Gartner

Buyer's Guide for Access Management

Published 14 December 2020 - ID G00727476 - 23 min read

By Analysts Henrique Teixeira, Michael Kelley, Abhyuday Data

Initiatives: Identity and Access Management and Fraud Detection

Access management solutions are mature, rich with features and offer a broadened scope that overlaps with many adjacent areas. Security and risk management leaders responsible for IAM and fraud should follow these five steps to select a long-lasting, cost-efficient AM solution.

Overview

Key Challenges

- Access management (AM) initiatives can be championed by disparate stakeholders with different goals for external and internal users. AM initiatives with an initial focus on only one population can be expensive or lack features when extended to another.
- AM capabilities keep growing, overlapping and converging with adjacent identity and access management (IAM) and security markets, like user authentication, identity governance and administration (IGA) and API security. Such overlap complicates mapping the organization's own IAM business requirements and use cases relevant to AM.
- Recent AM technology buying initiatives have been driven by tactical needs, like securing remote access to employees, workforce collaboration and customer portals, leading to emergency investments and disproportionate spending.
- RFPs very often include other adjacent requirements that are not core to AM, reducing the quality of the responses and the mix of vendors that participate.
- Choosing a shortlist of vendors to participate in an RFP process can be daunting given the sheer number of viable companies that deliver some (but not all) of the core AM capabilities.

Recommendations

Security and risk management (SRM) leaders overseeing IAM and fraud detection should:

- Align disparate stakeholders by identifying and communicating clear drivers for making the AM investment. Explain its importance for enabling business, enhancing user experience (UX), improving operational efficiencies, improving security or meeting compliance requirements.

- Take a structured approach to inventorying AM business requirements by assessing use cases, application inventory and scope of AM adjacencies for both external and internal users.
- Evaluate the AM needs of your organization by mapping internal drivers and use cases to external trends like convergence of IAM features, SaaS adoption, passwordless authentication, adaptive access, open source and cybersecurity mesh.
- Write a high-quality RFP by highlighting and comparing only AM core capabilities, and be explicit about whether an integration or embedded capability is expected for adjacent areas.
- Draw up a shortlist of AM vendors using Gartner's Magic Quadrant and Critical Capabilities research on access management as a guide. Support this with your own research by following a five-step process to include vendors that are aligned with your main drivers, and that address your inventory of apps and use cases, for today and for the future.

Introduction

AM technologies are mature and feature-rich as ever, with a broad, fuzzy border of capabilities that overlap with many IAM adjacent areas like IGA, API on-premises management and user authentication (see IAM Leaders' Guide to Access Management).

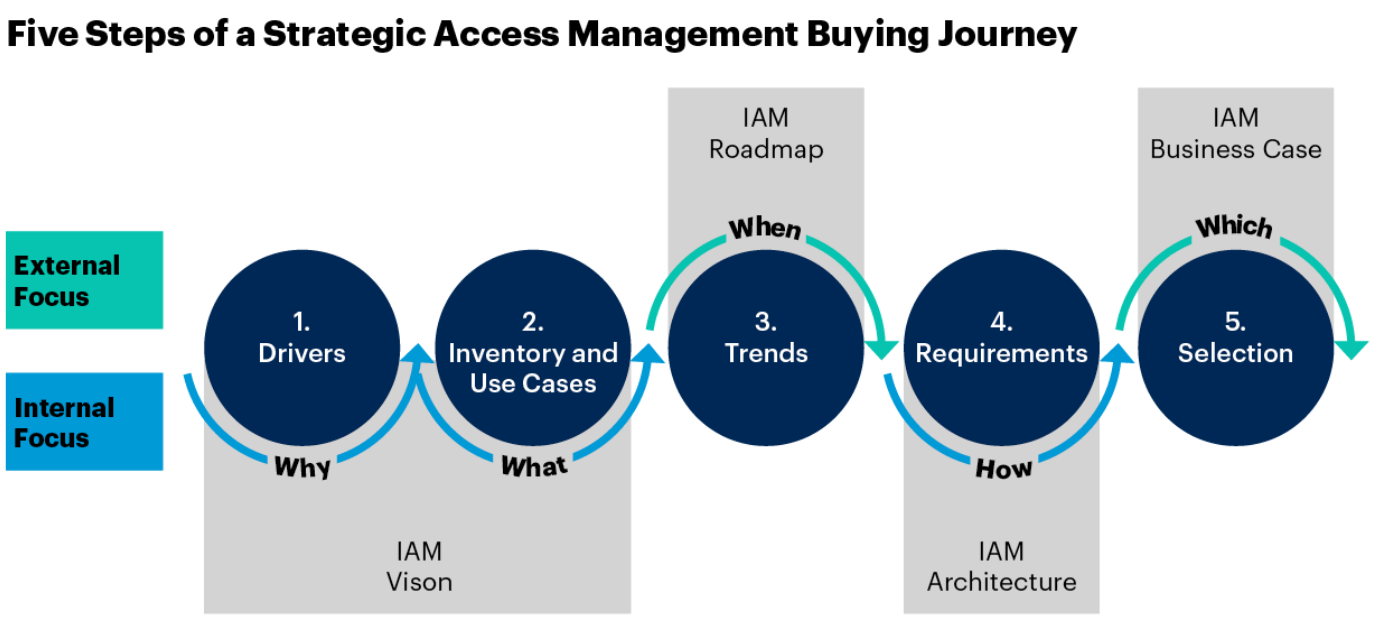
The recent enforced movement to lockdowns and remote work trends has been driving AM acquisitions for tactical emergency response purposes, including securing remote access to employees, workforce and B2B collaboration, and customer portals.

