OMDIA UNIVERSE

Publication date
June 28, 2023

Author

Don Tait, Senior Analyst,
Cybersecurity, Identity Authentication Access

Rik Turner, Senior Principal Analyst,
Cybersecurity, Emerging Cybersecurity

Omdia Universe: Identity-as-a-Service Solution, 2023

OMDIA

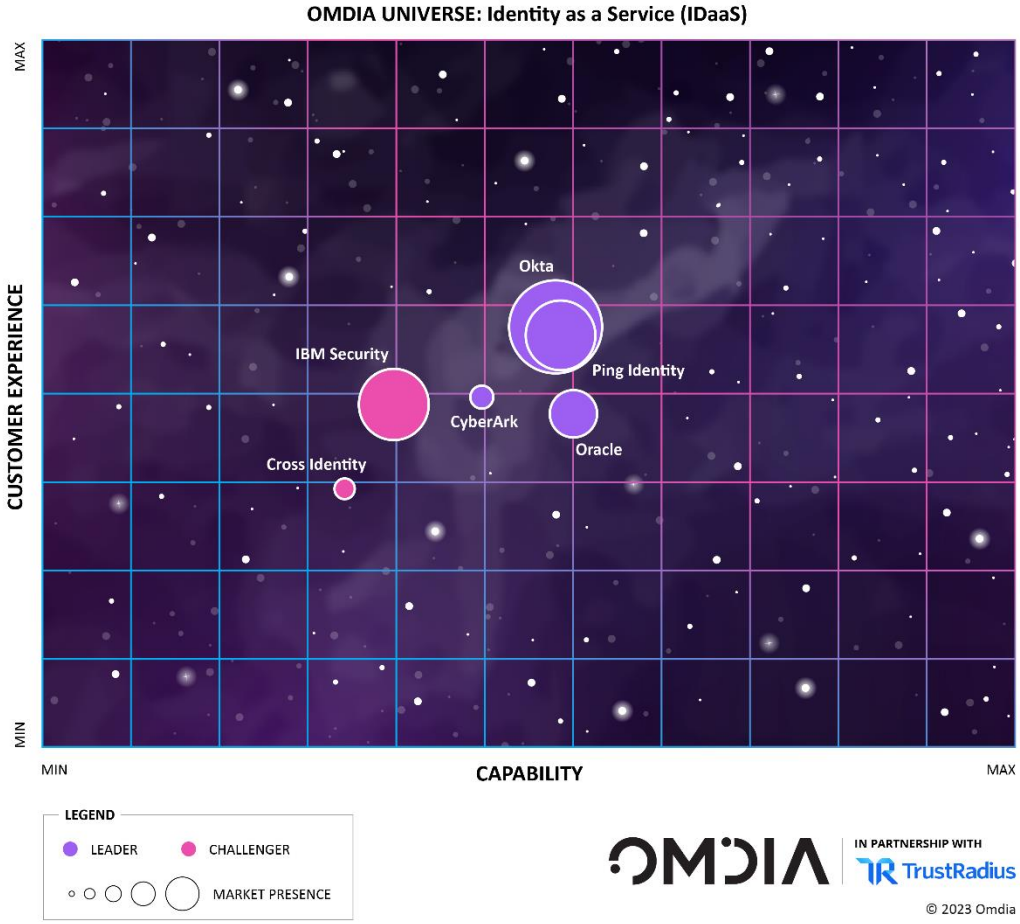
Brought to you by Informa Tech

Summary

Catalyst

Enterprises are increasingly employing cloud-based, or at least hybrid, environments that integrate optimally with cloud-based systems. Enterprises should consider whether cloud-based identity could be deployed more quickly and help reduce costs around scalability. Cloud-based software-as-a-service (SaaS) applications have transformed the business world. Omdia predicts that about four-fifths of enterprises will embrace SaaS by 2023. The identity-as-a-service (IDaaS) segment is the natural evolution of on-premises identity and access management (IAM).

Figure 1: The Omdia Universe for IDaaS



Source: Omdia, in partnership with TrustRadius

Omdia view

The cloud was a natural place for this “vanilla” IAM to migrate to, enabling the technology to move from product to service and from capex to opex. It also broadened the market beyond large enterprises that could afford on-premises IAM to the midsize and even small and medium-sized business (SMB) segments. Large corporates, meanwhile, could use it to address the challenges of mergers and acquisitions, integrating companies they had acquired more easily and quickly than when they had to add all the new employees to the on-premises IAM directory.

IDaaS should be considered as an opportunity to streamline IAM and provide an enterprise-wide approach that grants access to on-premises and cloud-based assets such as data and applications. In recent years, the number of identity management vendors offering fully featured IDaaS has grown, as IDaaS specialists that started out delivering cloud-only products have challenged the incumbent IAM vendors, for whom IDaaS is a natural extension of their core identity portfolios.

Analyzing the IDaaS universe

Market definition

In this report, Omdia considers a series of features and functionality that would reveal differentiation between the leading solutions in the marketplace. The criteria against which IDaaS solutions are classified are as follows:

Solution capabilities

- **IDaaS service delivery** addresses service delivery capabilities for cloud, web, and on-premises requirements and covers key operational environments that need to be supported (business to business (B2B), business to employee (B2E), machine to machine (M2M), and Internet of Things (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.
- **Single sign-on (SSO)** covers the range of facilities supported, a platform's on-premises and cloud interoperability and threat protection capabilities, and its security controls.
- **Provisioning** covers the provisioning facilities provided and the services supported, including deprovisioning and associated reporting and alerting services.
- **Directory service** includes directory management facilities to provide support for the leading directories used in IAM, along with associated requirements for directory synchronization.
- **Reporting, alerting, and monitoring** consider a platform's ability to monitor user behaviors such as login attempts and its facilities for alerting on suspect activities and providing reports to senior management.
- **Management and infrastructure** cover elements such as the range of applications supported with prewritten APIs, key industry standards supported, and the third-party IAM systems each IDaaS service can work alongside and integrate with.
- **Coverage** includes the extent to which IDaaS services are delivered at a country, regional, or global level. Language, technical support, and where data centers are located are also considered under this category.
- **New features and business models** highlight some of the new features that vendors plan to add or retire and explore future business models over the next few years.

- **Certification** entails the types of entitlement and separation of duties, policies, and proper certification documentation.

Market dynamics

Migrating to IDaaS helps enterprises modernize by delivering SSO across all cloud-based applications and being able to respond quickly when new cloud-based apps are added. It also frees up security resources previously tied up on tedious commodity IAM tasks to focus on higher-value work and unique organizational projects that cannot be outsourced. An additional benefit of the as-a-service model is that, within the IDaaS space, vendors are continually innovating, which helps to keep enterprises up to date with advances in IAM technology.

Enterprises and corporate users also need to consider how the data is stored within a cloud service such as an IDaaS solution. In general, IDaaS products do not sync and store password hashes from users. However, several providers do offer this as an option to maintain the same passwords between multiple accounts (local directory, IDaaS, and even SaaS applications). Offering this option is one way that vendors can differentiate themselves from vendors that do not offer this option.

In an ever-changing world where data breaches are on the increase, IDaaS solution providers need to continually innovate to stay ahead of the curve and remain one jump ahead of hackers. This will be a differentiator over vendors that do not innovate on a frequent basis. Through innovation, vendors can add to their capabilities and product features, which helps in winning new business and keeping existing customers happy.

Most IDaaS products offer the ability to customize the synchronization process (where directory users and groups are pulled into the service), where user attributes are allowed to be synchronized. The reasons for customizing attribute synchronization are for security or for privacy.

Having IDaaS products that offer the ability to provide business partners with SSO access to apps through a portal functionally identical to the one available to normal corporate users can be a key differentiator. This allows companies to foster business relationships without having to automatically give partners direct access to their corporate networks.

Figure 2: Vendor rankings in the IDaaS Universe

Vendor	Product(s) evaluated
Leaders	
CyberArk	CyberArk Identity Security Platform
Okta	Okta Workforce Identity Cloud
Ping Identity	PingOne Cloud Platform
Oracle	Oracle Cloud Infrastructure (OCI) Identity and Access Management
Challengers	
IBM	IBM Security Verify
Cross Identity	Compact Identity

Source: Omdia

Market leaders

This category represents the leading solutions that Omdia believes are worthy of a place on most technology shortlists. The vendors have established a commanding market position with products that are widely accepted as best of breed.

Market challengers

The solutions in this category have a good market positioning, and the vendors are selling and marketing the product well. The products offer competitive functionality and a good price-performance proposition and should be considered as part of the technology selection.

