Ovum
TMT intelligence | informa

Ovum Decision Matrix: Selecting an Identity-as-a-Service (IDaaS) Solution, 2016–17

Publication Date: 07 Dec 2016 | Product code: IT0022-000836

Andrew Kellett

Summary

Catalyst

Identity-as-a-service (IDaaS) is the cloud alternative to maintaining identity and access management (IAM) products on-premise. Fully featured IDaaS offers authentication, access control, single sign-on (SSO), provisioning and password management, infrastructure and directory management, reporting, alerting, and monitoring services, and is hosted, managed, and delivered as a cloud-based service.

IDaaS is relevant to a wide range of organizations, including first-time clients that see it as providing an identity management opportunity they can benefit from and afford. It is relevant to existing IAM users that want a new way of working with identity management that doesn't involve owning and maintaining the on-premise infrastructure. Organizations that need to extend their IAM coverage to the cloud would also benefit from a hybrid approach to the IDaaS service delivery model. Similarly, companies that already have a significant investment in an IAM platform might take advantage of an IDaaS service, say for a new business unit, to avoid the overhead involved in adding an entirely new group of people into their on-premise identity infrastructure.

Ovum view

IDaaS is relevant to public and private sector organizations that are prepared to allow their IAM services to be managed and maintained from the cloud, and are willing to work with a third-party service provider. Data protection regulations, risk, and security concerns are commonly cited as reasons for not going ahead, but a growing number of CIOs and CISOs consider the business risk to be acceptable and are building their IDaaS strategies.

Traditional approaches to IAM continue to have their place, but are often seen as overly complex and costly, leaving clear ground for the providers of lightweight IDaaS to push forward with the efficiencies, flexibilities, and cost savings that are said to be an inherent part of the IDaaS approach.

However, not all IDaaS service providers can deliver all the expected components of identity management. Some are interested only in enabling access to cloud-based applications with their technology, and are prepared to leave the enterprise heavy lifting to technology partners or competitors that can deal with a hybrid mix of on-premise products and cloud-based services.

The cloud-only approach misses the important point about how next-generation identity management needs to evolve. It needs to be capable of providing an integrated strategy for the management of identity across business-to-business (B2B), business-to-employee (B2E), and business-to-consumer (B2C) operations, whether these services are delivered on premise, from the cloud, or federated with a trusted business partner.

A more sustainable approach, and a better way to consider IDaaS, is to recognize that it can and should offer the opportunity to streamline identity and access management and provide an enterprise-wide approach that deals with on-premise as well as cloud-based relationships. IDaaS technology is evolving but is still not mature. Nevertheless, the number of identity management vendors that now offer fully featured IDaaS is growing, as IDaaS specialists that started out delivering cloud-only solutions clash with early-to-market IAM platform vendors that see IDaaS as a natural extension to their core IAM portfolios.,

Therefore, to maintain and build on its early successes, the IDaaS community must begin to offer a balanced package of identity services that match the enterprise requirement of seamlessly and securely managing access to both cloud and on-premise systems.

Key findings

- The IDaaS market is relatively immature and continues to be led by the original group of specialist providers.
- IDaaS provides a mainly cloud and services-led approach to identity management using a hosted model to deliver core identity and access management services.
- IDaaS can offer a realistic, cloud-based alternative to maintaining IAM products on premise.
- A services-led approach to identity management is relevant to both public and private sector organizations and can meet the needs of most industry verticals.
- There were functional shortfalls in some first-generation IDaaS solutions that made them unfit for enterprise clients.
- Mainstream IAM providers were slow to recognize the need for an IDaaS strategy. Most are still playing catchup, and some will need to make acquisitions to get to the first rung on the ladder.
- Leading IDaaS providers offer a hybrid mix of identity management services that can support enterprise-wide operations.

Vendor solution selection

Inclusion criteria

IDaaS technology has to move on from a position of specialization where cloud usage and cloud service delivery were intrinsically connected. There are relatively few cloud-only businesses, and the majority of potential clients will have already deployed IAM solutions and have the supporting infrastructure services in place.

Some will be looking for a replacement strategy, and a few will be first-time users who see real possibilities in IDaaS. Most will be looking for a mixed, hybrid approach that brings together their on-premise and cloud-based operations to deliver an integrated set of identity management products and services. To achieve all these objectives requires IDaaS services to support mainstream B2E, B2B, and B2C usage and a full range of business and user demands. This includes most of the measures and facilities listed below:

- IDaaS technology needs to support multiple use cases, including cloud-only operations and a hybrid mix of cloud and on-premises systems, and must be capable of replacing or working alongside legacy, platform-based IAM tools.
- It needs the ability to support major client relationships including business-to-business (B2B), business-to-employee (B2E), and business-to-consumer (B2C), as well as machine-to-machine and IoT interactions.
- It should deliver core identity management services that include authentication, access controls, SSO, federated identity management, provisioning and de-provisioning services,

self-service registration and password management, directory integration and management, reporting, alerting and monitoring, and identity governance.

- It should have the ability to operate alongside and integrate with mainstream third-party IAM systems.

Exclusion criteria

There continue to be IDaaS specialists that focus only on particular disciplines, such as authentication-as-a-service, customer-facing identity management, or that only support cloud-based operations. Their coverage would be considered too narrow for this report. However, IDaaS continues to be positioned as an emerging business- and technology-focused approach to identity management and as such, some of the vendors included in this report cannot cover all areas of identity management without assistance from a technology partner. Vendors have been excluded if they:

- Only offer a narrow range of IDaaS services.
- Do not have the capacity or scale to deal with medium-to-large enterprise as well as small-to-medium business requirements.
- Do not have the facilities in place to work alongside mainstream technology partners in the identity management space.
- Do not have the maturity, revenues, or market presence to compete with the leading IDaaS providers.

Methodology

Technology/service assessment

In this assessment dimension, Ovum analysts have identified a series of features and functions that provide differentiation between the leading solutions in the marketplace. The criteria groups identified for IDaaS are as follows:

- IDaaS service delivery addresses service delivery capabilities for cloud, web, and on-premise requirements, and also covers key operational environments that need to be supported (B2B, B2E, B2C, M2M, and IoT), and the delivery of core identity management services.
- Authentication drills down into the capabilities supported, such as, for example, how one-time passwords (OTPs) can be generated and the approaches delivered, and the business and social mediums available.
- Single sign-on (SSO) covers the range of SSO facilities supported, its on-premise and cloud interoperability and threat protection capabilities, and its security controls.
- Federation and the range of facilities available are used to manage relationships between company and business partner networks, including the federation of SSO interactions.
- Provisioning facilities are provided and the services supported include de-provisioning and associated reporting and alerting services.
- Directory management facilities provide support for key directories that fall within the IDaaS and IAM criteria, along with associated requirements for directory synchronization.
- Reporting, alerting, and monitoring requirements and the levels of service that need to be maintained are considered.

- Management and infrastructure covers elements such as the range of applications supported with pre-written APIs, key industry standards supported, and the third-party IAM systems each IDaaS service can work alongside and integrate with.

Execution

In this dimension, Ovum analysts review the capabilities of the solution around the following key areas:

- Maturity: the stage that the product/service has achieved in the IDaaS maturity lifecycle is assessed here as it relates to the overall technology/service area.
- Interoperability and innovation: we assess how easily and how well the offerings and their forward-looking features are made available to allow them to be integrated within an organization's operational systems and services.
- Deployment: refers to a combination of usage and support elements that cover various deployment issues, including services, support, and update/release requirements.
- Scalability: points of referenceable achievement are used to show the scalability of the solution across small, medium, and large operational environments.
- Enterprise fit: covers the alignment of the solution to business requirements and the potential cost overheads identified.

Market impact

The global market impact of a solution is assessed in this dimension. Market Impact is measured across four categories:

- Revenues and growth: each solution's IDaaS revenues are identified and measured alongside the revenue growth that has been achieved over the last 12 months.
- Geographic penetration: existing revenues across four major trading regions: North America, South America (LATAM), Europe, the Middle East, and Africa (EMEA), and Asia-Pacific, are taken into account.
- Vertical penetration: this is determined by each solution's overall presence in the following industry verticals: banking, energy and utilities, education, investment services, healthcare, insurance, legal services, life sciences and pharmaceuticals, manufacturing, media and entertainment, professional services, public sector, retail, wholesale, and distribution, and telecoms, and travel transportation and logistics.
- Size-band coverage: this determines the presence each vendor has across small, medium, and large business operations.

