Magic Quadrant for Access Management

16 November 2023 - ID G00781727 - 66 min read

By Henrique Teixeira, Abhyuday Data, **and 2 more**

Workforce access management is getting commoditized, while CIAM is innovating faster, presenting increased opportunities for B2B use cases. AM continues to be an attractive target for attackers, so ITDR will grow in importance in 2024, along with support for passkeys and identity verification.

Strategic Planning Assumption

By 2027, integration with identity verification for onboarding, credentialing & recovery will be a standard feature of access management tools, potentially reducing account takeover attacks against these processes by 75%.

Market Definition/Description

Gartner defines access management (AM) as platforms that include an identity provider (IdP) and establish, manage and enforce runtime access controls to at least cloud, modern standards-based web and classic web applications.

AM's purpose is to enable single sign-on (SSO) access for people (workforce, consumer and other users) and machines into protected applications in a streamlined and consistent way that enhances user experience. AM is also responsible for providing security controls to protect the user session in runtime, enforcing authentication (with multifactor authentication [MFA]) and authorization using adaptive access. Lastly, AM can provide identity context for other cybersecurity tools to enable identity-first security.

Must-Have Capabilities

The must-have core capabilities for this market include:

- A directory or identity repository for workforce or external users, including identity synchronization services.
- Identity administration for integrated applications, with basic life cycle management and profile management capabilities, with support for the System for Cross-Domain Identity Management

(SCIM).

- SSO and session management with support for standard identity protocols (OpenID Connect, SAML) and APIs for accessing standards-based and legacy apps (via proxies or agents).
- User authentication (including commodity MFA).
- Authorization enforcement (including support for modern authorization protocols, including OAuth 2.0).

Standard Capabilities

The standard capabilities for this market include:

- AM functions for machines (workload and devices) and API access control.
- Noncore user authentication methods, including support for phishing-resistant MFA methods (e.g., X.509, FIDO), controls to mitigate usage of compromised passwords and protections against common MFA token attacks.
- Noncore authorization, including risk-based, dynamic adaptive access decisions.
- Portable identity integration for federation and access control (aka bring your own identity [BYOI]).
- Delegated administration and partner management (business-to-business [B2B] customer IAM [CIAM]).

Optional Capabilities

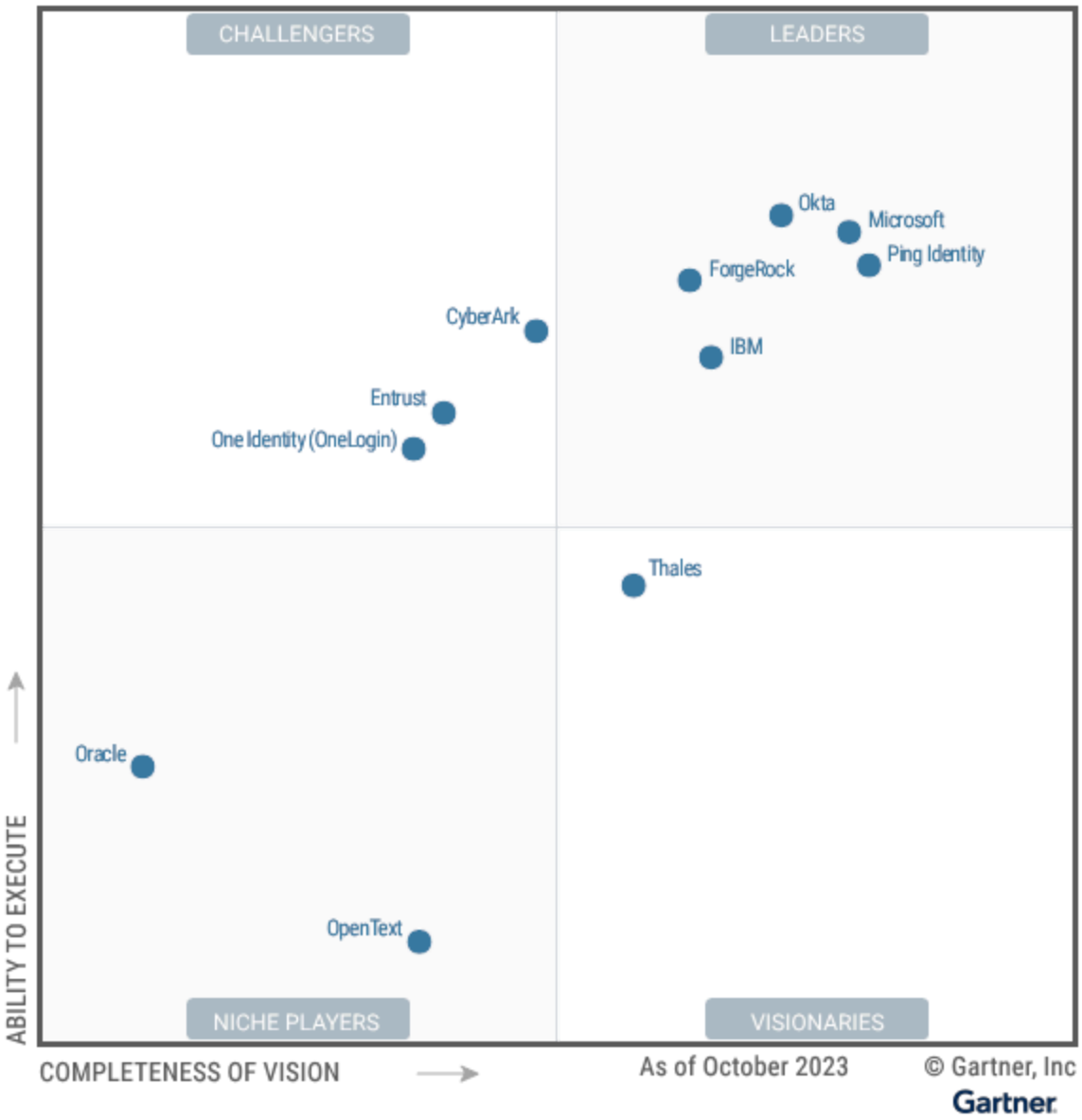
The optional capabilities for this market include:

- AM functions for business-to-business-to-anything (B2B2X) or government-to-constituent (G2C) use cases, advanced identity administration and life cycle management.
- Continuous adaptive trust functions, passwordless authentication methods, support for biometric authentication mechanisms, decentralized identities and verifiable claims.
- Fraud detection, account takeover (ATO) prevention and identity threat detection and response (ITDR).
- Progressive profiling and consent management, personally identifiable information (PII) data management and anonymization, customer analytics.
- Journey-time orchestration, and other low-/no-code interfaces for customization and extensibility in the context of access management.

See the Notes section at the end of this document for a detailed explanation of the acronyms and other important information while reading this Magic Quadrant.

Magic Quadrant

Figure 1: Magic Quadrant for Access Management



Vendor Strengths and Cautions

CyberArk

CyberArk is a Challenger in this Magic Quadrant. Its AM products are delivered as SaaS and sold in bundles for workforce (Workforce Standard, Premium and Enterprise), endpoint security with MFA (Adaptive Secure Desktop and Secure Desktop), and for CIAM (B2B Standard and B2C Standard), or in individual modules. CyberArk's operations are geographically diversified, and most CyberArk AM clients are small to midsize organizations using its products for workforce scenarios.

Recently added features include improved JTO capabilities, MFA prompt bombing mitigation, and flows for ITDR incident response. CyberArk's roadmap includes a secure browser for application and infrastructure access, a JTO marketplace and some more IAM converged features.

