Magic Quadrant for Access Management

11 November 2025 - ID G00826010 - 55 min read

By Brian Guthrie, Nathan Harris, and 2 more

Workforce AM vendors present unique and innovative features. CIAM vendors continue to offer differential capabilities for machine IAM support and enhanced capabilities to support complex CIAM and partner requirements. IAM leaders should focus on the features that differentiate vendors in this market.

Market Definition/Description

This document was republished on 11 November 2025. The version you are viewing is the corrected version. For more information, see Gartner's ***Corrections*** *page.*

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

AM's purpose is to give people (employees, consumers and other users) and machines access to protected applications in a streamlined and consistent way that enhances the user experience. For people, SSO is part of the enhanced experience. AM is also responsible for providing security controls to protect the user session during runtime. It enforces authentication and runtime 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 and SAML) and social logins to access standards-based applications and legacy applications (via proxies or agents)
- User authentication, including:
  - Support for phishing-resistant multifactor authentication (MFA) methods (e.g., X.509 and FIDO2) and other account takeover (ATO) protections
  - Controls to mitigate usage of compromised passwords
  - Protections against common MFA attacks, either directly or via out-of-the-box integration with third-party authentication services
  - Support for passwordless authentication methods
- Authorization policy definition and enforcement for any resources, such as applications and APIs, directly defined in the system
- Adaptive access based on dynamic evaluation of identity trust and access risk
- A directory or integrated identity repository, which includes identity synchronization services, for all constituencies
- Basic identity life cycle management, including support for enabling create, read, update and delete (CRUD) operations across all user types

Common Features

The common features for this market include:

- Identity threat detection and response (ITDR) functions, including out-of-the-box extended detection and response (XDR) integrations
- Journey-time orchestration and other low-code/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, consent management, personally identifiable information (PII) 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
- Continuous passive authentication, iterative authentication flows and other features, such as shared signals (e.g., Continuous Access Evaluation Profile [CAEP] and Risk & Incident Sharing and Collaboration [RISC]), that enable continuous adaptive trust (CAT)
- AM functions for machines (workloads, services, applications and agentic AI)
- Externalized authorization policy management and enforcement for entitlements in applications and services (aka fine-grained authorization), including the ability to control authorization via attribute-based access control (ABAC) and/or role-based access control (RBAC)

Magic Quadrant

Figure 1: Magic Quadrant for Access Management

Gartner

Vendor Strengths and Cautions

Alibaba Cloud

Alibaba Cloud is a Niche Player in this Magic Quadrant. It offers two AM products — IDaaS EIAM for workforce and IDaaS CIAM for customer identity access management. Alibaba Cloud supports all user constituencies. Alibaba Cloud's customer base is primarily in Greater China (China, Taiwan, Hong Kong) and the Middle East and Africa. Its primary industries include government, utilities and manufacturing.

It has recently added security capabilities for AI, including secure identity authentication for client-side AI agents, a newly designed administration console, and authentication for

machine access. Alibaba Cloud's recent roadmap updates include enabling API permission management for AI agents, authentication capabilities for IoT devices, and enhancing ITDR capabilities.

Strengths

- **Marketing strategy:** Alibaba Cloud's marketing strategy depends on strong regional brand recognition and strategic partnerships.
- **Innovation:** Alibaba Cloud has allocated a greater-than-average proportion of its business revenue to innovation, encompassing both product development and nontechnical initiatives within its strategic innovation plan.
- **Vertical strategy:** Alibaba Cloud offers strong regulatory compliance, scalability, industry-specific features, and proven success across multiple verticals within its main geolocation, making it attractive for organizations in highly regulated, high-volume and rapidly evolving markets.
- **Customer experience:** Alibaba Cloud's infrastructure supports mission-critical workloads, high availability and has a reputation for reliability. Customers benefit from rapid resource provisioning and autoscaling capabilities, enabling them to efficiently manage fluctuating workloads and business growth.

Cautions

- **Product:** Alibaba Cloud's IDaaS product offers limited global compliance certifications and regional data residency choices, which can create challenges for organizations with worldwide operations.
- **Geographic strategy:** Alibaba Cloud's global expansion is challenged by geopolitical risks and major competition from established North American AM providers. Potential customers should ensure that Alibaba Cloud can address international data privacy and regulatory compliance laws if outside its primary region.
- **Sales execution/pricing:** Alibaba Cloud offers complex pricing models with various product tiers; service fees and professional services fees are automatically added in. Base workforce and CIAM pricing tiers were below-average, compared with other AM vendors evaluated in this research. Potential customers could find it challenging to understand the total cost of ownership.

- **Market responsiveness:** Alibaba Cloud may prioritize the needs of its primary user base in local regions, potentially lagging in delivering enhancements and integrations, and capturing emerging trends specifically tailored to international customers.

CyberArk

CyberArk is a Challenger in this Magic Quadrant. As of July 2025, Palo Alto Networks has agreed to acquire CyberArk. It offers CyberArk Workforce Identity for workforce and CyberArk Customer Identity for CIAM. Both AM products are offered as SaaS, and can be purchased as a bundle or separately. No on-premises version is sold. CyberArk supports all user constituencies. Its customers are mainly in North America and Europe, and its primary industries include banking, insurance, and communications and media.

CyberArk has recently added workforce AI-powered ITDR and an administration assistant for workforce AM use cases, major enhancements to its CyberArk CORA AI model (built into its Identity Security Platform), and new product features to secure AI agents. CyberArk's recent roadmap updates include FIDO2-enabled end-to-end passwordless access, posture scoring based on multifactor authentication (MFA), and generative AI (GenAI) updates to its CORA AI framework.

