Magic Quadrant for Access Management

Published 17 November 2020 - ID G00450534 - 50 min read

By Michael Kelley, Abhyuday Data, **and 1 more**

As remote work increases access management tool adoption, and security controls shift to identity, the ability to secure access with AM strategies aligned with continuous adaptive risk and trust assessment is paramount. Cost optimization for IT spending (e.g., AM) will also increase during 2021.

Strategic Planning Assumptions

By 2024, 50% of all workforce access management (AM) implementations will leverage native, real-time, user and entity behavior analytics (UEBA) capabilities and other controls. This will provide continuous adaptive risk and trust assessment (CARTA)-aligned functionality, which is a major increase from fewer than 10% today.

By 2024, driven by cost optimization exercises, 30% of all new purchasing for AM solutions will be “best fit,” as opposed to “best in class.”

By 2024, at least one AM vendor will introduce a converged offering that will provide market-competitive functionality in AM, identity governance and administration (IGA), and privileged access management (PAM).

Market Definition/Description

Gartner defines the AM market as technologies that use access control engines (identity providers, authorization servers, policy servers, etc.) to provide the following core capabilities:

- Support for internal (B2E) or external (B2B, B2C, G2C or gig economy) types of identities, and AM use cases
- Authorization and adaptive access
- User self-service capabilities, including registration, password management, profile management and delegated administration
- User authentication methods, multifactor authentication (MFA) and single sign-on (SSO)

- Session management
- Access enforcement for standard and nonstandard target applications
- Support for modern identity protocols, such as Security Assertion Markup Language (SAML), OAuth, System for Cross-Domain Identity Management (SCIM) and OpenID Connect (OIDC)
- Event logging and reporting
- API access control — authentication and authorization of APIs and software development kit (SDK) capabilities for mobile applications
- Bring your own identification (BYOI) integration — the ability to use public identities, such as social media at least, for access
- Directory and identity synchronization, including identity repository services

Optionally, AM vendors may provide these capabilities:

- Manage nonhuman types of identities — bots, Internet of Things (IoT)
- Progressive profiling
- Advanced user authentication methods, such as Fast IDentity Online (FIDO) and passwordless
- Identity life cycle management (LCM) and user provisioning
- Proxy services, agents or other mechanisms for nonstandard application enablement
- Access orchestration for decision tree support of external authentication and authorization methods
- Consent, preference, and privacy management and integration
- Fraud detection, security and UEBA integration
- Identity analytics
- Advanced BYOI integration — social, bank, government, mobile network, corporate and decentralized identification
- Developer self-service for application integrations and administration

Target applications may have traditional web application architectures, using web browsers and web application servers, or they could be native or hybrid mobile applications. These applications may

also run on things with or without human operators. Protected target systems may include web application services or APIs, and may run on customer's premises or in the cloud.

CARTA-Aligned Functionality

The future of AM in digital transformation initiatives requires continued adoption of open standards and federation. However, this approach, although well-suited for the operational demands of global and ubiquitous application access, often lacks real-time visibility and controls for detrimental changes to the user session.

As outlined in Secure Application Access by Applying the Imperatives of CARTA to Access Management, applying the seven imperatives of CARTA to AM happens largely within three main areas. These are controls, secure architecture and visibility, as applied to the life cycle of AM; session establishment; session management; and session termination.

To embrace a CARTA-aligned approach, Gartner has evaluated AM vendors' capabilities to address visibility, secure architecture, and controls, and noted those controls in the vendor writeup.

Contextual and Adaptive Access: With "continuousness" representing the goal in the context of visibility and control, adaptive and contextual access controls enable risk and trust to be automatically assessed for every interaction throughout every session. Many AM vendors can consume a rich set of contextual signals. These include IP address, endpoint status and signals coming from user behavior, which can feed into adaptive access controls to determine the appropriate level of authentication and the appropriate level of access.

For example, a user accessing a critical application from outside the corporate network (using IP address and network information as contextual signals), may trigger step-up authentication, using an additional factor. A user trying to access a critical application from an untrusted device (using device information as a contextual signal) would be denied access. Perhaps the user would be allowed reduced privileges to the application, compared with access from a trusted device.

Application Access Proxy: Also known as an identity-aware proxy, or reverse proxy, these products have traditionally been used for AM vendors to facilitate access to nonstandard applications, applications unable to natively support modern identity protocols (e.g., SAML, OAuth and OIDC). In addition, with a CARTA-aligned approach, a proxy can represent an in-line mechanism, able to provide visibility and control for any user session.

Granular Session Management: Session management controls how tokens, (or cookies), are managed. This, in turn, controls how sessions are managed. For AM vendors that provide only a single global session management setting, all applications, high-risk or low-risk, are treated the same. Many AM vendors can provide granular session management settings, which means that applications can be grouped by risk (or potentially addressed individually), and be provided different levels of access from a session management perspective.

For example, a user might be granted access to a low-risk application for up to three months without being asked to authenticate again (this assumes that no other CARTA-aligned elements are involved, or are triggered). (A high-risk application may provide only a three-day window for access before the user is required to reauthenticate.) From a CARTA-aligned approach, it is important to have AM vendors that can provide granularity from a risk-based perspective.

Orchestration Approaches for Authentication and Authorization: Although adaptive and contextual access has traditionally used native capabilities, many AM tools support open integration of or data interchange with third-party tools. These approaches allow an ever-increasing level of contextual signals, both native and third party, to be used for adaptive access decisions. These additional functionalities are still accurately described as adaptive access. Many vendors are providing a "no-code," graphical user interface (GUI)-based approach. This enables customers to create complex authentication and authorization journeys. This means they can easily "orchestrate" these native and third-party signals, combined with native capabilities, for trust elevation or other appropriate security strategies for application access.

