FORRESTER®

The Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019

The 10 Providers That Matter Most And How They Stack Up

by Andras Cser and Merritt Maxim
June 12, 2019

Why Read This Report

In our 37-criterion evaluation of providers of identity-as-a-service (IDaaS) for enterprise, we identified the 10 most significant ones — Google, IBM, Idaptive, Microsoft, Okta, OneLogin, OpenText, Ping Identity, Secret Double Octopus, and Simeio Solutions — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals select the right one for their needs.

Key Takeaways

Okta And Idaptive Lead The Pack
Forrester's research uncovered a market in which Okta and Idaptive are Leaders; OneLogin, Microsoft, Google, Ping Identity, and IBM are Strong Performers; Simeio Solutions and OpenText are Contenders; and Secret Double Octopus is a Challenger.

Mobile App, API Support, And Implementation Ecosystem Are Key Differentiators
As on-premises IAM technology becomes more expensive to maintain and less effective: 1) improved support for IDaaS functions as a native mobile app; 2) API support for apps and policies; and 3) strength of the implementation ecosystem will dictate which providers will lead the pack.

The Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019

The 10 Providers That Matter Most And How They Stack Up

by Andras Cser and Merritt Maxim
with Stephanie Balaouras, Matthew Flug, and Peggy Dostie
June 12, 2019

Table Of Contents

Related Research Documents

Best Practices: Customer And Employee Authentication

The Forrester Wave™: Cloud Security Gateways, Q1 2019

Now Tech: Authentication Management Solutions, Q3 2018

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

IDaaS Provides Better UX, Self-Services, And Hybrid-Cloud Support

IDaaS has been undergoing a transformation in the past two to three years, with every IDaaS solution offering an application portal and some kind of multifactor authentication (MFA) capability. Consequently, S&R pros are: 1) expanding their IDaaS implementations to cover not only SaaS but also on-premises apps to replace legacy, costly-to-maintain web access management or single sign-on (SSO) solutions; and 2) offering self-service, fully fledged user account provisioning and access reviews. S&R pros are also acceding to employees' demands for a friendlier, more consumer-like user experience (UX) and the need to support, in some cases, wholesale workload migrations from on-premises to cloud.

As a result of these trends, S&R pros should look for IDaaS providers that:

› **Expose full IDaaS functionality in native mobile applications.** Enterprises have long demanded mobile-first development. Because of this, IDaaS solutions have to jump on this bandwagon and offer, in their native mobile application, a configurable app portal, full user self-service such as password reset and enrollment, SSO for native mobile applications, versatile MFA, access request management and reviews, and attestation interfaces.

› **Master API security and solution APIs.** S&R pros that have cloud, IoT, and legacy application integration requirements and need to replace legacy SSO solutions must evaluate IDaaS solutions that offer: 1) capabilities to enforce access control on API calls (authentication and authorization) and 2) headless integration by exposing inbound and outbound APIs for token validation, provisioning, and even IDaaS services for policy management.

› **Maintain a broad, international implementation partner ecosystem.** IAM is a translation of people relationships (org hierarchies, business partnerships, etc.) and processes (joiner, mover, leaver, transfer) into identity management and governance, as well as access policy enforcement technology — and not simply a technical implementation.[1] IDaaS vendors can't map and re-engineer business processes and navigate organization politics single-handedly. They need strong implementation partners that understand their clients' business and help with fitting IAM processes and tools to the clients' organizational DNA.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our Now Tech: Authentication Management Solutions, Q3 2018; The Forrester Wave™: Identity Management And Governance, Q3 2018; and The Forrester Wave™: Customer Identity And Access Management, Q2 2017.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019

