2024 Planning Guide for Identity and Access Management

Published 4 October 2023 - ID G00796445 - 69 min read

By Analyst(s): Erik Wahlstrom, Homan Farahmand, Mary Ruddy, Paul Rabinovich, Nat Krishnan, Gautham Mudra, David Chase

Initiatives: Identity and Access Management for Technical Professionals; Meet Daily Cybersecurity Needs

> IAM is a foundational enabler of business. Security and risk management technical professionals must mature their IAM architecture strategies, resolve IAM technical debt, and reestablish basic hygiene to provide identity-first security that enables all required IAM use cases.

Overview

Key Findings

- Identity and access management (IAM) is about business enablement, and all security strategies are now identity-first security strategies. Threat actors are increasingly targeting single identities as well as the IAM infrastructure itself, increasing the relevance and the scope of IAM. It all places growing demands on IAM architecture, integrations, usability and teams.
- Identity-first security requires identity fabric approaches to IAM architecture in order to reduce gaps; provide composability, interoperability and agility; and minimize delays in detecting and responding to problems.
- IAM technical debt — a technical accumulation of suboptimal or inefficient IAM decisions — reduces maintainability, slows development, hinders innovation and increases the risk with an aggregation of badly managed IAM tools and identities.
- AI and advanced identity data analytics are playing a growing role in almost every area of IAM, and it enables IAM operations to be more risk-aware and automated with better visibility.

Recommendations

As a security and risk management technical professional focused on IAM, you should:

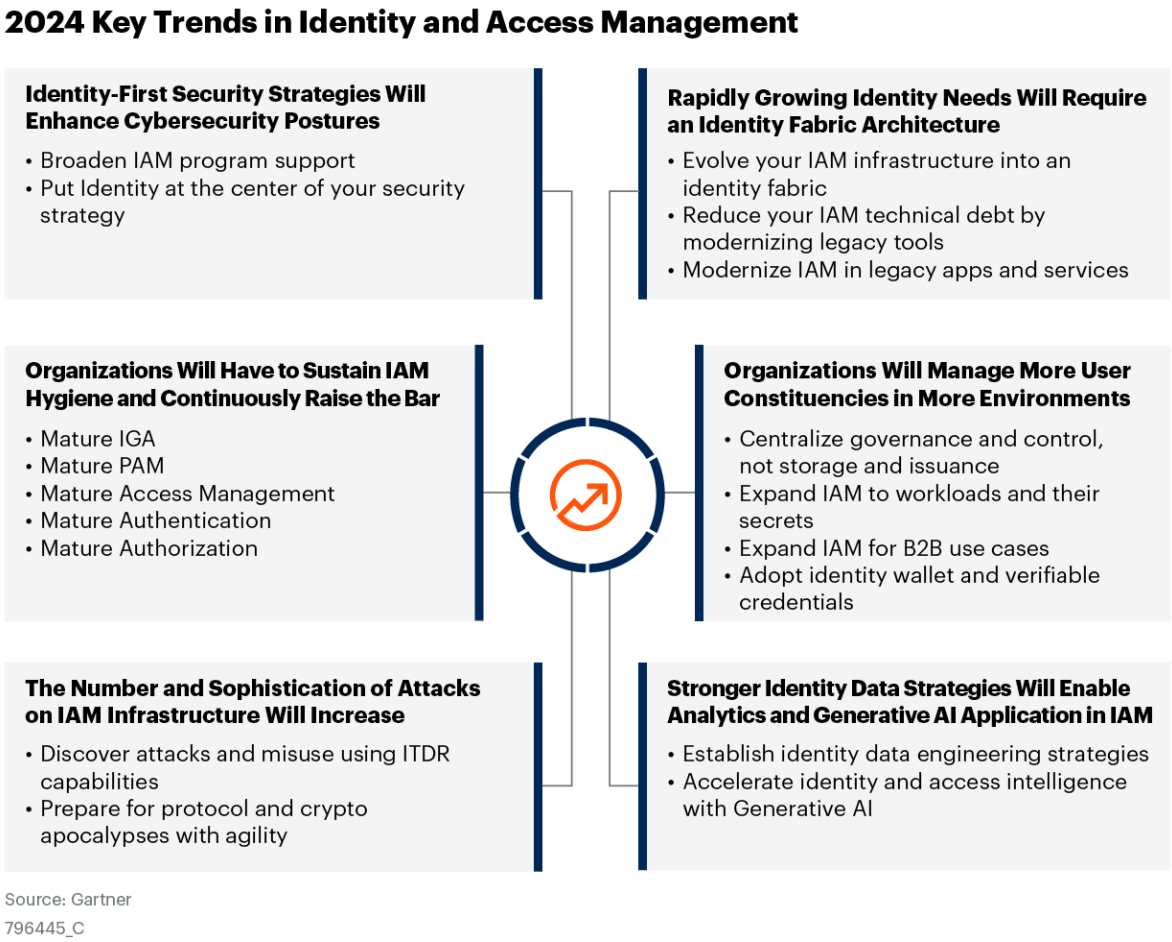
- Broaden the IAM program support and help remove both organizational and technical silos by establishing identity-first security strategies to meet growing security demands.
- Evolve your IAM infrastructure to become a flexible and composable identity fabric that supports broader IAM use cases in hybrid or multicloud environments for all types of entities by embracing the 10 identity fabric principles outlined in this research.
- Reduce IAM technical debt and manage it proactively. It's time to raise the bar from low levels of IAM hygiene to appropriate levels for the organization, and establish processes to stay at the right level. Do so by maturing your core IAM components, modernizing legacy IAM tools and integrations, and establishing guiding principles.
- Manage an ever-expanding user base, diverse environments, and intricate systems by embracing the undeniable future of multicloud computing using centralized/decentralized security (CeDeSec) strategies and by implementing strategies for APIs, workloads, B2B users and decentralized identities.
- Prepare for the day that crypto and protocols break, and implement identity threat detection and response practices. This establishes higher resilience and availability strategies. Prepare using continuous monitoring and discovery.
- Achieve higher levels of insights and risk-aware automation by establishing identity data engineering practices. Accelerate identity and access intelligence with generative AI.

Identity and Access Management Trends

The theme for the 2024 IAM Planning Guide is the need for new architectures to support hybrid and multicloud environments, visibility, and agility, and to manage IAM technical debt. The growing and changing demands that IAM teams have experienced in the last few years are not "one-off" occurrences. The requirements for organizations to develop new business and operating models in times of rapid change, together with increasing cyberthreats, mean that IAM infrastructure and teams need to evolve, from both a technical and an organizational standpoint, to creatively sustain high rates of change.

Figure 1 shows six key IAM planning trends for 2024, along with their associated planning considerations, which correspond to categories of IAM tools, deployment architecture and best practices.

Figure 1: 2024 Key Trends in Identity and Access Management



Source: Gartner
796445_C

Continually evolve your organization's IAM infrastructure into a well-woven identity fabric — a more secure, resilient, composable and distributed IAM infrastructure. It's mission-critical to keep pace with ever-changing IAM demands.

Key factors that will impact IAM planning in 2024 include the following:

- Identity-first security strategies, an increasing number of threats, and the growing digital surface that IAM teams need to protect while reducing silos and gaps are continuing to drive the need for a new approach to IAM operations and architecture.
- The need to evolve an existing IAM infrastructure into an identity fabric that is composable, orchestrated and resilient, provide IAM services that support all user constituencies (humans and machines such as workloads and devices), and enable a use-case, instead of a single tooling, approach to IAM.

- Challenges to finding quality IAM resources and skills as well as the geopolitical and economic uncertainty require organizations to do more with less.
- The need to reimplement, modernize and mature IAM capabilities and IAM support in applications and services to start resolving technical debt and support new business scenarios.
- Increasing demands for higher levels of visibility and automation and more sophisticated use of analytics, identity data and identity configuration data.
- Generative AI holds immense promise with its abilities to both attack and improve IAM systems, but its current hype often requires responsible implementation and thorough understanding of its limitations and the importance of quality IAM data.

Mature your IAM — GenAI is coming!

The factors above are framed by the following 2024 IAM technical planning trends:

- Identity-first security strategies will enhance cybersecurity postures.
- Rapidly growing identity needs will require an identity fabric architecture.
- Organizations will have to reestablish IAM hygiene and raise the bar.
- Organizations will manage more user constituencies in more environments.
- The number and sophistication of attacks on IAM infrastructure will increase.
- Stronger identity data strategies will enable analytics and generative AI application in IAM.

These planning trends are discussed in detail in subsequent sections. Their relative importance depends on your organization's current IAM maturity. Gartner continues to observe a significant gap between organizations with a mature IAM program and those that are lagging from a process, technology and/or organizational perspective.

Identity-First Security Strategies Will Enhance Cybersecurity Postures

Identity-first security is an approach to security design that makes identity-based controls the foundational element of an organization's protection architecture. It represents a fundamental shift from perimeter-based controls that became obsolete due to the decentralization of assets, users and devices.

This trend is an evolution of last year's identity-first security trend. Keeping up with IAM infrastructure best practices requires an ongoing program, not a series of one-time ad hoc projects. As organizations recognize the growing importance of IAM to security, they must not only evolve their IAM infrastructure but also mature their IAM operations to be complete. Ad hoc stopgap tactics are no longer good enough when it comes to IAM.

Identity-first security requires tighter collaboration of IAM and cybersecurity teams to ensure alignment and put IAM at the heart of security strategy. It also requires better alignment of IAM with other business and IT functions because secure digital access is key to enabling almost every business function.

To support IAM in these efforts, IAM technical professionals must:

- Broaden IAM program support.
- Put identity at the center of your security strategy.

Planning Considerations

Broaden IAM Program Support

Identity and access management technical professionals must increase IAM program coverage across the enterprise and reprioritize their IAM projects using a minimum, effective mindset. IAM teams always have a long to-do list. Effectively prioritizing this list requires a four-pronged approach:

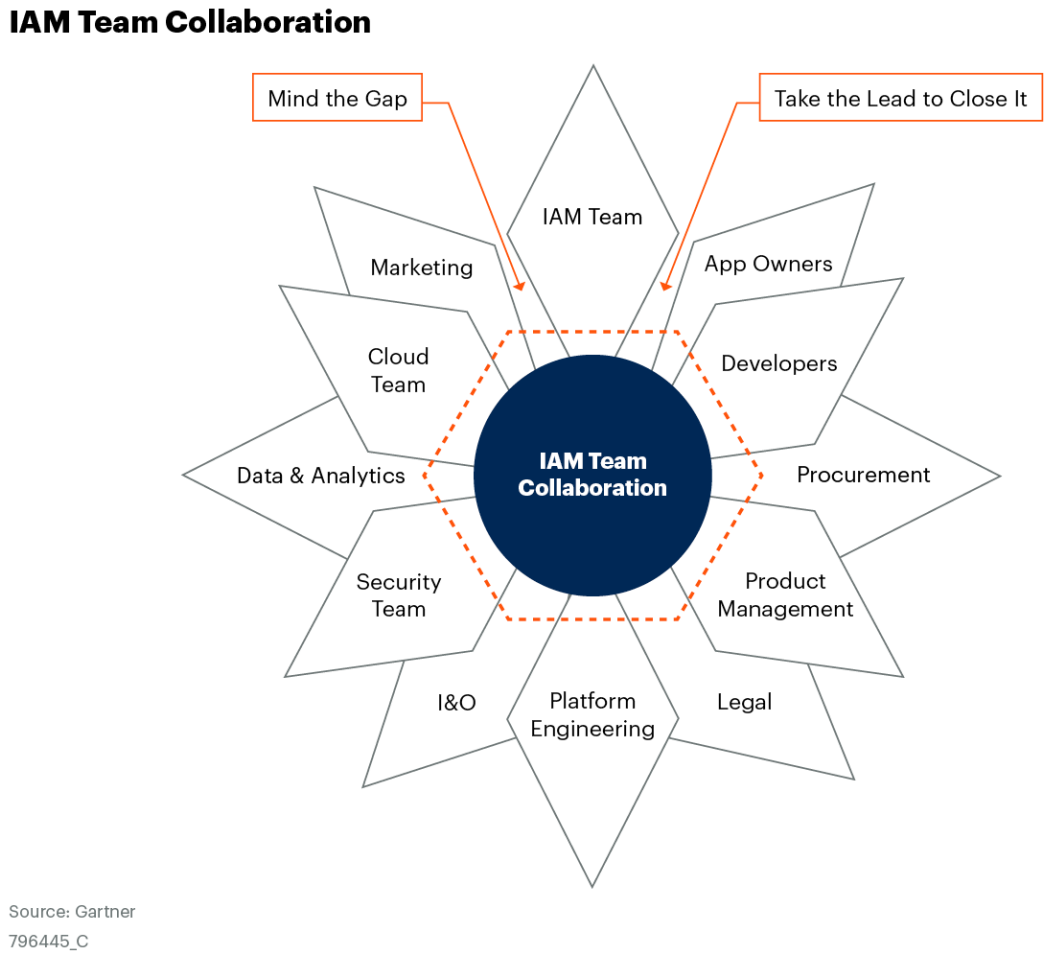
- Normalize handling IAM tasks as part of an ongoing program, rather than a series of separate projects. This is increasingly important in today's environment where failure to keep IAM configurations, integrations and policies current can result in breaches.

