Magic Quadrant for Access Management

Published 1 November 2021 - ID G00740722 - 64 min read

By Henrique Teixeira, Abhyuday Data, **and 1 more**

Access management has become the source of trust for identity-first security. Increased dependence on identities for access anywhere, anytime, requires AM to be more reliable and easier to adopt. Identity orchestration, IAM convergence and SaaS resilience importance will increase during 2022.

Strategic Planning Assumptions

By 2025, converged IAM platforms will be the preferred adoption method for AM, IGA and PAM in over 70% of new deployments, driven by more comprehensive risk mitigation requirements.

By 2024, low-code/no-code orchestration tools will be a critical capability for all AM products, up from 15% today.

Market Definition/Description

Gartner's view of the market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

The access management (AM) market is defined by customers' needs to establish, enforce and manage runtime access controls for internal and external types of identities, interacting with cloud, modern standards-based web and legacy web applications.

An AM vendor provides, at minimum, the following core capabilities:

- Identity administration of internal and external types of identities, including directory and identity synchronization services
- User self-service, including end-user and administrative interfaces for user registration, password management, profile management and delegated administration
- A workforce launchpad of applications or application gallery for single sign-on (SSO)
- Authorization and adaptive access, and support for modern identity protocols like OAuth 2.0

- Session management
- User authentication methods, including multifactor authentication (MFA), and SSO
- Bring your own identity (BYOI) integration, to use public identities, such as social media accounts, for access
- API access control for handling authentication and authorization to API targets
- Standard application enablement, including capabilities to enable rapid access, SSO and MFA to SaaS and standards-based web applications by leveraging modern identity protocols like SAML and OpenID Connect
- Nonstandard application enablement, including capabilities to enable access, SSO and MFA to legacy web applications that do not support standards-based SSO protocols
- Analytics capabilities, including historical reports, logs and identity analytics information about administration and runtime access events

Optionally, an AM vendor may provide these capabilities:

- Management of machine identities (bots, workloads, Internet of Things [IoT]), and support B2B2C and B2B2E use cases. May also be able to manage access to non-web applications, like client/server apps.
- Support for at least basic identity governance and administration (IGA) capabilities like identity life cycle management, user provisioning, access requests with approvals and access certifications.
- Support for virtual directory capabilities. The AM tool may also provide identity data aggregation and integration with external platforms like marketing, CRM and customer analytics.
- End-user and administrative interfaces for progressive profiling, consent, preference and privacy management, and multichannel support.
- Low-code/no-code orchestration interfaces for developers and administrators.
- Fine-grained authorization, externalized authorization management (EAM), access orchestration and workflows for decision tree support of external authentication and authorization methods.
- Online fraud detection, identity proofing and affirmation, security and user and entity behavior analytics (UEBA) capabilities, cloud access security broker (CASB), either natively or via integration with third-party providers.
- Supporting application-by-application settings for session control and adding attributes to the token for session management purposes.

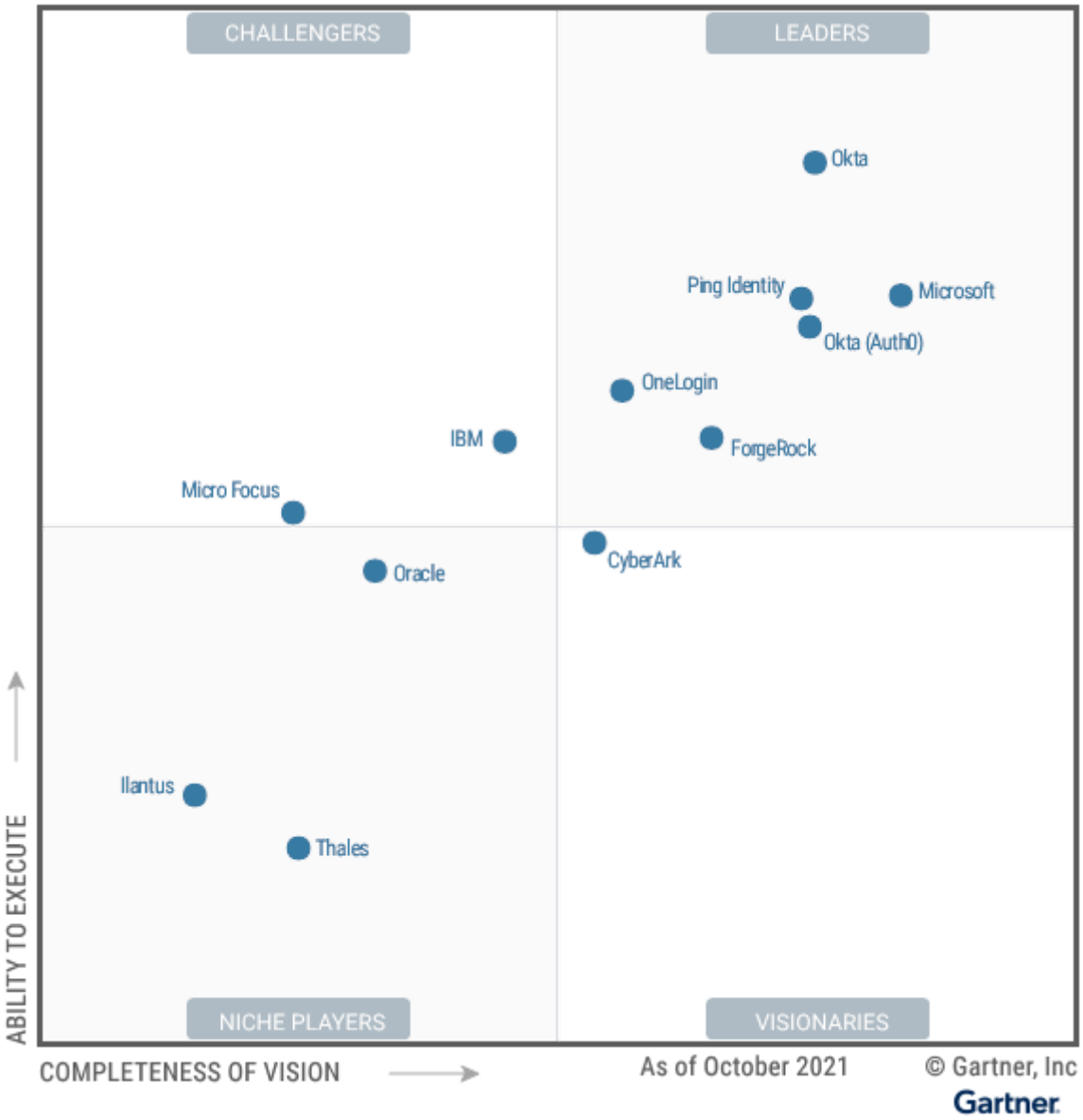
- Support for a broader range of MFA methods, including X.509 and FIDO hardware and software tokens, device native and third-party biometrics, and options for passwordless and continuous authentication.
- Advanced BYOI integrations with cloud service provider identities (like Apple, Microsoft and Google IDs), bank ID, government ID, mobile network ID and decentralized identity services.
- Advanced API access controls that provide either libraries, sidecar containers or out-of-the-box (OOB) integrations with APIs and API mediators to centralize authentication and authorization decisions to the authorization server. It may also include developer self-service capabilities for managing apps and services. It may support flows such as the OAuth Mutual Transport Layer Security (mTLS), the JSON Web Token (JWT) and SAML grant types, device flow, token exchange, introspection and revocation. It may provide strong and agile cryptographic mechanisms for signing tokens.
- Developer tools for containerization and modern architecture deployments.
- Multiple key signing support for standard application enablement.
- Diagnostic, predictive and prescriptive analytics. May also include UEBA and identity threat protection capabilities (advanced threat protection, compromised identities, and malicious insider actions). It may also offer Web App Firewalls, and other identity security protection capabilities based on analytics and ML.

Pricing

To illustrate a high-level perspective for vendor pricing in the vendor descriptions in this Magic Quadrant, we comment on the pricing of individual products, using such terms as “well above average,” “above average,” “average,” “below average” and “well below average.” The average for a particular component refers to the average score for all vendors evaluated in this research for a variety of different AM pricing scenarios.