Some examples of sources of risk context information are external threat intelligence (TI), externalized authorization architecture, online fraud detection (OFD), a cloud access security broker (CASB), and a web application firewall (WAF). Context information is also provided by zero-trust network access (ZTNA; formerly software-defined perimeter), an enterprise UEBA tool or an API gateway.

UEBA: These analytics have shown promise in identifying behavior that deviates from the norm for a particular user. Understanding when and where an account, or session, has been hijacked is important for the ability to respond. AM vendors have been adding some basic behavior analytics (e.g., UEBA) functionality to their products, which creates another contextual signal, driving a response when the change has been detected.

Pricing

To illustrate a high-level perspective for vendor pricing in the vendor descriptions in this Magic Quadrant, we comment on the pricing of individual products, using such terms as "well-above average," "above average," "average," "below average" and "well-below average." The average for a particular component refers to the average score for all vendors evaluated in this research for a variety of different AM pricing scenarios.

Magic Quadrant

Figure 1: Magic Quadrant for Access Management

Source: Gartner (November 2020)

Vendor Strengths and Cautions

Auth0

Auth0 is a Challenger in this Magic Quadrant.

Auth0 is known for its developer-focused products. It sells four products, beginning with Free Plan for as many as 7,000 users; Developer for B2C and Developer Pro; and Enterprise for B2E, B2B and B2C. In addition to the base product offering of SSO and MFA, additional licensing is required for more than 10 connections, enterprise and contextual MFA, and machine-to-machine authentication, among others listed here.

CARTA-aligned functionality includes light UEBA capabilities, such as anomaly detection, automated attack prevention, granular session management controls, and orchestration of authentication and authorization through Auth0 Hooks and Rules.

Strengths

- Auth0 has a strong focus and specialization in customer identity and access management (CIAM), for both B2C and B2B scenarios. It also has one of the most-extensive lists of BYOI integrations, including support for Apple's new Sign-in With Apple (SiWA) authenticator and support for some government IDs.
- Auth0 provides strong, native API access control capabilities, and embeds a complete set of API security capabilities.
- Auth0's orchestration capability, Auth0 Rules and Hooks, provides the ability to craft complex authentication and authorization stories.
- Auth0 is priced competitively, with almost all pricing scenarios below, and sometimes well below, the average of the market as a whole.

Cautions

- Auth0 does not provide reverse-proxy or agent technology to integrate nonstandard apps; rather, it only supports NGINX third-party libraries and Apache SDKs that support this form of integration.
- Auth0 provides a limited catalog of preconfigured software as a service (SaaS) application integrations, requiring organizations to configure more of their own integrations.
- Auth0 is not geographically diverse, although it does provide some global coverage, its sales and support coverage is primarily concentrated in North America and Europe.
- Reporting capabilities are quite limited, a dashboard is available, but creating custom reports is manual and complicated.

CyberArk (Idaptive)

CyberArk (Idaptive) is a Challenger in this Magic Quadrant.

CyberArk's SaaS AM product provides SSO, MFA and endpoint controls. CyberArk includes UEBA functionality and optional external threat feeds with its Adaptive MFA product (licensed separately).

CARTA-aligned features include adaptive access, mature UEBA, granular session management controls and endpoint controls.

Strengths

- CyberArk customers are assigned a dedicated technical relationship resource at no additional cost. This type of service is typically charged separately by other vendors.
- Idaptive has continued to mature its UEBA capabilities, including these signals in adaptive MFA and SSO.
- The Idaptive product can provide endpoint visibility and authentication context signals with its endpoint management and agents for Windows and macOS clients.
- Similar to its existing brokered authentication, Idaptive now offers cloud-brokered MFA for endpoints, which allows devices to join the adaptive cloud, even without access to the source directory — for example, Active Directory (AD).

Cautions

- The Idaptive installed base is heavily focused on internal identity use cases. It has a small installed base for CIAM and external identities in general.
- Market responsiveness has slowed, and crucial items such as consent, preference and privacy, API security, and BYOI integration remained mostly unchanged since last year. Innovation consisted mostly of catch-up features.
- CyberArk (Idaptive)'s geographic strategy is less diverse than other vendors; customer counts have increased in North America, while they've dropped in the Asia/Pacific (APAC) region and Japan.
- The pricing for the scenarios evaluated by Gartner in this research tends to be somewhat above average for all use cases, with more-complex CIAM scenarios more expensive than its competitors.

ForgeRock

ForgeRock is a Leader in this Magic Quadrant.

The ForgeRock identity platform includes modules such as Intelligent Access, SSO, Lifecycle Management and Directory. The ForgeRock Identity Cloud comes as a base product that includes AM, identity LCM, SSO, MFA and ForgeRock Trees, its orchestration engine. Additional features such as contextual/adaptive access, continuous authorization, and CIAM functionality (e.g., social IDs, self-service, progressive profiling and privacy) are available at an additional cost.

CARTA-aligned functionality includes granular session management, orchestration of authentication and authorization through Trees, and with optional components, contextual and adaptive access, and

an application access proxy.

Strengths

- ForgeRock has scored above average for its product capabilities, and has achieved the highest score in adaptive access and authorization capabilities.
- ForgeRock is one of the thought leaders in the AM space, and it is heavily involved in standardization efforts for new protocols, including UMA and OAuth.
- ForgeRock previously had CIAM and Open Banking products available as SaaS. During the past year, ForgeRock has released SaaS-based options for more of its products, including workforce.
- ForgeRock has done extensive work providing access and controls to “things” and IoT devices, as well as microservices with its edge capability.

Cautions

- Although ForgeRock offers BYOI functionality, no decentralized identity approaches are supported out of box.
- The SaaS delivery option for Internal Identity AM modules are quite new. Prospective buyers should closely examine the service and leverage POCs to validate availability and scalability.
- UEBA capabilities are not mature, compared with the market.
- ForgeRock software product pricing analyzed for a series pricing scenario prices tends to be uneven, with below-average pricing for software, however, with above-average pricing for SaaS and CIAM, in particular.