Market prospects

The solutions in this category are also worthy of inclusion on a shortlist. They typically provide the core functionality needed, but vendors may be newcomers, specialize in a particular segment, or have a regional focus.

The scoring of the Universe is performed by independent analysts against a common maturity model, and the average score for each subcategory and dimension is calculated. The overall position is based on the weighted average score, where each subcategory in a dimension is allocated a significance weighting based on the analyst's assessment of its relative significance in the selection criteria.

Opportunities

- **Growing adoption of cloud:** The growing adoption of all forms of cloud computing bodes well for the IDaaS sector. For companies that have no legacy on-premises IAM in place, it is a logical choice for them to use identity services in the cloud if an increasing amount of their applications and business systems are delivered from there. Even for companies that have already deployed an on-premises IAM platform and are still amortizing that investment, IDaaS represents an easier way to bring new business units, such as ones that come to them through acquisitions, onboard, particularly if their application estate is cloud-based.

- **IDaaS democratizes identity management:** IDaaS democratizes identity management, making it available to companies of all sizes, so brand-new customers are very much the norm, and the bulk of the revenue here is from new subscriptions to the service. At the same time, IDaaS should offer enterprises with an existing IAM infrastructure the ability to migrate that functionality into the cloud at a pace that suits them. The unexpected events of 2020—with the pandemic forcing millions to work from home for long periods of time—have led to even faster growth of cloud-based identity: IBM itself says growth has exceeded its 10% prediction for this year.

- **Good roadmap of features in adjacent segments:** Omdia believes that a good roadmap of features in adjacent segments will help vendors in this space in the next couple of years. This includes adding features in the areas of identity validation and proofing (for both standalone and integrated services), identity analytics and risk-based authentication, privacy and consent management, passwordless authentication, targeted attack detection, risk alerts, risk dashboards, decentralized identity, and zero logins, to name but a few. All these additional features should help vendors get new customers and keep existing ones.

Threats

- **Market consolidation**. Enterprises are growing increasingly comfortable with cloud computing in both its most readily consumable form (SaaS) and in those that require more work from the customer (infrastructure and platform as a service (IaaS/PaaS)). We are already seeing variation within cloud in the form of edge computing as vendors and service providers recognize the desirability of locating some functionality in the core of the cloud and other parts closer to the end user (i.e., at the edge). All this is very positive for IDaaS because it argues against hefty investment in on-premises IAM and favors a more lightweight, cloud-based approach to identity services, swapping capex for opex and enjoying both the flexibility and the scalability that cloud enables. It surely also catches the attention of technology vendors not currently in the IDaaS market, attracting them to consider a play there. This may take the form of acquiring a vendor in the IDaaS space or launching their own products/solutions.

- **New entrants:** It is in the nature of SaaS that customers can change providers more easily than with on-premises infrastructure because if another vendor comes along with a compelling alternative, it is easier to swap out the current supplier. So, if one or two of the tech sector's

most creative giants were to step into IDaaS with a particularly compelling offering, the leading vendors' positions in this market could be jeopardized.

- **Innovation:** Vendors need to show potential customers that it is innovative in the IDaaS space. This also entails developing and launching new products and features at a quicker pace. In an ever-changing marketplace, this could be a key differentiator against the competition.

Changes from the previous report

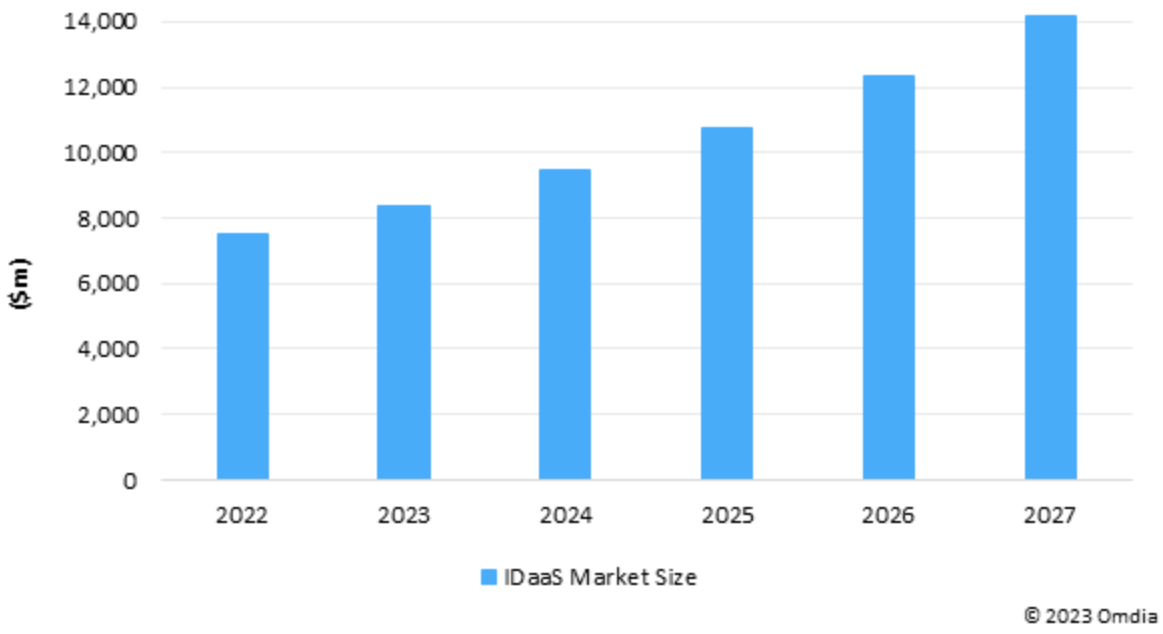
CyberArk, Okta, and Ping Identity retained their leadership positions from the previous report, and Oracle improved their challenger classification to be recognized as a market leader for the first time. IBM Security remained a challenger, and Cross Identity was featured in the report for the first time.

Market outlook

The world market for IDaaS increased to $7.5bn in 2022. With cloud adoption continuing throughout the forecast period, this segment is projected to increase to $14.2bn by 2027, with a CAGR of 13.5%.

The increase in the number of home workers and the acceleration in companies moving to the cloud were key growth drivers for the IDaaS market in 2020. It is worth mentioning the fact that IDaaS is cloud-based authentication built and operated by a third-party provider. Omdia believes that the trend away from on-premises products toward cloud solutions such as IDaaS will continue during the next five years. Indeed, the unexpected events of 2020, with the pandemic forcing millions to work from home for long periods of time, have led to even faster growth of cloud-based identity management (see **Figure 3**).

Figure 3: The world market for IDaaS, 2022–27 ($m)



Source: Omdia

Vendor analysis

Cross Identity (Omdia recommendation: Challenger)

Cross Identity should appear on your shortlist if you are an SMB that wants to transition to the cloud

Overview

Cross Identity is a provider of identity management technology headquartered in Bengaluru, India. While it has only existed with its current name since February 2023, the business has been in existence since 2000, when it was formed as Ilantus, initially as a professional services company, implementing many of the major IAM brands of the day. Its experience eventually led it to develop its own IAM platform called Compact Identity.

It was in 2022 that Ilantus took the decision to split its product and services businesses into separate companies, and in February 2023, the product side became Cross Identity while the services arm retained the Ilantus name (and was acquired by Network Intelligence, a cybersecurity provider headquartered in New York).

