Critical Capabilities for Access Management

Published 9 November 2021 - ID G00740721 - 49 min read

By Analyst(s): Abhyuday Data, Michael Kelley, Henrique Teixeira

Initiatives: Identity and Access Management and Fraud Detection

AM tools are increasingly adopted by security and risk management leaders for providing centralized authentication, adaptive access, authorization enforcement and single sign-on to target applications/services. To enable secure access to target systems.

This Critical Capabilities is related to other research:

Magic Quadrant for Access Management

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- Among all identity and access management (IAM) markets, access management (AM) has been leading the charge to offer converged IAM capabilities, typically SaaS-delivered.
- High availability, effective resiliency, reduced need for support staff and dynamic scalability of AM services have become far more important, resulting in SaaS being the dominant delivery model for AM.
- Customer IAM (CIAM) continues to gain widespread popularity, with business-to-business (B2B) use cases in particular seeing accelerated demand.
- Balancing security and user experience (UX) to support multiple authentication factors for different use cases and different personas with lower total cost of ownership (TCO) for AM cases is challenging. This is driving the adoption of access orchestration capabilities, which consume both native and external signals in a low-code/no-code approach to build complex authentication and authorization flows.

Recommendations

Security and risk management (SRM) leaders responsible for IAM should:

- Prioritize single-vendor strategies for various AM use cases and carefully evaluate the roadmap of converged adjacent IAM capabilities in SaaS-delivered AM tools.
- Focus on vendors' offerings in terms of superior SLAs compared to other vendors, workarounds available in case of an AM service outage and dynamic scalability for AM use cases.
- Assess the growing overlap of B2B and CIAM offerings and carefully evaluate B2B-specific functionalities like delegated administration, mature identity federation, flexible identity management and JIT provisioning features to leverage a single-vendor offering for all external AM use cases.
- Begin to evaluate low-code/no-code approaches offered by AM tools for orchestrating authentication and authorization flows to solve issues related to the cost and complexity of integrating and maintaining disparate IAM products and services.

What You Need to Know

IAM-focused SRM leaders (hereafter IAM leaders) frequently evaluate and implement AM tools to secure and streamline runtime access to target applications/services for internal and external users' access use cases. Targets may have traditional web application architectures, using web browsers and web application servers. Targets may also include APIs and machine identities that consist of workloads or devices running on customers' premises or in the cloud.

Along with the core capabilities offered by AM tools (see Note 1), Gartner sees AM vendors continue to add limited capabilities from adjacent markets, such as identity governance and administration (IGA) and privileged access management (PAM). Additional capabilities for IGA include identity administration, provisioning, identity analytics and maturing identity governance features.

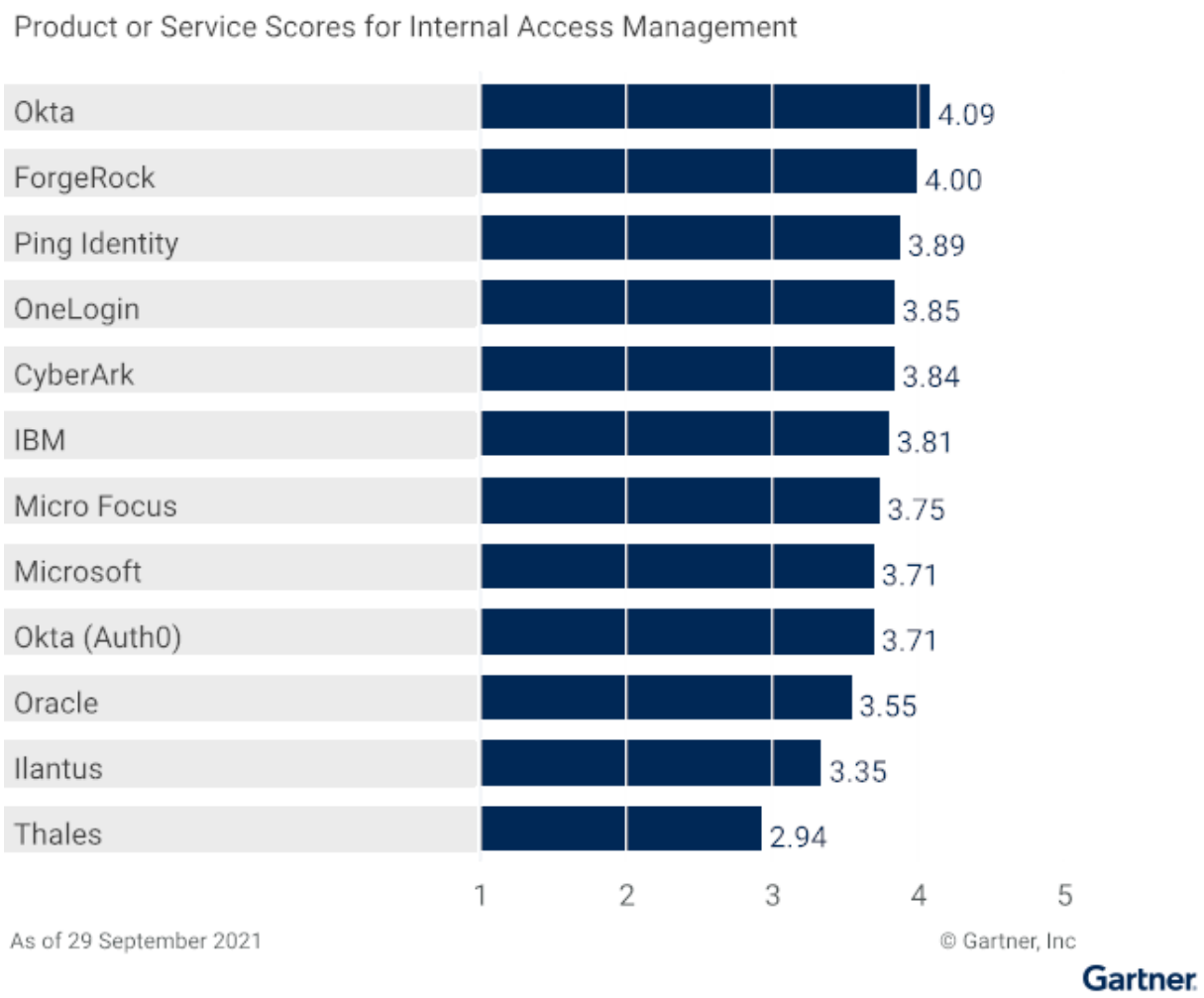
For this Critical Capabilities research, we have defined three use cases in terms of two distinct constituencies: internal identities (workforce and extended workforce, excluding gig workers) and external identities (B2B [including vendors and business partners], gig workers, CIAM and G2C). Although there will be some specialization for the various user communities in each constituency, features and functionalities can be loosely, but accurately, grouped according to these definitions.

This research evaluates vendors on 12 distinct critical capabilities that organizations need in order to support the above mentioned use cases (see the Critical Capabilities Definition section below). IAM leaders should use this research as a companion to the Magic Quadrant for Access Management to understand the key use cases and capabilities of enterprise AM tools and to compare vendor offerings. They should also evaluate vendors' product roadmaps and alignment with long-term business goals.