The combination of a growing scope of capabilities and tactical short-term planning for buying AM solutions often limits the broader use of AM solutions for future use cases. SRM leaders either overlook gaps in capabilities of such solutions or cannot plan for alternatives, growth and integration requirements.

What should organizations do to avoid buyer's remorse and choose a future-proof AM solution?

SRM leaders responsible for IAM should follow the five-step process in this research for selecting a long-lasting, cost-efficient AM solution (see Figure 1). Some steps require a deeper internal look, to make decisions aligned with the organization's IAM vision and architecture. External focus is recommended for IAM roadmap alignment with market trends and for a successful business case for vendor selection.

Figure 1: Five Steps of a Strategic Access Management Buying Journey



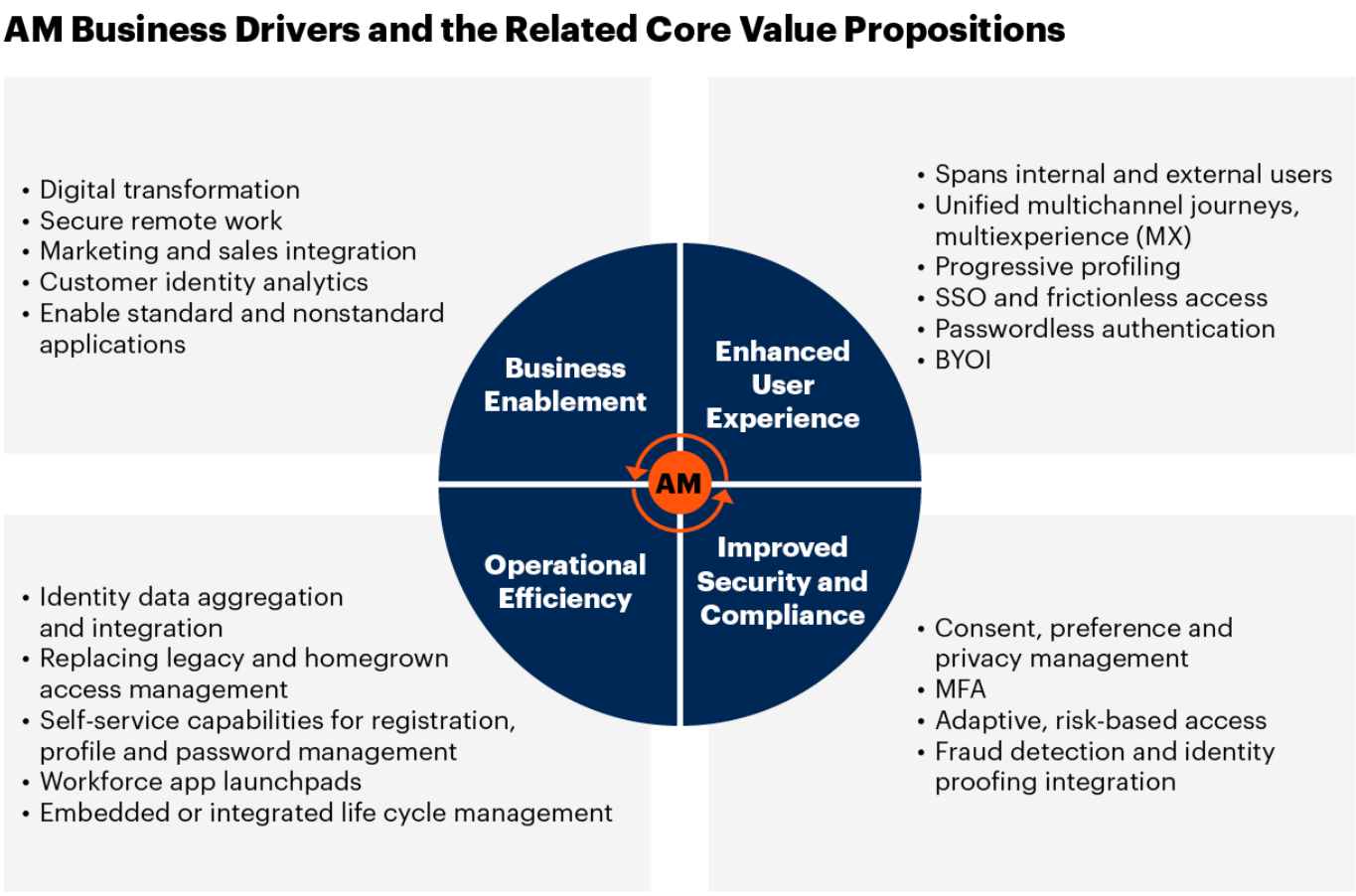
Source: Gartner
Note: IAM = identity and access management
727476_C