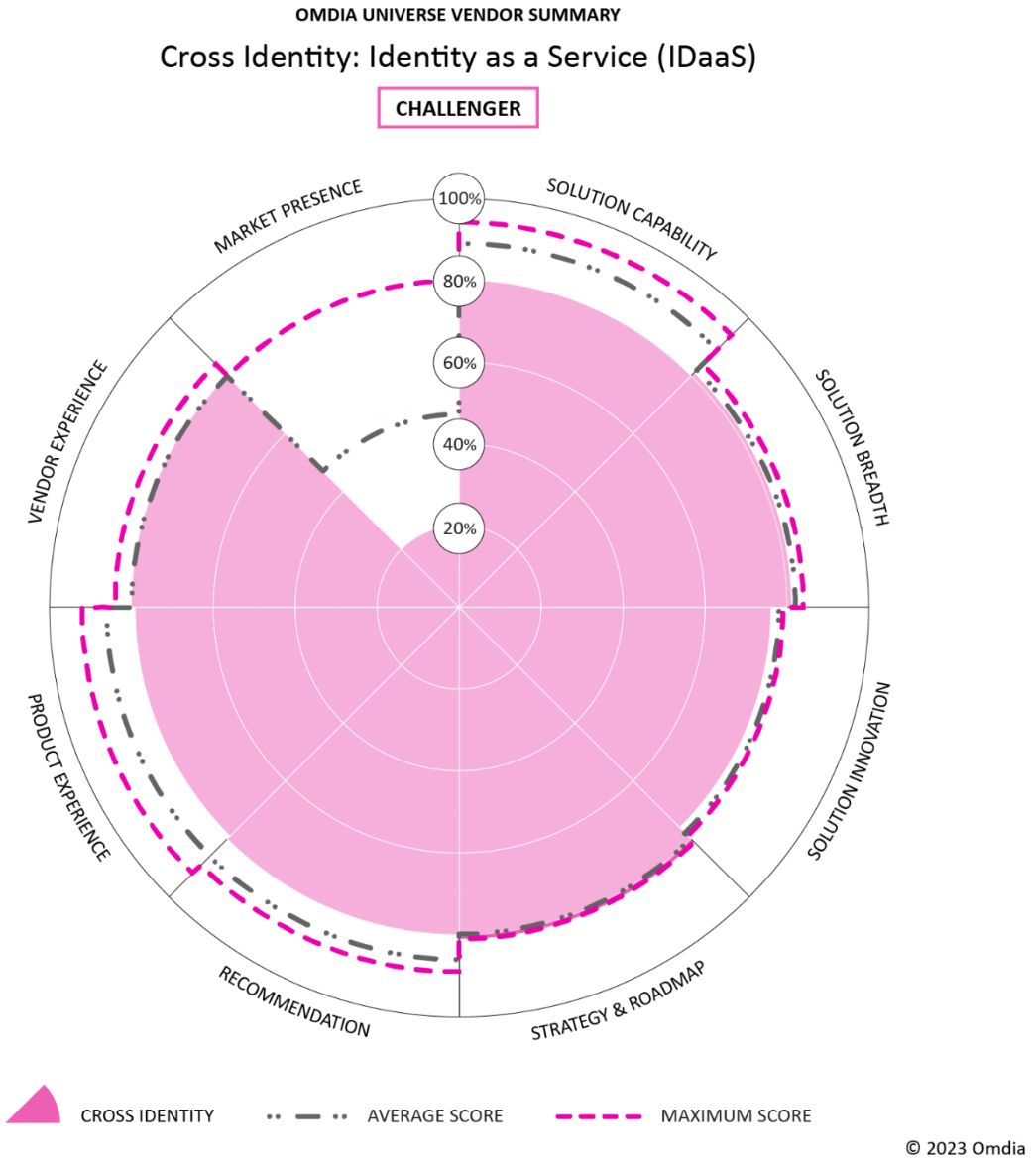
As such, Cross Identity's mission is to take forward the Compact Identity technology developed by Ilantus, targeting the workforce use case (i.e., B2E) primarily. It describes Compact Identity as "converged" IAM, in that it combines, in a single platform:

- The kind of "vanilla" IAM/IDaaS that typically provides identity management for the general workforce of a company, including:
    - A Universal Directory and all the requisite access management capabilities, such as SSO.
    - Multifactor authentication (MFA) that can be triggered depending on the context.
    - Password management.
    - Web access management.
    - A passwordless authentication capability involving a FIDO-compliant mobile app to which an identity can be pushed.
- A privileged access management (PAM) capability for those identities that require extra attention by virtue of the sensitive or confidential data to which they have access rights.

- An identity governance and administration (IGA) capability that might otherwise require a customer to go to a specialist provider such as SailPoint.

Figure 4 shows Cross Identity's strongest categories were solution capability (82%), strategy and roadmap (81%), solution breadth (81%), and customer recommendation (80%). In terms of capabilities, Cross Identity's strengths were authentication/MFA (100%), SSO (96%), and provisioning (90%). Its weakest capability was directory service (64%).

Figure 4: Omdia Universe ratings—Cross Identity



Source: Omdia

Strengths

This “one-stop-shop” approach is a key element in Cross Identity’s marketing in that it is designed to address the challenges of managing multiple providers, not to mention those of actually operating their platforms and navigating the disparate data formats used within them.

Consumption-based charging

The vendor also seeks to differentiate its offering with its charging mechanism. While traditional user-based licenses (i.e., headcount-based pricing with volume discounts) are available, in early 2023 the vendor introduced another alternative: a pay-per-use model rather than per-user subscriptions. Aside from differentiation, Cross Identity also argues that this consumption-based approach is more attractive for its target customer base in the SMB segment.

The platform is architected to support multitenant deployments, and its various modules can integrate with third-party systems within the identity universe, such as those from Okta or Microsoft. Cross Identity says it often deploys its IGA technology alongside those vendors’ IAM/IDaaS platforms, for instance. There are also connectors for widely used SaaS applications such as Workday in HR departments, as well as integrations with directory services vendor JumpCloud and, via a Cross Identity API, with all the leading security incident and event management (SIEM) platforms.

Similarly, customers are at liberty to connect their IAM and PAM modules to third-party directories such as Active Directory and Azure AD. And since a lot of SMBs have no directory in place and want to keep their costs down, Compact Identity also supports simple CSV files in the absence of an overarching “source of truth.” This also comes in useful when a customer is dealing with contractors: since they will not be in their Active Directory environment, Compact Identity can simply import a CSV file for them.

Deployment options

As for its deployment options, Compact Identity is entirely software and, as such, can be delivered for installation in a customer’s private cloud environment, in SaaS mode, or even to reside on the customer’s own premises if so desired.

The vendor has made a point of developing user-friendliness for a non-technical audience to be able to configure and use the platform, for example, providing guided help so that line managers can set up a new employee’s identity on the system in just a few clicks and without complex workflows.

This makes sense given Cross Identity’s target market, where there may well not be a large team dedicated to managing the identity platform, and the line of business may need to onboard and manage identities for itself. The Compact Identity platform similarly has a multi-level approval capability, enabling access requests to be addressed in a delegated fashion rather than requiring a single individual within an organization to handle them all. Users also find Compact Identity easy to use, secure, and cost-effective compared to other IDaaS products on the market.

Limitations

Omdia has seen criticism of the Cross Identity product, that it was not very stable and that outages happened, especially at peak times. However, Cross Identity has tried to mitigate these outages by

utilizing several strategies, including implementing robust monitoring and alert systems, regular testing and simulation, fault tolerance and failover mechanisms, and utilizing cloud scalability features and load-balancing methods.

There were also those who felt that their customer support could be improved. To address this issue, Cross Identity has implemented an improved and enhanced customer support and satisfaction assurance process (which includes monitoring and analyzing customer feedback regularly, responding promptly to customer inquiries, and a multi-channel approach with ticketing systems, phone, and email).

There are a number of items on Cross Identity's technology roadmap. These include:

- Support for micro-certifications, which are access reviews triggered in real time or very soon after at-risk access has been discovered. They happen when a policy violation has occurred by a specific change to user access. This means an individual has gone outside the normal IGA process, commonly referred to as "out-of-band" access. Micro-certifications alert application owners of the policy violation and enable them to immediately perform a limited access review focused on the access that triggered the event.

- Cross Identity will provide two approaches to Support for separation of duties (SOD) (online SOD and offline SOD) in the next release on July 15, 2023:

    - Online SOD refers to real-time monitoring and enforcement of the segregation of duties within the IAM system. This approach involves implementing controls and checks directly within the IAM system to prevent users from performing conflicting actions or accessing sensitive resources simultaneously. This online SOD will ensure that users are granted only the necessary privileges based on their roles and responsibilities. For example, if a user can create and approve financial transactions, an online SOD control would prevent them from approving their own transactions.

    - Offline SOD, on the other hand, involves periodic reviews and analysis of user access and activities outside of the IAM system. In this approach, SOD violations are identified and addressed after the fact rather than in real time. The IAM system may generate reports or logs that are then reviewed by auditors or security teams to identify potential SOD conflicts. Once identified, appropriate actions can be taken to rectify the conflicts.

- **Integrated Windows Authentication (IWA):** This will allow users to log in to a Windows domain and automatically authenticate with other services without providing additional credentials.

- **Native App SSO:** Cross Identity support SSO for native mobile apps, which will provide a comprehensive IAM platform that can integrate SSO functionality into mobile applications.

- **Custom Windows Login:** This will enable Cross Identity as a custom Windows login provider, integrating Cross Identity's authentication services with the Windows operating system.