- Cultivate effective communication with both IT and business stakeholders. Best practice IAM controls affect both end users and IT personnel. Putting identity at the center of security operations as part of an identity-first security program requires being able to discuss identity with all the relevant constituencies. These stakeholders can include security, application development (DevOps), software procurement, applications owners, data and analytics, infrastructure and operations, cloud, marketing, product management, platform engineering teams, legal, and compliance teams as depicted in Figure 2.

- Anticipate new IAM requirements to avoid creating bottlenecks. This can require deeper alignment with senior leadership plans such as new product initiatives, expansion into new geographies (especially those with differing data residency laws), and mergers, acquisitions and divestitures. Effective communications must extend in both directions. Evangelize and teach IAM best practices to your IT and business communities. Mind the gap between teams. IAM teams must take the lead to close it. Doing this effectively will require the IAM team to learn more about the practices of other groups, such as security and app development practices. This step is key to developing effective IAM that evolves as the organization's needs evolve.

- Adopt a minimum effective mindset. That means focusing on value creation and using the minimum effort needed to achieve an effective outcome. A "boil-the-ocean" approach to IAM was never effective. Now that IAM is used by more humans and machines in more locations, it is crucial that IAM teams focus their efforts on what is most important. Instead, aim for a minimum effective toolset by focusing on what use cases to solve and then choosing tools that support multiple IAM functions where practical.

Figure 2: IAM Team Collaboration



Source: Gartner
796445_C

Small and midsize businesses (SMBs) especially, and also some larger organizations, should move away from a focus on firefighting by adopting more agile/simple processes. Some IAM processes are complex by nature. Selecting IAM tools that support agile journey-time orchestration to manage vendor integrations simplifies assessment of risk at each event in the journey, and facilitates delivering dynamic user experience (UX). Policy orchestration can also help make this shift. As can ruthlessly automating routine processes, so that IAM professionals have the breathing room to focus on more strategic, leveraged activities.

Recommendations:

- Deliver maximum impact by taking on a minimum effective mindset. That means focusing most of your IAM energy on the activities, process and tools that provide the most value. For example, reduce IAM deployment complexity by resolving technical debt and removing legacy tools.

- Broaden IAM program coverage outside core IAM teams across the enterprise to improve operations and reduce security gaps. Use the program to identify initiatives requiring IAM changes early in their project life cycles, to prevent business and IT teams making ad hoc identity decisions that don't follow identity best practices.
- Communicate the value and prioritize IAM efforts by adopting outcome-driven metrics (ODMs) that measure the business value of IAM investments, including but not limited to security risk management improvements. Create a business context for IAM investment by using ODMs to align IAM investments with business outcomes.

Relevant research:

- Improve IAM Architecture by Embracing 10 Identity Fabric Principles
- Busting 4 Cybersecurity Myths to Unlock More Value (additional license might be needed)
- Identity-First Security Maximizes Cybersecurity Effectiveness (additional license might be needed)
- Use Outcome-Driven Metrics to Drive Value for Identity and Access Management (additional license might be needed)

Put Identity at the Center of Your Security Strategy

The broad adoption of cloud services and remote access by partners and employees working from anywhere has eroded the value of legacy security controls at the perimeter of the corporate network. This positions identity as the foundational layer for cybersecurity.

An identity-first approach puts identity-based controls at the center of an organization's cybersecurity architecture. Identity-first security, with its emphasis on consistency across all resource locations, reliance on context, and promotion of continuous risk assessment, incorporates zero trust principles and can greatly contribute to organizations' zero trust implementations. This calls for tighter cooperation between technical security and IAM teams.

Recommendations:

- Put identity at the center of your security strategies by forging stronger bonds between technical security and IAM teams.
- Reduce the likelihood that the security team makes identity decisions without consulting the identity team and vice versa. Align the teams.
- Search for and identify opportunities for security and identity tool integration. Integrate security and IAM tools to ensure the consistent usage of policies and enable a better user experience regardless of the type of access required. For example, access management tools are best-positioned to support adaptive access to SaaS and web applications. They also provide authentication and identity context to zero trust network access (ZTNA) tools and cloud access security brokers (CASB), foundational components of the secure service edge (SSE) framework. In addition, analytics-driven approaches support adaptive access and continuous adaptive trust, and can integrate with cloud, endpoint and network security tools. Identity threat detection and response (ITDR) capabilities can cross-pollinate with other detection and response tools to deliver better protection against identity-based attacks.
- Establish a long-term strategy together with the security team that builds out a cybersecurity mesh architecture (CSMA) where security tools leverage the organization's existing IAM tools, share policy and exchange signals. CSMA is an emerging approach for architecting composable, distributed security controls to improve your overall security effectiveness. Start aligning roadmaps for security and IAM technologies that plug into a mesh. See The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA) for further details.

Relevant research:

- The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)
- How to Build a Zero Trust Architecture
- Identity-First Security Maximizes Cybersecurity Effectiveness (additional license might be needed)

Rapidly Growing Identity Needs Will Require an Identity Fabric Architecture

The adoption of identity fabric principles will continue to play a significant role in security and IAM initiatives in 2024. Traditional IAM tools consist of too many silos and are often not designed for a distributed and agile development approach. Many legacy IAM tools do not support capabilities such as adaptive access, multifactor authentication (MFA) and passwordless authentication. IAM teams must also support a more decentralized set of IAM capabilities in hybrid and multicloud environments. In order to support new security initiatives, organizations should evolve their current IAM services to be more integrated, resilient and distributed.

Modernization of IAM using identity fabric principles cannot be achieved using a "big bang" approach. Especially in a climate where organizations have to do more with less. This requires continuous improvements to the existing IAM architecture based on identity fabric principles. Over time, such an approach provides an opportunity to streamline existing IAM capabilities, ensure better cross-generational IAM tools and improve organizational ROI.

To support IAM in these efforts, IAM technical professionals must:

- Evolve your IAM infrastructure into an identity fabric.
- Reduce your IAM technical debt by modernizing legacy IAM tools.
- Modernize IAM in legacy apps and services.

Relevant research:

- Improve IAM Architecture by Embracing 10 Identity Fabric Principles
- Identity-First Security Maximizes Cybersecurity Effectiveness (additional license might be needed)

Planning Considerations

Evolve Your IAM Infrastructure Into an Identity Fabric

The term "identity fabric" is used loosely by the industry, and vendors' misuse of the term as a marketing buzzword causes further confusion. This trend and planning consideration is a continuation of last year's identity fabric trend. In 2024, the understanding of *what* an identity fabric is and isn't, and *why* and *how* to evolve an IAM infrastructure to a mature identity fabric, is critical.

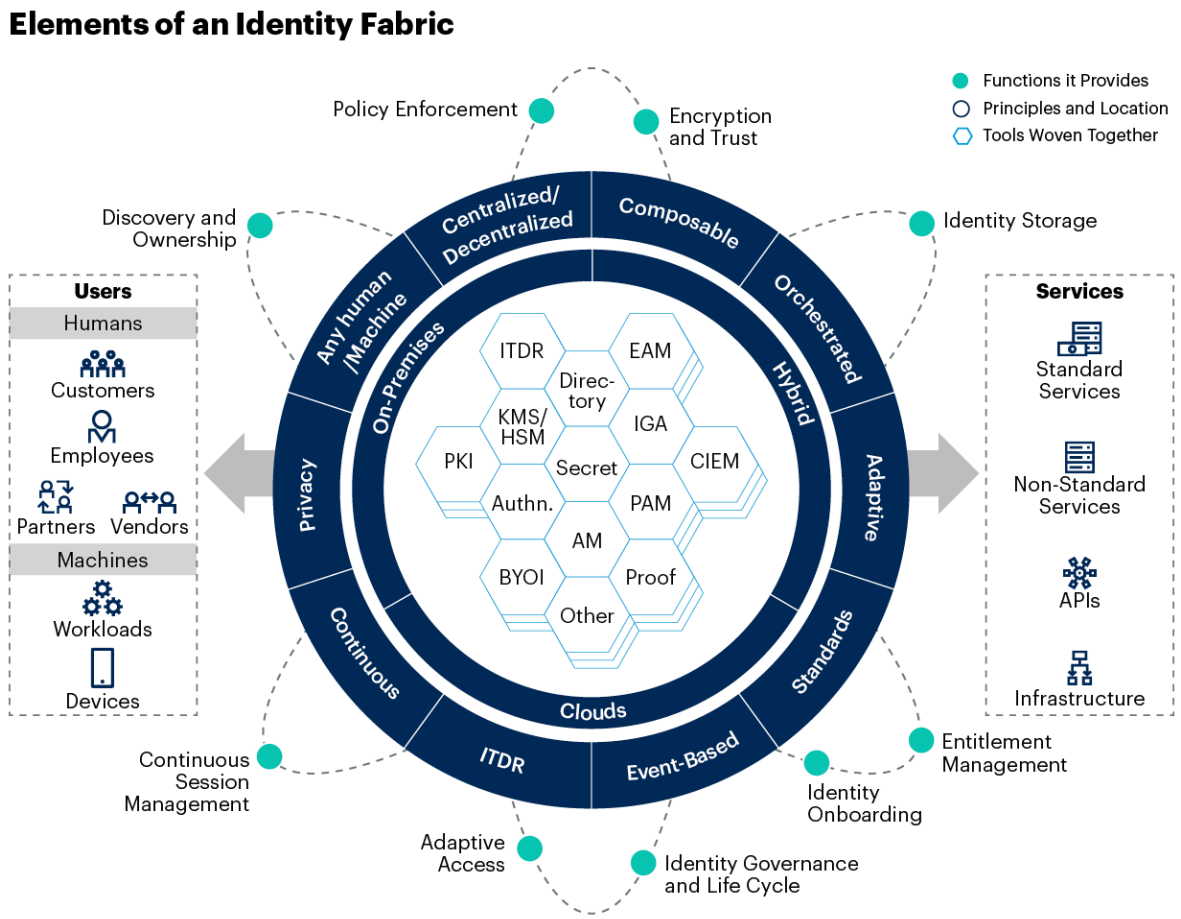
> An identity fabric must leverage and broker context to provide and support adaptive, continuous risk-aware and resilient access controls in a consistent manner for any human or machine in scope.

An identity fabric provides, operates and consists of:

- **Functions** — the functions that SaaS, internal applications, APIs and security tools use. These are the integration points to the identity fabric and are typically accessed using modern identity protocols. The functions are depicted in Figure 3 as "electrons" around the "nucleus."
- **Principles** — the 10 identity fabric principles under which it must operate as defined by Gartner in Improve IAM Architecture by Embracing 10 Identity Fabric Principles. In short, the 10 identity principles are:
  - Scope — any human or machine
  - Topology — centralized control and decentralized enablement
  - Architecture — composed, orchestrated and journey-oriented
  - Security — adaptive, continuous, risk-aware and resilient
  - Standards — pervasive
  - Connectivity — event-based integration
  - Change — continuous and automated
  - Threat detection and response — prescriptive and remediating
  - Privacy — for everyone
  - Observability — continuous visibility
- **Locations** — the location(s), such as a hybrid and multicloud environment, where the identity fabric must provide its functions.
- **Tools** — Under the covers, it's still the discrete IAM tools that offer the functions and features. Tools are woven together to provide the identity functions.

Figure 3 depicts these elements of an identity fabric.

Figure 3: Elements of an Identity Fabric



To evolve IAM, the center of attention must be on IAM functions instead of single tools. Each IAM use case requires a set of composable tools that are orchestrated for a specific use case. You can do more with less by reusing and integrating existing tooling. For example, for API access control, organizations may need one or more API gateways, an access management tool that federates with existing AM tooling, a secrets manager, public-key infrastructures (PKIs), and/or an externalized authorization manager to orchestrate access appropriately.

An identity fabric strategy is not at odds with ongoing convergence trends, where vendors provide IAM suites, nor with organizations' strategies for minimizing the number of tools in use.

No vendor does it all. Point tools, cloud-native tooling, new user constituencies and auxiliary security tools need to be part of, or integrated into, an organization's identity fabric. Strategies that evolve an IAM infrastructure into a mature, composable and agile identity fabric result in support of new use cases and minimize vendor lock-in.

Recommendations:

- Envision your IAM infrastructure as, and evolve it to, an identity fabric — that is, an integrated system of systems.
- Talk about IAM functions instead of tools with other teams. This encapsulates internal complexity within the identity fabric and enables agility and composability since the functions might be offered by multiple tools.
- Support all user constituencies: humans such as employees, partners and customers; and machines such as workloads and devices.
- Embrace current and emerging identity standards to reduce integration effort and make IAM services more composable.
- The open and extensible architecture, which is another key take-away from the principles, will improve composability. For example, when the currently used IAM tool does not keep up with newer requirements or renewal costs are higher than planned, IAM teams must have the architectural flexibility to replace the existing tool with another competitive solution from the market.
- Look for event-based connectivity between tools to improve sharing of risk signals, offer targeted alerts and improve security.
- Identify gaps, look for opportunities to integrate IAM tools, find necessary and unnecessary overlaps in toolsets, and incorporate solutions, with a focus on orchestration.