Strengths

- CyberArk obtained the highest score among evaluated vendors for customer experience. Its customers mention the products' ease of use and simplicity of the user interface as key advantages.
- CyberArk has demonstrated a strong Ability to Execute, and benefits from a sales strategy that leverages its PAM installed base. This strategy has been successful, and the vendor's AM installed base has increased significantly year over year. CyberArk's AM products can be a good choice for clients looking for the benefits of combining AM with its PAM portfolio.
- CyberArk scored above average for resilience. It claims only the CyberArk DevOps team has access to the AM production infrastructure.
- CyberArk scored above average for marketing execution and business model. CyberArk offers good internationalization support for its AM product set, including admin and end-user interfaces, with an extensive list of languages supported for its various AM offerings.

Cautions

- CyberArk's AM products are among the most expensive on the market. For this research, pricing for several scenarios evaluated is well above average for both workforce and complex CIAM scenarios.
- Despite customer count growth, CyberArk has not demonstrated good traction of its AM products with B2B and B2C CIAM clients, developer use cases or larger clients. Its sales strategy is enterprise focused, lacking a more robust developer and technical user message. Its product set lacks stronger API access control capabilities and the vast majority of its customer base use CyberArk only for workforce use cases.
- A big portion of CyberArk's roadmap items are not AM focused, and instead relate to its greater PAM business and other adjacent areas. This lack of focus in AM has impacted CyberArk's Completeness of Vision, resulting in below-average scores for innovation and offering (product) strategy.
- While it may be suitable for more standardized out-of-the-box AM use cases, CyberArk can be complex to customize. It scored below average for customization and extensibility, and support for portable identity integration.

Entrust

Entrust is a Challenger in this Magic Quadrant. Its Entrust Identity as a Service (IDaaS) product is delivered as SaaS and sold in bundles for workforce and CIAM. Entrust operations are geographically diversified. Most Entrust clients are in the banking and government industries, and use its AM product for workforce scenarios.

Recently added features include passkeys compatibility, MFA prompt bombing mitigation, and identity proofing as a service. Entrust's roadmap includes an AI/ML-driven risk engine, a JTO tool and enhanced reporting features.

Strengths

- Entrust achieved the highest score for user authentication among all vendors in this research. Its phishing-resistant X.509 and FIDO methods are enhanced by supporting a diverse array of authenticators applicable to different verticals. Entrust also has the capability to manage external risk engines that enhance detection capabilities and signals gathering, and extend to IDV tools.
- Entrust's pricing for several scenarios evaluated in this research is consistently lower than market averages.
- Entrust offers capabilities across AM, public-key infrastructure (PKI), digital signatures and IDV to satisfy strong customer authentication (SCA). It offers a risk-based authentication and an SDK with examples for the European Payment Services Directive (PSD2).
- Entrust scored above average for market responsiveness and track record. Within a very short time frame, it has added more AM features to catch up with functionality already offered by other AM vendors in the market, demonstrating good Ability to Execute.

Cautions

- Entrust's direction for AM is driven by its user authentication specialty, rather than by a strong connection to drivers of the overall AM market. Entrust obtained the lowest score in this research for marketing strategy, and one of the lowest scores for market understanding. Its business model for AM is also unclear. The market perceives Entrust as an authentication vendor first, and its business strategy for AM doesn't clearly extend beyond this to staffing, funding and marketing for other critical AM capabilities.
- Entrust has a clear vision, but that vision is neither strongly derived from, nor well aligned with, market research or customer sentiment about AM. As a result, Entrust has closed the lowest number of new deals in the last year out of all vendors in this research.
- Entrust does not offer a 99.99% SLA — it stops at 99.9%. Entrust's geographical coverage of its SaaS offering is also limited when compared with other evaluated vendors.
- Entrust obtained below-average scores for B2C and B2B CIAM capabilities, as well as for API access control, customization and extensibility. There is no marketplace for third-party

integrations, and there are no preconfigured portable identity integration options. Customizing and extending the product requires pro-coding abilities.

ForgeRock

ForgeRock is a Leader in this Magic Quadrant. Its ForgeRock Identity Cloud product is delivered as a converged SaaS IAM platform and sold in a combination of core packages and additional modules. ForgeRock also offers its Access Management product as software. ForgeRock's operations are geographically diversified, and most ForgeRock clients are large organizations using its software-delivered product for CIAM scenarios.

Recently added features include additional signals for threat detection, new flows and connectors to its JTO tool, and passkeys compatibility. ForgeRock's roadmap includes additional fraud and threat detection capabilities, improvements to both its JTO tool and marketplace, and more SaaS-converged IAM features.

In August 2023, Thoma Bravo, the firm that owns Ping Identity, announced that it had finalized the acquisition of ForgeRock and combined it with Ping Identity. The announcement was made after the cutoff date for this research.

Strengths

- ForgeRock obtained the highest score in this research for its product capabilities, especially regarding B2B and B2C CIAM features, authorization and adaptive access. ForgeRock offers various no-code/low-code approaches, and it is one of the very few vendors in the market that offer a JTO tool with a visual flow designer (ForgeRock Trees). It differentiates itself in terms of customizability and extensibility, allowing hybrid deployment models (on-premises, cloud, hosted). It also offers a good marketplace for integrations.
- ForgeRock has demonstrated strong marketing execution, showing good results in CIAM sales.
- ForgeRock obtained one of the highest scores for its business model, presenting a comprehensive and ambitious vision and purpose that align well with industry trends.
- ForgeRock obtained above-average scores in user authentication. ForgeRock offers a visual policy builder for SCA in PSD2 and open banking. It is also FAPI-CIBA certified.

Cautions

- While ForgeRock has had success in CIAM sales, it has recently experienced customer churn due to reduced investments in its OEM customer base. ForgeRock also lags in SaaS adoption, reporting the lowest number of SaaS customers of all the Leaders in this Magic Quadrant.
- Prospective and existing customers are advised to inquire about ForgeRock's future product plans after the announcement of its merger with Ping Identity.

- ForgeRock pricing is above average for all the scenarios evaluated in this research, except for very large CIAM use cases.

- ForgeRock is not an easy solution to deploy, and it scored below average for its product's AM threat reporting capabilities. Obtaining analytics insights about runtime data is complex. Generating reports is not intuitive, and requires exporting JSON files. The existing threat dashboards are quite rigid and are not customizable.

IBM

IBM is a Leader in this Magic Quadrant. Its IBM Security Verify products are delivered as SaaS and sold in a bundle or individual modules. IBM also offers IBM Security Verify Access as software. IBM's operations are geographically diversified, and most IBM clients are large organizations using its software-delivered product for both workforce and CIAM scenarios.

Recently added features include passkeys compatibility, embedded ITDR capabilities for preventing use of compromised passwords and blocking suspicious traffic, and increased SLA to 99.99% availability. IBM's roadmap includes a JTO tool with a visual flow designer, access delegation to trusted parties and a decentralized identity product.

Strengths

- IBM demonstrates a strong and improved Completeness of Vision with one of the highest scores for product strategy (roadmap) that includes many near-term AM-specific functionalities, like DCI and a JTO tool. Its current offering's consent management capabilities for CIAM use cases are some of the strongest in this research.

- IBM offers good value, with prices that are consistently lower than those of its competitors.

- IBM obtained the highest score for geographic strategy due to it introducing new cloud regions to cover the United States, the U.S. federal government, Canada, Europe, China, Japan and Australia. It has also increased its AM SaaS SLA to 99.99%.

- IBM Security Verify obtained above-average scores for product capabilities like customization and extensibility, and user authentication. It offers a comprehensive collection of APIs, SDKs and documentation, support for gateways and agents as container form factors, and native integration with OpenShift apps, Red Hat Single Sign-On and Keycloak. IBM has obtained FAPI-CIBA certification (for its software product).