CyberArk (Omdia recommendation: Leader)

CyberArk should appear on your shortlist if you are looking for a provider of SaaS-delivered identity management services

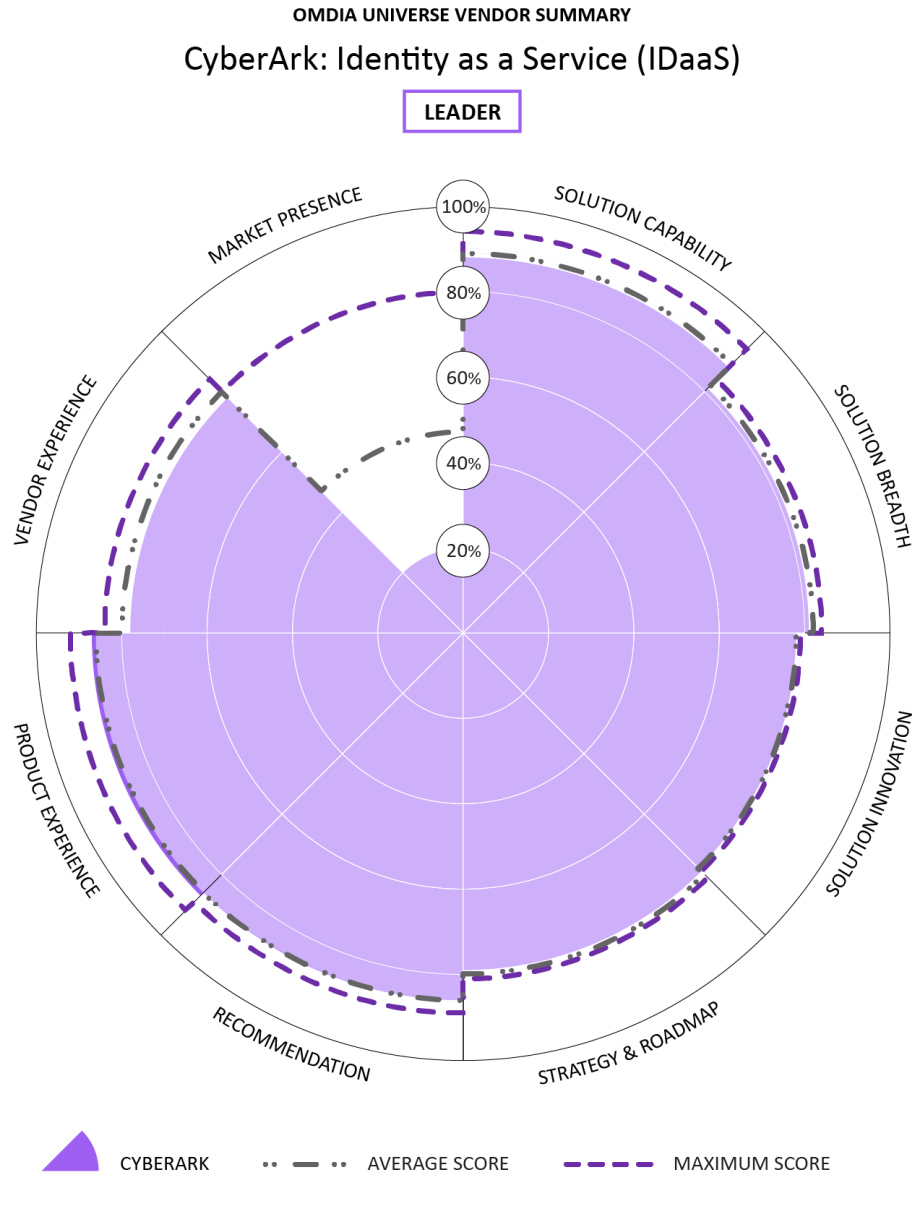
Overview

CyberArk Identity, an integral part of the CyberArk Identity Security Platform, combines Workforce and Customer Access and Identity Management solutions. Workforce Access capabilities include SSO, App Gateway, Adaptive MFA, User Behavior Analytics, Endpoint Security, Workforce Password Management, and Secure Web Sessions. Identity Management solutions include Identity Lifecycle Management, Identity Flows, Identity Compliance, and Directory Services.

CyberArk Identity secures access to cloud-based apps and supports non-SaaS apps deployed on-premises via its App Gateway service. It also integrates with on-premises user repositories, such as Active Directory and LDAP-based directories, by deploying a connector service installed on the customer's on-premises server.

Figure 5 shows that CyberArk's strongest categories were solution capability (89%), product experience (87%), and recommendation (86%). The company's weakest category was market presence (20%). In terms of capabilities, CyberArk's strengths were authentication/MFA (100%), IDaaS service delivery (100%), certification (100%), and management and infrastructure (90%). Its weakest capability was new features and business model (75%).

Figure 5: Omdia Universe ratings—CyberArk



Source: Omdia

Strengths

CyberArk acquired Idaptive in May 2020. Idaptive came into existence in October 2018, but its technology has a longer history, because the vendor was previously the IDaaS business unit that was spun out that year from PAM vendor Centrify, a company that was founded in 2004.

Reviewers frequently refer to the platform's ease of use, both for the end-user and the IT department. There is also consistent praise for the simplicity of adding custom Security Assertion Markup Language (SAML) apps and the ability to give an SSO-like experience to non-SAML apps. Users also found it easy to configure to script-automated utilities and to troubleshoot user issues. Having a good and intuitive user experience are good features for users to comment upon.

Omdia believes that CyberArk has a key strength in CyberArk Identity Flows—a no-code identity automation and orchestration service—and this is seen as being the glue to help customers operationalize identity processes. Also, CyberArk has been using AI and machine learning (ML) in its User Behavior Analytics solution for a number of years. This bodes well for the future in light of the explosion of interest in AI.

Limitations

Omdia has seen criticism of the CyberArk Identity that sometimes the customer support can take time to begin. However, it was also said that once the support started, the CyberArk team was actively involved in the resolution of the issue.

There were also those who felt there was an inability to prompt users for more fields with logins containing more than username/password and that there was limited customization of password reset notifications.

Roadmap

CyberArk has a broad roadmap of CyberArk Identity features that it plans to add to its Identity Security Platform in the next 12–18 months, and they can be apportioned into the following three categories:

- **Workforce Access:** Additional access security controls using a purpose-built, hardened CyberArk Secure Browser and Secure Web Sessions, differentiating features to the Workforce Password Management solution, additional passwordless factors including Passkeys and behavioral biometrics, additional threat intelligence, and security insights.

- **Identity Management:** Additional integrations, flows catalog with quick start orchestration and automation flows, centralized access request workflow, and an intelligent AI/ML-driven governance service for the Identity Security Platform.

- **Customer Access:** Enhanced developer tools with additional widgets and developer software development kits (SDKs), fine-grained consent, and preference management.

Additionally, CyberArk will also be incorporating AI-powered identity, improving user experience, and improving managed security service providers into their platform.

IBM Security (Omdia recommendation: Challenger)

IBM Security should appear on your shortlist if you are a company that increasingly requires privacy and consent management

