2022 Planning Guide for Identity and Access Management

Published 11 October 2021 - ID G00753956 - 67 min read

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

Initiatives: Identity and Access Management for Technical Professionals

Ubiquitous anytime, anywhere computing requires new approaches to IAM architecture and operations. Security and risk management technical professionals must leverage identity and access management trends to further evolve IAM roadmaps and architecture as part of their 2022 initiatives.

Overview

Key Findings

- Architecting higher levels of IAM integration and enabling more rapid IAM change require deeper coordination with other functions and business units.
- Increased IT diversity and choice, greater interconnectedness and a faster pace of change are leading to disjointed architectural decisions.
- Many of the existing IAM architectural patterns are not flexible enough to sustain high rates of change. Organizations should evolve their IAM capabilities over time to operate as a distributed identity fabric. An identity fabric is a key component of the emerging cybersecurity mesh architecture approach.

Recommendations

Security and risk management technical professionals focused on IAM should:

- Improve security by removing implicit user (human and machine) trust from all computing infrastructure over time and replacing it with explicitly evaluated, real-time adaptive trust for just enough access to enterprise resources.
- Reduce risk by prioritizing the rollout of foundational best practices such as multifactor authentication (MFA), zero standing privileges and zero-trust architecture if not already fully implemented.

- Enhance IAM agility and reach by removing silos and incrementally adopting the distributed, composable cybersecurity mesh architecture approach when making architectural decisions.
- Optimize distributed architecture by evolving IAM governance, processes and infrastructure to efficiently support hybrid/multicloud environments.

Identity and Access Management Trends

Download All Graphics in This Material

The theme for 2022 is the need to empower IAM teams to support ongoing change. This includes change driven by the continued evolution of technology best practices, change in organizational priorities, change in user expectations and change in opportunities and threats. A transformation has occurred. Digital business is now business, and business now relies on digital trust, which, in turn, is enabled by IAM. Therefore, security and identity now are an essential foundation of your business ecosystem. In a world where change is the norm, it is now much more important for organizations to architect IAM infrastructure to be flexible and for IAM to partner with other functions to meet changing organizational requirements.

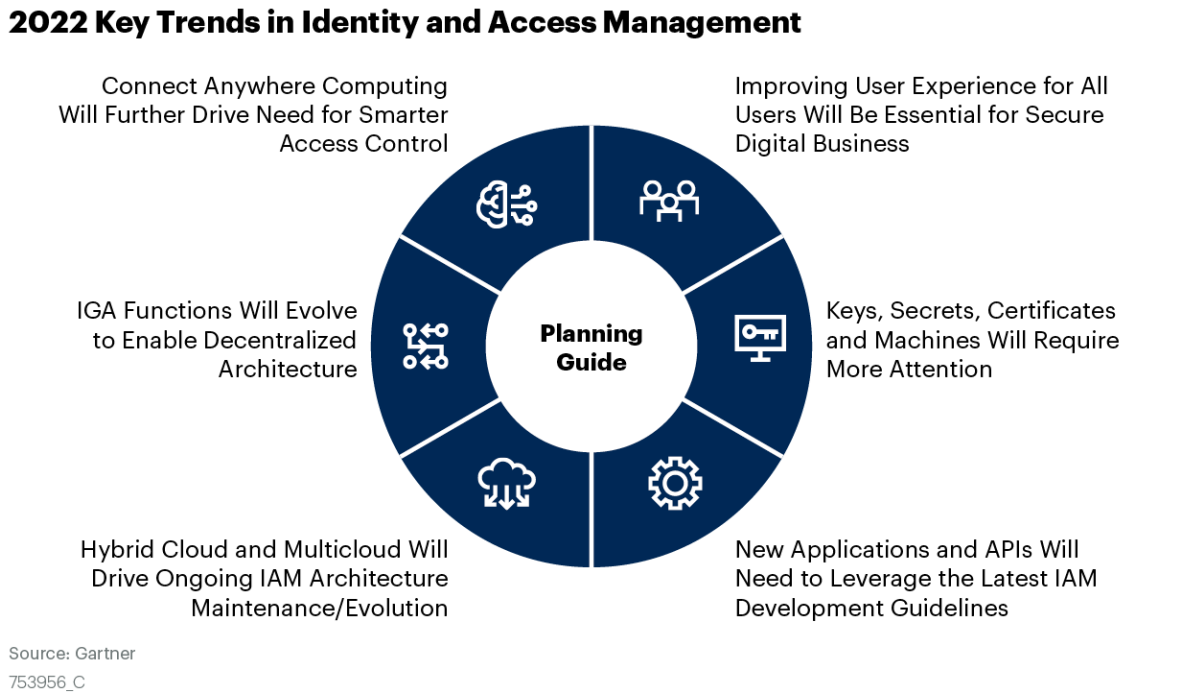
As organizations prioritize their IAM initiatives for 2022, they should choose ongoing and incremental projects to evolve their IAM deployments to better fit changing organization needs by being more flexible and less siloed and by requiring even fewer manual operations.

Gartner Welcomes Your Feedback

We strive to continuously improve the quality and relevance of our research. If you would like to provide feedback on this document, please visit Gartner GTP Content Feedback to fill out a short survey. Your valuable input will help us deliver better content and service in the future.

