Magic Quadrant pour la gestion des accès

16 novembre 2023 - ID G00781727 - 65 min de lecture

Par**et 2 autres** Henrique Teixeira, Données Abhyuday,

La gestion des accès du personnel devient banalisée, tandis que CIAM innove plus rapidement, offrant ainsi des opportunités accrues pour les cas d'utilisation B2B. La fabrication additive continue d'être une cible attrayante pour les attaquants, c'est pourquoi l'ITDR gagnera en importance en 2024, tout comme la prise en charge des mots de passe et de la vérification d'identité.

Hypothèse de planification stratégique

D'ici 2027, intégration avec vérification d'identité pour l'intégration, l'accréditation et l'authentification. la récupération sera une fonctionnalité standard des outils de gestion des accès, réduisant potentiellement les attaques de piratage de compte contre ces processus de 75 %.

Définition/description du marché

Gartner définit la gestion des accès (AM) comme des plates-formes qui incluent un fournisseur d'identité (IdP) et établissent, gèrent et appliquent des contrôles d'accès d'exécution au moins au cloud, aux applications Web modernes basées sur des normes et aux applications Web classiques.

L'objectif d'AM est de permettre l'accès par authentification unique (SSO) aux personnes (personnel, consommateur et autres utilisateurs< a i=3>) et machines en applications protégées de manière rationalisée et cohérente qui améliore l'expérience utilisateur. AM est également chargé de fournir des contrôles de sécurité pour protéger la session utilisateur lors de l'exécution, en appliquantg l'authentification (avec authentification multifacteur [MFA]) et nous autoriseing accès adaptatif fournir un contexte d'identité à d'autres outils de cybersécurité pour permettre l'identification -première sécurité. peutAM Enfin, .

Les capacités de base indispensables pour ce marché comprennent :

- Un directeurou un référentiel d'identités pour le personnel ou les utilisateurs externes, y compris les services de synchronisation d'identité.< /span>
- Administration des identités pour les applications intégrées, avec fonctionnalités de base de gestion du cycle de vie et de gestion des profils, avec prise en charge pourou le système de gestion des identités inter-domaines (SCIM).

- SSO et gestion de sessions avec prise en charge des protocoles d'identité standard (OpenID Connect, SAML) et des API d'accès applicationsbasées sur des standards et ancienness (via des proxys ou des agents).
- Authentification des utilisateurs (y compris MFA de base).
- Application de l'autorisation (y compris la prise en charge des protocoles d'autorisation modernes , y compris OAuth 2.0).

Les capacités standard pour ce marché comprennent :

- AFonctions M pour machines (charge de travail et appareils) et Contrôle d'accès API.
- Méthodes d'authentification des utilisateurs non principales, y compris la prise en charge des méthodes MFA résistantes au phishing (par exemple, X.509, FIDO), des contrôles pour atténuer l'utilisation de mots de passe compromis et des protections contre les attaques courantes de jetons MFA.
- Autorisation Noncore, y compris risquebasée sur les risques , décisions dynamiques en matière d'accès adaptatif.
- Intégration d'identité portable pour la fédération et le contrôle d'accès (c'est-à-dire apportez votre propre identité [BYOI]).
- Administration déléguée et gestion des partenaires (IAM client business-to-business [B2B] [CIAM]).

Les fonctionnalités facultatives pour ce marché incluent :

- Fonctions AM pour business-to-business-to-anything (B2B2X) et la gestion du cycle de vie. administration avancée des identités, a ou cas d'utilisation de gouvernement à constituant (G2C)
- Fonctions de confiance adaptatives continues, pméthodes d'authentification sans mot de passe, prise en charge des mécanismes d'authentification biométrique, d< /span>. identités décentralisées et revendications vérifiables
- Détection des fraudes, prévention des piratages de compte (ATO) et idétection et réponse aux menaces liées à l'identité (ITDR).
- Profilage progressif et gestion du consentement, gestion et anonymisation des données d'informations personnelles identifiables (PII), analyse client.
- Orchestration du temps de parcours et autres interfaces low/no-code pour la personnalisation et l'extensibilité dans le contexte de la gestion des accès.

Consultez la section Notes à la fin de ce document pour une explication détaillée des acronymes et d'autres informations importantes lors de la lecture de ce Magic Quadrant.

Quadrant magique

Figure 1 : Magic Quadrant pour la gestion des accès

Points forts et mises en garde du fournisseur

CyberArk

CyberArk est un challenger dans ce Magic Quadrant. Ses produits AM sont livrés en SaaS et vendus en bundles pour la main-d'œuvre (Workforce Standard, Premium et Enterprise), la sécurité des points finaux avec MFA (Adaptive Secure Desktop et Secure Desktop) et pour CIAM (B2B Standard et B2C Standard), ou en modules individuels. . Les opérations de CyberArk sont géographiquement diversifiées et la plupart des clients de CyberArk AM sont des petites et moyennes organisations qui utilisent ses produits pour des scénarios de main-d'œuvre.

Les fonctionnalités récemment ajoutées incluent des capacités JTO améliorées, une atténuation rapide des bombardements MFA et des flux de réponse aux incidents ITDR. La feuille de route de

CyberArk comprend un navigateur sécurisé pour l'accès aux applications et à l'infrastructure, une place de marché JTO et d'autres fonctionnalités convergées IAM.

Forces

- CyberArk a obtenu le score le plus élevé parmi les fournisseurs évalués pour l'expérience client. Ses clients citent la facilité d'utilisation des produits et la simplicité de l'interface utilisateur comme avantages clés.

- CyberArk a démontré une forte capacité d'exécution et bénéficie d'une stratégie commerciale qui exploite sa base installée de PAM. Cette stratégie a été couronnée de succès et la base installée de fabrication additive du fournisseur a considérablement augmenté d'année en année. Les produits AM de CyberArk peuvent constituer un bon choix pour les clients recherchant les avantages de combiner l'AM avec son portefeuille PAM.

- CyberArk a obtenu un score supérieur à la moyenne en matière de résilience. Il affirme que seule l'équipe CyberArk DevOps a accès à l'infrastructure de production AM.

- CyberArk a obtenu des résultats supérieurs à la moyenne en termes d'exécution marketing et de modèle économique. CyberArk offre une bonne prise en charge de l'internationalisation pour son ensemble de produits AM, y compris des interfaces d'administration et d'utilisateur final, avec une liste complète de langues prises en charge pour ses différentes offres AM.

Précautions

- Les produits AM de CyberArk sont parmi les plus chers du marché. Pour cette recherche, les prix de plusieurs scénarios évalués sont bien supérieurs à la moyenne, tant pour les scénarios de main-d'œuvre que pour les scénarios CIAM complexes.

- Malgré la croissance du nombre de clients, CyberArk n'a pas démontré une bonne traction de ses produits AM auprès des clients B2B et B2C CIAM, des cas d'utilisation des développeurs ou des clients plus importants. Sa stratégie commerciale est axée sur l'entreprise et manque d'un message plus solide pour les développeurs et les utilisateurs techniques. Son ensemble de produits ne dispose pas de capacités de contrôle d'accès API plus solides et la grande majorité de sa clientèle utilise CyberArk uniquement pour les cas d'utilisation du personnel.

- Une grande partie des éléments de la feuille de route de CyberArk ne sont pas axés sur la FA, mais concernent plutôt son activité PAM plus vaste et d'autres domaines adjacents. Ce manque de concentration dans la fabrication additive a eu un impact sur l'intégralité de la vision de CyberArk, entraînant des scores inférieurs à la moyenne en matière d'innovation et de stratégie d'offre (produit).

- Bien qu'il puisse convenir à des cas d'utilisation de fabrication additive plus standardisés et prêts à l'emploi, CyberArk peut être complexe à personnaliser. Il a obtenu des résultats inférieurs à la moyenne en termes de personnalisation et d'extensibilité, ainsi que de prise en charge de l'intégration d'identité portable.