Cautions

- Due to IBM's focus on large enterprises, it is not a popular choice among small and midsize businesses, and demonstrates lower traction in this market segment than other Leaders.

- Despite its above-average extensibility and customization capabilities, IBM has a limited portfolio of integrations in its marketplace when compared with other vendors' marketplaces. Additional

integration effort and costs must be considered for nonstandards-based types of integrations.

- IBM obtained one of the lowest scores for marketing execution. This is reflected in lower brand awareness of its AM product when compared with other Leaders. IBM's overall vision, strategy and business plan for its AM capabilities are very much "part of the suite" of the bigger IBM Security portfolio.

- IBM offers less-mature capabilities for B2B CIAM than many of its competitors. Almost all delegated admin flows evaluated in this research require customization via APIs.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its Microsoft Entra ID (formerly Azure AD) and Azure AD External Identities are, respectively, workforce and CIAM products delivered as SaaS. The products are sold in a converged IAM platform in bundles and individual modules. Microsoft operations are geographically diversified and primarily used for workforce use cases.

Recently added features include a decentralized identity (DCI) product called Microsoft Entra Verified ID, a machine identity management product (Microsoft Entra Workload ID), and a security posture management (SPM) capability called Microsoft Entra recommendations (formerly Azure AD recommendations). Microsoft's roadmap includes a GenAI interface for SPM and recommendations, multicloud support for workload identities, and embedded DCI into the CIAM product.

Microsoft announced the rebranding of Azure AD to Microsoft Entra ID in July 2023.

Strengths

- Microsoft obtained the highest scores in this research for overall viability, marketing execution, business model and sales execution/pricing. It has grown its installed base to an impressive 700,000 paid clients.

- Microsoft's overall pricing is below the market average. In particular, Microsoft's CIAM use case pricing is well below the average among vendors in this Magic Quadrant.

- Microsoft obtained the highest score of evaluated vendors for market understanding. This is partly due to its early movements in machine identity and DCI support, but also because of enhancements it is making to more established AM capabilities.

- Microsoft obtained the highest score in threat reporting and ITDR. It offers Microsoft Entra recommendations and an SPM measurement capability with security scores. Microsoft Entra is a core piece of the vendor's overall cybersecurity strategy, which is tightly integrated with Microsoft 365 and Azure as a whole.

Cautions

- Azure AD External Identities (for B2C and B2B) still lacks maturity compared with other Leaders' solutions. Most complex CIAM flows require extensive customization and professional services

help.

- Large rebrand exercises like Microsoft Entra tend to create confusion about what features and functionalities exist in which products. That confusion is apparent from Gartner client inquiries, especially with Azure AD External Identities, which will have its B2C features replaced by a new CIAM platform called Microsoft Entra External ID.

- Specific AM features of Microsoft Entra ID — such as Entra ID Protection — require additional licensing. Given the prevalence of attacks on identity infrastructure, many organizations will have to account for additional costs.

- Microsoft obtained the lowest score among all Leaders for customization and extensibility. Despite having a decent catalog of centralized portable identity integrations, Microsoft Entra ID requires significant customization to deliver common user flows and onboarding alternative MFA methods. It is complex to integrate with non-Microsoft tools for external adaptive access or fine-grained authorization (FGA).

Okta

Okta is a Leader in this Magic Quadrant. Its AM products are delivered as SaaS and sold in bundles (Workforce Identity Cloud [WIC], Customer Identity Cloud [CIC, formerly Auth0]) and individual modules as part of a converged IAM platform. Okta's operations are geographically diversified and most of its clients use its products for either workforce or CIAM use cases.

Recently added features include a phishing-resistant MFA (Okta FastPass), a configurable list of FIDO authenticators and FedRAMP High Authorization to Operate (ATO). Okta's roadmap includes a way for developers to build SaaS apps in CIC that automatically integrate with Okta's WIC platform, SPM capabilities and an FGA tool.

Strengths

- Okta obtained the highest score out of all vendors for its centralized portable identity integrations, and one of the highest scores for user authentication. It offers a comprehensive catalog of external IdP integrations for CIAM. It also provides compromised password detection that can be helpful in protecting against MFA attacks.

- Okta obtained one of the highest scores for threat reporting and ITDR. It offers an SPM feature in the WIC platform called HealthInsight, which audits an organization's security settings and suggests remediations.

- Okta demonstrated the strongest Ability to Execute out of all vendors in this Magic Quadrant. It obtained the highest score in operations, and one of the highest scores for overall viability and product capabilities. Okta has the highest growth in CIAM of all evaluated vendors. Its growth in terms of number of clients overall is also one of the highest.

- Okta received one of the highest scores for its offering (product) strategy. Roadmap items include plans like FGA and SPM, and desktop integration for its MFA tool. Okta also demonstrates thought leadership in regard to multidevice FIDO credentials, which is crucial for providing strong passkeys support in the future.

Cautions

- Okta's pricing continues to be well above average, and Gartner clients mention the high cost of the vendor's solution. Gartner has noticed an increased number of clients engaged in contract negotiation discussions to get an appropriate discount rate with Okta.

- Okta has two very different platforms for workforce and CIAM that are not seamlessly integrated. CIC, for example, does not support System for Cross-Domain Identity Management (SCIM) like WIC does, and WIC does not support the same ITDR features as the CIC platform.

- All adaptive access capabilities offered by Okta require additional licensing. Given the prevalence of attacks on identity infrastructure, many organizations will have to account for additional costs.

- While Okta scores above average for CIAM use cases, it does not provide basic consent management. It also lacks a JTO tool. Okta's current workflow capability, while useful for IGA, is not a JTO tool for CIAM use cases.

One Identity (OneLogin)

One Identity (OneLogin) is a Challenger in this Magic Quadrant. One Identity is an independent brand, operating under the Quest umbrella, and OneLogin is the AM product within One Identity's IAM portfolio. One Identity (OneLogin)'s AM products are delivered as SaaS and are sold in bundles and individual modules. One Identity (OneLogin) operations are geographically diversified, and most of its clients use its products for workforce use cases.

Recently added features include MFA using inbound federation support, free bot detection and MFA prompt bombing mitigation. One Identity (OneLogin)'s roadmap includes a native version of passkeys integrated within OneLogin's mobile application, self-service mobile device trust, and ingesting third-party signals for supporting ITDR functions.

Strengths

- One Identity (OneLogin) obtained the highest score in sales strategy out of all vendors. It approaches the market with a differentiating managed services provider (MSP) strategy. This allows MSPs to package One Identity's AM, PAM and IGA offerings and recommend them for inbound SMB deals. Over 100 MSPs have created services around One Identity (OneLogin)'s AM products.

- One Identity (OneLogin) received above-average scores for ease of deployment. It offers advanced configuration approaches like migration hooks that can eliminate the need for users to re-enroll or change their passwords when migrating from legacy AM tools.

- The OneLogin product has a history of being a good option for cost benefit and the vendor continues to offer competitive pricing for small to midsize workforces and more standardized CIAM use cases.

- One Identity (OneLogin) offers good internationalization support for its AM product, including admin and end-user interfaces, with an extensive list of languages supported for its various AM offerings.

Cautions

- One Identity (OneLogin) has not gained significant traction in CIAM use cases. Its pricing for complex CIAM use cases is above market averages.

- Despite having a strong sales strategy leveraging MSPs, One Identity (OneLogin)'s overall number of AM customers and revenue has remained almost flat year over year, and SaaS subscription of its OneLogin AM revenue actually shrank. Its sales strategy lacks a developer and technical user message and its product lacks strong API access control capabilities.