- To overcome barriers and to faster mature your IAM infrastructure into an identity fabric, reduce technical debt, and assess IAM tools that help weave other IAM tools together with focus on identity orchestration, provisioning and policy orchestration. Also modernize IAM in legacy applications. Do so according to the next two planning considerations below.

Relevant research:

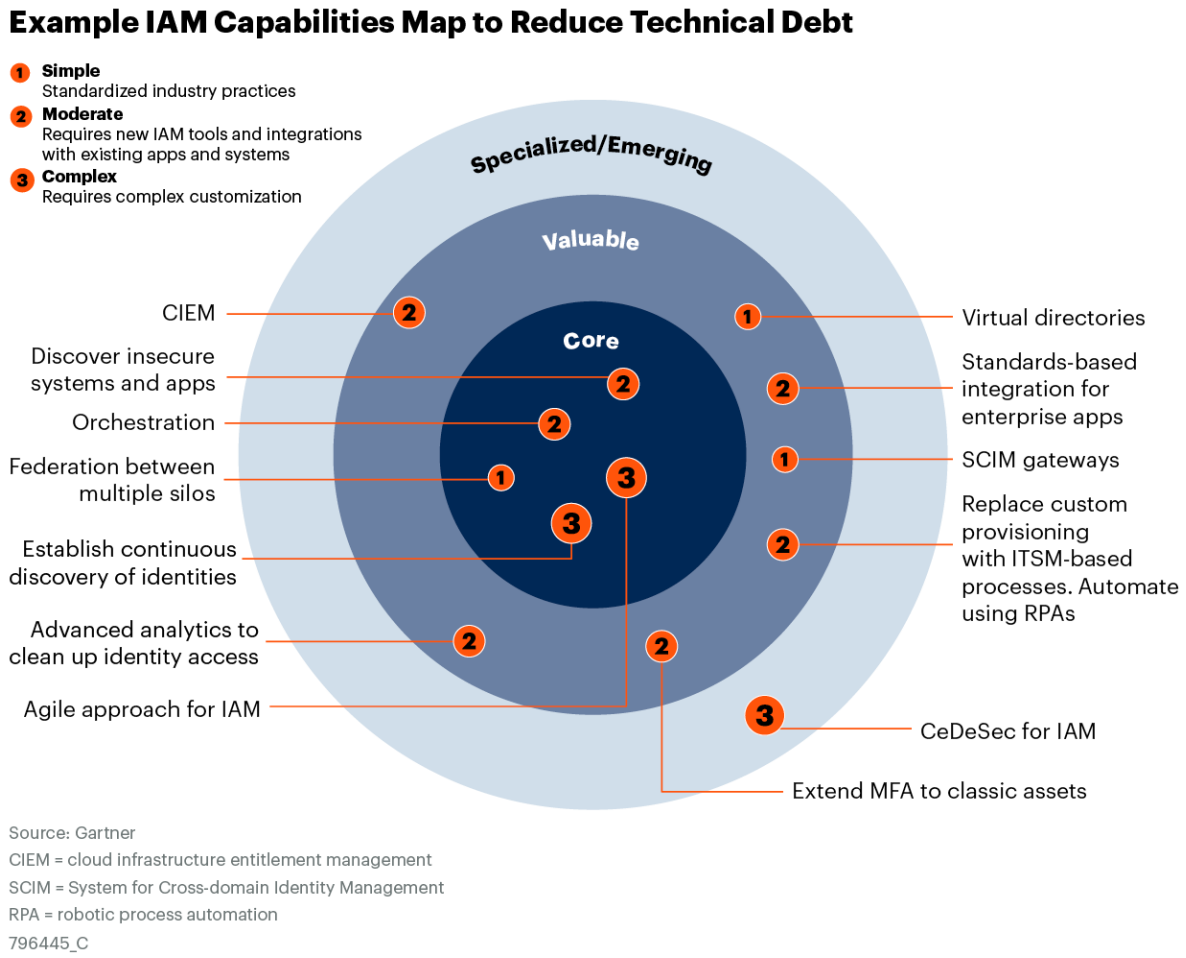
- Improve IAM Architecture by Embracing 10 Identity Fabric Principles
- The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

Reduce Your IAM Technical Debt by Modernizing Legacy IAM Tools

Managing large IAM technical debt is a drain on an IAM team at a time of skills shortages. In the past, IAM solutions were designed based on vendor-specific architecture and integrations for implementing IGA, PAM or access management. Over time, this results in multiple siloed tools and increasing IAM technical debt. IAM teams with large technical debt are challenged with lack of agility, longer delivery timelines and poorer quality.

The modernization of legacy IAM tools reduces technical debt but this does not always mean replacing all existing IAM tools with new tools. Instead, this means unifying the capabilities of multigenerational identity tools using tools and standards. Figure 4 shows common approaches that improve interoperability between the legacy and new solutions to reduce technical debt. The approaches are depicted using two perspectives: *relevance* (center of the bulls eye) and *impact* (dots ranging from 1 to 3).

Figure 4: Example IAM Capabilities Map to Reduce Technical Debt



Source: Gartner
CIEM = cloud infrastructure entitlement management
SCIM = System for Cross-domain Identity Management
RPA = robotic process automation
796445_C

Recommendations:

- Take a use-case instead of a linear step-by-step approach when resolving technical debt, since each organization has its own challenges and business priorities. Start with the most *relevant* and *impactful* approach based on the needs of your IAM program.
- Build bridges to the cloud to mitigate identity sprawl and provide a central holistic view. Leverage cloud-provided directory sync solutions to sync user and access data from legacy LDAP directories to the cloud directory. This will provide a unified view of identities across multiple systems. Use this “low-hanging fruit” approach as a first step to migrate users, aliases, groups, and other data for on-premises identities to the cloud. To transform attributes and selectively synchronize identities, leverage synchronization rules and add custom attributes mapping and identity exclusions.

- Do more with modern capabilities of virtualization. Identity virtualization tools provide real-time identity data and identity configuration data across multiple platforms, not just directories. Virtualization platforms can also be leveraged to synchronize data among them. Authentication is a primary use case to unify identity repositories but other use cases, such as personalization, identity data analysis and observability, also benefit with virtualization. Virtual directory vendors are also adding the discovery functionality, alerting on identity anomalies and providing visibility.

- Leverage third-party solutions to migrate authentication to cloud-based IAM solutions. Modernizing legacy IAM tools can be complicated since they are being used by a variety of on-premises applications using different techniques, such as Kerberos, headers and cookies, to handle the user session. Assess new identity orchestration tools to operate and/or migrate from legacy to modern IAM tools. Leverage web access management (WAM) based tools (also called reverse proxies, identity-aware proxies or application proxies) to connect on-premises applications to modern IAM tools.

- Augment legacy PAM solutions with just-in-time privilege functions. Many organizations vault their on-premises infrastructure credentials but do not mature further to manage privileged sessions. PAM tools offer capabilities to replace standing privileges with just-in-time assignment of access across hybrid platforms. When an organization lacks JIT support in its existing PAM tools, just-in-time privilege (JITP) tools can be leveraged to perform privileged operations through multiple mechanisms, such as JIT dynamic group/role, membership/assignment, JIT token, or JIT session.

- Leverage identity analytics to modernize legacy processes. Analytics-based tools will speed up legacy onboarding processes, as well as help reduce costs and labor with IGA processes, such as access reviews, user clean up and role management. Machine-learning-based behavioral analytics and complex risk models can also aid in risk-based access governance. IAM teams can develop analytics-based tools to discover unused access and remediate it using manual or automated processes. Third-party identity analytics tools can also augment existing IGA with establishing least privilege access, role modeling and risk-based access reviews.

Relevant research:

- Implement IAM Best Practices for Your Active Directory
- Modern Approaches to Identity Governance and Administration Role Modeling

Modernize IAM in Legacy Apps and Services

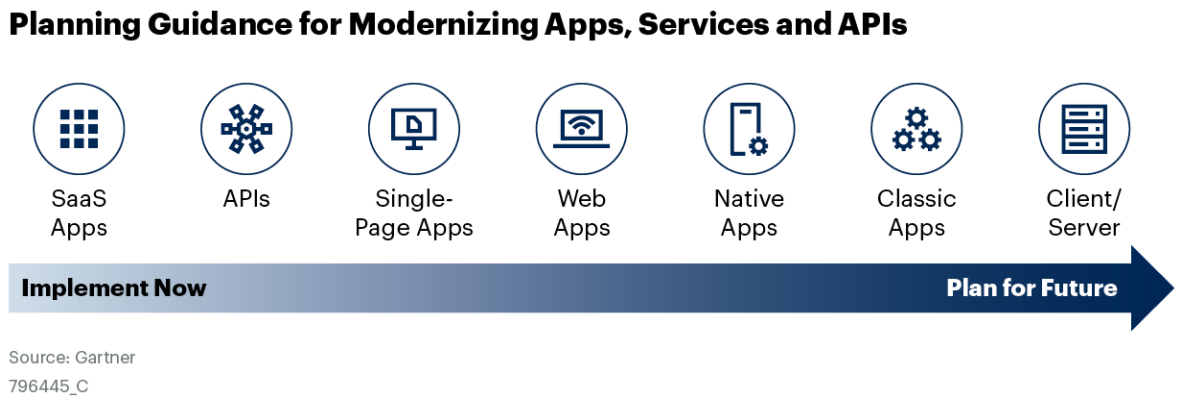
IAM protects cloud, standards-based and legacy applications. Often, applications need to be modernized to use modern IAM capabilities, but historically it's been too large of an undertaking.

The first step to modernization is to understand the type of applications and accounts that should be secured and governed. IAM teams should leverage application portfolio management (APM) best practices to catalog the necessary IAM controls for all applications and systems. This is a continuous process and will define the necessary administrative and runtime tasks that should be included in the IAM roadmap.

Modernizing IAM in legacy applications and services starts with a comprehensive discovery process, which can leverage the best practices of the APM processes.

Organizations cannot prioritize all discovered applications. Categorize and prioritize with an initial focus on minimizing future technical debt, as depicted in Figure 5. For example, SaaS apps and APIs can be integrated using standards based on current available capabilities, but native apps, classic apps and client/server apps require long-term planning.

Figure 5: Planning Guidance for Modernizing Apps, Services and APIs



Source: Gartner
796445_C

Recommendations:

- **Discover and track applications IAM controls using APM processes.** IAM teams must define what authentication, authorization and encryption mechanisms are to be used, for all new and legacy systems. To do so, additional tools may be required to help discover and define the integration. Domain controller network monitoring and API-based infrastructure as a service (IaaS) discovery tools can be leveraged to identify applications that perform authentication requests against user stores, gather insights based on monitoring, and in some cases also enforce policies. If an organization uses a configuration management database (CMDB) to store configuration of all the assets, IAM teams can leverage vendor-provided discovery services to discover applications in real time and update the CMDB. Once applications are discovered, start tracking app owners and define strategies for legacy systems that do not fit modern strategy according to Figure 5. Add compensating controls in the short term and a replacement approach in the long run.

- **Define IAM standards based on the application type.** Divide and conquer based on the type of applications used, such as SaaS, APIs, single-page web applications or native applications. For SaaS apps, make IAM an evaluation criterion for SaaS applications as defined in How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria. For other types of applications, focus on modern federation and life cycle management protocols such as OpenID Connect and support for System for Cross-domain Identity Management (SCIM) and MFA for administrative access.

First, define patterns for APIs, SPAs and web apps so that developers have the right guidance to secure their applications. Then shift focus to legacy web applications and client/server-based applications that often need gateways but also provide long-term guidance when reimplemented.

- **Deploy authentication forwarding for legacy applications.** Authentication forwarding solutions monitor authentication traffic and invoke additional authentication based on policies out of band, without requiring direct application integration. For example, AD-bound legacy applications can leverage the tools to implement MFA without changing application code.

- **Replace custom provisioning using standardized tools.** Complex custom provisioning may be required to provision and deprovision user access in applications that are not supported by the organization's IGA solution. IAM teams can reduce the reliance on custom development by replacing this with indirect provisioning to IT service management (ITSM), database and LDAP. A robotic process automation (RPA) tool can be leveraged to complete the fulfillment. For applications that do not support SCIM and are not supported by a deployed IGA vendor, IAM teams should leverage a SCIM gateway in addition to the IGA vendors provisioning capabilities. This will provide predefined integrations to reduce the need of building, deploying, managing and supporting custom adapters.
- **Secure privileged credentials for legacy tools.** Application-to-application password management (AAPM) tools eliminate the challenges with storing hard-coded, unencrypted and static credentials. Legacy applications and services gain access to application credentials in a secure manner through proprietary SDKs and command line interfaces (CLIs). PAM vendors support agent-based and agentless architecture approaches. Although the modification is usually simpler, IAM teams should include development teams to test the changes thoroughly. Modern applications such as containers and cloud-native workloads should leverage platform-provided identities.

Relevant research:

- Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0
- Guidance for Identity Governance and Administration
- How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria

Organizations Will Have to Reestablish IAM Hygiene and Raise the Bar

IAM is a well-established practice within the IT industry, but many organizations are still plagued by gaps in their core IAM capabilities (see Table 1).