Magic Quadrant

Figure 1: Magic Quadrant for Access Management



Source: Gartner (November 2021)

Vendor Strengths and Cautions

CyberArk

CyberArk is a Visionary in this Magic Quadrant. Its CyberArk Identity product is focused on a SaaS-delivered AM approach. Its operations are geographically diversified, and its AM clients tend to be small to midsize organizations looking for workforce AM.

Recent innovations include passwordless capabilities using QR codes and FIDO2, an AM extension for adaptive MFA for desktops and servers, and identity affirmation services through a partnership with Ekata (acquired by Mastercard). CyberArk plans to invest up to 23% of its revenue in R&D to build a new SaaS platform for converged identity and access management (IAM) services and add continuous authentication.

Strengths

- In Gartner's evaluation, CyberArk achieved the highest score for operations. It has kept the majority of the experienced AM product leadership and engineering teams from the Idaptive acquisition in 2020.

- CyberArk demonstrates good vision and response to market trends, resulting in the several product innovations mentioned. It has R&D plans for expansion of its AM product into a SaaS IAM converged platform.

- CyberArk offers above-average analytics capabilities, with over 70 out-of-the-box reports and seven dashboards. It can also consume external user analytics and risk signals, and use those for adaptive access flows.

- The CyberArk AM product can be a good choice for clients looking for the benefits of AM integration with the broader CyberArk privileged access management (PAM) portfolio. It is the only vendor in this research that offers a complete PAM solution.

Cautions

- The overall renewal rate for CyberArk SaaS-delivered AM products has decreased since last year and is the lowest evaluated for this research. It also received below-average scores for ease of deployment.

- The pricing for several scenarios evaluated in this research is well above average for more complex workforce AM scenarios, with customer IAM (CIAM) scenarios marginally above average.

- There is no 99.99% SLA option for availability (it stops at 99.9%).

- CyberArk offers fewer features for CIAM and developer use cases, and only scores average for API access control and developer tools.

ForgeRock

ForgeRock is a Leader in this Magic Quadrant. ForgeRock sells its Access Management product stand-alone or in a bundle, delivered as SaaS or software. Its operations are geographically diversified, and its clients tend to be larger organizations, mostly in banking, communications, media and service sectors, looking for SaaS-based, on-premises or hybrid deployments for internal and external AM use cases.

Recent innovations include support for B2B2C/B2B2E scenarios, and a feature for developers that provides user authorization to data streams. ForgeRock went public in September 2021, and plans to

invest 25% of its revenue in R&D to grow its developer capabilities, analytics, data science, emerging OAuth2 standards, UEBA, edge computing and financial transaction authorization.

Strengths

- ForgeRock offers strong product capabilities for internal and external AM use cases, combined with good features for API access control and developer tools. The product offers a good balance in adoption for internal and external AM as well as developer use cases.
- ForgeRock scored high for market understanding, with special focus on customer experience, developers, and vertical alignment with the healthcare and finance sectors.
- ForgeRock offers a 99.95% availability SLA, with free nonproduction environments in every SaaS subscription and free access to the software versions of the SaaS products (to be installed on hybrid deployments).
- ForgeRock scored high in its AM product identity administration capabilities, with strong directory services. In addition, ForgeRock sells IGA software products that can provide synergies for clients looking for a converged single-solution vendor.

Cautions

- ForgeRock's pricing for all scenarios evaluated in this research is above average compared to its competitors.
- ForgeRock has scored below average in its product's AM analytics capabilities. There's no UEBA capability, and obtaining analytics insights about runtime data is complex.
- While there was growth in revenue, ForgeRock's customer count growth lags behind other Leaders in this research.
- ForgeRock scored below average in innovation and did not deliver on some features that were in the roadmap last year, such as UEBA.

IBM

IBM is a Challenger in this Magic Quadrant. Its product is offered as software (IBM Security Verify Access) and SaaS-delivered (IBM Security Verify) options, focused on a converged approach for AM and other IBM Security products. Its operations are geographically diversified, and its clients tend to be large organizations, mostly in the banking and public sector industries, looking for on-premises and hybrid deployments.

Recent product innovations include new data privacy and consent management features, a software development kit (SDK) for adaptive access flows and a containerized version of its proxy. IBM plans to invest in simplifying integration of legacy applications, more CIAM capabilities for trusted delegation and decentralized identities.

Strengths

- IBM offers good value, with pricing for the series of scenarios evaluated in this research consistently lower than its competitors.
- IBM has released a dedicated instance of its SaaS service (IBM Security Verify Dedicated) that can be run on other clouds. This potentially offers useful features for clients looking for data privacy and more resilience, and using multicloud/multiregion deployment strategies.
- IBM plans to invest in more synergies for its AM product with Cloud Pak and Red Hat OpenShift. Clients that have invested into IBM's or Red Hat's ecosystems may find synergies through additional integrations and support planned for its AM products.
- IBM scored the highest in identity administration with strong capabilities for identity synchronization. It also offers fraud detection capabilities embedded within its SaaS AM product, as well as integration with other IBM Security products, including IGA.

Cautions

- Except for the consent management capabilities and a dedicated instance for SaaS AM, IBM has only added incremental innovations to its product since last year.
- IBM scored below average for customer experience, and has no 99.99% SLA option for availability (it stops at 99.9%). The products are also complex to use. Gartner clients describe a steep learning curve to implement and support the product.
- IBM is not a popular choice among small to midsize enterprises, and based on Gartner client inquiry, interest in the IBM product has declined.
- IBM scored below average for its marketing and product strategy. It also saw some turnover in its IAM product leadership teams.

Ilantus

Ilantus is a Niche Player in this Magic Quadrant. Its Compact Identity product is mainly focused on delivering AM as part of a converged SaaS-delivered IAM platform for small to midsize organizations. Its operations are mostly focused on the Asia/Pacific (APAC) region, with a smaller portion of clients in the Middle East, Europe and North America.

Recent product innovations include a risk engine, adaptive access, an access management bundle tailored to midsize enterprises and accompanying professional services packages for implementation. Ilantus plans to invest 15% of its revenue in R&D to add consent management, robotic process automation and identity proofing capabilities to its platform.

Ilantus did not respond to requests for supplemental information, or for a review of the draft contents of this research. Therefore, Gartner analysis is based on other credible and accepted public sources.

Strengths

- Ilantus' pricing, evaluated for a series of less complex AM scenarios, is consistently below the market average.
- Ilantus offers a 99.95% availability SLA as standard, with an optional paid SLA of 99.99%.
- Ilantus scored above average for identity administration capabilities, and supports inbound and outbound SCIM, account linking, dynamic data retrieval, and webhook integration patterns.
- Ilantus' Compact Identity is a good option for small to midsize enterprises looking for a lower-cost, all-in-one converged IAM platform for AM, IGA and PAM.

Cautions

- The Compact Identity product is broad in other adjacent areas of IAM; however, except for identity administration and ease of deployment, it scored below average for its AM product capabilities. For example, it lacks a native app for mobile push MFA, native support to government eIDs, and stronger developer tools such as a visual flow designer or orchestration.
- Ilantus scored lowest among vendors in this research in offering (product) strategy, and innovation. Ilantus' vision and roadmap are catching up with other AM vendors, enhancing its current SSO and life cycle management capabilities.
- Ilantus has the least amount of documentation, by far, among any vendor evaluated in this Magic Quadrant. Compared to most vendors evaluated in this research, the provided documentation touches on all capabilities, but is lacking in detail.
- Based on Gartner client inquiry, brand awareness of the Ilantus product is very low, with very few mentions when compared to other vendors in this research. There are also no Gartner Peer Insights reviews for Ilantus at the time of this publication.

Micro Focus

Micro Focus is a Challenger in this Magic Quadrant. Its NetIQ Access Manager software and NetIQ AM SaaS modules are mainly focused on hybrid deployments with on-premises applications and

cloud extensibility. Its operations are geographically diversified, and clients tend to be large organizations in manufacturing, banking and the public sector.

Recent product innovations include its first AM SaaS modules, additional DevOps capabilities for its API management tool and extension of MFA capabilities to nonweb targets. Micro Focus plans to invest 22% of revenue in R&D, to continue to release more SaaS and containerized versions of its products, add more privacy capabilities, and expand analytics features.

