Magic Quadrant for Access Management

2 December 2024 - ID G00805920 - 54 min read

By Brian Guthrie, Nathan Harris, **and 2 more**

Workforce access management capabilities are mature, but innovation is slowing. CIAM product features are thriving, machine IAM capabilities are increasing and partner IAM capabilities are in demand. This research features AM vendors with advanced capabilities that differentiate them in this market.

Market Definition/Description

Gartner defines access management (AM) as tools that include authentication and single sign-on (SSO) capabilities, and that establish, manage and enforce runtime access controls for modern standards-based and classic web applications and APIs.

AM's purpose is to enable SSO access for people (employees, consumers and other users) and machines to protected applications in a streamlined and consistent way that enhances the user experience. AM is also responsible for providing security controls to protect the user session in runtime, enforcing authentication and authorization using adaptive access. Lastly, AM can provide identity context for other cybersecurity tools and reliant applications to enable identity-first security.

Mandatory Features

The mandatory features for this market are:

- SSO and session management, with support for standard identity protocols (e.g., OpenID Connect, OAuth 2.0., SAML) for accessing standards-based and legacy apps (via proxies or agents).
- User authentication, including:
  - Support for phishing-resistant multifactor authentication (MFA) methods (e.g., X.509, FIDO).
  - Controls to mitigate usage of compromised passwords.
  - Protections against common MFA attacks directly or via out-of-the-box integration with third-party authentication services.
  - Support for any type of passwordless authentication methods.

- Authorization policy definition and enforcement for any resources directly defined in the system such as applications and APIs (including support for OAuth 2.0).
- Adaptive access capability based on dynamic evaluation of identity trust and access risk.
- A directory or identity repository for all constituencies, including identity synchronization services.
- Basic identity life cycle management, including support for enabling create, read, update and delete (CRUD) operations for all user types.

Common Features

The common features for this market include:

- Journey-time orchestration, and other low-/no-code interfaces for customization and extensibility in the context of AM.
- Identity administration for managed integrated applications, including profile management capabilities, and support for the System for Cross-Domain Identity Management (SCIM) standard.
- Progressive profiling and consent management, personally identifiable information (PII) data management and anonymization.
- Delegated administration, including provisioning for the workforce of partners and customers.
- Identity verification (IDV), either out of the box or via prebuilt integration with third-party IDV providers.
- Support for decentralized identities, verifiable credentials, and portable digital identity integration for federation and access control.
- Support for account takeover (ATO) prevention controls, continuous passive authentication, iterative authentication flows and other features enabling continuous adaptive trust (CAT).
- Threat detection and response (TDR) functions, including out-of-the-box extended detection and response (XDR) integrations.
- AM functions for machines (workloads, services and devices).
- Externalized authorization policy management and enforcement for entitlements in applications and services (also called fine-grained authorization), including the ability to control authorization via attribute-based access control (ABAC), but not limited to just group-/role-based access.

Magic Quadrant

Figure 1: Magic Quadrant for Access Management

Gartner

Vendor Strengths and Cautions

CyberArk

CyberArk is a Challenger in this Magic Quadrant. It offers two AM packages: Workforce Access for workforce and Customer Access for customer identity and access management (CIAM). Both AM products are offered as SaaS, and can be purchased as a bundle or separately. CyberArk's customers are mainly in North America and Europe, and in banking, insurance, and communications and media.

CyberArk has recently added workforce-enhanced passwordless features, workforce-zero standing access and an attack simulator for CIAM use cases. Its roadmap items include an AI assistant to improve security, multilevel organization support with fine-grained delegated

administration for partner IAM use cases and enhanced low-code/no-code journey-time orchestration for AM and CIAM use cases.

Strengths

- **Market responsiveness:** CyberArk launched CORA AI, a new AI engine focused on insights, response recommendations and automated actions.
- **Product:** CyberArk has expanded coverage in detection and response. Its enhanced adaptive multifactor authentication (MFA) bypass attempts circumventing identity infrastructure controls and malicious credential theft.
- **Customer experience:** CyberArk offers multiple professional service assistance programs that provide valuable product knowledge to its customers. The services span deployment maturity models, enhanced security methodology programs, framework best practices and suggested phased roadmaps.
- **Sales strategy:** CyberArk has accomplished a strong partner training program and established an identity security framework program called CyberArk Blueprint.

Cautions

- **Marketing execution:** CyberArk is not as widely recognized as an AM vendor as other vendors in this research. Gartner believes that low brand recognition may affect AM product awareness over the long term.
- **Overall viability:** CyberArk has fewer partner IAM and CIAM customers than other vendors in this research.
- **Pricing:** CyberArk's pricing is well above average for workforce and CIAM, compared to its peers in this research.
- **Market understanding:** CyberArk's market understanding is heavily influenced by its strengths and background in the privileged access management (PAM) market.

Entrust

Entrust is a Challenger in this Magic Quadrant. It offers a single platform approach for workforce and CIAM that can be deployed in the cloud as SaaS, on-premises or in hybrid mode. Entrust offers workforce and CIAM separately or as a bundle. Its customers are mainly in North America and Europe, and in banking and government.

Entrust acquired Onfido in April 2024. It recently added fine-grained consent management for CIAM and a standards-based approach to externalized authorization policy management for CIAM. Entrust's roadmap items include AI-driven threat detection and response, an enhanced single pane of glass, and enhanced adaptive access flows.