Ovum ratings

- **Leaders:** This category represents the leading solutions that we believe are worthy of a place on most technology selection shortlists. Each vendor has established a commanding market position with a product/service that is widely accepted as best of breed.
- **Challengers:** Each solution in this category has a good market positioning and offers competitive functionality and good price-performance proposition, and should be considered as part of the technology selection.

Market and solution analysis

Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17

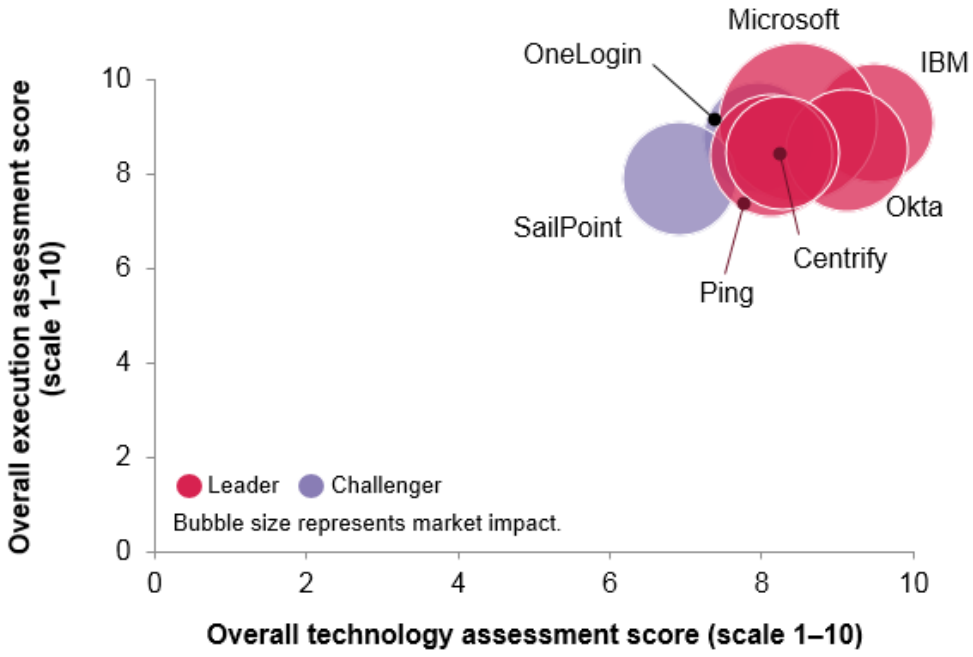
Identity-as-a-service (IDaaS) offers a viable alternative to traditional on-premise identity and access management (IAM) platforms. IDaaS efficiencies and cost-savings are relevant to most business operations, but not necessarily as a complete replacement for existing technology, because hybrid IDaaS and core IAM platforms can be deployed and coexist to the benefit of organizations and their users.

The emerging IDaaS market consists of two main groups: next-generation identity management providers such as Centrify, Okta, OneLogin, and Ping that came into being to deliver identity-based services from the cloud, and established IAM platform vendors, including IBM, Microsoft, and SailPoint, that have already gone some way toward developing their IDaaS strategies.

For the cloud-driven originators of IDaaS, the starting position was to deliver secure access to cloud-based services. The leaders in this market have now gone on to develop enterprise delivery strategies and services that support the hybrid identity management requirements of both on-premises systems and cloud-based applications.

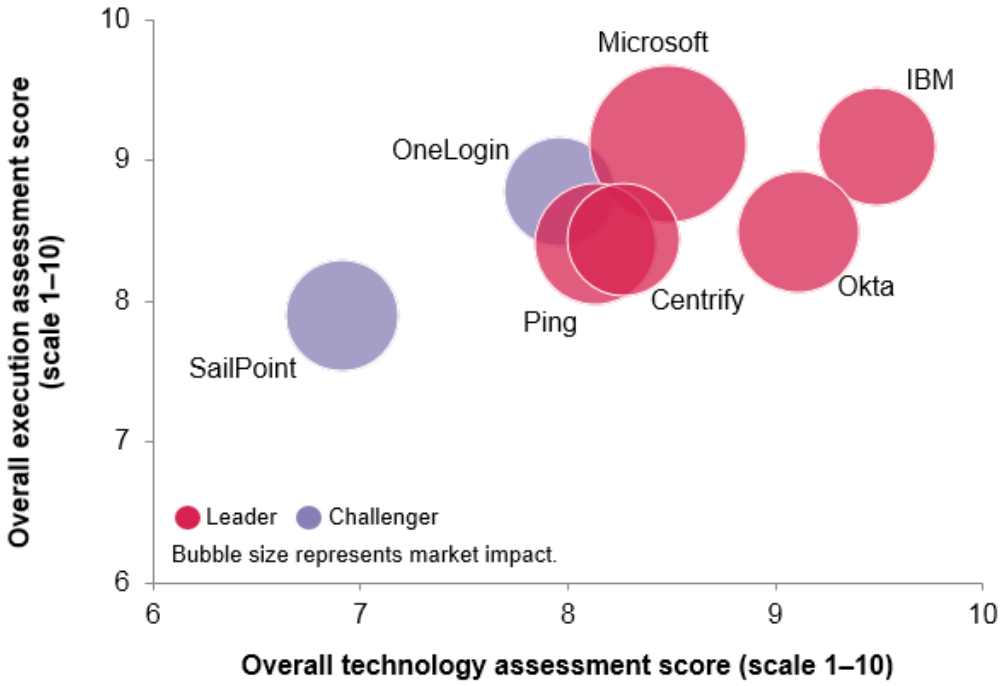
Established IAM platform vendors see IDaaS either as an opportunity to build new services and address new markets, or as a problem that threatens the status quo. Some have made an effective response and are developing technology solutions that operate alongside their on-premise facilities, either as an extension to the existing IAM infrastructure or as free-standing alternatives. Others were late to market, have more technology on their roadmap than in production, and will be playing catch-up for some considerable time.

Figure 1: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17



Source: Ovum

Figure 2: Expanded view of Ovum Decision Matrix: IDaaS 2016–17



Source: Ovum

Table 1: Ovum Decision Matrix: IDaaS 2016–17

Market leaders	Market challengers
Centrify	OneLogin
IBM	SailPoint
Microsoft	
Okta	
Ping	

Source: Ovum

Market leaders: vendor solutions

The market leaders group consists of an eclectic mix of cloud-focused identity management vendors: Centrify, Okta, and Ping. It also includes the established IAM platform provider IBM whose IDaaS credentials were established following the acquisition of Lighthouse and its IDaaS technology in 2014, plus Microsoft, which retains traditional IAM coverage but has a stronger and more natural sense of presence in the IDaaS community.

Centrify delivers its portfolio of identity management products and services from the cloud, and from the company's inception has maintained a cloud-first service delivery strategy. Its IDaaS approach covers its core identity management and its privilege management portfolios. For both products,

Centrify provides a multi-tenant, cloud-based, software-as-a-service (SaaS) solution. It offers context-aware and adaptive multifactor authentication, enterprise and federated SSO, provisioning and password management, and cloud and web-centric access control facilities.

IBM launched its IDaaS offering two years ago with the acquisition of the Lighthouse Security Group, and its Cloud Identity Service (CIS) continues to evolve to meet future identity management and business protection requirements. IBM CIS is now an integrated component of the company's IAM portfolio and supports its complete range of identity management, web access management, and federated identity management services.

Microsoft's IDaaS facilities are delivered using the company's Azure Active Directory products. As a pure IDaaS solution, Azure Active Directory provides SSO access to the cloud-based applications organizations choose to deploy. For hybrid environments, it delivers secure remote access to on-premise and web-based applications. Microsoft also provides integration with on-premise directories and connectors to synchronize with their cloud-based equivalents.

Okta is a cloud-native provider of IAM services. Since the company's foundation in 2009, all its identity-based services have been delivered from the cloud. It offers a full range of IDaaS products and services including directory controls and management, SSO, user and device lifecycle management that includes provisioning services, adaptive and multi-factor authentication (MFA), enterprise mobility management, and API access management.

Ping offers a comprehensive suite of IDaaS products that deliver a seamless approach to identity management across business and consumer environments. Its identity-as-a-service capabilities provide secure access to all supported applications, and federated management extends control so that organizations can manage inter-company relationships and provide secure access to shared applications, resources, and services. Ovum is particularly encouraged by the recent expansion of its consumer identity capabilities with the acquisition of UnboundID.

Market challengers: vendor solutions

As was the case for the leaders group, the challengers consist of an IDaaS specialist (OneLogin) and a vendor that straddles the divide between core IAM platform services and a next-generation approach to IDaaS (SailPoint).