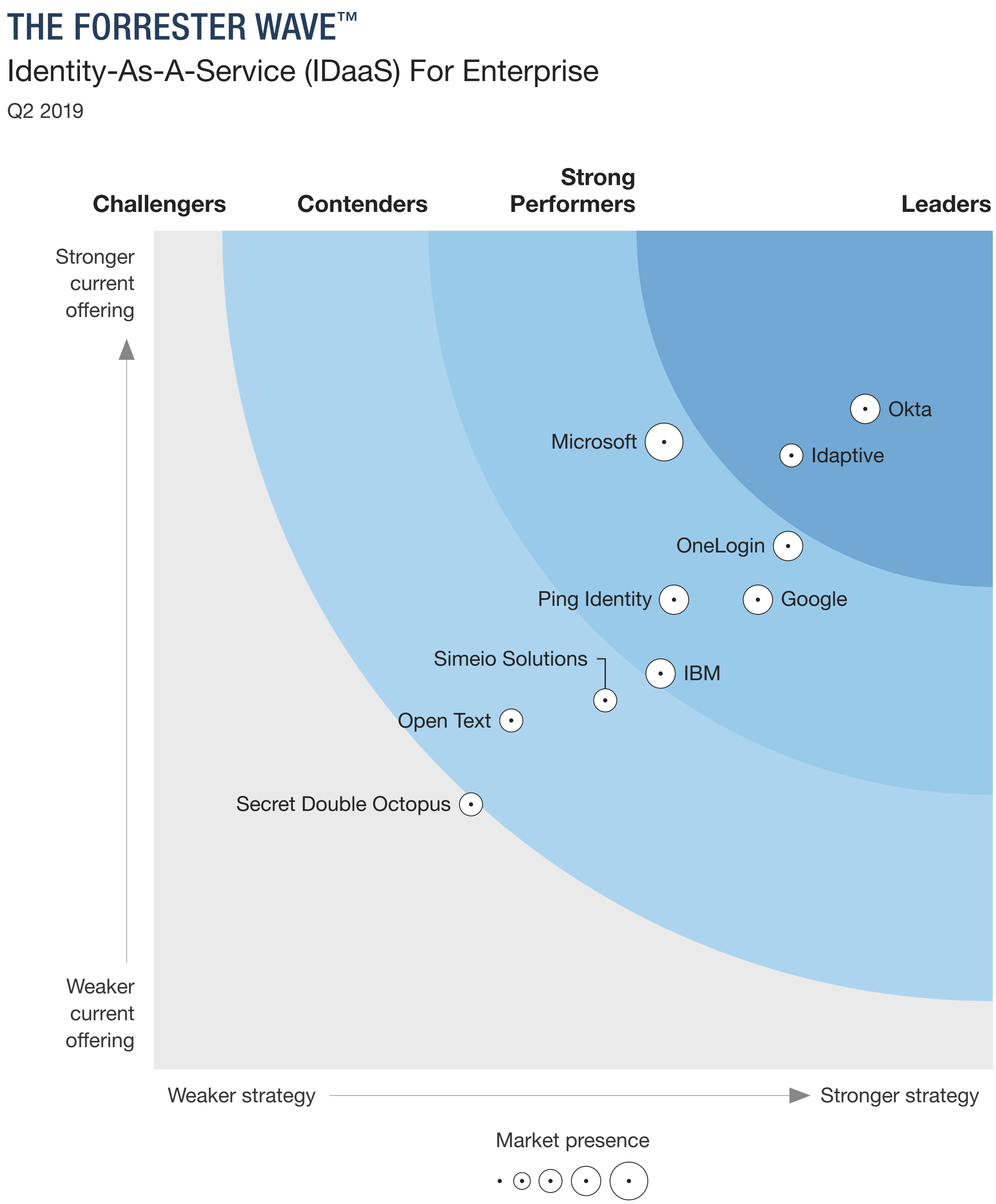

FIGURE 2 Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise Scorecard, Q2 2019