Figure 1 shows six key IAM planning trends for 2022, which correspond to categories of IAM tools, deployment architecture and best practices, along with their associated planning considerations.

Figure 1. 2022 Key Trends in Identity and Access Management

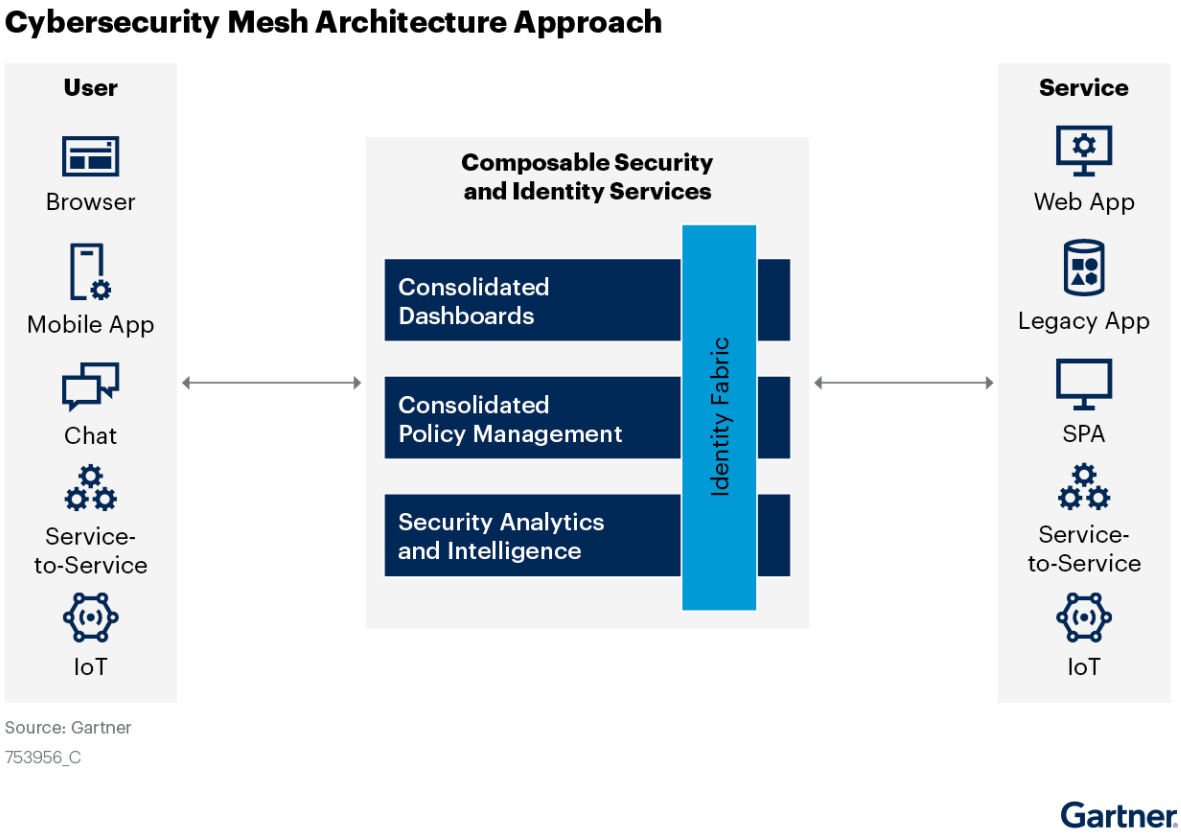


Evolving a more secure, resilient, composable and distributed IAM infrastructure is now mission-critical for all organizations to keep-up with ever-changing IAM demands.

To address this need for more IAM adaptability, cybersecurity mesh architecture (CSMA) is an emerging scalable architecture for extending security controls to all your assets by enabling centralized or delegated administration and policy configuration for decentralized applications, services and other digital resources. CSMA is not something that you can buy. It is a distributed approach that addresses the growing complexity of security and identity deployments by eliminating unnecessary silos. Rather than every security and identity tool running in its own silo, a cybersecurity mesh architecture enables tools to plug into a broader framework. This could include unifying mobile and call center authentication as part of an omnichannel approach that enables sharing of data and session across channels to improve customer service. It could also include consolidating multiple disconnected dashboards to reduce administrative overhead and improve responsiveness. Note that a cybersecurity mesh may still include multiple instances of specific types of IAM tools to meet security domain, data residency requirements and other such requirements. CSMA is not a prescription to overconsolidate; for example, many organizations legitimately have more than one access management tool.

As shown in Figure 2, cybersecurity mesh architecture is composed of four components, one of which is an identity fabric.