Analysis

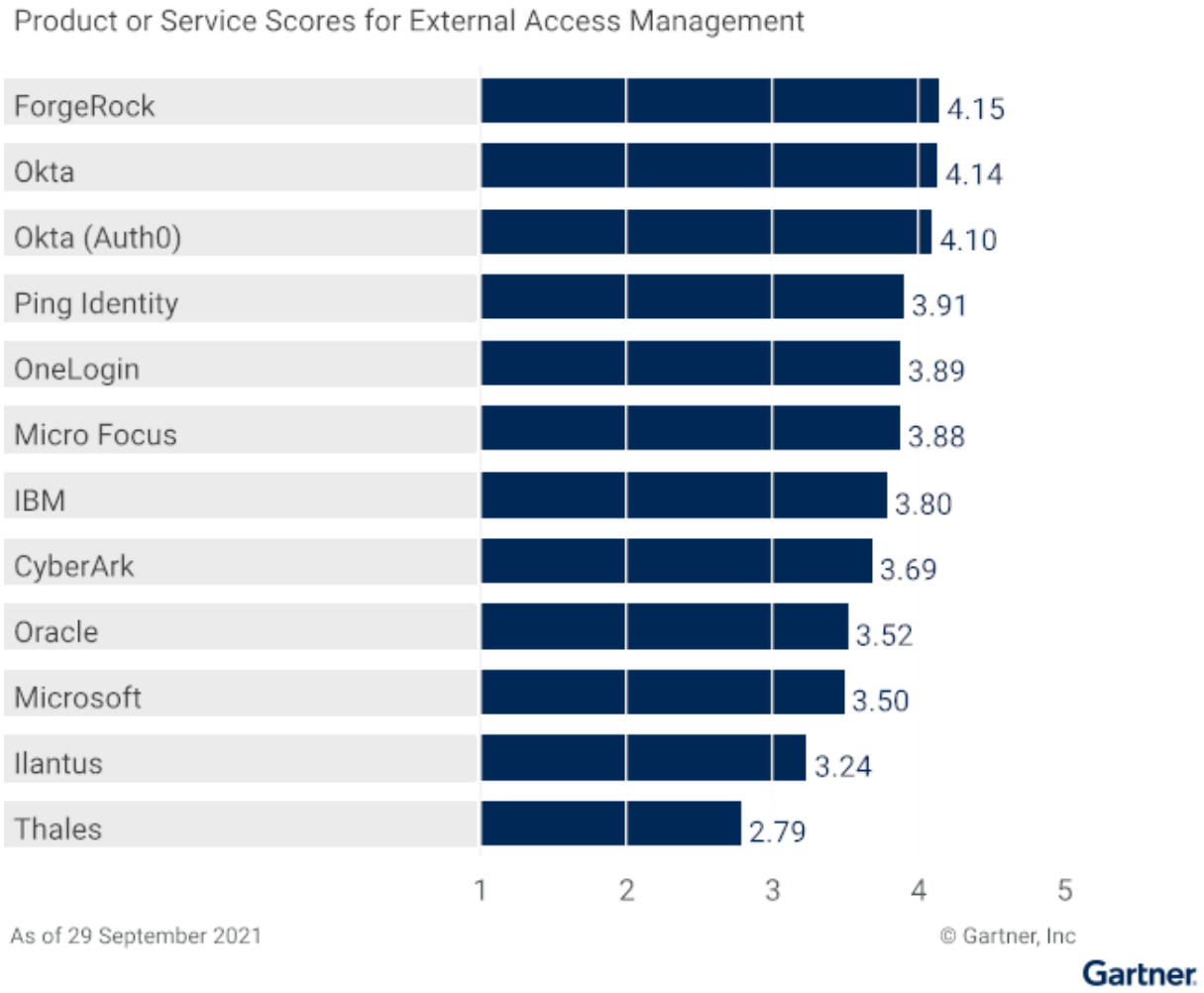
Critical Capabilities Use-Case Graphics

Vendors' Product Scores for the Internal Users Access Management Use Case



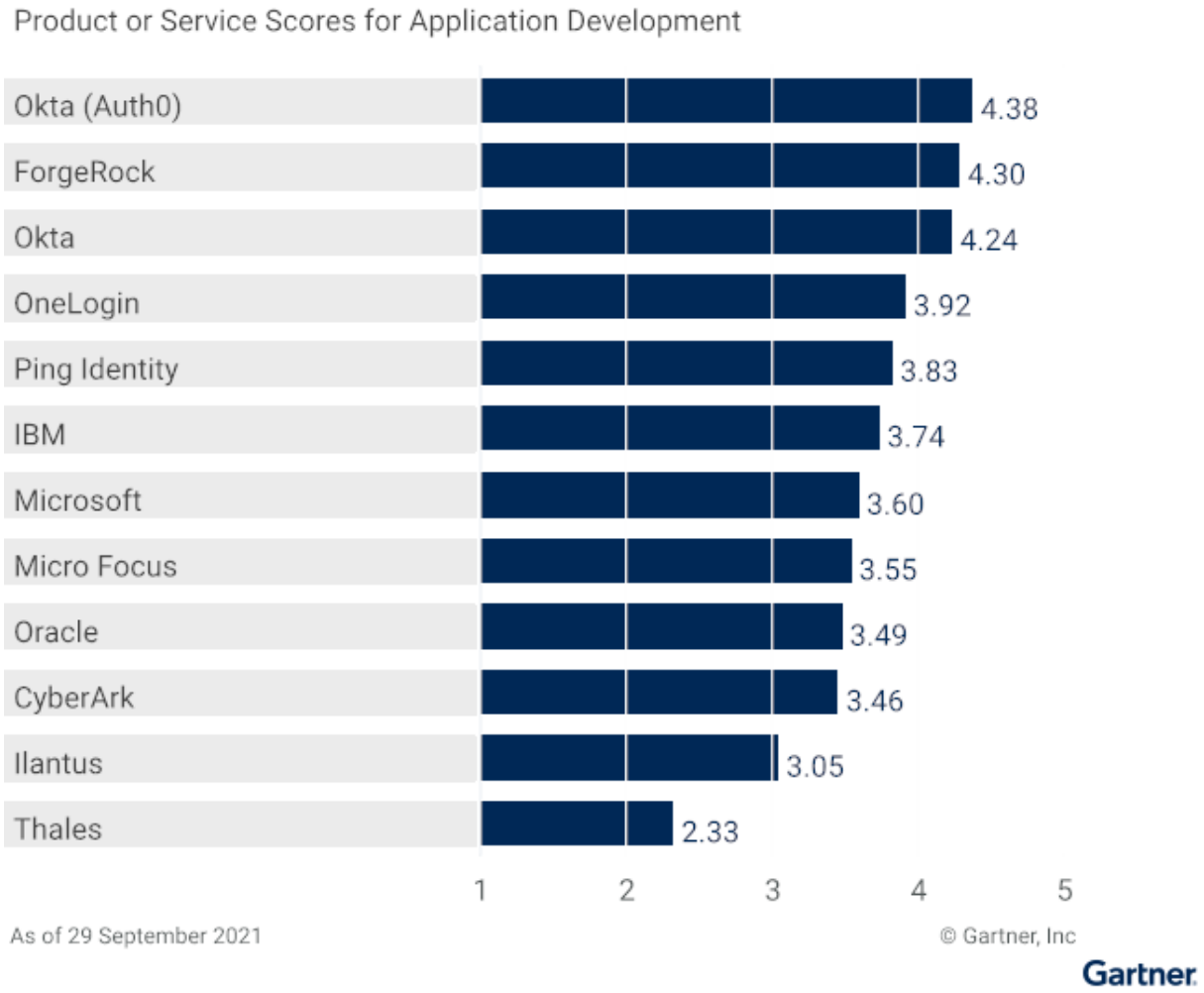
Source: Gartner (November 2021)

Vendors' Product Scores for the External Users Access Management Use Case



Source: Gartner (November 2021)

Vendors' Product Scores for the Application Development Use Case



Source: Gartner (November 2021)

Vendors

CyberArk

CyberArk AM products are SaaS-delivered. It offers CyberArk Identity Standard Single Sign-On and Adaptive Single Sign-On, and Identity Standard Multi-Factor Authentication and Adaptive Multi-Factor Authentication products under the Access portfolio of its Identity Security Platform.

CyberArk enhanced its AM functionalities by including passwordless capabilities using QR codes for registration and authentication, an endpoint agent to expand MFA capability to desktops and servers and identity affirmation services through a partnership with Ekata (acquired by Mastercard) for external AM use cases.