Strengths

- In a series of pricing scenarios evaluated in this research, Micro Focus' pricing is below the average.
- Micro Focus offers a 99.95% availability SLA.
- Micro Focus scored above average for its product capabilities in BYOI integration, as well for its authorization and adaptive access due to the integrations with adjacent tools, Fortify and ArcSight Intelligence (formerly Interset), for application development security and behavior analytics.
- Micro Focus' new Cloud Bridge service simplifies identity synchronization with on-premises directories. Micro Focus continues to be a good fit for larger organizations and for more complex hybrid environments (especially existing Micro Focus clients) that prefer the flexibility of managing on-premises deployments.

Cautions

- As noted last year, Micro Focus provides a limited catalog of only a few hundred preintegrated applications, compared with thousands from other vendors.
- NetIQ Access Manager scored below average in ease of deployment. Gartner clients have shared opinions about the extensive and rich features available in the product; however, there is a steep learning curve for deployment and management.
- Micro Focus obtained the lowest score among vendors in this research for the offering (product) strategy. Except for the planned consent governance capability, the product roadmap consists of mostly catch-up features that already exist in other AM vendors, or features that are not core to AM, like data governance and administrative APIs.
- Micro Focus has started to deliver some of its AM products as a service, but, to date, only three core AM services are generally available: NetIQ Advanced Authentication, NetIQ Risk Service and NetIQ Cloud Bridge. As of this writing, other components are still in beta, making Micro Focus the only vendor in this research without a full suite of AM capabilities that can be consumed as SaaS.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its Azure AD product is sold in bundles and is focused on delivering AM as part of a converged SaaS IAM platform for internal and external AM use cases. Its operations are geographically diversified, and its clients vary in size and industry. Most Microsoft clients use its products for workforce scenarios.

Recent product innovations include the addition of FIDO2 support (for passwordless authentication), an agent for joining AD forests and adaptive access for CIAM. Microsoft plans to invest 10% of its security revenue in R&D for risk protection in multicloud infrastructures, enhancing embedded adjacent IAM capabilities, and improving decentralized identity and verifiable credential features.

Strengths

- Microsoft has the strongest vision among all vendors in this research. It achieved the highest score for offering (product) strategy due to its identity-first, security-aligned AM roadmap plans. These include work in decentralized identity standards, multicloud security embedded to AM (through the acquisition of CloudKnox Security in July 2021), and planned PAM and IGA capabilities.
- Microsoft's overall pricing analyzed for various scenarios in this research is below the market average, with external AM use-case pricing well below the average compared to its competitors (but see first caution below).
- Microsoft offers 99.99% availability SLA.
- Microsoft achieved the highest score in overall viability and sales strategy. The decision of bundling Azure AD with Microsoft 365 and EMS licenses helped Microsoft to double the number of its clients, to more than 300,000 organizations in 2020. This wide adoption helps organizations find trained resources.

Cautions

- Azure AD received the lowest aggregate score for product capabilities among Leaders in this research. External AM use cases and session management capabilities are immature compared with other vendors' offerings, and most clients are using the product for workforce scenarios only.
- Azure AD suffered two outages of over 16 hours in late 2020 and early 2021 (the biggest among all vendors in this research). That affected the vendor's scoring in security, resiliency and coverage. Microsoft has not yet offered hybrid failover options for its services (from cloud to on-premises), like a few other vendors have started to do.
- Despite substantial investments in security R&D, Microsoft's AM product capabilities are still lagging behind other Leaders in this research, especially in CIAM.
- Last year's product innovations consisted mostly of catch-up features (FIDO2 support, agent for disconnected AD cloud sync, adaptive access for CIAM).

Okta

Okta is a Leader in this Magic Quadrant. It offers a SaaS-delivered converged AM platform, focused on both internal and external AM use cases. Its operations are geographically diversified, and its clients tend to be small to midsize organizations.

Recent product innovations include new developer and CIAM-oriented products acquired in May 2021 through Auth0's merger. It has also launched Okta Workflows for Customer Identity, new FedRAMP certifications and improvements to the Okta Access Gateway. Okta plans to invest 27% of revenue in R&D for a new consumer initiative called Personal Okta, device posture management for Windows and macOS (Okta Devices), identity orchestration expansions, and on-premises extensions for managing Active Directory.

Strengths

- Okta scored highest among all vendors for its product capabilities. It enabled its identity orchestration (Workflows) for all AM use cases and improved its user interface. Okta also scored highest in user self-service, standard application enablement and ease of deployment.
- Okta received the highest score for customer experience in this Magic Quadrant. Gartner clients have mentioned the product's ease of use, flexibility in integrating with a broad number of apps and the high quality of documentation available.
- Okta scored highest for security, resiliency and coverage. Okta can now offer automatic failover from cloud to on-premises, which is an extremely necessary feature among SaaS AM vendors. It offers 99.99% SLA availability to all customers, even for free tiers, which is also unique among all vendors surveyed.
- Okta scored very high in innovation, with the completed acquisition of Auth0 and its plans to invest above market average in R&D. Aside from the executed innovations, it plans to grow its AM products into a converged IAM platform with IGA and PAM capabilities, including the acquisition of atSpoke, a workplace operations platform, in August 2021.

Cautions

- Pricing continues to be well above average, and Gartner clients have consistently mentioned the high cost of Okta's solution.
- Directory integration and identity life cycle continue to be limited, especially when compared with other AM vendors that have, since last year, added more robust identity administration capabilities.
- Although Okta has a diversified geographical operation (with instances of the service in the U.S., Germany, Ireland, Singapore and Australia), Okta's installed base is still largely concentrated in North America.

- Okta's leadership teams have seen significant turnover, including a new CTO, CFO and CMO. The success of the merger with Auth0 will depend on how well both products and people will work together, and on the integration's impact on innovation.

Okta (Auth0)

Okta (Auth0) is a Leader in this Magic Quadrant. Auth0 is an independent product unit within Okta (acquired in May 2021). Its AM products focus mostly on SaaS-delivered developer-centric and CIAM use cases. Its operations are geographically diversified; its clients tend to be small to large organizations looking to add AM controls to custom-developed, API-driven applications.

Recent innovations include more B2B partner and customer management capabilities, platform extensibility, and embedded credential-stuffing attack detection and remediation. Auth0 plans to invest in growing its capabilities in B2B2E/B2B2C use cases and new areas like fine-grained authorization, and to deepen integration with Okta Workflows.

Strengths

- Auth0 achieved the highest score for innovation, with several AM product enhancements, and plans for high investment in R&D (percentually). Nontech innovations were also noteworthy: Auth0 struck a deal with Salesforce and created an OEM product for CIAM that will be sold by Salesforce in its customer cloud platform. The Okta acquisition can bring potential opportunities for more cash funding for its roadmap plans.

- Auth0's pricing is competitive, with scalable developer pricing, including free tiers. Almost all pricing scenarios are below and sometimes around the average of the vendors in this research.

- Auth0 offers 99.99% uptime SLA to all customers and an option for dedicated and hosted services in Amazon Web Services (AWS). Together with a solid list of CRM integrations and the most comprehensive BYOI integration list in this research, this makes Auth0 a popular solution for CIAM.

- Great UX flows and UI customization abilities can host entirely modified pages beyond simple white labeling. Combined with comprehensive developer tools and full API support (with signing key rotation), this makes Auth0 the best option for AM developer use cases.

Cautions

- Auth0's acquisition by Okta could cause overlap and confusion for prospective buyers if the combined companies' vision convergence, product alignment and integration aren't smooth.

- Auth0 scored below average on identity administration because it depends entirely on external tools (and API integrations) for basic functions, like life cycle management and workflows. It doesn't offer out-of-the-box SCIM-based connectors, only a generic SCIM adapter that needs to be customized every time you want to integrate with target applications.

- Auth0's product is weak for internal AM (workflorce) use cases, and it has a limited catalog of preconfigured SaaS application integrations. The workforce dashboard with SSO launchpad is not installed by default; it requires a custom deployment.
- Auth0's approach for nonstandard application enablement is limited, and it has to rely on either an external identity-aware proxy; or service providers, like NGINX, AWS Application Load Balancer (ALB), Okta Access Gateway and third-party libraries; or Apache SDKs.