Table 1: Recent Examples Illustrating Gaps in Organizations' Foundational IAM Capabilities

Area ↓	*Example* ↓
MFA as a strong security control mitigating account takeover attacks	Only 46% of small and midsize businesses (SMBs) implement MFA. [1] Just 22% of monthly active users in Microsoft Entra ID (formerly Azure Active Directory, or Azure AD) use MFA. [2]
Cloud access	Less than 2% of cloud entitlements are actually used. [3]

Source: Gartner (October 2023)

Based on Gartner's IT Score (a Gartner service for CIOs that help measure IT maturity) the maturity of IAM programs averages only 2.3 out of 5. [4] Although IT Score identified several IAM-program-level gaps (development of a vision and strategy, compliance enablement, delivering and demonstrating business value, and others), it also clearly showed deficiencies in technical IAM implementations.

Organizations must progressively raise the bar, often from low levels, among all core pillars of IAM and establish processes to stay at organization-appropriate levels.

To support IAM in these efforts, IAM technical professionals must:

- Mature identity governance and administration (IGA)
- Mature access management (AM)
- Mature privileged access management (PAM)
- Mature authentication
- Mature authorization

Planning Considerations

Mature IGA With Focus on Operations and Analytics

Because of the dynamic nature of organizational requirements, new apps and tooling, evolving complexity of IT, and the fact that organizations are asked to do more with less, IGA hygiene and maturity may not be where it needs to be to serve the governance needs of an organization. Bad IGA hygiene is often a result of low maturity of IGA controls, inefficient life cycle management, operating IGA in a silo or just poor maintenance of the IGA solution.

Confusion also persists within the IGA market. It is especially difficult to determine what functionality a light IGA versus a suite solution can provide, and whether it will be adequate for an organization's requirements. While some IGA vendors in the market are providing more capable analytics, analytics adoption by organizations is slow and mostly based on descriptive (reporting) or some risk scoring capabilities. In addition, IGA tools have not kept up with demand for machine identity management capabilities, forcing client companies to pursue separate solutions in many cases.

Enhancing IGA maturity requires a shift in the mindset of the organization from being reactive to proactive and moving from periodic access reviews to a continuous and context-enabled governance model. A mature IGA also requires implementing advanced IGA controls that provide long-term value, such as advanced identity analytics, risk-based access certification and automated role modeling, in addition to foundational controls. Comprehensive discovery, management and remediation of both on-premises and cloud infrastructure entitlements either through native capabilities or through adjacent toolsets are the key steps in evolving the maturity of the identity governance.

Recommendations:

- **Evaluate light IGA as a primary IGA solution.** But only when compliance and auditing requirements are minimal. See Is Light IGA Right for Your IAM Needs? for further details.
- **Weave IGA into the identity fabric to increase visibility.** Break the IGA silo to provide better governance across the organization. Address the IGA solution blindspots around privileged accounts, cloud infrastructure entitlements and machine identities through integration with adjacent IAM tools within the organization. Integrate IGA with PAM, cloud infrastructure entitlement management (CIEM), data access governance (DAG) and other IAM components to improve the IGA system visibility. Cover standard and privileged access for both human and machine identities across on-premises systems, IaaS and SaaS applications, so that an organization can get a 360-degree view of all access associated with all identities across the organization.

- **Increase the IGA controls maturity.** Implement IGA controls that provide long-term value, such as automated role modeling and event- and risk-based access certification.
- **Optimize identity life cycle management processes.** Streamline complex and inconsistent life cycle management processes. Assess the joiner, mover and leaver workflows to make sure they cover all accounts across the entire IT landscape. Identify broken processes by running IGA scans to detect orphan and rogue accounts. Schedule continuous scans to clean up orphan and rogue accounts. Cleaning up accounts is a band-aid. Identify the root cause and fix broken processes.
- **Leverage AI/ML-based identity analytics.** Use predictive and prescriptive analytics for assisting in decision making and automating action to some extent. Autonomous governance requires advanced analytics, which is a differentiating factor for IGA vendors. Explore the native identity analytics capabilities of your IGA solution and complement it with adjacent tools if required. Optimize access certification to go beyond the basics by using AI/ML-based analytics to calculate risk and provide context signals during the access certification process. Risk scores can also be used to automate a small portion of low-risk certification items. Use identity analytics to make recommendations for additional access for quicker business enablement. Take a conservative approach when using recommendations for access requests to avoid overprovisioning of entitlements.

Relevant research:

- Guidance for Identity Governance and Administration
- Modern Approaches to Identity Governance and Administration Role Modeling
- Best Practices for Optimizing IGA Access Certification
- Solution Comparison for Identity Governance and Administration
- Is Light IGA Right for Your IAM Needs?

Mature PAM With Focus on JIT/ZSP

PAM is foundational in mitigating and managing risk for elevated credentials and accounts in an organization. In order to secure different applications and systems, privileged accounts and credentials are created and stored in multiple locations, including on-premises data centers, cloud infrastructure from different vendors, and SaaS applications. Securing privileged credentials used by human and machine identities in a hybrid environment can be achieved by using PAM solutions and secrets managers respectively.

PAM vendors have improved their SaaS offering to be on par with their software-delivered solutions. Many of them started offering advanced JIT capabilities and management of cloud entitlements in multicloud environments. Although PAM tools continue to mature and expand their scope, many organizations still lag in maturity, leaving some of the highly privileged credentials very vulnerable.

PAM teams often stop at vaulting the credentials but not maturing the management of privileged access effectively.

- The majority of access granted to human identities are standing privileges, which increase the chances of being compromised over time.
- Today, machine identities outnumber human identities, but many organizations do not have a well-defined approach to govern them. PAM capabilities do not secure all credentials used by machines, such as keys, secrets, and certificates.

This requires a comprehensive PAM strategy based on the zero standing privileges (ZSP)/JIT model. At the highest maturity level, all privileged access is only temporarily granted, by elevating normal accounts, using ephemeral access or leveraging other JIT approaches.

Recommendations:

- **Deploy discovery such that no privileged account is left behind:**
  - **Make discovery comprehensive.** The discovery process must identify all privileged identities in the on-premises, cloud infrastructure and SaaS applications. Discovered accounts should not be limited to human administrators but also include DevOps credentials and machine identities.
  - **Make discovery continuous.** Discovery of identities is not a one-time activity. It should be run on regular intervals so that new identities are discovered.
  - **Make discovery extensive.** A single tool will not perform comprehensive discovery in most cases. For example, cloud service providers (CSP)s and PAM suites often do not discover certificates and secrets. Organizations should use third-party tools that discover certificates, SSH keys and secrets.

- **Implement just enough privilege (JEP) to enforce least-privilege access.** IAM teams must implement processes to remove excess access for privileged identities, and PAM tools can facilitate the just-enough privileges assigned during privileged access. For example, service desk users do not need access to domain admin credentials to reset passwords for end users. Another scenario is when a developer requests read-only access to query a production database. Privileged access session management (PASM) capabilities can inject a read-only access credential and not the read/write credential.
- **Secure administrative access.** Vaulting privileged credentials is a good first step but it does too little to prevent exposing credentials to the users. Leverage PAM controls, such as privileged account and session management (PASM) and privilege elevation and delegation management (PEDM), to establish sessions with transparent credential injection, so that the users are connected to privileged resources based on policies but the credentials are not revealed.
- **Automate processes for DevOps.** Managing privileged credentials used by DevOps teams should not be done manually. Rather, use automated processes that enable centralized governance and control. Secrets management tools offered by CSPs or third-party tools can be integrated with the tools that development and operations teams use. They are also integrated with DevOps pipelines tools to get identities at runtime to deploy services.

- **Remove excess access for privileged identities.** Overentitlement is common among privileged identities since new privileged accounts are created from existing accounts. PAM teams should stop copying access, and instead create identities with only minimum required access. Excess access for privileged identities should also be removed based on the current usage. For example, policy insights in Google Cloud Platform (GCP) can provide recommendations on removing overentitlement for cloud infrastructure access.
- **Replace standing privileges with just-in-time access.** PAM tools allow privileged identities to gain access just-in-time before the actual usage and remove the access after the predefined time. In some cases, the accounts or permissions may also be enabled or generated just-in-time so that there are no administrative credentials made available permanently with highly-sensitive access. For example, Amazon Web Services (AWS) cloud console can be accessed based on just-in-time-generated temporary credentials.
- **Automate manual tasks to reduce human access and errors.** In an ideal PAM world, human access is needed only for unplanned and exceptional scenarios. Organizations should use repetitive tasks that can replace repeated manual steps executed in cloud systems. The goal is to reduce the complexity and likelihood of human error in privileged operations.
- **Review standing privileges periodically.** Until all privileged access follows the JIT model, a regular review of standing privileges should be conducted by either leveraging native PAM capabilities or by using adjacent systems, such as IGA access reviews.

Identity-focused technical professionals must make discovery comprehensive and continuous to identify all accounts, extend PAM tools to manage sessions, and reduce standing privileges by using just-in-time (JIT) approaches. This, combined with privileged access governance, will improve the privileged access hygiene of an organization.

Relevant research:

- Securing Privileged Access to the Cloud Using PAM
- Guidance for Privileged Access Management
- Managing Machine Identities, Secrets, Keys and Certificates

Mature Access Management With Focus on Continuous Adaptive Trust

Access management, which emerged as a set of capabilities to facilitate workforce access to SaaS and web applications, has matured to support:

- Partner and customer access
- MFA for many back-end enterprise use cases and PC logon
- API access control
- SSO to non-web applications through integrations with VPN, VDI, ZTNA and other tools
- Access to nonstandard applications using vendor-provided proxies and password vaulting

This is a mature market, but it doesn't stand still. Gartner is observing the following trends in the technology itself and in its use:

- Many organizations are migrating to a second- or third-generation of AM, often abandoning on-premises deployments in favor of SaaS-delivered ones. Application migration is typically the most challenging component of the migration process, but policy and configuration migration are also a common concern.
- An increasing number of third-party integrations enable AM tools to support authentication for legacy use cases (for example, PC and mobile device logon, access to Active Directory-integrated applications).
- Some cloud-delivered AM tools (e.g., Microsoft Entra ID and Okta) are evolving into converged IAM platforms that offer lightweight IGA and PAM capabilities, including identity life cycle management, entitlement management, access certifications and privileged access for platform and application administrators. In addition, many AM tools support at least some application and/or directory provisioning functionality. SCIM, a lightweight provisioning standard, is now common among leading AM providers.
- Most vendors that offer AM functionality continue to improve their adaptive access capabilities by adding new risk and recognition signals, especially those related to device trust. Support for journey-time orchestration (JTO) and fine-grained authorization is also increasing.

- A new crop of third-party tools emerged to support resilience in cloud-delivered AM services. They include backup and recovery tools, and tools that improve security posture management and threat detection and response.
- Non-AM authentication vendors now universally provide at least some AM capabilities, such as an identity provider supporting standards-based SSO for SaaS and web applications, adaptive access, and coarse-grained authorization management for applications.

In the next twelve months, Gartner expects AM vendors to increase their support for non-web access use cases through partnerships with, or acquisitions of, passwordless authentication and MFA vendors. Vendors should also deepen their adaptive access capabilities to include advanced JTO features, online fraud detection (in customer-facing scenarios), and support for continuous adaptive trust (CAT), a model for continuous in-session risk assessment and mitigation. [5]

Recommendations:

- Implement an AM tool if you haven't already done so. An average midsize to large organization uses hundreds of SaaS applications. Managing access separately for each application simply doesn't scale.
- If using a SaaS-delivered AM tool, assess the feasibility of integrating your non-web access use cases with that tool (taking security and availability requirements into account), possibly moving away from a more traditional Active Directory-centric architecture.
- Take full advantage of adaptive access capabilities provided by your incumbent AM tool. Evaluate CAT capabilities if your vendor already supports CAT.
- Each user-constituency such as customers, partners, APIs and workforce might require their own AM tooling. Federate using modern identity protocols such as OpenID Connect between them when needed.
- Only let your APIs trust one access management tool. Use the inbound federation support in your API-focused access management tool to enable integrations between other access management tools.

Relevant research:

- Solution Path for Modernizing Access Management

- Architect a Modern API Access Control Strategy
- Modern Identity: OpenID Connect, OAuth 2.0, JWTs and SCIM 2.0

Mature Authentication With Focus on Passwordless

User authentication must be risk-appropriate and requires a multipronged, layered approach. MFA emerged as the foremost security control to protect organizations against account takeover (ATO) attacks. Regulators and cybersecurity insurers increasingly demand that organizations implement MFA. However, MFA adoption is uneven.

In addition, many organizations take an all-or-nothing approach to MFA: authentication is either based solely on passwords or requires some kind of MFA, any MFA, without recognizing that not all MFA methods deliver the same level of trust. All authentication methods have their strengths and weaknesses; a careful trade-off analysis is required to decide on the most appropriate method, and additional protections may be needed. For example, Gartner qualifies SMS-delivered one-time passwords (OTPs) as providing only low assurance (when combined with a password) (2 out of 5 on Gartner's Authentication Trust Scale). Organizations can continue to use SMS (for low-risk applications), especially if they further protect it with auxiliary controls such as SIM swap checks available from several MFA and communication platform as a service (CPaaS) vendors.

Attackers are constantly looking for ways to subvert widely used MFA methods, even those historically considered strong. For instance, push bombing attacks [6] (also called MFA fatigue attacks) are on the rise: In a recent survey, 12% of respondents said they had experienced at least one such attack in the previous 12 months. [7] One large Gartner client deprecated the use of mobile push for authentication due to concerns over MFA fatigue. Less drastically, organizations can — and should — implement session binding and location matching, increasingly supported by authentication and AM vendors.