- One Identity (OneLogin) scored lower for overall Completeness of Vision than last year, receiving below-average scores for innovation and offering (product) strategy. It has added some items to its short-term roadmap to catch up on the current-state market, but AM differentiation from leading vendors is missing from its roadmap. Its long-term product roadmap is focused on catching up with those vendors that offer non-AM core functions like IGA, while dedicating lower spending on R&D than the industry average.

- The standard SLA that the vendor offers is only 99.9%, and anything beyond that requires additional costs. In the last 12 months, One Identity (OneLogin) suffered seven total outages and five incidents of degraded performance, with more than 35 hours of downtime.

OpenText

OpenText is a Niche Player in this Magic Quadrant. OpenText makes the inclusion in this Magic Quadrant for the first time after the acquisition of Micro Focus in January 2023. Its NetIQ Access Management product is delivered as SaaS or as software, and is sold in bundles or individual modules. OpenText operations are geographically diversified, and clients tend to be large organizations using its software product broadly across workforce and CIAM use cases.

Recently added features include an authentication API, passwordless authentication and Bluetooth proximity validation to use a device as a token. OpenText's roadmap includes general enhancements to its user interface, adaptive risk service and passwordless authentication.

Strengths

- OpenText can be a good fit for larger organizations and for addressing more complex hybrid AM use cases, especially for organizations that need the flexibility of managing on-premises or hosted

deployments. Its AM solution is a good fit for integrating with nonstandard and legacy applications due to its deployment flexibility.

- OpenText NetIQ Access Management offers flexible delivery models, and supports containerized deployment models leveraging Docker, Kubernetes and OpenShift. All AM modules are available for on-premises or hosted deployments.

- OpenText NetIQ Access Management supplies comprehensive protection for compromised passwords (built-in lists, manual lists and third-party lists), including turnkey integration with the Have I Been Pwned database.

- OpenText obtained above-average scores in portable identities. NetIQ Access Management provides out-of-the-box centralized linking of social identities, and canned integrations with government IDs and some bank IDs.

Cautions

- OpenText's SaaS AM product is consistently more expensive than other SaaS products evaluated in this research. Its SaaS product SLA is 99.95%, and anything beyond that requires additional cost.

- OpenText obtained the lowest score for sales strategy, and has demonstrated very slow progress in its transition to SaaS, either via direct sales or via OEM relationships. It has the lowest number of AM SaaS customers out of all vendors in this Magic Quadrant.

- OpenText obtained one of the lowest scores in market understanding out of all vendors evaluated in this report. AM is just a small part of a very large portfolio of OpenText products, and brand awareness of NetIQ Access Management continues to decline, according to the reducing number of Gartner client mentions.

- Aside from its flexible deployment options, NetIQ Access Management is difficult to customize and extend. The integration APIs are limited to authentication, and documentation lacks details. There is no marketplace for third-party integrations, and the tool lacks more advanced low-code support.

Oracle

Oracle is a Niche Player in this Magic Quadrant. Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) is a SaaS product delivered with Oracle's cloud service. Oracle also offers Oracle Access Manager (OAM) as software. Its operations and clients tend to be geographically diversified.

Recent innovations have included a log generation feature for an IAM domain, a Linux pluggable authentication module and a new password validation policy. Oracle plans to continue to focus on unifying its cloud IAM platform and adding other adjacent IAM capabilities in the future, catering to its Oracle Cloud clients. Most Oracle clients use the on-premises OAM product for workforce use cases. OCI IAM is typically used to provide access to Oracle infrastructure and applications.

Oracle did not respond to requests for supplemental information or to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.

Strengths

- Oracle's SaaS AM product is less expensive than the market average for all pricing scenarios evaluated in this research.
- OCI IAM runs on Oracle's cloud data centers, and it offers cross-region disaster recovery to all OCI global regions where there is a second in-country region, or where laws enable data to move to another specific region. This is a differentiator for customers looking to run AM as SaaS in other clouds that are not provided by either Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform.
- Oracle has a very large installed base for its database and apps (over 400,000 customers). Its marketing strategy is largely focused on targeting these existing customers and promoting its IAM tools on the strength of Oracle apps, making it easier for current users of Oracle applications to use its IAM tools.
- 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.

Cautions

- Oracle is the only vendor in this Magic Quadrant that does not offer an SLA. Instead, Oracle provides a service-level objective (SLO) of 99.95% for its AM SaaS product.
- Oracle received the lowest score for a series of categories that impact its Ability to Execute, including product/service capabilities, market responsiveness and track record, and market understanding.
- OCI IAM is complex to deploy and manage. As a result, it received the lowest score for ease of deployment, and for customization and extensibility (which requires pro-coding abilities). OCI IAM offers very limited SDK capabilities and there is no support for low-code or no-code approaches.
- Overall, Oracle's recent strategy has mostly been internally focused on unifying its diverse legacy IAM products onto its SaaS platform, rather than providing innovation and market-leading AM features. As a result, Oracle obtained the lowest scores for innovation in this Magic Quadrant.

Ping Identity

Ping Identity is a Leader in this Magic Quadrant. Its PingOne Cloud Platform is delivered as SaaS and is sold in bundles and individual modules. Ping Identity also offers several AM products (PingFederate, PingAccess, PingDirectory and PingCentral) as software. Ping Identity operations are geographically diversified, and its clients tend to be large organizations using both on-premises and cloud deployments, across workforce and CIAM use cases.

Recently added features include a new decentralized ID service with verifiable claims (PingOne Neo), a risk engine with fraud detection (PingOne Protect) and MFA prompt bombing mitigation. Ping Identity's roadmap includes preconfigured packaged solutions for different use cases, a new digital credential issuing and transformation service for DCI, and new ITDR features.

In August 2023, Thoma Bravo, the firm that owns Ping Identity, announced that it had finalized the acquisition of ForgeRock and combined it with Ping Identity. The announcement was made after the cutoff date for this research.

Strengths

- Ping Identity demonstrated the strongest Completeness of Vision out of all vendors in this Magic Quadrant. It obtained the highest score for offering (product) strategy and innovation. Aside from the roadmap items already mentioned, it plans to launch a marketplace for its JTO tool, and obtain FedRAMP High ATO and StateRAMP certifications.

- Ping Identity obtained the highest score for marketing strategy this year and one of the highest for market understanding. Its marketing strategy is clear, focused and highly market aligned, with plans directly based on customer feedback.

- Ping Identity also obtained the highest score in market responsiveness and track record, having launched several new features to its platform. Aside from the features already mentioned, it has added AM-converged fraud detection, a form-based configuration option for JTO, OAuth token anomaly detection, FGA to APIs, and many more. Its software products have already achieved FAPI-CIBA certification.

- Ping Identity offers mature capabilities for both customer and partner AM use cases. It is one of the very few vendors that offer a JTO tool with a visual flow designer (PingOne DaVinci) and a DCI service.

Cautions

- Even though Ping Identity's pricing for workforce is competitive and below the market average, its pricing for various CIAM use cases is consistently above that of other vendors evaluated in this research.

- The Ping Identity AM portfolio can be complex to understand and deploy. Configuration of adaptive access, for example, is more complex than average.

- Prospective and existing customers are advised to inquire about Ping Identity's portfolio plans after the announcement of its merger with ForgeRock.

- Many B2C and B2B use cases either require customization or use of the JTO tool at additional cost. Additional cost is also required for using Ping Identity's risk engine, API access control and

advanced authorization. Given the prevalence of attacks on identity infrastructure, organizations will have to account for licensing additional modules for many capabilities.

Thales

Thales is a Visionary in this Magic Quadrant. Thales offers a workforce-focused suite of products composed of OneWelcome Workforce Access Management (formerly SafeNet Trusted Access), delivered as SaaS and sold as a bundle with additional modules. Thales also offers the OneWelcome Identity Platform as SaaS, focused on CIAM. Thales acquired OneWelcome in July 2022. Thales operations are geographically diversified with a strong presence in Europe, and most of its clients tend to be large organizations using its product for workforce use cases.