Figure 2. Cybersecurity Mesh Architecture Approach



- **The identity fabric layer** enables any user or thing to safely and conveniently access any application or service from any device anywhere: The identity fabric [1] layer is a distributed identity framework that supports all of the IAM functions through the integration of one or more IAM tools. In its first phase, the identity fabric largely consists of your existing IAM infrastructure. For example, an identity fabric includes directory services, adaptive access and entitlements management. It orchestrates a full range of identity use cases from customer access to API access. Today, an organization's identity tooling consists of a loosely connected IAM infrastructure with islands of tools that solve individual IAM use-cases. Deeper integrations between the tools are now required, and integrated tools form a composable identity fabric. An example is the integration of an MFA tool and it's adaptive access functionality with the PAM tool. As integrations become more standardized and interconnected, the identity fabric will become the composable element that enables any user, any device, any service IAM use cases in hybrid and multicloud environments. The evolution of an organization's identity fabric must be done in phases.

- **The security analytics and intelligence layer** is the foundation: It consumes data streams, including log data from the identity fabric, and provides risk signals and events to other components and services/endpoints/targets.

- **The consolidated policy management layer:** As security and IAM use cases proliferate, policy logic, including authorization and access policies, has become overly fragmented. Organizations should architect for more centralized policy management and expect more distributed policy runtime evaluation so that policy enforcement is performed near the resource being protected.

- **The consolidated dashboard layer** is able to consume events and other information from multiple sources as well as provide integrated and consolidated dashboards for users: Today, in many organizations, ongoing operations and rapid incident response are hampered by the proliferation of siloed dashboards.

The unrelenting push to reduce labor and license costs and make even more efficient use of IAM infrastructure to improve security and usability is increasing pressure on organizations to further optimize their IAM infrastructure. For example, Gartner has a Strategic Planning Assumption:

- By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a cooperative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.

In this time of rapid technology change, expect to see both continued convergence of more mature IAM functions and the need for third-party add-ons (including identity resolution and fraud detection) that don't disproportionately increase operational overhead.

An identity fabric is an important architectural approach to incorporate into your planning. What other factors should organizations consider as they plan their IAM initiatives for 2022 to meet current requirements and incrementally evolve their IAM toward a cybersecurity mesh architectural approach?

Key factors that will impact IAM planning in 2022 include:

- Sustained importance of strong adaptive authentication and authorization to enable user access from anywhere to anywhere.
- Requirement to continually improve user experience for all users (both end users and administrative users) as they conduct more of their interactions online and as administrative users need to support higher rates of digital change.
- Imperative to better protect digital keys and secrets as well as manage the digital identities for a growing number of machines (devices and workloads).
- Need to further standardize API and applications access control best practices and secure the DevOps toolchain as part of software development processes.
- Growing necessity of maturing IAM infrastructure architecture, especially its relationship to the hybrid and multicloud resources it protects and the use of native cloud infrastructure and platform services (CIPS)-specific IAM resources.
- Demand for more flexible and easier to use identity governance functions that reduce complexity, protect from cyberthreats and adjust to meet the needs of a wider range of organizations.

These factors are framed by the following 2022 IAM technical planning trends:

- Connect anywhere computing will further drive need for smarter access control.
- Improving user experience for all users will be essential for secure digital business.
- Keys, secrets, certificates and machines will require more attention.

- New applications and APIs will need to leverage the latest IAM development guidelines.
- Hybrid cloud and multicloud IT will drive ongoing IAM architecture maintenance/evolution.
- Identity governance and administration (IGA) functions will evolve to enable decentralized architecture.

These planning trends are discussed in detail in subsequent sections. The relative importance of each of these trends and their planning considerations depends on the organization's current IAM maturity. Gartner has observed a growing gap between organizations with a mature IAM program and those that are behind from a technology and/or organizational perspective.

Connect Anywhere Computing Will Further Drive Need for Smarter Access Control

The transition to more remote, connect anywhere computing is placing greater demands on access management deployments. Remote access increases the attack surface, and organizations must implement additional mitigating controls to contain this risk. Identity is now the ultimate perimeter that controls access, and that perimeter is constantly being challenged. Therefore, access management platforms must become increasingly sophisticated in order to differentiate between valid users and malicious bots or fraudsters without annoying legitimate users. This risk is further exacerbated by the need to support remote access not only for internal end users, but also for administrators and other privileged personnel as well as external parties such as vendors and partners. To cope with this increasing complexity, organizations and vendors are using more advanced (often machine-learning-based) analytics to automatically process ever higher volumes of authentication and access data and logs.

Organizations also must grapple with the challenges of multicloud adoption, proliferation of devices, newer approaches to IT delivery (DevOps), new architectural patterns (service meshes, containers) and a growing number of users including human and machines (i.e., nonhuman users). The need to support new architectural patterns is exacerbated by the growing recognition that many organizations will continue to operate multiple generations of IT technology. Therefore, most organizations need to provide secure multigenerational access management for the indefinite future. Gartner has seen an uptick in inquiries on how to integrate legacy and header-based web applications into a flexible modern identity infrastructure (identity fabric). Organizations want to support multiple options for user and device access as well as multiple generations of digital assets. However, they do not want to rely on siloed approaches of the past that unnecessarily duplicate elements (such as authentication and authorization) for each access channel and digital service.