Strengths

- **Pricing:** Entrust's all-inclusive pricing for several scenarios evaluated in this research is consistently lower than average compared to its peers. Entrust's sales model allows for significantly reduced pricing for nonprofit organizations and educational institutions.
- **Customer experience:** Entrust's simple deployment model eliminates the need for a professional services partner or third-party integrator service. Among vendors in this research, Entrust has a higher percentage in product sales that do not require such services.
- **Market responsiveness:** Entrust released access management security enhancements and improved privacy features with decentralized identity and verifiable credentials for private cloud deployments.
- **Product strategy:** Through its acquisition of Onfido, Entrust expanded its product offering in 2024 to include enhanced low-code/no-code workflow orchestration, biometric authentication, public-key infrastructure (PKI) as a service and digital signing integrations.

Cautions

- **Market execution:** Entrust lacks AM brand awareness and recognition compared to other vendors evaluated in this research. From Gartner's observations, Entrust's low brand recognition can potentially impact clients' decision making.
- **Vertical strategy:** Entrust has established its brand awareness primarily within the banking and government agency verticals, with more than half of its customers focused in these two areas.
- **Market understanding:** Entrust's market intelligence is very focused on security drivers and security-sensitive client organizations; however, this increases the risk that its marketing will not fully address the needs of organizations that place a high priority on user experience, which is more common for CIAM customers.
- **Marketing strategy:** Entrust is better known for its workforce product than for its CIAM product, although the balance is changing with the addition of Onfido.

IBM

IBM is a Leader in this Magic Quadrant. IBM Verify offers SaaS, on-premises and hybrid deployment models. IBM Verify's features can be purchased individually or as a bundle. Its customers are mainly in North America and Europe, and are primarily in banking, insurance and government.

IBM recently added a new GenAI cybersecurity assistant, advanced delegated administration and expanded orchestration features. IBM's roadmap items include continuous access evaluation profile (CAEP) enhancements, user registration enhancements and OpenBanking financial grade APIs (FAPI 2.0) expansion. Roadmap items also include an expanded framework to support complex, multilevel, multipermission and multipersona-delegated administration use cases.

Strengths

- **Pricing:** IBM is priced competitively, with workforce scenarios priced below average when compared to its peers. Pricing for customer and partner scenarios is well below the average for the market as a whole. In addition, IBM offers its top clients enterprise license agreements, which may provide additional savings.
- **Innovation:** IBM's CIAM feature enhancements include user relationship mapping of Internet of Things (IoT) devices, multipersona-delegated administration and privacy enhancements.
- **Geographic strategy:** IBM's global presence enables it to provide effective support for its AM product in some regions, which are not well-supported by most vendors in this research, including Asia/Pacific and South America.
- **Product:** IBM Security Verify provides a developer portal that simplifies application onboarding.

Cautions

- **Marketing execution:** IBM lacks market awareness and brand name recognition for both its CIAM and workforce AM solutions.
- **Business model:** IBM's main customer base is large organizations, so small to midsize businesses perceive IBM as not a good fit.
- **Product strategy:** IBM has been slow to obtain specialized government certifications, impacting its competitive edge.
- **Market responsiveness:** IBM is the only AM vendor not to change its cost model, pricing or product bundling over the last 24 months.

Microsoft

Microsoft is a Leader in this Magic Quadrant. It offers Microsoft Entra ID for workforce and two CIAM products: Microsoft Entra External ID and Microsoft Azure AD B2C. All three are offered as SaaS. Microsoft has a global customer base within all evaluated verticals.

Microsoft recently added centralized management of external-facing applications for CIAM, Orchestrator, and expanded support for open standards like SCIM, CAEP, FIDO and Verifiable Credentials. Microsoft's roadmap items include support device-bound passkeys in Microsoft Authenticator, Copilot for Security (embedded in Microsoft Entra ID), and real-time Face Check with Entra Verified ID for CIAM users.

Strengths

- **Pricing:** Microsoft's pricing for its AM products is very competitive. Its customer and partner product pricing is well below its peers in this research.
- **Business model:** Microsoft's current AM business approach is evaluated very highly for the business model category. Microsoft has a strong focus in product strategy and builds on its strengths when collaborating with third-party vendors for features not offered by Microsoft Entra ID.

- **Product:** Microsoft has centralized and consolidated product administration into a single platform across workforce, external and workload identities.

- **Overall viability:** Microsoft's overall viability was evaluated as very strong. Its strategy of offering Microsoft Entra ID as a core piece of its overall cybersecurity strategy, tightly integrated with Microsoft 365 and Microsoft Entra as a whole, continues to resonate with clients and has resulted in its AM installed base growing significantly year over year.

Cautions

- **Marketing execution:** Microsoft clients continue to express frustration with the continued product name rebranding and license confusion of their CIAM products. Additionally, Microsoft will continue to offer two CIAM products until Microsoft consolidates its External ID product into one offering.

- **Customer experience:** Microsoft's deployment, support and overall product administration continue to be confusing and complex for organizations, especially where additional integration coding is required.

- **Product:** Microsoft's Azure AD B2C requires significant customization and configuration to deliver user workflows and onboarding alternative MFA methods.

- **Market understanding:** Microsoft offers multiple workforce license portfolios, causing customer confusion. However, Microsoft has started a licensing consolidation strategy. Two business models will be offered for Workforce: Consumptive for external users and machines, and annual licensing per user/month subscription.

Okta

Okta is a Leader in this Magic Quadrant. It offers multiple SaaS-delivered AM products: one for Workforce Identity Cloud (WIC) and several for Customer Identity Cloud (CIC). No on-premises versions are available. Okta has a global customer base within almost all evaluated verticals.

Okta recently added stronger onboarding and recovery features across both workforce and CIAM; secure continuous authentication; workflow centralization across all resources, devices and workloads; and fine-grained authorization capabilities. Okta's roadmap items include enhanced identity threat detection and response (ITDR), expanded identity verification (IDV) capabilities to support digital credentials for CIAM, and advanced bot detection with enhanced machine learning.