Analysis

1. Identify and Communicate Drivers

Start by looking internally first, and identify why making the AM investment is important. This is part of the definition of the organization's IAM vision. Gather stakeholders and identify where the AM initiative fits. Verify its alignment with the overall IAM program and business goals (see A Successful IAM Program Begins With a Vision). Make sure to also include tech professionals like enterprise architects as part of the team of stakeholders and make them participate in the inventory of use cases discovery, as shown in Step 2. Define responsibilities for each stakeholder and find agreement, then document and communicate the biggest drivers of the AM initiative (see Figure 2).

Figure 2: AM Business Drivers and the Related Core Value Propositions

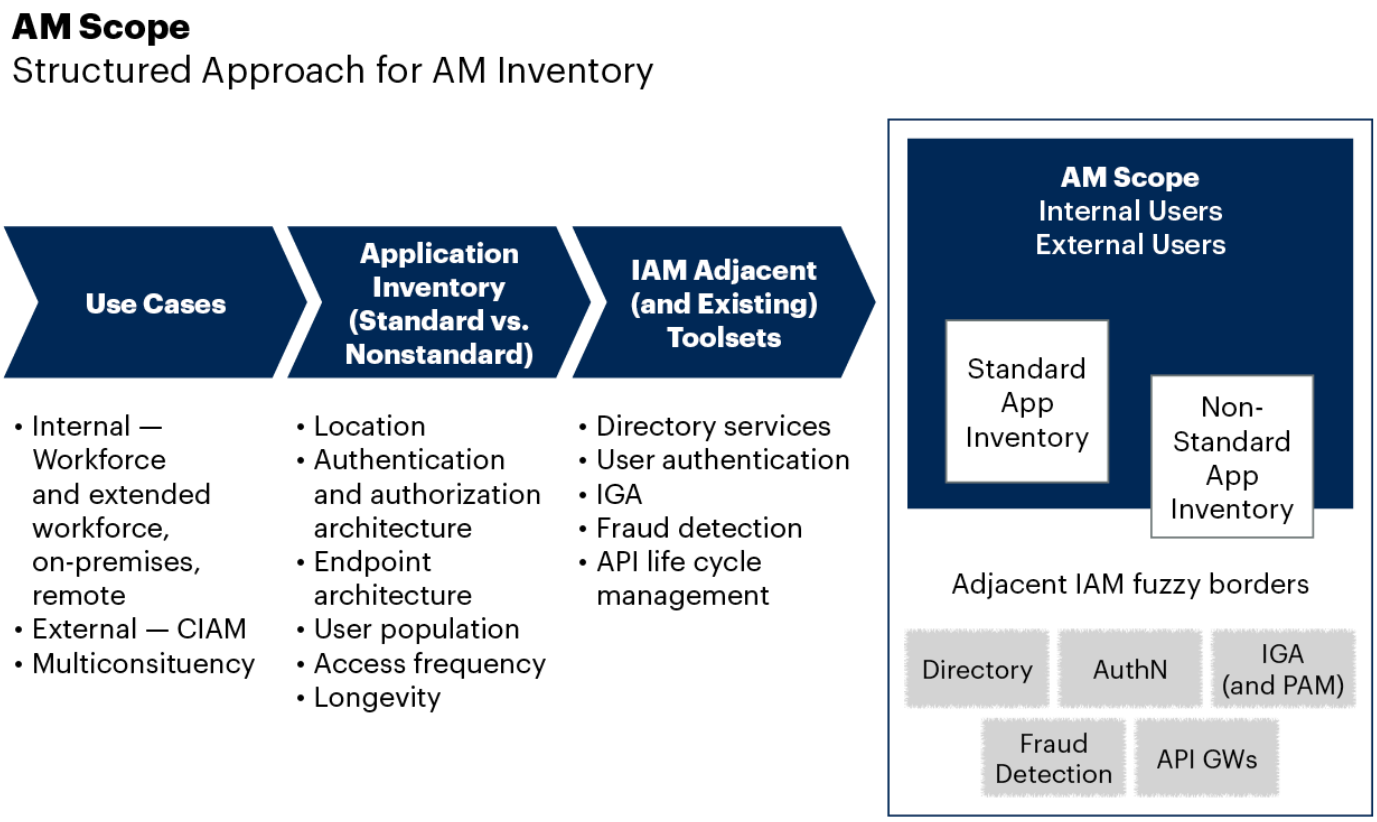


Source: Gartner
Note: AM = access management; BYOI = bring your own identity; MFA = multifactor authentication; SSO = single sign-on
727476_C