Confier

Entrust est un challenger dans ce Magic Quadrant. Son produit Entrust Identity as a Service (IDaaS) est fourni sous forme de SaaS et vendu sous forme de forfaits pour le personnel et le CIAM. Les opérations d'Entrust sont géographiquement diversifiées. La plupart des clients d'Entrust appartiennent aux secteurs bancaire et gouvernemental et utilisent son produit AM pour des scénarios de main-d'œuvre.

Les fonctionnalités récemment ajoutées incluent la compatibilité des mots de passe, l'atténuation des bombardements rapides MFA et la vérification de l'identité en tant que service. La feuille de route d'Entrust comprend un moteur de risque basé sur l'IA/ML, un outil JTO et des fonctionnalités de reporting améliorées.

Forces

- Entrust a obtenu le score le plus élevé en matière d'authentification des utilisateurs parmi tous les fournisseurs dans cette recherche. Ses méthodes X.509 et FIDO résistantes au phishing sont améliorées en prenant en charge un large éventail d'authentificateurs applicables à différents secteurs verticaux. Entrust a également la capacité de gérer des moteurs de risque externes qui améliorent les capacités de détection et de collecte de signaux, et s'étendent aux outils IDV.

- Les prix d'Entrust pour plusieurs scénarios évalués dans cette recherche sont systématiquement inférieurs aux moyennes du marché.

- Entrust offre des fonctionnalités de fabrication additive, d'infrastructure à clé publique (PKI), de signatures numériques et d'IDV pour satisfaire à l'authentification forte du client (SCA). Il propose une authentification basée sur les risques et un SDK avec des exemples pour la directive européenne sur les services de paiement (PSD2).

- Entrust a obtenu un score supérieur à la moyenne en termes de réactivité au marché et d'antécédents. En très peu de temps, il a ajouté davantage de fonctionnalités de FA pour rattraper les fonctionnalités déjà proposées par d'autres fournisseurs de FA sur le marché, démontrant ainsi une bonne capacité d'exécution.

Précautions

- L'orientation d'Entrust en matière de FA est motivée par sa spécialité en matière d'authentification des utilisateurs, plutôt que par un lien étroit avec les moteurs du marché global de la FA. Entrust a obtenu le score le plus bas dans cette recherche pour la stratégie marketing et l'un des scores les plus bas pour la compréhension du marché. Son modèle économique pour la fabrication additive n'est pas non plus clair. Le marché perçoit Entrust comme un fournisseur d'authentification avant tout, et sa stratégie commerciale pour la FA ne s'étend clairement pas au-delà de cela au personnel, au financement et au marketing pour d'autres capacités AM critiques.

- Entrust a une vision claire, mais cette vision n'est ni fortement dérivée ni bien alignée sur les études de marché ou le sentiment des clients à l'égard de la fabrication additive. En

conséquence, Entrust a conclu le plus petit nombre de nouvelles transactions au cours de la dernière année parmi tous les fournisseurs participant à cette recherche.
- Entrust n'offre pas de SLA de 99,99 % — il s'arrête à 99,9 %. La couverture géographique d'Entrust de son offre SaaS est également limitée par rapport aux autres fournisseurs évalués.

- Entrust a obtenu des scores inférieurs à la moyenne pour les capacités CIAM B2C et B2B, ainsi que pour le contrôle d'accès, la personnalisation et l'extensibilité des API. Il n'existe pas de marché pour les intégrations tierces, ni d'options d'intégration d'identité portables préconfigurées. La personnalisation et l'extension du produit nécessitent des capacités de pro-codage.

ForgeRock

ForgeRock est un leader dans ce Magic Quadrant. Son produit ForgeRock Identity Cloud est fourni sous la forme d'une plate-forme SaaS IAM convergée et vendu dans une combinaison de packages de base et de modules supplémentaires. ForgeRock propose également son produit de gestion des accès sous forme de logiciel. Les opérations de ForgeRock sont géographiquement diversifiées et la plupart des clients de ForgeRock sont de grandes organisations utilisant son produit logiciel pour les scénarios CIAM.

Les fonctionnalités récemment ajoutées incluent des signaux supplémentaires pour la détection des menaces, de nouveaux flux et connecteurs à son outil JTO et la compatibilité des clés d'accès. La feuille de route de ForgeRock comprend des capacités supplémentaires de détection des fraudes et des menaces, des améliorations de son outil JTO et de sa place de marché, ainsi que davantage de fonctionnalités IAM convergées vers SaaS.

En août 2023, Thoma Bravo, la société propriétaire de Ping Identity, a annoncé avoir finalisé l'acquisition de ForgeRock et l'avoir combinée avec Ping Identity. L'annonce a été faite après la date limite de cette recherche.

Forces
- ForgeRock a obtenu le score le plus élevé dans cette recherche pour les capacités de ses produits, notamment en ce qui concerne les fonctionnalités CIAM B2B et B2C, l'autorisation et l'accès adaptatif. ForgeRock propose diverses approches no-code/low-code, et c'est l'un des très rares fournisseurs du marché à proposer un outil JTO avec un concepteur de flux visuel (ForgeRock Trees). Il se différencie en termes de personnalisation et d'extensibilité, permettant des modèles de déploiement hybrides (sur site, cloud, hébergé). Il offre également un bon marché pour les intégrations.

- ForgeRock a démontré une solide exécution marketing, affichant de bons résultats dans les ventes CIAM.

- ForgeRock a obtenu l'un des scores les plus élevés pour son modèle commercial, présentant une vision et un objectif complets et ambitieux qui s'alignent bien avec les tendances du secteur.

- ForgeRock a obtenu des scores supérieurs à la moyenne en matière d'authentification des utilisateurs. ForgeRock propose un outil de création de politiques visuelles pour SCA dans PSD2 et open banking. Il est également certifié FAPI-CIBA.

Précautions

- Bien que ForgeRock ait connu du succès dans ses ventes CIAM, elle a récemment connu une perte de clientèle en raison de la réduction des investissements dans sa clientèle OEM. ForgeRock est également à la traîne en matière d'adoption du SaaS, rapportant le plus faible nombre de clients SaaS parmi tous les leaders de ce Magic Quadrant.

- Il est conseillé aux clients potentiels et existants de se renseigner sur les futurs projets de ForgeRock après l'annonce de sa fusion avec Ping Identity.

- Les prix de ForgeRock sont supérieurs à la moyenne pour tous les scénarios évalués dans cette recherche, à l'exception des très grands cas d'utilisation CIAM.

- ForgeRock n'est pas une solution facile à déployer et ses résultats sont inférieurs à la moyenne pour les capacités de reporting des menaces AM de son produit. Obtenir des informations analytiques sur les données d’exécution est complexe. La génération de rapports n'est pas intuitive et nécessite l'exportation de fichiers JSON. Les tableaux de bord des menaces existants sont assez rigides et ne sont pas personnalisables.

IBM

IBM est un leader dans ce Magic Quadrant. Ses produits IBM Security Verify sont fournis sous forme SaaS et vendus sous forme d'offre groupée ou de modules individuels. IBM propose également IBM Security Verify Access sous forme de logiciel. Les opérations d'IBM sont géographiquement diversifiées et la plupart des clients d'IBM sont de grandes organisations utilisant son produit logiciel pour les scénarios de main-d'œuvre et CIAM.

Les fonctionnalités récemment ajoutées incluent la compatibilité des clés d'accès, des capacités ITDR intégrées pour empêcher l'utilisation de mots de passe compromis et bloquer le trafic suspect, ainsi qu'une disponibilité accrue des SLA à 99,99 %. La feuille de route d'IBM comprend un outil JTO avec un concepteur de flux visuel, une délégation d'accès à des parties de confiance et un produit d'identité décentralisé.