OneLogin has from its inception been a cloud-based IAM vendor, with identity management delivered using an IDaaS approach. The company started out providing identity-based access to cloud applications for SMEs, but has since expanded into a full-fledged IDaaS platform, and its customer base now also includes large enterprises. It supports a full range of business-to-employee (B2E) and business-to-business (B2B) identity services and is looking to add more business-to-consumer (B2C) features.

SailPoint is an established provider of IAM technology. It started out with an on-premise software product in the second half of the last decade, and in 2013 added IdentityNow a cloud-based service product. IdentityNow offers a full IAM service in the cloud, with user provisioning, SSO (including support for federated SSO), password management, access certification, and data governance features.

Emerging vendors

Table 2: Emerging vendors: IDaaS 2016–2017

Amazon Web Services (AWS)	Janrain
CA Technologies	Oracle
Gigya	Salesforce.com (SFDC)
Google	VMware

Source: Ovum

The emerging vendors section looks at companies that did not make it onto the list of those subjected to our full examination for the vendor comparison process, but that we nonetheless consider worthy of our readers' attention. For example, two IAM incumbents, CA and Oracle, are moving into the IDaaS market, but were not quite ready to submit to the full comparison process. Smaller, dedicated IDaaS players that focus primarily on the business-to-consumer side of the market and describe what they provide as customer identity and access management (Janrain) or customer identity management (Gigya) are included here. The final group includes major industry players that are neither traditional IAM vendors nor IDaaS startups, but which by virtue of their clout elsewhere in the hi-tech sector are well placed to move into cloud-based identity management. These include Amazon Web Services, Salesforce.com, Google, and VMware.

New entrants

CA Technologies recognizes that a growing number of its business clients require full-featured IAM services that can be delivered from the cloud. Its new IDaaS facilities, which at the time of publication of this report were being released, will offer authentication, provisioning, and entitlements management, SSO services, and access controls that support the hybrid mix of on-premise and cloud-based services that most organizations have deployed.

Oracle has been looking toward the development of an IDaaS offering for some time, but didn't actually launch its Identity Cloud Service (IDCS) until September 2016. IDCS was designed specifically as a cloud service and is an extension of the company's Oracle Identity Manager (OIM) product. It isn't, however, the finished article, and the company will continue to add features over the next 18 months. IDCS is designed to work independently and alongside on-premise IAM technology from Oracle and third-party IAM vendors.

Smaller, dedicated B2C players

Gigya offers three levels of its Customer Identity Management (CIM) service, positioning it strongly on the B2C side of IAM. Its basic identity service comprises social login/plugin facilities; profile management; password-less mobile authentication; roles and permissions; analytics; customer insights; identity access for managing high volumes of user records; and identity compliance with support for privacy legislation. Identity Plus adds to the above with registration-as-a-service; customer insights plus; and progressive and conditional profiling. Identity Enterprise then adds a data storage feature for user-related data; federation; two-factor and risk-based authentication; signals to define and track on-site activities; auditing; and SSO.

Janrain provides customer identity and access management (CIAM), positioning it on the B2C side of IAM. Delivering IDaaS-based CIAM technology from the cloud, Janrain offers six distinct products: Social Login, which enables website and mobile users to log into a company's site; Registration, which provides the tools to acquire customers across all web and mobile properties; Profile Data Storage, which enables companies to collect, store, and manage data; SSO for single customer registration and login; Engagement to promote real-time conversations; and Customer Insights, which provides dashboards to visualize and segment customer data.

Major industry players

Amazon Web Services (AWS) is the market leader in cloud infrastructure services, with 10 times more computing capacity than the next 14 cloud providers combined. In 2010, the company added IAM services to help its expanding customer base manage secure employee access to AWS instances. AWS, with its IDaaS approach to identity management, enables customers to manage access to compute, storage, database, and application services in the AWS Cloud.

Google is an established player in identity management, insofar as it has 1 billion people logging into Google accounts around the globe supported by the use of social login/social sign-in facilities. From an enterprise perspective, its IDaaS credentials are less well established, but are specifically focused on the vast business-to-consumer (B2C) market. This also explains its research into and strong interest in the usability for consumers of stronger authentication methods, and the usability of federated sign-in options.

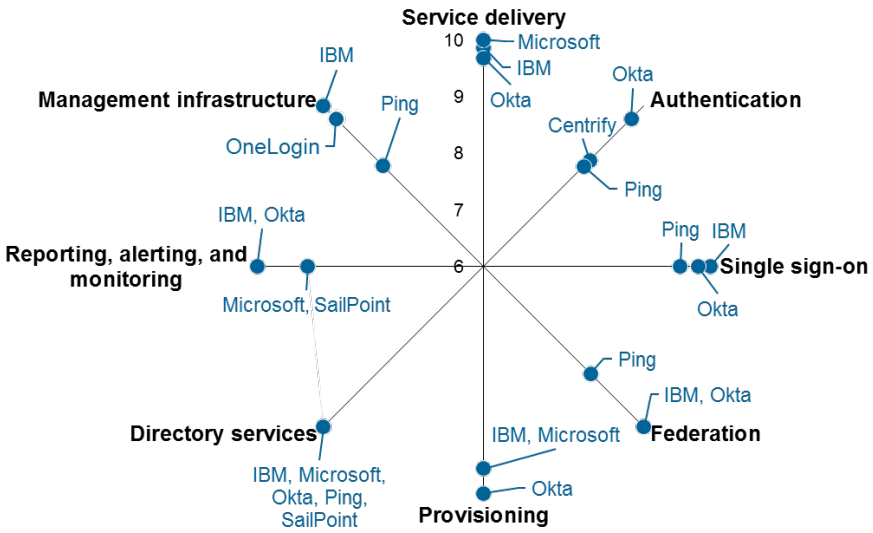
Salesforce.com (SFDC) has been in the IDaaS market since October 2013, when it launched the Salesforce Identity service. Its services are targeted at all the major use cases of identity management including business-to-employee (B2E), business-to-business (B2B), and business-to-consumer (B2C). Its plan is to enable CIOs to deliver a simple, productive, and customized user experience across all available web, mobile, and on-premise applications.

VMware's VMware Identity Manager delivers the company's identity-as-a-service (IDaaS) offering. It is available as part of VMware Workspace ONE and provides secure access to corporate applications across all supported devices and platforms. It delivers SSO access to the cloud, as well as a range of web and native applications; portal access to employee applications; and conditional access to business applications based on the device, network, and user. It also offers application provisioning and self-service catalog facilities, and AirWatch technology adds to the company's IDaaS proposition and brings mobility and mobile access into the equation.

Market leaders

Market leaders: technology

Figure 3: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17, Market leaders – technology



Source: Ovum

Centrify provides IDaaS technology services for IAM and PAM environments, and while its multi-tenant, B2B, B2E, and B2C approach to IDaaS saw it score well across most technology areas, it only made the market leader grid for authentication where it appeared alongside Okta and Ping.

IBM CIS addresses serviceability with a mobile-first approach that supports ongoing change management requirements in fast-moving business environments. Its IDaaS solution includes the same depth of identity management, web access control, and federation that are found in the on-premise platform version of its IAM technology. As a result, IBM was a consistently strong performer across most of the listed IDaaS technology components and appeared on the leader board for service delivery, SSO, federation, provisioning, directory services, reporting/alerting/monitoring, and management infrastructure.

Microsoft with its Azure Active Directory technology provides portal-based access to services and applications for all user types and was successful on the leader table across half of the major technology components, including service delivery, provisioning, directory services, and reporting/alerting/monitoring.