Recently added features include the new CIAM capabilities from OneWelcome, FGA, dynamic progressive profiling, and a data stewardship system for delegation of consent. Thales' roadmap includes out-of-the-box delegation models with prebuilt flows for B2B CIAM, JTO improvements with a visual flow designer, and new analytics and ITDR features.

Strengths

- Thales obtained above-average scores in innovation. It plans to focus on big CIAM challenges, like B2B use cases. FedRAMP and HIPAA certifications are also on its roadmap to address the needs of the federal government and healthcare verticals.
- Thales also obtained above-average scores for market responsiveness. It has added unique capabilities to its CIAM portfolio, like the ability to provide delegation of consent management to selected users based on relationship (for example, power of attorney and parent-child relationship).
- Thales' acquisition of OneWelcome adds synergistic CIAM capabilities to its user authentication specialty, as well as workforce AM-focused capabilities of SafeNet/Gemalto product lines.
- Thales offers some of the most mature B2C capabilities evaluated in this research, including robust self-service registration and profile management, progressive profiling, out-of-the-box configurable customization of registration flows, T&C consent, and attribute-based consent management.

Cautions

- Thales received the lowest score for overall viability out of all vendors in this Magic Quadrant. This was partly due to its reduced focus on smaller clients, which has resulted in total customer counts decreasing year over year, and a renewal rate for its SaaS offering that was among the lowest of vendors evaluated.
- Thales scored below average for ease of deployment, and for customization and extensibility. Its AM portfolio is a result of several acquisitions and it is not yet fully integrated into a single

platform. There is no marketplace, not even a public website, that shows out-of-the-box third-party integrations available for adding external signals in journey-time flows. Nonstandard integrations and product extensibility are professional services intensive, and customization requires pro-coding abilities.

- Thales offers limited geographic coverage for hosting its SaaS offerings compared with other vendors evaluated in this research, and this may be a challenge for prospects in other regions. Its customer base is mostly concentrated in Europe.

- Thales' OneWelcome scored below average in noncore user authentication use cases, notably for not having native protection against compromised passwords.

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

- Entrust
- OpenText
- Thales

Dropped

Micro Focus has been dropped as its acquisition by OpenText has now been completed (in January 2023).

Inclusion and Exclusion Criteria

This Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant vendors and their products in a market. By default, Gartner applies an upper limit of 20 vendors in order to provide a concise list of the most relevant vendors in a market.

To qualify for inclusion, vendors needed to:

- Have marketed and sold generally available products and services in their FY22 to support both workforce (B2E) and external (B2B, B2C, G2C or B2B2x) use cases. 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 either:
  - Annual revenue of $60 million from AM products and subscriptions (inclusive of maintenance revenue but excluding professional services revenue) in FY22.
  - At least 1,100 current AM customers as of 5 June 2023. 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). They must not be customers for other products, and they must have their own contracts with the vendor. Nonpaying customers (those using the solutions on a free-of-charge or "freemium" basis) 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 Asia/Pacific (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 vendor's AM product/service core capabilities must address all of the following five functional requirements, **delivered as a SaaS product**:

- **Directory services:** Must provide, at minimum, a directory or identity repository for workforce and consumer users, including identity synchronization services and inbound SCIM support.
- **Identity administration:** Must provide basic life cycle management capabilities with AD sync, SCIM (outbound) provisioning capabilities. It also must include ways to invite and register external users, enable profile management, and support basic consent-based flows for registration.
- **Single sign-on (SSO) and session management:** Must provide a workforce launchpad of applications or application gallery for SSO and support standard identity protocols (OpenID Connect and SAML). Session management must include capabilities and granularity, according to which the AM tool can control session state for user-present interactions with applications. The AM tool should also be able to control 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. Lastly, it must provide capabilities to enable access, authentication and SSO to applications that do not support standard identity protocols, using technologies like proxy services, agents or other mechanisms.
- **User authentication:** Must provide different user authentication methods, including MFA. Minimal MFA requirements should include out-of-band simple message service (SMS), one-time password

(OTP) phone-as-a-token (app), and mobile push.

- **Authorization:** Include capabilities to implement authorization decisions and enforcement, create policy and provide sources of stored and contextual data used to evaluate risk and dynamically render access decisions. Provide native support for standard authorization protocols, including OAuth 2.0.

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 B2B2x) use cases. For example, solutions without substantial customer numbers for each use case, and those that are only or mostly marketed to support one use case, will be excluded.
- Pure user authentication products and services, or products that began as pure user authentication products and were then 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 predominantly designed to support operating systems, IT infrastructure 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 AM products, rather than being provided through delivery of the vendor’s own intellectual property.
- AM functions are provided only as part of a 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 provided as open-source offerings.
- Stand-alone 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 API Management**).
- Endpoint protection platforms (EPPs) 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**).

- Cloud access security brokers (CASBs), which represent a separate but related market covered by other Gartner research.

Inclusion and exclusion criteria remain mostly unchanged since last year, with the following exceptions:

- New requirement for the vendor's AM product/service core capabilities, which must be delivered as a SaaS product.
- Revenue and customer counts increased to $60 million and 1,100, respectively.

Honorable Mentions

Vendors Covering All Assessed AM Use Cases

Fortinet: Fortinet offers its AM product as a software/appliance (FortiAuthenticator), which provides centralized authentication services for the Fortinet Security Fabric, including SSO services, certificate management and guest management with temporary accounts, along with FortiToken for MFA. Fortinet also has a SaaS product (FortiTrust Identity) that offers user authentication (including MFA and passwordless approaches), SSO and self-service portals. Fortinet was not included in this Magic Quadrant 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 using proximity badges. It offers desktop-based enterprise SSO, standards-based SSO, MFA, PAM, privacy and IGA functionality in its software-delivered products. Imprivata was not included in this Magic Quadrant due to not meeting the technical inclusion criteria.

RSA: RSA separated from its RSA Conference business in 2022 to refocus exclusively on IAM. RSA offers products for AM, user authentication and IGA. RSA sells AM as SaaS, as part of its ID Plus platform. RSA was not included in this Magic Quadrant due to not meeting the technical inclusion criteria.

SecureAuth: SecureAuth provides Arculix, which supports passwordless continuous authentication, adaptive access and risk-based authentication. SecureAuth also offers SecureAuth Identity Provider, which includes adaptive access and IdP capabilities. The solutions can be used independently or to complement each other, and are available through multiple subscription plans. Both support SaaS, software or hybrid deployments. SecureAuth was not included in this Magic Quadrant due to not meeting the overall inclusion criteria for customer count/revenue.

Vendors Covering Only CIAM

Akamai: Akamai provides the Akamai Identity Cloud, an AM offering for external identities resulting from its acquisition of Janrain. The Akamai Identity Cloud is a SaaS-delivered product. Akamai was

not included in this Magic Quadrant due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

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 in this Magic Quadrant due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

Transmit Security: Transmit Security offers an AM platform for primarily CIAM use cases. Its focus is on providing a CIAM platform with JTO, authentication (including passwordless authentication), user management, authorization, IDV, identity data validation, and fraud detection and response. Transmit Security was not included in this Magic Quadrant due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

Cloud Platform Vendors

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, SSO, authorization and audit reporting. Alibaba Cloud was not included in this Magic Quadrant due to not meeting the overall inclusion criteria for customer count/revenue.

Amazon Web Services (AWS): AWS offers AM functionality that includes SSO, MFA and directory services. AWS IAM Identity Center is an IaaS offering for the workforce, and Amazon Cognito serves CIAM. AWS was not included in this Magic Quadrant due to not meeting the technical inclusion criteria.