To further reduce risk, organizations are investigating zero-trust approaches. Achieving a zero-trust architecture for all your digital resources requires that you authenticate all users of all types and explicitly authorize access near service endpoints. Access management tools are the cornerstone of a zero-trust strategy and are typically used to enable web access for workforce and external users. Access management tools can assess risk and trust dynamically and apply continuous adjustments of risk or trust in an explicit manner to, for example, block or terminate access. To obtain a comprehensive zero-trust architecture a, zero-trust network access (ZTNA) tool is also required. ZTNA reduces implicit trust for access to nonweb and web applications for internal users and B2B users. ZTNA technologies typically start with remote access needs such as augmenting or replacing a less granular VPN. ZTNA technologies generally rely on access management tools to provide user authentication.

Organizations want to enable any user or machine to safely and conveniently access any application or service from any device anywhere, and to accomplish this broader integration with a minimum of IAM license and labor costs. This requires smarter, more flexible access management deployments that have more-automated and efficient administrator user interfaces.

Planning Consideration

Finish Rolling Out and or Improving MFA for All Users

Passwords alone are insufficient for protecting assets. Although this statement comes as no surprise, most organizations still need to broaden or begin to deploy MFA. A recent Gartner survey revealed that only 55% of respondents have implemented MFA for administrator access to Active Directory. [2] Client inquiry reveals that regular user authentication is worse yet.

As in previous years, passwords are still the primary method of compromising accounts. Phishing, credential stuffing and spraying are effective attacks against accounts lacking an additional authentication factor. Even simple SMS-based authentication mechanisms can block up to 100% of automated bots, 99% of bulk phishing attacks and 66% of targeted attacks. [3]

IAM technical professionals should, if not already implemented:

1. **Require MFA for all privileged access:** Privileged accounts are a primary target for account takeovers. Compromises lead to breaches of the most sensitive data and shut down entire organizations. There are a variety of tools and strategies available to control authentication for privileged accounts such as jump boxes and zero standing privileges.

2. **Broaden MFA to all user constituencies:** SMS, voice, biometrics, phone-as-a-token, FIDO2 tokens, passwordless authentication and smart cards are supported by most MFA vendors. Although no single factor may suffice for all user constituencies, or provide a high enough level of assurance, by combining the various factors, nearly all users can be incorporated.

3. **Integrate more applications:** There will always be applications that lack integration with modern identity protocols. However, by prioritizing the selection of applications that support the protocols and implementing VPNs and ZTNA, more applications can be integrated with a centralized authentication service.

Although MFA can increase the reliability of user authentication, the user experience (UX) can be negatively impacted. By utilizing adaptive authentication strategies and passive authentication methods, users can be prompted often enough to maintain security and familiarity with the authentication factors, but not so often to be intrusive.

Organizations should:

- Centralize authentication to take advantage of analytics and adaptive policies.
- Evaluate each application's risk and level of effort to integrate MFA. However, note that the breadth of coverage of SSO often proves more beneficial.
- Select an MFA vendor that supports multiple authentication factors so that users are provided a factor that meets the organization's security needs.

Relevant research:

- Solution Comparison for Cloud MFA Services
- Avoid the Top 9 Pitfalls of Implementing MFA

Strengthen Adaptive Access Control as a Key Element of Zero-Trust Architecture

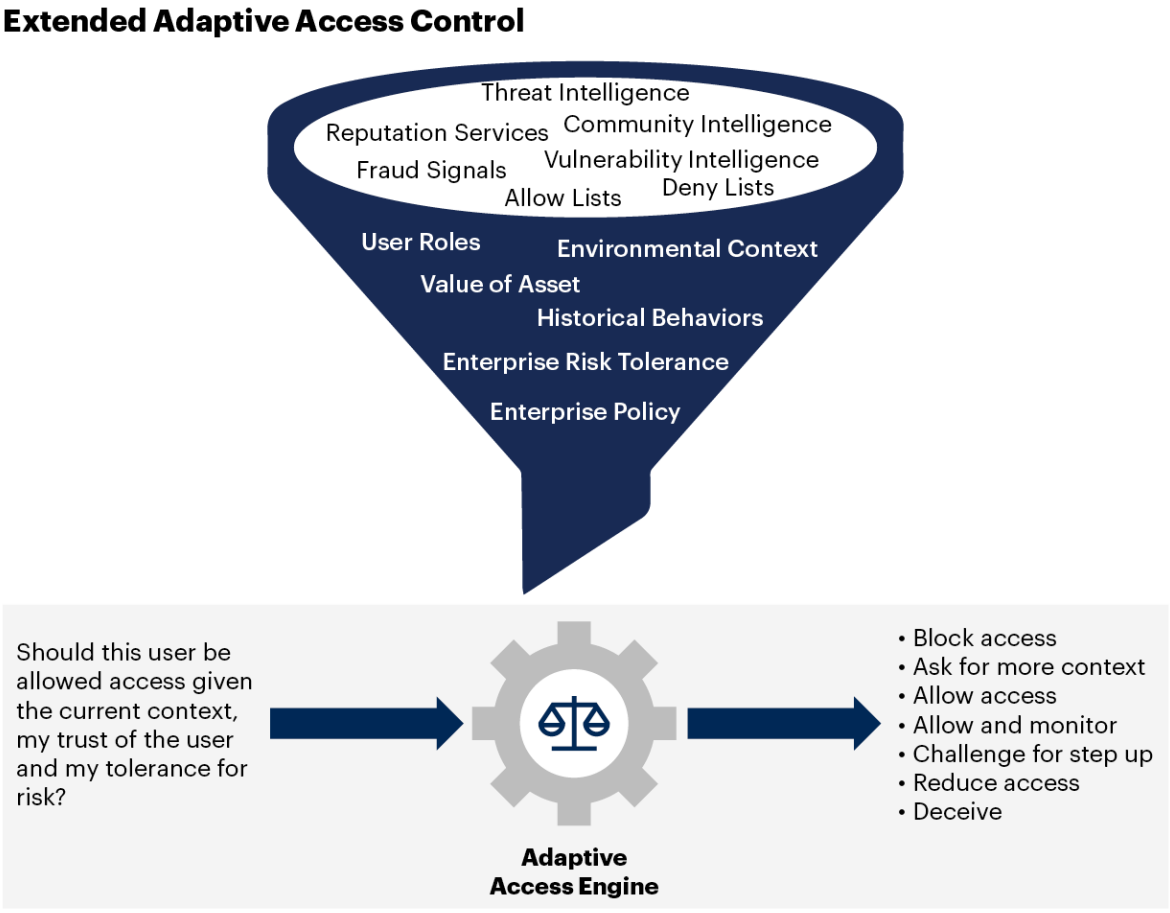
Gartner defines adaptive access control as context-aware access control that acts to balance trust against risk at the moment of access using some combination of trust elevation and other dynamic risk-mitigation techniques. Although adaptive access techniques predate recent acceptance of the zero-trust model as the desired end state for organizations, they espouse the same principles:

- **No implicit trust:** Porous enterprise network perimeters, the need to support access by remote workers and external partners, and applications' location independence mean that implicitly trusted zones (such as secure corporate networks) no longer exist.
- **Reliance on context:** Credentials and access tokens can be stolen, compromised or misused. Organizations must evaluate additional evidence ("context") to distinguish valid access requests.
- **Support for multiple types of risk signals and risk-mitigating actions:** Modern implementations may incorporate any risk signals related to users' devices, locations and networks, behavioral characteristics, historical data, and information from third-party tools. Similarly, access decisions are no longer binary (allow or deny), but can include "shades of gray" (see Figure 3).
- **Continuousness:** Risk assessment should not stop once a session token is granted. Users can walk away from their devices without logging out. Malware can steal browser cookies. A user's device may become noncompliant, or an indicator of compromise received from a third-party tool may increase the perceived risk associated with the user's account.

Adaptive access control can also act as a vehicle for improving user experience (UX). For example, organizations can perform (passive) risk assessment based on available information and prompt for MFA only when absolutely needed.

Access management (AM) tools and authentication tools that provide lightweight AM deliver the strongest adaptive access functionality, but cloud access request brokers (CASB), web application firewalls (WAF), and zero-trust network access (ZTNA) products can also support it. There are also security service edge (SSE) tools that combine SWG, CASB, ZTNA and sometimes WAF. These tools can also complement one another: An organization may choose AM for access to SaaS, and ZTNA for legacy or nonweb applications. A ZTNA tool should integrate with an AM tool to deliver step-up authentication. A reverse proxy-based CASB may pick up adaptive access where an AM tool left off because the latter doesn't remain in-flow after users complete authentication.

Figure 3. Extended Adaptive Access Control



Source: Gartner
753956_C

Gartner

Organizations should:

- Develop a comprehensive zero-trust strategy with the understanding that different use cases will require different approaches and tools.

- Implement a centralized access management solution to enable modern identity, including adaptive access, for SaaS and custom web applications.
- Select tools that assess risk and trust based on both affirmative and negative contextual signals.
- Prioritize tools that augment rule-based techniques with advanced analytic techniques.
- Evaluate advanced capabilities such as continuous adaptive access and integrations with additional sources of risk-related information.
- Evaluate other tools such as CASB, SSE and ZTNA for use cases that cannot be addressed by access management solutions alone.

Related research:

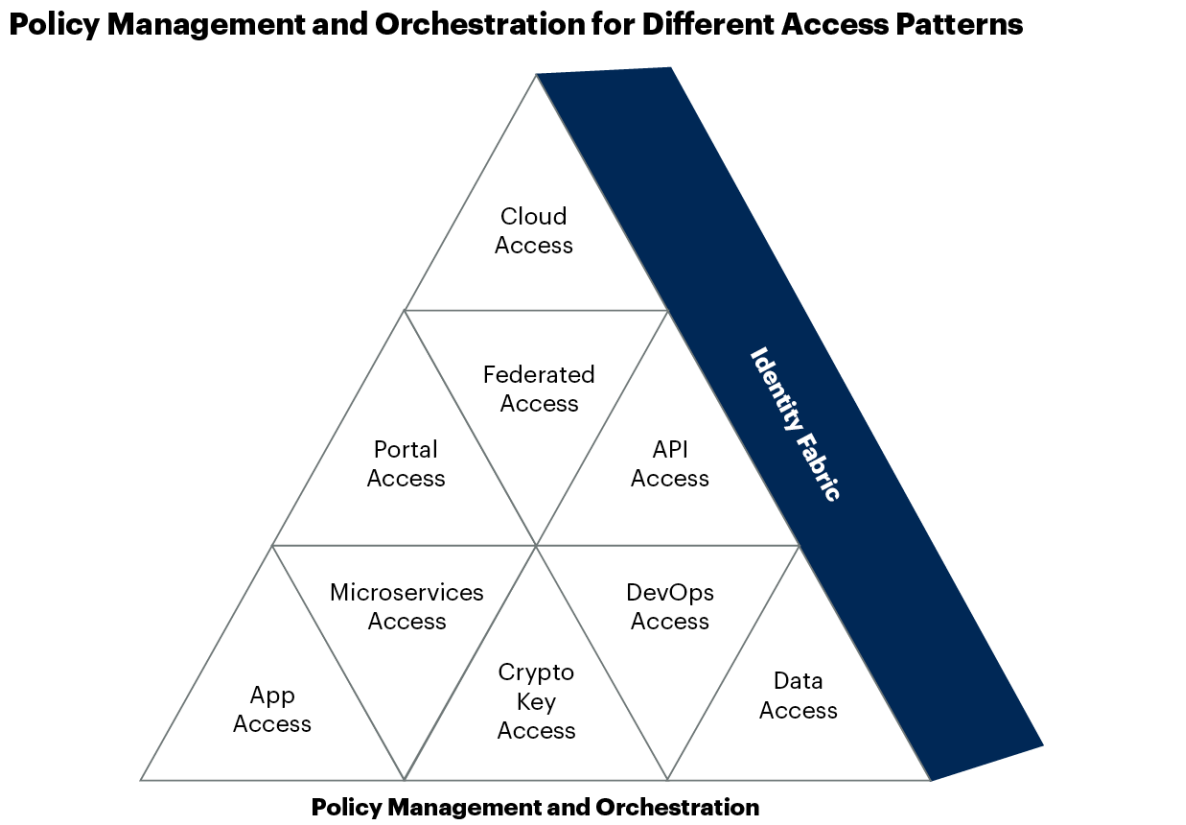
- Enhance Remote Access Security With Multifactor Authentication and Access Management
- Quick Answer: How Do Access Management and Zero Trust Network Access Tools Work Together?
- Solution Comparison for Cloud MFA Services
- Guidance for Microsoft Office 365 Identity Management

Evolve Authorization Model Toward an Identity Fabric Approach

An identity-centric approach to security (as required in cybersecurity mesh architecture) depends on managing identities and their relevant access (authorization) policies. That's why runtime authorization is evolving as the key enabler of the cybersecurity mesh architecture by providing policy management and orchestration capabilities. This includes support for both human and machine use cases with high-volume and high-velocity access to modern apps, computing units, data objects and underlying networks in different domains.

This is in contrast with current runtime authorization controls and related policy management practices, which are fragmented in most organizations. The current state is increasingly unsustainable and not only exposes organizations to a higher level of access risk and cost, but also hinders agility and digitalization initiatives. Runtime authorization use cases increasingly require more sophisticated policy-driven solutions. Particularly, emerging runtime authorization patterns — such as accessing cloud platforms, analytics, APIs, microservices (in a service mesh), DevOps pipelines and cryptographics keys — require a more consolidated approach to policy management. The Open Policy Agent (OPA) framework is becoming a viable candidate for evaluating and implementing lower-level access controls in cloud-native systems with potential for extension to legacy use cases on-premises (see Figure 4).

Figure 4. Policy Management and Orchestration for Different Access Patterns



Source: Gartner
753956_C

Gartner

Organizations should:

- Continue improving authorization architecture by externalizing authorization controls in their identity fabric. Authorization controls should be:
  - **Lean:** Optimize externalized authorization policy management and decisions to improve the quality and efficiency of policy deployment and enforcement.
  - **Adaptive:** Enable dynamic and flexible risk-based authorization controls by supplying contextualized policy decisions in admin-time and runtime for applicable domains.
  - **Intelligent:** Ensure trust and the integrity of authorization controls by providing or consuming policy insight and recommendations for roles and entitlements using machine learning capabilities.

Well-known authorization methodologies include role-based access control (RBAC), attribute-based access control (ABAC) and policy-based access control (PBAC). Each has its unique purpose and value. Technical professionals should implement a practical approach for designing modern authorization controls in each domain using a combination of these methodologies as needed.