Strengths

- **Product strategy:** Okta demonstrates one of the strongest product strategies and delivered product sets in this market.

- **Marketing strategy:** Okta has the strongest overall marketing strategy and execution in this market with comprehensive and effective marketing plans.

- **Innovation:** Okta provides increased attack surface visibility, enhanced universal logout features, and improved fine-grained governance and authorization controls across applications

and resources.

- **Product:** Okta's product is evaluated as above average in every category except sales execution/pricing. The two core categories where Okta is most competitive are market execution and product strategy.

Cautions

- **Pricing:** Okta's pricing is a common complaint among Gartner clients, as it continues to be among the most expensive in the AM market. However, Okta recently added developer-focused product enhancements and capabilities without any changes to pricing.
- **Geographic strategy:** Nearly three-quarters of Okta's customers are in North America, the highest single regional concentration among all AM vendors in this research.
- **Business model:** Okta's sales have faced challenges. However, Okta has evolved its business model, showing year-over-year improvements through specialized roles and partner engagement.
- **Operations:** Okta's lack of timely response to cybersecurity incidents caused brand setbacks, which resulted in confusion among Gartner clients and increased concern for potential buyers. Okta has since created an initiative for identity attack awareness named Okta Secure Identity Commitment (OSIC).

One Identity

One Identity (part of Quest Software) is a Niche Player in this Magic Quadrant. Its AM solution, OneLogin, is offered as a SaaS-only solution and is built on One Identity's cloud infrastructure. It can be purchased as a bundled product or sold separately with individual modules. One Identity's customers are mainly in North America and Europe, and within banking, communications and media, and services.

One Identity recently added Web Authentication (WebAuthn) support for FIDO2 passkeys, desktop MFA for macOS, and enhanced identity threat detection and response options. Its roadmap items include multitenant failover, phishing resistant authentication and bring your own device (BYOD) self-service device registration.

Strengths

- **Pricing:** One Identity's AM product, OneLogin, has a history of being a more affordable option than others in this research. Its pricing continues to remain below market averages for a series of evaluated pricing scenarios.
- **Marketing execution:** One Identity has developed a solid narrative around its brand and targets its marketing toward the benefits of ease of use, accelerated deployment and its minimal to no on-premises requirements.
- **Sales strategy:** One Identity offers a very strong partner training program, go-to-market webinars and multiple accreditation programs.

- **Innovation:** One Identity offers comprehensive data analytics engines and enhanced risk detection, and adopted a passwordless approach by default for all user personas. It has improved in innovation from last year when it was evaluated lower than average.

Cautions

- **Overall viability:** One Identity had some of the lowest company revenue and customer count growth among the vendors evaluated in this AM research. OneLogin has had slower growth compared to other AM vendors evaluated in this research.

- **Operations:** Although One Identity is averaging 99.99% uptime for all customers, One Identity's monthly mean uptime achieved was 99.9752% for its SaaS product from January 2023 to January 2024 across all regions, which is one of the lowest evaluated for AM vendors.

- **Market understanding:** One Identity has low brand awareness but is focusing on increasing brand awareness for ease of use, accelerated deployment and a minimal-hardware approach for on-premises deployments.

- **Product:** One Identity does not support machine access management, account linking, correlation and deduplication through custom coding or manually; it's the only AM vendor in this research that does not support all three categories.

OpenText

OpenText is a Niche Player in this Magic Quadrant. Its AM solution, OpenText Access Manager with Managed Services (NetIQ), is offered as a SaaS or an on-premises solution that can be purchased as a bundle or as individual modules. OpenText's customers are mainly in North America and Europe, and are primarily in banking, government and healthcare.

OpenText's recently added features include continuous authentication, new authorization microservices based on OPA standards, and enhanced authorization risk services. OpenText roadmap items include event-based authentication and authorization, API enforcement points, biometric enrollment, and CIAM as a service.

Strengths

- **Innovation:** OpenText is evaluated favorably for innovation. Its enhancements include just-in-time (JIT) integration using built-in threat services, CIAM identity verification and validation feature updates, and policy decision enforcement improvements in DevOps continuous integration/continuous delivery (CI/CD) pipeline authorizations commonly used by developers.

- **Sales execution:** OpenText provides a wide variety of pricing models, discounted packaging pricing and flexible licensing schemes for buyers to customize product selection.

- **Market understanding:** OpenText is above average for this market in tracking market needs, opportunities and gaps. It also highlights some market opportunities not being addressed by most vendors.

- **Overall viability:** OpenText's revenue growth in the last fiscal year was among the highest of the AM vendors evaluated in this research.

Cautions

- **Pricing:** OpenText's pricing is uneven when evaluated for a series of scenarios in this research, and pricing for small and midsize scenarios is above the AM market average.
- **Market responsiveness:** OpenText deployed fewer roadmapped items than expected due to market shift and customer demands.
- **Marketing execution:** OpenText's adoption of its SaaS product this year has been slower than desirable.
- **Marketing strategy:** OpenText's go-to-market strategy was below average when compared to others in this research. However, OpenText is providing greater investments toward marketing to improve visibility and market presence.

Ping Identity

Ping Identity is a Leader in this Magic Quadrant. Ping Identity offers a broad portfolio of AM products. Its two primary SaaS offerings are PingOne for Customers and PingOne for Workforce. Ping Identity's customer base is global, but mainly in North America and Europe, with customers in multiple verticals.

In August 2023, Thoma Bravo merged ForgeRock with Ping Identity. Over the past year, Ping Identity has added new AI features, orchestration enhancements and partner IAM-specific features. Its roadmap items include a common SDK layer for developers, a single "mission control" administration interface for all Ping products and enhanced fraud capabilities.