	Forrester's weighting	Google	IBM	Idaptive	Microsoft	Okta	OneLogin	OpenText	Ping Identity	Secret Double Octopus	Simeio Solutions
Current offering	50%	2.80	2.36	3.66	3.74	3.94	3.12	2.08	2.80	1.58	2.20
User directory support	8%	1.00	3.00	1.00	1.00	5.00	3.00	1.00	3.00	5.00	5.00
Access management policy administration	8%	3.00	3.00	5.00	3.00	5.00	5.00	1.00	1.00	1.00	1.00
Identity management policy administration	8%	1.00	1.00	5.00	5.00	3.00	3.00	1.00	3.00	1.00	5.00
End user self-service from the solution's web portal	8%	1.00	1.00	5.00	3.00	5.00	5.00	1.00	3.00	1.00	1.00
Mobile IDaaS functionality	8%	1.00	1.00	5.00	5.00	3.00	3.00	0.00	3.00	0.00	5.00
API security and solution APIs	8%	3.00	5.00	5.00	1.00	5.00	1.00	3.00	3.00	0.00	0.00
Reporting	8%	5.00	1.00	5.00	5.00	1.00	1.00	3.00	3.00	1.00	3.00
Scalability: managed users	7%	5.00	5.00	1.00	5.00	3.00	3.00	5.00	5.00	3.00	1.00
Scalability: connected on-premises applications	7%	5.00	3.00	3.00	5.00	1.00	3.00	5.00	5.00	1.00	1.00
Scalability: connected SaaS applications	7%	3.00	3.00	1.00	5.00	5.00	5.00	3.00	5.00	1.00	1.00
Navigation, integrated environment	7%	3.00	1.00	5.00	3.00	5.00	5.00	3.00	1.00	5.00	1.00
Static and contextual documentation	8%	1.00	3.00	5.00	3.00	5.00	1.00	1.00	1.00	1.00	1.00
Certifications	8%	5.00	1.00	1.00	5.00	5.00	3.00	1.00	1.00	1.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 2 Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise Scorecard, Q2 2019 (Cont.)

	Forrester's weighting	Google	IBM	Idaptive	Microsoft	Okta	OneLogin	OpenText	Ping Identity	Secret Double Octopus	Simeio Solutions
Strategy	50%	3.60	3.02	3.80	3.04	4.24	3.78	2.13	3.10	1.89	2.69
Access management plans	6%	3.00	1.00	3.00	1.00	3.00	5.00	5.00	3.00	1.00	3.00
Identity management plans	6%	3.00	3.00	5.00	1.00	5.00	3.00	1.00	3.00	1.00	3.00
Access governance plans	6%	5.00	3.00	5.00	3.00	5.00	5.00	1.00	1.00	1.00	1.00
Two-factor authentication plans	6%	1.00	3.00	3.00	3.00	3.00	5.00	1.00	5.00	1.00	3.00
Mobile device and IoT management plans	6%	1.00	3.00	5.00	3.00	5.00	3.00	3.00	5.00	5.00	3.00
IoT IAM plans	6%	1.00	1.00	3.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00
Data analytics plans	7%	3.00	1.00	5.00	1.00	3.00	3.00	1.00	3.00	1.00	3.00
Solution delivery	8%	3.00	1.00	5.00	3.00	5.00	3.00	1.00	1.00	5.00	5.00
Vendor's RFP response	7%	5.00	5.00	3.00	1.00	5.00	5.00	1.00	5.00	1.00	1.00
Vendor's PoC and demonstration	7%	5.00	5.00	5.00	3.00	5.00	5.00	1.00	3.00	1.00	3.00
Services and partners	7%	5.00	3.00	3.00	5.00	5.00	3.00	0.00	5.00	0.00	0.00
Development staffing	7%	3.00	5.00	5.00	5.00	5.00	3.00	3.00	1.00	1.00	1.00
Sales staffing	7%	5.00	5.00	1.00	5.00	5.00	3.00	3.00	3.00	1.00	1.00
Support staffing	7%	5.00	5.00	3.00	5.00	5.00	3.00	5.00	1.00	1.00	5.00
Pricing terms and flexibility	7%	5.00	1.00	3.00	3.00	3.00	5.00	5.00	5.00	5.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 2 Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise Scorecard, Q2 2019 (Cont.)