IBM

IBM is a Challenger in this Magic Quadrant.

IBM offers the IBM Security Verify Access, formerly known as IBM Security Access Manager, for software-delivered AM, and IBM Security Verify, formerly known as IBM Cloud Identity, for SaaS-delivered AM. AM functionality in both products includes SSO, MFA, directory, UEBA, identity analytics and provisioning. Access provides more traditional web access management (WAM) functionality, including a proxy, and Security Verify includes a cloud directory for user identity data.

CARTA-aligned functionality includes granular session management, contextual and adaptive access, and UEBA. IBM can also sell services with adjacent technologies, such as WAF, CASB and its full Trusteer risk analysis tool.

Strengths

- IBM offers good embedded identity LCM capabilities in the IBM Security Verify SaaS product. For more-complex use cases, Security Verify subscribers are entitled to the full IGA suite of capabilities provided by the IBM Identity Governance and Intelligence product, at no additional cost.
- IBM includes its anti-fraud Trusteer service (a subset of the full Trusteer product), which provides adaptive risk scoring in both products, at no additional cost.
- Strong API access control and above-average API protection capabilities are included out-of-the-box in both solutions.
- IBM SaaS product pricing for all the scenarios it supports consistently undercuts its competitors.

Cautions

- Except for the various IBM products that are now bundled or integrated with Security Verify, other innovations added to the product since last year were merely incremental.
- B2B and B2C support is limited. Basic, out-of-the-box, self-service registration flows and customization are only supported by the software-based product. Even self-service profile management customization, which is a basic requirement addressed by other vendors, is not supported in the SaaS version out-of-the box, and requires development using APIs, or leveraging the on-premises product.
- Password resets support only email validations in the SaaS product. For more-advanced password reset options, the software product is required.
- IBM has created a confusing branding choice for naming all AM products of the portfolio under the Verify brand.

Micro Focus

Micro Focus is a Niche Player in this Magic Quadrant.

Micro Focus offers the NetIQ Access Manager as a software-delivered product. Starting with Version 4.5, the product can be deployed by customers in cloud infrastructure services. The base product includes SSO. Adaptive access is an additional product, as is MFA. Micro Focus is a WAM-centric technology, but it does support modern identity protocols.

CARTA-aligned functionality includes Interset UEBA, the Micro Focus Risk Engine, an application access proxy, adaptive and contextual access, and granular session management controls.

Strengths

- Interset UEBA is integrated into the NetIQ Access Manager platform, for developing additional risk signal calculations.

- Micro Focus is a good fit for larger organizations (especially existing Micro Focus clients) that prefer the flexibility of managing on-premises deployments, and don't mind the additional complexity.
- NetIQ Access Manager has a strong BYOI integration offering out-of-the-box, with more than 14 prebuilt integrations with social IDs and integrations available for a number of public, bank and national IDs.
- Micro Focus has strong controls for the industrial IIoT (IIoT), with multiple examples for providing authentication and authorization for IIoT use cases.

Cautions

- Micro Focus has not delivered on its promise to offer a true SaaS AM offering. NetIQ Access continues to be an infrastructure as a service (IaaS)-hosted model, meaning it offers virtual machines (VMs) running AM software for customers to manage. Micro Focus still offers no readily available SaaS services. It remains the only vendor in this Magic Quadrant survey that lacks a true SaaS product.
- As noted last year, Micro Focus provides a limited catalog for preintegrated applications, containing only a few hundred, compared with thousands for other vendors.
- For logging and reporting, a small number of prebuilt reports are available.
- Pricing is uneven, with smaller scenarios being slightly below market averages, whereas larger and more-complex deals tend to be priced above market averages.

Microsoft

Microsoft is a Leader in this Magic Quadrant.

Microsoft Azure AD is SaaS, although usually tied closely to AD for the synchronization of identity data.

Azure AD offers SSO, MFA, a catalog of preintegrated applications, and some light identity governance. Azure AD is sold on a tiered basis, in which more-advanced functionality requires a higher (and more-expensive) license, but starts with a free tier.

CARTA functionality includes Conditional Access rules for adaptive and conditional access. Adjacent technologies available in the Microsoft platform include CASB, endpoint management and threat detection.

Strengths

- Microsoft has benefited from increased remote work activity driven by the global health crisis, with some of its Azure services achieving high double-digit growth month over month. This has

increased its already-high marks in overall viability.

- Azure AD premium includes Conditional Access, which is a popular and heavily leveraged adaptive access tool. This past year, Microsoft has added an audit-only mode, which has become popular with customers.
- Microsoft simplified pricing for its B2C offering, moving to a monthly authenticated users (MAU) model, with no charge for the first 50,000 external identities. Overall pricing analyzed for various scenarios in this research is below the market average.
- Microsoft is one of the vendors demonstrating not only meeting Web Content Accessibility Guidelines (WCAG) standard for compliance reasons, but also concerned with providing a strong positive experience to people with disabilities.

Cautions

- Licensing of Azure AD is designed in a way that "bundles" features, which means that modules can't be acquired individually. Organizations have to move to a more-expensive subscription package to be able to access more-advanced functionality in Azure AD.
- CIAM experience is still lacking, when compared with other market leaders, and most B2B and B2C functions are offered in separate tenants.
- The session management functionality in Azure also continues to be less mature than the market, lacking application by application granularity and other controls. Microsoft is betting on the adoption of continuous access evaluation protocol (CAEP) to resolve this; however, this protocol is new, and universal adoption is not a forgone conclusion.
- Programmatic interfaces into Azure AD are limited to the Graph API.

Okta

Okta is a Leader in this Magic Quadrant.