Strengths

- **Product:** Ping Identity placed highest in authentication and identity verification for both its workforce and customer products for all AM vendors evaluated in this research. Additionally, Ping Identity offers flexibility for managing complex identity groups and business relationships that can be tied to CIAM or workforce, or are specific to partner IAM use cases.
- **Product strategy:** The Ping Identity orchestration tool provides extensive and advanced drag-and-drop features for workforce and CIAM use cases.
- **Innovation:** Ping Identity is very strong in innovation, providing features like fraud prevention with behavioral biometrics, advanced centralized fine-grained authorization (FGA) and AI advancements across its portfolio.
- **Market understanding:** Ping Identity demonstrates strong market tracking, including a clear view of its own strengths and weaknesses in the market, and identifies some market considerations not seen by most vendors.

Cautions

- **Business model:** Ping Identity's focus has primarily been serving midsize to large enterprises, which may result in fewer features catering to small businesses.
- **Sales execution:** Ping Identity has a complex portfolio that was made even more complex after the merger and acquisition of ForgeRock. Additionally, Ping Identity's pricing for a series of scenarios evaluated in this research is above market averages compared to other vendors, especially for workforce and partner use cases.
- **Overall viability:** Ping Identity's SaaS growth was below average when compared to other AM vendors in this research.
- **Geographic strategy:** Ping Identity does not have as strong or broad regional support as its top competitors in some regions, including APAC and South America.

RSA

RSA, new to this Magic Quadrant, is a Niche Player. RSA is known for its strength in workforce use cases. Its AM portfolio is branded under the name of RSA ID Plus. RSA ID Plus is offered as a SaaS, on-premises or hybrid solution, and is offered for both workforce and CIAM. RSA ID Plus is offered as a subscription with good, better or best editions and multiple add-ons. Its customer base is concentrated in North America and Europe, with new cloud investments supporting growth across Asia/Pacific. RSA's customers are primarily in the banking, securities, insurance and government sectors.

RSA recently introduced identity insights, enhanced integration capabilities enabling customers to bring their own identity verification solutions, and expanded OAuth 2.0 capabilities for machine-to-machine and IoT access. RSA's roadmap items include mobile passkey, unified directory enhancements and further investments into existing machine learning and AI capabilities to assist security administrators.

Strengths

- **Product:** RSA's unique high-availability resilient failover process for MFA allows organizations to fail over from the cloud to on-premises hardware, then to local agents, avoiding complete outages.
- **Sales strategy:** RSA's comprehensive proof of concept (POC) program allows potential buyers the ability to integrate with their own identity data and applications. This unique approach allows the buyer to preserve all configurations and changes after product purchase.
- **Operations:** RSA has the highest professional services, sales and marketing retention rate of all of the AM vendors evaluated in this research.
- **Customer experience:** RSA is evaluated as above average in customer experience. It has a wide variety of AM-relevant services available after sale that help its clients mature their AM after the initial deployment.

Cautions

- **Product:** RSA offers fewer CIAM features, compared to other AM vendors, such as limited BYOI capabilities. It also has the least mature product capabilities for partner management and decentralized identity (DCI) among vendors in this research.
- **Pricing:** RSA offers a named user pricing model, even for nonworkforce user constituencies, which makes its pricing well above market averages for a series of customer use case pricing scenarios evaluated in this research.
- **Marketing strategy:** Due to RSA being well-known for its authentication solutions, its access management brand name awareness is lower compared to other AM vendors in this research.
- **Viability:** RSA's customer base is primarily workforce. While a majority of those customers are currently operating on-premises, likely due to RSA's unique on-premises failover process, many are migrating toward cloud and hybrid environments with RSA's support.

Thales

Thales is a Visionary in this Magic Quadrant. Thales offers two AM products: OneWelcome Identity Platform for CIAM and SafeNet Trusted Access for workforce. OneWelcome Identity Platform is sold as SaaS-only, while SafeNet Trusted Access is sold as SaaS or software. Thales' primary customer population is in North America and Europe, in banking, insurance, communications and media.

Thales recently added delegated administration enhancements, and new privacy and consent management features, and consolidated multiple passwordless authentication methods under a Passwordless 360° brand. Thales' roadmap items include enhanced workforce passkey life cycle management to augment its FIDO and PKI authenticator portfolio, an updated authentication orchestration flow editor, and a new enrollment, recovery and help desk verification process integrated with Thales' ID verification options.

Strengths

- **Product:** Thales offers a strong delegated administration feature providing easy persona manageability for partner, customer and other external identity relationships. Thales' privacy and consent management module is purpose-built for global privacy regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA) and India's Digital Personal Data Protection Act (DPDPA).
- **Innovation:** Thales is evaluated as above average in innovation compared to other AM vendors in this research due to adding many innovative partner IAM features to its portfolio, along with an extensive list of roadmap items.
- **Marketing execution:** Thales is executing a compelling marketing plan, including highly targeted messaging by sector/industry and constituency (workforce, partner and customer).
- **Sales strategy:** Thales' AM product provides unique product packaging and a tailored product selection, allowing customers to select from multiple tiered B2X capability options.

Cautions

- **Pricing:** Thales' pricing is uneven when evaluated for a series of scenarios in this research. Its pricing for small and midsize scenarios is below average, and pricing for large-size scenarios is above the market average.
- **Overall viability:** Thales has one of the lowest renewal rates for its AM products compared to other vendors evaluated for this research.
- **Geographic strategy:** Thales is popular in Europe but has relatively lower brand awareness in other regions. Its geographical strategy suggests Thales is addressing this problem by investing more in marketing and sales in other regions.
- **Vertical strategy:** Although Thales is focused on extending its global customer base for both workforce and CIAM, Thales' strategic priority is to shift focus from midmarket to enterprise customers, especially for its CIAM capabilities.