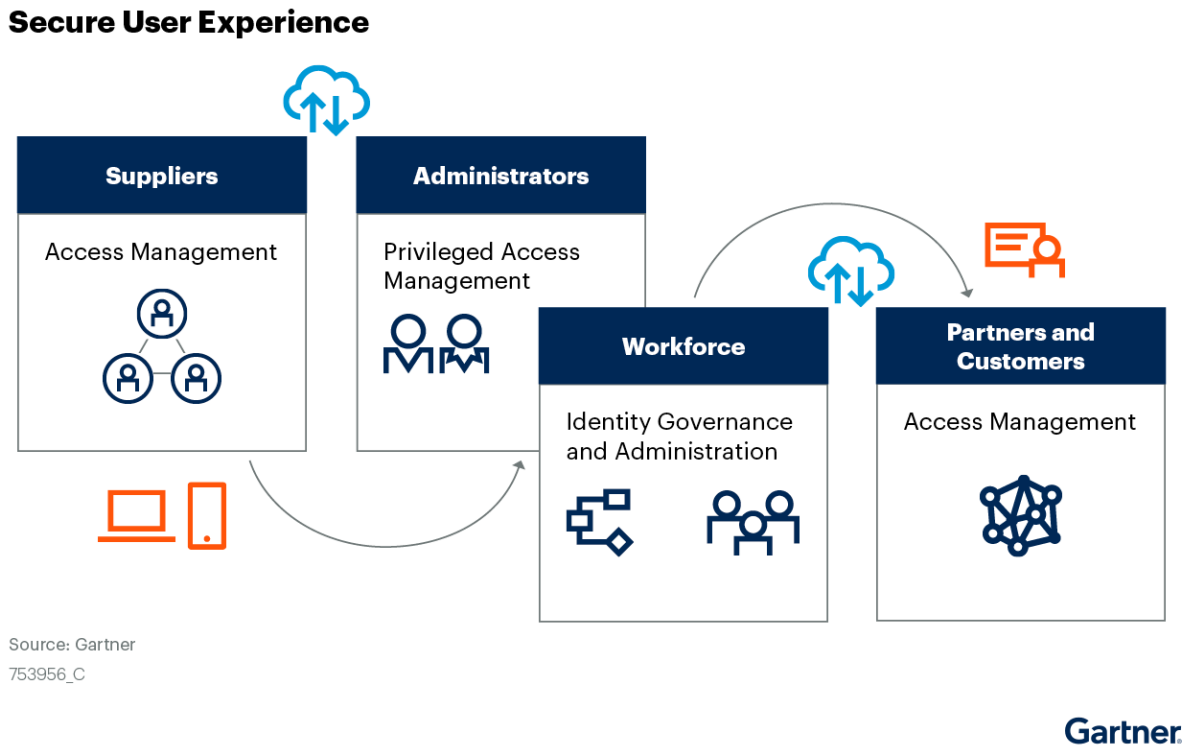
Related research:

- Guidance for Modernizing Authorization Architecture
- Architecting Modern Policy-Based Runtime Authorization

Improving User Experience for All Users Will Be Essential for Secure Digital Business

The increase in the number and importance of digital interactions means that users expect better digital user experiences. IAM teams must provide safer, more privacy-protecting access while improving digital IAM user experience (UX). Providing a great UX is of course important for all of your external users, including big business customers, brokers, distributors, citizens, consumers, patients, residents, small business customers, students and vendors. And it is increasingly important for all of your users, including end users, administrators and managers (see Figure 5).

Figure 5. Secure User Experience



Expectations of what constitutes a great UX continue to expand. Effective IAM deployments depend on well-maintained and well-monitored IAM configurations. Therefore, to keep IAM configurations current in an environment of rapid change, it is important to make it even easier to configure and administer IAM tools. Vendors are responding to these needs by streamlining user interfaces. Examples include creating even more extensible low-code and no-code workflow processing capabilities and supporting risk-based machine-learning-enabled automation of entitlement policy maintenance (hyperautomation).

Ease of use is especially important and nuanced for developers and privileged users. These users require a UX that is efficient enough that it encourages users to comply with access controls rather than find clever ways to work around controls. Gartner predicts that:

By 2024, organizations providing a total experience will outperform competitors by 25% in satisfaction metrics for both customer and employee experience.

— Source: Gartner (Top Strategic Technology Trends for 2021: Total Experience)

Total experience is a strategy that creates superior shared experiences by interlinking the customer experience, employee experience, multiexperience and user experience disciplines. It improves experiences at the intersection of multiple constituents to achieve a transformational business outcome.

For 2022, most organizations should reassess the experience for each of their external and internal user constituencies — both end-user and administrative. For example, they should review the user journeys with an eye to identifying gaps and areas, such as user registration, address change and authentication, that need further extension or enhancement. For organizations that have already made significant investments in IAM processes, this may involve further refining the user experience by eliminating additional IAM UX friction or extending the range of interactions supported digitally.

Pay special attention to infrequent processes that may not have been optimized in previous efforts. Less-mature organizations may need to replace or add access management infrastructure to their identity fabric to achieve the required UX, flexibility and security. This is especially true in the area of authentication. For example, the continued pace of technical change in the areas of cybersecurity threat and fraud detection makes the challenge of external user access too complex for one vendor to provide all of the needed capabilities for all organizations. Gartner continues to recommend a layered approach.

A great UX requires resiliency. As more of an organization's activities are conducted digitally, the organization becomes more dependent on digital access. IAM must be ubiquitous and reliable. Revisit your plans for high availability/clustering/redundancy. IAM should degrade gracefully. For instance, it should slow down, rather than crash, under periods of high volume. Ideally, an identity fabric flexes rather than tears, or experiences only small, localized tears that can be fixed quickly rather than experiencing large destabilizing rips.