Okta offers a SaaS service with SSO, a large catalog of preintegrated applications, a user directory, MFA, analytics and some device management. Software-delivered components include the Access Gateway and various agents.

CARTA-aligned features include contextual and adaptive signals, granular session management, an application access proxy, orchestration for authentication and authorization with Okta hooks, and a risk engine with multiple risk feeds, including threat insights.

Strengths

- Okta has scored above average for its product capabilities, in particular for adaptive access, user authentication methods and standard application enablement.

- Okta has expanded its UEBA capabilities, adding them to Okta ThreatInsight, a service provided to all customers that provides identity and access analytics from usage patterns across the entire Okta cloud.
- Okta is popular with its customers, earning above-average customer experience scores.
- By adding the new workflows capabilities to Okta hooks, customers can orchestrate complex authentication and authorization scenarios with a no-code approach.

Cautions

- Directory integration and its identity life cycle capabilities continue to be limited, especially when compared with other AM vendors that have, since last year, added more-robust identity governance capabilities.
- Okta's geographic strategy is not as diverse as others in the market, Okta's installed base is largely concentrated in North America.
- CIAM scenarios enabled by Okta are still more simplistic than the competition; consent and preference management continues to be very basic, and there is no out-of-the-box support for bank IDs, or government digital identities (eIDs).
- Pricing continues to be well above average, which is becoming a larger concern for companies working through cost optimization exercises.

OneLogin

OneLogin is a Leader in this Magic Quadrant.

OneLogin offers a SaaS-delivered AM solution, with three levels: Starter, with just SSO and MFA; Enterprise, which adds Directory and RADIUS; and Unlimited, which adds directory management and HR-driven identity. OneLogin offers all of its modules for workforce, and external identities (B2B and B2C).

CARTA functionality includes an application access proxy; granular session management controls; contextual and adaptive access, including endpoint signals; and a risk engine called Vigilance AI.

Strengths

- OneLogin is popular with customers; it has earned above-average scores in customer experience.
- OneLogin significantly expanded programmatic access to the OneLogin platform, with more than 40 APIs and additional SDKs that enable customers who want to, to manage their AM environments with code.

- For difficult nonstandard applications, such as Oracle EBS, Oracle PeopleSoft, JIRA and Atlassian Confluence, OneLogin Access provides a reverse proxy and agents to support SSO and session management.
- OneLogin's pricing is competitive, and is well in line with the industry averages, with external identity management scenarios below the average of the market as a whole.

Cautions

- OneLogin has improved API functionality, compared with last year; however, its API protection functionality remains immature, compared with the market overall.
- CIAM functionality, such as progressive profiling, is technically possible; however, it requires a significant assembly with API interfaces. Consent and privacy management functionality is less mature than others in the market.
- OneLogin has taken steps to be a global provider of AM products and services; however, most of OneLogin's customers continue to be in North America and Europe.
- BYOI functionality is not mature compared with the market, lacking support for government, banking, mobile network or decentralized IDs.

Oracle

Oracle is a Challenger in this Magic Quadrant.

Oracle offers two solutions, the software-delivered Oracle Access Manager (OAM), providing WAM-based capabilities, including SSO, MFA and session management. Its SaaS offering, Identity Cloud Service (IDCS), offers standards-based SSO, MFA and a directory. Additional technologies (e.g., TI, CASB and UEBA) are available as additional licensing.

CARTA-aligned features include contextual and adaptive access, session management controls, an application access proxy and access to adjacent technologies in the Oracle portfolio, such as WAFs, CASBs and threat feeds.

Strengths

- Programmatic interfaces are mature for both platforms, with OAM offering a large set of APIs, and IDCS offering a set of SDKs for access.
- Oracle has a strong global presence, leading the market in areas of geographic support, including the availability of cloud@customer, a private cloud service that addresses data residency and reliability concerns.
- Oracle customers can leverage the synergies between Oracle's OAM products and other Oracle IAM technologies, such as IGA and Identity Analytics.

- The Oracle cloud marketplace provides customers with easy integrations for partner technologies.

Cautions

- Innovation of new features and functionality for both IDCS and OAM was limited to catch up features this past year, including a lack of any new functionality in social identity and IoT support. For example, BYOI features continue to be immature, with no out-of-the-box support for government, banking, mobile network or decentralized IDs.
- No native UEBA capabilities exist in either OAM or IDCS; Oracle recommends leveraging adjacent technology, such as CASB, to address that gap.
- Oracle OAM does not support U2F or WebAuthn for OAM; IDCS does not support FIDO2.
- Oracle pricing is above — and, in many cases, well above — the market averages for almost all of the evaluated AM scenarios for its software offering. SaaS product pricing for internal use cases is around the market averages and, for external use cases, below the market averages.

Ping Identity

Ping Identity is a Leader for this Magic Quadrant.

Ping provides both software and SaaS-delivered AM components. PingFederate (SSO), PingAccess, (proxy) and PingDirectory are software-delivered products. SaaS services include PingID, PingIntelligence for APIs, and two bundles, Ping One for Enterprise (SSO, MFA, Directory), and Ping One for Customers (SSO, MFA, Directory, self-service). Ping has also introduced a private SaaS solution called Ping Cloud.

CARTA functionality includes granular session management controls, an application access proxy, contextual and adaptive signals, and, for UEBA functionality, PingIntelligence for APIs and PingID.

Strengths

- Ping Identity scored very high for product capabilities. With a comprehensive set of plug-ins for PingFederate and the PingAccess platform, Ping is a leader for nonstandard application integration, API access controls and user self-service capabilities.
- Ping Identity scored very high for customer experience. Customers appreciate the product's integration flexibility, ease of deployment and administration.
- Ping experienced solid adoption of its new SaaS products (PingOne for Customers and PingOne for Enterprise), with growth near the 100% mark.
- Ping has introduced a self-service capability for developers and application owners for application integration called PingCentral.