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

RSA

Dropped

- Oracle has been dropped due to not meeting inclusion criteria.
- ForgeRock was dropped due to its merger with Ping Identity.

Inclusion and Exclusion Criteria

This Magic Quadrant research identifies and analyzes the most relevant vendors and their products in the AM market.

Inclusion and exclusion criteria are mainly unchanged since last year. The most significant changes are a total of six mandatory requirements and nine common features.

To qualify for inclusion, vendors need to:

- Have marketed and sold generally available products and services in their FY23 to support both workforce (all workforce, including employees, contractors, consultants and gig workers) and customer (individual customer, partner IAM, customer, consumer and citizen) 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 FY23.

Or,

- 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 six functional requirements, delivered as a SaaS product. Products/services needed to be in production (general availability) as of 8 July 2024 to be considered in the evaluation:

- Single sign-on (SSO) and session management with support for standard identity protocols (OpenID Connect, OAuth 2.0., SAML) for accessing standards-based and legacy apps (via proxies or agents).
- User authentication including support for phishing-resistant and other account takeover (ATO) prevention MFA methods (e.g., X.509, FIDO), controls to mitigate usage of compromised passwords and protections against common attacks against MFA directly or via out-of-the box integration with third-party authentication services. Support for any type of passwordless authentication methods.
- Authorization policy definition and enforcement for any resources directly defined in the system, including applications and APIs (including support for at least, but not limited to, OAuth 2.0).

- Adaptive access capability based on dynamic evaluation of identity trust and access risk.
- A directory or identity repository for all constituencies, including identity synchronization services.
- Basic identity life cycle management, including support for enabling create, read, update and delete (CRUD) operations for all user types.

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

- AM products that cannot support, or are not marketed to support, both workforce and customer 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 access management products, rather than being provided through delivery of the vendor’s own intellectual property.
- AM functions 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 identity governance and administration (IGA) vendors, 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**).
- IDV is also being offered as part of broader platforms. Many stand-alone IDV vendors focus on IDV alone. However, some vendors now offer IDV as part of a broader biometric authentication tool. Future market consolidation is likely as IDV vendors consider acquiring competitors to buy market share in new geographies or gain a foothold in new industries.

- 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** and **Market Guide for Unified Endpoint Management Tools**).

Honorable Mentions

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 was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

Amazon Web Services (AWS): AWS provides a comprehensive suite of identity and access management services across workforce and customer identity. Core services include AWS IAM for fine-grained permissions, AWS IAM Identity Center for centralized workforce access management, IAM Roles Anywhere for extending IAM capabilities beyond AWS, and Amazon Cognito for customer identity. Amazon was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

Exostar: Exostar offers Access: One as part of its IAM product suite. Access: One provides workforce, partner and CIAM solutions delivered as a service. Access: One is relatively unique in the service delivery approach serving as an identity and access governance “hub” for specific highly regulated industry partner communities. Exostar’s AM services are also bundled with third-party (supplier/partner) vetting and onboarding/supplier management services, which is also not common in this market. Exostar was not included in this Magic Quadrant due to not meeting the access management customer and revenue inclusion criteria.

Fortinet: Fortinet offers FortiAuthenticator. FortiAuthenticator is an AM product sold as hardware and virtual appliances. FortiAuthenticator enables identity and role-based security policies in the Fortinet identity fabric with or without Active Directory integration. FortiAuthenticator features include centralized management of user identity information, secure multifactor/OTP/passwordless authentication with full support for FortiToken. RADIUS, LDAP, SAML OIDC and FIDO2 Authentication. Fortinet was not included in this Magic Quadrant due to not meeting the access management customer and revenue inclusion criteria.

Google: Google Cloud Platform (GCP) 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 access management revenue inclusion criterion.

Imprivata: Imprivata offers many different IAM products. Imprivata Enterprise Access Management (formerly known as OneSign and Confirm ID) offers SSO, MFA, user access analytics, and passwordless authentication options such as phone as a token, proximity tokens, face recognition, fingerprint biometrics and hands-free authentication. Imprivata was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

Salesforce: Salesforce offers both workforce and CIAM products. Salesforce is offered as a SaaS solution only. For workforce, Salesforce identity services offer SSO and MFA. For CIAM, Salesforce offers SSO, BYOI and API integration. Salesforce was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

SAP: SAP offers both workforce and customer solutions. SAP's Customer Identity and Access Management solution is offered in four enterprise solutions: CIAM, partner IAM, enterprise consent and preference management, and data integration and deployment. SAP's CIAM solution is deployed in the cloud and is available as SaaS. SAP was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

SecureAuth: SecureAuth offers CIAM and workforce solutions via SaaS, hybrid and on-premises deployments to provide SSO, passwordless, and AI/ML risk-driven adaptive MFA across business assets, such as web apps, workstations, virtual desktop infrastructures (VDIs) and mobile devices, as well as key CIAM capabilities, including FGA, consent management, identity orchestration, and open banking. Additionally, SecureAuth supports partner IAM/B2B2C use cases requiring flexible user interaction journeys with subtenancy, sub-branding and administrative delegation. SecureAuth was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

Transmit Security: Transmit Security offers a SaaS-based AM platform, "Mosaic," primarily for large-scale CIAM use cases. Transmit Security offers active-active AM solutions spanning fraud, identity detection and response (ITDR), identity verification (IDV), strong risk-based authentication, user ID consolidation, CIAM and partner IAM (B2B) identity management, and identity orchestration. Transmit Security was not included in this Magic Quadrant due to not meeting the access management inclusion criteria.