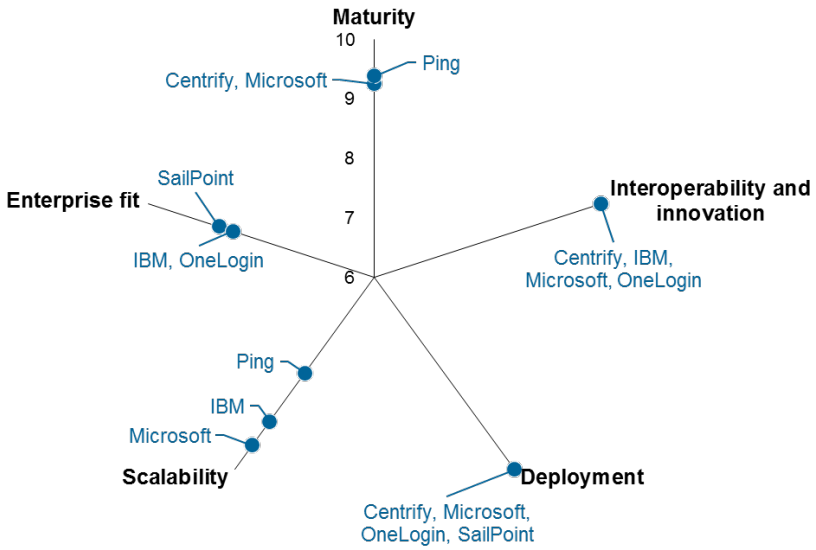
Okta provides a full IDaaS platform offering and continues to add essential new functionality. This approach shows up well in the technology leaders section, with Okta appearing in the top group in every area apart from management infrastructure. Ping, which has similar cloud-based origins, performed almost as well, with leader group appearances for authentication, SSO, federation, directory services, and management infrastructure.

OneLogin has an established reputation for covering all the basic components of an IAM platform when delivered from the cloud, particularly in the areas of provisioning, SSO, authentication, and federation. It scored well in all these areas, but was just outside the leading positions and only featured in the top group for management infrastructure.

SailPoint, which brings a decade of solid performance in the IAM market to the IDaaS arena, is primarily seen as an enterprise player, but it only made the top three for directory services and reporting/alerting/monitoring.

Market leaders: execution

Figure 4: Ovum Decision Matrix: Identity-as-a-Service (IDaaS) 2016–17, Market leaders – execution



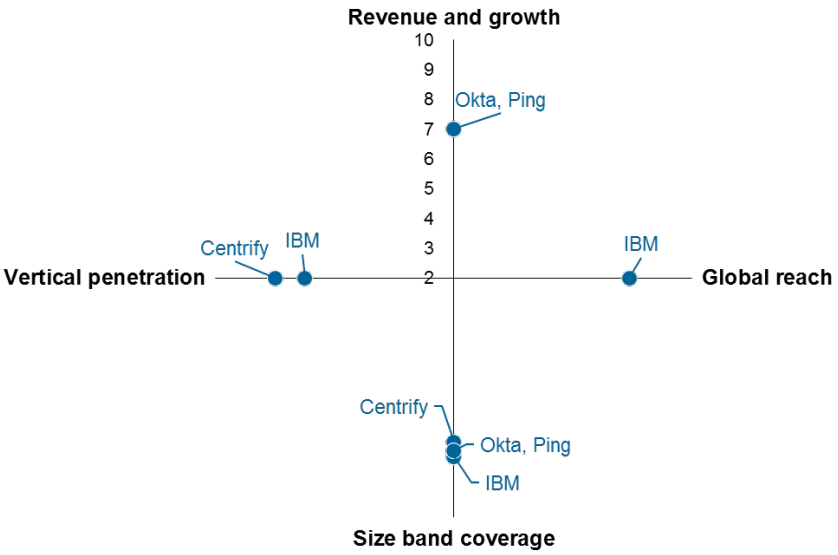
Source: Ovum

The market execution section focused on the key areas of product and services maturity, interoperability and innovation, deployment of service, scalability, and enterprise fit. Not surprisingly, most of the leaderboard (top three) positions in these key areas for business were taken up by the IDaaS market leaders. Microsoft led the way, appearing in four out of the five sections (maturity, interoperability and innovation, deployment, and scalability). Centrify (maturity, interoperability and innovation, and deployment), IBM (interoperability and innovation, scalability, and enterprise fit), and OneLogin (interoperability and innovation, deployment, and enterprise fit) featured as leaders in three out of the five categories.

The remaining leadership positions were shared between Ping (maturity and scalability) and SailPoint (deployment and enterprise fit).

Market leaders: market impact

Figure 5: Ovum Decision Matrix: Identity-as-a-Service 2016–17, Market leaders – market impact



Source: Ovum

The main areas of focus within the market impact section were on revenue and growth, global reach, size band coverage, and vertical penetration. All of these are extremely relevant measures of success in emerging markets such as IDaaS, where take-up and use in the business community is growing but remains at the early-adopter stage of the business usage lifecycle.

Combining revenue and growth provided some interesting results, with most vendors able to report year-on-year growth figures that exceeded 25% over the last financial year. However, in most cases, growth was measured against previously modest sales figures. Therefore, for all but the market leaders, performance levels were held back by the actual revenues involved. The two vendors that clearly outperformed the rest were the long-established IDaaS vendors Okta and Ping, both of which were able to maintain high levels of growth alongside revenue figures well above market average.

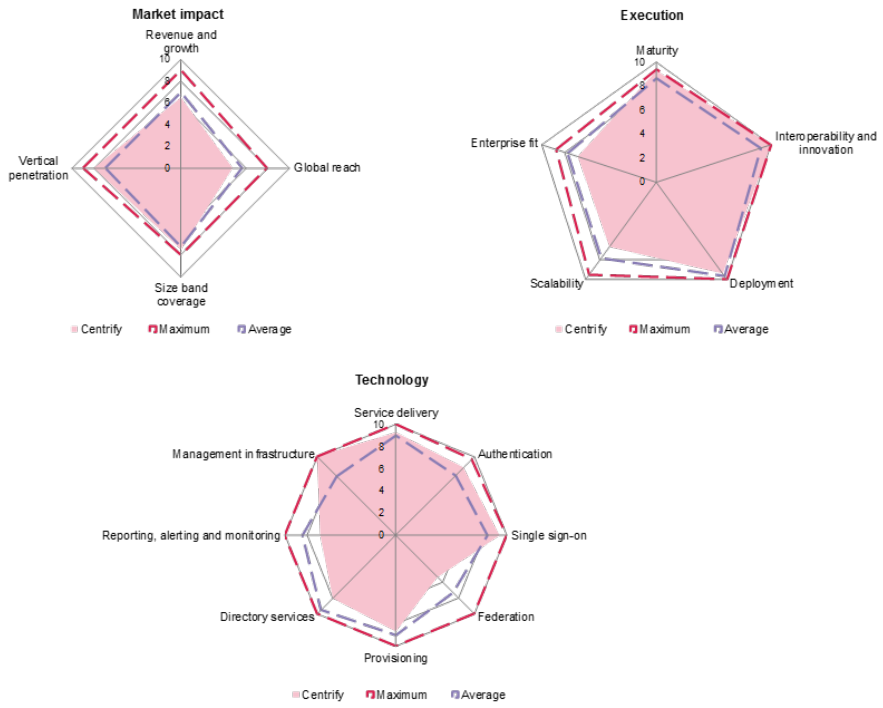
Global reach was also an area where most struggled to establish a strong position. Only IBM was able to confirm an established and even split of sales across the four key regional markets of North America, South America, EMEA, and Asia-Pacific. Others appeared to have a strong US marketing bias and some had very little presence in other areas.

Size band coverage provided a stronger position for a fair proportion of the vendors, with Centrify, IBM, Okta, and Ping having a good split of clients across small, medium, and large enterprise markets. Two of these three vendors, Centrify and IBM, were also able to quantify their vertical penetration position across the key industry verticals specified for the report.

Vendor analysis

Centrify (Ovum recommendation: leader)

Figure 6: Centrify radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Security is at the center of the Centrify approach to IAM

Centrify's IDaaS architecture has been built from the ground up to address the protection requirements of all its users, with the emphasis on maintaining secure access to their data. Its secure cloud-based infrastructure doesn't expose, store, or log users' Active Directory (AD) credentials, or unnecessarily replicate any AD or customer data to support its operations.

Centrify IDaaS delivers identity and privileged identity services

Centrify provides two main products for the IDaaS market. Its Identity Service offers a full-featured SaaS approach and is aligned with the company's well-respected EMM mobile and Mac management solution. Its Privilege Service also offers a SaaS solution that manages shared and privileged account management in the PAM environment.

Portal-based facilities simplify access for business users

A customizable and cloud-based user portal provides one-click access to web and SaaS applications for business users with B2E relationships. It provides user self-service for mobile devices, improves visibility over users' AD account attributes, delivers activity reports detailing personal usage to help

identify suspicious activities, and provides self-service account management to deal with locked accounts and password resets.

B2B and B2C relationship management extends coverage to business partners and social environments

B2B federation capabilities allow business partners to federate their own identity provision with Centrify, enabling Centrify's clients to share approved applications and resources without the need to manage partner identities. B2C services support social login and self-service sign-up from key providers such as Facebook, Google, LinkedIn, and Microsoft.