For external AM use cases, user self-service is above average, as it offers easy-to-enable customer journeys for registration, profile management and setup for basic consent management. API access control is below average, as developer self-service tools are very basic, it does not offer a visual flow designer, and it requires custom integration with external API gateways for implementing consent, scope to claims mappings or sidecars. Security, resilience and coverage is average, with relatively inferior SLAs compared to competitors. BYOI integration is below average, with limited OOTB plug-ins for social IDs and none available for decentralized IDs, government eIDs and bank IDs.

For internal AM use cases, identity administration is average. For authorization and adaptive access, CyberArk offers adaptive authentication and, although it does offer a workflow product for provisioning, it doesn't offer access orchestration for authentication and authorization. It also offers a comprehensive set of contextual signals and some built in UEBA functionality. Session management is above average, as it offers granular controls and per-application settings.

User authentication is above average, with a breadth of authentication methods supported. Analytics is above average, as it can also consume external user analytics and risk signals and use that for adaptive access flows. It also offers over 70 OOTB reports and the ability to create custom reports. Standard application and nonstandard application enablement is average compared to competitors.

CyberArk received its highest score for the internal AM use case. It is rated above average for the internal AM use case, average for the external AM use case and below average for the application development use case.

ForgeRock

ForgeRock offers the ForgeRock Access Management product as part of its ForgeRock Identity Platform. The software product consists of multiple modules, such as Intelligent Access, Single Sign-on, Identity Federation and User Self Service. ForgeRock also sells a separate API gateway product, Identity Gateway (IG). It also offers Identity Cloud as a SaaS-delivered AM product available in different editions.

ForgeRock enhanced its AM functionalities by including advanced support for B2B2C/B2B2E scenarios and a feature for developers' authorization to data streams.

For external AM use cases, user self-service is above average, as it offers prebuilt self-service flows and strong orchestration capabilities with a visual flow designer (ForgeRock Trees). It is easy to enable customer journeys for registration, profile management and setup for basic consent management. BYOI integration is above average, as it offers OOTB plug-ins for many social IDs and cloud service provider IDs, with user-driven consent flows supported. Security, resiliency and coverage is above average as customers can choose between 15 regions for Identity Cloud, tenants are completely isolated from each other (data layer to execution layer), and identity data stays in the preferred region. They offer a 99.95% SLA and only had five minutes of outages last year. API access control is also above average, as it offers mature embedded advanced capabilities for API access control, like token exchange, proof-of-possession support, micro gateways and microservices for token validation. It also offers a very intuitive mobile app integration for developers.

For internal AM use cases, identity administration is above average, as it offers good directory services features for managing large-scale user populations and robust life cycle management capabilities. For authorization and adaptive access, it supports common contextual signals for authorization decisions and provides a low-code/no-code approach for access orchestration, using internal and external signals. Session management is above average, with good granularity and the ability to reanalyze session data in session through a variety of token manipulation techniques but missing UEBA capabilities.

User authentication is average where it is missing support for out-of-band (OOB) voice modes. Analytics is average. Standard application enablement is also average. Nonstandard application enablement is above average, as it offers low-code or framework approaches for integration with nonstandard apps and endpoints using Trees.

ForgeRock received the highest score for the external AM use case. It also performs solidly for all the other use cases evaluated in this research.

IBM

IBM offers IBM Security Verify Access as a software-delivered AM product. The SaaS-delivered AM functionality is available as part of IBM Security Verify SaaS.

IBM enhanced its AM functionalities by including an SDK for adaptive access user journeys, a containerized version of its proxy, and new data privacy and consent management features.

For external AM use cases, user self-service is below average, as even basic profile management for CIAM is not supported OOTB and requires customization. IBM's SaaS product does not offer OOTB prebuilt flows for registration; however, basic consent management is supported. BYOI integration is average. Security, resiliency and coverage is above average, with good security controls for IBM data centers, and geographic presence is diverse, including China. It had no long-standing outages registered in the last year, even though it only provides a 99.9% SLA. API access control is above average, as it provides good support for API OAuth 2.0 flows, except OAuth 2.0 Mutual Transport Layer Security (mTLS) client authentication. IBM offers support for Docker, Kubernetes and OpenShift deployments (using its software product), which is also available on the AWS marketplace and Docker Hub. Verify SaaS has extensions to allow Red Hat SSO and Keycloak clients to integrate with IBM Security Verify for more MFA capabilities.

For internal AM use cases, identity administration is above average, as it offers one of the best identity sync capabilities, with inbound and outbound SCIM sync and WebHook support. Authorization and adaptive access is below average. IBM can offer a good set of contextual signals for adaptive authentication but will require additional licenses for Trusteer and MaaS 360 for IBM Verify Access. Only IBM Verify SaaS offers granular session management that can be applied on an application-by-application basis. Access orchestration is not available with either product. Session termination is also different with the software product and far more robust than the SaaS product. For additional visibility, and in some cases to provide comparable session management functionality to other vendors, clients should plan to use the IBM gateway proxy (included with Verify).

User authentication is above average, with a breadth of authentication methods supported. Analytics is above average, as it offers robust risk scoring and anomaly detection backed by integration with IBM X-Force Red (IBM's ethical hacking services), automatic identification of dormant accounts, orphaned accounts and access that has not been recertified (all without additional cost). Nonstandard application enablement is average. Standard application enablement is slightly above average, as IBM offers an extensive list of OOTB SSO connectors for SaaS apps.

IBM received its highest score for internal AM use case. It is rated above average for the internal and application development use cases but average for the external AM use case.

Ilantus

Ilantus offers the Compact Identity product, which is mainly focused on delivering AM as part of a converged SaaS IAM platform. Compact Identity offers the following AM modules: Access Management, Identity Administration and Passwordless Authentication.

Ilantus enhanced its AM functionalities by including a risk engine, more granular context-based authentication and an access management bundle offering tailored to midsize enterprises and accompanying professional services packages for implementation.

For external AM use cases, user self-service is average but API access control is below average, as it doesn't offer developer self-service tools, a visual flow designer, nor support for OAuth 2.0 mTLS, device flow, token exchange, introspection and revocation. BYOI integration is also below average, as it only supports a few OOTB plug-ins for social IDs, and for other approaches it only supports SAML-compliant identity providers (IDPs). Security, resiliency and coverage is also below average. Even though the service runs in AWS, it is not readily available in most regions, and there is no public page that tracks global availability of its services.

For internal AM use cases, identity administration is above average, with strong directory services and identity sync and replication capabilities, including inbound SCIM. For authorization and adaptive access, Ilantus requires the purchase of an additional MFA product that supports adaptive access controls and offers a good set of contextual signals. No access orchestration capability is available, and session management controls are basic, limited only to global settings.

User authentication is average. Analytics is below average, as all analytics insights provided are based on historical descriptive reports. It does not provide diagnostic, predictive or prescriptive analysis. Nonstandard and standard application enablement is also below average, as it does not offer any low-code or framework approaches for integration with nonstandard apps and endpoints other than APIs.

Ilantus received its highest score for the internal AM use case. However, it is rated below average for all the use cases evaluated in this research.

Ilantus did not respond to requests for supplemental information or a review of the draft contents of this research. Therefore, Gartner analysis is based on other credible and accepted public sources.

Micro Focus

Micro Focus offers NetIQ Access Manager as software. For SaaS-delivered AM functionality, Micro Focus offers the following modules: Advanced Authentication Service, Single Sign-On Service and Access Gateway Service.

Micro Focus enhanced its AM functionalities by including its first AM SaaS modules, additional DevOps capabilities with risk-based controls for its API management tool and extension of MFA capabilities to nonweb targets.

For external AM use cases, user self-service is average. Security, resiliency and coverage is below average for the three SaaS modules available so far, and they are only available in North America and European regions. BYOI integration is above average, and it scored the highest in this category as it supports various OOTB plug-ins for BYOI mechanisms through social IDs, government eIDs, bank IDs and cloud service provider IDs. API access control is below average where most developer activities are through scripting interfaces, and there are no access orchestration or visual flow abilities. Most API access control features are only available in NetIQ Access Manager.