Forces

- IBM démontre une vision complète et complète améliorée avec l'un des scores les plus élevés pour la stratégie produit (feuille de route) qui comprend de nombreuses fonctionnalités spécifiques à la FA à court terme, comme DCI et un outil JTO. Les capacités de gestion du consentement de son offre actuelle pour les cas d’utilisation CIAM sont parmi les plus performantes de cette recherche.

- IBM offre un bon rapport qualité-prix, avec des prix systématiquement inférieurs à ceux de ses concurrents.

- IBM a obtenu le score le plus élevé en matière de stratégie géographique grâce à l'introduction de nouvelles régions cloud couvrant les États-Unis, le gouvernement fédéral américain, le Canada, l'Europe, la Chine, le Japon et l'Australie. Il a également augmenté son SLA AM SaaS à 99,99 %.

- IBM Security Verify a obtenu des scores supérieurs à la moyenne pour les fonctionnalités du produit telles que la personnalisation, l'extensibilité et l'authentification des utilisateurs. Il offre une collection complète d'API, de SDK et de documentation, la prise en charge des passerelles et des agents en tant que facteurs de forme de conteneur, ainsi qu'une intégration native avec les applications OpenShift, Red Hat Single Sign-On et Keycloak. IBM a obtenu la certification FAPI-CIBA (pour son produit logiciel).

Précautions

- En raison de l'accent mis par IBM sur les grandes entreprises, IBM n'est pas un choix populaire parmi les petites et moyennes entreprises et démontre une moindre traction sur ce segment de marché que les autres leaders.

- Malgré ses capacités d'extensibilité et de personnalisation supérieures à la moyenne, IBM dispose d'un portefeuille limité d'intégrations sur son marché par rapport aux marchés d'autres fournisseurs. Des efforts et des coûts d'intégration supplémentaires doivent être pris en compte pour les types d'intégrations non basés sur des normes.

- IBM a obtenu l'un des scores les plus bas en matière d'exécution marketing. Cela se reflète dans la moindre notoriété de la marque de son produit AM par rapport aux autres leaders. La vision globale, la stratégie et le plan commercial d'IBM pour ses capacités de fabrication additive font partie intégrante de la suite du plus grand portefeuille de sécurité d'IBM.

- IBM propose des fonctionnalités moins matures pour le CIAM B2B que bon nombre de ses concurrents. Presque tous les flux d'administration déléguée évalués dans cette recherche nécessitent une personnalisation via des API.

Microsoft

Microsoft est un leader dans ce Magic Quadrant. Ses Microsoft Entra ID (anciennement Azure AD) et Azure AD External Identities sont, respectivement, des produits de main-d'œuvre et CIAM livrés en SaaS. Les produits sont vendus sur une plateforme IAM convergée sous forme de offres groupées et de modules individuels. Les opérations de Microsoft sont géographiquement diversifiées et principalement utilisées pour les cas d'utilisation du personnel.

Les fonctionnalités récemment ajoutées incluent un produit d'identité décentralisé (DCI) appelé Microsoft Entra Verified ID, un produit de gestion de l'identité des machines (Microsoft Entra Workload ID) et une fonctionnalité de gestion de la posture de sécurité (SPM) appelée recommandations Microsoft Entra (anciennement recommandations Azure AD). La feuille de route de Microsoft comprend une interface GenAI pour SPM et les recommandations, une prise en charge multicloud pour les identités de charge de travail et un DCI intégré dans le produit CIAM.

Microsoft a annoncé le changement de nom d'Azure AD en Microsoft Entra ID en juillet 2023.

Forces

- Microsoft a obtenu les scores les plus élevés dans cette recherche en termes de viabilité globale, d'exécution marketing, de modèle commercial et d'exécution des ventes/tarification. Sa base installée a atteint le nombre impressionnant de 700 000 clients payants.

- Les prix globaux de Microsoft sont inférieurs à la moyenne du marché. En particulier, les prix des cas d'utilisation CIAM de Microsoft sont bien inférieurs à la moyenne des fournisseurs de ce Magic Quadrant.

- Microsoft a obtenu le score le plus élevé parmi les fournisseurs évalués en matière de compréhension du marché. Cela est dû en partie à ses premiers progrès en matière d'identité de machine et de prise en charge de DCI, mais également aux améliorations apportées aux capacités AM plus établies.

- Microsoft a obtenu le score le plus élevé en matière de reporting sur les menaces et d'ITDR. Il propose des recommandations Microsoft Entra et une capacité de mesure SPM avec des scores de sécurité. Microsoft Entra est un élément central de la stratégie globale de cybersécurité du fournisseur, qui est étroitement intégrée à Microsoft 365 et Azure dans leur ensemble.

Précautions

- Azure AD External Identities (pour B2C et B2B) manque encore de maturité par rapport aux solutions d'autres Leaders. Les flux CIAM les plus complexes nécessitent une personnalisation approfondie et l'aide de services professionnels.

- Les grands exercices de changement de marque comme Microsoft Entra ont tendance à créer une confusion quant aux caractéristiques et fonctionnalités qui existent dans quels produits. Cette confusion ressort des demandes des clients de Gartner, en particulier concernant les identités externes Azure AD, dont les fonctionnalités B2C seront remplacées par une nouvelle plate-forme CIAM appelée Microsoft Entra External ID.

- Les fonctionnalités AM spécifiques de Microsoft Entra ID, telles que Entra ID Protection, nécessitent une licence supplémentaire. Compte tenu de la prévalence des attaques contre les infrastructures d'identité, de nombreuses organisations devront prendre en compte des coûts supplémentaires.

- Microsoft a obtenu le score le plus bas parmi tous les leaders en matière de personnalisation et d'extensibilité. Malgré un catalogue décent d'intégrations d'identités portables centralisées, Microsoft Entra ID nécessite une personnalisation importante pour fournir des flux d'utilisateurs courants et intégrer des méthodes MFA alternatives. Il est complexe à intégrer à des outils non Microsoft pour un accès adaptatif externe ou une autorisation à granularité fine (FGA).

Okta

Okta est un leader dans ce Magic Quadrant. Ses produits AM sont livrés en SaaS et vendus sous forme de offres groupées (Workforce Identity Cloud [WIC], Customer Identity Cloud [CIC,

anciennement Auth0]) et de modules individuels dans le cadre d'une plateforme IAM convergée. Les opérations d'Okta sont géographiquement diversifiées et la plupart de ses clients utilisent ses produits soit pour le personnel, soit pour des cas d'utilisation CIAM.

Les fonctionnalités récemment ajoutées incluent un MFA (Okta FastPass) résistant au phishing, une liste configurable d'authentificateurs FIDO et une autorisation élevée d'exploitation FedRAMP (ATO). La feuille de route d'Okta inclut un moyen permettant aux développeurs de créer des applications SaaS dans CIC qui s'intègrent automatiquement à la plate-forme WIC d'Okta, aux fonctionnalités SPM et à un outil FGA.

Forces

- Okta a obtenu le score le plus élevé parmi tous les fournisseurs pour ses intégrations centralisées d'identité portable, et l'un des scores les plus élevés pour l'authentification des utilisateurs. Il propose un catalogue complet d'intégrations IdP externes pour CIAM. Il fournit également une détection des mots de passe compromis qui peut être utile pour se protéger contre les attaques MFA.

- Okta a obtenu l'un des scores les plus élevés en matière de reporting sur les menaces et d'ITDR. Il propose une fonctionnalité SPM dans la plateforme WIC appelée HealthInsight, qui audite les paramètres de sécurité d'une organisation et suggère des mesures correctives.