Cautions

- The most mature and feature-rich AM functionality comes with software-delivered components, and may be required for cloud components.
- Important identity life cycle capabilities are missing. Even basic identity life cycle and workflow processes for onboarding users securely into the platform would require acquiring and integrating with external IGA tools.
- Although Ping is seen as a global provider, sales and support in regions such as Latin America, the Middle East and Africa are not as robust as services in North America and the European Union.
- Pricing is uneven for the SaaS offering, with different pricing scenarios set at above or below market averages, compared with other vendors offering SaaS-delivered AM, especially when comparing new bundles. Consideration of competitive bids and the functionality provided is necessary to ensure receiving the best price.

Thales (Gemalto)

Thales (Gemalto) is a new entry in the Magic Quadrant, and is a Niche Player.

SafeNet Trusted Access (STA) is a SaaS-based AM product that includes extensive authentication capabilities, including MFA through the Gemalto Digital Identity Services Platform and SSO. Software products include Thales traditional authentication products, such as SafeNet Authentication Service.

CARTA-aligned functionality is limited to adaptive and contextual access, as well as some basic UEBA signals.

Strengths

- STA provides strong user authentication capabilities, and can provide access to additional adjacent Thales products for identity proofing.
- Banking on the Gemalto brand name and a long-standing history in the user authentication market, Thales has a strong partner channel for sales enablement activities across the globe.
- Thales' large, global installed base takes advantage of the legacy Gemalto presence globally.
- STA offers a simplified all-inclusive pricing model with two levels, which is beneficial for companies looking for cost optimization possibilities. Thales' pricing is competitive for internal AM use cases.

Cautions

- STA is primarily focused on internal identities from an AM perspective; fewer than 1% of its installed base addresses external identities use cases, and pricing for CIAM use cases is well above the market average.

- Thales received a score lower than its peers for customer experience. Based on Gartner Peer Insights comments, customer complaints include problems with the mobile interface reliability and performance.
- STA has basic and limited AM capabilities, when compared with other vendors in this Magic Quadrant. API access controls lack a developer self-service interface, and the product is not recommended for organizations with even basic API access control requirements.
- STA provides only agent-based capabilities for nonstandard application enablement, which is not as efficient as a proxy approach.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Thales (Gemalto) was added this year for its SafeNet Trusted Access product.

Dropped

Three previous Magic Quadrant vendors were dropped this year, based on the inclusion criteria. The minimum number of AM customers requirement was increased to 800 for inclusion this year, and SecureAuth was excluded based on that criteria, as was Atos (Evidian). A minimum annual revenue inclusion was added this year; Optimal IDM was excluded based on that criteria.

CA/Broadcom, now known as Broadcom Symantec, was a Visionary in last year’s Magic Quadrant. Although we believe that Broadcom Symantec meets the inclusion criteria, Broadcom Symantec declined to participate in the research. The result is that Gartner had insufficient data to analyze the Symantec SiteMinder product, so the vendor was excluded for 2020. Last year, CA/Broadcom was a Visionary, and the SiteMinder product continues to have a large installed base. However, it has seen little innovation or architectural updates, and it has not developed a SaaS-delivered capability. That has not changed as of the date of this Magic Quadrant.

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant and Critical Capabilities research identifies and then analyzes the most relevant providers and their products in a market. Gartner uses by default an upper limit of 20 vendors 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, vendors need:

- Products or services that deliver all core capabilities for AM, as described in the Market Definition section.
- $15 million in annual revenue from AM products and subscriptions (including maintenance revenue, but excluding professional services revenue) in their 2019, 12-month fiscal year. In addition, they need 800 or more current AM customers as of 30 March 2020. These must be discrete AM customer organizations (i.e., “net logos,” meaning different business units or dependencies of the same company should not be counted as a separate customer). They should not be customers for other products; they must have their own contracts with the vendor. Free or freemium nonpaying customers are not to be included in customer totals.
- Global capabilities with customers, delivery and support capabilities in all major markets: the Americas (North and South America combined); Europe, the Middle East and Africa (EMEA); and APAC (including Japan). (You must have customers in each market with no more than 85% of your customer count or revenue in your primary region.)
- To have marketed and sold products and services in their 2019, 12-month fiscal year to support all major use cases (internal and external identity access). Substantial customer numbers for each use case will be required. For example, solutions that are only or mostly marketed to support only B2C use cases will be excluded.
- To own the intellectual property for the AM products and services they sell. Vendors that resell other vendors’ products or that have merely augmented other vendors’ AM products and services for resale or for managed or hosted service offerings will be excluded.

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

- Vendors with fewer than 800 current AM customers as of 31 March 2020. These must be discrete AM customer organizations — not customers for other products — that have their own contracts with the vendor. Free or freemium nonpaying customers are not to be included in customer totals.
- Vendors with less than $15 million in annual revenue (including maintenance revenue, but excluding professional services revenue) from AM products and subscriptions in their 2019, 12-month fiscal year.
- AM offerings that lack any of the core capabilities, as described in the AM market definition. This includes 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.

- AM offerings that were designed predominantly or only to support OSs and/or PAM (see Magic Quadrant for Privileged Access Management).
- AM products that cannot support or are not marketed to support all major use cases — internal (B2E) and external (B2B, B2C, G2C or gig economy). For example, solutions that are only or mostly marketed to support only B2C, or only B2E use cases will be excluded.
- AM products that are not marketed and supported globally. Vendors must have global capabilities with customers, delivery and support capabilities in all major markets — the Americas (North and South America combined), EMEA, and APAC (including Japan). Vendors must have customers in each market with no more than 85% of your customer count in its primary region.
- Remote or on-premises "managed" AM — 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 (IP).
- 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.
- AM products that are marketed predominantly or only as open-source offerings.
- Identity governance and administration functionality. This is a separate, but related market covered by other Gartner research (see Magic Quadrant 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).
- Enterprise mobility management (EMM), which is a separate, but related, market covered by other Gartner research.
- CASB, which is a separate, but related market covered by other Gartner research (see Magic Quadrant for Cloud Access Security Brokers).