For internal AM use cases, identity administration is above average, with strong directory services and support for inbound SCIM. For authorization and adaptive access, only the SaaS product supports externalized authorization management, but Micro Focus does offer a comprehensive set of contextual signals, including native UEBA features when used in conjunction with the separately priced Interset product, for adaptive access approaches. Session management is above average, offering granular controls for both global and application-by-application settings.

Micro Focus supports a breadth of authentication methods with its Advanced Authentication service SaaS product, including its own proprietary biometric method. Only the QR code scan for registration/enrollment flows is missing. Analytics is below average, as it is difficult to extract analytics insights and will require three different products: NetIQ AM, NetIQ IGA and ArcSight. Nonstandard application enablement is average. Standard application enablement is above average, as it offers a reasonable catalog of OOTB SSO connectors to SaaS apps.

Micro Focus received its highest score for the internal AM use case. It is rated average for internal and external AM use cases but below average for the application development use case.

Microsoft

Microsoft's AM product, Azure AD, is sold in bundles, focused on delivering AM as part of a converged SaaS IAM platform. It offers Azure AD Premium for internal AM use cases available in two editions, Premium1 (P1) and Premium2 (P2), and Azure AD External Identities for external AM use cases. Microsoft also offers some basic AM functionality as part of O365 bundled licenses.

Microsoft enhanced its AM functionalities by including support for FIDO2, an agent for synchronization with disconnected AD forests to enable use cases, such as joining two domains during a merger or acquisition, and adaptive access for CIAM scenarios.

For external AM use cases, user self-service is below average. Microsoft offers limited B2B support with basic customization abilities for B2B user flows and relatively basic delegated administration capabilities, mostly focused on frontline worker enrollment, rather than on external B2B scenarios. BYOI integration is below average, with limited OOTB support for social IDs compared to competitors, and no OOTB plug-ins are available for other BYOI through government IDs or bank IDs. However, Microsoft is one of the only few AM vendors working on a native decentralized identity (DCI) product. Its Verifiable Credentials product is in public preview. Security, resiliency and coverage is also below average, as Azure AD suffered long-standing outages last year of over 14 hours combined. There are no good workarounds for failing over from cloud to on-premises compared to competitors that offer that for nonstandard apps.

For internal AM use cases, identity administration is below average, as it offers limited support to external authoritative sources of identity. Microsoft Identity Manager (MIM), a software product, is needed for most attribute linking and directory synchronization with non-AD sources. Account linking requires custom policies, and Azure AD also offers very basic identity administration capabilities with a three-step approval workflow. For authorization and adaptive access, Microsoft's conditional access rules offer a comprehensive set of prebuilt adaptive access rules, even though its contextual access signals are missing a number of inputs from endpoints and phones. Clients with Intune, a unified endpoint management product, can gain back a number of those endpoint signals. While users can build their own conditional access rules, it does not offer access orchestration as compared to competitors. Session management controls are below average, lack capabilities compared to other vendors and have only global settings available. Microsoft has begun offering continuous access evaluation protocol (CAEP) for access to Microsoft applications, which provides additional inputs and controls.

User authentication is below average, with missing support for both X.509 software and hardware tokens. Analytics is above average, as it offers a good error resolution tool for access event log troubleshooting. Obtaining analytics insights is complex and requires several steps but offers rich information. Nonstandard application enablement is average, with the addition of HTTP header-based authentication in Azure AD Application Proxy. For standard application enablement, it offers an extensive set of OOTB SSO connectors to SaaS apps via Azure AD app gallery.

Microsoft received its highest score for the internal AM use case. It is rated average for the internal and application development use cases but below average for the external AM use case.

Okta

Okta offers a SaaS-delivered AM platform. It sells its functionality in two editions — IT Products, intended for internal AM use cases, and API Products, intended for the developers and external AM use cases. Okta acquired Auth0 in May 2021.

Okta enhanced its AM functionalities by including no-code identity orchestration (provisioning and access requests) through Okta Workflows for Customer Identity, new Federal Risk and Authorization Management Program (FedRAMP) certifications and improvements to Okta Access Gateway.

For external AM use cases, user self-service is above average, as Okta offers strong B2B features, progressive profiling and basic consent. API access control is also above average, with good developer tools like its Okta Workflows, but support for OAuth 2.0 mTLS and device flows are missing. BYOI integration is above average. Along with supporting multiple global and regional social ID providers OOTB, Okta also integrates with SecureKey products to support BYOI mechanisms through decentralized IDs. Okta also obtained the highest score for security, resiliency and coverage. Okta offers a 99.99% availability SLA even for its free tiers and failover from cloud to on-premises.

For internal AM use cases, identity administration is average, with a good workflow product, but it has limited identity sync and replication capabilities with no inbound SCIM. Session management is above average, as those controls are extensive and granular, with both global and application settings available. Okta also provides contextual signals for adaptive access, only missing some endpoint signals, and while it does not offer native UEBA capabilities, its Threat Insight product provides an additional contextual signal from the Okta Identity Cloud. While Okta offers Okta Workflows for provisioning and access request workflows, that tool does not orchestrate authentication and authorization functions for access.

Okta scored above average for standard application enablement featuring an extensive catalog of more than 7,000 OOTB SSO connectors. It also offers coarse-grained access controls to SaaS apps. Okta has matured its functionality for nonstandard application enablement through Okta Access Gateway. Analytics is above average, with a very good offering for OOTB reports; however, in depth analysis requires exporting data to external tools. User authentication is also above average where Okta provides support for an extensive range of methods, but it is missing QR code scan for registration/enrollment flows.

Okta obtained the highest score among all vendors for its overall product capabilities and is one of the easiest-to-deploy AM tools. It excels in the internal AM use case and performs solidly for the other two use cases evaluated in this research.

Okta (Auth0)

Okta (Auth0) AM products are SaaS-delivered, with multitenant and private cloud options, sold as an all-inclusive bundle under the label of Auth0 Enterprise service. Auth0 was acquired by Okta in May of 2021, but it remains a separate product unit.

Auth0 enhanced its AM functionalities by recently including more B2B partner and customer management capabilities, platform extensibility, and embedded credential stuffing attack detection and remediation. It also included Fast Identity Online (FIDO)2/Web Authentication (WebAuthn) support last year.

For external AM use cases, user self-service is above average, as Auth0 offers interface customization and can host custom pages built by clients. It also offers strong consent and profile management features and B2B self-service flows with efficient delegated administration configuration. Security, resilience and geographical coverage is above average. Beyond the standard SaaS model, it also offers a private-cloud, single-tenant deployment option that can be either hosted by Auth0 or by the client itself in Amazon Web Services (AWS). Auth0 is very mature in regards to developer tools and offers the strongest features for API-driven AM deployments. Bring your own identity (BYOI) integration is above average, as it offers an extensive list of out-of-the-box (OOTB) plug-ins for social IDs. It also offers integrations with some government and digital bank IDs, including Danish NemID, Norwegian BankID, Swedish BankID and Scandinavian National through a partnership with Criipto Verify.

For internal AM use cases, identity administration is average. Auth0 is particularly weak for workforce scenarios. For example, Auth0 only offers basic features for integration with HR systems. Authorization and adaptive access is slightly above average, with externalized authorization for applications offered through APIs, but support for contextual signals is not as comprehensive as others, and there is no native user and entity behavior analytics (UEBA) capability. However, Auth0 Hooks and Rules offers some basic access orchestration capabilities for authentication and authorization exercises. (See authorization and adaptive access in the Critical Capabilities Definition section). Session management controls are granular, offering both global and application-by-application settings.