- Okta a démontré la plus grande capacité d'exécution parmi tous les fournisseurs de ce Magic Quadrant. Il a obtenu le score le plus élevé en termes d'opérations et l'un des scores les plus élevés en termes de viabilité globale et de capacités du produit. Okta affiche la plus forte croissance en matière de CIAM parmi tous les fournisseurs évalués. Sa croissance en termes de nombre de clients global est également l'une des plus élevées.

- Okta a reçu l'une des notes les plus élevées pour sa stratégie d'offre (produit). Les éléments de la feuille de route incluent des plans tels que FGA et SPM, ainsi que l'intégration de bureau pour son outil MFA. Okta fait également preuve de leadership éclairé en ce qui concerne les informations d'identification FIDO multi-appareils, ce qui est crucial pour fournir une prise en charge solide des mots de passe à l'avenir.

Précautions

- Les tarifs d'Okta restent bien supérieurs à la moyenne et les clients de Gartner mentionnent le coût élevé de la solution du fournisseur. Gartner a remarqué un nombre croissant de clients engagés dans des négociations contractuelles afin d'obtenir un taux de remise approprié avec Okta.

- Okta dispose de deux plates-formes très différentes pour le personnel et le CIAM, qui ne sont pas parfaitement intégrées. CIC, par exemple, ne prend pas en charge le système de gestion des identités inter-domaines (SCIM) comme le fait WIC, et WIC ne prend pas en charge les mêmes fonctionnalités ITDR que la plate-forme CIC.

- Toutes les fonctionnalités d'accès adaptatif proposées par Okta nécessitent une licence supplémentaire. Compte tenu de la prévalence des attaques contre les infrastructures d'identité, de nombreuses organisations devront prendre en compte des coûts supplémentaires.

- Bien qu'Okta obtienne des résultats supérieurs à la moyenne pour les cas d'utilisation CIAM, il ne fournit pas de gestion de base du consentement. Il lui manque également un outil JTO. La capacité de flux de travail actuelle d'Okta, bien qu'utile pour IGA, n'est pas un outil JTO pour les cas d'utilisation CIAM.

Une identité (OneLogin)

One Identity (OneLogin) est un challenger dans ce Magic Quadrant. One Identity est une marque indépendante, opérant sous l'égide de Quest, et OneLogin est le produit AM du portefeuille IAM de One Identity. Les produits AM de One Identity (OneLogin) sont livrés sous forme SaaS et vendus sous forme de offres groupées et de modules individuels. Les opérations de One Identity (OneLogin) sont géographiquement diversifiées et la plupart de ses clients utilisent ses produits pour des cas d'utilisation de main-d'œuvre.

Les fonctionnalités récemment ajoutées incluent la MFA utilisant la prise en charge de la fédération entrante, la détection gratuite des robots et l'atténuation des bombardements rapides MFA. La feuille de route de One Identity (OneLogin) comprend une version native des mots de passe intégrés dans l'application mobile de OneLogin, la confiance des appareils mobiles en libre-service et l'ingestion de signaux tiers pour la prise en charge des fonctions ITDR.

Forces

- One Identity (OneLogin) a obtenu le score le plus élevé en matière de stratégie commerciale parmi tous les fournisseurs. Elle aborde le marché avec une stratégie différenciante de fournisseur de services gérés (MSP). Cela permet aux MSP de regrouper les offres AM, PAM et IGA de One Identity et de les recommander pour les transactions entrantes avec les PME. Plus de 100 MSP ont créé des services autour des produits AM de One Identity (OneLogin).

- One Identity (OneLogin) a reçu des scores supérieurs à la moyenne pour sa facilité de déploiement. Il propose des approches de configuration avancées telles que des hooks de migration qui peuvent éliminer le besoin pour les utilisateurs de se réinscrire ou de modifier leur mot de passe lors de la migration à partir d'outils AM existants.

- Le produit OneLogin a toujours été une bonne option en termes de rapport coût-avantage et le fournisseur continue d'offrir des prix compétitifs pour les petites et moyennes équipes et des cas d'utilisation CIAM plus standardisés.

- One Identity (OneLogin) offre une bonne prise en charge de l'internationalisation pour son produit AM, y compris des interfaces d'administration et d'utilisateur final, avec une liste complète de langues prises en charge pour ses différentes offres AM.

Précautions

- One Identity (OneLogin) n’a pas gagné en popularité dans les cas d’utilisation CIAM. Ses tarifs pour les cas d'utilisation complexes du CIAM sont supérieurs aux moyennes du marché.

- Malgré une stratégie commerciale solide tirant parti des MSP, le nombre total de clients AM et les revenus de One Identity (OneLogin) sont restés presque stables d'une année sur l'autre, et l'abonnement SaaS à ses revenus OneLogin AM a en fait diminué. Sa stratégie commerciale ne comporte pas de message destiné aux développeurs et aux utilisateurs techniques, et son produit ne dispose pas de solides capacités de contrôle d'accès aux API.

- One Identity (OneLogin) a obtenu des scores inférieurs à ceux de l'année dernière pour l'exhaustivité globale de la vision, obtenant des scores inférieurs à la moyenne pour l'innovation et la stratégie d'offre (produit). Il a ajouté certains éléments à sa feuille de route à court terme pour rattraper son retard sur le marché actuel, mais la différenciation AM par rapport aux principaux fournisseurs est absente de sa feuille de route. Sa feuille de route de produits à long terme vise à rattraper les fournisseurs qui proposent des fonctions de base non AM comme IGA, tout en consacrant des dépenses en R&D inférieures à la moyenne du secteur.

- Le SLA standard proposé par le fournisseur n'est que de 99,9 %, et tout ce qui dépasse ce chiffre entraîne des coûts supplémentaires. Au cours des 12 derniers mois, One Identity (OneLogin) a subi sept pannes au total et cinq incidents de dégradation des performances, avec plus de 35 heures d'indisponibilité.

Texte ouvert

OpenText est un acteur de niche dans ce Magic Quadrant. OpenText fait son entrée dans ce Magic Quadrant pour la première fois après l'acquisition de Micro Focus en janvier 2023. Son produit NetIQ Access Management est livré sous forme de SaaS ou de logiciel, et est vendu sous forme de bundles ou de modules individuels. Les opérations d'OpenText sont géographiquement diversifiées et les clients ont tendance à être de grandes organisations utilisant son produit logiciel largement au niveau de la main-d'œuvre et des cas d'utilisation CIAM.

Les fonctionnalités récemment ajoutées incluent une API d'authentification, une authentification sans mot de passe et une validation de proximité Bluetooth pour utiliser un appareil comme jeton. La feuille de route d'OpenText comprend des améliorations générales de son interface utilisateur, son service de risque adaptatif et son authentification sans mot de passe.

Forces

- OpenText peut convenir parfaitement aux grandes organisations et pour répondre à des cas d'utilisation de FA hybride plus complexes, en particulier pour les organisations qui ont besoin de la flexibilité nécessaire pour gérer des déploiements sur site ou hébergés. Sa solution AM convient parfaitement à l'intégration d'applications non standard et héritées en raison de sa flexibilité de déploiement.

- OpenText NetIQ Access Management propose des modèles de livraison flexibles et prend en charge les modèles de déploiement conteneurisés exploitant Docker, Kubernetes et OpenShift. Tous les modules AM sont disponibles pour des déploiements sur site ou hébergés.

- OpenText NetIQ Access Management offre une protection complète contre les mots de passe compromis (listes intégrées, listes manuelles et listes tierces), y compris une intégration clé en main avec la base de données Have I Been Pwned.

- OpenText a obtenu des scores supérieurs à la moyenne en matière d'identités portables. NetIQ Access Management fournit une liaison centralisée prête à l'emploi des identités sociales et des intégrations prédéfinies avec les identifiants gouvernementaux et certains identifiants bancaires.