2. Inventory AM Business Requirements and Use Cases in a Structured Way

Continuing with an internal focus on the IAM vision, take a structured approach to inventorying AM business requirements, including use cases, application inventory and scope of AM adjacencies (see Figure 3).

Figure 3: AM Scope Results From Use Cases, Applications and IAM Adjacencies Inventory



Source: Gartner

Note: AM = access management; CIAM = customer identity and access management; GWs = gateways; IGA = identity governance and administration; PAM = privileged access management

727476_C

Start by segmenting internal and external access use-case needs. These use cases should be aligned with the business drivers (and core value propositions) documented in Step 1. As described in Technology Insight for Customer Identity and Access Management, one of the most popular requests in CIAM inquiries with Gartner is for recommendations for either using the same or separate IAM identity repository instances for internal and external identities. Except on rare occasions (i.e., very small user populations with similar security and UX requirements), organizations should have separate instances for internal and external identities (these could be both from the same vendor as long your requirements are addressed). Document what AM use cases need to be addressed today and in the future, for both external and internal access.

- **Internal access:** Include business requirements for controlling access by the workforce and extended workforce (like contractors, outsourcers, temporary workers and partners that work as an extension to the workforce).
- **External access:** Requirements for controlling access for B2C, other B2B, G2C and gig economy users (including, but not limited to, consumers, external partners, citizens and contingent freelance talent).

- **Multiconstituency:** Organizations with multiconstituency requirements have a need to address both internal and external users.

Security and risk management leaders can then make an inventory of application and endpoint infrastructure. The keys to success include identifying in-scope applications and determining their current architectures (e.g., if they leverage APIs) and the relative ease with which authentication and authorization can be externalized to an AM solution. Define the following for each app, and separate apps between standard and nonstandard architecture types (both web and nonweb). Be cognizant that nonweb legacy apps, especially those planned to be decommissioned, may never be included as part of the scope for integration:

- Application locations (on-premises, hosted, SaaS)
- Authentication and authorization architecture. Standard: SAML, OIDC, OAuth. Nonstandard web: HTTP header authentication, Microsoft Active Directory (AD) integration, Kerberos, other web-based ERP and collaboration suites. Nonweb legacy apps: LDAP integration, RDBMS, local repositories, proprietary client/server apps
- Provisioning standard (SCIM, SAML and OIDC JIT provisioning, others)
- Endpoint architecture (mobile clients, thick clients, web clients, APIs; used on computers, mobile devices or kiosks)
- User population (on-premises workers, remote workers, customers, partners) and volumes
- Access frequency (as needed — a couple times a year; frequently — a few times a week/month)
- Application longevity (estimated application lifetime)

As part of the discovery, delineate a well-defined scope for the AM inventory by assessing the fuzzy border areas of IAM that are adjacent to AM. Sometimes, an adjacent IAM or security specialist tool will be the best option for addressing specific requirements that are not core to AM. A few, but not all, examples of fuzzy adjacencies include the following:

- **Directory services.** Many AM projects will start with a directory consolidation initiative. A directory synchronization or virtual directory approach can be used in lieu of a full-blown Microsoft AD consolidation initiative, using virtual directory tools. For example, the effort can consolidate identity data and reduce the number of separate user repositories for authentication that need to be integrated. Fewer target directories helps simplify the externalization of authentication and authorization to AM.
- **User authentication.** AM has been incorporating user authentication (most notably multifactor authentication [MFA] capabilities) for a long time. In instances where the use cases are limited to user authentication, a full AM suite may not be needed. Always evaluate if there are scenarios that would better be addressed by a discrete authentication capability (i.e., ease of implementation, need for more

granular authentication policies, native support for OTP tokens) instead of an integrated AM solution (see IAM Leader's Guide to User Authentication).