Google: Google Cloud Platform and Google Workspace provide SSO, MFA, directory services and related AM features for Google Cloud customers. Google was not included in this Magic Quadrant due to not meeting the technical 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 are used to comparatively evaluate providers in this research.

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods or procedures that enable IT vendors to be competitive, efficient and effective, and that 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. These include current product and service capabilities, quality, feature sets and skills. They can be offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Subcriteria:

- Core access management
- User authentication
- Authorization and adaptive access
- Portable identity integration
- Business to business capabilities
- Business to consumer capabilities
- Customization and extensibility
- API access control
- Threat reporting and ITDR
- Resilience
- Ease of deployment

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 examines the likelihood of the organization to continue to offer and invest in the product, as well as the product's position in the vendor's current portfolio.

Subcriteria:

- Financial health
- Success in AM market by AM revenue 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
- Pricing under several scenarios — This subcriterion is weighted heavily. Vendors were asked to identify actual expected deal pricing with appropriate discounts for different scenarios. Lower costs for the same scenario among vendors scored higher.

Market Responsiveness and Track Record: The 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 to changing market demands.

Subcriteria:

- General responsiveness to market trends and competitor activities over the last 12 months — new features added
- Track record (roadmap items from 2022 that were delivered in the past 12 months)

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message 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 and account support. This may also include ancillary tools, customer support programs, availability of user groups and service-level agreements.

Subcriteria:

- Technical support
- Professional services
- Customer satisfaction

Operations: The ability of the organization to meet goals and commitments. Factors include the 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
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Low
As of October 2023	

Source: Gartner (November 2023)

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 the challenges that buyers in the market are facing, and to shape their product offerings to help buyers meet those challenges.

Market Understanding: The 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:

- Competitors
- Strengths and weaknesses
- Market opportunities
- Threats

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 do not know about. We evaluate specific product marketing metrics, not corporate marketing. We look at how much awareness about specific AM messages is shared with the vendor's target audience, and the extent to which the customer's voice influences the vendor's AM product/service offerings.

Subcriteria:

- Marketing strategy and brand awareness
- Customer sentiment

Sales Strategy: A sound sales strategy uses the appropriate networks, including direct and indirect sales, marketing, service and communication. Partners 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 roadmap
- Differentiation

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

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 and divestitures. We focus on technical and nontechnical innovations introduced since last year, as well as the vendor's future innovations over the next 18 months.

Subcriteria:

- Near-term innovations related to trends (18 months)
- Longer-term innovation (18+ months)

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its "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

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

Evaluation Criteria ↓	Weighting ↓
As of October 2023	

Source: Gartner (November 2023)

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 AM specialization, and may offer a broader IAM portfolio. 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 and specialized product features, and have significant customer bases. However, they have not shown the Completeness of Vision for AM that Leaders have. Rather, their vision and execution for marketing, technology, methodology and/or means of delivery tend to be more focused on sales execution and doubling down on strengths of adjacent IAM capabilities, rather than making large investments in AM innovation. Challengers may see AM as a key part of a broader IAM 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. They may also have a large legacy AM installed base. Visionaries are noted for their innovative approach to AM technology, methodology and/or means of delivery. They often offer unique features and may be focused on a specific market segment or set of use cases, like CIAM. 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 market segments by customer size, typically offering AM 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 large customers, as well as a strong specialization in some areas

of AM (for example, user authentication). 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 to current offerings. Some Niche Players' pricing might be considered too high for the value they provide. 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

Workforce AM Is Mature, CIAM Is Growing

All vendors evaluated in this Magic Quadrant offer a SaaS-delivered product, and for vendors that offer multiple delivery models, only its SaaS product has been rated for the Product/Service criterion.

The AM market is still growing both for workforce and for CIAM, and uptake/adoption of CIAM solutions overall (49% of survey respondents who have some involvement or responsibility in their organizations' IAM) is still lower than for all workforce access management solutions (58% of survey respondents who have some involvement or responsibility in their organizations' IAM). [1]

Workforce AM use cases are relatively mature and are getting commoditized. Workforce AM innovation is slowing and having a lower impact on the market over time. However, the market growth and innovation potential for CIAM is higher, and Gartner is seeing significant demand from client organizations moving from unsecure CIAM capabilities to commercial vendor solutions at a faster pace than in previous years.

For all of these reasons, this year's Magic Quadrant for Access Management increases the focus on CIAM capabilities, including dedicated product/service evaluation for B2B and B2C features.

Given this, when evaluating AM tools:

- Clearly document your AM requirements for workforce and CIAM, and top priority outcomes for your AM capabilities.
- Make use of the interactive features of this research to create a custom view for your organization that prioritizes the different areas evaluated in alignment with your priorities.
- Organizations that need both CIAM and workforce AM capabilities, and prefer a single vendor approach, should weigh their CIAM capabilities more highly in solution selection. CIAM capabilities are more varied, while workforce AM capabilities are more commoditized. If having a single vendor isn't a major consideration for you, continue to evaluate and select each separately.

AM Is Evolving Its B2B Capabilities

Business customers and partners now routinely use more digital services, conduct more complex and sensitive interactions, and otherwise engage more deeply with organizations online. This has

resulted in the increasing need for flexible, delegated life cycle management for B2B users. Consider the following questions when dealing with B2B relationships:

- Which IAM tools should you consider for authentication, authorization, federation and governance functionality for your B2B users, like partners and supply chain providers?
- How should you handle delegated administration for your B2B users? This is one of the biggest feature differences between B2B and B2C use cases.
- How do you ensure tailored adaptive access policies are in place to define and trust B2B users differently in your AM instance.
- Can you use a single AM tool to support B2E, B2C and B2B use case requirements?

To meet these needs, tailored delegated administration and life cycle management features are increasingly available in AM offerings to cater to B2B use cases. AM tools have evolved in the past few years and are now positioned as the key to ubiquitous application access, enabling any type of user (B2E, B2B or B2C) to access any application, anytime, anywhere. They may be sufficient for most scenarios, except for more complex and highly regulated B2B use cases.

Sixty-four percent of AM vendors surveyed in this research offer out-of-the-box (OOTB) features to invite and register B2B users by delegating user registration to an internal user in the parent organization or to an administrator in a partner organization. However, less than one-third of all AM vendors surveyed offer OOTB features to delegate B2B users' registration and identity management to a third-party trusted identity (contact center or a trusted person). Most of the AM vendors evaluated still don't offer OOTB delegated administrator roles and access certifications for delegated admins.

Recommendations when evaluating AM vendors to support B2B use cases:

- Choose AM tools that support both B2B and B2C features when the organization has requirements for enabling business customer relationships that consist of both larger companies and sole proprietorships.
- Focus on delegated administration, identity federation, flexible identity management including life cycle management and provisioning/deprovisioning, extensible user account schema, OOTB delegated admin roles, and dedicated B2B customer subtenants' key features.
- Choose a solution that offers a wide range of authentication methods for B2B users. Augment with recognition and risk signals to address account takeover (ATO) risk, to meet cyber insurance requirements and to protect intellectual property.

- Augment your chosen AM tool with an IGA tool, or privacy management solution if needed, for more complex and highly regulated governance requirements for B2B users.

- If you find that your B2B requirements do not align well with the vendors covered in this Magic Quadrant, be quick to pivot; consider approaching CIAM vendors highlighted in the Honorable Mentions section of this research or other CIAM specialist vendors.