Honorable Mentions

Vendors Covering All AM Use Cases

Atos (Evidian): Atos provides a traditional WAM product, Evidian WAM, as well as an enterprise SSO, (ESSO) product (Evidian Enterprise Access Management), both of which are delivered as software. (Atos [Evidian] was not included due to the criteria for number of customers.)

Optimal IdM: Optimal IdM offers a full-service offering for customers with complex environments and/or a desire to outsource AM operations. The Optimal IdM product is offered as a single-tenant or multitenant SaaS. (Optimal IDM was not included due the criteria for amount of revenue.)

SecureAuth: SecureAuth provides the SecureAuth Identity Platform, an AM product that is available through multiple subscription plans, and supports SaaS, software or hybrid deployments. (SecureAuth was not included due to the criteria for number of customers.)

Transmit Security: Transmit Security offers the Transmit Security Platform, a SaaS-based AM platform, with integrated orchestration and online fraud detection. (Transmit Security was not included due to criteria for number of customers.)

Vendors Covering Only External Identities

Akamai: Akamai, provides the Akamai Identity Cloud, an AM offering for external identities based on its acquisition of Janrain. The Akamai Identity Cloud is a SaaS-delivered product. (Akamai was not included due to the criteria for the number of customers.)

SAP: SAP provides the SaaS-delivered SAP Customer Data Cloud, which offers three enterprise solutions: SAP CIAM for B2C, SAP CIAM for B2B, and SAP Enterprise Consent and Preference Management. (SAP was not included due to the criteria for number of customers.)

Salesforce: Salesforce's CIAM offering is known as Customer 360 Identity. The Salesforce platform for AM for external identities is a SaaS-delivered product. (Salesforce was not included due to not meeting the overall inclusion criteria.)

Platform Vendors

AWS: Amazon Web Services (AWS) offers AM functionality to AWS customers, including SSO, MFA and directory services. AWS is an IaaS offering. (AWS was excluded due to not meeting the technical inclusion criteria.)

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

Evaluation Criteria

This is how organizations and products were evaluated. The evaluation criteria and weights tell you the specific characteristics and their relative importance, which support the Gartner view of the market. They will be used to comparatively evaluate providers in this research.

Ability to Execute

Gartner analysts evaluate vendors on quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to

positively affect revenue, retention and reputation in Gartner's view of the market.

Product or Service: The architecture, security and capabilities, quality and feature sets of AM that can be integrated with any of a variety of enterprise and cloud-based systems. We evaluate offerings that were generally available and documented as of 30 May 2020.

The range and quality of AM features, richness of support for mobile endpoints, incorporation of third-party identities, and controls demonstrated to help ensure the continuity, security and privacy of customers and their data were also assessed.

The applicability and suitability of these offerings to a wide range of use cases and different application architectures, across different communities of users and different enterprise and cloud-based systems, were evaluated. Elements of evaluation criteria include:

- General product architecture
- Security, scalability, availability and regional coverage
- Administer internal and external identities
- Directory and identity synchronization
- User self-service capabilities
- Authorization and adaptive access
- User authentication methods
- API access controls
- BYOI integration
- Standard application enablement
- Nonstandard application enablement
- Event logging and reporting

Overall Viability: The vendor's overall financial health, its financial and practical success in the AM market. The likelihood that the vendor will continue investing in its AM portfolio and sustain its presence in the AM market was also evaluated. We also assessed its success in the AM market, as demonstrated by its customer acquisition, competitiveness, retention and customer significance in terms of implementation scale.

Criteria include:

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

Sales Execution/Pricing: The vendor's capabilities in such areas as deal management, presales support and the overall effectiveness of the sales channel, including value-added resellers (VARs) and third-party managed service providers (MSPs). The vendor's track record in competitive wins and business retention was also assessed, as was its pricing over a number of different scenarios.

Criteria include;

- Sales execution
- Revenue breakdown by channel
- Pricing under different scenarios

Market Responsiveness/Record: The vendor's 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 considered the vendor's history of responsiveness to changing market demands. How the vendor can meet customers' evolving AM needs over a variety of use cases was assessed, as was how the vendor has embraced standards initiatives in the AM and adjacent markets, and responded to relevant regulation and legislation.

Criteria include:

- General responsiveness
- Meeting customer needs in different use cases
- Responsiveness to embracing open standards

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the vendor'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, thought leadership, social media, referrals and sales activities.

Criteria include:

- Marketing activities and messaging
- Visibility

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

Criteria include:

- Customer relationship and services
- Customer satisfaction

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

Criteria include:

- People
- Processes

Table 1: Ability to Execute Evaluation Criteria

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

Evaluation Criteria ↓	Weighting ↓
Operations	Medium
As of October 2020	

Source: Gartner (November 2020)

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 that demonstrate a high degree of completeness of vision, demonstrate a capacity to understand challenges that buyers in the market are facing, and for shaping their product offerings to help buyers meet those challenges.

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

Criteria include:

- Understanding and meeting customer needs
- Vendor awareness of the future of the AM market, and its strategy for responding

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

Criteria include:

- Deal close rate
- Lead development breakdown

Sales Strategy: A sound strategy for selling the vendor's AM offerings that uses the appropriate networks, including direct and indirect sales, marketing, service, and communication. Whether the vendor has partners that extend the scope and depth of its market reach, expertise, technologies, services and customer base was also assessed.