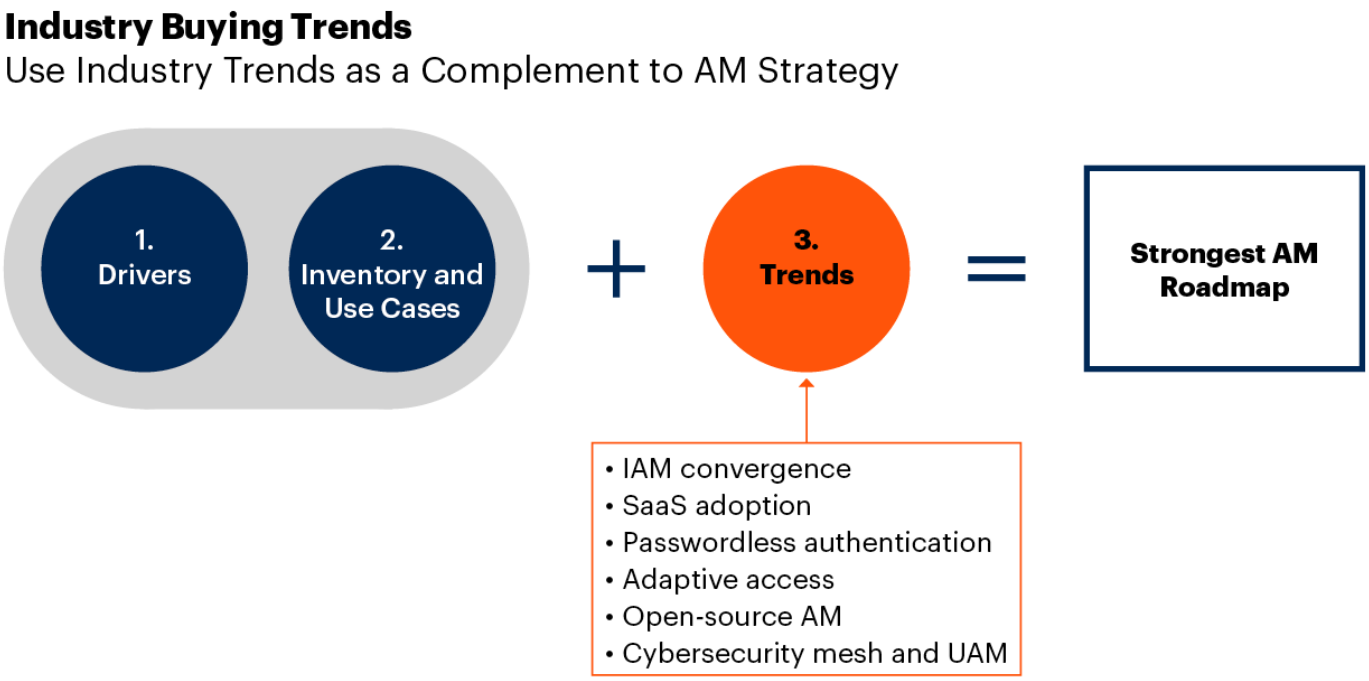
- **Identity governance and administration (IGA)**. Good AM strategies will invariably include identity life cycle requirements. In order to get users authenticated and authorized by AM, their credentials must exist in the directory used by AM, and the users' life cycle needs to be managed. Some AM vendors will include a basic subset of identity life cycle capabilities found in IGA tools (see IAM Leaders' Guide to Identity Governance and Administration). However, it is fundamental to keep a clear separation between IGA and AM requirements. If administration type of controls (like identity life cycle, provisioning, access requests and analytics) are the main drivers instead of runtime authentication and authorization, then IGA should be considered first instead of an AM solution. IGA capabilities for password synchronization or password management tools can also be considered for implementing reduced sign-on strategies to nonstandard applications in scope, which would not support a native AM integration pattern.
- **Fraud detection and identity-proofing.** These requirements are very common, especially in CIAM use cases (see Market Guide for Identity Proofing and Affirmation, Market Guide for Online Fraud Detection).
- **Full API life cycle management.** This type of requirement typically appears in API access control discussions (see the "API access control" profile in Hype Cycle for Identity and Access Management Technologies, 2020).

Finally, evaluate existing toolsets to potentially reduce spending on new solutions. Then, go to the market for solutions that support the existing gaps and anticipated future needs, and that can be implemented with appropriate speed and time to value.

3. Assess AM Trends and Map Them to Your Roadmap Growth Strategy

Now it is time to look outside of the organization and study market and industry trends to define a roadmap. The best approach to avoid a regrettable AM acquisition is to define a roadmap that includes both immediate and long-term goals. Also, make sure the AM roadmap (including drivers, inventory and use cases as defined in Steps 1 and 2) is aligned with external market and industry trends (see Figure 4).

Figure 4: Use Industry Buying Trends to Complement Your AM Strategy



Source: Gartner
Note: AM = access management; IAM = identity and access management; UAM = unified access management
727476_C

Evaluate the future AM needs of your organization. Examples may include the following:

- **Capacity growth (or reduction):** Account for both user population projected growth and new user population constituencies (i.e., a whole new set of external identities for customers as a result of new marketing and business development strategies). Be mindful of instances where you can predict capacity reductions, such as divestitures. SaaS-delivered AM solutions are generally best at managing sharp fluctuations in capacity growth.
- **Infrastructure and application changes:** Look out for changes to the IT infrastructure, including but not limited to applications that may be retired and new applications that may be acquired — a digital transformation shift of workloads to cloud services, for example.
- **New regulations:** Customer data privacy laws, new jurisdictions or other types of governance frameworks may require different approaches for access controls, like strong customer authentication, or may limit choices of AM SaaS providers.