Weaknesses

Centrify doesn't have a strong enough position in IoT and M2M management

Centrify has built its functionality within the IDaaS space to extend from its core B2E position, and it now also supports B2B and B2C relationships. However, progress in the important areas of Internet of Things (IoT) and machine-to-machine (M2M) management hasn't received a similar boost, and this appears to be especially true on the privilege side.

Opportunities

Up to a quarter of all business data interacts directly between originating device and SaaS-based applications

As growing volumes of data flow outside traditional on-premise network infrastructures, a more inclusive approach to user and data protection is needed. This by implication puts greater emphasis on the need for identity-based controls that can provide secure and measurable access to all information resources. Specifically, this would include service providers such as Centrify that can deliver safe access over public networks to commonly used cloud services such as Microsoft Office 365, Amazon Web Services, Google, Salesforce.com, and Box.

Mobile and cloud are the key drivers for the next generation of customer-facing IAM services

Mobility and cloud (mobile device and access channel of choice) are important usability drivers, especially in the consumer space. For this sector in particular, mobile devices are also increasingly used to support and deliver MFA. Scale and flexibility are the key issues when organizations select an IDaaS provider capable of dealing with their consumer-facing IAM requirements and the fast-moving nature of the apps that support these services.

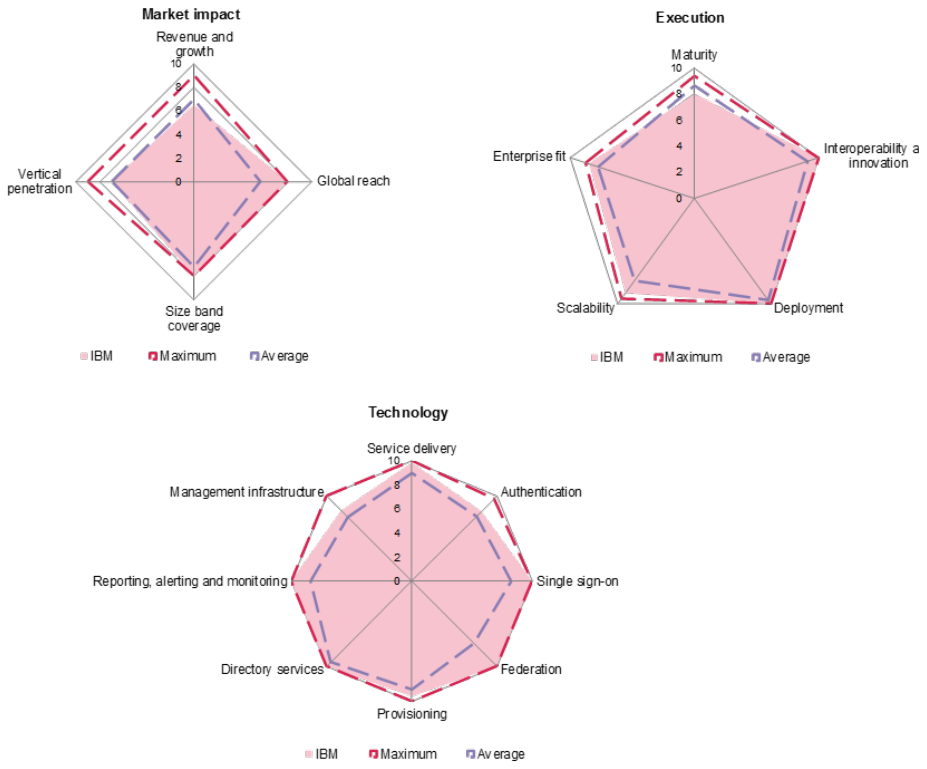
Threats

Not all organizations are ready for identity to be delivered from the cloud

Centrify leads the market in its strategy to deliver everything within the identity and privileged account management arena from the cloud. While the enterprise direction of travel continues to be toward the delivery of identity from the cloud, a significant number of organizations still see cloud-based identity and privilege management as a step too far.

IBM (Ovum recommendation: leader)

Figure 7: IBM radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

IBM Cloud Identity Service deals with cloud, on-premise, and the hybrid mix

IBM Cloud Identity Service is targeted at organizations that want to deploy IAM as a complete set of IDaaS cloud-driven facilities. It also has the enterprise functionality and alignment capabilities to operate in combination with IBM's existing on-premise infrastructure, extend operations out to the cloud, and deliver hybrid enterprise requirements.

An inclusive set of identity and access management services are on offer

IBM Cloud Identity Service identity management components offer enterprise scale provisioning and de-provisioning, self-service management, governance, user monitoring, analytics, and security intelligence. Web access management provides multi-factor, risk-based, and step-up authentication as well as auditing and user authorization services, and its federation services deliver federated SSO and federated provisioning services.

Global and local SoftLayer datacenter platforms support the IDaaS operation

SoftLayer infrastructure-as-a-service (IaaS) datacenter platforms provide global and local coverage for the service. They offer broad geographic coverage and availability that help clients address

security and data privacy regulations, including industry and local requirements, and assist in overall performance by reducing local latency.

Weaknesses

IBM needs to grow IDaaS sales beyond the enterprise

The natural comfort zone for IBM IDaaS is large enterprise, including its own IAM customer base. It needs to extend to include a wider variety of SaaS and PaaS buyers, including SMBs, line-of-business decision-makers, and developers, and in what is becoming a highly competitive sector of IAM, success will also be measured by take-up from beyond the enterprise.

Opportunities

IBM's established expertise in the security and IAM markets helps deliver its IDaaS services

The delivery of IDaaS services needs the support of industry experts. IBM's long and established expertise in the security and identity management markets puts it in a strong position to develop and support the types of IDaaS services that will address the next-generation identity protection and usability demands of enterprise clients.

There are future convergence opportunities on the IDaaS roadmap

IBM already has a full stack of IAM services available. However, further integration and convergence opportunities have been identified for its roadmap strategy, including integration with QRadar intelligence services, convergence with IBM's Fiberlink MaaS360 mobile device management (MDM) to deal with mobile access, and shared information flows with cloud access security broker (CASB) technologies, including IBM's own Cloud Security Enforcer product.

Threats

Agility and the need to support cloud and hybrid services can add unwanted complexity

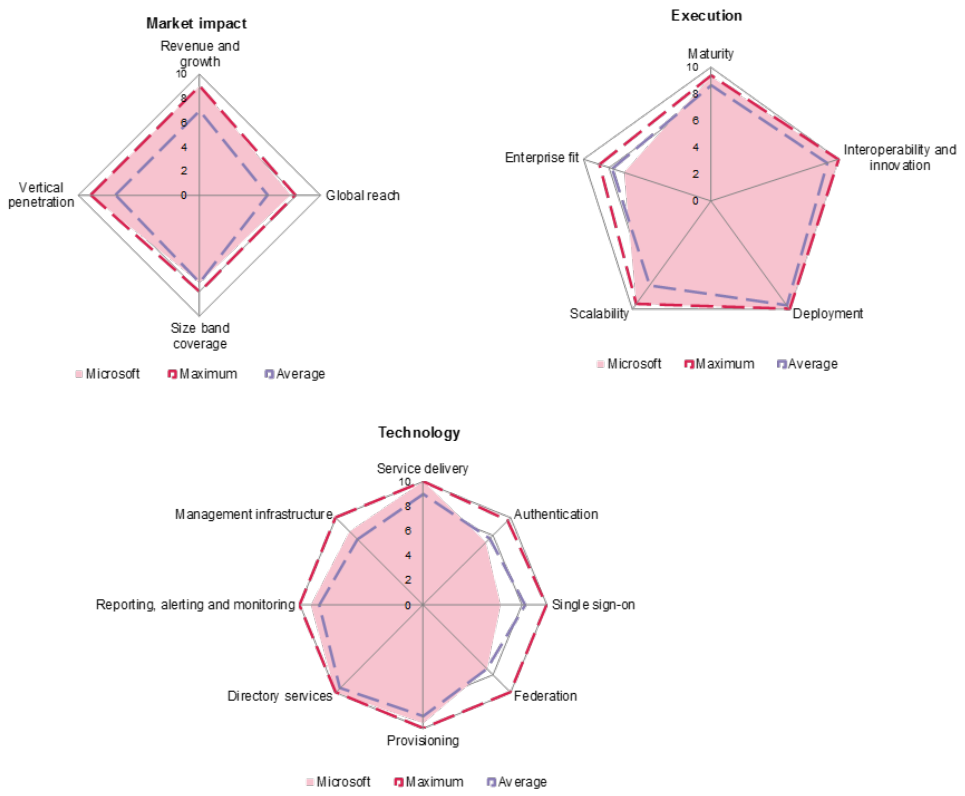
The IDaaS message from IBM is one of technology completeness alongside the ability to support an often complex mix of hybrid enterprise deployments. Others are going for the simplicity of use and deployment message, which during new business competitions can sound like a more compelling message. Increased focus is needed on how IBM will compete with the newer IDaaS players and their lightweight operational structures.