Criteria include:

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

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes market differentiation, functionality, methodology and features, as they map to current and future requirements. How the vendor will increase the competitive differentiation of its AM products and services was assessed, as was the vendor's participation in AM and adjacent standards development. How the vendor's AM offerings and strategy fit into current and planned adjacent offerings in IAM, as well as other markets, was evaluated.

Criteria include:

- Meeting customers' selection criteria and the needs created by architectural and operational changes to endpoint, identity provider and target resources
- Specific development plans
- Miscellaneous strategy elements

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

- Purpose in the AM market
- Distinction in the AM market
- Milestones reached
- Future growth plans

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.

Criteria include:

- 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. The vendor's continuing track record in market-leading innovation, and the provision of distinctive products, functions, capabilities, pricing models and so on, were assessed. We focused on technical and nontechnical innovations introduced since January 2019, as well as the vendor's roadmap during the next few years.

Criteria include:

- Foundational innovations
- Recent innovations (during the past year)
- Planned innovations

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

Criteria include:

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

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Low
Sales Strategy	Medium

Evaluation Criteria ↓	***Weighting*** ↓
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Medium
As of October 2020	

Source: Gartner (November 2020)

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. They show evidence of how AM plays a role in a collection of related or adjacent product offerings. Leaders typically demonstrate solid customer satisfaction with overall AM capabilities, the sales process, and/or related service and support.

Challengers

Challengers show strong execution and 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 or restricted to specific functions, platforms, geographies or services. Challengers have relatively low brand awareness. 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. Visionaries are noted for their innovative approach to AM technology, methodology and/or means of delivery. They may see AM as a key part of a broader service portfolio, or they may provide functionality, marketing and sales to successfully target specific buying segments, such as developers. They often may have unique features and may be focused on a specific industry or specific set of use cases. In addition, they have a strong vision for the future of the market and their place in it.

Niche Players

Niche Players provide AM technology that is a good match for specific use cases. They may focus on specific industries or have a geographically limited footprint; however, they can outperform many competitors. Vendors in this quadrant often have relatively fewer customers than competitors in other quadrants, but they may have large customers, as well as a strong AM feature set. Brand awareness is usually low relative to vendors in other quadrants. Vision and strategy may not extend much beyond feature improvements in current offerings. Pricing might be considered too high for the value provided by some niche vendors. 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

According to Gartner's Security and IAM Solution Adoption Trend Survey, 2020, AM is the most often adopted IAM technology overall (76% of respondents). A majority of AM deployments run on-premises, managed by clients themselves (43% of all responses), versus 33% in the cloud. Thirty-three percent of all respondents plan to implement a SaaS-delivered AM solution by 2021, 11% by 2023, and 8% by 2025 or later.

The No. 1 reason for new AM solution replacements is for shifting an incumbent solution into a SaaS-delivered platform. When buying a new IAM solution (including AM), 51% of respondents believe the most important aspect would be a full feature set, and that the IAM products must be able to fulfill all of the organization requirements.

The second most important aspect for 40% of new buyers, was that IAM products must run as a service (SaaS or hosted/managed services). And the third aspect would be a cheaper, broader (bundled), converged platform that offers multiple IAM functions, even if it's not capable of fulfilling all of the requirements at once (42% agreed).

Internal and External Identities

Previous access management Magic Quadrant research has classified AM use cases under the broad categories of B2E (business-to-employee), B2B (business-to-business), and B2C (business-to-customer). Add to this the confusion of G2C (government-to-citizen), iterations such as B2B2C, gig workers, temp workers, etc., and the categories of use cases have multiplied, while the borders

separating them have become more muddied. In addition, the explosion in adoption for work from home (WFH) has blurred the line between types of workers.

In this context, for this Magic Quadrant research, we have broken out the use cases, and assigned features and functionalities for two categories, internal identities (workforce, extended workforce) and external identities (vendors, business partners, gig workers, consumers, citizens). Although there will be specialization for the various user communities, from an AM perspective, features and functionalities can be loosely, but accurately, grouped according to these definitions.

Remote Work

The vision for AM has always been remote-work-centric, or at least remote-work-agnostic, to ensure that "any user, can work anywhere, on any application, from any device." However, the global health crisis and the subsequent shutdowns across the world has brought this approach to reality far more quickly, and more definitively than any conventional technology or business driver could have.

At the beginning of the crisis, as companies began scrambling to enable large amounts of remote work, we saw a variety of AM vendors offering free deals for licensing. These deals might have been limited in a variety of ways, but they did provide helpful tools to businesses across the spectrum in terms of verticals, the ability to resume operations in the face of global shutdowns. And Gartner anticipates this will not be a temporary condition, it has long been within the capabilities of AM to facilitate this approach to work, but we see the market increasingly embracing this long term.

According to Forecast Analysis: Remote Workers Forecast, Worldwide through 2024, around 30% of all employees working remotely will permanently work from home. By the end of 2024, the change in the nature of work will increase the total available remote worker market to 60% of all employees, up from 52% in 2020. By 2024, in-person meetings will drop from 60% of enterprise meetings to 25%, driven by remote work and changing workforce demographics. These developments in the market will continue to benefit AM vendors and technology.

CARTA and Zero Trust

Driven by the factors of remote work, and the hybrid environment, securing application access has continued to grow in importance. The changing world of AM has been beneficial from an operational perspective, but less so from a security perspective (see Secure Application Access by Applying the Imperatives of CARTA to Access Management).

As companies worldwide transition many of their workforce to remote, the number of inquiries asking for strategies for leveraging AM following CARTA approaches have increased. However, as described in Zero Trust Is an Initial Step on the Roadmap to CARTA, many organizations that hear about zero trust are not necessarily sure about what it means. At its core, zero trust means replacing implicit types of access decisions with explicit, risk-appropriate, lean-trust access decisions. By leveraging identity data and a wide variety of contextual and other signals, modern AM platforms can assess risk and trust dynamically, and apply continuous adjustments of risk or trust in an explicit manner.