Précautions

- Le produit SaaS AM d'OpenText est systématiquement plus cher que les autres produits SaaS évalués dans cette recherche. Le SLA de son produit SaaS est de 99,95 %, et tout ce qui dépasse ce chiffre nécessite des coûts supplémentaires.

- OpenText a obtenu le score le plus bas en matière de stratégie commerciale et a démontré des progrès très lents dans sa transition vers le SaaS, soit via des ventes directes, soit via des relations OEM. Parmi tous les fournisseurs de ce Magic Quadrant, il compte le plus petit nombre de clients AM SaaS.

- OpenText a obtenu l'un des scores les plus bas en matière de compréhension du marché parmi tous les fournisseurs évalués dans ce rapport. La fabrication additive ne représente qu'une petite partie d'un très vaste portefeuille de produits OpenText, et la notoriété de la marque NetIQ Access Management continue de décliner, en fonction du nombre réduit de mentions de clients Gartner.

- Outre ses options de déploiement flexibles, NetIQ Access Management est difficile à personnaliser et à étendre. Les API d'intégration sont limitées à l'authentification et la documentation manque de détails. Il n'existe pas de marché pour les intégrations tierces et l'outil ne dispose pas d'une prise en charge low-code plus avancée.

Oracle

Oracle est un acteur de niche dans ce Magic Quadrant. Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) est un produit SaaS fourni avec le service cloud d'Oracle. Oracle propose également Oracle Access Manager (OAM) sous forme de logiciel. Ses opérations et ses clients ont tendance à être géographiquement diversifiés.

Les innovations récentes incluent une fonctionnalité de génération de journaux pour un domaine IAM, un module d'authentification enfichable Linux et une nouvelle politique de validation de mot de passe. Oracle prévoit de continuer à se concentrer sur l'unification de sa plate-forme IAM cloud et sur l'ajout d'autres fonctionnalités IAM adjacentes à l'avenir, pour répondre aux besoins de ses clients Oracle Cloud. La plupart des clients Oracle utilisent le produit OAM sur site pour les cas d'utilisation du personnel. OCI IAM est généralement utilisé pour fournir un accès à l'infrastructure et aux applications Oracle.

Oracle n'a pas répondu aux demandes d'informations supplémentaires ni de révision du contenu préliminaire de ce document. L’analyse de Gartner s’appuie donc sur d’autres sources crédibles.

Forces

- Le produit SaaS AM d'Oracle est moins cher que la moyenne du marché pour tous les scénarios de tarification évalués dans cette recherche.
- OCI IAM fonctionne sur les centres de données cloud d'Oracle et offre une reprise après sinistre interrégionale à toutes les régions du monde OCI où il existe une deuxième région dans le pays, ou lorsque les lois autorisent le déplacement des données vers une autre région spécifique. Il s'agit d'un différenciateur pour les clients souhaitant exécuter la fabrication additive en tant que SaaS dans d'autres cloud qui ne sont fournis ni par Amazon Web Services (AWS), ni par Microsoft Azure ni par Google Cloud Platform.
- Oracle dispose d'une très large base installée pour sa base de données et ses applications (plus de 400 000 clients). Sa stratégie marketing est largement axée sur le ciblage de ces clients existants et la promotion de ses outils IAM en s'appuyant sur les applications Oracle, permettant ainsi aux utilisateurs actuels des applications Oracle d'utiliser plus facilement ses outils IAM.
- Oracle dispose d'une présence mondiale étendue en matière d'opérations et de services, ce qui facilite l'acquisition de produits AM dans des régions où d'autres fournisseurs AM ne sont pas présents.

Précautions

- Oracle est le seul fournisseur de ce Magic Quadrant à ne pas proposer de SLA. Au lieu de cela, Oracle fournit un objectif de niveau de service (SLO) de 99,95 % pour son produit AM SaaS.
- Oracle a reçu la note la plus basse pour une série de catégories qui ont un impact sur sa capacité d'exécution, notamment les capacités des produits/services, la réactivité et les antécédents du marché, ainsi que la compréhension du marché.
- OCI IAM est complexe à déployer et à gérer. En conséquence, il a reçu la note la plus basse pour la facilité de déploiement, ainsi que pour la personnalisation et l'extensibilité (qui nécessitent des capacités de pro-codage). OCI IAM offre des capacités SDK très limitées et il n'existe aucune prise en charge des approches low-code ou no-code.
- Dans l’ensemble, la stratégie récente d’Oracle s’est principalement concentrée en interne sur l’unification de ses divers produits IAM existants sur sa plate-forme SaaS, plutôt que sur l’innovation et les fonctionnalités AM leaders du marché. En conséquence, Oracle a obtenu les scores les plus bas en matière d'innovation dans ce Magic Quadrant.

Identité Ping

Ping Identity est un leader dans ce Magic Quadrant. Sa plateforme cloud PingOne est livrée en SaaS et vendue sous forme de bundles et de modules individuels. Ping Identity propose également plusieurs produits AM (PingFederate, PingAccess, PingDirectory et PingCentral) sous forme de logiciels. Les opérations de Ping Identity sont géographiquement diversifiées et ses

clients sont généralement de grandes organisations utilisant à la fois des déploiements sur site et dans le cloud, parmi les effectifs et les cas d'utilisation CIAM.

Les fonctionnalités récemment ajoutées incluent un nouveau service d'identification décentralisé avec des réclamations vérifiables (PingOne Neo), un moteur de risque avec détection de fraude (PingOne Protect) et une atténuation rapide des bombardements MFA. La feuille de route de Ping Identity comprend des solutions packagées préconfigurées pour différents cas d'utilisation, un nouveau service d'émission et de transformation d'identifiants numériques pour DCI et de nouvelles fonctionnalités ITDR.

En août 2023, Thoma Bravo, la société propriétaire de Ping Identity, a annoncé avoir finalisé l'acquisition de ForgeRock et l'avoir combinée avec Ping Identity. L'annonce a été faite après la date limite de cette recherche.

Forces

- Ping Identity a démontré la plus grande exhaustivité de vision parmi tous les fournisseurs de ce Magic Quadrant. Il a obtenu le score le plus élevé pour la stratégie d'offre (produit) et l'innovation. Outre les éléments de feuille de route déjà mentionnés, il prévoit de lancer une place de marché pour son outil JTO et d'obtenir les certifications FedRAMP High ATO et StateRAMP.

- Ping Identity a obtenu cette année le score le plus élevé en matière de stratégie marketing et l'un des meilleurs en matière de compréhension du marché. Sa stratégie marketing est claire, ciblée et fortement alignée sur le marché, avec des plans directement basés sur les commentaires des clients.

- Ping Identity a également obtenu le score le plus élevé en termes de réactivité et d'expérience sur le marché, après avoir lancé plusieurs nouvelles fonctionnalités sur sa plateforme. Outre les fonctionnalités déjà mentionnées, il a ajouté la détection de fraude convergente AM, une option de configuration basée sur un formulaire pour JTO, la détection des anomalies de jeton OAuth, FGA vers les API et bien d'autres. Ses produits logiciels ont déjà obtenu la certification FAPI-CIBA.

- Ping Identity offre des fonctionnalités matures pour les cas d’utilisation AM des clients et des partenaires. C'est l'un des rares fournisseurs à proposer un outil JTO avec un concepteur de flux visuel (PingOne DaVinci) et un service DCI.

Précautions

- Même si les tarifs de Ping Identity pour la main-d'œuvre sont compétitifs et inférieurs à la moyenne du marché, ses tarifs pour divers cas d'utilisation CIAM sont systématiquement supérieurs à ceux des autres fournisseurs évalués dans cette recherche.

- Le portefeuille Ping Identity AM peut être complexe à comprendre et à déployer. La configuration de l’accès adaptatif, par exemple, est plus complexe que la moyenne.