Strengths

- **Product:** CyberArk has above-average capabilities for access control (including adaptive access), machine IAM capabilities, and delegated administration.
- **Innovation:** CyberArk has invested a higher-than-average percentage of revenue toward innovation, and its innovation plan includes product and nontechnical (CyberArk business process) enhancements.
- **Sales strategy:** CyberArk's sales strategy is supported by its strong partner ecosystem, vertical market expertise, and ongoing focus on customer success.
- **Customer experience:** CyberArk's customers benefit from a recently redesigned administration interface, accelerated customer onboarding features, and supplementary tools that improve and simplify administration tasks.

Cautions

- **Business model:** Following Palo Alto Networks' acquisition of CyberArk, changes in branding, sales channels, and go-to-market messaging may result in confusion for both

existing and prospective clients. Integration with Palo Alto Networks' existing security offerings may also introduce new complexity.

- **Market understanding:** CyberArk continues to influence its market understanding using its adjacent tooling, making it potentially less likely to adjust and respond to AM market emerging capabilities and product differentiators.
- **Market execution:** CyberArk has lower brand visibility for its access management solutions compared to its peers.
- **Sales execution:** Although CyberArk's standard workforce offering is priced competitively, its enterprise Workforce offering, which includes additional security controls, may present budgetary challenges for organizations seeking a cost-effective solution.

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. Entrust supports all user constituencies. Its customers are mainly in North America, Europe and Latin America. Entrust's primary industries include banking, hospitality and healthcare.

Entrust recently added phishing-resistant AI/ML, validation and presentation for OpenID for Verifiable Credentials (OID4VC) and ISO 18013-5 verifiable credentials, as well as authentication enhancements that allow for phishing-resistant biometric authentication with passkeys. Entrust's recent roadmap updates include enhancements to CIAM capabilities for customer and partner onboarding user flows, authentication flows, and a self-service portal for account management.

Strengths

- **Sales strategy:** Entrust tailors its sales strategy to address vertical-specific challenges, such as regulated verticals, compliance, and fraud prevention.
- **Market understanding:** Entrust's market intelligence is strongly aligned with AM market realities, including a clear view of its strengths, weaknesses, opportunities, and threats in the market.
- **Marketing strategy:** Entrust leverages its broad portfolio, including Identity Verification, to offer comprehensive, integrated solutions for customers, allowing it to cross-sell and

bundle its products.

- **Market responsiveness:** Entrust has responded positively to market demands. Examples of this include its first authentication journey orchestration for CIAM use cases, identity verification deepfake detection and enhancements to its Entrust Identity App, which now supports device-bound passkeys.

Cautions

- **Geographic strategy:** Entrust's direct sales, partner networks and service infrastructure are mainly located in North America, Europe and Latin America. Therefore, organizations in other parts of the world should carefully assess Entrust's geographical strategy to ensure alignment with their global deployment and compliance needs.
- **Viability:** Entrust does not have the same global market share as larger AM providers, impacting its availability of third-party integrations, community support and partner resources.
- **Marketing execution:** Entrust has lower AM visibility and reduced brand recognition in the global space.
- **Product:** Entrust provides connectors for legacy systems; however, some organizations may encounter challenges when attempting deep customization or integration with highly custom or outdated applications.

IBM

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

IBM recently added enhanced phishing-resistant authentication for nonbrowser flows, third-party adapter creation for provisioning use cases, and expanded risk signal sharing. IBM's recent roadmap updates include login enhancements to support advanced analytics and updates to simplify the administrative console.

Strengths

- **Sales strategy:** IBM competes effectively in the AM market from a sales strategy built on global brand strength, large customer base, vertical specialization, and partner

ecosystem.

- **Market responsiveness:** IBM has introduced new features such as enhanced multifactor authentication options, improved user experience for self-service registration, and expanded support for social login providers, demonstrating responsiveness to evolving customer needs and security trends.
- **Product:** IBM has strong product capabilities for identity data, profile and life cycle management (for both workforce and customer); partner management and delegated administration, orchestration and extensibility; and service resilience.
- **Innovation:** IBM has a robust near-term and long-term innovation plan, combined with higher-than-average innovation investment for the AM market that is strongly market-aligned.

Cautions

- **Marketing strategy:** IBM's extensive security portfolio can infrequently dilute or obscure the specific value proposition of its AM platform. As a result, potential customers focused on AM solutions or evaluations may be less likely to understand how IBM's AM offering is relevant to them.
- **Customer experience:** IBM's complex user journeys for CIAM can be time-consuming. Organizations may find themselves planning for additional training, support and resources to mitigate potential delays during implementation. However, IBM mitigates this challenge by offering its orchestration engine at no cost, enabling low-code creation of user journeys to streamline deployment and reduce overhead.
- **Business model:** IBM's reliance on long-term contracts and enterprise-level commitments may limit flexibility for organizations seeking agile, consumption-based pricing or the ability to scale services up and down in response to changing business needs.
- **Sales execution:** IBM has augmented its sales execution to also include a select coverage model, product-led growth, and an expanded partner ecosystem to make IBM Verify more accessible and scalable. Organizations of all sizes should carefully assess whether these changes fully address their specific requirements and support needs before adoption.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Microsoft offers Microsoft Entra ID for workforce and Microsoft Entra External ID for CIAM, and both are offered as SaaS. Microsoft supports all user constituencies, and it has a global customer base within all evaluated industries.

Microsoft recently added Microsoft Entra Agent ID and Agent Registry, enabling control and visibility for AI agents and AI-based development tools to create highly customized user flows in External ID. Microsoft's recent roadmap updates include a Conditional Access optimization agent to detect policy coverage gaps, an access package analyzer to simplify workforce access modeling and changes, and automation for manual CIAM migrations.

Strengths

- **Sales strategy:** Microsoft's AM offerings benefit from its most popular products by bundling its AM offering with widely used Microsoft products, making AM less expensive to acquire relative to its competitors.
- **Geographic strategy:** Microsoft's AM offering excels in geographic strategy through its global infrastructure, localized partner ecosystem, and scalable architecture, enabling organizations to support workforce and customer identities across diverse regions and regulatory compliance.
- **Viability:** Microsoft demonstrates exceptional viability due to its financial strength, global infrastructure, security leadership, compliance coverage, and its commitment to ongoing enhancements.
- **Product:** Microsoft's security products remain a strong differentiator due to its generative AI features, machine access management support, and robust AM capabilities for both workforce and CIAM — including identity life cycle management, authentication, and adaptive access.

Cautions

- **Customer experience:** While integration with Microsoft services is seamless, connecting with third-party or legacy applications may require additional effort and technical resources.
- **Business model:** Microsoft tends to bundle its products and offer discounts that could lead to vendor-lock in and high reliance, making it difficult and costly to migrate to alternative AM solutions.

- **Marketing strategy:** Microsoft positions its AM solution as an integrated component of its comprehensive security platform. While this approach emphasizes the advantages of a unified security ecosystem, it can make it difficult for prospective customers to clearly identify and assess the unique capabilities, features and differentiators specific to Microsoft's AM solution.
- **Product:** Microsoft Entra ID does not have granular visual user journey orchestration capabilities, but offers extensibility points on the authentication flow, as well as platform-native authentication APIs to customize the desired user journey.

Okta

Okta is a Leader in this Magic Quadrant. It offers multiple SaaS-delivered AM products, across workforce, customer and nonhuman identity use cases. No on-premises version is available. Okta supports all user constituencies, and has a global customer base within almost all evaluated industries.

Okta recently added enhanced management of agentic AI, prebuilt orchestration workflows, and device-bound single sign-on. Okta's recent roadmap updates include advancing risk detection and response across users and devices, enhancing verifiable digital credentials management capabilities, and increasing account takeover detection.

Strengths

- **Sales strategy:** Okta's sales strategy strengths include its global market recognition, strong partner ecosystem, and unique customer onboarding processes.
- **Vertical strategy:** Okta offers prebuilt integrations and customizable workflows tailored to many different verticals, enabling organizations to address the unique needs and regulatory requirements of diverse industries.
- **Product:** Okta delivers a set of AM products that have above-average capability for all constituencies, and it excels in supporting application development scenarios.
- **Marketing execution:** Okta's marketing initiatives are not only thorough in their coverage of product features, but also carefully aligned with evolving market trends and customer needs.

Cautions

- **Operations:** Okta's net-new customer growth in 2025 was lower than some peers included in this research. This dynamic reflects both intensified competition from established and emerging AM vendors, as well as a trend among organizations to deepen adoption with existing providers by expanding into broader identity capabilities.
- **Sales execution/pricing:** Okta offers both a-la-carte and bundled pricing models, which may lead to contract renewal restructuring conversations and additional questions from net-new customers to help them select the pricing model aligned with their current business requirements.
- **Product strategy:** Okta does not yet natively support W3C verifiable credentials, though this is on its roadmap. Its identity verification is delivered through standards-based integrations embedded into native flows, rather than a proprietary solution — an approach that may not suit customers seeking a single-vendor option.
- **Marketing strategy:** Okta's marketing emphasizes broad applicability, rapid deployment and ease of use. Prospective customers should still evaluate the full scope of product ownership to ensure alignment with their specific requirements and implementation complexity.

One Identity

One Identity is a Niche Player in this Magic Quadrant. Its AM solution, OneLogin, is built on One Identity's cloud infrastructure, and is offered as a SaaS-only solution. No on-premises version is available. It can be purchased as a bundled product or sold separately. One Identity supports all user constituencies. Its customers are mainly in North America and Europe, and within banking, communications and media, and services.

One Identity has regional and dedicated OneLogin deployments, AI-enhanced preauthorized risk scoring for authentication (dynamic authorization), and phishing-resistant authentication factors to all users across all devices. One Identity's recent roadmap updates include enhanced security capabilities for AI, including secure identity authentication for client-side agents; increased ITDR capabilities; and support of identity authentication capabilities for IoT devices.

Strengths

- **Marketing strategy:** One Identity's marketing strategy is well-aligned with current market needs and emphasizes the company and product's strengths, including AM market

expertise and its product offerings in adjacent IAM markets.

- **Sales execution:** One Identity positions its AM solution as part of an overall unified suite. This integrated approach enables the sales team to address a broad range of customer needs, cross-sell, and drive larger, multisolution deals.
- **Market understanding:** One Identity demonstrates stronger-than-average market understanding, including full consideration for all market drivers (security, compliance, user experience, cost/ease of implementation and support).
- **Vertical/industry strategy:** One Identity's ongoing regional investments and localized delivery capabilities support its ability to serve organizations in different geographic and cultural contexts, resulting in a large customer base and strong partnerships.

Cautions

- **Market responsiveness:** One Identity's slower response to integrating emerging features and market responsiveness may erode its competitive position in the AM market.
- **Product:** One Identity's authorization and adaptive access, portable and decentralized identity, and API access control is average when compared to other AM vendors evaluated in this research.
- **Marketing execution:** One Identity has less market visibility and less name awareness compared to other AM vendors evaluated in this research, particularly in regions or verticals where competitors have established stronger brand equity.
- **Customer experience:** One Identity's workflows configuration can be complex, particularly for organizations without prior experience in AM or those with limited in-house technical expertise.

OpenText

OpenText is a Niche Player in this Magic Quadrant. OpenText's AM product, OpenText Access Manager (formerly known as NetIQ Access Manager), is offered as a SaaS or on-premises. It can be bundled or purchased in individual modules. OpenText supports all user constituencies. Its customers are mainly in North America and Europe, and are primarily in banking, government, and healthcare.

OpenText's recently enhanced its access gateway as a service and enhanced authentication and authorization events risk scores, as well as its UX user interface for both administrators

and CIAM experiences (used for workflow, behavioral and development enhancements) to be consistent with the user experience across the broader OpenText product portfolio. OpenText's recent roadmap updates include embedding reverse proxy access gateway features into its SaaS offering (a capability that to date has only been available to on-premises deployments), updates to its Process Automation Workflow Service feature, and a newly redesigned software development community platform.

Strengths

- **Viability:** OpenText AM is offered as part of a broader suite of security and information management solutions, allowing seamless integration with other OpenText products and third-party applications.
- **Market understanding:** OpenText targets messaging for verticals such as healthcare, financial services, and government, highlighting features and benefits that resonate with the unique operational and regulatory demands of these industries.
- **Customer experience:** OpenText delivers flexible, secure, and user-centric experiences through automated features, adaptive authentication, and strong privacy controls. These strengths contribute to higher user satisfaction, increased trust, and improved customer retention.
- **Product:** OpenText's product set is above-average in the market for identity data, progressive profiling, life cycle management for workforce, and highly flexible directory service, making OpenText a forward-thinking AM vendor.

Cautions

- **Marketing strategy:** OpenText faces difficulties in achieving strong brand recognition, resulting in continuous adaptation and adjustments in its messaging and branding strategies to distinguish itself in the highly competitive AM landscape.
- **Pricing:** OpenText's pricing demonstrates inconsistency across various scenarios examined in this research, with costs for small and midsize deployments exceeding the average for the AM market.
- **Operations:** OpenText's SaaS version does not hold key compliance certifications, including FedRAMP and SOC 2.
- **Geographic strategy:** OpenText's SaaS version does not currently provide flexible data residency options or data storage locations. Failure to address data sovereignty concerns

can restrict market access.

Ping Identity

Ping Identity is a Leader in this Magic Quadrant. The Ping Identity Platform offers single-tenant and multitenant multi-SaaS solutions for customer, workforce, partner, and machine identities. Ping also continues to invest in innovation and maintenance of software AM tools for customers that prefer or require a self-managed AM solution. Ping Identity supports all user constituencies. Its customer base is global, but mainly in North America and Europe, with customers in multiple industries.

Ping Identity has recently added security capabilities for AI, including secure identity authentication for client-side agents, enhanced ITDR capabilities, and authentication capabilities supporting IoT devices. Ping Identity's recent roadmap updates include enriching B2B features, enhancing delegated administration functions, and enhancing impersonation threat mitigation capabilities.

Strengths

- **Product:** Ping Identity's product capabilities are above-average for all user constituencies covered in this research. Its strengths include partner management, delegated administration, portable and decentralized identity, orchestration and extensibility, API access control, and machine access management.
- **Market understanding:** Ping Identity has demonstrated exceptional performance within highly regulated markets, delivering solutions tailored to banking and financial markets, including deepfake protection measures, as well as protection against sophisticated identity fraud attacks and impersonation threats.
- **Marketing strategy:** Ping Identity has substantially invested both time and money in its marketing strategy this year, resulting in strong market intelligence and a clear understanding of its product positioning.
- **Customer experience:** Ping Identity has enhanced customer experience through personalized journeys and customer engagements.

Cautions

- **Business model:** Ping Identity has traditionally concentrated on serving midsize to large enterprises, which may lead to a perception that it cannot serve small business needs.

- **Geographic strategy:** Ping Identity's customer base is primarily concentrated in North America and Europe. While the company is expanding its presence in APAC and South America, sales coverage in these regions may not be as extensive as in its core markets.
- **Market responsiveness:** Since the acquisition of ForgeRock, organizations should be aware of potential challenges in Ping Identity's ability to maintain its historically agile market responsiveness.
- **Sales execution/pricing:** Ping Identity's pricing across multiple scenarios assessed in this research is above market averages, particularly for workforce and partner use cases, when compared to other vendors.

RSA

RSA is a Niche Player in this Magic Quadrant. Its AM portfolio is branded under ID Plus, which is offered as a SaaS, on-premises, or hybrid solution for both workforce and CIAM. RSA supports all user constituencies except machines. Its customer base is concentrated in North America, Europe, and Asia, primarily in the banking, securities, insurance, and government sectors.

RSA recently introduced unified passwordless access, enhancements to its posture management features, and receiver/transmitter shared signal service supporting CAEP. RSA's recent roadmap updates include expanding use of AI and machine learning to support automated access decisions; life cycle administration and threat detection; and enhancing onboarding features and credential recovery capabilities.

Strengths

- **Customer experience:** RSA offers an enhanced interface that simplifies use for both end users and administrators, potentially providing higher customer satisfaction and reduced friction during login and account management processes.
- **Sales strategy:** RSA benefits from a sales strategy rooted in a strong partner ecosystem, cross-selling opportunities and multichannel support.
- **Vertical strategy:** RSA has extensive experience serving highly regulated industries such as financial services, healthcare, government and critical infrastructure.
- **Market understanding:** RSA demonstrates a strong understanding of the drivers and unique considerations for workforce AM use cases, but it is below-average for CIAM

capabilities.

Cautions

- **Business model:** RSA should leverage its brand equity in regulated sectors, invest in vertical customization, and modernize its delivery to capture new growth opportunities.
- **Product:** RSA's product capabilities are not as strong as most vendors in this research. Specifically, its capabilities are below-average for authorization and API access control, and very limited for portable and decentralized identity
- **Operations:** RSA has recently realigned its go-to-market model, which could introduce transitional risks as new structures and leadership are established.
- **Marketing execution:** RSA is primarily recognized for its authentication solutions; its overall brand awareness as an AM vendor covering all user constituencies is less than the other AM vendors included in this research.

Thales

Thales Group is a Visionary in this Magic Quadrant. Thales offers two AM products: OneWelcome Identity Platform for customers and partners, 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 supports all user constituencies. Thales' primary customer population is in North America and Europe, in banking, securities and insurance, manufacturing, and government.

Thales recently added the European Union's Cybersecurity Certification Scheme for Cloud Services (EUCS) certification, allowing for enhanced sovereignty-focused CIAM features for European regions, ITDR for partner IAM, and a new FIDO passkey management system. Thales' recent roadmap updates include fine-grained authorization (FGA) policy orchestration, enhancements, and improved hygiene management capabilities using GenAI-powered assistants.

Strengths

- **Market understanding:** Thales has demonstrated an understanding of the distinct requirements and regulatory complexities that characterize the AM market within the European Union. This experience has benefited it in helping customers in navigating EU-specific mandates such as GDPR, eIDAS, and sectoral compliance standards.

- **Innovation:** Thales' strengths in innovation are reflected in its adaptive authentication, biometric verification, and real-time risk-based assessment controls for fraud prevention and account takeover (ATO) protection.
- **Customer experience:** Thales has a strong focus for its customers within regulated industries, offering specialized compliance support and integration expertise for complex environments.
- **Product:** Thales' product capabilities are excellent for partner management and delegated administration, as well as for identity data, profile, and life cycle management for customers and partners, including numerous national identity providers and other verifiable credentials.

Cautions

- **Sales execution/pricing:** Thales' complex pricing structure is based on user volumes, deployment models (cloud, on-premises, hybrid), and feature sets. Lack of transparent pricing or unclear cost breakdowns can deter prospects, especially when compared to competitors offering straightforward subscription models.
- **Business model:** Certain compliance or data residency features may be available only in specific regions or as add-ons, potentially increasing costs for multinational organizations with diverse regulatory requirements.
- **Product:** Thales' current product offering has below-average capabilities for machine access management, and for authorization and adaptive access capabilities for workforce.
- **Vertical/industry strategy:** Thales lacks some certifications required by certain regulated sectors, such as FedRAMP for U.S. federal government agencies. Organizations operating in this sector should conduct thorough due diligence to ensure that Thales meets all necessary certification standards.

Transmit Security

Transmit Security is a Leader in this Magic Quadrant. Transmit Security's AM platform, Mosaic, is available as a SaaS only; no on-premises version is available. Mosaic modules can be purchased as a bundle or sold separately. Mosaic supports all user constituencies, but the majority of Transmit Security's customers are CIAM and partner identity and access

management (PIAM). Transmit Security's primary customer population is in North America in banking, security and insurance.

Transmit Security recently added predictive AI to preemptively detect and block anomalous identity behavior from agentic or autonomous actors, enhanced threat detection and response workspace, as well as AI-augmented application logic orchestration. Transmit Security's recent roadmap updates include support for digital wallets, verifiable credentials, a third-party integration marketplace, predictive AI for synthetic identity detection, fine-grained authorization via RBAC, and a no-code orchestration builder that empowers business users to create secure identity journeys.

Strengths

- **Product:** Transmit Security's product capabilities are above-average in passwordless authentication, adaptive authentication, orchestration, ITDR and native fraud detection, making it well-suited for regulated and high-assurance environments.
- **Customer experience:** Transmit Security offers a strong overall customer experience, including passwordless authentication and streamlined digital identity journeys.
- **Marketing execution:** Transmit Security's go-to-market approach for Mosaic leverages a combination of direct sales, channel partnerships and strategic alliances.
- **Sales execution/pricing:** Transmit Security has one of the highest sales efficiency ratios of all AM vendors evaluated. It offers clear, straightforward bundled pricing models, enabling organizations to accurately forecast costs.

Cautions

- **Geographic strategy:** While Transmit Security maintains a more focused geographic field presence than some peers, global organizations should validate its fit for their specific requirements.
- **Marketing strategy:** Transmit Security primarily focuses on large and extra-large enterprises. This emphasis on its marketing strategy often leads small and midsize businesses to consider alternative AM vendors that offer solutions better-suited to their scale, operational simplicity, and cost considerations.
- **Vertical/industry strategy:** Transmit Security has established expertise in financial services and is expanding into other regulated industries such as telecom, retail, and

transportation. Clients should carefully assess whether the platform meets their specific compliance requirements to ensure regulatory alignment and avoid potential gaps.

- **Business model:** Transmit Security's business model is primarily focused on CIAM. However, the company also offers a limited workforce AM solution, delivering a reduced suite of core features compared to the AM vendors evaluated in this research.

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

- Alibaba Cloud
- Transmit Security

Inclusion and Exclusion Criteria

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

To qualify for inclusion, vendors need to:

- 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 $65 million from AM products and subscriptions (inclusive of maintenance revenue but excluding professional services revenue) in FY25.

Or:

- At least 1,100 current AM customers as of 21 May 2025.
    - 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, primarily delivered as a SaaS product, but can be also delivered as software:

- Single sign-on (SSO) and session management with support for standard identity protocols (OpenID Connect, OAuth 2.0., and SAML) and social logins for accessing standards-based and legacy apps (via proxies or agents).
- User authentication, including support for phishing-resistant and other 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:

- 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) 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**).
- Identity verification (IDV). The purpose of IDV is to establish confidence in the real-world identity of a person during a digital interaction when curated credentials do not exist, are not available or do not provide sufficient assurance (see **Magic Quadrant for Identity Verification**).
- 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 and **Market Guide for Endpoint Management Tools**).

- Cloud access security brokers (CASB). CASB, now essential elements of cloud security strategies, help security and risk management leaders to discover cloud services and assess cloud risk. They identify and protect sensitive information, detect and mitigate threats, and institute effective cloud governance and compliance (**see How to Protect Your Clouds with CSPM, CWPP, CNAPP and CASB**).

Honorable Mentions

Cisco Duo Security: Duo Security was acquired by Cisco in 2018. It provides a SaaS-based solution for runtime AM controls, including Directory (IdP), MFA, SSO, adaptive access authentication, and device health checks. Its platform helps organizations verify user identities and device trust before granting access to applications, supporting both cloud and on-premises environments. Recently, Duo has fortified its offering with posture management ISPM and ITDR functionality, additional options for phishing-resistant MFA, and identity verification workflows. Duo enables organizations to enhance security and meet compliance requirements. Duo was not included in this Magic Quadrant due to not meeting technical requirements before the inclusion deadline.

Descope: Descope primarily supports CIAM, PIAM and agentic IAM use cases. It offers authentication, authorization and user management capabilities. Descope's developer-first platform enables businesses to easily add secure, passwordless authentication and identity workflows to applications, AI agents and MCP servers. Key CIAM and PIAM features include multifactor authentication, social login, SSO, journey-time orchestration, user life cycle management, delegated administration, and compliance. Agentic IAM features include MCP server authorization, token management and policy-based access control. Descope provides APIs, SDKs, and no-code/low-code tools to simplify integration into web apps, mobile apps, and AI/MCP systems. Descope was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

Exostar: Exostar specializes in access management for highly regulated industries. Its cloud-based platform offers identity verification, authentication, SSO, user life cycle management, and access governance, enabling secure collaboration internally and externally with partners and suppliers. Exostar's solutions are certified by Kantara as a full-service CSP that meets strict security and compliance standards, including MFA, risk-based access controls, and regulations like NIST, CMMC, FedRAMP, and HIPAA. Exostar's PKI solutions are cross-certified

with the Federal Bridge Certificate Authority. Exostar was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

Fortinet: Fortinet's access management solutions are delivered through FortiAuthenticator and FortiToken. FortiAuthenticator offers centralized authentication, SSO and MFA integration for secure network and application access. FortiToken provides hardware and mobile tokens for MFA, strengthening user verification. These products help organizations enforce access controls, manage identities, and meet compliance across on-premises and cloud environments, and integrate with Fortinet's broader security ecosystem. Fortinet was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

Google: Google's access management system is delivered through its Identity Platform. It offers authentication options (password, passwordless, social, and enterprise logins), multifactor authentication, and centralized user management. The platform is highly scalable, supports millions of users, and provides APIs and SDKs for easy integration. It also helps organizations meet security and privacy compliance requirements, enabling secure and seamless customer identity experiences for web and mobile applications. Google was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

Imprivata: Imprivata's access management system, primarily through Imprivata Enterprise Access Management, is designed for mission-critical industries such as healthcare, manufacturing and government. Imprivata offers SSO and secure authentication for heterogeneous IT environments using proximity cards, passkeys, biometrics, or passwords. Imprivata also provides mobile access management, access analytics, and clinical workflows for enhanced security, usability, and efficiency. Imprivata supports compliance with healthcare regulations like HIPAA and EPCS, enhancing both security and operational efficiency for healthcare and other organizations. Imprivata was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

Keycloak: Keycloak is an open-source access management product built by the contributors to the open-source project. The open-source version is not supported and is only available directly from Keycloak's GitHub. Additionally, a fully supported version is available and supported by Red Hat directly. It provides authentication, authorization, and user management for web and mobile applications. Key features include SSO, support for passwordless, social, and enterprise logins (SAML, OpenID Connect), user federation with

Lightweight Directory Access Protocol (LDAP) and Active Directory, role-based access control, and MFA. Keycloak also allows customizable login flows and branding. It is widely used for secure and scalable access management across cloud and on-premises environments, making it a popular choice for organizations seeking flexible AM solutions. Keycloak was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement. *Keycloak did not participate in requests to review the draft contents of this document. Gartner's analysis is therefore based on other credible sources.*

Salesforce: Salesforce features MFA, SSO, and auditing tools that enhance security and compliance. Its system ensures only authorized users access sensitive information, supporting data protection, regulatory compliance, and operational efficiency. Regular reviews and best practices, such as least-privilege access, help mitigate risks and maintain robust access controls across the organization. Salesforce was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

SAP: SAP Business Technology Platform (BTP) provides robust identity and access management for customers, offering secure registration, modern authentication options, and consent management while ensuring privacy and regulatory compliance. SAP CIAM manages customer access to applications and APIs, integrates with SAP and non-SAP platforms, and scales to millions of users, delivering analytics on user behavior and security events. SAP Cloud Identity Services enables SSO, authentication, provisioning and authorization for secure data access. SAP was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

SecureAuth: SecureAuth features AI/ML-driven adaptive MFA, SSO, and passwordless authentication for enhanced security and user experience across all workforce, customer and agentic AI IAM use cases. The system provides real-time identity governance and security analytics, and supports on-premises, air-gapped, hybrid and SaaS deployment models. SecureAuth helps organizations comply with regulations like GDPR and HIPAA by offering robust audit trails and reporting. SecureAuth was not included in this Magic Quadrant due to not meeting the business inclusion criteria requirement.

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: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following 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: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Financial health

Success in AM market by AM revenue and customer population

Sales Execution/Pricing: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

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: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

General responsiveness to market trends and competitor activities over the last 12 months — new features added

Track record (roadmap items from 2024 that were delivered in the past 12 months)

Marketing Execution: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Marketing activities and messaging executed in the last 12 months

Marketing execution — ROI, cost per win, conversion rate, marketing metrics

Customer Experience: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Customer relationship and services

Professional services

Customer satisfaction

Operations: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

People

Processes

Organizational changes

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 September 2025	

Source: Gartner (November 2025)

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: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Competitors

Strengths and weaknesses

Market opportunities

Threats

Marketing Strategy: Customers cannot buy products that they do not know about. We evaluated specific product marketing metrics, not corporate marketing. We looked 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. We also looked at the following subcriteria:

Marketing strategy and brand awareness

Customer sentiment

Sales Strategy: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Deal strategies

Sales organization and partnerships

Revenue breakdown by channel

Program for internal sales enablement

Offering (Product) Strategy: We considered how the vendor will increase the competitive differentiation of its AM products and services through product engineering, product management and overall product strategy. We also evaluated the following subcriteria:

Product roadmap

Differentiation

Business Model: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

General business models

Core purpose and aspirations in this market

Vertical/Industry Strategy: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following subcriteria:

Customer breakdown by industry

Trends in customer industry breakdown

Strategy for verticals and other segmentation

Other segmentations like midmarket and service providers

Innovation: We considered 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 focused on technical and nontechnical innovations introduced since last year, as well as the vendor's future innovations over the next 18 months. We also evaluated the following subcriteria:

Near-term innovations related to trends (18 months)

Longer-term innovation (18+ months)

Geographic Strategy: In addition to the criteria outlined in the Evaluation Criteria Definitions section below, we evaluated the following 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

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High

Evaluation Criteria	*Weighting*
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High

Source: Gartner (November 2025)

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

The goal of any Magic Quadrant is to provide a level view of comparable vendors to address the demands of a wide variety of buyers. Not every company's requirements are identical. We encourage clients to review the accompanying Critical Capabilities research to review use case and functionality requirements, and this research to align industry expertise, vision, technology and cost requirements to the right vendor, regardless of the vendor's dot position within the Magic Quadrant.

AM's purpose is to give people and machines access to protected applications in a streamlined and consistent way. AM is also responsible for providing security controls to protect the user session during runtime. It enforces authentication and runtime authorization using adaptive access. Lastly, AM can provide identity context for other cybersecurity tools and reliant applications to enable identity-first security.

This year, CIAM is the primary contributor to the growth of the AM market. Gartner is seeing a significant increase in demand from client organizations moving from existing home grown CIAM platforms to a commercial/modern solution. According to the worldwide security

software revenue market share for 2024 (**Market Share: Security Software, Worldwide, 2024**), the AM market totaled $6.851 million (an increase of 14.2% from 2023).

AM for workforce (employees): AM empowers employees to securely and efficiently access workplace applications and systems in a user-friendly manner. By reducing login friction, lowering risk levels, and supporting self-service, these solutions contribute to a more productive, compliant, and secure work environment. With SSO enabled, employees use one set of credentials to access multiple platforms, minimizing password fatigue and login hassles while improving overall efficiency. Robust authentication protocols, such as MFA, protect employee accounts from unauthorized access and cyberthreats, safeguarding personal and organizational data. In summary, workforce access management is essential for protecting sensitive enterprise assets, enabling operational efficiency, ensuring regulatory compliance, and fostering a secure and productive work environment.

AM for CIAM (customer identity): CIAM is designed to support millions of users. CIAM systems ensure reliable and high-performing access during peak usage periods, enhancing customer satisfaction. CIAM is essential for organizations seeking to secure customer identities, deliver seamless digital experiences, comply with regulations, and leverage identity data for business growth. CIAM solutions implement robust authentication mechanisms such as MFA and adaptive risk-based controls, protecting customer accounts from fraud and unauthorized access. CIAM drives customer trust, satisfaction and operational efficiency. CIAM focuses on securely managing customer identities, authentication, authorization and profile data across digital channels. CIAM platforms enable customers to control their personal data and consent preferences, helping organizations comply with privacy regulations such as GDPR and CCPA. In summary, CIAM delivers secure, seamless and privacy-compliant digital experiences for customers.

AM for partners: Partner access management empowers organizations to securely extend access to their digital ecosystem — including applications, data, and resources — to external partners such as suppliers, distributors, and service providers. By leveraging modern identity standards like SAML, OAuth 2.0, and OpenID Connect, individuals and organizations can facilitate seamless federated authentication and single sign-on for partner users, reducing friction while maintaining strong security postures. Delegated administration capabilities allow partner organizations to manage their own user accounts and permissions within defined boundaries, streamlining onboarding and ongoing management. Robust access controls, including granular role-based access and adaptive authentication, ensure that partners only interact with resources relevant to their business relationship, thereby

minimizing risk and supporting regulatory compliance. Additionally, advanced consent and privacy management features help organizations meet data protection requirements and foster trust with external stakeholders. Ultimately, partner access management in CIAM delivers a balanced approach that enhances security, simplifies compliance and optimizes user experience for all participants in the extended digital ecosystem.

Several AM vendors have made significant advancements to their platforms, focusing on bolstering security, streamlining automation and elevating user experiences. Notable new features include emergent AI-related capabilities that enable more intelligent and proactive threat detection, as well as risk-based authentication and adaptive access controls that dynamically respond to evolving risk profiles. Vendors are also leveraging AI assistants and natural language processing to deliver more intuitive and seamless user interactions, further enhancing the overall user experience. In response to the growing complexity of digital ecosystems, AM solutions now offer robust mechanisms for securing machine identities and AI agents, ensuring that both human and nonhuman actors are governed effectively. AI-powered analytics and insights provide deeper visibility into access patterns, enabling organizations to make data-driven decisions and respond swiftly to potential threats. Additionally, the introduction of custom workflows through user journey orchestration allows for tailored access processes that align with unique business requirements, driving operational efficiency and agility. Collectively, these innovations position AM vendors at the forefront of identity and access management, empowering organizations to address modern security challenges, reduce administrative overhead and deliver superior digital experiences.

Negotiating with access management vendors requires a strategic, informed, and methodical approach to ensure your organization secures the best value, functionality, and support for its investment. The best way to negotiate with access management vendors is to approach the process with thorough preparation, clear requirements, and competitive leverage. Focus on total cost, service quality, compliance, and future scalability, while carefully reviewing contract terms and maintaining the ability to switch vendors if needed. Strategic negotiation not only secures favorable pricing and features, but also establishes a strong foundation for a long-term, value-driven partnership.

To ensure the AM vendor is right for your organization, consider a proof of concept (POC). A POC is a critical step when evaluating access management vendors, allowing organizations to validate a solution’s capabilities, compatibility and performance in a controlled environment before making a full commitment. The best approach to POCs for access

management vendors should be structured, measurable and collaborative. Provide clear objectives, focus on key use cases, engage stakeholders, replicate real-world conditions, and measure outcomes rigorously. Collaboration with vendors and end-user feedback are essential for validating both technical and operational fit. A well-executed POC reduces risk, clarifies vendor capabilities, and empowers organizations to make informed, confident decisions.