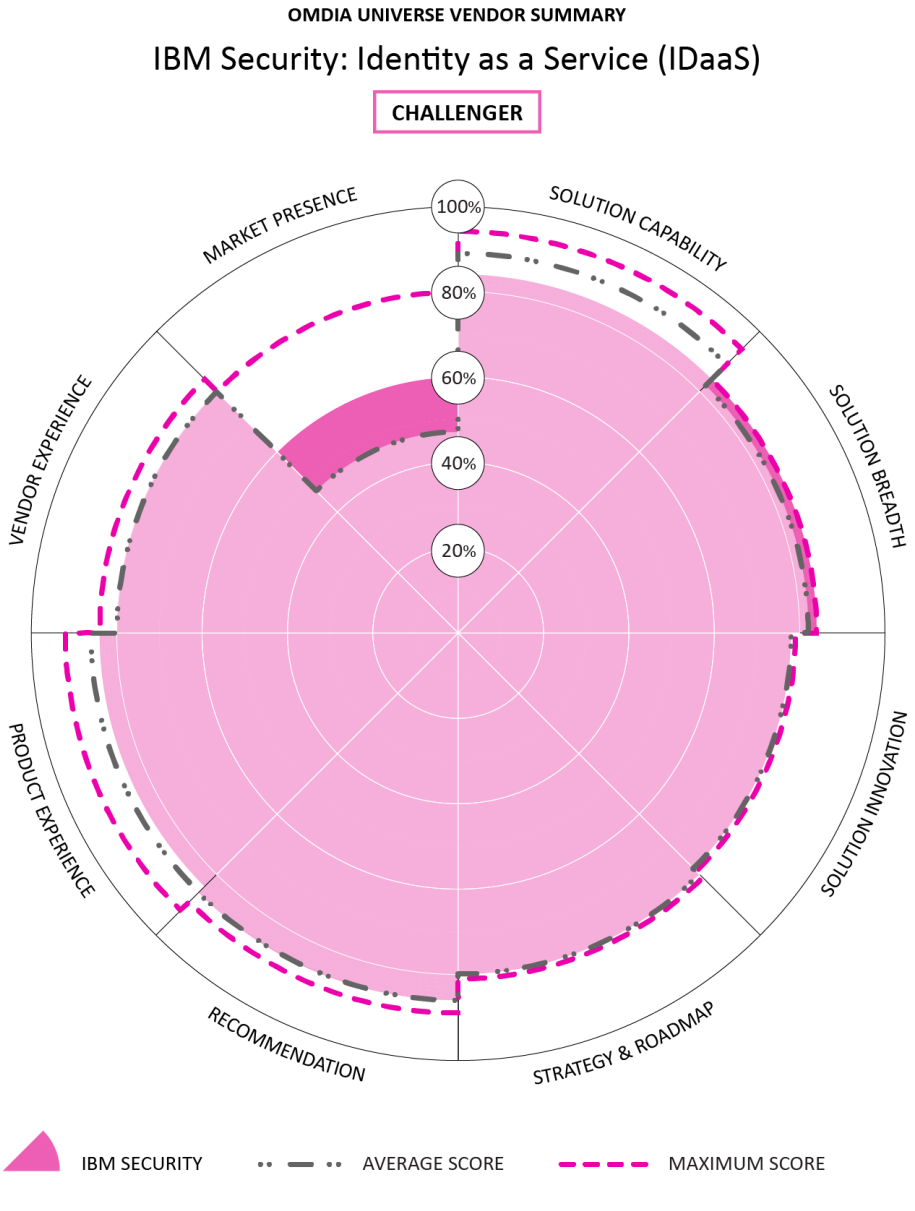
Overview

IBM has a long heritage in the IAM market, dating back at least two decades. In 2002 it bought a company called Access360, whose enroll product was rebranded as Tivoli Identity Manager, or TIM (it had acquired systems management software vendor Tivoli for $760m in 1996). The Tivoli brand was retained through 2012 when it was phased out, with TIM being renamed as IBM Security Identity Manager (ISIM).

Over the last decade, the technology has been migrated to the cloud, and its name has changed again to the IBM Security Verify portfolio of products, which are offered in a cloud-first manner, with on-premises versions available if required.

Figure 6 shows the high-level performance of IBM, where IBM is classified as a challenger in this Universe. IBM was strongest in the supplier capability subcategories of SSO (100%), management and infrastructure (95%), and authentication/MFA (94%). The company was weakest in certification (67%).

Figure 6: Omdia Universe ratings—IBM Security



Source: Omdia

Strengths

The vendor's considerable experience and expertise in identity services mean it presents a comprehensive set of capabilities that span on-premises IAM, cloud-based IDaaS, IGA, and even privileged access management (PAM) via an OEM deal with Thycotic (now Delinea). This means that not only will the vast majority of your requirements from such platforms be available from IBM by

default, but they will almost certainly have someone in their organization who, in the event that you have a more custom requirement, will know what you need and should be able to develop it for you.

The platform supports both the B2E/B2B (i.e., workforce and partner) and B2C (consumer/customer identity and access market (CIAM)) identity use cases. Thanks to increasing regulatory oversight, the latter application these days requires privacy and consent management, and here IBM uses a dedicated engine for the purpose. This is something the vendor considers to be a significant differentiator vis-à-vis the competition because other vendors rely exclusively on user attributes to manage consent and privacy.

Limitations

IBM offers Security Verify in both on-premises software and SaaS delivery modes, arguing that the two meet different use cases. The SaaS hosting geographies for data residency are only available in six regions (the US, Canada, Europe, Japan, China, and Australia).

Even after spinning out its infrastructure services business as Kyndryl in 2021, IBM remains a huge company that is naturally well suited to serving enterprise and midsize customers in both the public and private sector.

All IBM partners go through a certification process to ensure they are equipped to sell the product. If they are not certified, the product cannot be sold. IBM's partners are certified in the product but have varying core focus areas in the IAM space. This may be more challenging for SMBs who may be limited in resources or have less of a focus on IAM. That said, if your identity management needs are pretty standard, you should still be fine with the Security Verify service.

Roadmap

A strategic priority for IBM in 2023 is to make Security Verify easier to consume, with an eye on driving usage outside of the traditional identity admin teams. In order to encourage more line-of-business users to engage directly with the platform, the company is developing a drag-and-drop orchestration engine with a GUI-based editor.

Also on the roadmap is support for the Client Initiated Backchannel Authentication (CIBA) specification from the OpenID Foundation. Whereas typical OpenID Connect flows rely on browser redirects or require user interaction with the client, CIBA enables a decoupled flow where authentication can be initiated on one device and carried out on another. In other words, there is no requirement for user interaction with the client initiating the flow, and there are no HTTP redirects through the user's browser. Instead, CIBA enables direct communication between the Relying Party (client) and the OpenID provider (Authorization Server). In this way, the client can obtain tokens from the Authorization Server for a given user at one device after the same user authenticated and granted consent through another device.

A further enhancement planned for IBM Security Verify is support for Verifiable Credentials (i.e., tamper-evident credentials that can be verified cryptographically). The three essential components of verifiable credentials are that they must be:

- Machine-verifiable.

- Secure and tamper-evident.
- Issued by a competent authority.

IBM plans to offer a mobile wallet with an SDK for customers to handle such credentials, complying with both W3C and decentralized identity standards.

Okta (Omdia recommendation: Leader)

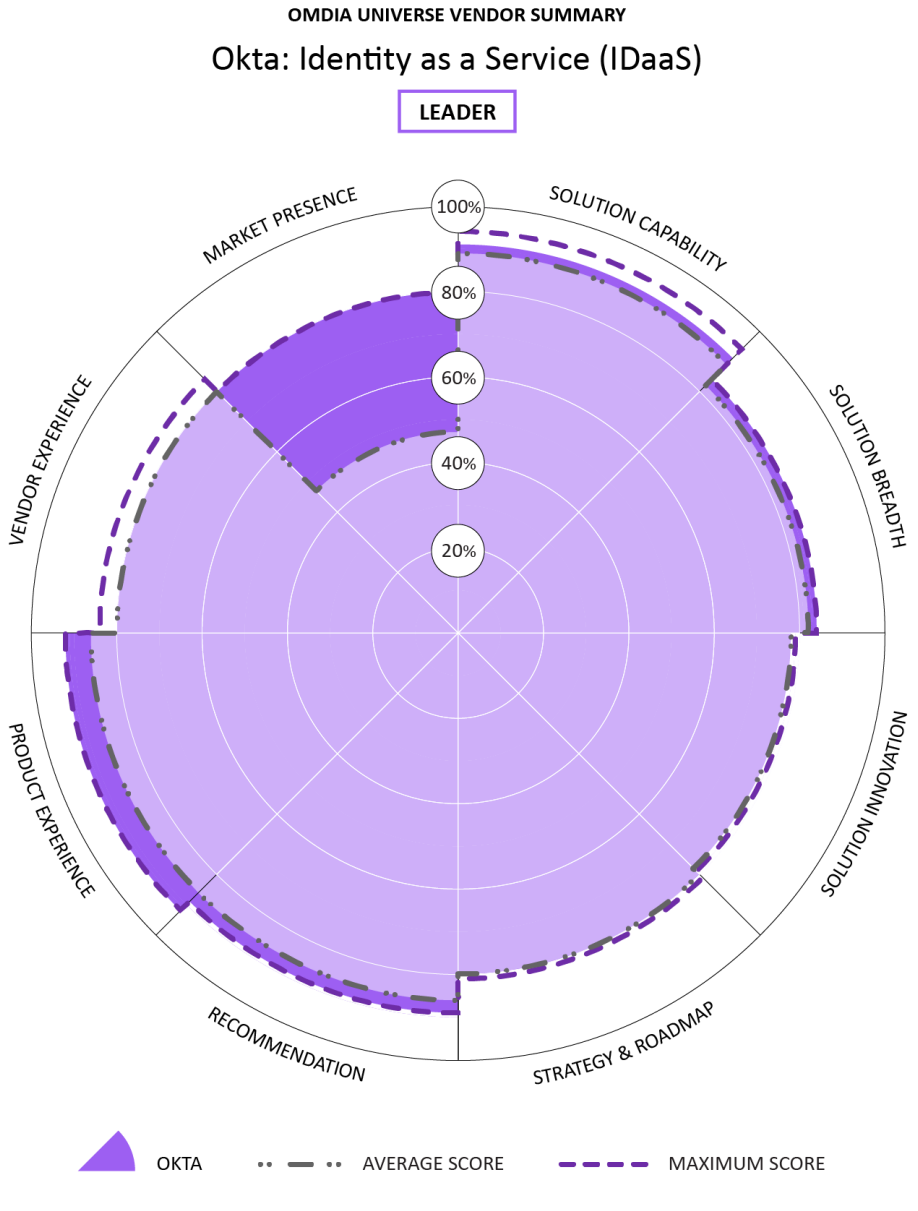
Okta should appear on your shortlist if you need to deliver identity services to employees from the cloud