Another common attack that can lead to ATO is phishing. Gartner strongly recommends that organizations evaluate the use of FIDO2, a set of standards that support phishing-resistant MFA and passwordless authentication. Although until now most FIDO2 implementations had to rely on security keys (dedicated hardware tokens), the FIDO Alliance and the World Wide Web Consortium (W3C) are close to ratifying a new specification supporting cross-device authentication enabling smartphones to act as software-based roaming authenticators. [8] Both Apple and Google already support this capability in their respective mobile OSs.

The FIDO2 standards also provide a practical way forward for implementing passwordless authentication. Gartner is observing a significant increase in client questions about passwordless technologies. Many organizations implement passwordless authentication using capabilities of incumbent vendors and passwordless specialists. Frequently used methods include phone-as-a-token (typically using a vendor-provided mobile authenticator app), endpoint-as-a-user-proxy (enabling remote authentication without a challenge once the user is logged in to their device — possibly with additional risk assessments that may require user action), and biometric authentication.

Gartner also projects a quick adoption of FIDO2 passkeys, portable FIDO2 keys natively supported by popular web browsers and OSs (from Apple and Google). But initially, this will mostly be in low-risk customer-facing scenarios where assurance concerns related to key portability are less pronounced and the passkeys' ease of use in same-device and cross-device authentication is especially appealing.

Recommendations:

- Implement MFA if you haven't already done so. Evaluate the general MFA capabilities of your incumbent AM vendor or include your MFA requirements in your AM RFPs if you are shopping for both MFA and AM. Gartner predicts that by 2027, 90% of enterprises will fully meet their MFA needs for remote and cloud access using the native capabilities of access management tools, thus lowering the total cost of ownership by 40%. [9]
- Enhance your existing implementation by identifying specific assurance requirements for all applications that may require MFA and applying risk-appropriate MFA to each use case. Allow weak methods such as SMS- or voice-delivered OTPs only for low-risk applications.
- Evaluate auxiliary controls to protect your MFA against misconfiguration, bypass and abuse.
- Implement passwordless MFA for high-traffic use cases that will benefit the largest number of users. While for most organizations complete password elimination is not in the cards, removing passwords from common authentication flows improves security and UX, and provides a pathway to eventual drastic reduction in your organization's overall dependency on passwords.

Relevant research:

- Avoid the Top 9 Pitfalls of Implementing MFA
- Shift Focus From MFA to Continuous Adaptive Trust
- You, Too, Can Start Enjoying the Benefits of Passwordless Authentication Today

Mature Authorization With Focus on Policy Management

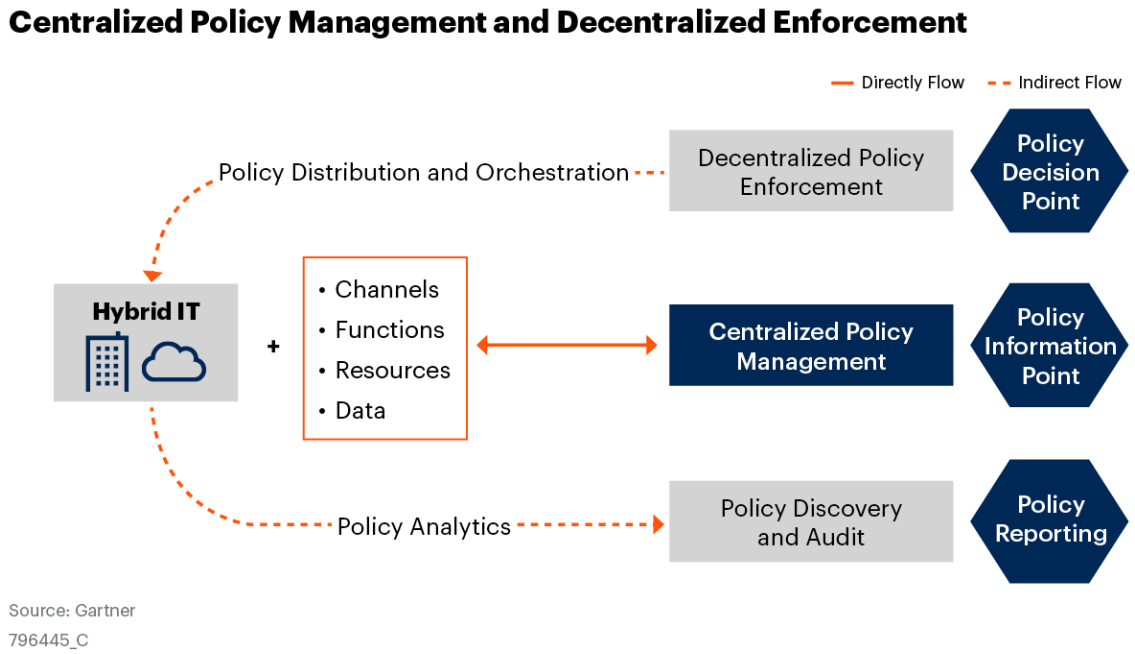
Authorization evolution accelerated in recent years due to increased demand for runtime fine-grained access control. This has led to more vendors entering the market as well as the introduction of new technologies (beyond existing XACML and NGAC specifications), such as Open Policy Agent (OPA), IDQL, Cedar, and Google Zanzibar, that can enable more use-case coverage and scaling of authorization solutions.

As the number of policies and systems increases, many organizations need to manage policies more centrally at the enterprise level. Technical professionals should define a centralized approach to managing policies where possible. A practical approach is to consolidate policy management for similar use cases such as portal access (for employees or customers), API access (via API gateways), cloud access (for IaaS, PaaS, or SaaS), and data and analytics access. This should consider constraints such as regulatory or organizational requirements.

Technical professionals should also enable decentralized policy enforcement either by policy distribution to different systems' designated policy decision points (PDPs) or policy orchestration into key platforms to augment the platforms' native policy decision/enforcement capabilities. Policy orchestration examples are pushing policies to IaaS cloud platforms (Azure, AWS, GCP), OPA agents, or data and analytics platforms (Databricks, Snowflake).

Policy management centralization should start with policy consolidation for specific use cases such as channels (APIs and portals), business application functions, infrastructure resources, and/or data. The policy management should enable decentralized policy enforcement in systems either on-premises or in the cloud for each of the relevant use cases, enabled either through policy distribution or orchestration. The resulting enforcement log data can be used to generate policy analytics for policy audit and reporting purposes (see Figure 6).

Figure 6: Centralized Policy Management and Decentralized Enforcement



Recommendations:

- If the authorization system requires strict isolation, use stand-alone policy administration and policy storage functions to meet compliance requirements. When the authorization system requires strict separation as part of business model, legal or regulatory requirements (e.g., separate lines of business or geographical operations due to regulations), there is not much that IAM architects can do. This type of restriction leads to separation of the authorization systems as part of the broader architecture. Although business separation doesn't necessarily have to lead to technical separation (some vendors have a "name spacing" option for separating the policies between different domains), the decision quite often becomes a business choice.
- If the authorization system requires complex policies, centralize policy administration and policy storage functions within the authorization domain by relevant use case or pattern such as authorization for channels (portal or API access), functions in business applications, infrastructure resources and DevOps, or different types of data access.

- If the authorization system requires frequent change and auditing (e.g., sensitive systems in banks, healthcare, defense industries), allow distributed policy administration, but centralize policy storage within the authorization domain by relevant use case or pattern.

Relevant research:

- Guidance for Modernizing Authorization Architecture
- Architecting Modern Policy-Based Runtime Authorization
- Designing Policy-Based Authorization Control for Data and Analytics Pipelines

Organizations Will Manage More User Constituencies in More Environments

There is always more. More use cases, more user constituencies and more environments. Everything needs to be managed, but in 2024, organizations must pay extra attention to cloud-native IAM tooling, workload identities, APIs, B2B users and decentralized identities:

- **Cloud-native IAM tooling:** For most organizations, regardless of size, multicloud computing is inevitable. Each cloud, or individual tenants within a single provider, use local, specialized and optimized cloud-native tools that need to be integrated. Native tooling offers a best-of-breed support in its own platform, providing automated issuance of identities for workloads, life cycle management and native policy languages. Organizations must establish a multicloud IAM architecture and shift focus from legacy strategies that force centralized issuance and usage of identities to instead centralized governance and control over more tools.
- **Workloads:** The rapidly growing number of machines that are deployed escalates the importance of managing machine identities and their secrets, keys and certificates. At the same time, most internet communication is now API-based, making API access control — authentication and authorization of APIs — a vital part of API strategies. Organizations must expand their identity fabric's scope to more workloads, APIs and secrets. And do so at scale in a multicloud environment.

- **B2B users:** As ever more complex business processes are digitized, B2B IAM needs to handle the increasing sophistication. The bar keeps rising for what it means to provide great B2B IAM, and the penalties for failing to keep up with the state of the art are also growing (such as lost revenue or fines for failing to protect data). IAM technical professionals tasked with enabling IAM for external business users need to support the expansion of scope of the B2B use case. In today's competitive and threat landscape, many IAM teams need to enable a broader set of B2B digital capabilities.
- **Decentralized identities:** Decentralized identity (DCI) will disrupt identity management by enabling privacy-enhanced verifiable identity data exchange over the internet. DCI is an attractive alternative to traditional models of storing, sharing and verifying identity data. DCI allows an entity to control their own digital identity by using decentralized identifiers (DIDs) to connect and authenticate themselves to other entities. Private keys and verifiable credentials (VCs) are contained in identity wallets, supported by an identity trust fabric (distinct from the identity fabric) for making DIDs discoverable. By establishing trust, privacy and security, organizations should identify relevant use cases to implement, such as supporting identity wallet and verifiable credentials in their IAM infrastructure, and thereby enable more user constituencies.

To support IAM in these efforts, IAM technical professionals must:

- Centralize governance and control, not storage and issuance.
- Expand IAM to workloads and their secrets.
- Expand IAM for B2B use cases.
- Adopt identity wallet and verifiable credentials.

Planning Considerations

Centralize Governance and Control, Not Storage and Issuance

In 2024, a strategic shift is needed from focusing on centralized storage and issuance to instead centralized governance and control in a decentralized IAM environment. Centralized IAM architectures that were once sufficient are no longer adequate, and they can't meet regulations or security, hybrid and multicloud, and geopolitical requirements. New architectural constructs are required that do not focus on single monolithic tooling strategies of previous generations of IAM but instead on centralized governance and control of multiple IAM tools.

Gartner defines this as a centralized/decentralized security (CeDeSec) pattern. This planning consideration is an evolution of last year's trend on CeDeSec, and there are already many established IAM examples of this pattern that showcase the powers of CeDeSec, such as:

- Centralized life cycle management and provisioning of identities in decentralized user stores using the provisioning protocol SCIM
- Centralized authentication using single sign-on in a decentralized application environment using OpenID Connect or SAML
- Centralized certificate management across decentralized certificate authorities using certificate management tools

---

The usage of the CeDeSec pattern must now be applied to all the major pillars of IAM: AM, IGA, PAM, authentication and authorization across all user constituencies (humans and machines).

The CeDeSec pattern must be applied to areas such as secrets management and policy management, and across multiple tenants within a single organization that all require the usage of multiple tools with the fundamental need for centralized control.

Recommendations:

- Accept and architect for the diversity of multiple IAM tools and environments. Make CeDeSec IAM architectures an accepted pattern and don't overconsolidate storage and issuance. This is a change, and it goes against the grain of single dashboards and easier management, instead focusing the strategies on enablement and reach into target platforms.
- Continue to de-silo ungoverned and uncontrolled environments using traditional IAM strategies. That said, where appropriate, keep multiple systems but focus on centralized governance and control to make sure the environments operate according to policy.
- Establish processes for discovery, ownership, automation and ensuring IAM systems are policy-compliant and expand CeDeSec strategies to more types of IAM tools and use cases.