- Il est conseillé aux clients potentiels et existants de se renseigner sur les projets de portefeuille de Ping Identity après l'annonce de sa fusion avec ForgeRock.

- De nombreux cas d'utilisation B2C et B2B nécessitent soit une personnalisation, soit l'utilisation de l'outil JTO moyennant des frais supplémentaires. Des frais supplémentaires sont également requis pour l'utilisation du moteur de risque de Ping Identity, du contrôle d'accès API et de l'autorisation avancée. Compte tenu de la prévalence des attaques contre l'infrastructure des identités, les organisations devront prendre en compte l'octroi de licences pour des modules supplémentaires pour de nombreuses fonctionnalités.

Thalès

Thales est un visionnaire dans ce Magic Quadrant. Thales propose une suite de produits axés sur la main-d'œuvre composée de OneWelcome Workforce Access Management (anciennement SafeNet Trusted Access), livré en SaaS et vendu sous forme de bundle avec des modules supplémentaires. Thales propose également la plateforme d'identité OneWelcome en SaaS, axée sur le CIAM. Thales a acquis OneWelcome en juillet 2022. Les opérations de Thales sont géographiquement diversifiées avec une forte présence en Europe, et la plupart de ses clients sont généralement de grandes organisations utilisant son produit pour des cas d'utilisation de la main-d'œuvre.

Les fonctionnalités récemment ajoutées incluent les nouvelles fonctionnalités CIAM de OneWelcome, FGA, le profilage progressif dynamique et un système de gestion des données pour la délégation du consentement. La feuille de route de Thales comprend des modèles de délégation prêts à l'emploi avec des flux prédéfinis pour le CIAM B2B, des améliorations JTO avec un concepteur de flux visuel et de nouvelles fonctionnalités d'analyse et d'ITDR.

Forces

- Thales obtient des scores supérieurs à la moyenne en innovation. Il prévoit de se concentrer sur les grands défis CIAM, comme les cas d'utilisation B2B. Les certifications FedRAMP et HIPAA figurent également sur sa feuille de route pour répondre aux besoins du gouvernement fédéral et des secteurs verticaux de la santé.

- Thales obtient également des scores supérieurs à la moyenne en matière de réactivité au marché. Elle a ajouté des fonctionnalités uniques à son portefeuille CIAM, comme la possibilité de déléguer la gestion des consentements à des utilisateurs sélectionnés en fonction de la relation (par exemple, procuration et relation parent-enfant).

- L'acquisition de OneWelcome par Thales ajoute des capacités CIAM synergiques à sa spécialité d'authentification des utilisateurs, ainsi que des capacités axées sur la gestion AM du personnel des gammes de produits SafeNet/Gemalto.

- Thales offre certaines des fonctionnalités B2C les plus matures évaluées dans cette étude, notamment une gestion robuste de l'enregistrement et des profils en libre-service, le profilage progressif, la personnalisation configurable prête à l'emploi des flux d'enregistrement, le consentement aux conditions générales et le consentement basé sur les attributs. gestion.

Précautions

- Thales a reçu la note la plus basse en termes de viabilité globale parmi tous les fournisseurs de ce Magic Quadrant. Cela s'explique en partie par sa concentration réduite sur les petits clients, ce qui a entraîné une diminution du nombre total de clients d'une année sur l'autre, et par un taux de renouvellement de son offre SaaS qui figurait parmi les plus bas des fournisseurs évalués.

- Thales a obtenu des résultats inférieurs à la moyenne en termes de facilité de déploiement, ainsi que de personnalisation et d'extensibilité. Son portefeuille AM est le résultat de plusieurs acquisitions et il n’est pas encore entièrement intégré dans une plateforme unique. Il n'existe pas de marché, pas même de site Web public, qui présente des intégrations tierces prêtes à l'emploi disponibles pour ajouter des signaux externes dans les flux de temps de trajet. Les intégrations non standard et l'extensibilité des produits nécessitent beaucoup de services professionnels, et la personnalisation nécessite des capacités de pro-codage.

- Thales offre une couverture géographique limitée pour l'hébergement de ses offres SaaS par rapport aux autres fournisseurs évalués dans cette étude, ce qui peut constituer un défi pour les prospects dans d'autres régions. Sa clientèle est majoritairement concentrée en Europe.

- OneWelcome de Thales a obtenu des résultats inférieurs à la moyenne dans les cas d'utilisation non essentiels de l'authentification des utilisateurs, notamment en raison de l'absence de protection native contre les mots de passe compromis.

Fournisseurs ajoutés et supprimés

Nous révisons et ajustons nos critères d’inclusion pour les Magic Quadrants à mesure que les marchés évoluent. En raison de ces ajustements, la composition des fournisseurs dans n'importe quel Magic Quadrant peut changer au fil du temps. L'apparition d'un fournisseur dans un Magic Quadrant une année et non l'année suivante n'indique pas nécessairement que nous avons changé notre opinion à l'égard de ce fournisseur. Cela peut être le reflet d'un changement sur le marché et, par conséquent, d'un changement de critères d'évaluation, ou d'un changement d'orientation de la part de ce fournisseur.

Ajoutée

- Confier

- Texte ouvert

- Thalès

Abandonné

Micro Focus a été abandonné car son acquisition par OpenText est désormais finalisée (en janvier 2023).

Critères d'inclusion et d'exclusion

Cette recherche sur le Magic Quadrant et les capacités critiques identifie puis analyse les fournisseurs les plus pertinents et leurs produits sur un marché. Par défaut, Gartner applique une limite supérieure de 20 fournisseurs afin de fournir une liste concise des fournisseurs les plus pertinents sur un marché.

Pour être éligibles à l'inclusion, les fournisseurs devaient :

- Ant commercialisé et vendu des produits et services généralement disponibles au cours de leur exercice 22 pour soutenir à la fois la main-d'œuvre (B2E) et externe (B2B, B2C, G2C ou B2B2x). Les solutions sans nombre de clients substantiel pour chaque cas d'utilisation, ou qui sont commercialisées uniquement ou principalement pour prendre en charge un cas d'utilisation, sont exclues.
- Posséder la propriété intellectuelle des produits et services AM qu'ils vendent. Les fournisseurs qui revendent les produits d'autres fournisseurs, ou qui ont simplement augmenté les produits et services AM d'autres fournisseurs pour la revente, ou pour des offres de services gérés ou hébergés, sont exclus.
- Avoir soit :
  - Revenu annuel de 60 millions de dollars provenant des produits et abonnements AM (y compris les revenus de maintenance mais hors revenus des services professionnels) au cours de l'exercice 22.
  - Au moins 1 100 clients AM actuels au 5 juin 2023. Il doit s'agir d'organisations clientes AM distinctes (c'est-à-dire des « logos nets », ce qui signifie que différentes unités commerciales ou dépendances de la même entreprise ne doivent pas être comptées comme un client distinct). Ils ne doivent pas être clients d'autres produits et doivent avoir leurs propres contrats avec le vendeur. Les clients non payants (ceux qui utilisent les solutions gratuitement ou « freemium ») ne sont pas inclus dans le total des clients.
- Avoir des capacités mondiales avec les clients, des capacités de livraison et de support sur tous les principaux marchés : Amériques (Amérique du Nord et Amérique du Sud combinées), EMEA et Asie/Pacifique (y compris le Japon). Les fournisseurs doivent avoir des clients sur chaque marché, avec pas plus de 80 % de leur nombre de clients ou de leurs revenus dans leur région principale.

En outre, les fonctionnalités principales du produit/service AM du fournisseur doivent répondre aux cinq exigences fonctionnelles suivantes, **livrées en tant que produit SaaS** :

- **Services d'annuaire :** doivent fournir, au minimum, un annuaire ou un référentiel d'identités pour le personnel et les utilisateurs grand public, y compris des services de synchronisation d'identité et une prise en charge SCIM entrante.