Overview

Okta delivers identity services for workforce or consumer use cases from the cloud, including features such as authentication and MFA, authorization, user management, and lifecycle management. The platform enables system-to-system access, whereas Okta's Workforce Identity service offers API access management and server access. It can also add a large number of new employees all at once without engaging in a long, slow process of onboarding each of them via a corporate directory. Okta's IAM service can be delivered via public cloud or private cloud services. Okta's products can be licensed on a licensed user basis for Workforce Identity use cases or on a monthly active user basis for CIAM use cases.

Figure 7 shows the high-level performance of Okta, where Okta scored an average of 92% in the capability dimension, 92% in product experience, 89% in customer recommendation, and 80% in market presence. In terms of capabilities, Okta's strengths were authentication/MFA (100%); reporting, alerting, and monitoring (100%); and SSO (96%). Its weakest capability was solution innovation (78%).

Figure 7: Omdia Universe ratings—Okta



Source: Omdia

Strengths

Okta has been in existence since 2009 and has established itself as the first name that comes to mind when the IDaaS topic comes into the conversation. It is almost always the first company that vendors in other areas of security, such as PAM and network and endpoint security, and those in the XDR spectrum mention when listing their integrations with cloud-based identity providers.

Reviewers frequently refer to the platform's ease of use, both for the end user and the IT department. There is also consistent praise for the company's customer support, the strong user community, and good product reliability.

As of September 2021, all customers also have access to Okta Workflows, the company's no-code/low-code identity automation and orchestration platform. This allows customers to automate identity-based actions such as provisioning, joiner-mover-leavers processes, access requests/approvals, as well as security-oriented workflows to detect and remediate anomalous behavior. Omdia sees workflows as being a critical feature that vendors need to incorporate into their IDaaS products/solutions.

Since 2022, Okta SSO and Adaptive SSO have been expanded with the following features: Okta Insights (HealthInsight, UserInsight, ThreatInsights), Suspicious Activity Reports, Okta Verify OTP, Agentless Desktop SSO, integrations with VPNs, RDP, and ADFS, new Identity Providers, and IDP Discovery/Routing rules.

For Workforce Identity use cases, Okta provides SSO or Adaptive SSO for access management (AM) functionality. Okta SSO provides authentication functionality (username/password, RADIUS, Integrated Windows Authentication), password management (password reset via SMS or email), a federation engine for outbound (SAML, WS-Fed, and OpenID Connect) and inbound federation (SAML, OpenID Connect), directory functionality in the form of a user store and fixed set of attributes (over 30), out-of-the-box directory integrations for AD and LDAP with delegated authentication, group-based access policy (to the IDP and per app). They also provide a rich set of authentication APIs, enhanced security for WebAuthn FIDO2 authenticators, integration to MDM solutions (third-party vendors), session management capabilities, support for a wide range of MFA authenticator—including their own phishing-resistant passwordless authenticator "FastPass"—as well as integrations with leading first-party MFA providers.

Okta Adaptive SSO includes all base access management functionality mentioned above as well as a full set of contextual access policy capabilities, such as network user behavior, IP Reputation, Geolocation, or Device Trust. Universal Directory is typically purchased with Okta SSO for access to the full capabilities of the directory (attribute mapping and transformation) and for AD/LDAP password reset. Okta Adaptive Multifactor Authentication (MFA) is added for the full set of authenticators, such as SMS, email, and Yubikey, as well as for all contextual access policy capabilities mentioned with Adaptive SSO. Okta API Access Management adds support for OAuth.

Limitations

One customer commented that integrations with on-premise directories can be complicated to set up. A couple of users said that the mobile app opens to the browser, which can be a bit annoying, especially if you are signing in with a work account. It would be a lot easier and quicker if it recognized you have the mobile app.

Roadmap

There are a number of items on Okta's roadmap. These include:

- Allow List for WebAuthn to restrict the type of WebAuthn authenticators and WebAuthn Profiles to manage Security Keys vs Passkeys differently.

- To introduce Discoverable Credentials to support passwordless with passkeys.
- Connector Builder webhook support and new connectors (2Q23).
- Workflows for CIC (3Q23).
- RBAC and Public API (4Q23).
- Additionally, Okta plans to expand our offering to support MFA to unlock desktop devices across Windows and MacOS.

Oracle (Omdia recommendation: Leader)

Oracle should appear on your shortlist if you are an enterprise that wants to move to the cloud

Overview

Oracle launched its first product in the identity management space, Oracle Internet Directory, in 1999, since when it has been expanding its offering through both internal development and acquisition, adding innumerable features, including directory synchronization, secure directory administration, and a Web SSO service. In the mid-2000s, it made strategic acquisitions, such as Phaos and Oblix in access management, Thor in identity lifecycle management, and OctetString, a virtual directory provider. Other investments brought the vendor capabilities in identity federation, fraud detection, and role management.

A major expansion for Oracle in the identity market came in April 2009 when the database and enterprise software maven acquired Sun Microsystems for $7.4bn. The latter brought with it considerable expertise in IAM technology.

Oracle remains a major player in the identity market, with tens of thousands of IAM customers, particularly in the large enterprise and government segments. Oracle's flagship IDaaS service, OCI IAM, also manages access for nearly 1 million Oracle Cloud customers who benefit from the service at no additional cost. The OCI IAM service manages access for over 550 million identities, not to mention a further 170,000 belonging to Oracle employees.

As a vendor that had a significant presence when IAM was an entirely on-premises business, Oracle has faced the challenge over the last 15 years of developing a cloud-based offering. It initially addressed this issue by offering its on-premises technology in SaaS mode while at the same time developing a cloud-native offering (introduced in 2016).

In addition to addressing workforce and consumer IAM use cases, Oracle Identity Cloud Service (IDCS) grew to become important for Oracle Cloud customers as well and was eventually merged

with OCI IAM to create a combined IDaaS service that serves Oracle Cloud customers as well as more traditional IDaaS use cases.