With continuous visibility of risk/trust levels, security infrastructure can adapt accordingly — for example, blocking downloads or terminating access.

CARTA is a strategic life cycle approach to information security that can be applied to access protection. Although improving initial access decisions can be improved with the adoption of adaptive access/conditional access, this alone is not enough. A full CARTA-inspired offering would continue monitoring user and device risk/trust signals throughout the entire session. This would enable security infrastructure to adapt accordingly, if the risk measured is too high, or the trust in the user/device falls too low. Finally, a complete solution would also analyze entitlements used versus provisioned and offer suggestions on how to reduce risk via entitlement trimming.

AM vendors are providing ever-advancing security controls, from more-advanced identity proofing approaches, and other sources of risk, to allow more visibility and control during session authorizations. We are seeing AI and ML sorting out massive amounts of data and providing CARTA-aligned visibility and control for AM practitioners. And we are seeing vendors start to provide simple, straightforward orchestration capabilities, enabling customers (typically working with the application owner) to easily craft complex authentication and authorization journeys. For this research, controls that contribute to CARTA approaches have been highlighted, especially in regard to critical capabilities such as authorization and adaptive access controls.

Although this maturity in approach has benefited many companies and users, the anchor of legacy infrastructure has tempered that success. With some exceptions, AM is not the right approach for protecting resources such as nonweb, (client/server or thick client) types of applications, or resources such as network-attached devices. For these resources, an important adjacency has been gaining traction — ZTNA, also referred to as a software-defined perimeter, (SDP). Although this research does not cover ZTNA, AM practitioners must be aware of how the complexity of their application portfolio may drive them to additive approaches such as ZTNA, in combination with and as a natural adjacency to AM.

Convergence

More than 80% of organizations are planning to pursue a security vendor consolidation strategy during the next two to three years. The main reason (37%) is improvement of organizational risk posture (see Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?). We continue to see a convergence between the AM and IGA markets, and some vendors are even bringing PAM functionality into the AM universe.

In an example from the past year, platform vendors such as Oracle, IBM, ForgeRock and Microsoft can bring adjacencies to bear from large portfolios of products. IBM, is including its full IGA platform with no additional cost with its AM subscription of IBM Verify. Oracle has included light IGA capabilities with IDCS, but continues to offer Oracle Identity Manager and Oracle Identity Governance separately. ForgeRock has added more governance capabilities to provide a full IGA module as a

separate product. And Microsoft has been building elements of identity governance and privileged access management in the Azure AD product.

Okta has slowly expanded its basic IGA functionality with LCM, by adding workflow capabilities, and have added a subset of PAM capabilities with Okta Advanced Server access. Ping Identity brings data governance and fine-grained dynamic authorization to the forefront with PingDataGovernance. Finally, Idaptive's acquisition by CyberArk brings the potential for merging PAM capabilities with AM functionality.

Cost Optimization

As we see companies across the world continue to recover, and hopefully renew, from the impacts of the global health crisis, we anticipate that many difficult cost optimization conversations will be taking place. From an IT budgeting perspective, those conversations may be driving many companies to consolidate investments in duplicate IAM products, prioritizing products that are easier to manage and support. This is also expected to drive organizations to select vendors offering more-extensive suites of IAM tools, even if every IAM tool is not the best in the market, over vendors that are specialists in a particular area. We expect this to maintain pressure on AM vendors to continue to add convergence into other IAM towers for their products.

Market Overview

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

- The AM market has evolved to support more diversity in user authentication methods and flows, managing basic access to IoT devices, contextual and more comprehensive adaptive access, mobile computing, and API target services. These feature sets continue to mature in 2021.
- Vendors that have developed AM as a service have risen in popularity. Gartner estimates that 90% or more of clients based in North America, and approximately 65% in Europe and the APAC region countries, are also seeking SaaS-delivered models for new AM purchases. This demonstrates a preference for agility, quicker time to new features, elimination of continual software upgrades, reduction of supported infrastructure and other SaaS versus software benefits demonstrated in the market. (See How to Choose Between Software and SaaS Delivery Models for Identity and Access Management.)
- Large, established vendors and others that provided only traditional software- and appliance-based AM solutions have moved to offer SaaS delivery models as options for their AM tools.

All but one of the vendors covered in this Magic Quadrant deliver AM as SaaS as their only delivery model, or as an option. Several vendors are offering a managed service offering as well:

- **Only as a Service**: CyberArk (Idaptive), Microsoft, Okta and OneLogin

- **Software and/or SaaS-Delivered AM:** Auth0, ForgeRock, Thales (Gemalto), IBM, Oracle and Ping Identity
- **Only as Software:** Micro Focus

Gartner estimates that the AM market revenue for the vendors covered in this Magic Quadrant was $1.7 billion at the end of 2019. Readers, particularly investment clients, are cautioned not to interpret this revenue estimate as accounting for all AM products and services available in the market. Numerous vendors that could not be included in this Magic Quadrant can meet at least partial requirements — for example, by providing user authentication and SSO, when authorization enforcement is not needed by the customer.

Evidence

Primary Research; Gartner's Security and IAM Solution Adoption Trend Survey, 2020: This study was conducted to learn what security solutions are organizations benefiting from and what factors affect their choice/preference for such solutions. The research was conducted online during March through April 2020, among 405 respondents from North America, Western Europe and APAC regions. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at the manager level or above (excluding C-suite), and they should have a primary involvement and responsibility in risk management role for their organizations.The study was developed collaboratively by Gartner Analysts and the Primary Research Team, which follows SRM:

- Vendor surveys
- Peer Insights
- Secondary resource services
- Gartner inquiries

Evaluation Criteria Definitions

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business

unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

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

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

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

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

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

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

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