- **Identity administration:** Must provide basic life cycle management capabilities with AD sync, SCIM (outbound) provisioning capabilities. It also must include ways to invite and register external users, enable profile management, and support basic consent-based flows for registration.
- **Single sign-on (SSO) and session management:** Must provide a workforce launchpad of applications or application gallery for SSO and support standard identity protocols (OpenID Connect and SAML). Session management must include capabilities and granularity, according to which the AM tool can control session state for user-present interactions with applications. The AM tool should also be able to control the ability to manage session times by issuing and refreshing time-limited access tokens (or cookies), and the ability to terminate sessions. It must provide, at minimum, a global setting for session management and single logout. Lastly, it must provide capabilities to enable access, authentication and SSO to applications that do not support standard identity protocols, using technologies like proxy services, agents or other mechanisms.
- **User authentication:** Must provide different user authentication methods, including MFA. Minimal MFA requirements should include out-of-band simple message service (SMS), one-time password (OTP) phone-as-a-token (app), and mobile push.
- **Authorization:** Include capabilities to implement authorization decisions and enforcement, create policy and provide sources of stored and contextual data used to evaluate risk and dynamically render access decisions. Provide native support for standard authorization protocols, including OAuth 2.0.

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

- AM products that cannot support, or are not marketed to support, both internal (B2E) and external (B2B, B2C, G2C or B2B2x) use cases. For example, solutions without substantial customer numbers for each use case, and those that are only or mostly marketed to support one use case, will be excluded.
- Pure user authentication products and services, or products that began as pure user authentication products and were then functionally expanded to support SSO via SAML or OpenID Connect, but cannot manage sessions or render authorization decisions. For more information on this market, see **Market Guide for User Authentication**.
- AM offerings that are only or predominantly designed to support operating systems, IT infrastructure and/or privileged access management (for more information on this market, see **Magic Quadrant for Privileged Access Management**).
- Remote or on-premises “managed” AM; that is, services designed to take over management of customers’ owned or hosted AM products, rather than being provided through delivery of the vendor’s own intellectual property.

- AM functions are provided only as part of a broader infrastructure or business process outsourcing agreement. AM must be provided as an independently available and priced product or service offering.
- AM products that are only or predominantly provided as open-source offerings.
- Stand-alone IGA suites, which are full-featured IGA products that offer the complete range of IGA functionality, without embedded AM capabilities. This is a separate but related market covered by other Gartner research (see **Market Guide for Identity Governance and Administration**).
- Full life cycle API management. This is a separate but adjacent market covered by other Gartner research (see **Magic Quadrant for API Management**).
- Endpoint protection platforms (EPPs) or unified endpoint management (UEM). EPP and UEM are separate but related markets covered by other Gartner research (see **Magic Quadrant for Endpoint Protection Platforms**).
- Cloud access security brokers (CASBs), which represent a separate but related market covered by other Gartner research.

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

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

Honorable Mentions

Vendors Covering All Assessed AM Use Cases

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

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

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

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

Vendors Covering Only CIAM

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

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

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

Cloud Platform Vendors

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

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

Google: Google Cloud Platform and Google Workspace provide SSO, MFA, directory services and related AM features for Google Cloud customers. Google was not included in this Magic Quadrant due to not meeting the technical inclusion criteria.

Evaluation Criteria

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

Ability to Execute

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

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

Subcriteria:

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

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

Subcriteria:

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

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

Subcriteria:

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

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

Subcriteria:

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

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

Subcriteria:

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

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

Subcriteria:

- Technical support
- Professional services
- Customer satisfaction

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

Subcriteria:

- People
- Processes
- Organizational changes

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Low

Evaluation Criteria ↓	*Weighting* ↓
As of October 2023	

Source: Gartner (November 2023)

Completeness of Vision

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

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

Subcriteria:

- Competitors
- Strengths and weaknesses
- Market opportunities
- Threats

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

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

Subcriteria:

- Marketing strategy and brand awareness
- Customer sentiment

Sales Strategy: A sound sales strategy uses the appropriate networks, including direct and indirect sales, marketing, service and communication. Partners extend the scope and depth of

market reach, expertise, technologies, services and their customer base.

Subcriteria:

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

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

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

Subcriteria:

- Product roadmap
- Differentiation

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

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

Subcriteria:

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

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or preemptive purposes. We consider the vendor's continuing track record in market-leading innovation and differentiation. This includes the provision of distinctive products, functions, capabilities, pricing models, acquisitions and divestitures. We focus on technical and nontechnical innovations introduced since last year, as well as the vendor's future innovations over the next 18 months.

Subcriteria:

- Near-term innovations related to trends (18 months)

- Longer-term innovation (18+ months)

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

Subcriteria:

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

Table 2: Completeness of Vision Evaluation Criteria

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

Evaluation Criteria ↓	*Weighting* ↓
As of October 2023	

Source: Gartner (November 2023)

Quadrant Descriptions

Leaders

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

Challengers

Challengers show strong execution, complete and specialized product features, and have significant customer bases. However, they have not shown the Completeness of Vision for AM that Leaders have. Rather, their vision and execution for marketing, technology, methodology and/or means of delivery tend to be more focused on sales execution and doubling down on strengths of adjacent IAM capabilities, rather than making large investments in AM innovation. Challengers may see AM as a key part of a broader IAM portfolio. Challengers' clients are relatively satisfied.

Visionaries

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

Niche Players

Niche Players provide AM technology that is a good match for specific use cases. They focus on market segments by customer size, typically offering AM add-on capability to other products used by their existing customer base. They can outperform many competitors in their specific area of focus. Vendors in this quadrant often have large customers, as well as a strong specialization in some areas of AM (for example, user authentication). Brand awareness of their AM product is usually low relative to vendors in other quadrants. Vision and strategy may not extend much

beyond feature improvements to current offerings. Some Niche Players' pricing might be considered too high for the value they provide. However, inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused spectrum. Niche solutions can be very effective in their areas of focus.

Context

Workforce AM Is Mature, CIAM Is Growing

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

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

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

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

Given this, when evaluating AM tools:

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

AM Is Evolving Its B2B Capabilities

Business customers and partners now routinely use more digital services, conduct more complex and sensitive interactions, and otherwise engage more deeply with organizations online. This has resulted in the increasing need for flexible, delegated life cycle management for B2B users. Consider the following questions when dealing with B2B relationships:

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

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

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

Recommendations when evaluating AM vendors to support B2B use cases:

- Choose AM tools that support both B2B and B2C features when the organization has requirements for enabling business customer relationships that consist of both larger companies and sole proprietorships.
- Focus on delegated administration, identity federation, flexible identity management including life cycle management and provisioning/deprovisioning, extensible user account schema, OOTB delegated admin roles, and dedicated B2B customer subtenants' key features.
- Choose a solution that offers a wide range of authentication methods for B2B users. Augment with recognition and risk signals to address account takeover (ATO) risk, to meet cyber insurance requirements and to protect intellectual property.
- Augment your chosen AM tool with an IGA tool, or privacy management solution if needed, for more complex and highly regulated governance requirements for B2B users.
- If you find that your B2B requirements do not align well with the vendors covered in this Magic Quadrant, be quick to pivot; consider approaching CIAM vendors highlighted in the Honorable Mentions section of this research or other CIAM specialist vendors.