Relevant research:

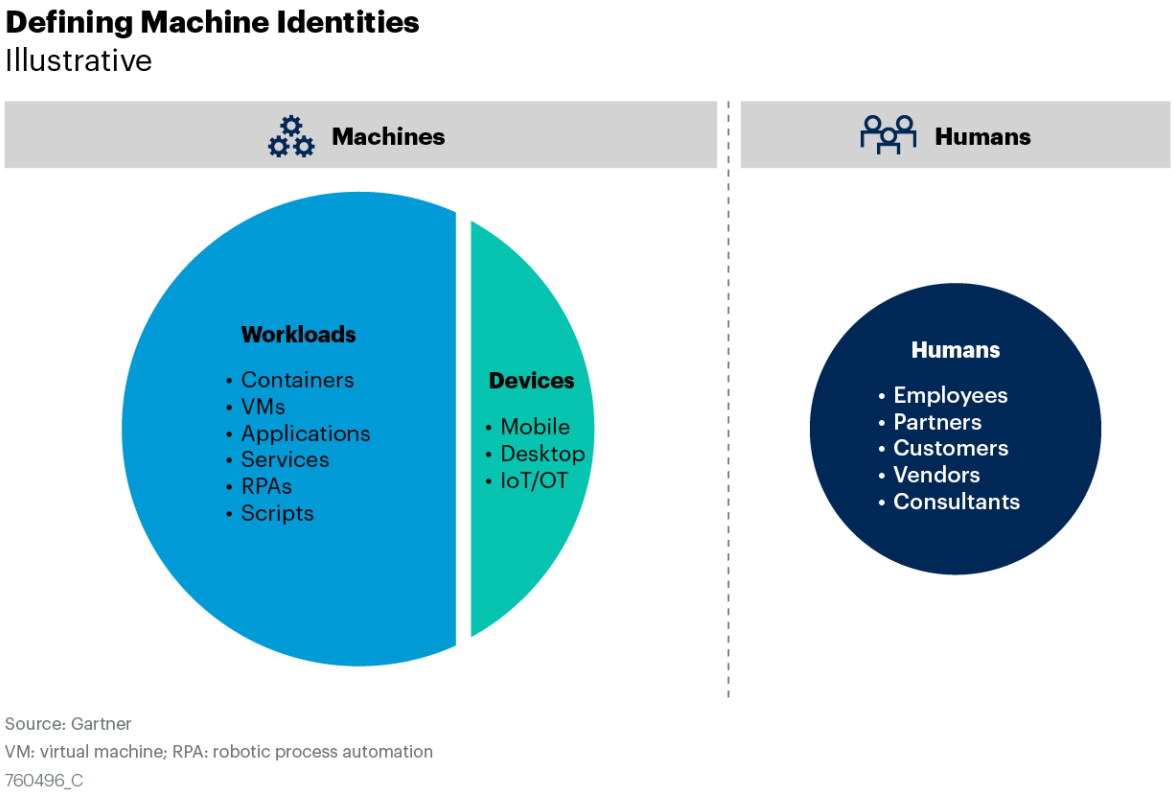
- Improve IAM Architecture by Embracing 10 Identity Fabric Principles
- Managing Machine Identities, Secrets, Keys and Certificates
- Architecting Modern Policy-Based Runtime Authorization
- A Multicloud Strategy Is Complex and Costly, but Improves Flexibility

Expand IAM to APIs, Workloads and Their Secrets

DevOps teams and developers move fast. When workloads are deployed to production multiple times a day from a DevOps pipeline, human intervention is no longer practical. Workloads all need identities and credentials such as secrets, keys and certificates. This planning consideration is therefore a continuation of last year's machine identity management trend. Sadly, credentials are still commonly stored in siloed local tools or are embedded in source code, environment variables and scripts. This leaves some of the organization's most powerful credentials at risk.

Visibility and automation is key, but in attempts to resolve this, different teams have their own tooling preferences. Cloud teams promote cloud-native tools; IAM teams promote existing IAM tools. It's not uncommon for development teams to set up their own tooling, especially for secrets. At the same time, security teams want a unified dashboard across all tools and the identities defined in Figure 7. This leaves organizations' automation, usability, security, compliance and single source of truth requirements unmet. Multiple tools are then involved, and each use-case pattern defines what type of tool is needed.

Figure 7: Defining Machine Identities



Source: Gartner
VM: virtual machine; RPA: robotic process automation
760496_C

Recommendations:

- Don't treat machines as humans and don't reuse human identities for your machines. Add machine identity management to the scope of the organization's IAM program and establish cross-functional teams that can make anchored tooling decisions that meet the multiple teams' needs.
- Work closely with platform engineering teams to help provide strategies for secrets and better API access control practices. The platform engineering team delivers, maintains and improves a platform as a product that supports development teams delivering custom-built software.
- Categorize your machines into devices and workloads. Workloads are more challenging than devices and require the introduction of new tooling. A crisp definition on what's in scope and what's not in scope makes it easier to lay out a phased approach and solve the organization's urgent needs.

- Leverage platform-provided identities for workloads such as the ones managed by cloud or container environments. It solves “secret zero” and life cycle management problems and avoids storing credentials at rest.
- Don’t expect a single technical “one and done” API access control pattern. Instead, define more evolved strategies that can scale to handle thousands of unique APIs. Focus on how to integrate IAM tools, authentication, authorization, and encryption strategies in and behind the API gateways.
- Establish a multitooling strategy for secrets management and make secrets management configuration part of an app migration playbook. Assess emerging vendors that provide secrets discovery in apps and dispersed secrets managers and provide secrets synchronization and rotation that enables centralized governance and control, instead of focusing on centralized storage and issuance.

Relevant research:

- Use Platform Engineering to Scale and Accelerate DevOps Adoption
- Managing Machine Identities, Secrets, Keys and Certificates
- Architect a Modern API Access Control Strategy
- Innovation Insight: Secrets Management Tools (additional license might be needed)

Expand IAM for B2B Use Cases

B2B use cases include vendor, contractor and subcontractor access, as well as customer access, such as business customer, partner, franchise, research collaboration and G2B interactions. Historically these two categories have been addressed by different vendors. Customer B2B capabilities are generally supported by customer IAM (CIAM) tools, and vendor/contractor/subcontractor access has been enabled by workforce tools.

The primary drivers of these two approaches have been the assumptions that customers need a branded experience, while workforce does not, and that sophisticated role-based authorization was needed for workforce but not for customers. For some organizations, this now is changing. Branding can be important for some partner relationships, such as sports franchises, and some organizations need more granular entitlement management for their business customers. IAM teams should engage broadly with all the parts of their organization that support digital B2B interactions (including marketing, development, security, legal, and compliance) to ensure that IAM services continue to evolve to support emerging business objectives.

Recommendations:

B2B user expectations, technology and legislation evolve rapidly. Because B2B IAM supports some of an organization's most important and sensitive digital transactions, it is crucial that B2B IAM be treated as a first-class citizen and reviewed on a regular basis. Best practices include:

- Improve security by extending adaptive access, SSO and MFA to B2B users. This includes using external privileged access management, where appropriate. For many organizations, third-party access is the weakest link in their security defenses.
- Roll out IGA for B2B users as warranted. Some organizations will require more-sophisticated B2B policies going forward, and will need to manage policies and entitlements more tightly.
- Use journey-time orchestration to improve B2B processes such as registration, SSO and authentication to provide a user experience that is both safer and more convenient.
- Augment existing journey-time orchestration processes with additional fraud-detection tools as warranted, to support security posture.
- Leverage industry-specific clouds where available.
- Prepare for a world in which more customers are bots. For some organizations, this may be a relatively natural extension of existing service-to-service capabilities. For others, it will require redesigning services.
- Synchronize your B2B IAM with other B2B data systems such as MDM, CDP and contractor data systems.

- Supplement B2B IAM capabilities with consumer-type self-service registration capabilities to support SMB partners and ad hoc business relationships as needed.

Relevant research:

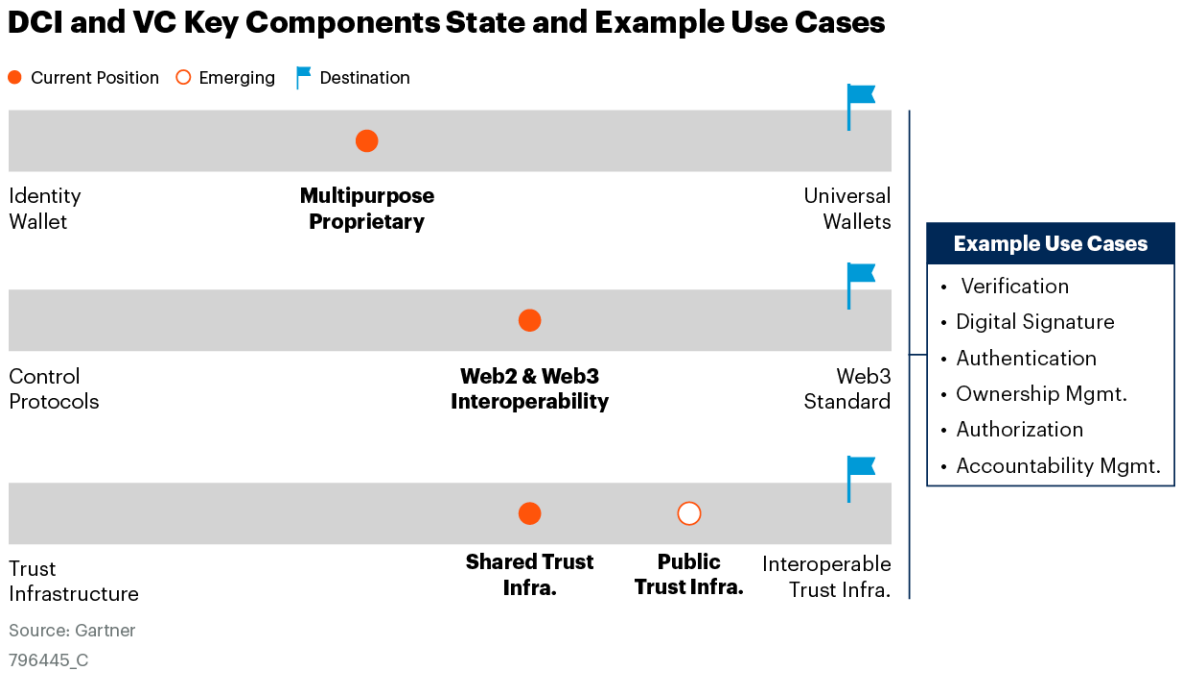
- Three Key Trends in B2B Customer/Partner Identity and Access Management
- Maverick Research: Fire Your B2B Sales Development Reps and Replace Them With Digital Humans
- Assessing External-Sharing Options in Microsoft 365

Adopt Identity Wallet and Verifiable Credentials

Decentralized identity and verifiable credentials enhance efficiency, privacy, and security while challenges such as key management and user experience are being addressed. This is further driven by electronic identification (eID) initiatives across the public sector as well as more privacy regulations. Technical professionals should consider decentralization as a spectrum in which the goal is to maximize decentralization as much as organizations and technical constraints allow. That means in its current form, decentralized identity may have centralized components. The current architecture relies on key components such as identity wallets, control protocols and services, and trust infrastructure. The industry is currently on a journey to drive standardization and interoperability for each component (see Figure 8):

- **Identity Wallet:** There are currently multipurpose identity wallets that are proprietary. The goal is to have standardized universal wallets like what we have seen with internet browsers' evolution. The OpenWallet Foundation initiative is a step toward this goal.
- **Control protocols:** There are currently interoperability protocols such as OpenID for Verifiable Credential Issuance that enable adoption of verifiable credentials using OpenID Connect in identity wallets with an available trust infrastructure.
- **Trust infrastructure:** There are currently centralized and shared trust infrastructure as well as emerging public trust infrastructure using blockchain that can enable identity wallet and verifiable credentials. The goal is to reach interoperable trust infrastructure services.

Figure 8: DCI and VC Key Components State and Example Use Cases



It is important to note that once decentralized identity goes mainstream, it enables typical identity functions such as passwordless authentication or some form of authorization using verifiable credentials. It will also enable other emerging Web3 services such as ownership and accountability services. While the true DCI and VC value will be realized when there are standards for identity wallets, protocols, and interoperable trust infrastructure, organizations can get value in the short term by implementing an identity wallet and verifiable credentials.

Recommendations:

- Implement identity wallet for users to enable verifiable credentials using a centralized, partially decentralized, or decentralized trust infrastructure.
- Use the identity wallet for remote onboarding, passwordless authentication, and other internal or external identity/credential verification.
- Extend identity wallet use cases to authorization to verify user eligibility for services and/or entitlements to gain access to resources.

Benefits:

- Increase efficiency: DCI/VC open opportunities to reinvent business processes to reduce friction in interactions/transactions that materially improve speed with cryptographic assurance.
- Improved security: DCI/VC reduce the number of centralized identity data repositories and data proliferation, which reduces the risk of data breaches, account takeovers and compliance issues.
- Enhanced privacy: DCI/VC give users more control of their identity/data by allowing them to hold their cryptographically signed credentials/data that can be shared only with their consent.

Prerequisites:

- Decentralized identity with a higher assurance level requires identity verification to bind the identity wallet to an entity. This may rely on existing identity verification services and/or trusted identity systems such as government or bank-issued identities.
- Decentralized identity success is highly dependent on establishing an ecosystem or marketplace of participating entities (identity owners, identity network operators and identity consumers). These entities must sign up and agree to trust policies and adapt their usage and services to required processes.

Cautions:

- Decentralized key management remains an area that requires ongoing work to address outstanding issues such as standards, interoperability and common approaches. These issues range from technical challenges — such as key generation, transport, maintenance and recovery — to ensuring rightful ownership of the identity wallet and reducing user administrative burden.

Relevant research:

- Guidance for Decentralized Identity and Verifiable Claims

The Number and Sophistication of Attacks on IAM Infrastructure Will Increase

Identity-first security strategies make the IAM infrastructure a primary target for attackers. Additionally, as identity furthers business enablement, this has also made resilience of the identity systems foundational to business functionality.

The identity threat detection and response (ITDR) trend is an expansion of last year's trend to improve protection of IAM infrastructure with ITDR practices and functions. Tools that support an ITDR practice bring monitoring and intelligence to identity systems. When posture drift or behavior analytics indicate an attack, actions and alerts can help to mitigate the threat. ITDR is a practice not a tool due to two important factors. First, no single vendor exists that supports all needed ITDR capabilities but there are tools that support the practice. Secondly, organizations are looking for detection and automated remediation, but manual handling is often needed.