OneLogin

OneLogin is a Leader in this Magic Quadrant. Its SaaS-delivered products are mainly focused on delivering AM capabilities with converged lightweight identity administration features. Its operations are geographically diversified, and its clients tend to be small to midsize organizations mostly using the product for internal AM use cases.

Recent product innovations include extensibility through a feature called Smart Hooks to facilitate customization, new APIs and interfaces for delegated administration, and a dashboard for identity security insights. OneLogin plans to invest 20% of revenue in R&D to enhance its Smart Hooks capabilities, expand geographically, and develop its decentralized identity, CIAM and identity proofing.

Strengths

- OneLogin's product offers competitive pricing for external AM use cases.
- OneLogin received one of the highest customer satisfaction scores in this research. Gartner customers have mentioned the ease of management and administration, integration and deployment.
- OneLogin plans to continue to invest in resiliency, and today offers a service called HydraBoost that supports 1 million login operations a minute. OneLogin didn't suffer outages in the past year (only five incidents of service degradation, five hours total) and offers a paid option of 99.99% SLA for availability. The standard for all customers is 99.9%.
- OneLogin received the highest score among vendors in this research for market understanding. The vendor's awareness of its own strengths and weaknesses is important for customers looking for best-fit solutions, as OneLogin may have a better accuracy in targeting opportunities that are a best match to its products.

Cautions

- OneLogin's scores for innovation were below average; aside from the HydraBoost announcement, product enhancements were mostly catch-up.
- OneLogin scored lower than other Leaders in this Magic Quadrant for vision, with below-average scores for vertical/industry strategy and geographic strategy. Even though OneLogin's features and

capabilities could appeal to the needs of larger clients, it tends to sell to smaller clients.

- OneLogin suffered a significant amount of turnover among its employees last year, including leadership and product teams. Stability of workforce is an area of concern for OneLogin; it experienced a much higher rate of employee churn than the other vendors in this research, and both product and sales leaders have been with the company less than a year.
- For BYOI, OneLogin is less mature than the other Leaders, with fewer social IDs supported out of the box. It is also missing support for decentralized identity approaches.

Oracle

Oracle is a Niche Player in this Magic Quadrant. Its Oracle Access Manager and Identity Cloud Service products are software and SaaS offerings, respectively, and mainly focused on delivering AM capabilities to existing Oracle customers. Its operations are geographically diversified; its clients vary in size and industry, and are mostly using its on-premises products.

Recent product innovations include SaaS-based support for FIDO2, FedRAMP enhancements and deeper integration with Oracle cloud and enterprise applications. Oracle plans to enhance its SaaS product global presence, improve embedded IGA capabilities in the AM cloud product and migrate the software-delivered product into a microservices architecture.

Strengths

- Pricing for Oracle's SaaS AM product IDCS was well below market averages in the series of pricing scenarios evaluated in this research. Oracle also introduced discounts for existing software clients that wish to migrate to the cloud.
- Oracle has an extensive global presence for operations and services, making it easier to acquire AM products in regions where other AM vendors are not present. It also launched a global professional services upgrade factory with more than 50 partners, which can be very helpful for current on-premises clients looking to upgrade legacy installations into the latest software version.
- Oracle is aggressively increasing the number of its data centers, which will be good news for customers of the Oracle cloud looking for localized data residency.
- Oracle scored above average for its identity administration capabilities. It offers complete and flexible directory services capabilities, inbound and outbound SCIM, self-service user administration, delegated administration, user provisioning, application catalog, and access request capabilities embedded in the AM SaaS services at no additional cost. It also offers optional IGA capabilities available via software modules.

Cautions

- Oracle scored the lowest in customer experience among all vendors. Gartner clients have cited limited features in the cloud version and deployment complexity for the software product. Gartner has observed a decline in interest in Oracle's products, reflected in a reduction in the number of mentions in client inquiries.
- Oracle scored the lowest in innovation among all vendors. The vendor introduced mostly catch-up features, like FIDO2 support and integrations with its own Oracle Cloud Applications.
- Oracle received the lowest score in marketing strategy among the vendors in this research. The company appears to target only existing OAM customers and to upsell into the Oracle Cloud Infrastructure.
- Oracle only provides a Service Level Objective (SLO) of 99.95% for its SaaS product, not a full service-level agreement. It's the only vendor in this Magic Quadrant not to offer an SLA.

Ping Identity

Ping Identity is a Leader for this Magic Quadrant. Its AM products are sold in several bundles and modules as both SaaS and software with converged AM, identity proofing and fraud detection capabilities. Its operations are geographically diversified, and its clients tend to be large organizations looking for hybrid on-premises and cloud deployments for internal and external AM use cases.

Recent product innovations include new identity proofing capabilities, a low-code flow designer, and a risk engine and analytics framework. Ping Identity plans to invest 24% of revenue in R&D to create a marketplace for technology integrations, expand identity proofing capabilities, improve fine-grained authorization features in SaaS and launch PingOne Fraud.

Strengths

- Ping Identity has expanded its capabilities through acquisitions: decentralized identity and identity proofing via ShoCard in October 2020 (which became PingOne Verify), Symphonic in November 2020 (PingAuthorize), and SecuredTouch in June 2021 (which will become PingOne Fraud).
- Ping Identity received the highest score for business model, with a clear focus on large enterprises that helps define its goals and future investments in areas that are important to that segment of the market. For example, it offers 99.99% SLA availability to all customers.
- Ping Identity received the highest score in marketing execution. Multiple ads and campaigns throughout the year raise the profile of its products, especially for CIAM. Ping Identity CIAM scenarios priced below market averages.
- Ping Identity product adoption is balanced between clients using it for internal and external AM use cases, with the strongest score among vendors in this research for nonstandard application enablement scenarios.

Cautions

- Ping Identity clients tend to be larger organizations that have already made (or can afford to make) investments in other IAM-adjacent capabilities. However, it does not offer an AM product with enough embedded identity administration capabilities to be useful for smaller organizations, or for organizations looking for an AM solution with embedded IGA or PAM capabilities.
- Ping Identity made several acquisitions between 2020 and 2021, and the success of the mergers will depend on how efficiently the company can incorporate the products into its portfolio, without the unnecessary distractions that could impact execution and innovation.
- Ping Identity's revenue generation slowed in 2020 compared to other Leaders, attributed to a change in accounting from traditional software to SaaS sales. Existing software customers or organizations looking for deploying software on-premises should weigh the potential impact of this change in their forecasting.
- New software bundles were introduced, which resulted in uneven pricing, with different internal AM use-case scenarios priced above market averages.

Thales

Thales is a Niche Player in this Magic Quadrant. Thales offers SafeNet Trusted Access (STA) as SaaS and SafeNet Authentication Service as software, with separate modules for hardware tokens and smart cards. Its operations are geographically diversified, and its clients tend to be small to midsize organizations looking to address internal AM use cases and with a need for strong user authentication.

Recent product innovations include collaboration features between multiple tenants to share corporate applications, contextual Windows logons and hybrid deployment models for its products. Thales plans to spend 20% of revenue in R&D to integrate its products with other IAM platforms and expand its current CIAM capabilities.

Strengths

- Thales' STA provides strong user authentication capabilities and can provide access to additional Thales products for document-centric identity proofing.
- Thales offers 99.99% SLA availability to all customers.
- Thales has expanded a cross-portfolio partnership with Google for providing AM to Google Workspace and, integrating its CipherTrust Cloud Key Manager, enabling client-side encryption for Google Workspace.
- Thales received above-average scores for operations, with a long history in the authentication market (Gemalto, SafeNet) and strong partner channels and global presence.

