has consistently been a leading vendor in the identity and access management market.

IDCS is a natural evolution of Oracle technology. It has been built from the ground up as a modern cloud service with a microservices architecture, REST APIs for every interaction, and a hybrid design that provides a single pane of glass with Oracle's existing on-premise solution. IDCS enables enterprises to securely and simply synch existing LDAP directory information to the cloud and extend on-premise SSO and federation across both internal and external environments, including custom apps and commercially available applications and resources. Today, Oracle's Cloud Services can be hosted in public or private clouds as well as provided as a service for an on-premise deployment with Oracle Cloud at the customer site.

As a vendor, Oracle offers customers the assurances of proven software scalability, a wide portfolio, and the ability to service and maintain a global customer base. Oracle's focus on a gradual, carefully prepared transition to cloud deployments appeals to customers. Further, Oracle is committed to open standards and has historically played a leading role in standards committees. The vendor is a lead author of SAML, the editor of the SCIM specification, and a board member of OpenID, which authors OAuth and OpenID Connect.

IDC believes that natural market entry points for Oracle's IDCS include the vendor's existing SaaS customers, existing Fusion middleware environments, and hybrid IDM deployments with Oracle IDM 11*g* customers.

CHALLENGES/OPPORTUNITIES

Opportunities

All industries face the same business, security, and integration issues in the march toward digital business transformation. Critical security considerations are driven by these ongoing phenomena. Common concerns focus on how to close loopholes to keep the bad guys out; how to make things easy and compelling to let more good guys in; and how to consistently scale and securely deploy across diverse platforms, devices, and users. (A related technology, cloud access security broker [CASB] provides additional security capabilities related to SaaS use — e.g., identifying the "shadow IT" unsanctioned use of SaaS and protecting data stored in SaaS clouds — and IDC believes that IDaaS and CASB capabilities may be merged over time.)

Cloud-based identity can provide the solution to some of these issues, but before jumping into IDaaS, organizations should take the opportunity to closely examine and refine their current business practices. When moving to a hybrid cloud, businesses should adjust their internal processes. This can ensure greater agility, omit redundancies, create more dynamic and optimal customer service interaction, and lead to better integration of Big Data and analytics. In this context, IDaaS can serve as a secure conduit for digital business transformation. IDC research estimates that the percentage of enterprise security spending allocated to SaaS-based security solutions could increase from 11% in 2015 to almost 15% by 2020.

Challenges

Organizations must understand that "good enough" today will probably not be enough for tomorrow. To this end, customers must be very clear on which particular capabilities an IDaaS solution does or does not provide. There are many IT vendors in this field. Large, established companies with a track record of delivering on-premise IAM solutions are now introducing offerings, along with a variety of smaller IDaaS providers that were earlier to the market. Customers must cut through the market noise to match the optimal cloud approach with both their current and future scenarios.

CONCLUSION

Enterprises, employees, and applications — all of which used to sit comfortably behind the network wall — are now moving outward to embrace mobile, social, and digital services. This digital business transformation holds much promise but also increased risk. From a security perspective, the steep costs associated with monitoring and maintaining security systems; the sprawl of enterprise security devices; the difficulty of attracting, hiring, and retaining security professionals; the dynamic threat landscape; and the evolving role of the chief information security officer (CISO) are all driving adoption of SaaS security services.

A robust and scalable IDaaS solution can help provide the necessary IAM elements to meet cloud-scale business demands. This includes delivering multichannel user experience, federated identity, API security, and identity analytics capable of providing detection and response. Customers will gain faster and transparent software upgrades, the ability to easily add on more components when they become available, and/or the ability to extend the service to protect remote workers and siloed resources.

For hybrid cloud environments, preference should be given to vendors offering true multitenant solutions that adhere to common industry standards. These should be proven to be both vertically and horizontally scalable and to integrate well with existing on-premise IAM solutions. Security should be implemented at all levels — datacenter, hardware, data, application, and network. With IDaaS, the enterprise can increase security while expanding the reach of the business itself to social entities, partners, and other third-party organizations.

Identity management is moving with the times to provide a more holistic, hybrid approach to enterprise identity issues. The net result is increased effectiveness of security throughout the organization.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com