User authentication is above average, supporting a breadth and depth of authentication methods. Analytics is average compared to competitors. Though it offers good anomaly detection features and a dashboard with analytics, it lacks OOTB reports and relies on data exports to other tools. It scored average for standard application enablement. For nonstandard application enablement, Auth0's approach is limited and relies on an external identity-aware proxy or service providers, like F5's open-source NGINX libraries, AWS ALB, Apache, Okta Access Gateway or other third-party libraries.

Auth0 excels in the application development use case and performs solidly in the external AM use case. It is rated above average for external AM and average for internal AM use cases.

OneLogin

OneLogin offers SaaS-delivered AM products that are available in basic, advanced and professional bundles.

OneLogin enhanced its AM functionalities by including extensibility through a feature called Smart Hooks, new APIs and interfaces for delegated administration, a dashboard for identity security insights, and new developer tools for API access controls.

For external AM use cases, OneLogin offers above-average user self-service features, including strong B2B features, with the ability to create subtenants and granular access control and a new delegated administration UI. However, BYOI capabilities are just slightly above average, with not many OOTB plug-ins available, but it recently added Apple ID into its integrations list. Security, resilience and coverage is average. API access control is above average, as there are good options for developers looking for containerized deployments, and OneLogin is also available in the Terraform marketplace as well AWS, with good examples in GitHub.

For internal AM use cases, OneLogin scored above average for authorization and adaptive access, as it offers a competitive set of contextual signals, missing some endpoint inputs, along with missing interaction statistics as a contextual data point. However, its adaptive access functionality benefits from a native UEBA capability called Vigilance AI. Vigilance AI provides some additional information inside the session when contextual elements have changed. Identity administration is average. Session management controls are granular, supporting both global and application-level controls. It uses its Smart Hooks approach for access orchestration; however, this is not a low-code/no-code approach like other vendors offer.

User authentication is below average, with missing support for FIDO2 external software authenticators and X.509 phone tokens. Analytics is below average. Though it offers good canned reports and Vigilance AI service for threat detection, there are not a lot of options for easily extracting insight, and it offers limited support for diagnostic, predictive and prescriptive analytics. It also offers above average features for standard as well as nonstandard application enablement. For nonstandard, it provides agents or proxies to support SSO and session management for several hard-to-integrate applications, including OOTB-packaged SSO solutions for Oracle E-Business Suite (EBS), Oracle PeopleSoft, Atlassian JIRA and Atlassian Confluence.

OneLogin received its highest score for the application development use case. It is one of the easiest-to-deploy AM products and is also rated above average for the other two use cases evaluated in this research.

Oracle

Oracle offers Oracle Access Manager (OAM) as a software-delivered AM product. The SaaS-delivered AM functionality is available as part of Identity Cloud Service (IDCS).

Oracle enhanced its AM functionalities by including SaaS-based support for FIDO2, FedRAMP enhancements and deeper integration with Oracle cloud and enterprise applications.

For external AM use cases, user self-service is average, with features available for self-service profile management, registration and invitation for third-party identities. However, BYOI integration is below average, with limited OOTB plug-ins available for social IDs compared to competitors. API access controls are average. Security, resiliency and coverage is also below average, as it is the only vendor in this research that doesn't offer an SLA for its SaaS products (only an SLO). Also, there is not a lot of transparency around the service's performance and availability.

For internal AM use cases, identity administration is above average, as it offers very good directory services, both on cloud and on-premises, as well as average identity administration capabilities in IDCS. Authorization and adaptive access is below average, as both OAM and IDCS are missing a number of key endpoint and UEBA contextual signals for adaptive access. It also does not offer access orchestration functionality with either product. However, OAM offers granular session management, with both global and application-by-application settings, but IDCS only offers global controls for session management.

User authentication is average but analytics is below average. Though it is possible to extract good insights through custom reports, there are not a lot of OOTB capabilities for AM event analytics. Nonstandard application enablement is average. Standard application enablement is also average, with limited OOTB SSO connectors to SaaS apps compared to competitors.

Oracle received its highest score for the internal AM use case. However, it is rated below average for all the use cases evaluated in this research.

Ping Identity

Ping Identity AM products are sold in several bundles and modules under the label of PingOne platform as both SaaS and software with converged AM, identity proofing, and fraud detection capabilities. It also offers a single-tenant SaaS offering in the form of PingOne Advanced Services.

In terms of innovation, Ping Identity enhanced its AM functionalities by including a low-code flow designer, a risk engine and an analytics framework, and new document-centric identity proofing capabilities.

For external AM use cases, user self-service is above average, offering a very easy setup of self-service capabilities for customer registration with progressive profiling and consent management. Security, resiliency and coverage is also above average, offering a 99.99% availability SLA to all of its clients, with aggregated outages across all regions last year summing less than 140 minutes. API access control is above average, with support for mTLS, token exchange, and an API threat protection tool that integrates with commonly used API gateways, as well as a new flow designer. BYOI integration is above average where Ping Identity is one of the few AM vendors to offer its own DCI product with the acquisition of ShoCard, along with offering user-driven consent flows for social ID approaches.

For internal AM use cases, identity administration is below average, as the existing features are very basic. There's no inbound SCIM function in the SaaS product, so even basic life cycle management features will require third-party integrations with dedicated IGA platforms. For authorization and adaptive access, it provides a comprehensive list of contextual signals for adaptive access and uses its MFA tool, PingID, to do so. Clients can also add PingAuthorize, an additional licensed product, to add functionality for externalized authorization management. PingFederate, the software product, does not offer UEBA but can use Ping One Risk, offered natively in the SaaS offerings like PingOne, for UEBA signals. Ping Identity recently released an access orchestration tool, Experience Designer, currently in public preview. Both products, software and SaaS, scored above average for session management, offering granular controls, including global and application-by-application settings. In addition, its PingOne Fraud tool (formerly SecuredTouch) provides passive behavior biometrics to detect anomalies in contextual signals for fraud and bot mitigation.

User authentication is above average where Ping Identity provides support for an extensive range of methods, including support for its own proprietary biometric model through PingOne Verify. It also offers a library of adapters to integrate with nonstandard applications. In addition, the capabilities of PingFederate are extended with PingAccess, a reverse proxy/gateway that can facilitate credential injection into HTTP headers, and thus scored above average for nonstandard application enablement. For standard application enablement, it offers more than 1,000 OOTB SSO connectors for SaaS apps. Analytics is average but can offer anomaly and peer detection.

Ping Identity received its highest score for the external AM use case. It is rated above average for all the use cases evaluated in this research.

Thales

Thales AM products are sold under the label of SafeNet. It offers SafeNet Trusted Access (STA) as SaaS and SafeNet Authentication Service as software, with separate modules for hardware tokens and smart cards.

Thales enhanced its AM functionalities by including collaboration features between multiple tenants to share corporate applications, contextual Windows log-ons and hybrid deployment models for its products.

For external AM use cases, user self-service is below average, as user registration flows are not customizable and require external applications to be fully developed by clients in order to call products' APIs for B2B and B2C scenarios. BYOI integration is also below average, as no OOTB plug-ins are available even for social IDs and user-driven consent flows are also absent. Security, resiliency and coverage is below average. Though it offers a very good availability SLA of 99.99%, it suffered a high number of incidents counting over 11 hours of cumulative unavailability among the three regions it operates in. Its services are also only available in North American and European data centers. For API access controls, it does offer an OAuth 2.0 authorization server. However, its policy engine API is not exposed for clients to use, it cannot receive authorization calls from client APIs, and it does not implement consent nor handles scope to claim mappings.

For internal AM use cases, identity administration is below average, as its directory services are very limited where the schema allows the creation of only three custom attributes in addition to the standard ones. It does support inbound SCIM calls for creating users and groups into STA, but it doesn't support outbound SCIM. It does not support multiple authoritative sources of identity data without using a third-party unifying directory and also requires third-party products for most identity administration tasks. For authorization and adaptive access, it offers a moderate number of contextual signals, so adaptive access will be somewhat limited, lacking signals for several key endpoint and UEBA inputs. It does not offer access orchestration for authentication and authorization but does offer granular session management capabilities, allowing controls at both global and per application levels.