IDaaS pricing is becoming more competitive

Downward market pressures on pricing from the newer generation of IDaaS providers is putting pressure on the pricing structures of established players such as IBM and its mainstream competitors.

Microsoft (Ovum recommendation: leader)

Figure 8: Microsoft radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Microsoft Active Directory provides a single infrastructure for IAM

Microsoft provides pure cloud as well as a hybrid mix of cloud and on-premise IDaaS solutions that support the whole spectrum of B2E and B2B, and more recently B2C relationships. Cloud-controlled Azure Active Directory components provide portal-based access to services and applications for users and for the administration layer. On-premise bridging components are available to support directory management and directory synchronization between on-premise directories and their cloud-based equivalents. Browser and application plugins support user mobility for SSO access including the use of multi-factor and risk-based authentication.

Access management remains a key service deliverable and business protection requirement

Conditional access management is enforced using rule- and policy-based controls. These controls continue to be positioned as core business protection requirements for its clients and are key components of the Microsoft approach to IDaaS. Its facilities focus on user and device authentication, which is of particular relevance given the increasing number of mobile devices in use. This also extends to user and device compliance with usage policies, application and data sensitivity, and the associated monitoring of everyday usage patterns.

Business-focused security and user protection are core components of Microsoft's IDaaS strategy

Microsoft Azure Active Directory supports the use of risk-based, multi-factor authentication. This ties in with its support for strong access control facilities and helps deal with mobility issues and user-based controls over the devices and access channels being used. Issues such as the health and security of each device, user location when requesting access, and associated risk-based calculations (that cover issues such as the sensitivity of the data being accessed) are also being addressed. An identity and risk score is calculated for users each time an access request is made, and security alerts and reports are generated when unacceptable usage trends are identified.

Weaknesses

On-premise components appear to be the poor relation as Microsoft focuses on cloud connectivity

For on-premise identity management requirements, Microsoft offers its Identity Manager solution at no additional cost. Microsoft Identity Manager synchronizes identity between directories, databases, and applications. It provides the self-service management of passwords, user groups, and certificates; and has policy management, systems administration, and security responsibilities. However, it appears subservient to the next-generation IDaaS components.

Opportunities

IDaaS is a maturing segment of the IAM sector and Microsoft continues to build its market presence

Previous versions of Azure Active Directory focused on B2E and B2B requirements. This left a significant shortfall in the increasingly important and rapidly evolving B2C identity management space. This issue was addressed in 2015 and further developments were undertaken to deal with scalability and access control requirements for B2C coverage.

Active directory credentials can now be used to access virtual machine environments

Azure Active Directory Domain Services now supports access to virtual machines without the need to deploy domain controllers. Users that sign in to Linux and Windows virtual machine environments can use their corporate active directory credentials to provide seamless access to approved corporate assets. These approved assets are maintained using group policy controls and are based on role and departmental requirements.

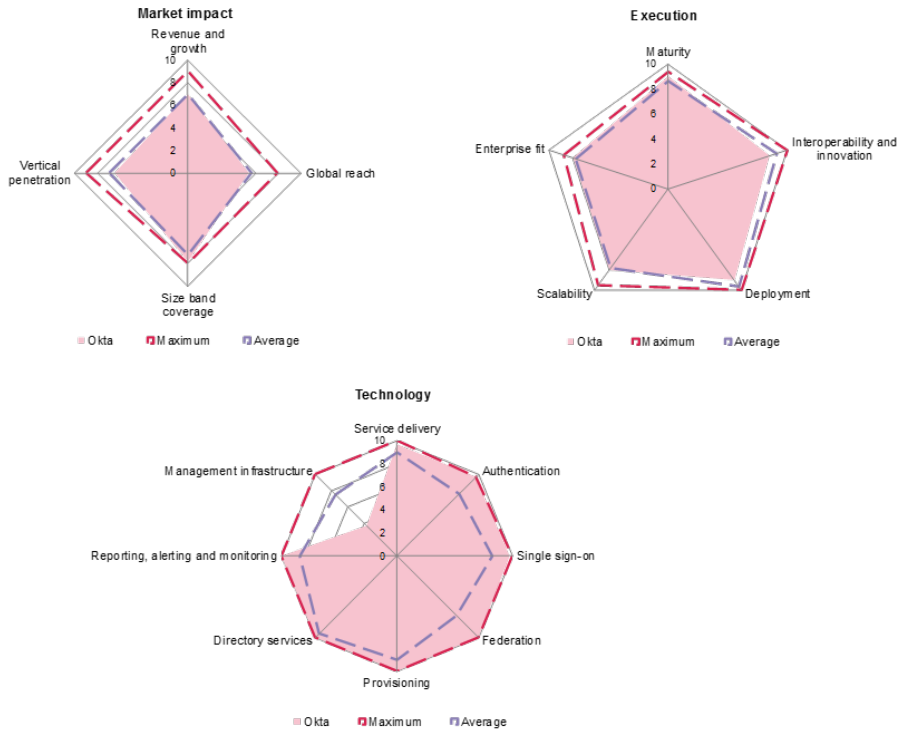
Threats

The company is still mainly perceived as a supplier of Microsoft-centric technology

Although Microsoft Azure Active Directory has been available for the last three years and its cloud directory services for at least five years, the perception remains that its identity management platforms, particularly its IDaaS services, are mainly Microsoft-centric. The company is looking to address these issues through its move to open SSO access to any cloud and its support for open protocols via its Azure Active Directory Free, Basic, and Premium editions.

Okta (Ovum recommendation: leader)

Figure 9: Okta radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

Okta covers all major IAM requirements

With provisioning, SSO, reporting, social login, identity federation, and authentication, Okta delivers all the main elements of an IAM infrastructure from the cloud. It facilitates out-of-the-box integration of its technology with cloud and on-premise apps and provides tools for third-party developers to integrate Okta into their applications.

Okta is dedicated entirely to IDaaS

Okta is not an enterprise application developer that has identity as an add-on, making it agnostic to whatever applications its customers use it to access. It architected its product from the outset for cloud delivery and so has had none of the issues of migrating an on-premise product or customer base to an "as-a-service" mode of operation. It claims the scalability to handle hundreds of millions of users.

Weaknesses

CIAM functionality should be more visible

Okta approaches CIAM by providing the foundation on which key CIAM features such as registration can be enabled through the application programming interface (API). While it produces a data stream

of identity events available for any analytics system/data warehouse, it argues that there are better tools for customer analytics than CIAM platforms because identity-related data is just one data stream of many. This is a reasonable stance, but Ovum feels it should go further to highlight its CIAM capabilities, for instance by adding registration as an out-of-the-box feature. We note that this particular capability is clearly a high priority on Okta's roadmap, and look forward to seeing it as part of the service offering in the near future.

Okta has no legacy IAM customer base

On-premise IAM heavyweights such as IBM, Oracle, and CA are moving into the IDaaS market. They have significant on-premise customer bases, which they can either migrate across wholesale over time or sell IDaaS to as an add-on capability for new greenfield projects. This option is not open to Okta, putting it at a competitive disadvantage for these accounts.

Opportunities

"Cloud-first" companies are drawn to IDaaS

Many start-ups come into existence nowadays with a "cloud-first" bias for technology acquisition. Therefore, for them, a SaaS platform for identity is clearly preferable to one that requires software to be licensed and deployed on their premises. The same goes for small greenfield projects within larger corporations, where Okta's ability to interact with on-premise corporate assets serves as a further incentive to consider its services.

The cloud is now a mainstream delivery mechanism for identity

The delivery of identity services from the cloud has become a serious alternative to on-premise IAM, particularly for start-up companies that need the benefits of identity management without the financial and operational overhead of running software in their data centers. Many large companies also approach Okta seeking the agility, scalability, and versatility offered by the cloud. Okta already has brand recognition as a leader in this space.