Evaluation Criteria

The evaluation criteria and weights tell you the specific characteristics and their relative importance, which support Gartner's 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:

- ID data, profile, life cycle management - workforce
- ID data, profile, life cycle management - customer

- Authentication, ID verification - workforce
- Authentication, ID verification - customer
- Access control - workforce
- Access control - customer
- SSO, session management, application support - workforce
- SSO, session management, application support - customer
- Partner management and delegated administration
- Orchestration and extensibility
- Portable and decentralized Identity
- API access control
- Service security and resilience
- Machine access management

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 2023 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:

- Customer relationship and services
- 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	Medium
Operations	Low
As of October 2024	

Source: Gartner (December 2024)

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:

- Deal strategies
- 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.

- General business models
- Core purpose and aspirations in this market

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
- Other segmentations like midmarket and service providers

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
As of October 2024	

Source: Gartner (December 2024)

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, and 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 AM use cases or methodologies. They may focus on specific industries or customer segments, and can actually outperform many competitors. They may focus their AM features primarily on a specific use case, technology stack and/or infrastructure. Vendors in this quadrant often have a small installed base, a focus on specific customer segments, a limited investment in AM, or a geographically limited footprint. Or they may focus on other factors that inhibit them from providing a broader set of capabilities to enterprises. However, this does not reflect negatively on the vendor's value in the more narrowly focused service spectrum. Niche Players can be very effective in their area of focus.

Context

All vendors evaluated in this Magic Quadrant offer a SaaS-delivered product; for vendors that offer multiple delivery models, only their SaaS product was rated for the Product/Service criterion.

The Access Management Market Is Growing

The access management market continues to grow significantly. According to the **worldwide security software revenue market share in 2023**, the AM market totaled $5,847 million. Additionally for 2023, the AM market grew 17.6%.

Overall, customer identity and access management is the primary contributor to the growth of the AM market. Gartner is seeing significant demand from client organizations moving from old CIAM deployments to commercial vendor solutions at a faster pace than in previous years.

CIAM Is Thriving

CIAM is in higher demand this year and has grown due to several factors. These include the discontinuation of homegrown solutions, enhanced admin/user interfaces (UX), centralization of

customer identity processes (removal of siloed approaches), the need for strong customer authentication (SCA), the need for BYOI, and new out-of-the-box features and capabilities. [2]

The 2023 Gartner IAM Modernization Preventing Identity First Security Survey reveals that 58% of respondents deployed workforce AM and 49% used CIAM solutions. [1] Also, the Gartner survey suggested that CIAM was Asia/Pacific's largest area for budget increases in 2024.

For these reasons, this year's Magic Quadrant for AM increases the focus on CIAM capabilities, including increased differentiation between CIAM and workforce features in the product evaluation.

New Identity Threat Detection and Response Capabilities Are Emerging

This year, AM vendors have significantly increased their threat detection and response capabilities. AM vendors have focused their efforts on bolstering their security posture and helping reduce attack surface. AM vendors have introduced new features, such as automated ITDR alerting, custom device posture checking, and AI/ML-based detections to protect against injection attacks.

Other types of controls against identity attacks have become popular in 2024. They are AI-driven attack simulators (to help organizations test and improve their security posture by simulating various cyberattack scenarios); reducing attack surfaces (increased visibility and providing real-time response to attacks/threats); and enterprisewide ITDR (support of all identity security needs for any attack vector across customer and workforce use cases, including deeper integrations for smarter security detections and recommendations).

In addition, AM vendors have considerably reduced time frames for administrators for complex configurations, such as AI assistance with creating and configuring an access policy for protected resources, and reducing complexity when creating, updating and managing external authorization management policies.

AM vendors have also improved other areas. These include consolidating and simplifying administrative consoles (offering comprehensive insights for administrators, highlighting risks that may require attention or remediation, and providing simplified visual orchestration/journey-time capabilities), and providing developer-friendly tools that ensure apps are safe, secure and compliant.

Access Management Capabilities for Machine Users Are Maturing

As organizations continue their move to the cloud and digital business transformation, the number of machine users (devices and, most significantly, workloads) also continues to increase. API enablement, automation (both software-based and RPA) and, more recently, AI adoption including the use of AI agents are all machine-actor dependent. This increases the need for strong, sustainable access management capabilities for machine users over time.

Due to the increased need, this year's research adds a dedicated evaluation for machine AM capabilities. Significantly, the first year's results of vendor assessments for machine AM

capabilities show that there is a wide range of machine AM capabilities already available in the market. Several vendors included in this Magic Quadrant demonstrate a strong overall capability for access management for machine users.

When evaluating AM tools for machine capabilities:

- Clearly identify your requirements for AM functions for machine users in your environment and in your customer population (some machines are on the customer side).
    - Limit these to requirements appropriate for AM tooling, as a complete solution for machine IAM will require capabilities from IGA, credential management and PAM as well. Expect your AM tooling to provide only AM functions for machines; do not expect it to take over adjacent functions/capabilities.
- Prioritize machine AM capabilities relative to your organization's workforce AM, CIAM and partner IAM needs based on your overall IAM strategy and business objectives.
- Evaluate AM vendor candidates for support for your machine AM requirements.
- If your preferred vendor can support your requirements, use the same vendor for AM capabilities for multiple constituencies.
- If your preferred vendor for other constituencies cannot meet your machine AM requirements, evaluate best-of-breed machine IAM vendors/tools.