User authentication is average but missing support for X.509 phone tokens. Analytics is below average. Though it does offer a good number of OOTB descriptive (historical) reports and some anomaly reports, especially about authentication tokens usage, it does not offer diagnostic insights, predictive and prescriptive analysis, and customizations of reports are extremely labor-intensive. Standard and nonstandard application enablement is also below average, as its integration catalog includes only a few hundred OOTB SSO connectors, as opposed to thousands in competitors.

Thales received its highest score for the internal AM use case. However, it is rated below average for all the use cases evaluated in this research.

Context

This Critical Capabilities research can help IAM leaders select a suitable AM tool for either or both internal and external access use cases. However, product capabilities alone should not form the basis of a purchasing decision. This Critical Capabilities report must be used in conjunction with the complementary Magic Quadrant for Access Management for guidance on the market positions of AM vendors.

The AM market remains at a mature stage in terms of adoption and enterprise experience. Gartner continues to see strong interest in AM as organizations pursue remote work as a result of COVID-19. This is expected to remain steady in the near term. SaaS is now the dominant delivery model for AM services. Buyers of SaaS-delivered AM have established that the benefits of ease of deployment and use, time to value, and frequent and easy-to-consume functional upgrades outweigh the risks of having a third party manage their authentication and authorization services and hold personal information.

In this research, we evaluate a variety of AM capabilities, including the must-have capabilities as defined in the technical inclusion criteria, along with many new and emerging capabilities that are increasingly relevant. The individual use cases identified, internal and external AM use cases, continue to be the most common discussed among Gartner client inquiries over the course of the last year. While many organizations will find one use case to be representative of their needs, some may find a mix of use cases — or an in-depth focus on specific capabilities — to be most relevant. In the latter case, buyers can employ customization facilities in the online version of the research to adjust criteria weightings to best reflect their needs.

Gartner has observed the following key trends that are increasingly relevant for IAM leaders:

- SaaS-delivered AM tools have become very popular, by far the preferred way the majority of customers want to consume their AM services. However, as more and more applications are integrated, the AM tool becomes the doorway to all applications, and conversely, the blast radius of any kind of outage becomes impactful from a business perspective. Therefore, the availability and scalability of AM services is far more important now. In this analysis, we have also evaluated AM tool capabilities from a security, resiliency and geographical coverage perspective.
- External AM, specifically for B2C, is a pivotal use case for AM implementations, and AM vendors are increasingly maturing their offerings to address the specific needs. Gartner has also observed the growing demand for B2B external AM use cases. In this analysis, emerging AM tool capabilities for B2B-specific functionalities were also evaluated.
- IAM convergence activity is rapidly increasing. The AM market has been leading the charge to offer converged IAM capabilities. IAM use case feature consolidation has also been observed with leading multiconstituency AM vendors now offering capabilities for delivering external, internal AM and developer-oriented use cases. Increased functionality convergence from other adjacent IAM markets like IGA and PAM has also been observed. In this research, some converged capabilities from an IGA offering perspective are also evaluated.
- Emerging access orchestration capabilities can enforce better balance between security and UX along with lowering TCO for different use cases. In this research, AM tools' capabilities for access orchestration in the form of a low-code/no-code approach to building complex authentication and authorization flows were also evaluated.

Product/Service Class Definition

AM tools use access control engines to establish, enforce and manage runtime access controls for internal and external types of identities, interacting with cloud, modern standards-based web and legacy web applications. Increasingly, AM tools may provide IGA capabilities, including features and functions to administer internal and external identities, directory services and identity provisioning to target systems.

Critical Capabilities Definition

Identity Administration

This capability offers features and functions to manage internal and external types of identities, including at minimum, a directory or identity repository, identity synchronization services and SCIM support.

Optionally, it may manage machine identities (bots, workloads, IoT) and support B2B2C and B2B2E use cases. Identity administration may also offer basic identity governance and administration (IGA) capabilities like identity life cycle management, user provisioning, access requests with approvals and access certifications. Lastly, it may provide virtual directory capabilities and identity data aggregation and integration with external platforms like marketing, CRM and customer analytics.

User Self-Service

This capability provides end-user and administrative interfaces for user registration, password management, profile management and delegated administration. It also provides a workforce launchpad of applications or application gallery for single sign-on (SSO).

Optionally, it may offer end-user and administrative interfaces for progressive profiling, consent, preference and privacy management, and multichannel support, as well as low-code/no-code orchestration interfaces for developers and administrators.

Authorization and Adaptive Access

This capability implements coarse-grained authorization decisions and enforcement, policy creation, and sources of stored and contextual data used for rendering access decisions. It should provide at least native support for modern protocols like OAuth 2.0.

Optionally, it may offer fine-grained authorization. It may also offer access orchestration that consumes both native and external signals in a low-code/no-code approach to build complex authentication and authorization flows. The solution may also include online fraud detection, security and UEBA capabilities, and CASB, either natively or via integration with third-party providers that can drive risk-based, adaptive access decisions.

Session Management

This capability controls session state for interactions with applications, the ability to manage session times by issuing and refreshing time-limited access tokens, and the ability to terminate sessions. It provides a global setting for session management and single log-out.

Optionally, it may support application-by-application settings for session control and adding attributes in claims to the token for session management purposes.

User Authentication

This capability enables a variety of authentication methods, including multifactor authentication (MFA).

Optionally, it offers support for a broader range of MFA methods, including X.509 and FIDO hardware and software tokens, device-native and third-party biometric methods, and other options for passwordless and continuous authentication.

BYOI Integration

This capability provides integrations to use public identities, such as social IDs for access control. Core functionality includes using sign-up, sign-in and linking social media identities to AM customers' established user IDs and to set access policy based on the use of social IDs.

Optionally, it may offer advanced BYOI integrations with cloud service provider identities, bank ID, government ID, mobile network ID and decentralized identity services.

API Access Control

This capability offers an OAuth 2.0 authorization server, which implements consent, handles scope to claim mappings, and is capable of issuing customizable and self-contained JSON Web Tokens (JWTs) to web servers, mobile apps, modern web apps and services used for accessing API targets.

Optionally, it may offer advanced API access controls that provide either libraries, sidecar containers or OOTB integrations with APIs and API mediators to centralize authentication and authorization decisions to the authorization server. This capability also evaluates the available developer tools and distribution options of the AM product. It may also include developer self-service capabilities for managing apps and services and support for flows, such as the OAuth Mutual Transport Layer Security (mTLS), the JWT and SAML grant types, the device flow, token exchange, introspection and revocation, and provide strong and agile cryptographic mechanisms for signing tokens.

Standard Application Enablement

This capability integrates and enables rapid access, SSO and MFA to target applications by leveraging modern identity protocols like SAML and OpenID Connect. Optionally, it may offer multiple key signing support.

Nonstandard Application Enablement

This capability integrates and enables access, SSO and MFA to legacy applications that do not support standards-based SSO protocols, using technologies like proxy services, agents or other mechanisms.

It also evaluates the AM extensibility and customizability options to integrate with nonstandard application targets, third-party tools and user sources.

Analytics

This capability offers descriptive, historical information about all administration and runtime access events. It enables reporting and APIs for exporting event data to be analyzed by external analytics and SIEM or consumed by the solution's own adaptive risk engine.

It allows customers to use preconfigured and customized reporting functions to identify entitlements, audit access and identify access risks. Optionally, it also offers diagnostic, predictive and prescriptive analytics. It may also include user and entity behavior analytics (UEBA) and identity threat detection capabilities (advanced threat protection, compromised identities and malicious insider actions). It may also offer analytics and ML functions that feed into web app firewalls and other identity security protection tools.

Ease of Deployment

This capability evaluates the level of effort to deploy the AM product or service. It takes in consideration average deployment and onboarding time of applications, as well as different strategies offered for application and user onboarding.