Threats

Okta should do more to highlight its B2C capabilities

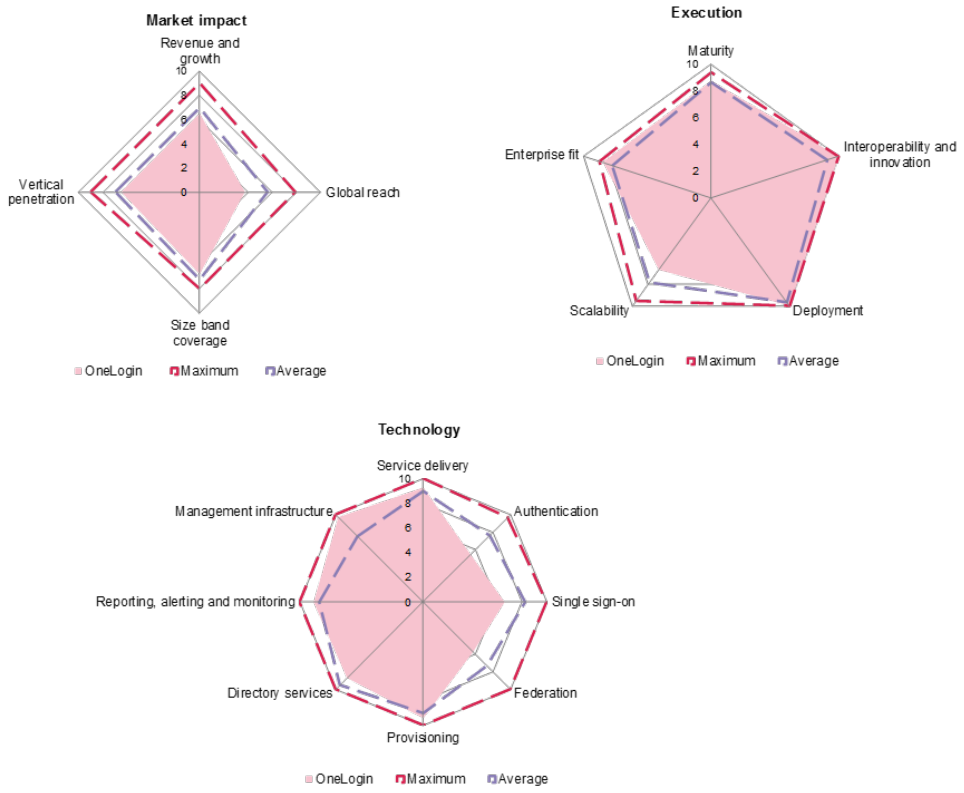
IAM started life in B2E identity services, with globalization and outsourcing taking it into the B2B sphere. The next stage is the move into B2C because customer interactions are increasingly online rather than face-to-face. Other vendors are touting their ability to address B2C requirements, and while Okta has made a good start by supporting social login, it should now productize its innate CIAM capabilities to show it is also in this market.

New IDaaS challengers come with many customers in other areas

As IDaaS becomes a serious contender for enterprise budgets against on-premise software, major players in the latter market segment are adding an IDaaS option to their technology, either by tweaking their existing platform, building an entirely new one, or buying one. Okta's ability to grow in this more competitive market may be constrained as new challengers come in with large customer bases they can leverage to expand their IDaaS business.

OneLogin (Ovum recommendation: challenger)

Figure 10: OneLogin radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

OneLogin has all the basic elements required for IDaaS

The OneLogin service is a full IDaaS offering, comprising a unified directory, identity bridging (to Active Directory, for example), user provisioning, SSO, MFA, web access management, mobile identity, device management, compliance reporting, and integration with the leading SIEMs. The company has recently moved to facilitate users' access to applications that do not support the SAML standard by acquiring password management vendor Portadi whose technology it is now adding to its platform.

OneLogin is exclusively an IDaaS vendor

OneLogin has designed and built its services for the cloud. It therefore has no legacy on-premises IAM customers and no on-premise revenues to protect. It is also solely focused on IDaaS, and so it has no other applications business, making it agnostic when it comes to connecting to enterprise applications.

Weaknesses

OneLogin lacks B2C features

OneLogin needs features for clients to manage interactions with their online customers to address the coming wave of customer IAM (CIAM), such as registration and customer behavior analytics.

Other IDaaS vendors have deeper pockets

OneLogin remains privately held and has raised a total of $42.7m. Its most recent funding round was a $25m Series C in December 2014. This compares unfavorably to the $228.5m raised to date by its largest direct competitor in IDaaS, Okta, which is currently exploring the potential for an IPO. Meanwhile, another big name in IDaaS, Ping Identity, was taken private in a $600m deal earlier this year, and it has already begun to make acquisitions. These developments make expansion for OneLogin beyond vegetative growth more challenging.

Opportunities

Cloud is the direction of travel for IAM

There is a growing requirement for identity services for employees, partners, and customers across multiple device types, and for accessing an ever-increasing number of applications. Cloud is the logical place for such functionality to reside, and the OneLogin platform is "cloud-native." There is particularly strong demand from start-ups and other small companies for IAM as a cloud service, but greenfield projects within larger enterprises may also prefer the convenience of IDaaS.

OneLogin is an established name in a growing market

The market for identity services delivered from the cloud is expanding, and OneLogin is already an established player that stands to benefit if it can keep pace with emerging new requirements and fend off competition from some of the IT heavyweights now moving into the space.

Threats

Other IDaaS platforms are adding CIAM capabilities

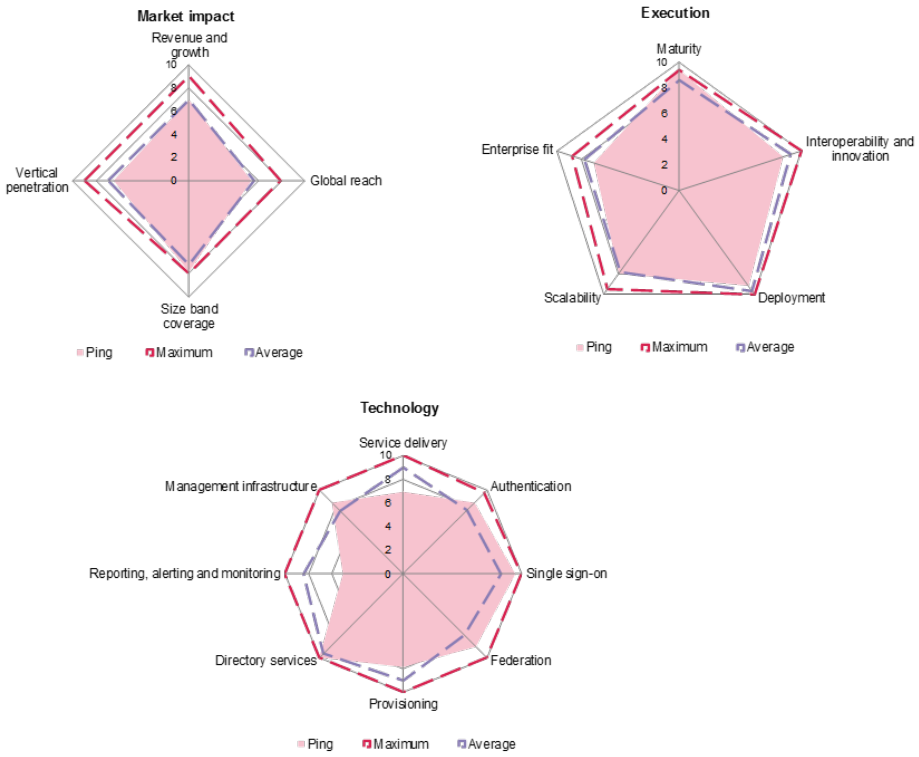
The OneLogin platform is already a broad IAM platform delivered from the cloud, as the company's 2,000 or so enterprise customers can testify. However, if it is to address the growing requirement for IAM to handle customer identities and access requirements, additional functionality will be required. One of its direct competitors, Ping, has recently acquired CIAM specialist UnboundID, and Ovum believes OneLogin needs to build or buy to keep up.

IT industry majors are moving into IDaaS

OneLogin is increasingly facing competition from larger IT industry players that are moving into the sector, such as IBM, Oracle, and CA. These companies are looking to leverage their extensive customer bases to get into IDaaS, a move that threatens to lock out OneLogin from these accounts.

Ping (Ovum recommendation: leader)

Figure 11: Ping radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

PingOne Cloud has all the elements for a fully-fledged IDaaS service

PingOne Cloud includes provisioning, SSO, MFA, directory integration, and application cataloging, making it a full IDaaS offering.