Your buying strategy should also consider the appropriateness of future AM needs against the following trends.

Convergence of IAM Features

AM is one of the IAM markets experiencing an emerging trend of convergence of adjacent capabilities (see Predicts 2020: Identity and Access Management). According to a recent Gartner survey (see Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?), user authentication (including MFA) is the top IAM technology that clients want to purchase as a consolidated feature from a single security vendor (41%), followed by AM (35%). [1] 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," meaning more suites with "good enough" capabilities instead of best-of-breed specialist tools. Popular AM solutions include light IGA functionality, including identity data sources integration via directories services, provisioning and basic workflows. Some basic privileged access management (PAM) functionality is included in at least a few AM vendor products.

- If your needs in IGA and PAM are basic, explore the IGA and PAM functionalities of AM vendors to see if there's an adequate fit.
- If your needs are more advanced in adjacent IAM areas, keep an eye on market development in the AM space, but invest in complementary tools for now. For example, add IGA and PAM to mitigate risk of inappropriate access, making sure those adjacent platforms can at least be integrated with AM for allowing centralized authentication.

SaaS Adoption

Gartner clients appear to have overcome their fears of the perceived risk of SaaS-delivered AM solutions (availability, security) in favor of the benefits. Those benefits include: better economics, especially for scaling up or down quickly with reduced operational costs, better reliability, and quicker time to value for new features and functionality. This has created a market that is very heavy for SaaS-delivered offerings. Gartner estimates about 80% or more of new AM products purchased in North America in 2021 will be SaaS-delivered offerings. However, driven by the requirements of hybrid environments, or by a high risk requirement for data residency, or need for control, there are still many customers who prefer software-driven AM solutions; for example, the majority of incumbent AM deployments are still on-premises managed by clients themselves (43%). [1]

- Customers with primarily modern applications and without an extensive set of requirements for data residency should include SaaS-only vendors in their shortlist for AM tools.
- Customers with hybrid environments and lots of legacy applications and/or data residency requirements should consider software-delivered AM tools, strong nonstandard application enablement capabilities (like reverse proxy support) in cloud-hybrid deployment approaches, or augment their SaaS-delivered tools with software-delivered components.

Passwordless Authentication

Client interest in passwordless authentication continues to build. However, there are many ways to eliminate passwords, and technological constraints make a single universal approach elusive. Several vendors have come to market with novel passwordless methods and we see increasing support for

FIDO2 authentication protocols. Gartner projects that multiprotocol “mobile MFA” apps will become mainstream in the next 12 to 18 months, facilitating the transition to FIDO2 as the preferred approach and enabling passwordless MFA (see Market Guide for User Authentication). However, many AM vendors enable passwordless authentication flows without the need for any novel technology and it’s likely that this will be many organizations’ first experience of passwordless authentication rather than mobile MFA or “raw” FIDO2. Organizations looking to implement passwordless strategies integrated with AM must clearly define use cases, infrastructure, UX and other goals (i.e., offline devices can be a challenging use case for AM-delivered passwordless authentication). Ubiquity is not necessary to make headway, but beware of marginalizing some constituencies. Also, give preference to AM tools that support open standards like FIDO2.

Adaptive Access

As described in Magic Quadrant for Access Management, 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 (see Secure Application Access by Applying the Imperatives of CARTA to Access Management). Organizations planning for implementing more seamless and secure access for remote workers and customers should look for strong adaptive access capabilities for session establishment, session management and session termination. 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.

- Expand the volume of contextual signals that are available, either through the AM tool, or an adjacent tool or technology, such as a cloud access security broker (CASB) or fraud detection tool.
- Develop adaptive access scenarios, taking a risk-based approach and using contextual and other signals to develop risk scores that indicate appropriate access to those applications.
- Consider adopting a low-code/no-code approach (from access orchestration capabilities in AM tools, or using a specialist tool) for mapping contextual signals to adaptive access flows to accommodate complex adaptive access decisions.

Open-Source AM

Some clients, driven by the possibility of lower licensing costs, along with open access to source code, are drawn to open-source AM tools. In fact, between 2017 and 2020 there was an 8% increase in respondents who wished to change their current AM solution to an open-source one. There are many good open-source tools on the market, including Gluu, Keycloak, IdentityServer, OpenIAM, Shibboleth, Soffid and WS02. But going open source involves considerations beyond licensing and support. Open source requires a very strong developer-oriented culture for an IAM organization.