It also evaluates out-of-the box options for integration, versus customization requirements. Lastly, it evaluates configuration management approaches and migration strategies.

Security, Resiliency and Coverage

This capability evaluates the security elements available in the AM product or service for protection against different types of attacks. It also evaluates mechanisms and different levels of service offered for availability and resiliency strategies.

Lastly, it evaluates geographical coverage for the service and variation of services provided in each region.

Use Cases

Internal Access Management

This includes AM capabilities for workforce identities (including, but not limited to, employees, temporary workers, and outsourcers and contractors, excluding gig workers).

This use case includes capabilities like access control engines to provide centralized authentication, SSO, session management and authorization enforcement for target apps/services to address AM requirements for B2E use cases like workforce (internal) identities (including, but not limited to, employees, temporary workers, outsourcers, and contractors, but excluding gig workers). This use case also includes, but is not limited to, adaptive and contextual authentication as core functionalities along with support for modern identity protocols, such as SAML, OAuth 2.0 and OIDC. Standard application enablement, authorization and adaptive access, analytics, and identity administration are important critical capabilities for these use cases.

External Access Management

This includes AM capabilities for B2C, B2B, G2C and gig economy use cases (including, but not limited to, consumers, partners, citizens, and contingent freelance talent).

It also includes B2C, B2B, G2C and gig economy, (external) identities use cases (including, but not limited to, consumers, partners, citizens, and contingent freelance talent). The use case also includes access control engines to provide centralized authentication, SSO, session management and authorization enforcement for target applications. User self-service, BYOI integration, user authentication and API access controls are important capabilities for this use case.

Application Development

This use case includes, but is not limited to, capabilities needed to embed access management controls into custom-developed applications.

API access control is the most important capability in this use case, which includes the ability to control authentication and authorization into API targets. The use case also includes developer tools like developer self-service interfaces and SDKs for the application development use case.

Vendors Added and Dropped

Added

Ilantus: Ilantus has met the inclusion criteria for this Critical Capabilities research with its SaaS-delivered converged IAM platform called Compact Identity.

Dropped

LoginRadius was dropped this year as it did not meet the following criterion:

- Vendors need to have marketed and must have sold products and services in their 2020, 12-month fiscal year to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases. For example, solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, will be excluded.

Inclusion Criteria

Critical Capabilities Inclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyses the most relevant providers and their products in a market. Gartner uses, by default, an upper limit of 20 providers to support the identification of the most relevant providers in a market. On some specific occasions, the upper limit may be extended by Methodologies where the intended research value to our clients might otherwise be diminished. The inclusion criteria represent the specific attributes that analysts believe are necessary for inclusion in this research.

To qualify for inclusion, providers need to:

- Have marketed and must have sold products and services in their 2020, 12-month fiscal year to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases. For example, solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case, will be excluded.
    - AM products that cannot support or are not marketed to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases will be excluded. However, solutions that support both internal and external use cases, even without substantial customer numbers for each use case, may be accepted.
- Own the intellectual property for the AM products and services they sell. Vendors that resell other vendors' products or that have merely augmented other vendors' AM products and services for resale or for managed or hosted service offerings will be excluded.
- Have BOTH 15 million USD in annual revenue from AM products and subscriptions (inclusive of maintenance revenue but excluding professional services revenue) in their 2020, 12-month fiscal year AND have 800 or more current AM customers as of 31 May 2021. These must be discrete AM customer organizations (that is, "net logos," meaning different business units or dependencies of the same company should not be counted as a separate customer) and not customers for other products, and they must have their own contracts with the vendor. Free or freemium nonpaying customers are not to be included in customer totals.
- Have global capabilities with customers, delivery and support capabilities in all major markets: Americas (North and South America combined), EMEA, and APAC (including Japan). Vendors must have customers in each market with no more than 80% of their customer count or revenue in their primary region.

In addition, the vendor's AM product(s)/service(s) must offer the following technical capabilities relevant to Gartner clients:

- Identity administration must provide at minimum a directory or identity repository for internal and external identities, including identity synchronization services and SCIM support.

- User self-service must include end-user and administrative interfaces for user registration, password management, profile management and delegated administration. It also needs to provide a workforce launchpad of applications or application gallery for single sign-on.
- Authorization and adaptive access must include capabilities for implementing at minimum coarse grained authorization decisions and enforcement, policy creation and sources of stored and contextual data used for rendering access decisions. Must provide native support to modern protocols like OAuth 2.0.
- Session management must include capabilities and granularity to which the AM tool can control session state for user-present interactions with applications, the ability to manage session times by issuing and refreshing time limited access tokens (or cookies), and the ability to terminate sessions. It provides at minimum a global setting for session management and single log-out.
- Must provide different user authentication methods, including multifactor authentication (MFA) and SSO. Minimal MFA requirements should include OOB SMS, OTP apps, mobile push, and support for OTP hardware tokens.
- Must provide BYOI integration to use public identities, such as social media at least, for access control. Core functionality includes using sign-up, sign-in, and linking social media identities to AM customers' established user identities, and to set access policy based on the use of social media identities.
- API access control at minimum offers an OAuth 2.0 authorization server, which supports and implements consent, handles scope to claim mappings and is capable of issuing customizable and self-contained JWT tokens to web servers, mobile apps, modern web apps and services used for accessing API targets.
- Must support both standard/modern and non-standard/legacy application enablement. Must support modern protocols like SAML and OpenID Connect, including capabilities to enable access and SSO to legacy applications that do not support standards-based SSO protocols, using technologies like proxy services, agents, or other mechanisms.
- Analytics capabilities must include at minimum descriptive, historical information about all administration and runtime access events. It must offer reporting and APIs for exporting event data to be analyzed by external analytics and security information and event management (SIEM) tools, or consumed by the solution's own adaptive risk engine. It allows customers to use canned and customized reporting functions to identify entitlements, audit access and identify access risks.

Critical Capabilities Exclusion Criteria

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

- AM products that cannot support or are not marketed to support both internal (B2E) and external (B2B, B2C, G2C or gig economy) use cases. For example, solutions without substantial customer numbers for each use case, or that are only or mostly marketed to support one use case will be excluded.
- AM products which are not marketed and supported globally. Vendors must have global capabilities with customers, delivery, and support capabilities in all major markets: Americas (North and South America combined), EMEA, and APAC (including Japan). Vendors must have customers in each market with no more than 80% of your customer count in your primary region.
- Pure user authentication products and services, or products that began as pure user authentication products and then were functionally expanded to support SSO via SAML or OpenID Connect, but cannot manage sessions or render authorization decisions (see Market Guide for User Authentication).
- AM offerings that are only or were predominantly designed to support operating systems and/or privileged access management (see Magic Quadrant for Privileged Access Management).
- Remote or on-premises “managed” AM; that is, services designed to take over management of customers’ owned or hosted access management products rather than being provided by delivery of the vendor’s own intellectual property.
- AM functions provided only as part of 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, marketed as open source offerings.
- Stand-alone identity governance and administration (IGA) suites, which are full-featured IGA products that offer the complete range of IGA functionality, without embedded AM capabilities. This is a separate, but related market covered by other Gartner research (see Market Guide for Identity Governance and Administration).
- Full life cycle API management. This is a separate, but adjacent market covered by other Gartner research (see Magic Quadrant for Full Life Cycle API Management).

- Endpoint protection platforms (EPP) or unified endpoint management (UEM). EPP and UEM are separate, but related markets covered by other Gartner research (see Magic Quadrant for Endpoint Protection Platforms and Magic Quadrant for Unified Endpoint Management).
- Cloud access security brokers (CASB). CASB is a separate, but related market covered by other Gartner research (see Magic Quadrant for Cloud Access Security Brokers).