Cautions

- Thales received below-average scores for customer experience. Based on Gartner clients' comments, customer complaints include mentions of the high learning curve using the administrative interfaces, and some periodic outages. Thales also received below-average scores for ease of deployment.
- Thales' pricing for external AM use cases is well above the market averages.
- Thales does not offer a strong service for CIAM, which depends on a varied number of different products that deliver pieces of the CIAM experience (which Thales plans to streamline in the future). API access control capabilities are also scored below average.
- Thales received the lowest score among vendors in this research for market responsiveness and track record of execution. Aside from new capabilities for delegated administration among tenants, innovations were mostly catch-up features.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Ilantus: Ilantus has made the inclusion criteria into this version of the Magic Quadrant after launching a SaaS-delivered converged IAM platform in 2018, focused on midsize enterprises (and which includes AM, PAM and IGA). Its platform gained traction very quickly, and it acquired several clients in the last 18 months.

Dropped

No vendors were dropped from this Magic Quadrant.

Inclusion and Exclusion Criteria

Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses by default an upper limit of 20 providers to support the identification of the most relevant providers in a market.

To qualify for inclusion, providers need to:

- Have marketed and must have sold products and services in their 2020 12-month fiscal year to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases. For example,

solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

- Own the intellectual property for the AM products and services they sell. Vendors that resell other vendors' products or that have merely augmented other vendors' AM products and services for resale or for managed or hosted service offerings are excluded.
- Have $15 million in annual revenue from AM products and subscriptions (inclusive of maintenance revenue, but excluding professional services revenue) in their 2020, 12-month fiscal year. They must also have 800 or more current AM customers as of 31 May 2021. These must be discrete AM customer organizations (i.e., "net logos," meaning different business units or dependencies of the same company should not be counted as a separate customer) and not customers for other products, and they must have their own contracts with the vendor. Free or freemium nonpaying customers are not included in customer totals.
- Have global capabilities with customers, delivery and support capabilities in all major markets: Americas (North and South America combined), EMEA and APAC (including Japan). Vendors must have customers in each market with no more than 80% of their customer count or revenue in their primary region.

In addition, the vendors' AM products or services must offer the following technical capabilities relevant to Gartner clients:

- Identity administration must provide at minimum a directory or identity repository for internal and external identities, including identity synchronization services and SCIM support.
- User self-service must include end-user and administrative interfaces for user registration, password management, profile management and delegated administration. It also needs to provide a workforce launchpad of applications or application gallery for single sign-on.
- Authorization and adaptive access must include capabilities for implementing, at minimum, coarse-grained authorization decisions and enforcement, policy creation, and sources of stored and contextual data used for rendering access decisions. The product or service must provide native support to modern protocols like OAuth 2.0.
- Session management must include capabilities and granularity to which the AM tool can control session state for user-present interactions with applications, the ability to manage session times by issuing and refreshing time-limited access tokens (or cookies), and the ability to terminate sessions. It must provide, at minimum, a global setting for session management and single logout.
- The products or solutions must provide different user authentication methods, including multifactor authentication (MFA) and SSO. Minimal MFA requirements should include OOB SMS, one-time password (OTP) apps, mobile push and support for OTP hardware tokens.

- The products or solutions must provide BYOI integration to use public identities, such as social media at least, for access control. Core functionality includes using sign-up and sign-in, and linking social media identities to AM customers' established user identities, and to set access policy based on the use of social media identities.

- API access control offers, at minimum, an OAuth 2.0 authorization server, which supports and implements consent, handles scope to claim mappings, and is capable of issuing customizable and self-contained JWT tokens to web servers, mobile apps, modern web apps and services used for accessing API targets.

- The products or solutions must support both standard/modern and nonstandard/legacy application enablement. They also must support modern protocols like SAML and OpenID Connect, including capabilities to enable access and SSO to legacy applications that may not support standards-based SSO protocols, using technologies like proxy services, agents or other mechanisms.

- Analytics capabilities must include, at minimum, descriptive, historical information about all administration and runtime access events. The products or solutions must offer reporting and APIs for exporting event data to be analyzed by external analytics and security information and event management (SIEM) tools, or consumed by the solution's own adaptive risk engine. This allows customers to use canned and customized reporting functions to identify entitlements, audit access and identify access risks.

This Magic Quadrant does not cover the following types of offerings:

- AM products that cannot support or are not marketed to support both internal (B2E), and external (B2B, B2C, G2C or gig economy) use cases. For example, solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case will be excluded.

- AM products that are not marketed and supported globally. Vendors must have global capabilities with customers, delivery and support capabilities in all major markets: Americas (North and South America combined), EMEA and APAC (including Japan). No more than 80% of a vendor's customer count may be in its primary region.

- Pure user authentication products and services, or products that began as pure user authentication products and then were functionally expanded to support SSO via SAML or OpenID Connect, but cannot manage sessions or render authorization decisions (for more information on this market, see Market Guide for User Authentication).

- AM offerings that are only or were predominantly designed to support operating systems and/or privileged access management (for more information on this market, see Magic Quadrant for

Privileged Access Management).

- Remote or on-premises “managed” AM; that is, services designed to take over management of customers’ owned or hosted access management products rather than being provided by delivery of the vendor’s own intellectual property.
- AM functions provided only as part of broader infrastructure or business process outsourcing agreement. AM must be provided as an independently available and priced product or service offering.
- AM products that are only, or predominantly, marketed as open-source offerings.
- Stand-alone identity governance and administration (IGA) suites, which are full-featured IGA products that offer the complete range of IGA functionality, without embedded AM capabilities. This is a separate but related market covered by other Gartner research (see Market Guide for Identity Governance and Administration).
- Full life cycle API management. This is a separate but adjacent market covered by other Gartner research (see Magic Quadrant for Full Life Cycle API Management).
- Endpoint protection platforms (EPP) or unified endpoint management (UEM). EPP and UEM are separate but related markets covered by other Gartner research (see Magic Quadrant for Endpoint Protection Platforms and Magic Quadrant for Unified Endpoint Management).
- Cloud access security brokers. CASB is a separate but related market covered by other Gartner research (see Magic Quadrant for Cloud Access Security Brokers).

Inclusion and exclusion criteria remained mostly unchanged since last year, with the exception of the requirement that vendors must have customers in each market with no more than 80% of their customer count or revenue in one primary region. That dropped from 85% last year. This year’s inclusion and exclusion criteria were also described in more granularity of detail.

Honorable Mentions

Vendors Covering All AM Use Cases

Entrust: Entrust offers three IAM products, together with other certificate and data protection solutions. Identity as a Service (formerly IntelliTrust) is a SaaS-delivered AM platform with identity proofing; Identity Enterprise (formerly IdentityGuard) is the software-delivered version; and Identity Essentials (formerly SMS Passcode) is an MFA solution for Windows desktops. (Entrust was not included due to not meeting the technical inclusion criteria.)

Imprivata: Imprivata offers a number of IAM services, primarily in the healthcare vertical, where it is well-known for its “tap and go” authentication approach for healthcare badges. It offers desktop-

based ESSO, standards-based SSO, MFA and identity governance functionality in its software-delivered products. (Imprivata was not included due to not meeting the technical inclusion criteria.)

SecureAuth: SecureAuth provides the SecureAuth Identity Platform, an AM product that includes support for passwordless authentication and adaptive access. The solution is available through multiple subscription plans, and supports SaaS, software or hybrid deployments. (SecureAuth was not included due to the criteria for number of customers.)

Transmit Security: Transmit Security offers a SaaS-based AM platform for internal and external AM use cases. Its focus is on providing passwordless approaches, and offers identity orchestration and fraud detection capabilities. It received $543 million in Series A funding in June 2021. (Transmit Security was not included due to criteria for number of customers.)

Vendors Covering Only External Identities

Akamai: Akamai provides the Akamai Identity Cloud, an AM offering for external identities based on its acquisition of Janrain. The Akamai Identity Cloud is a SaaS-delivered product. (Akamai was not included due to not meeting the overall inclusion criteria.)

OneWelcome: OneWelcome is the result of the merger of two European CIAM specialists in July 2021 — iWelcome and Onegini. It offers IAM products for customer journey management, consent management, B2B delegation and mobile security, and is focused on selling to European clients, mostly in regulated industries. (OneWelcome was not included due to not meeting the overall inclusion criteria.)

SAP: SAP provides the SaaS-delivered SAP Customer Data Solutions, which offers three enterprise solutions: SAP CIAM for B2C, SAP CIAM for B2B, and SAP Enterprise Consent and Preference Management. (SAP was not included due to not meeting the overall inclusion criteria.)