Ping is cloud-native and has just added CIAM

Ping Identity started out in 2002, enabling identity federation with its PingFederate server technology, with federation the foundation for intercompany IAM (the business-to-business or B2B side of the business). The company has since grown its platform, launching a full-blown IDaaS offering in 2012. In August this year it rounded out its CIAM capabilities with the acquisition of UnboundID.

Weaknesses

UnboundID is not yet integrated into PingOne Cloud

While Ovum applauded the acquisition of UnboundID as positioning Ping to address the expanding requirement for CIAM and to potentially span the worlds of CIAM and traditional B2E/B2B identity management with a single platform, the company now has to integrate the UnboundID technology into its own. Ping needs to carry out this process successfully and speedily for the acquisition to be a success.

Competition in IDaaS is heating up as IT majors enter the fray

The IDaaS playing field is changing. IT industry giants like IBM and Oracle are moving into the space, seeking to leverage their extensive enterprise relationships and their large customer bases in on-premise IAM. This development threatens to limit the potential for further growth for smaller vendors such as Ping, limiting their ability to penetrate enterprise accounts where there is an IAM incumbent but the customer is considering IDaaS for a new business unit, for example. Equally, companies with no legacy IAM infrastructure may be customers of the IT majors in another area of technology, representing an opportunity for them to upsell identity services.

Opportunities

PingOne Cloud benefits from a growing need for IDaaS

Ovum believes IDaaS is destined to become a major part of the IAM world, over time dwarfing on-premise software as companies move to cloud-based identity services to manage not only their employees and business partners, but increasingly also their online customers. As a full IDaaS offering, PingOne Cloud is well positioned to take advantage of this trend.

Cloud-based IAM is expanding into B2C

The cloud has become the logical place to locate identity services now that more and more enterprise applications are residing there, and access to these applications comes increasingly from outside corporate networks in the hands of remote workers, partner companies, or consumers. This trend favors providers such as Ping, and its recent acquisition of UnboundID positions the company particularly well to ride the next wave of IAM development as identity services are increasingly turned to the B2C environment.

Threats

PingOne Cloud needs to develop fast to stay ahead of the competition

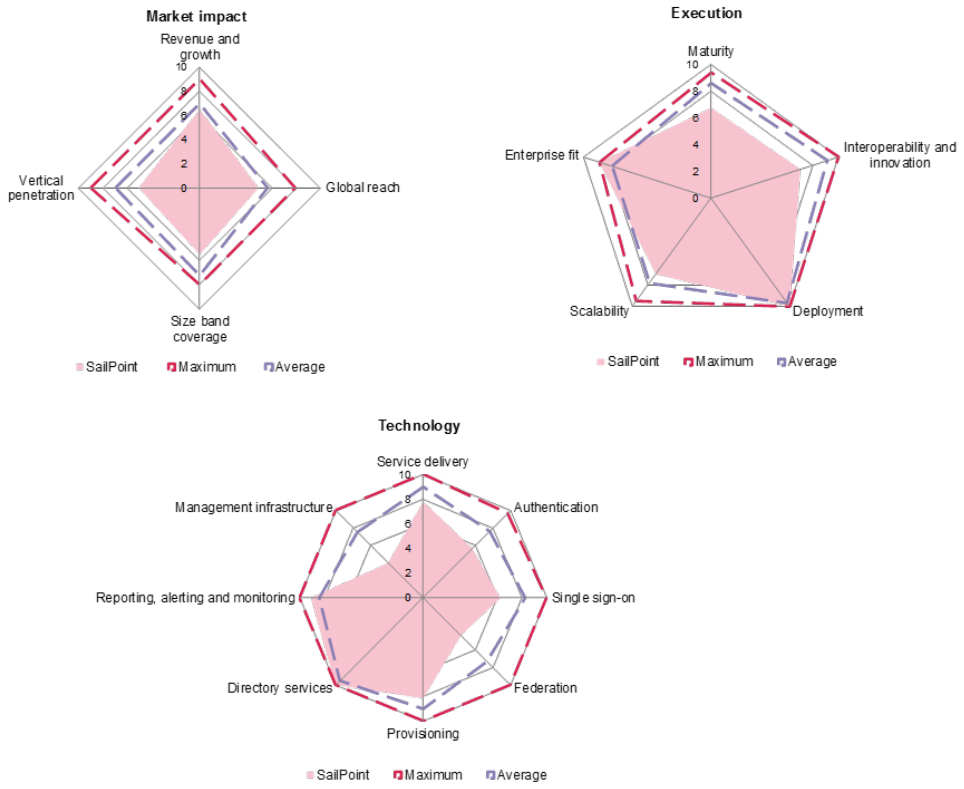
Ping Identity is a significant player in the IDaaS market, but still relatively small compared to some of the IT industry heavyweights now entering the fray. The challenge is therefore to keep PingOne Cloud up to date with the latest trends in the market, whether by internal development or by acquisition, as has just happened with the additional CIAM capabilities it got when it bought UnboundID. The company must maintain its momentum in adding new functionality to the platform lest it be overtaken by some of the larger competitors with bigger development budgets.

Competition in IDaaS is heating up as IT majors enter the fray

Ping was taken private in July this year for $600m and puts its customer base at around 1,400 enterprises. This makes it a major player at this stage in the development of the IDaaS market, but the playing field is changing. A number of IT industry giants including IBM and Oracle are moving into the space, seeking to leverage their extensive enterprise relationships and their large customer bases in on-premise IAM. This development threatens to limit the potential for further growth for the cloud-native IDaaS vendors such as Ping.

SailPoint (Ovum recommendation: challenger)

Figure 12: SailPoint radar diagrams



Source: Ovum

Ovum SWOT Assessment

Strengths

IdentityNow inherits SailPoint's experience with IdentityIQ

IdentityNow is a full IAM service in the cloud, with user provisioning, SSO (including support for federated SSO), password management, and access certification. With its IdentityIQ on-premise product having been in existence for the last decade, the company is transferring functionality across to its cloud platform.

SailPoint is an established IAM player

SailPoint has been in operation in the IAM market for a decade, selling to corporate entities with employee headcounts of at least 2,500. It has enterprise customers on both the on-premise and cloud sides of its business, including eight of the top 10 global banks and four of the 10 largest pharma concerns. This positions it to gauge whether existing on-premise customers want cloud-based identity services on any greenfield projects, for instance.

Weaknesses

IdentityNow is still B2E and B2B

The IdentityNow service started out with enabling companies to identify their employees and provide them with access to corporate assets (B2E). It is now also used to provide IAM services to partner

companies (B2B). However, as IAM adds functionality for online interactions with consumers (so-called CIAM), the SailPoint platform will need to add features such as registration, profile management, and customer behavior analytics.

SailPoint now needs to compete with much larger players

Since 2014, SailPoint is majority-owned by private equity firm Thoma Bravo and has been acquisitive, which suggests that its owners are prepared to spend money to support its growth and development. This will need to continue if it is to keep pace with changes in the IDaaS market, where major industry names including IBM and Oracle have entered the fray.

Opportunities

Cloud-based IAM is a growing requirement

Enterprise applications are increasingly residing in the cloud. Employees and partners access them from multiple locations and devices, most of which are not on the corporate network. The cloud is therefore the logical place from which to deliver identity services, even more so as IAM moves into the B2C world and becomes CIAM. IdentityNow can continue to ride this wave if it adds the requisite functionality.

SailPoint can grow in the IDaaS market

Demand for cloud-based identity services is growing at a healthy rate, and SailPoint is positioned to grow with it. This may require M&A activity to add functionality to keep up with the development of the market (in the CIAM space, for instance), and so far the signs are that Thoma Bravo is prepared to fund these moves.

Threats

Identity management is expanding into B2C

Although IAM started out in the B2E world, it has now expanded into B2B. With more customer interactions moving online, its next move must be into B2C, which will require new functionality to be added to platforms such as IdentityIQ and IdentityNow. Specifically, facilities such as easy self-registration, profile management, and customer behavior analytics are key features of CIAM, and SailPoint will need to address these requirements or risk staying behind market trends.

Competition is intensifying in the IDaaS market

While the IAM market is a mature and relatively stable one, the IDaaS space is rapidly becoming significantly more competitive, with heavyweights including IBM, CA, and Oracle from the on-premise world moving into cloud-based services. These are companies with marketing muscle and large existing IAM customer bases, which put pressure on smaller, more specialist firms such as SailPoint.

Appendix

Further reading

2017 Trends to Watch: Security, IT0022-000808 (October 2016)

Emerging Vendors in the IDaaS Market, IT0022-000809 (November 2016)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo