Magic Quadrant pour la gestion des accès

1 novembre 2022 - ID G00761397 - 58

Par **et 3 autres**Henrique Teixeira, Données Abhyuday,

La FA joue un rôle de plus en plus central dans les stratégies IAM des organisations et constitue désormais une cible de choix pour les attaquants. Les menaces modernes et les contraintes économiques exigent une FA plus résiliente et rentable. La détection et la réponse aux menaces d'identité, la convergence IAM et la résilience gagneront en importance en 2023.

Hypothèse de planification stratégique

D'ici 2026, 90 % des organisations utiliseront un type de fonction intégrée de détection et de réponse aux menaces d'identité à partir d'outils de gestion des accès comme principal moyen d'atténuer les attaques d'identité, contre moins de 20 % aujourd'hui.

Définition/description du marché

La vision du marché de Gartner est axée sur les technologies ou approches transformationnelles répondant aux besoins futurs des utilisateurs finaux. Il n'est pas axé sur le marché tel qu'il est aujourd'hui.

Gartner définit la gestion des accès (FA) comme des outils qui établissent, appliquent et gèrent les contrôles d'accès au temps de parcours vers le cloud, les applications Web modernes basées sur des normes et les applications Web héritées. Ils peuvent être utilisés par :

- Utilisateurs de la main-d'œuvre dans les cas d'utilisation d'entreprise à employé (B2E), y compris, mais sans s'y limiter :
  - Salariés
  - Travailleurs temporaires
  - Sous-traitants
  - Entrepreneurs
- Utilisateurs externes dans les cas d'utilisation d'entreprise à consommateur (B2C), d'entreprise à entreprise (B2B), de gouvernement à citoyen (G2C) et d'économie à la demande, y compris,

mais sans s’y limiter:

- Consommateur
- Partenaires
- Citoyens
- Contingent talent freelance

Les fonctionnalités de base fournies par les outils de FA sont les suivantes :

- Services d’annuaire
- Administration des accès internes (c.-à-d. intégration des utilisateurs, approvisionnement, gestion des mots de passe, fonctions de gestion des profils)
- Administration des accès externes (c.-à-d. inscription des utilisateurs, gestion des profils, administration déléguée, intégration BYOI et capacités de gestion des consentements)
- Outils de développement
- Autorisation et accès adaptatif
- Authentification unique et gestion des sessions
- Authentification de l’utilisateur
- Contrôle d’accès aux API
- Rapports

En option, les outils de FA peuvent également fournir des fonctionnalités pour :

- Gestion des identités des machines
- Fonctionnalités avancées de gestion du cycle de vie
- Profilage progressif
- Orchestration des temps de parcours dans le contexte de la gestion des accès
- Autres interfaces low-code/no-code pour la création de flux d’authentification dynamique complexes et d’autorisations affinées

Le modèle de livraison le plus courant pour la FA est via SaaS ; cependant, certains fournisseurs proposent également des déploiements fournis par logiciel ou appliance.

Prisée

Nous commentons les prix des produits individuels en fonction d'une échelle relative, en utilisant des termes tels que « bien au-dessus de la moyenne », « au-dessus de la moyenne », « moyen », « inférieur à la moyenne » et « bien en dessous de la moyenne ».La moyenne pour une composante de tarification particulière fait référence à la note moyenne de tous les fournisseurs évalués dans cette recherche pour une variété de scénarios de tarification AM différents.

Résilience

La plupart des fournisseurs de FA fournissent des SLA pour que la disponibilité de leurs services SaaS soit d'au moins 99,99%. Nous avons mis en évidence les fournisseurs qui ne le font pas par mise en garde.

Cas d'utilisation internes et externes de la FA

Par souci de concision et de clarté, nous appelons « CIAM » tous les cas d'utilisation externes de la FA (consommateurs, partenaires, fournisseurs, citoyens et talents indépendants occasionnels en B2C, B2B, G2C ou gig economy). De même, les cas d'utilisation internes de la FA (employés, travailleurs temporaires, sous-traitants et sous-traitants dans les cas d'utilisation B2E) sont simplement appelés « main-d'œuvre ».

Orchestration

Toutes les fonctionnalités de la solution d'orchestration du temps de parcours décrites dans Innovation Insight: Journey-Time Orchestration attigates Fraud Risk and Deliver Better UX sont simplement appelées « orchestration », par souci de brièveté. D'autres types d'orchestration, lorsqu'ils existent (tels que les workflows au moment de l'administration), sont appelés comme tels.

Magic Quadrant

Figure 1 : Magic Quadrant pour la gestion des accès

Source : Gartner (novembre 2022)

Forces et mises en garde des fournisseurs

CyberArk

CyberArk est un leader dans ce Magic Quadrant. Son produit CyberArk Identity est livré en mode SaaS et vendu sous forme de modules individuels ou sous forme d'offres groupées récemment introduites pour la sécurité des employés et des terminaux.Les opérations de CyberArk sont géographiquement diversifiées et la plupart des clients de CyberArk Identity sont des petites et moyennes entreprises qui utilisent ses produits pour des scénarios de main-d'œuvre.

Parmi les innovations récentes en matière de produits, citons une fonction d'enregistrement de session avec isolation et réauthentification des processus pour les sessions à haut risque, un outil de gestion de mots de passe pour le personnel (basé sur son coffre-fort de gestion des comptes privilégiés [PAM]) et des outils de développement de gestion de l'identité des clients (CIAM). CyberArk prévoit d'investir jusqu'à 29 % de son chiffre d'affaires dans la R&D, dont une partie est axée sur l'ajout de plus de détection et de réponse aux menaces d'identité (ITDR) avec des capacités de réponse automatisée et d'intégration de playbook et l'amélioration de la

réauthentification pour les sessions à haut risque. Le fournisseur prévoit également d'ajouter davantage de capacités IAM convergentes à son produit de FA.

Forces

- CyberArk a fait preuve d'une bonne réactivité sur le marché et de ses antécédents, en fournissant de nombreuses fonctionnalités prévues qui figuraient sur sa feuille de route, telles que la réauthentification pour les sessions à haut risque et les améliorations de la sécurité des sessions.
- CyberArk Identity a obtenu un score supérieur à la moyenne pour sa capacité à s'intégrer aux applications standard, ainsi que pour ses fonctionnalités d'authentification.
- CyberArk bénéficie d'une stratégie de vente qui tire parti de sa base installée PAM. Son produit de FA peut être un bon choix pour les clients qui cherchent à combiner les avantages de l'intégration de la FA avec le portefeuille plus large de CyberArk PAM, tels que l'enregistrement de session sécurisé avec isolation des processus.
- CyberArk démontre une compréhension supérieure à la moyenne du marché des tendances en matière de cybersécurité et a ajouté des éléments tels que l'ITDR, la convergence IAM, la sécurité axée sur l'identité et la sécurité DevOps à ses plans de feuille de route.

Cautions

- Though CyberArk introduced new product bundles last year, simplifying its pricing model, the prices for several scenarios evaluated in this research are well above average for workforce and complex CIAM scenarios.
- CyberArk's AM installed base is smaller than many of the other Leaders in this research, scoring lowest in overall viability.
- Aside from a good market understanding, and having mentioned ITDR and IAM convergence plans, many of CyberArk's roadmap items are not AM focused, but instead relate to its greater PAM business and other adjacent areas.
- CyberArk has not demonstrated good traction of its AM product with CIAM, developer use cases or larger clients. CyberArk Identity innovations for CIAM and developer use cases are catching up with the market, and the solution scores below average for developer tools and ease of deployment. CyberArk Identity does not support progressive profiling or granular consent management, and requires programming with APIs even for basic external identity administration use cases.

ForgeRock

ForgeRock is a Leader in this Magic Quadrant. ForgeRock's AM products are sold on a stand-alone basis and in bundles, delivered as SaaS (ForgeRock Identity Cloud) or software (ForgeRock Identity Platform). Its operations are geographically diversified and its clients tend to be larger organizations, mostly in the banking, communications, and government sectors. Most of

ForgeRock's AM clients use its software product, broadly across workforce and CIAM use cases. Most ForgeRock AM SaaS clients use its products for CIAM.

Recent product innovations included adding some ITDR capabilities to its Trees orchestration tool, and improvements to B2B2C CIAM features, such as advanced delegation, B2B2C orchestration, dynamic branding, new visual journey configuration interfaces and SaaS resilience improvements. ForgeRock plans to invest 25% of its revenue in R&D to ramp up SaaS IAM convergence, continue to enhance developer tools and CIAM performance. The vendor also plans to add more adaptive signals to its AM tool from endpoint security and its own identity governance and administration (IGA) tool, and launch a marketplace for orchestration flows and integrations.

Strengths

- ForgeRock obtained the highest score in this research for its offering (product) strategy. The roadmap items described above address many of the pressing needs of AM buyers.
- It also received one of the highest scores for its product capabilities, including strong SDK offerings, APIs and documentation, support for hosting customer pages and containers (Docker, Kubernetes). The product offers a good balance in features for internal and CIAM as well as developer use cases.
- ForgeRock has demonstrated strong market responsiveness. Its recent innovations differentiate it from its competitors, including improvements to its orchestration capabilities, new B2B2C CIAM features and resilience improvements for SaaS.
- ForgeRock has a strong marketing strategy for its new user and entity behavior analytics (UEBA) capabilities, autonomous access (ITDR) and "never login again" (passwordless) campaign. Its customer success organization has nearly doubled in size since January 2021.

Cautions

- ForgeRock received the lowest score for geographic strategy among all vendors. Although its operations are geographically diversified, the installed base is heavily concentrated in the U.S. and Europe. ForgeRock also has the smallest customer count among Leaders in this research.
- Even though ForgeRock pricing is competitive for very large CIAM use cases, its pricing is above average for all the other scenarios evaluated in this research.
- ForgeRock has scored below average in its product's AM reporting capabilities. Obtaining analytics insights about runtime data is complex. Generating reports is not intuitive, and requires exporting JSON files.
- While ForgeRock does work with the leading MSSPs, ForgeRock is very focused on their strategic alliance with Accenture, which may be a consideration for customers who typically leverage other popular MSSPs.

IBM

IBM is a Visionary in this Magic Quadrant. Its AM products are offered as software (IBM Security Verify Access) and SaaS (IBM Security Verify). IBM Security Verify is a converged IAM platform focused on an integrated approach with other IBM Security products. IBM's operations are geographically diversified and its clients tend to be large organizations, mostly in the banking and public sector industries. Most of IBM's clients use its software version of the product. Both the software and SaaS products are used broadly across workforce and CIAM use cases.

Recent product innovations include an enhanced webhook framework for integration with third-party multifactor authentication (MFA) vendors and additional ITDR capabilities. IBM plans to invest in simplifying integration of legacy applications, adding more CIAM capabilities for trusted delegation and decentralized identity (DCI) services.

Strengths

- IBM offers good value; for the series of scenarios evaluated in this research, its prices are consistently lower than its competitors'.
- IBM demonstrates strong market understanding, structuring marketing campaigns on solving both foundation and advanced IAM problems, leaning on its extensive security and IAM product portfolio to make the case that it is the best vendor to do so.
- IBM Security Verify is FAPI-CIBA certified, which is important for financial institutions. IBM has constructed a privacy portal in Verify specifically for data privacy officers, which is useful for CIAM use cases.
- IBM's SaaS product offers good developer tools, private and multicloud deployment options and native OpenShift integration, which can be a convenient solution for Red Hat developers. IBM Verify SaaS is included by default in all OpenShift contracts, as well as in IBM Cloud Paks for Security and Automation.

Cautions

- IBM has a solid list of features on its roadmap and has delivered some ITDR functions like credential stuffing and login anomaly alerts. However, it has failed to deliver on several items from last year, such as DCI services, and has offered no precise date for when those plans will be delivered.
- IBM's vision is influenced by meeting the demands of its largest clients, and is focused on its bigger IBM Security portfolio, instead of AM market trends. This may lead to AM product decisions that are not always useful to other consumers, and a lack of focus on AM innovation.
- IBM is not a popular choice among small to midsize enterprises, and based on Gartner client inquiry, interest in the IBM product continues to decline.
- IBM scored below average for customer experience, and Gartner clients describe a steep learning curve to implement and support its products. As last year, it has no 99.99% SLA option for availability (it stops at 99.9% as of the date of this survey).

Micro Focus

Micro Focus is a Niche Player in this Magic Quadrant. Its NetIQ Access Manager is sold as software, and there are additional SaaS modules for single sign-on (SSO), MFA, IGA and gateway services. The vendor's operations are geographically diversified, and clients tend to be large organizations in manufacturing, banking and the public sector. The vast majority of Micro Focus AM clients use its software product broadly across workforce and CIAM use cases.

Recent product innovations include enhancements to its adaptive access management capabilities, a common reporting service and new options for BYOI with government identities. In August 2022 Micro Focus entered an agreement to be acquired by OpenText. The vendor plans to invest 22% of its revenue in R&D in order to add identity proofing and identity administration to its SaaS modules, extend its adaptive access functions and enhance other adjacent IAM and cybersecurity products.

Strengths

- Micro Focus continues to be a good fit for larger organizations and for addressing more complex hybrid use cases, especially for organizations that need the flexibility of managing on-premises or hosted deployments.
- Micro Focus obtained above average scores in nonstandard application enablement due to its deployment flexibility. NetIQ AM supports Docker, Kubernetes and OpenShift. All AM modules are available as containers that support Docker/Kubernetes deployments, Amazon EKS and Microsoft Azure AKS.
- Micro Focus scored above average for its product capabilities in BYOI integration and added government identities as a very interesting differentiator.
- The pricing for the NetIQ AM software offering is below the market average. The SaaS product modules, on the other hand, are priced among the highest in this Magic Quadrant.

Cautions

- Micro Focus's overall ability to execute score is lower than last year. The vendor scored the lowest in sales execution, marketing execution, market responsiveness and track record. It failed to deliver many of last year's roadmap plans, like SaaS versions of its remaining AM features, privacy controls and analytics. Based on Gartner client inquiry, interest in the Micro Focus product continues to decline.
- Micro Focus obtained the lowest score in offering (product) strategy. Aside from plans to add more adaptive risk features and to launch more adjacent and converged SaaS IAM services, all other plans are mostly either catching up or not specific to AM.
- Micro Focus obtained the lowest score in market understanding, sales strategy and business model among all vendors evaluated in this report. Micro Focus is a large global vendor with a

very large software portfolio, so its focus on marketing and selling AM is not the same as that of the other players in this Magic Quadrant.
- NetIQ Access Manager is still not cloud native. The SaaS modules offered are not sufficient to address the use cases evaluated in this Magic Quadrant. Most advanced features will require the software to be installed on-premises or hosted in cloud infrastructure (IaaS).

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its Azure AD product is a SaaS-delivered converged IAM platform, sold as part of a rebranded IAM product family named Microsoft Entra that also includes CIEM and DCI services. The vendor's operations are geographically diversified and its clients vary in size and industry. Most Microsoft clients use its products for workforce scenarios.

Recent product innovations include improved session management controls with continuous access evaluation (CAE) for Microsoft apps, some ITDR capabilities, delegated administration and scalability improvements. Microsoft plans to invest 10% of its security revenue into R&D in order to launch a DCI and verifiable claims service (called Microsoft Entra Verified ID), life cycle management enhancements, Azure AD cross-tenant management and other adjacent IAM features.

Strengths

- Microsoft demonstrates a very strong ability to execute, obtaining the highest scores among all vendors in overall viability, sales execution/pricing, market responsiveness and track record. Microsoft has grown its installed base to more than 500,000 paid customers, and has established itself as the market share leader for workforce AM.

- Microsoft shows a strong vision, obtaining the highest scores among all vendors in market understanding, sales strategy, business model and geographic strategy. Microsoft Entra is a core piece of its cybersecurity strategy, which is tightly integrated with its successful Office and Microsoft 365 sales motions.

- Microsoft has continued to be a leader in promoting DCI, making it one of the three core capabilities for Microsoft Entra, which is a bold bet on the future of DCI-centric identity approaches.

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

Cautions

- Microsoft Azure AD suffered impactful outages during the evaluated time frame of this research. Its resilience roadmap plans revolve around Microsoft-controlled features, like fault isolation, and there is no support for a hybrid deployment model for failover.

- Despite substantial investments in security R&D, Microsoft's AM product capabilities still lag behind other Leaders in this research, especially in CIAM. For developers, Microsoft offers

Graph APIs and MSAL SDKs; however low-code approaches require using a separate tool (Microsoft's Power Platform). Its SDKs (MSAL and Graph) are also more limited than those of competing products, requiring more steps to achieve the same results.
- Large rebrand exercises like Entra tend to create confusion about what features and functionalities exist in the product. That confusion is apparent from Gartner client inquiries.

- Recent innovations, like CAE, are deliberately cloud-first, but are exclusive to first-party apps, a similar Microsoft-centric approach that has been used for initial rollout of features like this.

Okta

Okta is a Leader in this Magic Quadrant. It offers Okta Identity Cloud as a SaaS-delivered converged IAM platform broadly used across both workforce and CIAM use cases. Okta also sells the Auth0 Platform, a SaaS product commercialized for CIAM and developer use cases. Okta's operations are geographically diversified and the majority of its clients tend to be small to midsize organizations.

Recent product innovations include Auth0's private cloud deployment option on Azure, some ITDR functions, and sign-in services with Ethereum via partnership with Spruce. Okta Identity Cloud has added new passwordless security capabilities, custom admin roles and IGA features. Okta plans to invest 36% of its revenue into R&D in order to add marketing analytics, more ITDR features and fine-grained authorization in Auth0. Plans also include some ITDR functions and continuous authentication, as well other new and enhanced converged IAM features in the Okta Identity Cloud roadmap.

Strengths
- Okta demonstrates the strongest ability to execute among all vendors in this Magic Quadrant. Okta has established itself as the market share leader for CIAM use cases and has the second largest market share in the industry for workforce AM.

- Okta obtained the highest score among all vendors for its product capabilities. Okta offers some converged IAM functionality with one of the best workflow tools for access administration, as well as market leading SSO and analytics capabilities. It offers a long list of capabilities for CIAM in both Okta and Auth0 products, and one of the best combinations of developer tools for both offerings.

- Okta received the highest score for customer experience in this Magic Quadrant. Okta's track record for reliability and availability is very strong, and it has added ITDR capabilities to Auth0 (leaked password detection, reset stolen passwords, enhanced bot detection). Gartner clients have mentioned Okta Identity Cloud's ease of use and flexibility in integrating with a broad number of apps.

- Okta scored highest in marketing execution. Okta's "loginless" campaign and its approach of being a neutral and open vendor are differentiating.

Cautions

- Pricing continues to be well above average, and Gartner clients have consistently mentioned the high cost of Okta's solution.

- The Auth0 integration with Okta is taking longer than expected by Gartner. Okta is still selling two competing CIAM products at the time of this publication. Application developers also have a confusing combination of tools to choose from two platforms.

- Multiple priorities between the two lines of products are also affecting other areas of the company, causing delays in roadmap items and generating some duplicate effort, with separate ITDR plans for Okta and Auth0, for example.

- Okta demonstrates lower maturity in incident response communication than expected. Okta suffered a breach in January 2022. The impact of the breach to customers was revealed to be minimal. However, the communications from Okta during the incident were less than effective, in terms of proactiveness, transparency and accountability.

One Identity (OneLogin)

One Identity (OneLogin) is a Challenger in this Magic Quadrant. OneLogin was acquired in October 2021 by One Identity, a vendor with mature PAM and IGA tools. OneLogin is a SaaS-delivered AM product with converged lightweight identity administration features. One Identity (OneLogin) operations are geographically diversified and its clients vary in size and industry. Most One Identity (OneLogin) clients use its products for workforce scenarios.

Recent product innovations include OpenID Connect (OIDC) enhancements, MFA extensibility features, identity life cycle management enhancements and a user password migration tool. One Identity (OneLogin) plans to invest 20% of its revenue into R&D to add native signals from One Identity PAM and IGA tools, along with other third-party products. One Identity (OneLogin) also plans to add resilience capabilities (like DR between clouds) and DCI services, as well as to enhance endpoint MFA capabilities.

Strengths

- One Identity (OneLogin) received above average scores for its product capabilities, and with the addition of migration hooks this year it has also scored the highest among all vendors for ease of deployment.

- One Identity (OneLogin) received one of the highest customer experience scores in this research. Gartner customers have mentioned the ease of management and administration, integration and deployment of One Identity (OneLogin)'s solution.

- The OneLogin product has potential to improve One Identity's overall presence in the IAM market. OneLogin benefits from a modern architecture and good service development life cycle that could influence other lines of business within the vendor to modernize their IGA and PAM products and integrate roadmaps.

- One Identity (OneLogin) continues to offer competitive pricing for CIAM use cases. However, see the first caution below for workforce scenarios.

Cautions

- The OneLogin product has a history of being a good option for cost benefit, but pricing evaluated for a series of workforce use case scenarios is now marginally above market averages.
- One Identity (OneLogin)'s overall completeness of vision scored lower than last year, receiving below-average scores for innovation and market understanding. Improvements in life cycle management are late to the market.
- One Identity (OneLogin) has improved its product capabilities, but it still scores below average for API access control and nonstandard application enablement when compared to other vendors in this Magic Quadrant. It also lacks CIAM features like consent management.
- The success of the merger between One Identity and OneLogin will depend on how well both people and products will work together, as well as the integration's impact on innovation in its overall completeness of vision.

Oracle

Oracle is a Niche Player in this Magic Quadrant. Its products are offered as software (Oracle Access Manager [OAM]) and SaaS (Oracle Cloud Infrastructure Identity and Access Management [OCI IAM]) options. OCI IAM is focused on an integrated approach for AM and other Oracle cloud products and applications, delivering AM capabilities to existing Oracle customers. Its operations are geographically diversified and its clients vary in size and industry. Most Oracle clients use its on-premises AM product, for workforce use cases.

Recent product innovations include deeper integration of Oracle's SaaS AM product with Oracle Cloud, resilience enhancements with cross-region DR and an adaptive risk microservice. Oracle plans to add cross-region HA with failover, and ramp up converged IAM capabilities into OCI IAM.

Strengths

- Pricing for Oracle's SaaS AM product is well below the market average for the series of pricing scenarios evaluated in this research.
- OCI IAM runs on Oracle's cloud data centers, and it has added cross-region DR to all OCI global regions where there is a second in-country region, or where laws enable data to move to another specific region. This could be a differentiator for customers looking to run AM as SaaS in other clouds not provided by Amazon Web Services (AWS), Azure or Google.
- Oracle has a very large installed base for its database and apps (over 400,000 customers). Its marketing strategy is largely focused on targeting these existing customers and promoting its IAM tools on the strength of Oracle apps, making it easier for current users of Oracle applications to use their IAM tools.
- Oracle has an extensive global presence for operations and services, making it easier to acquire AM products in regions where other AM vendors are not present.

Cautions

- Oracle has obtained the lowest score among all vendors for its product capabilities. Many standard administrative tasks are too complex to be configured within the tool. SDKs available are very basic, and only enable authentication. Oracle offers no low-code approach for developers, integration with third-party apps or integrated PaaS approaches.

- Oracle obtained the lowest score in customer experience. Gartner clients have cited the lack of improvements in OAM, and that support is getting more expensive. In addition, while Oracle offers current customers the option to migrate to OCI IAM, Gartner inquiries do not show many clients taking that path.

- Oracle scored the lowest in innovation, marketing strategy and vertical/industry strategy. Aside from the cross-domain DR feature, other enhancements presented in OAM and OCI IAM were mostly catching up or only relevant to OCI clients. Examples include Identity Domains (for OCI users using IAM services) and Adaptive Risk microservices.

- Oracle provides only a service-level objective (SLO) of 99.95% for its SaaS product, not a full SLA. That makes Oracle the only vendor in this Magic Quadrant not to offer an SLA.

Ping Identity

Ping Identity is a Leader for this Magic Quadrant. Its AM products are sold under the PingOne Cloud Platform in several bundles and modules as multitenant SaaS, single-tenant SaaS (PingOne Advanced Services), and software. Its operations are geographically diversified and its clients tend to be large organizations using both on-premises and cloud deployments at similar proportions, broadly across internal and CIAM use cases.

Recent product innovations include the launch of its orchestration tool (PingOne DaVinci), online fraud detection (PingOne Fraud) and DCI functions with verifiable credentials. Ping Identity was acquired by Thoma Bravo in August 2022. It plans to invest 23% of its revenue into R&D to create a marketplace for technology integrations with PingOne DaVinci, add multicloud options and active-active resilience, including SaaS to on-premises failover. The vendor also plans to ramp up IAM convergence, make DCI improvements and introduce some ITDR capabilities.

Strengths

- Ping Identity demonstrates the strongest completeness of vision among all vendors in this Magic Quadrant. It obtained the highest score for innovation, launching several new features to its platform, and its roadmap is one of the most robust among vendors in this research.

- Ping Identity got the highest score for operations due to its strength in coverage for large enterprises and complex environments and its strong hybrid and multicloud approach, as it works to solidify its significant presence in these types of organizations.

- It received one of the highest scores for its product capabilities and customer experience, offering the only AM converged solution in this Magic Quadrant with identity proofing,

orchestration, DCI and fraud detection capabilities. It also scored above average for its fine-grained authorization, adaptive access, API access control and CIAM features.
- Ping Identity demonstrates its vision through promotion with its popular celebrity marketing campaigns. The campaigns highlight the core functions of its AM solution and many of its newly acquired products. For this reason, Ping Identity received the highest score for marketing strategy.

Cautions

- Even though Ping Identity's pricing for workforce is competitive and below the market average, the introduction of new bundles has resulted in scenarios in which its solution for CIAM use cases is priced above the market average.
- Ping Identity is not popular with small to midsize enterprises, and its ease of use score is average when compared to other vendors.
- Although it has added adjacent features, like identity proofing and fraud detection, and has a roadmap to invest in greater IAM convergence, Ping Identity lacks embedded IGA or PAM capabilities.
- Ping Identity scored below average for its developer tools. Deploying mobile apps takes more steps than its closest competitors', and the software and SaaS products require very different approaches.

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

No vendors were added to this Magic Quadrant.

Dropped

- **Auth0:** Auth0 is no longer included as a discrete vendor in this Magic Quadrant, as it has been functioning as a product unit within Okta since last year.
- **Ilantus:** Ilantus offers its Compact Identity product, delivering AM as part of a converged SaaS-delivered IAM platform that also includes IGA capabilities, for small to midsize organizations globally, with many of its clients in the Asia/Pacific region. However, it has not been included in this Magic Quadrant due to not meeting the overall inclusion criteria; Ilantus markets its AM module to support only workforce 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.

- **Thales:** Thales offers SafeNet Trusted Access (STA) as SaaS and SafeNet Authentication Service as software, with separate modules for hardware tokens and smart cards. Thales acquired OneWelcome in July 2022. OneWelcome itself was the result of a merger of two European CIAM specialists, iWelcome and Onegini, in July 2021. Thales has not been included in this Magic Quadrant due to not meeting the technical inclusion criteria at the time of the research cutoff date, but would meet the inclusion criteria after the acquisition is completed.

Inclusion and Exclusion Criteria

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

To qualify for inclusion, vendors need to:

- Have marketed and sold products and services in their FY21 to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) 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 $50 million from AM products and subscriptions (inclusive of maintenance revenue, but excluding professional services revenue) in FY21.

  - At least 950 current AM customers as of 6 June 2022. 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 the following 10 functional requirements:

- **Directory services:** Must provide at minimum a directory or identity repository for internal and external users, including identity synchronization services and outbound SCIM support.

- **Internal access administration:** Basic life cycle management capabilities with AD sync, SCIM (outbound) provisioning capabilities and a workforce launchpad of applications or application gallery for single sign-on.
- **External access administration:** Include ways to invite and register external users, and provide interfaces for managing permissions of delegated administration, as well as basic consent-based flows. User consent should exist at an attribute level before importing data to an AM tool directory. The products or solutions must provide BYOI integration to use public identities, such as social media at least, for identity federation and access control. Core functionality also includes using sign-up and sign-in, linking social media identities to AM customers' established user identities and setting access policy based on the use of social media identities.
- **Developer tools**: Support modern identity protocols (OpenID Connect, OAuth 2.0, SCIM) and interfaces, (APIs, SDKs) that are externally accessible to developers to build authentication, authorization and user management flows.
- **Authorization and adaptive access:** Include capabilities to implement authorization decisions and enforcement, create policy and provide sources of stored and contextual data used to evaluate risk and dynamically render access decisions. Provide native support for modern authorization protocols like OAuth 2.0.
- **Single sign-on (SSO) and session management:** Session management must include capabilities and granularity, according to which the AM tool can control session state for user-present interactions with applications. The AM tool should also be able to control the ability to manage session times by issuing and refreshing time-limited access tokens (or cookies), and the ability to terminate sessions. It must provide, at minimum, a global setting for session management and single logout.
- **User authentication**: Must support SAML and OIDC, and provide different user authentication methods, including MFA and SSO. Minimal MFA requirements should include out-of-band SMS, one-time password (OTP) apps, mobile push and support for OTP hardware tokens. The solution should also provide support for at least two of the following methods:
  - X.509
  - FIDO hardware and software tokens
  - device-native and third-party biometrics
  - passwordless authentication
  - continuous authentication
- **API access control:** Must offer an OAuth 2.0 authorization server, which supports and implements consent, handles scope-to-claim mappings and can issue customizable and self-

contained JSON web tokens to web servers, mobile apps, modern web apps and services used to access API targets.

- **Standard and nonstandard application enablement:** Include capabilities to enable access, authentication and SSO to both modern apps and legacy applications that do not support modern identity protocols, using technologies like proxy services, agents or other mechanisms.

- **Analytics and reporting:** Include at minimum descriptive, historical information about all administration and access events. The products or solutions must offer reporting and APIs to export event data for analysis by external analytics and security information and event management (SIEM) tools, or consumption by the solution's own adaptive risk engine.

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

- AM products that cannot support, or are not marketed to support, both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases. For example, solutions without substantial customer numbers for each use case, 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 and/or privileged access management (for more information on this market, see Magic Quadrant for Privileged Access Management).

- Remote or on-premises "managed" AM; that is, services designed to take over management of customers' owned or hosted access management products, rather than being provided by delivery of the vendor's own intellectual property.

- AM functions provided only as part of a broader infrastructure or business process outsourcing agreement. AM must be provided as an independently available and priced product or service offering.

- AM products that are only or predominantly provided as open-source offerings.

- Stand-alone IGA suites, which are full-featured IGA products that offer the complete range of IGA functionality, without embedded AM capabilities. This is a separate but related market covered by other Gartner research (see Market Guide for Identity Governance and Administration).

- Full-life-cycle API management. This is a separate but adjacent market covered by other Gartner research (see Magic Quadrant for Full Life Cycle 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 Magic Quadrant for Unified Endpoint Management Tools).
- Cloud access security brokers (CASB), which represent a separate but related market covered by other Gartner research (see Magic Quadrant for Cloud Access Security Brokers).

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

- New revenue threshold of $50 million in annual revenue or 950 or more current AM customers as of 6 June 2022.
- More specific requirements about outbound SCIM provisioning and developer tools.
- More specific requirements for internal and external access administration.

Honorable Mentions

Vendors Covering All Assessed AM Use Cases

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

Fortinet: Fortinet offers its AM product as a software/appliance (FortiAuthenticator), which provides centralized authentication services for the Fortinet Security Fabric, including single sign-on services, certificate management, and guest management with temporary accounts. Fortinet also offers a SaaS product (FortiTrust Identity), which offers user authentication (including MFA and passwordless approaches), SSO and self-service portals. Fortinet was not included due to not meeting the technical inclusion criteria.

Imprivata: Imprivata offers a number of IAM services, primarily in the healthcare vertical, where it is well-known for its “tap and go” authentication approach using proximity badges. It offers desktop-based enterprise SSO, standards-based SSO, MFA and identity governance functionality in its software-delivered products. Imprivata was not included due to not meeting the technical inclusion criteria.

SecureAuth: SecureAuth provides Arculix, resulting from the acquisition of Accepto in November 2021, which supports passwordless authentication, adaptive access, and contextual device-based risk authentication. It also offers SecureAuth Identity Provider, which includes adaptive access and IdP capabilities. The solutions can be used independently or to complement each other, and are available through multiple subscription plans. Both support SaaS, software or hybrid

deployments. SecureAuth was not included due to not meeting the overall inclusion criteria for customer count/revenue.

Vendors Covering Only External Identities

Akamai: Akamai provides the Akamai Identity Cloud, an AM offering for external identities based on its acquisition of Janrain. The Akamai Identity Cloud is a SaaS-delivered product. Akamai was not included due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

SAP: SAP provides the SaaS-delivered SAP Customer Data Solutions, which offers three enterprise solutions: SAP CIAM for B2C, SAP CIAM for B2B, and SAP Enterprise Consent and Preference Management. SAP was not included due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

Transmit Security: Transmit Security offers a SaaS-based AM platform for primarily CIAM use cases. Its focus is on providing a CIAM platform with orchestration, authentication (including passwordless authentication), user management, authorization, identity proofing and fraud detection. It received $543 million in Series A funding in June 2021. Transmit Security was not included due to not meeting the overall inclusion criteria. Solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, are excluded.

Cloud Platform Vendors

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

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

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

Evaluation Criteria

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

Ability to Execute

Gartner analysts evaluate vendors on 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. This includes current product and service capabilities, quality, feature sets, skills, etc. These may be offered natively or through OEM agreements/partnerships, as defined in the Market Definition and detailed in the subcriteria.

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

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

- Directory services
- Internal access administration
- External access administration
- Developer tools
- Authorization and adaptive access
- SSO and session management
- User authentication
- API access control
- Standard application enablement
- Nonstandard application enablement
- Analytics and reporting
- Ease of deployment
- Security and resilience

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
- Revenue breakdown by channel
- 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 functionality among vendors scored higher.

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

Subcriteria:

- General responsiveness to market trends and competitor activities over the last 12 months
- Ability to meet customer needs in different use cases

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand, increase awareness of products and establish a positive identification in the minds of customers. This "mind share" can be driven by a combination of publicity, promotional activity, thought leadership, social media, referrals and sales activities.

Subcriteria:

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

Customer Experience: Products and services and/or programs that enable customers to achieve anticipated results with the products evaluated. Specifically, this includes quality supplier/buyer

interactions, technical support and account support. This may also include ancillary tools, customer support programs, availability of user groups, service-level agreements, and so on.

Subcriteria:

- Customer relationship and services
- Support services, SLAs
- Professional services offerings

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	High
Marketing Execution	Medium
Customer Experience	High

Evaluation Criteria ↓	*Weighting* ↓
Operations	Low
As of August 2022	

Source: Gartner (November 2022)

Completeness of Vision

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

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

Subcriteria:

- Strengths and weaknesses:
  - Market research program and methodology
  - Understanding the competition and their own strengths and weaknesses
- Opportunities and threats:
  - Understanding customer needs
  - Understanding the future of the AM market, the biggest threats and their own place in this market

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

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

Subcriteria:

- Brand awareness
- Product marketing strategy plan
- Customer sentiment

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

Subcriteria:

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

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

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

Subcriteria:

- Product strategy
- Product roadmap, future plans
- Product gaps closed (catch-up features delivered)
- Product development life cycle

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

Subcriteria:

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

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

Subcriteria:

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

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

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

Subcriteria:

- Recent (i.e., the past 12 months) track record of (technical and nontechnical) innovations that differentiate the vendor's product/service
- Planned (nontechnical) innovations that will differentiate the vendor's product/service over the next 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 capabilities

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High

Evaluation Criteria ↓	*Weighting* ↓
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	High
As of August 2022	

Source: Gartner (November 2022)

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 converged IAM platforms or a broader IAM portfolio. Leaders typically demonstrate solid customer satisfaction with overall AM capabilities, the sales process and/or related service and support.

Challengers

Challengers show strong execution, complete and specialized product features, and have significant customer bases. However, they have not shown the Completeness of Vision for AM that Leaders have. Rather, their vision and execution for marketing, technology, methodology and/or means of delivery tend to be more focused on sales execution and doubling down on their

own strengths, rather than making large investments in 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 adjacent and converged IAM capabilities, and may be focused on a specific market segment or set of use cases. In addition, they have a strong vision for the future of the market and their place in it.

Niche Players

Niche Players provide AM technology that is a good match for specific use cases. They focus on market segments by customer size, typically offering AM add-on capability to other products used by their existing customer base; they can outperform many competitors in their specific area of focus. Vendors in this quadrant often have large customers, as well as a strong specialization in some areas of AM (like user authentication, for example). Brand awareness of their AM product is usually low relative to vendors in other quadrants. Vision and strategy may not extend much beyond feature improvements to current offerings. Some Niche Players' pricing might be considered too high for the value they provide. However, inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused spectrum. Niche solutions can be very effective in their areas of focus.

Context

ITDR

Identity systems are fundamental for business. Organizations' reliance on identity infrastructure, like AM tools, as means to enable collaboration, remote work and customer access to services has transformed those systems into a prime target for threat actors.

Conventional security and IAM preventive controls are not sufficient to protect identity systems from cyberattacks. Modern identity threats can subvert traditional IAM preventive controls, like multifactor authentication (MFA), making identity threat detection and response (ITDR) a top cybersecurity priority for 2022 and beyond (see Top Trends in Cybersecurity 2022). As described in Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response, ITDR is a security discipline that encompasses threat intelligence, best practices, a knowledge base, tools and processes to protect identity systems. It works through the implementation of detection mechanisms, investigation of suspect posture changes and activities, and response to attacks to restore the integrity of the identity infrastructure.

Some AM vendors have started to add more threat detection controls, but only for their own products/services, and most only focus on detection, not response mechanisms like playbook management. Organizations should plan to implement "defense in depth" that focuses on identity. They should evaluate the inherent risks of having a single point of failure when adopting an AM tool that claims to offer prevention, detection and response. They should also consider a

multivendor approach, with external ITDR-capable tools that can be used as an additional layer of defense.

Forty-four percent of vendors evaluated in the MQ have released some sort of ITDR capability, while 66% have mentioned plans to add more ITDR capabilities in the future. Thirty-three percent did not mention any plans to introduce ITDR.

Recommendations when evaluating AM vendors:

- Ask for step-up authentication, quarantining or session termination features to mitigate the risk of account takeover (ATO).
- Use established and emerging standards that can be provided in AM (e.g., OAuth 2.0, CAEP).
- Evaluate the ITDR capabilities of AM and infrastructure security tools, as well as those provided by specialist detection and response tools. A layered approach to ITDR is the best way to enhance preparedness for cyberattacks.

Journey-Time Orchestration in AM Context

Journey-time orchestration is an evolving approach to improving risk management along digital user journeys in real time as the user interacts with the application. Most organizations manage many runtime access controls through AM tools and adjacent identity-proofing, authentication and fraud detection tools. Journey-time orchestration manages vendor integrations, simplifies risk assessment at each point on the journey and facilitates the delivery of the best possible user experience (UX) with the minimum acceptable risk. For more context, please see Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX.

AM vendors position their tools as a journey-time orchestration layer for runtime access controls. The journey-time orchestration capabilities of AM enable the definition of runtime user access journeys through the integration of disparate external IAM tools (e.g., for authentication, identity proofing and affirmation [IPA] and fraud detection), and configuration of access flows. The latter typically takes place in a visual designer interface. This orchestration through AM is enabled through low-code, no-code and pro-code approaches to building sophisticated authentication and authorization flows. These flows would otherwise require professional coding abilities, as well as the ability to monitor and manage these fragmented IAM pieces.

AM vendors should offer journey-time orchestration capabilities to reduce the cost and complexity of integration of other disparate IAM tools and help contain IAM sprawl. This would reduce the need to buy new IAM tools, as it would enable existing pieces to be reused and connected, making them interoperable. These capabilities can offer value for CIAM use cases by replacing custom code in homegrown CIAM implementations with a more flexible integration platform.

Sixty-six percent of vendors have started to offer some journey-time orchestration capabilities, with only 22% (ForgeRock and Ping Identity) offering a visual flow designer option. The majority of

orchestration capabilities offer only low-code and pro-code approaches. See Critical Capabilities for Access Management for more information on the different types of orchestration approaches evaluated for AM vendors. Thirty-three percent of vendors still do not offer any journey-time orchestration capabilities. However, 44% of vendors plan to add more journey-time orchestration capabilities in the future.

Recommendations when evaluating AM vendors:

- Evaluate journey-time orchestration capabilities in AM vendor offerings to remove the complexity of integrating multiple IAM vendors and improve the efficiency of risk management along the digital user journey.
- Assess AM vendors' resilience and business continuity plans carefully when using AM as an orchestration layer, given the risk that presents itself when using a single vendor to manage connectivity to multiple downstream vendors.
- Deliver tailored and dynamic risk-based UX by using journey-time orchestration capabilities to connect the analytics and UI layers to broker calls between systems along the user journey.
- If you decide to select an AM vendor without native orchestration capability, then explore an orchestration vendor with which you can work independently of your interactions with the AM vendor. Ensure that integrations are possible.

Decentralized Identities

Decentralized identity is the foundation of the future decentralized web, which puts users in control of their data and prevents excessive data proliferation by enabling verifiable claims and credentials. This is achieved by implementing reusable identities and secure relationships. DCI approaches promise more secure, private and available access to holding and proving facts about someone's (or potentially, something's) identity. The mechanism that most DCI vendors use to provide this includes:

- A trust fabric — Essentially a private network on which all transactions take place, typically a decentralized ledger.
- A wallet — An electronic storage mechanism, typically an application on a mobile device, which establishes the user's identity on the trust fabric and holds identity attributes in the form of verifiable claims.

Verifiable claims (VCs) are encrypted pieces of data that present authoritative information representing identity attributes. The holder of the wallet can use those VCs to prove facts about themselves. VCs, along with the process of zero-knowledge proofs and zero knowledge claims, are where DCI gets its privacy and security benefits. For more context, please see Innovation Insight for Decentralized Identity and Verifiable Claims.

The DCI movement is impactful for AM vendors, especially for the external identity use cases. More people and companies are using DCI as a global identity approach (see Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control). Therefore, AM vendors that do not accommodate that identity approach, either through developing their own DCI tool or through supporting integrations for external identities, will be left behind. But even in internal use cases, experiments are taking place to use the DCI strategy for internal workers to gain access to applications and data. For example, VCs are used to represent authorization to applications, and then access tokens or cookies are created on the basis of those VCs, as opposed to being based on data in a centralized database.

The activity of AM vendors in this area is solidifying, led by IBM, Microsoft and Ping Identity, who have developed DCI products or functionality. All of the other vendors evaluated in this report support DCI networks through integrations, and at least two others are roadmapping future DCI functionality in their products.

Recommendations when evaluating AM vendors:

- Determine your DCI use case, define where VCs can create value and make proving identity data simpler and more secure for your users.
- If you only want to support identities coming from DCI networks for external users, ensure that the AM vendor you choose works with those partners.
- If you want to start using DCI for your internal or external users, consider one of the three AM vendors that offer native DCI functionality in their AM products, or in a separate product that they offer.
- If you decide to select an AM vendor without native DCI functionality, then explore a DCI vendor with which you can work independently of your interactions with the AM vendor. Ensure that integrations are possible.

IAM Convergence

IAM convergence is accelerating in 2022, and small-to-midsize enterprises with more basic IAM needs have helped a lot to popularize converged IAM platforms. Cost is still an important factor, but it is not the main one. More than half of Gartner clients believe it is more important to have a converged IAM platform solution that can mitigate more risks, than to have solutions that only partially cover their requirements.

Convergence is also being fueled by vendor consolidation trends. A recent Gartner survey shows that 75% of client organizations are pursuing a vendor consolidation strategy, up from 29% in 2020. [1] Consolidation takes time, however, and nearly two-thirds of respondents have been consolidating for three or more years. Sixty-five percent of organizations expect to improve their overall security efficacy and team efficiency through vendor consolidation.

Sixty-six percent of AM vendors evaluated in this Magic Quadrant currently offer converged IAM capabilities such as IGA, PAM, fraud detection or identity proofing. The rest have mentioned IAM convergence as being on their roadmaps. For more context, please see Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control.

Recommendations when evaluating AM vendors:

- Avoid current IAM toolset overlap by fully defining and documenting all use cases. Identify whether a best-of-breed AM vendor or a converged AM vendor can meet the needs of your organization. Compare prices of converged IAM features with those of best-of-breed suites.
- If you decide to select an AM vendor without converged features, then explore and prioritize the most appropriate best-of-breed vendor capable of strategically addressing each functional area individually.
- Reduce overall AM integration costs by choosing a converged AM tool before selecting other stand-alone IGA or PAM products.
- Embed AM into the organization's identity fabric — in simple terms, the organization's evolving IAM infrastructure. Make sure other IAM tools within your identity fabric integrate with the AM vendor. Converged platforms offer most, but not all, of the features and functions of an identity fabric.

Passwordless and Phishing-Resistant Authentication

Attacks exploiting weak or compromised passwords make up the overwhelming majority of initial vectors leading to data breaches. Pressures from regulators, auditors and insurance companies for "MFA everywhere" are pushing organizations to reevaluate their conventional password-plus-one-factor authentication (+1FA) approaches. Passwordless authentication is an aspirational goal of removing passwords in order to reap both UX and security benefits. Combining the removal of passwords as an authentication factor with the introduction of additional, phishing-resistant authentication directly addresses both risk exposure and mandates for MFA.

Every evaluated vendor has an offering for FIDO2 support and/or passwordless authentication flows. Their adoption, therefore, requires the deploying organization to adopt authentication methods that reduce the use of passwords.

Organizations will need to evaluate how their AM provider's passwordless and phishing-resistant MFA approaches integrate with their existing business processes. Apply adaptive access principles wherever possible. Plan to diversify the variety of authentication methods supported for both workforce and customer identities, so that the deploying organization can select the method (or set of methods) that best meshes with its threat models, UX needs and resources.

Recommendations when evaluating AM vendors:

- Request support for more phishing-resistant methods, like FIDO2. If passwordless strategies are being evaluated, ask for methods to add a higher-friction action (PIN or biometric method).
- Mitigate MFA prompt bombing attacks. Check whether the evaluated AM vendor solution can choke login attempts, provide additional context with prompt messages, bind the authentication to the session and require that the phone and endpoint used are in the same location. Make sure the AM solution can detect consecutive or abnormal MFA prompting activity.
- Make a plan to reduce the use of passwords in your environment, and prioritize vendors that are able to simplify migration from legacy password +1FA approaches to passwordess MFA (see Take 3 Steps Toward Passwordless Authentication).
- Be prepared to offer a variety of authentication options for both internal and external use cases so that buyers can select methods that are most appropriate for their situation.

Market Overview

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

- **Increased threats and attacks to identity systems** — Credential (i.e., password) misuse accounted for 40% of breaches in 2021. [2] Forty-four percent of vendors evaluated in the Magic Quadrant have released some sort of ITDR capability, but none has introduced response mechanisms, such as playbook management.
- **Journey-time orchestration** — Sixty-six percent of vendors have started to offer some journey-time orchestration capabilities, with only 22% offering a visual flow designer option for no-code approaches.
- **Decentralized identities** — The activity of AM vendors in this area is solidifying, with at least 33% of vendors offering DCI products or functionality. All of the other vendors in the Magic Quadrant support DCI networks through integrations.
- **IAM convergence** — Seventy-five percent of client organizations are pursuing a vendor consolidation strategy, up from 29% in 2020. Sixty-six percent of vendors evaluated in the Magic Quadrant currently offer some type of converged IAM capability, such as IGA, PAM, fraud detection or identity proofing.
- **Passwordless and phishing-resistant authentication** — Pressures from regulation, auditors and insurance companies for “MFA everywhere” are pushing organizations to reevaluate their conventional password +1FA approaches.

The worldwide AM market revenue was $4.17 billion at the end of 2021, representing a 6.8% share of the overall security software market. This share grew by 33.5% when compared to 2020 (see Market Share: Security Software, Worldwide, 2021). Gartner estimates that the AM market revenue for the vendors covered in this Magic Quadrant totaled $3.02 billion at the end of 2021.

Readers, particularly investment clients, are cautioned not to interpret this revenue estimate as accounting for all AM products and services available in the market. Numerous vendors that could not be included in this Magic Quadrant can meet at least partial requirements — for example, by providing user authentication and SSO, when authorization enforcement is not needed by the customer.

Evidence

[1] **2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey:** This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. A primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis. The research was conducted online during March and April 2022 among 418 respondents from North America (U.S., Canada), Asia/Pacific (Australia, Singapore) and EMEA (France, Germany, U.K.). Results were from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security.

Disclaimer: 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] 2022 Data Breach Investigations Report, Verizon.

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.