AM Is Still Under Attack

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

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

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

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

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

Recommendations when evaluating AM vendors:

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

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

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

IAM Vendor Consolidation and Convergence Is a Mixed Bag

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

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

Recommendations when evaluating AM vendors:

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

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

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

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

Effective Passkeys Support Needs More Than Just WebAuthn

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

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

However, the types differ in the following ways:

- Device-bound passkeys are highly recommended as a phishing-resistant authentication factor, especially for workforce use cases (see **Hype Cycle for Digital Identity, 2023** and **Innovation Insight for Many Flavors of Authentication Token**).
- Multidevice passkeys require an ecosystem account (Apple ID, Google Account or Microsoft account), passkey-capable hardware (PC, smartphone, tablet or security key), a compatible operating system and a compatible browser (to support cross-device authentication or to access passkeys from the native secure element).
- The benefits of synced passkeys are: quick user registration (if used, the ecosystem’s user identity is already known), improved UX (passwordless, as simple as unlocking the device), trust (phishing-resistant) and recovery (automatically backed up and synced). These benefits should be balanced against the following challenges:
  - Device-bound and synced passkeys have different user journeys (prerequisites, compatibility, benefits, etc.)
  - Identity trust is rooted in the process that the ecosystem vendor uses for IDV and authentication.
  - Passkey availability and recoverability are dependent on the mechanisms and infrastructure of the vendor ecosystem.
  - Synced passkeys are no longer solely in the possession of the end user (or on an organization-managed device).

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

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

Recommendations when evaluating AM vendors:

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

OAuth 2.0 Is Often Not Enough for All Authorization Use Cases

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

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

Recommendations when evaluating AM vendors:

- Carefully identify your authorization requirements, including a broad set of authorization use cases, for example:
  - Customer authorization of data sharing with applications and services
  - API flow authorization
  - Workforce authorization to specific applicationsAuthorization to functions inside applications and resources
  - Authorization to data within an application or resource

- Compare your use cases with vendor capabilities, being mindful of authorization use cases that cannot be addressed with OAuth 2.0. If you have only use cases for which OAuth 2.0 works, then this will likely not be a significant differentiator for you. If your use cases extend beyond what OAuth 2.0 can handle, look to vendors that offer full EAM capabilities. We have called out vendors with strengths and cautions for authorization.

Market Overview

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

- **Maturing of workforce AM, growth in CIAM —** All vendors evaluated offer a SaaS-delivered product, and for vendors that offer multiple delivery models, only its SaaS product has been rated for the Product/Service criterion of this Magic Quadrant. Workforce AM is a maturing use case that is getting commoditized. Fifty-eight percent of survey respondents with some involvement or responsibility in their organization's IAM have deployed workforce AM in 2023.1 Uptake in CIAM solutions is at 49%,1 an increase from 40% four years ago. Growth potential for CIAM is higher than workforce and there is significant demand from client organizations moving from homegrown CIAM.

- **Evolution of B2B CIAM —** 45% of all AM vendors surveyed in this research offer OOTB features to invite and register B2B users by delegating user registration to an internal user in the parent organization and to a delegated administrator in a partner organization. However, 64% of AM vendors evaluated still don't offer OOTB-delegated administrator roles and access certifications for delegated administrators.

- **ITDR and identity hygiene —** 63% of vendors evaluated have released some sort of ITDR capability, an increase from 44% last year. However, the majority of AM tools do not provide an

indication of identity data hygiene, much less misconfigurations in the tool itself, vulnerabilities or gaps in their deployment, which creates an exposed, unmonitored attack surface.

- **IAM suites and convergence** — 73% of AM vendors evaluated also offer adjacent IAM capabilities (IGA and PAM specifically). This is up from 66% just last year. However, most vendors offering solutions for adjacent capabilities deliver this as separate stand-alone products rather than a true converged platform.

- **Passkeys** — All vendors surveyed provide basic passkey-compatible WebAuthn API support, and 45% claimed support for multidevice passkeys. However, the depth of support for multidevice passkeys is uneven — 27% of all vendors have mentioned multidevice passkeys as a roadmap item.

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

Evidence

[1] **2023 Gartner IAM Modernization Preventing Identity-First Security Survey**. This survey was conducted to determine how far along the market is moving in toward identity first security. The survey was conducted online from 9 June to 24 July 2023 among 303 respondents from North America (n = 104 in the U.S. and Canada), Latin America (n = 41 in Brazil), Asia/Pacific (n = 59 in India, Australia and Singapore) and EMEA (n = 99 in Germany, France and U.K.). Respondents' organizations had $100 million or more in 2022 enterprisewide annual revenue and 250 or more employees. Respondents were required to have some involvement in their organizations' identity and access management and planning to have at least one among workforce, consumer or machine/nonhuman IAM in their organization within the next two years. Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

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

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

2022 Gartner CISO: Security Vendor Consolidation XDR and SASE Trends Survey: This study was conducted to determine how many organizations are pursuing vendor consolidation efforts, what the primary drivers are for consolidation, expected or realized benefits of vendor consolidation, and how those who are consolidating are prioritizing their consolidation efforts. The primary purpose of this survey was to collect objective data on extended detection and response (XDR) and secure access service edge (SASE) for consolidation of megatrend analysis. The research was conducted online during March and April 2022 among 418 respondents from North America (n = 277 in the U.S., Canada), Asia/Pacific (n = 37 in Australia and Singapore) and EMEA (n = 104 in France, Germany and the U.K.). Results were from respondents with $50 million or more in 2021 enterprisewide annual revenue. Industries surveyed included manufacturing, communications and media, information technology, government, education, retail, wholesale trade, banking and

financial services, insurance, healthcare providers, services, transportation, utilities, natural resources, and pharmaceuticals, biotechnology and life sciences. Respondents were screened for job title, company size, job responsibilities to include information security/cybersecurity and IT roles, and primary involvement in information security. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Note 1: What You Need to Know

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

AM can be used by:

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

Pricing

We comment on the pricing of individual products based on a relative scale, using terms such as “well-above average,” “above average,” “average,” “below average” and “well-below average.” In each pricing scenario, the average is the mean/median value of the pricing for all vendors evaluated in this research:

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

Resilience

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

Workforce Versus CIAM Use Cases

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

Passkeys

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

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

Orchestration

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

Identity Verification

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

Evaluation Criteria Definitions

Ability to Execute

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

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

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

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

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and

organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

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

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

Completeness of Vision

Compréhension du marché : Capacité du vendeur à comprendre les attentes des acheteurs. désirs et besoins et les traduire en produits et services. Les fournisseurs qui font preuve du plus haut degré de vision écoutent et comprennent les acheteurs. désirs et besoins, et peut les façonner ou les améliorer grâce à leur vision supplémentaire.

Stratégie marketing : Un ensemble de messages clairs et différenciés communiqués de manière cohérente dans toute l'organisation et externalisés via le site Web, la publicité, les programmes clients et les déclarations de positionnement.

Stratégie de vente Stratégie de vente de produits qui utilise le réseau approprié d'affiliés de vente directe et indirecte, de marketing, de service et de communication qui étendent la portée et la profondeur de la portée du marché, les compétences, l'expertise, les technologies, les services et la clientèle.

Stratégie d'offre (produit) : Approche du fournisseur en matière de développement et de livraison de produits qui met l'accent sur la différenciation, les fonctionnalités, la méthodologie et les ensembles de fonctionnalités en fonction des exigences actuelles et futures. .

Modèle commercial : La solidité et la logique de la proposition commerciale sous-jacente du fournisseur.

Stratégie verticale/sectorielle : Stratégie du fournisseur visant à orienter les ressources, les compétences et les offres pour répondre aux besoins spécifiques de segments de marché individuels, y compris les marchés verticaux.

Innovation : Agencements directs, connexes, complémentaires et synergiques de ressources, d'expertise ou de capital à des fins d'investissement, de consolidation, défensives ou préventives.

Stratégie géographique : La stratégie du fournisseur visant à orienter les ressources, les compétences et les offres pour répondre aux besoins spécifiques des zones géographiques en dehors du « domicile » ou zone géographique d'origine, soit directement, soit par l'intermédiaire de partenaires, de canaux et de filiales, en fonction de cette zone géographique et de ce marché.

Gartner