Another reason for considering open source is the access to source code. Open-source tools can provide customers with transparency for what the code driving their AM tool is actually doing. Geopolitical

concerns have made some customers cautious about adopting security tools developed in certain regions of the world, concerns that they may not have visibility into everything that is going on “under the covers.” An open-source tool eliminates those concerns with full visibility, transparency and access to the source code.

Finally, there is the element of participation in an open-source community, which shares solutions to common problems. For example, one customer may develop a function to ingest threat data from an obscure source of data, and that code can be easily reused by any other user of that software.

Is open source right for your organization?

- Assess the skills and culture of your IAM team and take stock of the appetite for developing, as opposed to configuring, functionality in an AM tool. The desire for (and ability to deliver) internal IAM initiatives, like deploying an authorization server that can act as an identity hub to all external-facing IAM systems, can be a good indicator of that appetite.
- Analyze licensing. While open-source options can be less expensive than commercial offerings, you may find that when accounting for training, support and other factors, cost may break even, or be close enough to not be a large factor in the decision.
- Understand and handle source code, including the inadequacies of such code in comparison to commercial options.

Cybersecurity Mesh and Unified Access Management

As described in Top Strategic Technology Trends for 2021, by 2025, the cybersecurity mesh model will support over half of digital access control requests. This means cybersecurity mesh will be paving the way to a more explicit, mobile and adaptive unified access management (UAM) model. It offers a more integrated, scalable, flexible and reliable approach to digital asset access control than traditional security perimeter controls. With this approach, security is no longer baked into assets; it is now modularly bolted on through APIs or HTTP. Early examples of this model, in the context of IAM, exist in the Open Policy Agent (OPA) standard and Styra’s product, which can be used to enforce policies in microservices, Kubernetes, continuous integration/continuous delivery (CI/CD) pipelines, API gateways, cloud and mobile apps, and more.

- Organizations that look toward microservices (and policy enforcement capabilities for microservices) should consider AM tools that offer fine-grained authorization and CARTA-aligned adaptive access control in AM, which are fundamental cornerstones for this trend.
- Look for more OPA support or integration in AM tools in the future, and possible emergence of other implementations of OPA for policy authorization and enforcement.
- Traditional externalized authorization management (EAM) specialized tools, and other fine-grained authorization solutions for policy definition and enforcement, can be an intermediary step into the definition of a UAM model for the cybersecurity mesh.

As a result of this step, the IAM leader responsible for selecting an AM tool must have a strong list of high-level technical requirements that can be separated into short-term and long-term ones. For example:

- **Short-term requirement:** Stronger API access control (because of microservices investments today), together with WAM for addressing a number of legacy on-premises nonstandard apps.
- **Long-term requirement:** Stronger adaptive access controls and passwordless authentication may be needed as customers' projected growth will require better frictionless user experiences.

4. Choose High-Impact AM Technical Requirements for a Short, Clean and Neat RFP

Looking again internally to the organization, start writing an RFP based on your own business and technical requirements instead of vendors' strengths. This will help you to avoid a "beauty contest," where the only differentiation between vendors is how nicely one vendor words its response over another. Also, add your business drivers (Step 1) right at the beginning of the RFP, and provide as much detail as possible about your AM inventory (Step 2). This step defines the technical requirements of your AM architecture.

When writing an AM RFP, remove redundant or extraneous requirements obtained in Step 3 by highlighting and comparing only core AM capabilities. If other adjacent capabilities are needed, be clear and concise if either an integration or embedded capability is expected. (See Step 2 above for the fuzzy borders of AM).

Leverage Gartner research to simplify the process of prioritization of technical requirements. Study Critical Capabilities for Access Management. Select one of the three use cases that best matches your own needs and use the guidance in Figure 5 below as a suggested prioritization of high-importance capabilities to be mandatory items in the RFP document.

Figure 5: AM Core Capabilities Mapped to Use Cases

AM Core Capabilities Mapped to Use Cases

■ Highest Score, Mandatory Capabilities Based on Use Case ■ Medium Score, Desired Capabilities Based on Use Case ■ Lower Score, Optional Capabilities

AM Critical Capablities	Use case		
	Internal	Exernal	Multiconstituency
Administer internal and external identities	M	M	H
Directory and identity synchronization	L	M	H
User self-service capabilities	L	H	H
Authorization and adaptive access	H	M	H
User authentication methods	H	M	M
BYOI integration	L	H	M
Standard application enablement	H	L	M
Nonstandard application enablement	H	H	M
API access controls	M	M	M
Event logging and reporting	L	L	L

Source: Gartner
Note: AM = access management; BYOI = bring your own identity
727476_C

Gartner

This guidance can be adjusted according to individual particularities and requirements of each organization.