AM Is Still Under Attack

AM tools have significantly helped with the simplification and centralization of controls and configurations of access policies for protected resources (applications). However, attacks on IAM infrastructure continue to grow, and identity-based attacks have been leveraging, and ultimately lead to, the use of stolen credentials via web application access — the top action in breaches and incidents. [2]

AM generally sits in the middle of this attack path — between malicious actors and web and cloud resources. AM tools misconfiguration, as well as vulnerabilities and poor identity data hygiene, represent a large unmanaged attack surface today.

All AM vendors surveyed provide at least custom reports and raw logs to help with identity data hygiene in the AM tool, like dealing with orphan accounts or long-standing privileges. These logs, however, require significant manual analysis to pinpoint problems in identity data to be fixed. They don’t offer an easy way to discover other misconfigurations in the AM tool (like disabling or blocking legacy life cycle authentication methods in use). Only 18% of the vendors in this research offer a configuration recommendation engine that can help in identifying some misconfigurations in AM tools or in the identity data. Combined with security defaults, these recommendation engines are a great help in improving the resilience of AM tools. But their capabilities are still nascent and cannot be used as the only way to achieve and maintain proper configuration of IAM tools and identity data hygiene.

Other types of controls against identity attacks that have become popular in 2023 are MFA prompt bombing prevention techniques, like number matching and IP rate limiting/blocking. And existing AM capabilities, like adaptive access controls, are also being used to provide ITDR value. These include typical user behavior analysis based on device, location or time-based anomalies, which is offered by seven of this year’s evaluated vendors — an improvement from five last year. Four vendors in this Magic Quadrant have added further detection techniques, beyond user and entity behavior analytics (UEBA), including tactics, techniques and procedures (TTP) and indicators of compromise (IOC).

IDV using ID+selfie is also emerging as a popular control against attacks, expanding its primary use from customer onboarding into an alternative user flow for high-trust transactions, credential recovery or as a response from a suspicious signal. In this research, 27% of vendors surveyed offer their own IDV add-ons, and all of them are capable of integration with third-party IDV tools.

Recommendations when evaluating AM vendors:

- When evaluating MFA capabilities from AM vendors, eliminate from your shortlist vendors that don't offer at least number matching for MFA in order to reduce the risk of prompt bombing attacks. In your AM vendor selection, you should also set a minimum baseline to include at least threat detection leveraging user behavior analysis based on device, location or time-based anomalies.

- Differentiate AM vendors by evaluating other mechanisms for MFA prompt bombing prevention, step-up authentication, quarantining or session termination features to mitigate the risk of ATO. Also, ask for compromised password detection and IDV capability integration to further reduce the risk of ATO.

- Cautiously evaluate security recommendation features offered today by AM tools. But for now, plan for integrating AM with external security tools and processes that can facilitate identity data hygiene, ITDR and overall threat exposure management.

IAM Vendor Consolidation and Convergence Is a Mixed Bag

As per Gartner's 2022 Security Vendor Consolidation Survey, 75% of client organizations are pursuing a security vendor consolidation strategy — up from 29% in 2020. [3] The viable opportunities for consolidation are continuing to increase over previous years. Seventy-three percent of all AM vendors evaluated in this Magic Quadrant also offer adjacent IAM capabilities (IGA and PAM specifically). This is up from 66% last year.

While there is additional potential value — including streamlined management, improved operations and total cost savings — for client organizations if they select a vendor whose IAM offerings are a converged platform (multiple functions in one product versus separate products for IGA, AM, PAM), there are very few options for this available in the market. Most vendors offering solutions for adjacent capabilities deliver this as a suite or bundles of stand-alone products rather than a true converged platform. The same is true for adjacent capabilities for different user constituencies (some vendors deliver CIAM and workforce capabilities as separate products, even just for AM capabilities). In short, vendor consolidation opportunities are increasing while full IAM platform convergence remains uncommon.

Recommendations when evaluating AM vendors:

- Apply identity fabric principles to guide this "suite vs. best of breed" type of decision (see **Definition: Identity Fabric**). Take into consideration the commoditization of workforce AM features as mentioned above. An identity fabric strategy is not at odds with ongoing convergence trends, and no single vendor does it all. So, evaluate the AM tool composability, orchestration and journey-oriented abilities to make a choice between converged options and a combination of best-of-breed options.

- Manage overall IAM toolset cost and complexity by first fully defining/documenting your key IAM use cases for all IAM markets and user constituencies and using this required set of use cases to evaluate all tool needs across your program/portfolio. This does not mean combining solution selection for all tools into one effort; it means actively considering the interactions and integrations you will require between tools when selecting any one tool.

- Select your candidate AM solution vendors based on your use cases and requirements, ensuring those included can meet your organization's AM-related needs.

- Within your finalist set of AM solution candidates, decide between a stand-alone AM tool, an IAM suite vendor offering adjacent capabilities and any true converged platform options. Do so by evaluating the licensing/subscription cost, related deployment costs and total integration costs impact on your overall IAM portfolio (not just your AM solution selection).

Effective Passkeys Support Needs More Than Just WebAuthn

Passkeys (based on FIDO Alliance standards) have enjoyed increasing momentum as websites, operating system vendors and cloud providers add support for these credentials.

Conversations about passkeys should start with establishing a common understanding of the terminology. The FIDO alliance uses the term passkeys to refer to both "device-bound" passkeys and "multidevice" or "synced" passkeys, which is coherent because both types belong to the FIDO2 family of credentials that share common traits: they can be secured using software or hardware (using a secure element in either a portable hardware token ["security key"], smartphone, tablet or PC); are based on public key credentials; and conform with the Web Authentication (WebAuthn) API and the Client-to-Authenticator Protocol (CTAP).

However, the types differ in the following ways:

- Device-bound passkeys are highly recommended as a phishing-resistant authentication factor, especially for workforce use cases (see **Hype Cycle for Digital Identity, 2023** and **Innovation Insight for Many Flavors of Authentication Token**).

- Multidevice passkeys require an ecosystem account (Apple ID, Google Account or Microsoft account), passkey-capable hardware (PC, smartphone, tablet or security key), a compatible operating system and a compatible browser (to support cross-device authentication or to access passkeys from the native secure element).

- The benefits of synced passkeys are: quick user registration (if used, the ecosystem's user identity is already known), improved UX (passwordless, as simple as unlocking the device), trust (phishing-resistant) and recovery (automatically backed up and synced). These benefits should be balanced against the following challenges:

- Device-bound and synced passkeys have different user journeys (prerequisites, compatibility, benefits, etc.)
- Identity trust is rooted in the process that the ecosystem vendor uses for IDV and authentication.
- Passkey availability and recoverability are dependent on the mechanisms and infrastructure of the vendor ecosystem.
- Synced passkeys are no longer solely in the possession of the end user (or on an organization-managed device).

For more, see **Quick Answer: Using Passkeys for Customer and Employee Authentication**.

AM vendor survey responses reflect varying degrees of understanding of what synced passkeys mean for CIAM vs. workforce use cases. All of the vendors surveyed have passkey-compatible WebAuthn API support, and 45% claimed support for multidevice passkeys. However, at the cutoff date for this research, their offerings do not make a distinction between workforce or customer applicability, prerequisites, registration, recoverability or passkey management. Twenty-seven percent of vendors have included multidevice passkeys as a roadmap item; and only 18% have offered early features — the capability to block the enrollment of a synced passkey in a workforce use case and SDK features to select what type of passkey to issue.