Platform and Developer-Oriented Vendors

Amazon Web Services: AWS offers AM functionality to AWS customers, including SSO, MFA and directory services. AWS is an IaaS offering. (AWS was not included due to not meeting the technical inclusion criteria.)

Google: The Google Cloud Platform (GCP) provides SSO, MFA, directory services and related AM features for GCP customers. (Google's IaaS AM offering was not included due to not meeting the overall inclusion criteria.)

Alibaba Cloud: Alibaba Cloud provides an AM product called Alibaba Cloud Identity as a Service (IDaaS). It is offered as SaaS and software-delivered models, offering identity administration for all types of user constituencies, directory services, centralized authentication, single sign-on, authorization and audit reporting. (Alibaba Cloud was not included due to not meeting the overall inclusion criteria.)

Evaluation Criteria

The evaluation criteria and weights tell you the specific characteristics and their relative importance, which support the Gartner view of the market. They were used to comparatively evaluate providers in this research.

Ability to Execute

Gartner analysts evaluate vendors on quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively affect revenue, retention and reputation in Gartner's view of the market.

Product or Service: Core goods and services that compete in and or serve the defined market. This includes current product and service capabilities, quality, feature sets, skills etc. This can be offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

We specifically looked at the breadth and depth of AM features, richness of support for a wide range of applications, different types of identities, and controls demonstrated to help ensure the continuity, security and privacy of customers and their data.

The applicability and suitability of these offerings to a wide range of use cases and different application architectures, across different communities of users and different enterprise and cloud-based systems were evaluated by these specific subcriteria:

- General product architecture
- Identity administration
- User self-service
- Authorization and adaptive access
- Session management
- User authentication
- BYOI integration
- API access control
- Standard application enablement
- Nonstandard application enablement
- Analytics

- Ease of deployment
- Security, resiliency and geographical coverage

Overall Viability: Viability includes an assessment of the organization's overall financial health, as well as the financial and practical success of the business unit. It views the likelihood of the organization to continue to offer and invest in the product as well as the product position in the current portfolio.

Subcriteria:

- Financial health
- Success in AM market by AM revenues and customer population

Sales Execution/Pricing: The organization's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support and the overall effectiveness of the sales channel.

Subcriteria:

- Sales execution
- Revenue breakdown by channel
- Pricing under several scenarios — This subcriterion weighted heavily. Vendors were asked to identify actual expected deal pricing with appropriate discounts for the different scenarios. Lower costs for the same functionality among vendors scored higher.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve, and market dynamics change. This criterion also considers the provider's history of responsiveness to changing market demands.

Subcriteria:

- General responsiveness to market trends and competitor activities (last 12 months)
- Meeting customer needs in different use cases

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be

driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities.

Subcriteria:

- Marketing activities and messaging executed in the last 12 months
- Marketing execution: ROI, cost per win, conversion rate, marketing metrics

Customer Experience: Products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer interactions, technical support or account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, and so on.

Subcriteria:

- Customer relationship and services
- Support services, SLA
- Professional services offerings
- Gartner client feedback — This subcriterion is weighted very highly

Operations: The ability of the organization to meet goals and commitments. Factors include quality of the organizational structure, skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently.

Subcriteria:

- People
- Processes
- Organizational changes

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High

Evaluation Criteria ↓	*Weighting* ↓
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium
As of October 2021	

Source: Gartner (November 2021)

Completeness of Vision

Gartner analysts evaluate vendors on their understanding of buyer wants and needs, and how well the vendors anticipate, understand, and respond with innovation in their product offerings to meet those needs. Vendors with a high degree of completeness of vision demonstrate a capacity to understand challenges that buyers in the market are facing, and for shaping their product offerings to help buyers meet those challenges.

Market Understanding: Ability to understand customer needs and translate them into products and services. Vendors that show a clear vision of their market are those that listen, understand customer demands, and can shape or enhance market changes with their added vision.

Subcriteria:

- Market research program and methodology
- Understanding the competition, and own strengths and weaknesses

- Understanding customer needs
- Understanding the future of the AM market, biggest threats and their own place in this market

Marketing Strategy: Clear, differentiated messaging consistently communicated internally, and externalized through social media, advertising, customer programs and positioning statements.

Customers cannot buy products that they don't know about. We evaluated specific product marketing metrics, not corporate marketing. We looked at how much awareness about specific access management messages is shared with the vendor's target audience, and how much of the customer voice influences its AM product/service offerings.

Subcriteria:

- Brand awareness
- Product marketing strategy plan
- Customer sentiment

Sales Strategy: A sound strategy for selling uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. Partners that extend the scope and depth of market reach, expertise, technologies, services and their customer base.

Subcriteria:

- Sales organization and partnerships
- Revenue breakdown by channel
- Program for internal sales enablement

Offering (Product) Strategy: An approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features as they map to current and future requirements.

We consider how the vendor will increase the competitive differentiation of its AM products and services through product engineering, product management and overall product strategy.

Subcriteria:

- Product strategy
- Product roadmap, future plans

- Product gaps closed (catch-up features delivered)
- Product development life cycle

Business Model: The design, logic and execution of the organization's business proposition to achieve continued success.

Subcriteria:

- Core purpose and aspirations of the vendor in the AM market
- Partnerships
- Path for growth

Vertical/Industry Strategy: The strategy to direct resources (sales, product, development), skills and products to meet the specific needs of individual market segments, including verticals.

Subcriteria:

- Customer breakdown by industry
- Trends in customer industry breakdown
- Strategy for verticals and other segmentation

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes.

We consider the vendor's continuing track record in market-leading innovation and differentiation. This includes the provision of distinctive products, functions, capabilities, pricing models, acquisitions, divestitures and so on. We focus on technical and nontechnical innovations introduced since the last year, as well as the vendor's future innovations over the next 18 months.

Subcriteria:

- Recent (technical and nontechnical) innovations rack record, that differentiate your product/service (in the past year)
- Planned (nontechnical) innovations that will differentiate your product/service (next 18 months)

Geographic Strategy: The provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through

partners, channels and subsidiaries, as appropriate for that geography and market.

Subcriteria:

- Customer breakdown by geography, with representation in all major markets
- Trends or changes in customer geographic breakdown
- Strategy for changes in geographic coverage
- Global support capabilities

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium
As of October 2021	

Source: Gartner (November 2021)

Quadrant Descriptions

Leaders

Leaders in the AM market generally have significant customer bases and a global presence for sales and support. They provide feature sets that are appropriate for current customer use-case needs and develop capabilities to solve new problems in the market. Leaders also show evidence of strong vision and execution for anticipated requirements related to technology, methodology or means of delivery. All leaders offer AM capability as SaaS, and some offer hybrid IT delivery models. They show evidence of how AM plays a role in a collection of related or adjacent product offerings. Leaders typically demonstrate solid customer satisfaction with overall AM capabilities, the sales process, and/or related service and support.

Challengers

Challengers show strong execution, complete product features, and have significant customer bases. However, they have not shown the Completeness of Vision for AM that Leaders have, and may not have all AM capabilities delivered as SaaS, for example. Rather, their vision and execution for marketing, technology, methodology and/or means of delivery tend to be more focused on or restricted to specific functions, platforms, geographies or services. Challengers may see AM as a key part of a broader product and service portfolio. Challengers' clients are relatively satisfied.

Visionaries

Vendors in the Visionaries quadrant provide products that meet many AM client requirements, but they may not have the market penetration to execute as Leaders do. Visionaries are noted for their innovative approach to AM technology, methodology and/or means of delivery. They often may have unique features and adjacent IAM capabilities, and may be focused on a specific industry or specific set of use cases. In addition, they have a strong vision for the future of the market and their place in it.

Niche Players

Niche Players provide AM technology that is a good match for specific use cases. They focus on specific industry verticals, geographies or market segments by customer size. Niche Players could also include vendors that sell AM as an add-on capability to other products used by their existing customer base; they can outperform many competitors in their specific area of focus. Vendors in this quadrant often have relatively fewer customers than competitors in other quadrants, but they may have large customers, as well as a strong specialization in some areas of AM (like user authentication, for example). Brand awareness of their AM product is usually low relative to vendors in other quadrants. Vision and strategy may not extend much beyond feature improvements in current offerings. Pricing might be considered too high for the value provided by some niche vendors.

However, inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused spectrum. Niche solutions can be very effective in their areas of focus.

Context

Return of the Convergence

IAM convergence activity increased aggressively for three years in a row. According to Top Security and Risk Management Trends 2021, by 2025, three-quarters of large organizations will be actively pursuing a vendor consolidation strategy, up from approximately one-quarter today. [1]

The trend is stronger, however, and different from the first generation of IAM suites of the early 2000s. It is now based on SaaS-delivered, embedded (and more services-oriented) composable IAM capabilities, not bolt-on integrations of on-premises products.

Among all IAM markets, AM has been leading more movements in convergence in three ways:

- **Vendor consolidation and innovation through merger and acquisition (M&A).** Okta acquired Auth0; One Identity acquired OneLogin (we evaluated OneLogin before the acquisition had been completed); iWelcome merged with Onegini; Microsoft acquired CloudKnox Security; Ping Identity acquired Singular Key (we evaluated Ping Identity before the acquisition had been completed); Imprivata acquired Xton Technologies.
- **Use-case capability consolidation.** This has been observed with leading multiconstituency AM vendors now offering the best capabilities for delivering external, internal AM and developer oriented use cases.
- **Functionality convergence.** This is ramping up, with all AM vendors in this Magic Quadrant already delivering MFA and several are investing to add IGA and PAM capabilities.

Recommendations:

- Organizations should prioritize single-vendor strategies for internal, external and developer AM use cases. Use multiple AM vendors only in exceptional cases, where extreme specialization is needed.
- Carefully evaluate the roadmap of converged IGA and PAM capabilities into AM cloud platforms in the next months.

The Rise of B2B CIAM and Application Development Use Cases

Most organizations have already deployed an AM initiative for their workforce. With the increased popularity of CIAM initiatives (72% of organizations want CIAM implemented by 2022 [3]), and given previous investments in workforce AM, organizations are more interested in AM tools capable of supporting both internal and external AM use cases. Because of the new reality of remote access

combined with the need for stronger digital collaboration between partner organizations, B2B scenarios are seeing accelerated demand, especially for more flexible life cycle management and BYOI approaches for business customers.

This year, Gartner observed an increase in inquiries about B2B, which surpassed B2C CIAM by 25%. To meet this need, flexible delegated administration features are increasingly available not just in IGA offerings, but also in AM platforms that cater to B2B and B2C users. The demand for B2B CIAM is growing; however, the majority of AM vendors in this research have not yet reached maturity in capabilities for the B2B use case.

In addition to B2B, and more complex CIAM use cases, there is also an increased need to support development use cases in AM tools. By 2019, 83% of HTTP traffic was already API requests, and only 17% used traditional web applications. [4] That means that the core use case for access management is no longer traditional browser-based access and its associated cookie-based session management. Gartner has seen the number of inquiries regarding API access control increase 300% in 2020.

In fact, any organization looking to embed authentication and authorization capabilities into custom-built apps and services require a different set of features not traditionally used in workforce AM. Examples include readily available SDKs, developer self-service interfaces, strong API access controls, orchestration (see next section) and a long list of integration with third-party developer tools. Developer tools are becoming a fundamental capability in AM, and we are starting to see two types of AM vendors catering to developers:

- **Developer-focused "traditional" AM vendors.** They typically participate in the creation of the many IAM standards, and delegate to organizations the responsibility to choose, implement and manage any tools to use those standards.
- **Developer-enabled "cool" AM vendors.** These vendors are focusing on organizations that don't want (or can't) learn about all the existing IAM specifications, and just want an SDK that solves business needs (like account creation, authentication and forgotten password) in the fastest way they can.

As the market for developer-oriented AM vendors evolves, education and documentation, commercial off-the-shelf (COTS) libraries, and SDKs provided by developer-enabled AM vendors are more important factors than just compliance with IAM standards (as a check-box requirement), like developer-focused "traditional" vendors.

Recommendations:

- Organizations should understand the growing overlap of B2B and B2C offerings, and carefully evaluate B2B-specific functionalities like delegated administration, mature identity federation, flexible identity management and JIT provisioning features for B2B users in an AM tool offering.

- Developers should be involved in the process of designing user experiences early in the AM vendor selection process. (see Top Trends in Customer IAM Solution Design). Organizations must consider the developer perspective, especially when selecting a CIAM tool.

Identity Orchestration: A New Hope to IAM Sprawl?

Identity orchestration is an optional capability offered by AM vendors, together with required API access control and other developer tools. It allows the definition of runtime user access experiences through integration with disparate external IAM pieces (for authentication, identity proofing and fraud detection, for example), and configuration of access flows, typically in a visual designer type of interface. It offers low-code and no-code approaches for tasks that otherwise would require professional coding abilities, and may include the ability to also monitor and manage these fragmented IAM pieces. Identity orchestration is becoming more popular after AM vendors have started to offer this type of functionality.

Identity orchestration can be used to:

- Help reduce the cost and complexity of integration of legacy IAM tools, as well give a “second chance in life” for legacy technologies that are narrowly focused on a particular legacy use case, and avoid ripping and replacing them. It can help contain IAM sprawl, reducing the need for buying new IAM tools by reusing and connecting the existing pieces together, and making them interoperable.

- Add extensibility capabilities of otherwise rigid IAM deployments, like homegrown CIAM solutions. Identity orchestration helps replace custom code with a more flexible integration platform for connecting customer authentication, identity proofing, authorization and fraud detection, for example. It can facilitate A/B testing of different user journeys or different combinations of capabilities to optimize pass rate, drop out rate, costs, latency and so on.

- Help developers to deploy apps, embedding IAM security faster than before. Identity orchestration can also empower citizen developers to build sophisticated IAM experiences that were not possible due to lack of skills.

Recommendations:

- IAM leaders should begin to evaluate low-code/no-code identity orchestration tools to solve issues related to cost and complexity of integrating and maintaining disparate IAM products and services, especially legacy IAM technologies.

Identity-First Security: The Last Perimeter?

Gartner’s Top Security and Risk Management Trends 2021 noted:

"'Identity as the new perimeter' (identity-first security) has reached critical mass due to technical and cultural shifts, coupled with a now-majority remote workforce as a result of COVID-19. Identity as the new perimeter demands a major shift in security priorities from traditional LAN edge design thinking. Identity-first security puts identity at the center of security design."

If identity-first security is now the center of security design, then AM tools are the focal point of an identity-first security strategy. In the identity fabric of modern enterprises, administrative tools like IGA and PAM define and enforce the principle of least privilege across all use cases. AM tools provide the runtime controls for users working and creating value for a business. That dynamic now applies no matter where, when or how that user is working.

AM tools include SSO into SaaS and internal web applications for remote users, strong authentication through MFA and session management controls, all of which helped to bring the possibilities of the "identity as a control surface" vision to life. In a zero trust architecture approach, balancing access management approaches with other security technologies, the emergence of zero trust network access (ZTNA) plugs the gap for legacy, nonweb applications, allowing the vision to be mostly completed. (See Quick Answer: How Do Access Management and Zero Trust Network Access Tools Work Together?)

The result of these technical and culture shifts is that "identity-first security" now represents the way all information workers function, regardless of whether they are remote or office-based. Instead of location-based controls, authorization and authentication decisions are identity- and context-based, which continues to propagate to other security elements like CASB, endpoint and network security. (See Top Strategic Technology Trends for 2022: Cybersecurity Mesh)

Recommendations:

- Inventory remote access use cases and create reference architectures for planning and validating secure approaches for each remote access use case.
- Develop a gap analysis between the organization's existing remote access capabilities (such as AM, VPN and ZTNA) and consider additional security tools like proxies and CASBs for additional visibility and control.
- Examine current security processes, procedures and logging practices and adjust as needed for more visibility and control, all by way of a risk-adjusted approach.
- Evaluate the technical skills of the organization's IT department, since many of these technologies require specialized skills, many of which a managed services provider could provide.