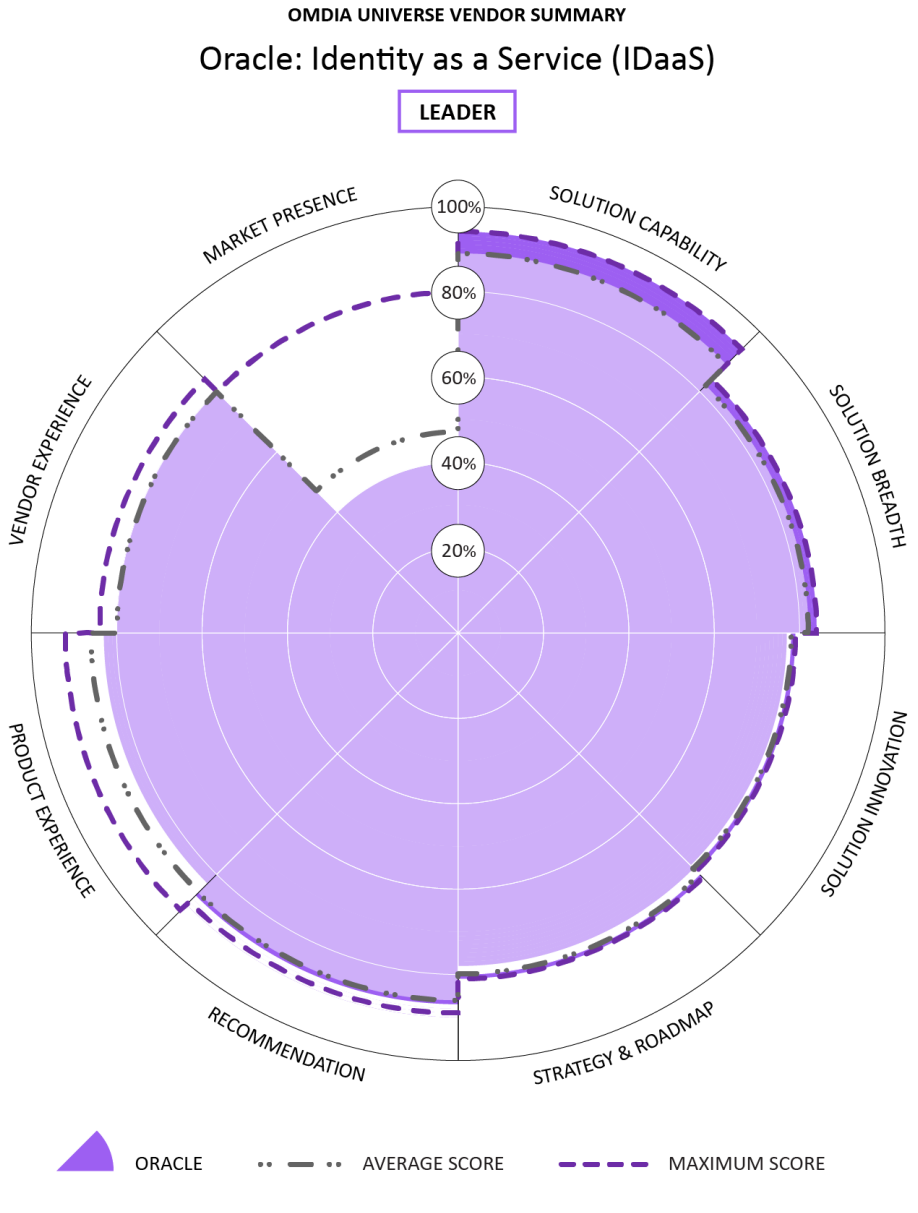
As such, OCI IAM now offers features such as identity federation, integration with on-premises Active Directory and Azure AD, identity lifecycle management, and SSO to apps that support standards such as SAML and OIDC, as well as legacy apps that may require HTTPS header-based authentication or a RADIUS proxy.

Significantly, the cloud-native offering was designed from the outset as an API-first platform, a condition that has now been extended to the entire, expanded OCI IAM. As such, all Oracle-provided consoles are now fully customizable or even replaceable. This is helpful for app developers who can access all OCI IAM features via APIs from within their own code or within their own app consoles.

OCI IAM is typically consumed as a SaaS service, but OCI customers have options such as deploying an Oracle Cloud dedicated region in their own data center or delivering IAM as part of Oracle's white-label cloud service called Oracle Alloy.

Oracle is classified as a leader (see **Figure 8**), an improvement in the last version of this report in 2021. Oracle's strongest categories were solution capability (94%), customer recommendation (87%), solution breadth (84%), and product experience (83%). The company's weakest category was market presence (40%).

Figure 8: Omdia Universe ratings—Oracle



Source: Omdia

Strengths

The depth of Oracle's expertise in identity management is undeniable. It has been in this market for over two decades and has an enterprise customer base that runs into the multiple thousands. It has also successfully developed a cloud-native identity platform to give customers a migration path that they can take at their own pace.

Oracle's identity platform comes with a lot of built-in security by default (i.e., at no extra cost, such as its CloudGuard (which provides cloud security posture management), DDoS protection, data encryption, Threat Intelligence, OCI Logging, and so on).

Oracle deliberately pitches its identity service at a low price point. A free version is available for Oracle Cloud customers. A very low-cost option ($0.25/user/month) is available for managing access to Oracle applications. For organizations requiring the Premium service for workforce access to non-Oracle assets, the maximum additional cost is $3.20/user/month.

Limitations

As a vendor managing a vast existing customer base and a product portfolio that stretches far beyond identity, Oracle may lack some of the agility of smaller and more specialist vendors that live and die on the strength of their identity management platform. If you are a large enterprise customer and/or your identity service requirements are fairly standard, you should be well served by Oracle in this department.

While the technology can be delivered as an on-premises deployment, Oracle Cloud dedicated regions require the customer to have a committed spend on Oracle Cloud Infrastructure (OCI), which may drive up your costs vis-à-vis buying a software-based solution designed to run on-premises, which the vendor also offers via Oracle Access Manager.

Roadmap

Oracle plans to enhance some of the workflows in the platform, with both an abstraction layer for entitlements and the ability to elevate business roles on a temporary basis. This can be thought of as a kind of "PAM lite" capability, with approval workflows and the curtailment of entitlements, etc.

Indeed, having end-of-lifed its dedicated PAM product in 2017, Oracle has been edging back into that market by adding some degree of PAM functionality into its IAM and IGA platforms in recent years.

Also on the roadmap is improved integration of Oracle Access Governance, i.e., the vendor's access governance cloud service, with OCI IAM, as well as deeper integrations with CloudGuard and Oracle Threat Intelligence. Sovereign cloud regions are also due to be released in the near future, with all Oracle cloud services available in them.

Ping Identity (Omdia recommendation: Leader)

Ping Identity should appear on your shortlist if you require a flexible and scalable IDaaS platform

Overview

Ping Identity has been a major player within the IDaaS market for over 20 years. In September 2019, Ping Identity became a private company when it was acquired by Thoma Bravo in October 2022. Ping Identity's sweet spot has traditionally been with enterprise customers, especially those in financial services, healthcare, retail, and manufacturing. All types of use cases are supported, including B2E, B2B, B2C, and government to citizen (G2C), and they have over 3 billion identities under its management.

Ping Identity has a broad IDaaS product portfolio and an extensive technology partnership program. Ping's market focus has traditionally been on large enterprises, and it has the services and support staff to make good on that interest. Ping is also selling products/solutions to the CIAM market.

Figure 9 shows the high-level performance of Ping Identity, where it scored 92.0% in the solution capability dimension, 90% in product experience, and 87% in customer recommendation. Its weakest category was 60% for market presence. In terms of capabilities, Ping Identity's strengths were authentication/MFA (100%), SSO (100%), provisioning (100%), certification (100%), and management and infrastructure (95%). Its weakest solution capability was coverage (79%) and directory service (79%).

Figure 9: Omdia Universe ratings—Ping Identity

Source: Omdia

Strengths

Ping Identity products are based on open standards. Customers can use as much or as little of the Ping suite as they like, depending on which other technologies have been implemented. PingOne Cloud Platform is ideal for customers looking for a scalable IAM solution capable of supporting multiple employee, customer, and partner identity use cases on-premises and in the cloud. The

platform is also suited for high-security applications that need to have secure data or standards-based and non-standards-based applications with more complex integration requirements.

PingOne Cloud Platform offers customers a choice of multiple deployment options, including offering solutions across hybrid, multicloud, multigenerational, cloud-first, or completely on-premise environments. This allows customers to retain access to the various integration accelerators/plug-ins that Ping provides with the flexibility of a SaaS-like deployment. Moreover, deployments are also possible via a cloud/docker and through APIs. Finally, Ping Central offers self-service application integration with prebuilt authentication and authorization templates for app owners across the organization.

A number of users of PingOne Cloud Platform have stated that it is easy to set up and is flexible and scalable. They find the platform easy to integrate new products and services and like the fact that they can choose what they need without vendor lock-in. This also helps to streamline multivendor architectures without the need for custom coding. Ping Identity also offers hundreds of integration kits, connectors, and templates to orchestrate flows that fulfill capabilities quickly, including identity verification, digital credentials, profile management, SSO/authentication, MFA, authorization, and threat protection.

Limitations

One customer stated that the product helm charts were not very flexible or easy to modify. Also, PingAuthorize—formerly PingDataGovernance and Symphonic—has a few bugs. Omdia believes that these issues can be ironed out and improved in newer versions of the product.

Another user said that the Ping solution was a bit complex to link to the Azure AD environment. They went on to say that the SSO link is very generated-looking and that they would like a way to make it more official. Also, this potentially adds another point of failure to the product.