Most important, when documenting the critical capabilities selected above, don't just ask yes/no questions. Instead, craft open-ended questions to uncover creative, superior or unexpected methods that vendors would suggest to address a specific requirement. This includes crucial advice on how to define a successful structure for the RFP and examples for wording of open-ended versus closed questions.

At the end of this step, you will have an RFP that is ready to distribute to a shortlist of vendors.

5. Draw Up an AM Shortlist for Vendor Selection

Finally, look externally again. Leverage Magic Quadrant for Access Management and Critical Capabilities for Access Management and do your own research (including calls with Gartner experts) to uncover additional vendors that could be part of your shortlist. Keep in mind that there are many successful vendors that are not listed in the Magic Quadrant, because they may only focus on a subset of the market. However, if your organization is in the focus of the vendor, there could be some great reasons to

take a closer look. Shortlisted vendors should be the ones that are aligned with your main drivers identified in Step 1; are able to address your inventory of apps and use cases defined in Step 2; are able to address future growth and trends documented in Step 3; and have strong technical abilities in the streamlined list of technical requirements obtained in Step 4.

At this stage, watch out for gaps in AM product functionality by identifying AM solution weaknesses relevant to your requirements. For example (not an exhaustive list):

- If you have a high percentage of legacy, on-premises apps, give preference to AM vendors with stronger capabilities for nonstandard app integrations.
- If your current or future strategy requires external use cases for CIAM, give preference to AM vendors with very strong user self-service capabilities and bring-your-own-identity (BYOI) integration, and prepare for preemptive integration planning with fraud detection, consent and privacy management.
- If you are embracing microservices development, Kubernetes or if extensive integrations with adjacent technologies are needed, choose vendors with strong API access control capabilities.
- If planning for AM for the workforce, look for solid directory services and IGA integration strategies.

Beware of AM vendors that don't offer out-of-the-box integration capabilities with adjacent IAM technologies that will be important to fulfill your requirements, as described in Step 2.

Negotiate strategically with finalist AM vendors by asking for pricing proposals that include your organization's AM growth requirements as documented in Step 3. This can lead to better volume discounts and future-proofed investments. Not all vendors charge based on the same usage models (per user, active users per month, infrequent users). Learn to differentiate and choose the best cost-efficient model based on your current and future requirements.

SRM leaders responsible for choosing an AM solution should use some general negotiation tips, as listed below:

- Negotiate discounts on the basis of the length of the term. Three years has become the standard, but there are exceptions being accepted for shorter terms. Contracts longer than three years should only be considered if significant discounts are offered. Look for volume discounts on individual products based on term length, number of products bought, and volume for which the products are being bought to get effective pricing.
- Acquire licenses needed for the current volume. Negotiations for *future* licenses should be done upfront. Once a contract has been signed and the base product has been deployed, the vendor's incentive to offer discounts for additional licenses is drastically reduced. Contracts should be negotiated on a global basis, based on current needs. Negotiate a fixed price for future additional licenses that may be needed during the term.

- Leverage third-party advice, such as Gartner BuySmart, before signing contracts. Contracts and proposals grow more complex every year. Vendors introduce new pricing, licensing models, maintenance options and audit clauses every day. Unless one has day-to-day market visibility, it is nearly impossible to keep up.

- Review vendor packaging deals. To address/suffice your AM requirements and get effective volume discounts on each product, look for pricing breakdown for individual products or modules to be bought. Be wary of "all inclusive package pricing" that does not individually list the price for individual components. Experience has shown that it is virtually impossible to drop an unused component later on. Always ensure that you are negotiating for the latest packages, and not just renewing existing entitlements. Don't expect the vendor or value-added reseller (VAR) to suggest lower-cost or more inclusive packages unprompted.

- Start renewal negotiations early. Renewal negotiations should begin at least six months before the contract expiration date, to provide enough time for competitive bidding and migration planning, if desired. Late renewal negotiations shift the advantage to the incumbent vendor, because there is not enough time to seriously consider switching to an alternative.

Evidence

[1] **Gartner's 2020 Security and IAM Solution Adoption Trend Survey:** This study was conducted to learn about which security solutions organizations are benefiting from and what factors affect their choice/preference for such solutions. The research was conducted online during March and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue of less than $500 million. Respondents were required to be at manager level or above (excluding the C-suite) and to have a primary involvement and responsibility in risk management roles for their organization.

The study was developed collaboratively by Gartner analysts and the Primary Research Team that follows security and risk management.

Additional references:

- Access Management Magic Quadrant and Critical Capabilities surveys
- Over 2,100 AM-related inquiries between December 2019 and December 2020

Recommended by the Authors

IAM Leaders' Guide to Access Management

Magic Quadrant for Access Management

Critical Capabilities for Access Management

Technology Insight for Customer Identity and Access Management

Solution Comparison for Customer Identity and Access Management Capabilities of 9 Vendors

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

Enhance Remote Access Security With Multifactor Authentication and Access Management