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	*Internal Access Management*	*External Access Management*	*Application Development*
Identity Administration	8%	8%	1%
User Self-Service	4%	12%	22%
Authorization and Adaptive Access	14%	12%	5%
Session Management	6%	4%	1%
User Authentication	8%	16%	1%
BYOI Integration	0%	11%	4%
API Access Control	5%	20%	58%
Standard Application Enablement	23%	2%	1%
Nonstandard Application Enablement	10%	6%	4%
Analytics	14%	1%	1%
Ease of Deployment	4%	3%	1%
Security, Resiliency and Coverage	4%	5%	1%
As of 12 November 2021			

Source: Gartner (November 2021)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	Okta (Auth0)	CyberArk	ForgeRock	IBM	Ilantus	Micro Focus	Microsoft	Okta	OneLogin	Oracle	Ping Identity	Thales
Identity Administration	3.1	3.5	3.9	4.2	4.0	3.9	3.0	3.3	3.4	3.7	2.6	2.0
User Self-Service	4.0	3.6	4.0	3.1	3.3	3.3	3.1	4.5	3.8	3.3	3.8	2.4
Authorization and Adaptive Access	4.0	4.0	4.2	3.6	3.6	4.1	3.8	4.0	4.1	3.8	4.0	3.1
Session Management	4.6	4.0	4.3	2.9	2.8	4.1	2.5	3.9	4.5	3.1	4.4	3.1
User Authentication	4.4	4.3	4.2	4.5	3.6	4.6	3.8	4.3	4.1	4.2	4.6	4.1
BYOI Integration	4.2	3.3	3.8	3.4	2.3	4.4	3.2	4.1	3.6	2.7	3.9	2.4
API Access Control	4.7	3.3	4.5	4.0	2.9	3.5	3.8	4.2	4.0	3.6	3.8	2.1
Standard Application Enablement	3.3	4.0	4.1	3.9	3.6	3.8	4.2	4.6	4.1	3.7	4.1	3.3
Nonstandard Application Enablement	3.5	4.0	4.2	3.7	3.3	3.8	3.8	4.1	3.8	3.5	4.4	3.1
Analytics	3.4	3.7	3.1	3.8	2.5	3.0	4.0	3.5	3.1	3.1	3.4	2.4
Ease of Deployment	3.7	3.4	3.9	3.6	3.8	3.3	3.6	4.1	4.0	3.1	3.5	2.7
Security, Resiliency and Coverage	3.7	3.4	4.1	4.1	3.2	3.3	3.1	4.5	3.5	3.1	3.6	3.0
As of 12 November 2021												

Source: Gartner (November 2021)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Scores in Use Cases

(Enlarged table in Appendix)

Use Cases	Okta (Auth0)	CyberArk	ForgeRock	IBM	Ilantus	Micro Focus	Microsoft	Okta	OneLogin	Oracle	Ping Identity	Thales
Internal Access Management	3.71	3.84	4.00	3.81	3.35	3.75	3.71	4.09	3.85	3.55	3.89	2.94
External Access Management	4.10	3.69	4.15	3.80	3.24	3.88	3.50	4.14	3.89	3.52	3.91	2.79
Application Development	4.38	3.46	4.30	3.74	3.05	3.55	3.60	4.24	3.92	3.49	3.83	2.33
As of 12 November 2021												

Source: Gartner (November 2021)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Evidence

Vendor surveys

Peer Insights

Secondary resource services

Gartner inquiries

Note 1: Access Management Core Capabilities

Access management (AM) tool capabilities have developed in response to the continued evolution of the tools and resources to which users need access, the rapid adoption of software as a service (SaaS) applications and the emergence of the Internet of Things (IoT). Across internal and external use cases AM tools provide the following core capabilities.

AM offerings include:

- Access policy management
- User authentication
- Single sign-on (SSO)
- Security token services and identity protocol translation
- Session management
- Coarse and fine-grained authorization
- Adaptive access, trust elevation and risk mitigation
- Sign-up/sign-in using social ID
- Access event logging and reporting

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Document Revision History

Critical Capabilities for Access Management - 17 November 2020

Critical Capabilities for Access Management - 7 October 2019

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Magic Quadrant for Access Management

IAM Leaders' Guide to Access Management

Buyer's Guide for Access Management

Technology Insight for Customer Identity and Access Management

Solution Criteria for Access Management

Top Trends in Customer IAM Solution Design

Secure Application Access by Applying the Imperatives of CARTA to Access Management

Enhance Remote Access Security With Multifactor Authentication and Access Management

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Internal Access Management*	*External Access Management*	*Application Development*
Identity Administration	8%	8%	1%
User Self-Service	4%	12%	22%
Authorization and Adaptive Access	14%	12%	5%
Session Management	6%	4%	1%
User Authentication	8%	16%	1%
BYOI Integration	0%	11%	4%
API Access Control	5%	20%	58%
Standard Application Enablement	23%	2%	1%
Nonstandard Application Enablement	10%	6%	4%
Analytics	14%	1%	1%
Ease of Deployment	4%	3%	1%
Security, Resiliency and Coverage	4%	5%	1%
As of 12 November 2021			

Source: Gartner (November 2021)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*Okta (Auth0)*	*CyberArk*	*ForgeRock*	*IBM*	*Ilantus*	*Micro Focus*	*Microsoft*	*Okta*	*OneLogin*	*Oracle*	*Ping Identity*	*Thales*
Identity Administration	3.1	3.5	3.9	4.2	4.0	3.9	3.0	3.3	3.4	3.7	2.6	2.0
User Self-Service	4.0	3.6	4.0	3.1	3.3	3.3	3.1	4.5	3.8	3.3	3.8	2.4
Authorization and Adaptive Access	4.0	4.0	4.2	3.6	3.6	4.1	3.8	4.0	4.1	3.8	4.0	3.1
Session Management	4.6	4.0	4.3	2.9	2.8	4.1	2.5	3.9	4.5	3.1	4.4	3.1
User Authentication	4.4	4.3	4.2	4.5	3.6	4.6	3.8	4.3	4.1	4.2	4.6	4.1
BYOI Integration	4.2	3.3	3.8	3.4	2.3	4.4	3.2	4.1	3.6	2.7	3.9	2.4

Critical Capabilities	*Okta (Auth0)*	*CyberArk*	*ForgeRock*	*IBM*	*Ilantus*	*Micro Focus*	*Microsoft*	*Okta*	*OneLogin*	*Oracle*	*Ping Identity*	*Thales*
API Access Control	4.7	3.3	4.5	4.0	2.9	3.5	3.8	4.2	4.0	3.6	3.8	2.1
Standard Application Enablement	3.3	4.0	4.1	3.9	3.6	3.8	4.2	4.6	4.1	3.7	4.1	3.3
Nonstandard Application Enablement	3.5	4.0	4.2	3.7	3.3	3.8	3.8	4.1	3.8	3.5	4.4	3.1
Analytics	3.4	3.7	3.1	3.8	2.5	3.0	4.0	3.5	3.1	3.1	3.4	2.4
Ease of Deployment	3.7	3.4	3.9	3.6	3.8	3.3	3.6	4.1	4.0	3.1	3.5	2.7
Security, Resiliency and Coverage	3.7	3.4	4.1	4.1	3.2	3.3	3.1	4.5	3.5	3.1	3.6	3.0
As of 12 November 2021												

Source: Gartner (November 2021)

Table 3: Product Scores in Use Cases

Use Cases	*Okta (Auth0)*	*CyberArk*	*ForgeRock*	*IBM*	*Ilantus*	*Micro Focus*	*Microsoft*	*Okta*	*OneLogin*	*Oracle*	*Ping Identity*	*Thales*
Internal Access Management	3.71	3.84	4.00	3.81	3.35	3.75	3.71	4.09	3.85	3.55	3.89	2.94
External Access Management	4.10	3.69	4.15	3.80	3.24	3.88	3.50	4.14	3.89	3.52	3.91	2.79
Application Development	4.38	3.46	4.30	3.74	3.05	3.55	3.60	4.24	3.92	3.49	3.83	2.33
As of 12 November 2021												

Source: Gartner (November 2021)