Recommendations when evaluating AM vendors:

- Establish a shared understanding of the terminology by specifically addressing the drivers, use cases and type of passkey. The requirements, user journeys, applicability and benefits will vary between the types of passkeys.
- Assess the vendor's capabilities by asking about the availability of prerequisite checks, preconfigured profiles, consent flows (if the Apple, Google or Microsoft accounts are used for registration), ability to customize (e.g., to launch an IDV flow to establish a higher level of identity assurance), and any built-in controls designed specifically for synced passkeys (e.g., device-binding). Don't forget to articulate any use case constraints (e.g., possession requirement in an SCA use case).
- Design an inclusive authentication strategy based on an understanding of the user journeys and the personas associated with each use case, and one that supplements credential-based methods with recognition and risk signals.
- For workforce and B2B CIAM, examine the AM vendor's vision by asking how they see the future of multidevice passkeys in the enterprise; for example, applicability for extended workforce (third-party contractors, partners or temporary workers) or if the enterprise AM tool provides or works

with a universal device management (UDM) to provide granular passkey controls. Complement with an authentication specialist tool if it's a better fit for your passkey-driven user journeys.

OAuth 2.0 Is Often Not Enough for All Authorization Use Cases

The approach to authorization services in the AM market is clearly diverging, with most vendors in the market betting that strongly enabling OAuth 2.0 token-based authorization will provide sufficient capability for their customers. However, there are challenges with OAuth token-based authorization that cannot be addressed without a full externalized authorization management (EAM) service. For example, OAuth cannot be used to externalize fine-grained authorization decisions/policy from applications — it can only be used to provide attributes (claims) to applications; the applications would then need to apply a locally defined and managed policy to these attributes.

Only 18% of vendors evaluated in this Magic Quadrant provide full externalized authorization capabilities across all user constituencies. The remaining vendors largely rely on OAuth 2.0 capabilities for enabling application and API authorization.

Recommendations when evaluating AM vendors:

- Carefully identify your authorization requirements, including a broad set of authorization use cases, for example:
  - Customer authorization of data sharing with applications and services
  - API flow authorization
  - Workforce authorization to specific applicationsAuthorization to functions inside applications and resources
  - Authorization to data within an application or resource
- Compare your use cases with vendor capabilities, being mindful of authorization use cases that cannot be addressed with OAuth 2.0. If you have only use cases for which OAuth 2.0 works, then this will likely not be a significant differentiator for you. If your use cases extend beyond what OAuth 2.0 can handle, look to vendors that offer full EAM capabilities. We have called out vendors with strengths and cautions for authorization.

Market Overview

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

- **Maturing of workforce AM, growth in CIAM —** All vendors evaluated offer a SaaS-delivered product, and for vendors that offer multiple delivery models, only its SaaS product has been rated for the Product/Service criterion of this Magic Quadrant. Workforce AM is a maturing use case that

is getting commoditized. Fifty-eight percent of survey respondents with some involvement or responsibility in their organization's IAM have deployed workforce AM in 2023.1 Uptake in CIAM solutions is at 49%,1 an increase from 40% four years ago. Growth potential for CIAM is higher than workforce and there is significant demand from client organizations moving from homegrown CIAM.

- **Evolution of B2B CIAM —** 45% of all AM vendors surveyed in this research offer OOTB features to invite and register B2B users by delegating user registration to an internal user in the parent organization and to a delegated administrator in a partner organization. However, 64% of AM vendors evaluated still don't offer OOTB-delegated administrator roles and access certifications for delegated administrators.
- **ITDR and identity hygiene —** 63% of vendors evaluated have released some sort of ITDR capability, an increase from 44% last year. However, the majority of AM tools do not provide an indication of identity data hygiene, much less misconfigurations in the tool itself, vulnerabilities or gaps in their deployment, which creates an exposed, unmonitored attack surface.
- **IAM suites and convergence —** 73% of AM vendors evaluated also offer adjacent IAM capabilities (IGA and PAM specifically). This is up from 66% just last year. However, most vendors offering solutions for adjacent capabilities deliver this as separate stand-alone products rather than a true converged platform.
- **Passkeys —** All vendors surveyed provide basic passkey-compatible WebAuthn API support, and 45% claimed support for multidevice passkeys. However, the depth of support for multidevice passkeys is uneven — 27% of all vendors have mentioned multidevice passkeys as a roadmap item.

Gartner estimates that the AM market revenue for 2023 will amount to $6.14 billion, representing a growth rate of 23.9% over 2022. The market will continue to witness expansion, although growth is expected to taper off in the coming two to three years (see **Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 3Q23 Update**).

Evidence

[1] **2023 Gartner IAM Modernization Preventing Identity-First Security Survey**. This survey was conducted to determine how far along the market is moving in toward identity first security. The survey was conducted online from 9 June to 24 July 2023 among 303 respondents from North America (n = 104 in the U.S. and Canada), Latin America (n = 41 in Brazil), Asia/Pacific (n = 59 in India, Australia and Singapore) and EMEA (n = 99 in Germany, France and U.K.). Respondents' organizations had $100 million or more in 2022 enterprisewide annual revenue and 250 or more employees. Respondents were required to have some involvement in their organizations' identity and access management and planning to have at least one among workforce, consumer or

machine/nonhuman IAM in their organization within the next two years. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[2] **Verizon 2023 Data Breach Investigations Report**, Verizon.

[3] Top Trends in Cybersecurity — Survey Analysis: Cybersecurity Platform Consolidation

2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey: This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. The primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis. The research was conducted online during March and April 2022 among 418 respondents from North America (n = 277 in the U.S., Canada), Asia/Pacific (n = 37 in Australia and Singapore) and EMEA (n = 104 in France, Germany and the U.K.). Results were from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Note 1: What You Need to Know

The most common delivery model for AM is through SaaS; however, some vendors also offer software- or appliance-delivered deployments.

AM can be used by:

- Workforce users in business-to-employee (B2E) use cases, including but not limited to employees, temporary workers, vendors, contractors and partners (who work as part of an extended workforce business-to-business [B2B] use case).
- External users in business-to-consumer (B2C), B2B providers, G2C and B2B2X use cases.
- Machine users, including workloads and devices.

Pricing

We comment on the pricing of individual products based on a relative scale, using terms such as “well-above average,” “above average,” “average,” “below average” and “well-below average.” In each

pricing scenario, the average is the mean/median value of the pricing for all vendors evaluated in this research:

- Well-above average includes the three highest price points (out of 11 vendors).
- Well-below average includes the three lowest price points.
- Above average are prices above the average price point but below the three highest prices.
- Below average is below the average price point, but above well below price points.

Resilience

Most AM vendors offer SLAs for their SaaS services with an availability of at least 99.99%. We have highlighted vendors with a lower metric as a caution.

Workforce Versus CIAM Use Cases

For the sake of brevity and clarity, we refer to all AM use cases related to consumers, partners, suppliers, citizens and contingent freelance talent in B2C, B2B, G2C or gig economy use cases as "CIAM." Similarly, AM use cases, including employees, temporary workers, outsourcers and contractors in B2E use cases are referred to simply as "workforce."

Passkeys

In this document, we use the term "passkeys" in reference to **multidevice FIDO credentials** (synced passkeys).

When we mention "passkeys compatibility," it means the vendor is offering basic support to the mainstream **WebAuthn** specification. It does not mean the vendor is necessarily addressing the known challenges inherent to this novel type of credentials, like registration, which today requires an Apple, Google or Microsoft account, device sync risks, or other cons listed in **Quick Answer: Using Passkeys for Customer and Employee Authentication**. We have highlighted vendors that are addressing this additional type of support as a strength.

Orchestration

All journey-time orchestration (JTO) solution capabilities — as described in the **Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX** — are referred to simply as "JTO," for the sake of brevity. Other types of orchestration, where they exist (such as administration-time workflows), are referred to as such.

Identity Verification

For the sake of brevity, all identity verification capabilities — as described in the **Market Guide for Identity Verification** — are referenced simply as "IDV."

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.

research is produced independently by its research organization without input or influence from any third party. For further information, see "**Guiding Principles on Independence and Objectivity**." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.