	Forrester's weighting	Google	IBM	Idaptive	Microsoft	Okta	OneLogin	OpenText	Ping Identity	Secret Double Octopus	Simeio Solutions
Market presence	0%	3.69	3.33	2.62	4.44	3.67	3.23	2.41	3.01	2.39	2.69
Total vendor revenue	8%	5.00	5.00	1.00	5.00	3.00	2.00	4.00	3.00	1.00	2.00
IDaaS revenue	15%	4.00	3.00	1.00	5.00	5.00	2.00	4.00	3.00	1.00	2.00
IDaaS revenue growth	15%	1.00	2.00	2.00	5.00	4.00	3.00	1.00	3.00	5.00	4.00
IDaaS direct installed base	15%	5.00	3.00	2.00	5.00	4.00	4.00	1.00	2.00	1.00	3.00
IDaaS indirect installed base	15%	5.00	3.00	5.00	5.00	4.00	4.00	1.00	3.00	2.00	2.00
North American presence	8%	3.00	2.00	4.00	1.00	5.00	3.00	4.00	4.00	1.00	2.00
Latin American presence	8%	4.00	5.00	4.00	3.00	1.00	5.00	4.00	4.00	1.00	2.00
EMEA presence	8%	3.00	4.00	2.00	4.00	3.00	3.00	2.00	3.00	5.00	5.00
AP presence	8%	3.00	5.00	3.00	5.00	2.00	3.00	3.00	3.00	5.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Vendor Offerings

Forrester included 10 vendors in this assessment: Google, IBM, Idaptive, Microsoft, Okta, OneLogin, OpenText, Ping Identity, Secret Double Octopus, and Simeio Solutions.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **Okta continues to expand to hybrid workloads.** Until very recently, Okta has been a true IDaaS service, with minimal on-premises components. Accelerated by its 2017 IPO, Okta has been expanding its install customer base from SMBs to larger enterprises. Okta appears in many of Forrester's clients' RFPs. In the future, Forrester expects the vendor to: 1) enable hybrid IT environments; 2) lay a foundation for Zero Trust by removing trust from static credentials; and 3) offer adaptive and continuous authentication to respond to changing user risk levels even at and after authentication.

From its single console, the solution offers strong user directory integration, access management policy definition capabilities, good integrated Windows authentication, and single logout configuration support and offers a broad range of productized multifactor authenticators. Its end user access request management and review workflows are versatile. However, the vendor's reporting and dashboarding portals are inflexible and show signs of aging compared with competitors.[2] Compared with other vendors, step-up authentication templates are less broad and there is no way to easily customize sequence of authentication events.[3] Its administrative role entitlement compositions are static and not changeable.[4] Customers with minimal on-premises IAM skills using large numbers of SaaS apps should buy Okta.

› **Idaptive adds its own identity threat intelligence to its IDaaS offering.** After its spin-out from Centrify, and despite headcount and administrative challenges, Idaptive has been maintaining its inherited security certifications, emphasizing its identity threat intelligence and device posture and management capabilities. The vendor plans to: 1) empower developers by building new SDKs for mobile and web platforms; 2) offer extensible identity life-cycle management using its connector framework to support provisioning into on-premises applications; and 3) offer cloud insight by collecting anonymized data from all of its cloud tenants to discover malicious IP addresses and detect anomalous behaviors.

The solution has granular and flexible SaaS app access policies and a provisioning workflow for SaaS cloud applications. It has a modular, building-block-based authentication support, and it's easy to add new TOTP/HOTP tokens. APIs are documented and flexible for IDaaS policy management and outbound integration.[5] However, the schema for its cloud directory is limited compared with other vendors. There is no geofencing of users (it's planned), and it lacks productized Azure and GCP admin console and role provisioning support.[6] Customers with heavy enterprise mobility management needs should buy Idaptive.

Strong Performers

› **OneLogin expands into on-premises apps' access policy management.** The vendor has made some management changes in the past 12 to 18 months to grow access to C-suite stakeholders. The solution has a very interesting, live Ideas page, which serves customer advocacy and allows customers to submit and track product enhancement ideas and requests. The vendor plans to: 1) enhance SSO and provisioning for on-premises apps; 2) roll out a FedRAMP certified offering; and 3) introduce a risk API for standalone, adaptive user authorization in apps.