In addition, inevitable and massive transformations in IT environments such as browser changes, quantum computers or just a bad implementation require monitoring, agility and control over IAM underpinnings such as protocols and cryptography. Organizations must establish agility strategies *before* the underpinnings break.

To support IAM in these efforts, IAM technical professionals must:

- Discover attacks and misuse using ITDR capabilities.
- Prepare for protocol and crypto apocalypses with agility.

Planning Considerations

Discover Attacks and Misuse by Using ITDR Capabilities

Tools that support an ITDR practice monitor both security posture and user behavior. If posture drifts or suspicious behavior is detected then the tools allow security teams to respond in an appropriate manner.

It is important to note that posture management and detection are different, but closely related. For example, tools that provide posture management and ITDR capabilities can detect that someone inappropriately has privileged access. However, they differ in their response. With tools supporting posture management, the detection occurs at administration time; for example, when generating a report. Tools that support ITDR continuously monitor activity at runtime. This brings real (or near real time) detection to posture drift or misuse of systems. They are both needed to discover attacks and intended or unintended misuse.

The primary capability IAM teams require is the "response" of ITDR, but a response first requires detection. Removing a privileged role, disabling a newly created account, or blocking access to a sensitive system all disrupt the next step of the attack chain. Disrupting the attack chain in real time is critical. Using reports to see the completed attack days later is of little use.

Tools come from a variety of backgrounds or have been created to fill specific gaps in the ecosystem. These are the different approaches:

- Monitor SaaS-delivered IAM providers using the providers APIs.
- Active Directory (AD) tools that detect changes via domain controller replication.
- Network agents that monitor user behavior.
- Creating decoys, or honeypots.
- Network or endpoint detection and response tools.

Unfortunately, most tools specialize in only one or two forms of detection, meaning a holistic detection strategy may require multiple tools.

For example:

- AD TDR tools can remove privileged accounts when added to inappropriate security groups.
- Network agents that can require users to use MFA before accessing a resource.
- Additional decoys may be deployed to confuse and slow attackers.

One form of response is uniformly supported: security information and event management (SIEM) integration for alerting. SIEM integration is crucial even if an automated response occurs. Someone must be responsible for the activity and the source of the threat must be mitigated. Just because a privileged role was removed doesn't mean the threat is completely mitigated. Who assigned the role, and how?

Recommendations:

- In vendor messages, don't mix up tools that support ITDR with tools that support posture management. Categorize them based on whether they are runtime or admin-time tools to understand how they technically operate.
- IAM and security teams must work together to develop and implement plans of action to meet the specific types of threats they may detect. All responses, particularly human-driven, need to have playbooks established prior to the event. The time from compromise to consequences shortens every day. During an attack is not the time to decide the appropriate response or contact a subject matter expert. Just as real-time detection is crucial, so is real-time response. IAM is accountable for incorporating the ITDR initiative into the identity fabric. The security operations center (SOC) team should be responsible for the ITDR process definition, along with execution and integration into SOC processes based on requirements.
- Fill gaps in ITDR requirements by assessing the full range of attack vectors and telemetry covered. Plan to use a mosaic of tools that complement each other, and may overlap, to meet the requirements for a comprehensive ITDR initiative.

Relevant research:

- Implement IAM Best Practices for Your Active Directory
- Quick Answer: Who Is Responsible for Identity Threat Detection and Response? (additional license might be needed)
- Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response (additional license might be needed)

Prepare for Protocol and Crypto Apocalypses With Agility

The day will come when your encryption, signing, authentication and federation technologies will experience an inevitable and massive transformation event that obsoletes them. It is only a matter of time as many transformational changes, or just bugs, have the potential to obsolete a technology or deployment. Examples are:

- Browser changes as the industry is considering privacy-preserving changes to browser redirects that deeply impact federation protocols, such as SAML and OpenID Connect, that heavily rely on them
- Compromised keys
- Large-scale quantum computers
- Hardware-related issues in the wake of bugs, such as Meltdown and Spectre
- Regulative or policy changes such as the U.S. memorandums for federal agencies to prepare for post-quantum cryptography, or Google announcing its intention to limit the lifetime of TLS certificates to 90 days

Rapidly discontinuing the usage of a tool, standard, algorithm or key is not easy, and requires planning and a high degree of monitoring and automation.

"Crypto-agility" is the answer to the "cryptopocalypse," and crypto-agility is all about how fast you can get back up on the other side.

Recommendations:

- Migrate away from legacy protocols such as SAML. Not because modern alternatives are immune to changes but because they are actively maintained and developed. SAML working groups have been inactive for over 15 years, and common SAML deployments rely on above-mentioned browser redirects as well as Web Services Security [WS-Security] that lack efforts that make it quantum-safe. Gartner doesn't expect legacy protocols to be updated, but instead recommends a faster migration to modern, still maintained, and often crypto-agile, alternatives such as OpenID Connect.

- Prepare for changes to cryptographic algorithms by building an inventory of metadata for applications that use cryptography. This should also include the access protocols used (also see the above Modernize IAM in Legacy Apps and Services section and Managing Machine Identities, Secrets, Keys and Certificates for further details). This will give your organization a way to scope the impact of new cryptography, determine the risk to specific applications, and prioritize incident response plans accordingly.
- Establish contingency plans for an organized and instant shift from one technology to another. Some things are harder than others. Establish manual plans where automation isn't possible.
- Continually monitor cryptographic alternatives, and ensure that any defined incident plans have a swap-out procedure. Monitor resources, such as the National Cybersecurity Center of Excellence's (NCCoE's) Migration to Post-Quantum Cryptography Building Block Consortium.
- Ensure that both the lifetime of the currently used encryption algorithm, and the time it takes to retool a solution, are less than the estimated time it takes for the algorithm to be broken.
- Quantum-safe preparedness will not only be an algorithmic problem but also (mainly) a manufacturing and logistic problem. All deployed hardware that generates and stores keys and performs crypto in the world must change. Ask your cryptographic hardware (such as hardware security module [HSM] and FIDO token) vendors to prepare for changes to algorithms and key generation beyond just proofs of concept.

Relevant research:

- Managing Machine Identities, Secrets, Keys and Certificates
- Preparing for the Quantum World With Crypto-Agility (additional license might be needed)

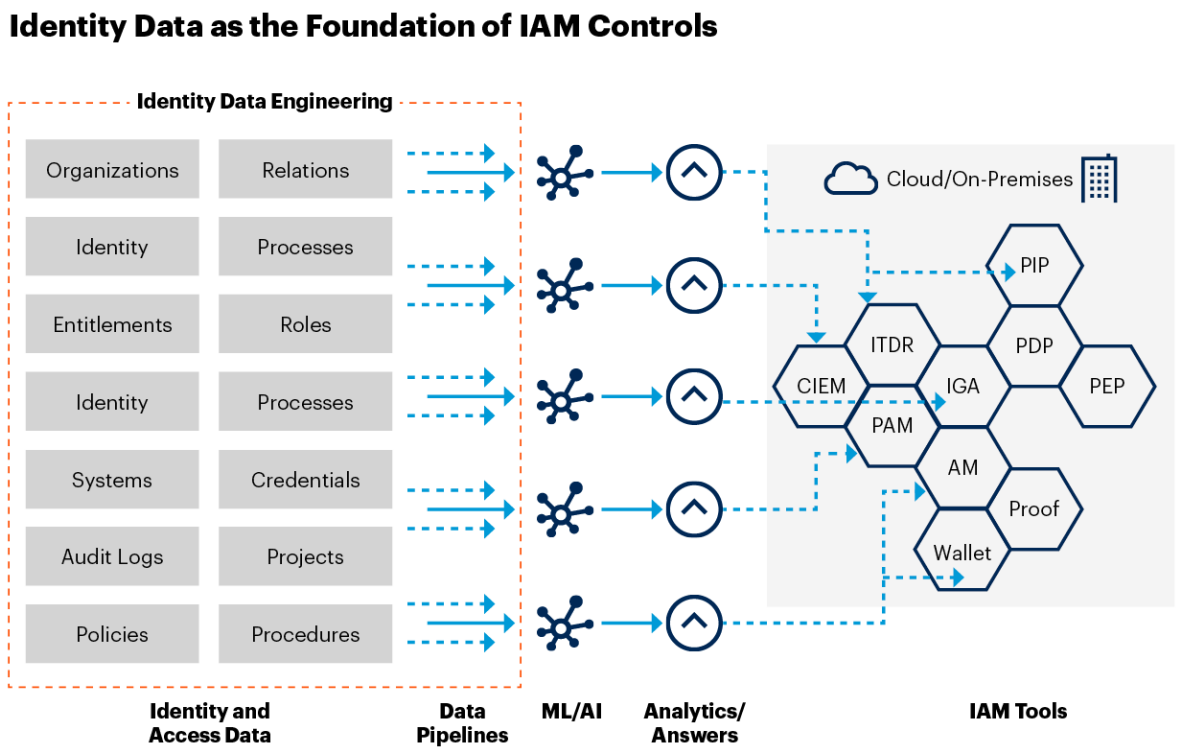
Stronger Identity Data Strategies Will Enable Analytics and Generative AI Application in IAM

IAM has become too complex and fast-changing for humans to identify entities and control their access without the help of automation that uses machine learning. The emerging IAM design vision is that the IAM systems and end users themselves should perform the majority of IAM tasks, with appropriate analytics guardrails. These guardrails remain under the supervision of IAM administrators, business managers and auditors via administrative and self-service user interfaces. However, this is increasingly dependent on identity and access data and the underlying data infrastructure (see Figure 9 for high-level concept). A continuous stream of data is needed for developing descriptive, diagnostic, predictive, and prescriptive analytics in many IAM use cases in almost all classic and emerging IAM tools. Examples use cases include:

- Enabling smart continuous adaptive access controls
- Discovering vulnerabilities and misconfiguration
- Detecting attacks on IAM infrastructure
- Role mining and policy automation

The data will also be needed to fine-tune foundation models for adopting generative AI in IAM to support a wide range of interactive and automation use cases. Generative AI has the potential to substantially alter how users, administrators, developers, and auditors interact with IAM systems, using natural language. This can happen through new GenAI-enabled channels such as an IAM copilot (an intelligent agent that can assist with IAM-related tasks) or through in-product features in IAM tools.

Figure 9: Identity Data as the Foundation of IAM Controls



Source: Gartner
796445_C

However, organizations are challenged to establish or sustain specialized IAM data management practices to support these IAM data products with timely quality data. This is due to a variety of reasons, such as siloed data, poor data hygiene, slow or broken data pipelines, data duplication and inconsistencies, and lack of metadata.

These challenges are exacerbated by the renewed drive to enhance security posture as well as the momentum to evolve ML/AI in IAM using generative AI to enhance automation in IAM controls. That's why organizations increasingly require formalization of ad hoc identity analytic functions as data products and adoption of generative AI in IAM functions. These analytics-driven data products and emerging generative AI tools will provide a set of identity and access intelligence (IAI) capabilities that will be critical for enhancing IAM controls.

IAI is highly dependent on identity data engineering, which allows technical professionals to clearly define data requirements and architecture moving forward. By establishing sound identity data engineering practices, organizations can increase the quality of identity and access data to enable smarter and more continuous access controls as well as accelerating GenAI adoption in IAM.

To support IAM in these efforts, IAM technical professionals must:

- Establish identity data engineering strategies
- Accelerate identity and access intelligence with generative AI

Planning Considerations

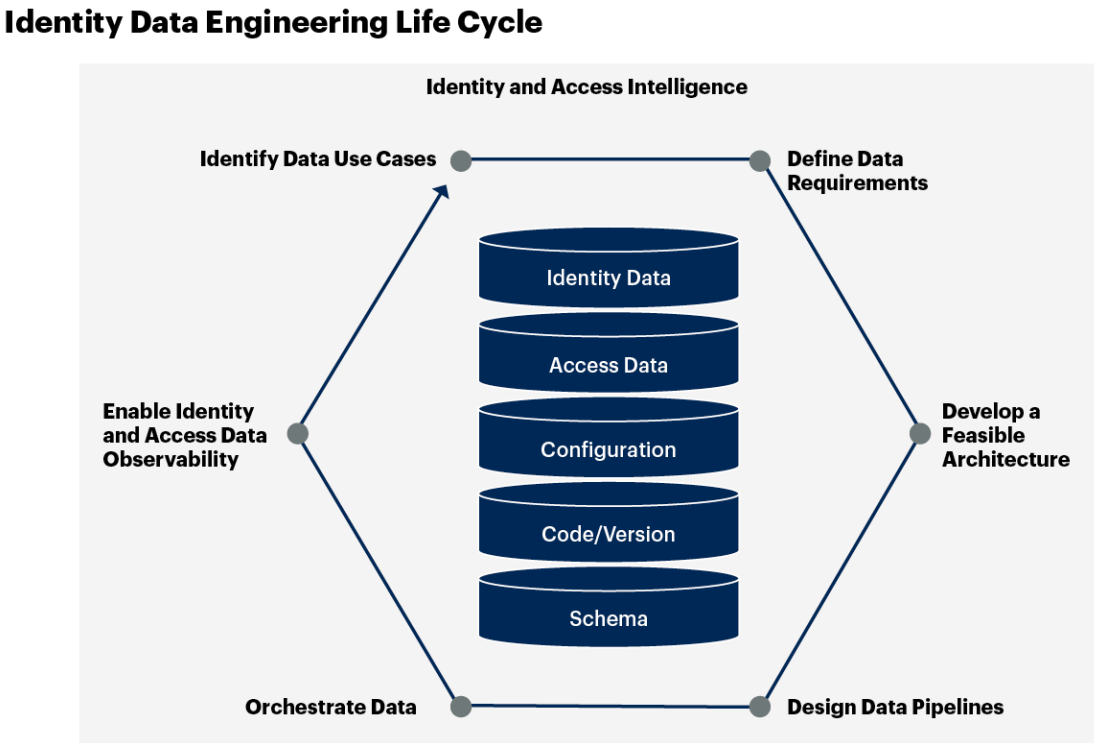
Establish Identity Data Engineering Strategies

Data engineering is the discipline of making data usable through data modeling, catalog, ingestion, storage, processing, integration, testing, and orchestration. Data engineering also provides a methodical approach to design data lakes and data warehouses and to implement data pipelines. The objective of identity data engineering is to help an organization move, store and/or transform/process identity and access data and prepare it in appropriate data platforms for enabling/supporting different IAM capabilities (AM, PAM, IGA, fine-grained authorization) across different environments (on-premises or cloud). The engineering aspect of this process is to ensure identity data quality and visibility consistently, efficiently, scalably, accurately and within compliance.