Resilience Strikes Back

SaaS-delivered AM tools have become very popular, and are by far the preferred way the majority of customers want to consume their AM services. However, as more and more applications are integrated, the AM tool becomes the doorway to all applications, and conversely, the blast radius of any kind of outage becomes impactful from a business perspective.

Availability

Utility level “always on” is now an expectation for any SaaS-delivered IAM service, especially for services as critical as access management. Unfortunately, many vendors have experienced outages, leaving their customers dark when it comes to application availability. And given the proliferation of SaaS services in most organizations, if the internet is down, and access to SaaS services is interrupted, very little activity is possible, outside of some desperate thumb twiddling. So, how do you mitigate the impact of an AM tool becoming unavailable, and how do you build resilience in the organization for when it does so?

While no one can predict the future, we have captured what vendors are offering in terms of SLAs, and promises of uptime, coupled with financial remediations for when an outage may occur. While none of these guarantee that outages will not occur, the vendor has a stake in the game to ensure that the service remains available.

Clients can explore some technical mitigations for the unavailability of an identity provider (IdP) or access management tool; however, these scenarios typically involve the cost of an alternate or failover AM tool, and potentially involve additional development work. While these are suggestions of possible mitigations, none of them are perfect approaches; and for organizations with a large number of applications to migrate, many of them will not be viable:

- Integrate an application into two different IdPs if possible (although very few applications support this).
- Some managed service providers can build an abstraction layer for the IdP that would allow a quick migration from one IdP to another. Note that while this could address application integrations, two fully licensed AM tools would be required.
- Consider longer session life cycles so that fewer authentications are required for fewer clients.
- Investigate the possibility of a hybrid approach, with a software-delivered IdP and a SaaS-delivered IdP with the ability to share sessions between them and easily failover if possible.
- Consider using a software-delivered, non-SaaS IdP exclusively. Note that this will require ongoing support of on-premises infrastructure.
- Install and maintain multiple SaaS IdPs, and perform business continuity activities, switching a critical application from one IdP to the next, and test functionality, then switch back. Note that this

requires two fully licensed AM products, and is not viable for an organization with hundreds of application integrations.

- Consider using application-initiated SSO. This ensures that users aren't hitting an IdP-based portal that may not be available, and as soon as each application is integrated into the new IdP, functionality is restored.
- Explore vendors providing an "edge" capability, which would cache IdP functionality internal to your organization in the event of a SaaS outage.

Consider the value of mitigating an AM outage: The investment you are making will typically be to address the last 9 for 99.99% availability. As noted in the Vendor Strengths and Cautions section, Microsoft experienced 16 hours of outages for its Azure AD service last year. The question is, does the cost of the technical mitigation, which may involve a significant investment for a duplicate AM product, along with the efforts of migration of applications, justify eliminating a 16-hour outage?

For some companies, the effort of mitigating this risk may not make sense. Perhaps their business can largely survive an outage of a few hours. But for some companies, such as an investment firm for whom millions of dollars could be lost over a matter of an hour, or even minutes, or a company that sells event tickets and that experiences an outage the moment the tickets for a hot concert go on sale, an additional investment in resilience may be appropriate. At minimum, it is worthwhile to investigate which AM vendor provides the best availability with their product.

None of this is intended to excuse AM vendors for inadvertent outages; as mentioned above, "always on" is a reasonable expectation for AM tools today.

Scalability

While dynamic scaling may not be completely irrelevant to workforce AM, it is usually not a concern. However, for CIAM use cases, consider the ability of your CIAM provider to manage scaling, potentially by massive amounts of traffic. Given the majority of modern AM tools used for CIAM use cases are SaaS, scaling is typically manageable. However, scaling in a scenario where your site's traffic doubles over two or three weeks is a different challenge compared to your site's traffic growing a hundredfold over a period of a few days.

Security Breaches

AM tools are a core part of many security programs and practices, and with identity representing the modern security control plane, AM tools will continue to represent critical tools for securing access to applications and data. As the fallout from the 2020 SolarWinds breach taught us, hackers will continue to attack in new and innovative ways, looking for the opportunities where security people aren't aware or aren't watching. Resilience for AM must be a part of a larger strategy for resilience, building toward a cyber-resilient organization (see Maverick* Research: You Will Be Hacked, So Embrace the Breach). Take a multifaceted approach, first focusing on minimally viable security

approaches, and then looking beyond software and tools to build resilience in your organization that ensures that the business is never interrupted by a cybersecurity event.

Recommendations:

- Choose an AM tool that has a good track record of reliability. Ensure that the AM tool you choose offers an SLA involving financial remediation for outages that exceed SLA. Pursue those financial remediations if outages occur, ensuring that vendors share your incentive for an always-on service.

- Ensure that the AM vendor you have chosen for CIAM can dynamically scale, both for traffic spikes that you anticipate, and for scenarios that you do not. If you wait until the situation exists where you need to dynamically scale, it is too late.

- Use Gartner research like Secure Application Access by Applying the Imperatives of CARTA to Access Management to ensure the basics of visibility and control are embedded in AM transactions. Consider how the concepts of a cyber-resilient organization might be applied to increase resilience in your larger IAM and AM practices (see Maverick* Research: You Will Be Hacked, So Embrace the Breach).

Market Overview

This Magic Quadrant was produced in response to market conditions for AM, including the following trends:

- **Continued convergence of IAM:** Includes the convergence of features (user authentication, AM, PAM, IGA), convergence of capabilities for use cases (internal and external identities, developers), and convergence of vendors (through M&A activity). More than half of Gartner clients believe it is more important to have a converged IAM solution that can mitigate more risks, over solutions that only cover their requirements partially. [2]

- **SaaS resilience and identity-first security:** Digital identity has achieved "utilitylike" status in everyone's lives, with "utilitylike" availability requirements. AM's job is no longer only to enable access to a handful of apps at work. In 2021, it is now the source of context for identity-first security strategies. It integrates with other security pieces of infrastructure and enables security access to customers, partners and also machine identities. AM unavailability has a much bigger blast radius of impact, which made it receive increased attention in this Magic Quadrant.

- **B2B CIAM:** Interest in B2B CIAM has surpassed B2C in Gartner inquiries by 25%.

- **Developer use cases:** CIAM, legacy AM project migrations and API-centric application development are driving demand for easier ways of implementing modern experiences for user access, including an increased need for AM developer tools and identity orchestration. Mentions to API access control in Gartner inquiries in 2020 increased 300% from 2019.

The worldwide AM market revenue was $2.98 billion at the end of 2020. It represented a 6% share of the overall security software market in 2020. This share grew 24.4% when compared to 2019 (see Market Share: Security Software, Worldwide, 2020). Gartner estimates that the AM market revenue for the vendors covered in this Magic Quadrant was $2.5 billion at the end of 2020. Readers, particularly investment clients, are cautioned not to interpret this revenue estimate as accounting for all AM products and services available in the market. Numerous vendors that could not be included in this Magic Quadrant can meet at least partial requirements — for example, by providing user authentication and SSO, when authorization enforcement is not needed by the customer.

Evidence

Primary Research: Gartner's 2020 Security and IAM Solution Adoption Trend Survey

Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?

Vendor surveys

Peer Insights

Secondary resource services

Gartner inquiries

[1] Top Security and Risk Management Trends 2021

[2] **Gartner's 2020 Security and IAM Solution Adoption Trend Survey:** This study was conducted to learn what security solutions are organizations benefiting from and what factors affect their choice/preference for such solutions. The research was conducted online during March through April 2020, among 405 respondents from North America, Western Europe and APAC regions. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at the manager level or above (excluding C-suite), and they should have a primary involvement and responsibility in risk management role for their organizations. The study was developed collaboratively by Gartner analysts and the Primary Research Team, which follows SRM.

Gartner asked survey respondents: "If you were to choose a new IAM product, what would be more important to you?" Of the 405 respondents, 52% answered "Completeness: Full feature set, the IAM product(s) must be able to fulfill all our requirements" as the No. 1 ranked option.

[3] IAM Survey 2019: Advancing Business Outcomes

[4] State of the Internet/Security: Retail Attacks and API Traffic, Akamai.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.