Roadmap

There is a comprehensive list of items on Ping Identity's technology roadmap. These include:

- New authentication platforms, including WhatsApp and voice recognition.
- In 2H23, Ping will release its first set of passwordless flow templates, specifically for the CIAM use case, enabling customers to easily configure passwordless flows that leverage all their IdPs and industry best practices.
- In 2023, the company intends to add the ability to use analytics and/or intelligence (AI/ML) to make recommendations on access improvements or efficiencies opportunities.
- A key component of Ping's orchestration and platform evolution is to continue to create integration kits, connectors, and flow templates to easily deploy the following capabilities: threat protection, identity verification, digital credentials, profile management, SSO/authentication, and MFA.
- Ping also plans to launch out-of-the-box (OOTB) Solutions that cross multiple capability sets and aligns them around specific customer use cases. The first two solutions will be for CIAM

Passwordless and Zero Trust. These solutions will incorporate capabilities from across Ping's services, packaged and delivered to enable customers to realize the benefits with only a few clicks. This means taking something like "passwordless" and providing OOTB, best practice flows that allow customers to choose their options as well as give their customers a path to migrate from a password to passwordless. Passwordless is one option, and Ping is building out these journeys in both horizontal solutions, like passwordless and zero trust, and vertical solutions, such as digital retail experience and finance client management.

- In 2023, Ping will create dashboards that create insights for customers across all of their Ping services. Dashboards will go beyond simple data readouts by service and ensure that customers see the key insights across all their services. These dashboards will enable customization by leveraging a data lake that contains key data from across the Ping ecosystem. In addition, the company’s DaVinci Orchestration platform will be expanding the metrics available so that customers have detailed insights into the journey paths their users are taking.

- Decentralized identity is a key part of Ping's roadmap. It is an approach to IAM that allows users to control their identity information. Sometimes referred to as self-sovereign identity, it eliminates the need for users to provide unnecessary amounts of personal information to access a service. Organizations issue users verifiable digital credentials that are stored in a digital wallet. Users present their credentials to organizations that verify the information instantly without contacting the issuer. PingOne Neo is Ping’s new decentralized identity solution. Neo verifies IDs, documents, and identity claims and issues digital credentials based on those. Users can share credentials with organizations to quickly and effortlessly prove who they are.

Other vendor(s) to watch

Microsoft Entra

Overview

Microsoft declined to be included in this IDaaS Omdia Universe due to the timing of its announcement of net-new features within the Microsoft Entra product family. However, Omdia considered it imperative to include a profile of the company's identity offering due to its size and influence on this market.

Microsoft has long seemed to play the role of "sleeping giant" in the identity market. While it never competed in the on-premises IAM market per se, nor indeed in PAM, its huge presence in the corporate directory sector with its Active Directory product gave it a commanding view of developments in the field. This positioned it to expand its activities, particularly as cloud computing grew as the new paradigm for enterprise IT, and in this context, the launch of the cloud-based version of the directory—Azure AD—in the year 2000 was a key development. Since then, the vendor has expanded its offerings in the broader identity market hugely.

At the start of June 2022, just before RSAC 2022, Microsoft announced a new product family, Microsoft Entra, which encompasses all of Microsoft's identity and access capabilities. Microsoft Entra products include:

- Azure Active Directory (Azure AD).
- Microsoft Entra Permissions Management (a new cloud permissions management (CPM)/cloud infrastructure entitlements management (CIEM) solution).
- Microsoft Entra Verified ID (a new decentralized identity product offering).

Microsoft Azure AD is now part of the Microsoft Entra family, and all its capabilities, such as conditional access and passwordless authentication, remain unchanged. Azure AD External Identities continues to be the vendor's identity solution for customers and partners under the Microsoft Entra family.

The automation of identity governance use cases

Identity governance for employees and partners is another area of focus for Microsoft. It's a significant challenge for IT and security teams to provision new users and guest accounts and manage their access rights manually. This can have a negative impact on both IT and individual productivity. New employees often experience a slow ramp-up to full effectiveness while they wait for the access required for their jobs. Similar delays in granting necessary access to guest users undermine a smoothly functioning supply chain. At the other end, without formal or automated processes for reprovisioning or deactivating people's accounts, their access rights may remain in

place when they change roles or exit the organization (the dangerous “orphan account” scenario that can be exploited by threat actors).

Microsoft believes that its **Identity Governance (in Azure AD)** offering addresses this with identity lifecycle management, which simplifies and speeds up the processes for onboarding and offboarding users. Lifecycle workflows automate assigning and managing access rights and monitoring and tracking access as user attributes change. Lifecycle workflow enhancements in Identity Governance entered public preview in July 2022.

Omdia believes that automating identity, authentication, and access features and tasks is a key trend within this space. There is an ever-increasing amount of security-related data/telemetry that companies need to keep secure and interpret when things go wrong, which is driving the need to automate features and tasks in order to keep up. Indeed, this increase in data drives automation in a number of segments within the identity, authentication, and access sector.

Microsoft Entra Permissions Management (Cloud Permissions Management)

Microsoft stated that the Microsoft Entra Permissions Management product/solution would be a standalone offering, as well as being integrated within the Defender for Cloud dashboard, extending Microsoft Defender for Cloud’s protection into the CPM realm (aka CIEM). It is worth recalling the history and development of this product. In July 2021, Microsoft acquired the market leader in CPM technology CloudKnox Security with a view to enabling businesses using its Azure Active Directory service to exercise tighter control over employees’ access rights to their cloud assets, regardless of which cloud they reside in.

CPM is an emerging technology segment, with most of the start-ups offering the capability dating from the late 2010s. CloudKnox was among the first, having been founded in 2017. So recent is the technology that it still has no standard name: one analyst firm calls it CIEM, which is both excessively wordy and confusing, given its similarity to SIEM and CIAM. Another calls it cloud identity governance, which is less self-explanatory than Omdia’s preferred name, cloud permissions management. Microsoft’s permissions management product/solution, which was an evolution of the CloudKnox technology, was made available worldwide in July 2022.

It is also worth noting that the Permissions Management product is cloud-agnostic, i.e., it is able to enforce the principle of least privilege in Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

Microsoft Entra Verified ID (decentralized identity)

Microsoft Entra Verified ID is a new product offering based on decentralized identity standards that makes portable, self-owned identity possible. Instead of granting broad consent to countless apps and services and spreading identity data across numerous providers, Verified ID allows individuals and organizations to decide what information they share, when and with whom they share it, and—when necessary—to take it back by rescinding access rights. The Verified ID product has been available since August 2022. Omdia sees that decentralized identity is gaining traction, and this announcement by Microsoft to launch a product in this space should help to turbocharge the segment.

Microsoft Entra External ID

On May 24, 2023, Microsoft announced new developer-centric capabilities for customer and partner identity experiences in their next-generation CIAM solution, called Microsoft Entra External ID. It represents an evolutionary step in unifying secure and engaging experiences across all external identities, including customers, partners, citizens, and others, within a single, integrated platform. It includes all familiar features of Azure AD External Identities plus new capabilities, now in public preview, including developer-centric tools to build secure, compliant web and mobile applications for customers, citizens, and partners—within minutes.

Microsoft Entra Verified ID SDK

On May 24, 2023, Microsoft also announced the next milestone in making Microsoft Entra Verified ID easy to integrate into any application with Microsoft Entra Verified ID SDK**.** Microsoft Entra Verified ID is an open standards-based verifiable credentials service that customers can use to automate verification of identity, such as government-issued identity documents, face matching, and electronic data verification, in a secure, privacy-respecting manner. The upcoming release of the Verified ID Wallet Library (iOS, Android) can be integrated into mobile apps to store and share digital Verified ID cards. This allows organizations to issue verifiable credentials for dozens of use cases, such as reducing the risk of fraud or account takeovers, streamlining app sign-ins, creating self-service account recovery, and helpdesk flows.

In July 2023, Omdia plans to produce a more detailed profile of Microsoft Entra and its roadmap of products within the identity, authentication, and access space.

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and Omdia's enterprise insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Vendors are interviewed and provide in-depth briefings on the current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

The criteria for inclusion of a vendor in the *Omdia Universe: Identity-as-a-Service Solution, 2023* report are as follows:

- The vendor must be a global vendor with customers in all three major business regions: Asia & Oceania, EMEA, and North America.
- 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 must support major client relationships, including business-to-business (B2B), business-to-employee (B2E), and machine-to-machine (M2M) and IoT interactions.

- It should deliver core identity management services that include authentication; access controls; SSO; provisioning and deprovisioning; self-service registration and password management; directory integration and management; reporting, alerting and monitoring; and identity governance.

Exclusion criteria

Some IDaaS specialists focus only on particular disciplines, such as authentication as a service or customer-facing identity management, or 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. That being the case, 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 enterprises 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, revenue, or market presence to compete with the leading IDaaS providers.

Authors

Don Tait, Senior Analyst, Cybersecurity, Identity Authentication Access

Rik Turner, Senior Principal Analyst, Cybersecurity, Emerging Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

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

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com