AM vendors participating in this research presented a range of pricing models and scenarios, reflecting the diversity and flexibility required to address varying organizational needs and deployment environments. These models typically include subscription-based licensing, usage-based pricing, tiered feature packages and enterprise agreements. However, it is important to note that not all qualified vendors disclosed detailed pricing information. In instances where vendors opted not to provide comprehensive pricing data, Gartner conducted a rigorous analysis, leveraging supporting data to quantify and validate pricing scenarios. Furthermore, for the vendors who disclosed detailed pricing information, Gartner conducted a comparative analysis, conducted high-level pricing reviews, and documented where each vendor's pricing positioned them relative to their peers — whether at market, above market, or below market rates. This benchmarking allowed Gartner to assess the competitiveness and value proposition of each solution in the context of industry standards.

Market Overview

The access management (AM) market is undergoing a period of rapid and profound transformation, driven by evolving business requirements, technological advancements, and escalating cybersecurity risks. AM vendors are no longer limited to providing basic authentication and authorization services; instead, they are broadening their portfolios to include sophisticated features such as adaptive access controls, AI-driven threat detection, and zero-trust security frameworks. These next-generation capabilities are engineered to address the unique challenges posed by distributed workforces, multicloud infrastructures, and increasingly dynamic user roles, thereby ensuring secure, frictionless access to corporate resources across diverse environments.

The proliferation of remote work and hybrid workplace models has fundamentally altered the risk landscape, necessitating more granular and context-aware access management solutions. Adaptive access controls leverage real-time risk analytics and behavioral

biometrics to dynamically adjust user privileges based on factors such as device posture, geolocation, and transaction context. Meanwhile, AI-driven threat detection systems utilize machine learning algorithms to identify anomalous access patterns and proactively mitigate potential breaches.

As regulatory requirements such as GDPR, CCPA, and emerging global data protection laws continue to tighten, organizations face mounting pressure to adhere to local and regional compliance laws. The complexity of managing access across multicloud environments, third-party integrations, and diverse user populations further underscores the need for unified, scalable AM solutions.

Strategic partnerships and mergers and acquisitions are accelerating innovation in this space, with leading vendors integrating capabilities such as passwordless authentication, identity orchestration, and consent management to deliver seamless, end-to-end user journeys. Furthermore, AM vendors are increasingly delivering unified platforms that cater to both workforce and CIAM use cases, enabling organizations to streamline identity life cycle management, enhance user experiences, and centralize consoles.

As digital transformation initiatives become a top priority for organizations worldwide, the ability to deliver secure, scalable, and user-centric access management is emerging as a key differentiator in the market. Industry analysts predict sustained growth in both workforce IAM and CIAM segments, fueled by the need for resilient security architectures, improved user engagement, and regulatory alignment within an increasingly complex digital ecosystem. The global AM market is expected to reach $24.1 billion by 2027, with CIAM solutions accounting for a significant share of this growth as enterprises seek to balance security, privacy and convenience in their digital interactions.

In summary, the AM market is at an inflection point, characterized by rapid innovation, heightened regulatory scrutiny, and a strategic shift toward integrated, intelligent access management solutions. Organizations that invest in advanced AM technologies will be better positioned to mitigate emerging cyberthreats, achieve regulatory compliance and deliver superior user experiences in a digital-first world.

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

Passwordless authentication: Widespread adoption of passwordless solutions — such as biometrics, FIDO2, and device-based authentication — which reduces friction, improves

security, and enhances user experience.

Adaptive and risk-based access controls: AM systems increasingly leverage real-time behavioral analytics and contextual data to dynamically adjust authentication requirements, balancing security and convenience.

Unified workforce, customer and partner IAM platforms: Organizations are consolidating AM, CIAM and partner into unified platforms for streamlined management, consistent policies, and improved visibility across all user types.

Cloud-native and hybrid deployments: Cloud-native architectures dominate, with hybrid deployment options supporting legacy integration, scalability and global accessibility.

Decentralized identity and verifiable credentials: Decentralized identity models (e.g., self-sovereign identity, blockchain-based credentials) gain traction for privacy, portability and user control.

Enhanced privacy and consent management: AM platforms are embedding robust privacy controls, consent management, and compliance features to address global regulations (GDPR, CCPA, etc.); however, this is covered in a separate Gartner market.

AI-driven threat detection and response: Artificial intelligence and machine learning are used to detect anomalous behaviors, automate threat response, and continuously improve security posture.

Seamless omnichannel experience: AM solutions focus on delivering consistent, frictionless authentication and access across web, mobile, IoT, and emerging digital channels.

API-first and developer-centric approaches: Vendors prioritize API-first architectures and developer friendly tools to accelerate integration, customization, and time-to-value.

Identity orchestration and automation: Automated workflows for onboarding, provisioning, and life cycle management reduce manual effort and improve efficiency.

Stronger integration with zero-trust architectures: AM vendors have increased zero-trust strategies. Moving to zero trust is moving from implicit trust to explicit trust, including enforcing least privilege, continuous verification, and segmentation across enterprise environments.

Focus on accessibility and inclusive design: AM platforms are improving accessibility features to ensure secure and convenient access for all users, including those with

disabilities.

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

FIDO2: The FIDO2 standard, developed by the FIDO Alliance and W3C, enables passwordless authentication with strong phishing protection by using public key cryptography and device-based passkeys. It supports both platform-bound and roaming passkeys, allowing users to securely access accounts through biometrics, hardware tokens, or PINs, eliminating traditional password vulnerabilities. By adopting FIDO2 passkeys, organizations can enhance security, user experience, and regulatory compliance while supporting zero-trust security models in modern enterprise and cloud environments.

⊕ Evidence

⊕ Evaluation Criteria Definitions