The solution has a configurable schema for the end user's portal interface, flexible and wizard-based SAML setup, risk scoring based authentication, and productized identity provider (IdP) proxying. However, it lacks full virtual directory support and OAuth 2.0 support and is behind other vendors' three-factor authentication (3FA).[7] It offers no API security, nor does it expose APIs for policy management. It requires Sumologic for dashboards. There is virtually no contextual help system in the solution. Customers looking to extensively manage cloud-based and on-premises web apps should buy OneLogin.

› **Microsoft integrates Active Directory into its Azure offering.** Microsoft's Azure AD offering continues to focus on securing Office 365 and Azure environments, and Forrester estimates that at least 50% of Azure AD licenses are offered in the framework of a larger E3 or E5 offering.[8] The vendor plans to: 1) extend Azure AD conditional access integration to Microsoft Information Protection and other solutions; 2) implement FIDO 2.0 and passwordless authenticators; and 3) improve service resilience.

  The solution has strong risk-based access controls and extensive and easy business-to-partner federation policy setup and has access reviews for privileged users. It also boasts a high number of security certifications. However, its support for non-AD user store infrastructures, virtual and meta directory are weaker than that of competitors. API security is largely missing, and dashboards are only in preview. Customers with a sizable Office 365 footprint should buy Microsoft's IDaaS solution.

› **Google works on IDaaS penetration based on existing IDaaS and its acquisition.** Google has been making strong moves toward becoming a credible IDaaS provider, completing and securing its G Suite and EMM offerings. Google uses machine learning for login risk assessment. Forrester expects that the vendor plans to: 1) build SCIM 2.0 API and HR-directed workflows and 2) support and extend RADIUS and Kerberos.

  The solution has strong role-based access control and role assignment policy definitions for administrators, extensive attribute-based provisioning, delayed, activity-based deprovisioning as well as broad API and SDK support for inbound and outbound integration. Its user self-service is very user friendly.[9] However, full AD sync requires two separate components (directory and password sync); there is no virtual or meta directory, and MFA setup is less versatile than other vendors.[10] There is no productized provisioning to on-premises apps and no generic inbound SCIM connector (this is planned.). In the light of actual implemented deals by the top five implementation partners in each geography, the implementation partner ecosystem is small for a vendor the size of Google. Customers standardized on G Suite should buy the vendor's IDaaS service.

› **Ping Identity builds on its tried-and-true on-premises offering for IDaaS.** With Vista Equity Partners now owning Ping Identity, the vendor's fiscal and operational discipline has improved tremendously. Ping Identity is one of the most trusted access management vendors in the IAM market, with one of the broadest access management policy definition capabilities. The vendor recently launched an API-first IDaaS solution with self-service support for developers and plans to: 1) advance identity intelligence using artificial intelligence and machine learning and 2) optimize mobile device support with intuitive registration flows, behavior biometric based, and passive authentication. Customers who already own PingFederate and PingAccess should buy PingOne to extend their IAM footprint to cloud apps.

The solution offers robust passwordless authentication, support for on-premises apps and IWA, a strong API for policy management, and an API gateway, as well as exposed and configurable high availability support. However, to support more complex enterprise use cases, PingOne for Enterprise and PingID by themselves are insufficient and require PingFederate and PingAccess (which represent additional implementation and operational costs). The solution lags behind other vendors in identity analytics, access request management, dynamic dashboards, and device reputation.

› **IBM debuts with a new Cloud Identity offering.** IBM has organically built its Cloud Identity (CI) offering for IDaaS, not to be confused with Cloud Identity Services (CIS), which is based on IBM's older acquisition of Lighthouse Gateway. Integration between the two solutions and IBM's large legacy ISIM/ISAM solutions is well underway but incomplete. The vendor plans to: 1) build solutions for decentralized identity management using blockchain technologies; 2) create passwordless authenticators using certificates on mobile devices, QR codes, tokens, and blockchain; and 3) make its currently beta Identity Analytics offering generally available to identify identity risks based on peer group analysis. Customers who already own CIS or IBM Security Identity Manager or IBM Security Access Manager should buy CI.