Access Management Capabilities for Partner IAM (B2B) Are in Demand

Business customers and partners now routinely use more digital services, conduct more complex and sensitive interactions, and otherwise engage more deeply with organizations online. Partner constituencies needing instant, secure and governed access to enterprise resources differ in IAM capabilities, levels of trust, relationship with the host organization and needed access, resulting in customized implementations lacking proper controls and agility. Achieving visibility and compliance are also challenging because identities and access rights are most commonly handled in applications and separate identity stores that are not intended for these use cases.

To meet the above needs, AM tools continue to evolve and are now positioned as the key to ubiquitous application access, enabling any type of user (workforce, partner or CIAM) to access any application — anytime, anywhere. They may be sufficient for most scenarios, except for more complex and highly regulated partner use cases. This year's research again focuses on evaluating AM capabilities for partner IAM user constituencies and demonstrates varying, but maturing, capabilities among AM vendors for partner IAM scenarios.

When evaluating AM tools for partner users:

- Determine the type of partner, and group each based on the level of maturity and the trust required to secure and govern partner access. Not all partners are equal; there will be major

differences between them based on their IAM maturity and the level of trust between host and partner.

- Evaluate AM tool capabilities based on the level of integration required by the partner and the host organization. Consider evaluating:
  - Extensive identity repository storage and flexible identity schema features for identity attributes storage, including their relationships and business roles.
  - Identity life cycle management through provisioning from a partner's system, JIT provisioning as part of federated SSO and self-service registration features for partner users.
  - Authentication of partner users including federated SSO and MFA with risk-based adaptive access.
  - Delegated administration, including multitiered delegation features to manage the identity life cycle of partner identities.
  - Access administration features, including an interface to request access to certain additional roles, access requests, tailored approval workflows and periodic access certifications.
  - Coarse-grained/fine-grained authorization and identity verification features applicable based on the type of relationship between the partner and the host organization.
- Evaluate best-of-breed partner IAM vendors/tools if your preferred vendor for other constituencies cannot meet your partner IAM requirements.

For more comprehensive guidance on partner IAM, please refer to Gartner research **Implementing Effective IAM Practices for B2B Partners**.

Access Management Is Foundational to Resilience

Access management is a critical part of an organization's cyber-resilience strategy. [3] Organizations use access management to significantly reduce their attack surfaces and limit damage from compromised credentials by controlling access to sensitive data and systems. Resilience means more than just preventing breaches, however; it includes the ways organizations operate during incidents and recover afterward. Robust access controls make organizations more resilient through minimized disruptions and the capability to isolate threats.

Access management tools include a variety of capabilities to increase resilience and improve security posture. These include the ability to produce canned reports of access events/risks, APIs that can export event data into analytics tools, and several threat detection and response mechanisms. These mechanisms can include:

- Threat detection methods, such as tactics, techniques and procedures (TTPs), user behavior analytics (UBA), and indicators of compromise (IOCs).

- Automated response actions embedded in tools (e.g., authentication, quarantining).
- Automated anomaly detection.

Knowledge of Pricing Models and Negotiation Tactics Is Crucial When Choosing a Vendor

Consider the License Model

The license models of AM tools for different user constituencies are:

- **Workforce AM use case:** AM tools are primarily sold on per named user pricing. A named user here means a standard business workforce/employee user stored in the identity repository of the AM tool and authenticating to the target app using the AM tool. However, some vendors offer their capabilities on the number of authentications through the AM tool type of license model, or a combination of number of named users and authentications.
- **Customer AM use case:** AM tools are primarily sold on a per active user type of pricing model for customer user constituencies. An active user here means a user who authenticates to the target app using the AM tool in a given time frame (monthly/yearly), not the entirety of the user base in AM tools' repository. Overall pricing is calculated based on monthly/yearly active usage for customer identities.
- **Partner AM use case:** Partner AM use case witnesses a mixed bag of pricing models. Some vendors practice named users, and some vendors practice an active user type of pricing model for partner identities. However, in most scenarios, it's the active user model that resonates more with end customers.
- **Machine AM use case:** Given the emerging nature of machine IAM capabilities, licensing models for machine AM tools are still highly variable. Licensing by machine account is common; however, some vendors license by machine identity (including when a given machine user has multiple accounts, it still counts as one identity for licensing purposes). Also, some vendors only offer full machine AM capabilities with purchase of their IGA product.

Second, from a delivery options perspective, a SaaS delivery option with subscription licensing is the norm for AM tools in the market today. Several AM vendors have stopped offering perpetual licensing for their products in the last five years and are selling software (if available) only on a subscription basis.

Negotiate Contract Terms Upfront

Ensure maximum uplifts. When negotiating SaaS or software subscription contracts, be aware of what may happen once the contract terminates. Gartner has noticed that special discounts granted for the duration of one contract will no longer be granted at the time of an extension, forcing an organization to pay significantly more to continue using the solution. Also, vendors tend to update their pricing models from time to time, and have in some cases forced organizations to renew their subscriptions at a rate that is unfavorable compared to the previous contract.

Negotiate maximum uplifts in the initial contract to cover the scenario when the current contract expires.

Acquire licenses needed for the current volume. Negotiations for a potential future license increase should be done upfront to take advantage of potential discounts for higher volume numbers as they happen and to limit uplifts when the contract is extended. Once a contract has been signed, and the base product has been deployed, the vendor's incentive to offer discounts for additional licenses is drastically reduced. Negotiate discounts on the basis of the length of the term. Three years has become the standard, but there are exceptions being accepted for shorter terms. Contracts longer than three years should only be considered if significant discounts are offered. Look for volume discounts on individual products based on term length, number of products bought, and volume for which the products are being bought to get effective pricing.