Technical professionals should use an identity data engineering life cycle to manage the growth of identity data systems and the number of identity data pipelines being built. The key steps, depicted in Figure 10, include:

- Identifying identity data use cases
- Defining data requirements
- Developing a feasible architecture
- Designing data pipelines
- Orchestrating data
- Enabling identity and access data observability

Figure 10: Identity Data Engineering Life Cycle



Source: Gartner
796445_C

Recommendations:

- Develop identity data use cases with a product mindset (considering quality, reliability, availability, interoperability and reproducibility) when developing data pipelines and data-driven IAM capabilities (such as policy information point, adaptive access, access modeling, access request, access certification, posture management).
- Create maintainable solutions that leverage an identity data catalog and accommodate new identity data sources (HCM, contractors, machines), relationships, and ever-changing requirements for data ingestion, data processing and data storage.
- Incorporate continuous data, and continuous code testing practices to detect and manage data drift, configuration drift and infrastructure drift. Incorporate data observability and build robust data operations to identify and catch bad data as quickly as possible.

- Collaborate with data management teams to add some level of data engineering skills that complement and build on top of IAM skills. Some of the critical data engineering skills include distributed systems architecture, databases (relational and nonrelational), data management, data modeling, and data analysis.

Cautions:

- Avoid overengineering, overabstraction and overgeneralization. Data engineering tools are already complex, and distributed systems are inherently complex. Avoid the urge to build everything in-house. Leverage commercially available technologies and tools such as data management capabilities with IAM tools and complement them with external data platforms' data engineering tools as needed.
- Data, framework, schema, infrastructure, code and models can be difficult to manage, track and correct. Automated tools to detect, manage and remediate drift, especially in data and machine learning models, are still in infancy, and hence, engineering practices must be in place to reduce the time to detect and remediate drifts.
- Lack of schema enforcement can lead to type inconsistency and corruption. Data catalog and schema management is extremely critical for large organizations and large teams looking to collaborate and share identity data and metadata across silos.

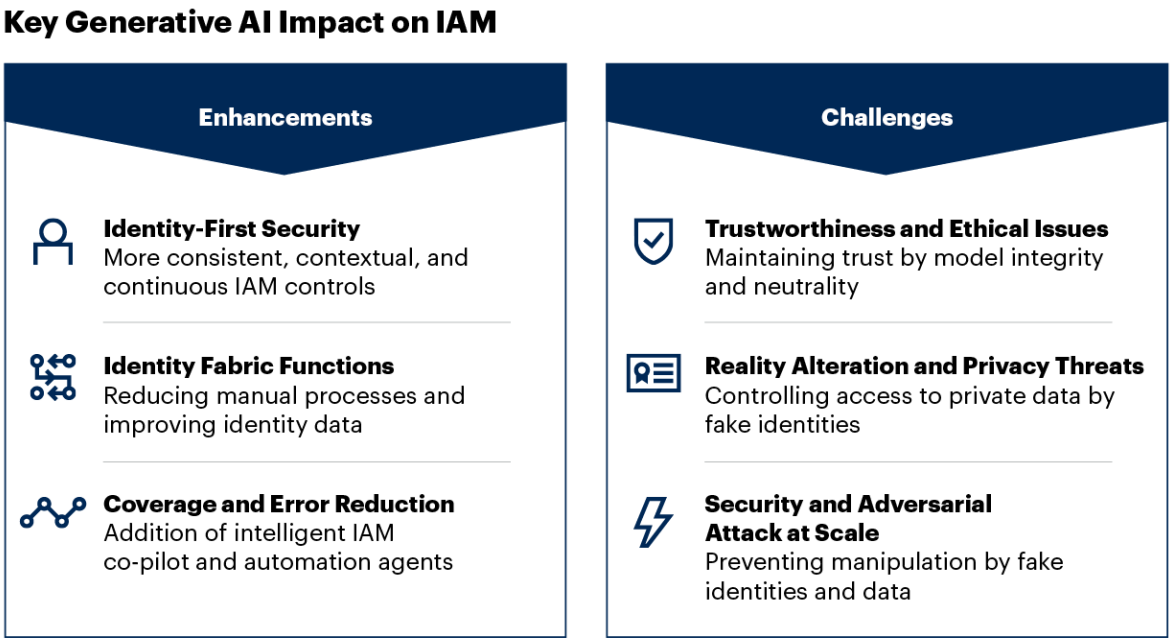
Relevant research:

- Data Engineering Essentials, Patterns and Best Practices

Accelerate Identity and Access Intelligence With Generative AI

The era of leveraging GenAI in IAM solutions is upon us. GenAI will disrupt IAM by providing a new user/admin experience through natural language that wasn't imaginable before. Organizations should prepare themselves to adopt GenAI as part of their IAM processes and infrastructure by developing IAI capabilities. Strategies require understanding the key IAI use cases and developing an IAI architecture. IAI enables implementing natural language interaction with IAM processes and systems using an IAM copilot or in-product IAI features to automate complex IAM tasks. Figure 11 shows some of the key benefits and challenges of GenAI in IAM.

Figure 11: Key Generative AI Impact on IAM



Source: Gartner
796445_C

While we are at the early days of GenAI and its application in IAM, this is a fast-moving technology that can quickly evolve and change the IAM threat landscape as well as how we implement and operate IAM controls.

GenAI holds reasonable promise to enhance identity governance, administration, and authorization capabilities to simplify policy language interpretation/generation and interoperability at scale by removing siloed systems' configuration. While the foundation of identity fabric remains the same, GenAI has the potential to significantly automate the tedious tasks, such as managing rules, entitlements, privileges, and access risk, as well as ensuring configuration completeness and identity security.

Identity and access intelligence (IAI) capabilities can harness the GenAI innovation in conjunction with IAM data and analytics efforts to take the application of machine learning in the IAM field to new heights:

- **Architecture:** IAI has two sets of key components, including an IAM GenAI model and IAM GenAI orchestration. The IAM GenAI model safely embeds IAM semantics (such as vocabularies for defining contextual access entitlement by roles, purposes, policies and relationships) in a customized LLM foundation model. The IAM GenAI orchestration allows the creation of sophisticated prompt pipelines (also known as chains) to integrate IAM semantic functions (as customized prompts) into identity fabric functions (in IAM tools) for automating complex tasks. IAM semantic functions are predefined prompts (or templates) designed for a specific IAM task.
- **Use cases:** IAI can support a wide range of use cases, using an IAM copilot or embedded capabilities to query, configure, extend, integrate, and orchestrate IAM tasks. However, GenAI is most feasible where users or systems can interact with IAI to obtain and tailor the information they need while they remain accountable and responsible for the secure and safe use of the data in IAM tasks. GenAI for full automation may become more feasible as organizations further use reinforcement learning from human feedback (RLHF) to enhance the quality and fidelity of models' output.

IAM technical professionals should initially focus on practical projects (in collaboration with the organization AI team) that can add value while establishing the foundation of the GenAI-enabled IAI initiative. This requires defining key use cases for each IAM system with appropriate datasets and then iteratively enabling them with training and tuning in each iteration. For example, an IAM copilot can help with both general and technical IAM use cases:

- **General use cases:** An IAM copilot can help users with general Q&A use cases such as systems search, support and queries. This assumes that IAI systems can be trained to leverage either the entire enterprise or domain-specific knowledge of contextual IAM artifacts, constructs, and data (or employing techniques to enrich the prompt through enterprise data that uses retrieval augmented generation).
- **Technical use cases:** An IAM copilot can help developers and administrators with a range of script and code generation to assist with system configuration use cases. These are scenarios for which identity fabric functions require customized scripts to perform some specific tasks. An IAM copilot can work on commands and API references to generate customized scripts for integration and orchestration services.

Recommendations:

- Evaluate and adopt practical IAI capabilities to complement classic ML/AI efforts with the addition of GenAI. Develop and maintain a feasible IAI architecture strategy that includes consideration for dependencies such as data quality and volume as well as identity data engineering disciplines.
- Evaluate relevant IAI use cases to incorporate GenAI capabilities as part of the enterprise identity fabric functions, such as the addition of an IAM copilot and in-product features. Large and complex organizations should evaluate key components such as GenAI large language models and orchestration technologies for implementing custom IAI solutions. Small and midsize organizations can start with adopting vendors' in-product capabilities.
- Develop an IAI assurance framework to govern responsible GenAI and classic ML/AI adoption in IAM. Establish input and output safety controls that ensure privacy and regulatory compliance as well as correctness and explainability of guidance and automation generated by GenAI capabilities. This should be done in alignment with the broader AI initiative in the organization.

Prerequisites:

- IAI training and tuning rely on extensive and high-quality data. This requires a disciplined approach to identity data governance and metadata management to enhance data visibility and remove blind spots. Some use cases may need capturing context using a vector database as part of the solution to further enrich user prompts with more relevant information to correctly comprehend and generate relevant recommendations.

Cautions:

- The integrity of an entity's identity (human or machine) and the trust foundation are at the core of IAM. Organizations should maintain the trust in identities and related data as well as the capabilities and the underlying models. However, the lack of transparency in GenAI mechanisms, data sources, and potential bias will cause hesitancy to automate action directly from outputs of GenAI applications. The ability to validate and explain the generated recommendations is critical to gain enough trust in the GenAI-enabled IAM capabilities to incrementally increase the level of automation. Good explainability could also become a differentiator for IAM vendors.

Relevant research:

- Identity and Access Intelligence Innovation With Generative AI

Evidence

[1] Global Small Business Multi Factor Authentication (MFA) Study, Cyber Readiness Institute (CRI).

[2] Identity Is the New Battleground, Microsoft.

[3] 2023 State of Cloud Permissions Risks Report, Microsoft Security.

[4] Infographic: Benchmark Data From the IT Score for Identity and Access Management

[5] See Shift Focus From MFA to Continuous Adaptive Trust for additional information.

[6] In a push bombing attack, the attacker induces an application to send multiple push authentication messages to the victim's smartphone until, confused or frustrated, that person clicks the accept button, allowing the attacker to get in.

[7] 2022 State of Passwordless Security, HYPR.

[8] Web Authentication: An API for Accessing Public Key Credentials Level 3, World Wide Web Consortium (W3C).

[9] Organizations with existing but distinct MFA and AM implementations may want to reevaluate their need for a separate MFA solution. Their AM tool's MFA capabilities may be more than adequate. See Market Guide for User Authentication.

Document Revision History

2023 Planning Guide for Identity and Access Management - 10 October 2022

2022 Planning Guide for Identity and Access Management - 11 October 2021

2021 Planning Guide for Identity and Access Management - 9 October 2020

2020 Planning Guide for Identity and Access Management - 7 October 2019

2019 Planning Guide for Identity and Access Management - 5 October 2018

2018 Planning Guide for Identity and Access Management - 29 September 2017

2017 Planning Guide for Identity and Access Management - 13 October 2016

Recommended by the Authors

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

Improve IAM Architecture by Embracing 10 Identity Fabric Principles

Guidance for Identity Governance and Administration

Guidance for Privileged Access Management

Solution Path for Modernizing Access Management

Avoid the Top 9 Pitfalls of Implementing MFA

Guidance for Modernizing Authorization Architecture

Managing Machine Identities, Secrets, Keys and Certificates

Essential Skills for IAM Architects

Identity and Access Intelligence Innovation With Generative AI

Table 1: Recent Examples Illustrating Gaps in Organizations' Foundational IAM Capabilities

Area	*Example*
MFA as a strong security control mitigating account takeover attacks	Only 46% of small and midsize businesses (SMBs) implement MFA. [1] Just 22% of monthly active users in Microsoft Entra ID (formerly Azure Active Directory, or Azure AD) use MFA. [2]
Cloud access	Less than 2% of cloud entitlements are actually used. [3]

Source: Gartner (October 2023)