The solution provides extensible, widely deployable MFA, is well on its way to implementing FIDO 2.0 WebAuthN, and uses administrator configurable machine learning with thresholds for identity analytics peer group analysis.[11] Its API-based integration and API-based policy management are very strong.[12] However, risk-based access management (RBA) has no real configuration GUI for policy management, CIS and CI are different with different policy management GUIs, and customers require both CIS and CI to achieve full IAM functionality.[13] CI has no end user facing, native mobile portal application today.

Contenders

› **Simeio Solutions adds its own intellectual property to OEMed solutions.** Long gone are the days when Simeio was only a managed IAM services provider. Today, in addition to its own, in-house-built intellectual property, to satisfy all use case requirements, Simeio OEMs, resells, supports, and manages Ping Identity for access management and Saviynt for identity management and governance use cases, as well as Gluu and OpenAM.[14] Of all vendors evaluated in this Forrester Wave, Simeio Solutions has the most complete agent-based and self-sovereign identity framework vision and tool set. The vendor plans to: 1) productize its robotic process automation bot assistant, EVA, to allow it to help with user access requests; 2) use artificial intelligence for access reviews and approvals; and 3) enhance its identity proofing capabilities. Customers with relevant Ping and Saviynt implementation expertise or install base looking for a managed IAM service should buy Simeio.

The solution offers extensive LDAP sync and schema mapping options, well thought-out identity orchestration, and identity proofing. However, since the solution contains OEMed Ping Identity and Saviynt components, complexity and training costs can be higher than those of competing offerings. The solution requires PingOne for a productized SaaS app catalog, SAML, OpenID Connect, and OAuth functionality, and they all require installation of the OEMed PingFederate component. This high use of OEMed intellectual property makes Simeio Solutions vulnerable to any changes in its OEM partners' product strategy.

- **OpenText reaches beyond its automotive and healthcare verticals.** Covisint's acquisition by enterprise content management veteran OpenText represents a great opportunity to integrate identity and access management into document flows and supplier management. OpenText has deep expertise in proofing and managing business-to-partner identities and an advanced IAM for IoT vision. The vendor plans: to 1) expand Covisint's IoT-centric IAM capabilities; 2) use reputation-based authorization, based on its large identity federation network; and 3) integrate Covisint IDaaS with OpenText Magellan for artificial intelligence. Customers requiring strong federation services and identity vetting for business partners' employees should buy OpenText's IDaaS solution.

  The solution offers robust RBA and application-level authorization policy definitions, user audits and reviews, and highly configurable application request flows. However, it sports a large number of components and lacks step-up authentication and FIDO support (the latter is planned).[15] Much functionality requires scripted configuration, and the solution has no native mobile portal application for end users. Customers report that the vendor's implementations are high-touch and require a lot of involvement from the vendor.

Challengers

- **Secret Double Octopus focuses on passwordless authentication.** The Israeli vendor has a small customer base and revenues — with increasing focus on the North American market — but offers highly innovative IDaaS services and an easy-to-use user and admin interface. The vendor plans: to 1) offer cross-channel, passwordless authentication solutions; 2) offer identity vouching (identification and authentication by authorized peers); and 3) provide identity analytics using integration with security analytics platforms such as Micro Focus, Splunk, and others. Firms with needs for innovative IAM features such as passwordless authentication and hybrid (cloud and on-premises) authentication needs should buy the solution.

  The solution offers very flexible support for user directories, including easy setup for AD integration. Its support for IdP functionality is also quite strong. It uses AES 256 cryptography for strong data protection. However, at the cutoff date for this evaluation it lacks FIDO and metadirectory support, has only minimal out-of-the-box support for SaaS applications, and requires Kibana (elastic.io) for reporting.[16] It has no mobile application portal or help. At this time the vendor has no implementation partner ecosystem.