IAM leaders responsible for choosing an AM solution should use some additional negotiation strategies, including:

- **Leverage third-party advice:** This may include accessing the Gartner BuySmart application (see Note 1), a proposal review process and scheduling Gartner analyst inquiries, which should be done well before signing contracts. Contracts and proposals grow more complex every year. Vendors introduce new pricing, licensing models, maintenance options and audit clauses every day. Unless one has day-to-day market visibility, it is nearly impossible to keep up.

- **Review vendor packaging deals:** To address your AM requirements and get effective volume discounts on each product, look for pricing breakdowns for the individual products or modules you're buying. Be wary of "all-inclusive package pricing" that does not individually list the price for each component. It is virtually impossible to drop an unused component later on. Always consider the latest bundled packages, and do not just renew existing toolsets. Don't expect the vendor or value-added reseller (VAR) to suggest lower-cost or more-inclusive packages unprompted.

- **Start renewal negotiations early:** If negotiations are stuck, switching vendors and products may be an alternative, but only if there is enough time. Gartner recommends renewal negotiations should begin at least six months before the contract expiration date, and earlier for complex or larger installations. This will provide enough time for competitive bidding and migration planning, if desired. Late renewal negotiations shift the advantage to the incumbent vendor, because there is not enough time to evaluate switching to an alternative.

FIDO2 Passkeys

FIDO2 is an authentication protocol developed by the Fast Identity Online (FIDO) Alliance that uses public-key credentials, or passkeys, activated by a "gesture" such as a PIN or a local biometric authentication method. Passkeys enable robust passwordless authentication. The two types are device-bound passkeys and multidevice passkeys.

Device-bound passkeys are more suited to workforce authentication use cases and instances where strong customer authentication is required. Multidevice passkeys are more suited to customer authentication use cases as a robust alternative to passwords. (See the "Device-Bound Passkeys" and "Multidevice Passkeys" profiles in **Hype Cycle for Digital Identity, 2024** for a discussion of the pros and cons of each.)

While all vendors provide WebAuthn API support that enables FIDO2 authentication, support for passkeys differs in the following ways:

- As of November 2024, only RSA offers its own smartphone authenticator app supporting device-bound passkeys as a roaming authenticator. Microsoft now has this in public preview in its workforce offering. Thales enables device-bound passkeys for mobile app authentication in its CIAM offering. Microsoft and CyberArk can explicitly support integration with apps from third-party vendors such as HYPR.
- All vendors support device-bound passkeys in FIDO2 security keys and platform authenticators, including Windows Hello for Business, in at least their workforce offerings.
- Eight of the 10 vendors evaluated in this research can support multidevice passkeys in their workforce offerings; nine can do so in their CIAM offerings.
- Three of the 10 vendors evaluated can fully segregate the use of different passkey flavors in their workforce offerings; two can do so in their CIAM offerings. Four other vendors have more limited capabilities in their workforce offerings; six have limited capabilities in their CIAM offerings.

Market Overview

All vendors evaluated in this research offer a SaaS-delivered product. For vendors that offer multiple delivery models, only their SaaS product was reviewed for the Product/Service criterion. This Magic Quadrant was produced in response to market conditions for AM, including the following trends:

- **Mature workforce capabilities, but innovation is slowing —** The AM market is growing. The AM market growth and innovation is much higher for CIAM than for workforce. Gartner is seeing significant demand from client organizations moving away from homegrown CIAM products to commercial vendor solutions at a faster pace than in previous years.
- **New identity threat detection and response —** This year, AM vendors have significantly increased attack detection and response capabilities. AM vendors have focused their efforts on bolstering their security posture and reducing attack surfaces by adding new features.
- **Access management and resilience —** Access management is a critical part of organizations' cyber-resilience strategy. Organizations use access management to significantly reduce their attack surfaces and limit damage from compromised credentials by controlling access to sensitive data and systems. Resilience means more than just preventing breaches, however; it includes the ways organizations operate during incidents and recover afterward.

- **Thriving CIAM —** The 2023 Gartner IAM Modernization Preventing Identity First Security Survey reveals that 58% of respondents deployed workforce AM and 49% used CIAM solutions.1 Also, the Gartner survey suggested that CIAM is the third largest area for budget increases in 2024.

- **Maturing access management capabilities for machine users —** As organizations continue their move to the cloud and digital business transformation, the number of machine users (devices and, most significantly, workloads) continues to increase in support of many use cases. This increases the need for strong, sustainable access management capabilities for machine users over time.

- **Increased demand for access management capabilities for partner IAM users —** Business customers and partners now routinely use more digital services, conduct more complex and sensitive interactions, and otherwise engage more deeply with organizations online. Partner constituencies needing instant, secure and governed access to enterprise resources differ in IAM capabilities, levels of trust, relationship with the host organization and needed access, resulting in customized implementations lacking proper controls and agility.

- **FIDO2 passkeys —** FIDO2 is an authentication protocol developed by the FIDO Alliance that uses public-key credentials, or passkeys, activated by a "gesture" such as a PIN or a local biometric authentication method. Passkeys enable robust passwordless authentication. Multidevice passkeys are more suited to customer authentication use cases as a robust alternative to passwords.

Evidence

[1] **2023 Gartner IAM Modernization Preventing Identity First Security Survey.** 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] Top Trends in Cybersecurity for 2024, Security and risk management leaders face disruptions on multiple fronts: technological, organizational and human. Preparation and pragmatic execution are vital to address these disruptions and deliver an effective cybersecurity program.

[3] Verizon 2024 Data Breach Investigations Report, Verizon.

Note 1: Gartner BuySmart™

The Gartner BuySmart™ application helps guide you through technology evaluations with templates containing requirements and scorecards to help you select the best providers for your

needs. Using a connected workflow, BuySmart enables you to conduct thorough evaluations to invest confidently. See the BuySmart template designed for evaluating **Access Management**.

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.