Evaluation Overview

We evaluated vendors against 10 criteria, which we grouped into three high-level categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include user directory support, access management policy administration, identity management policy administration, end user self-service from the solution's web portal, mobile IDaaS functionality, API security and solution APIs, reporting, scalability, navigation, static and contextual documentation, and certifications.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated the vendors' access management, identity management, access governance, two-factor authentication, mobile device and IoT management, IoT IAM, data analytics plans, their solution delivery and customers' satisfaction, RFP and proof of concept (PoC) responses, services partner ecosystem, and development, sales and support staffing, as well as their pricing flexibility and simplicity.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's total and IDaaS revenue, IDaaS revenue growth, direct and indirect installed base, North American, Latin American, EMEA, and AP presence.

Vendor Inclusion Criteria

Forrester included 10 vendors in the assessment: Google, IBM, Idaptive, Microsoft, Okta, OneLogin, OpenText, Ping Identity, Secret Double Octopus, and Simeio Solutions. Each of these vendors has:

› **A thought-leading IDaaS portfolio of products and services.** We included vendors that demonstrated IDaaS thought leadership and IDaaS solution strategy execution by regularly updating and improving their productized IDaaS product portfolio. They must have the ability to provide viable IDaaS functions for access and identity management in a multitenant, cloud-based, productized, and publicly available offering.

› **A comprehensive online demonstration environment available for independent testing.** We included vendors that could provide Forrester with a comprehensive, coherent online demonstration environment mirroring the vendor's commercially available, productized IDaaS solution. The vendor had to make the demonstration environment available for Forrester's independent testing of common usage scenarios in the Current Offering section of this Forrester Wave.

› **Total annual IDaaS revenues of at least $1 million with at least 15% growth.** We included vendors with at least $1 million annual IDaaS revenues which grew at least 15% in the 12 months ending on the cutoff date.

› **At least 30 paying IDaaS customer organizations in production.** We included vendors that have an install base of at least 30 paying IDaaS customer organizations in production.

› **An unaided mindshare with Forrester's customers.** The vendors we evaluated are frequently mentioned in Forrester client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.

› **An unaided mindshare with vendors.** The vendors we evaluated are frequently mentioned by other vendors during Forrester briefings as viable and formidable competitors.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by March 22, 2019 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

1 Firms have to expose their applications not only to their employees and contractors but also to their business partners and, in some cases, customers. This has led to the loss of physical and network perimeter controls, elevating IAM's importance in application and data access.

2 Okta's customers prefer API-based log integration. Data can be pushed out to third-party systems, including Okta's integrations with security analytics vendors like Splunk and Sumologic.

3 Okta plans to implement authentication factor sequencing in Q2 2019.

4 Okta plans to implement more customizable admin roles in Q3 2019.

5 The solution is equally scalable for on-premises and SaaS applications.

6 Azure admin console support productization is also planned.

7 The solution can require an X.509 certificate for 3FA.

[8] For information about E3 and E5, visit the Microsoft website. Source: "Office 365 Enterprise E5 overview and documentation," Microsoft Office (https://support.office.com/en-us/article/office-365-enterprise-e5-overview-and-documentation-f7407faa-6bcb-4f23-9056-7aba50d6942f) and "Office 365 E3," Microsoft Office (https://products.office.com/en-us/business/office-365-enterprise-e3-business-software).

[9] The solution is available as a standalone tool or via G Suite.

[10] Google plans to unify the directory and password sync agents in a future release.

[11] IBM bundles ready-to-consume reports in its IDaaS solution.

[12] IBM designs its IDaaS solution with an API-first approach.

[13] IBM plans to unify CIS and CI policy management interfaces. IBM designs its IDaaS solution to use reactive/adaptive web user interfaces that render correctly on both desktop and mobile browsers.

[14] In addition to the above solutions, Simeio's IO IAM platform has been integrated with other commercial IAM solutions, such as CA Technologies, ForgeRock, and Oracle.

[15] OpenText is in the process of unifying components.

[16] After the cutoff date, the vendor added FIDO support.