Due to ongoing digital transformation, IAM deployments must not only be resilient, secure and easy to use, they also must enable a broader more comprehensive range of digital activities. Therefore, external IAM deployments must integrate with more “back-office” systems. This is putting additional pressure on integrating legacy IT into modern SSO deployments. One example of this is enabling a consumer to locate a house for sale, do a virtual walk-through, apply for a loan, and digitally close on the sale of the house (where permitted by law). Note that some digital identity verification tools can more accurately detect forged IDs than a typical employee can.

Planning Considerations

Create a Cohesive Strategy for All External Users

The bar continues to rise on what constitutes a great total user experience. All users, but especially those that are paying you, expect to be able to perform all of their desired tasks remotely and securely without excessive friction. This includes consumers as well as business customers and partners. The line between contractors and partners can be blurry. Gartner is seeing more organizations reevaluate the IAM that supports their distributor, broker, dealer and agent relationships to reduce administrative overhead and improve safety and privacy.

Organizations should:

- **Align your external user enablement with overall organizational goals:** As organizations broaden and deepen their digital capabilities, B2B and B2C, IAM priorities must become much more aligned with business rather than just IT priorities.
- **Strengthen IAM team relationships with other functional areas of the organization including legal, security, sales, marketing, data and development:** The breadth of IAM impact continues to expand. Therefore, it is important to maintain ongoing dialogues with all the functions that drive IAM requirements. Proactively prepare for more CISO responsibility for customer IAM.
- **Focus on foundational competencies:** These include the ability to deliver an omnichannel experience, and on unifying customer identity and profiles if you have not already done so

- **Review user experience process flows (i.e., workflows, paths or journeys) for each type of user constituency:** This includes revisiting processes that are performed less frequently and may not yet be fully optimized. Identify situations with excessive friction or gaps in the functionality provided, such as a digital signature process that is missing or awkward, or has security gaps, especially for users without or unwilling to use smartphones.
- **Prioritize enhancing B2B IAM:** This will allow you to better meet the functional, security and privacy needs of your business relationships.
- **Evaluate whether your current access management (AM) platform supports your needs going forward:** For many organizations, replacing/consolidating aging customer AM solutions is now a higher priority. As access management systems become more intelligent and interconnected, the penalty for not consolidating unnecessary duplicate systems is rising. Note that, for organizations operating under multiple data residency laws, multiple instances may be required, and many organizations choose to use separate SSO solutions for workforce and external users.
- **Strengthen user authentication using layered approaches that leverage several factors tailored to each of your user constituencies (one size still does not fit all).**
- **Assess whether the organization needs to add or replace its user validation, identity proofing and/or fraud detection tools:** Plan to integrate with consent and privacy management or digital experience platform tools as needed.
- **Relentlessly search for remaining weak links in your external user authentication chain:** Look for things like lax authentication of help desk callers or people reenrolling a second authentication factor.
- **Periodically review the availability of new bring your own identity (BYOI) identity-proofed identities for your external user demographics:** Although these are still not available in all jurisdictions, their adoption has grown significantly in the past year in some locations (for example, Canada and Belgium). Where available, use of these identities can significantly reduce friction.

Related research:

- Three Key Trends in B2B Customer/Partner Identity and Access Management

Apply a Zero-Trust Approach to Your Digital Supply Chain

The growing landscape of digital business ecosystems is built on rapidly expanding B2B relationships that require both human and machine access to many interconnected platforms. This network of cross-domain dependencies has formed digital supply chains that are becoming increasingly complex from an access governance perspective. Flat network architectures and failure to use least-privilege best practices enable attackers to move laterally against the operating environment, putting the enterprise and broader ecosystem at greater risk. The importance of protecting digital supply chains has become more clear recently in light of SolarWinds and ransomware attacks. Gartner predicts that, by 2025, 45% of large enterprises will have experienced attacks on their software supply chains — a three-fold increase from 2021. The security of a digital supply chain is only as good as the most vulnerable partner in the chain. Sharing sensitive information with partners within an ecosystem should require establishing a set of key controls for all participating parties, including the originating organization itself.

The IAM team should:

- **Enhance purpose-built delegated IGA for partners:** This will provide end-to-end security and privacy protection of customer data and other digital ecosystem resources.
- **Implement robust remote privileged access management together with MFA:** Do this for inbound and outbound system access to protect against vulnerabilities in the digital supply chain. Vulnerabilities in this context are related to vendors' support and developers' staff using privileged credentials to access systems remotely to maintain or enhance systems. Vendor identity management and privileged access management (PAM) session management are key controls to enforce the least-privilege principle and monitor remote privileged sessions.
- **Harden the software delivery and integration pipelines access mechanism:** Do so by adopting machine identity management disciplines, configuring security controls in DevOps tools such as securing secrets, and signing code and container images. Follow the principle of least privilege. It is often tempting to overentitle a service account because it's easier than finding the exact privileges that a particular script or application needs. Vendors often require that service accounts used by their tools and applications belong to the domain administrators or other privileged groups. Organizations should review such requirements and grant the privileges only when absolutely needed.

- **Secure the operating environment for software engineers/developers:** Do this by governing access to resources using principles of least privilege such as limiting admin privileges in time and scope and using a “principle of zero-trust” security model.

Related research:

- Evaluation Criteria for Privileged Access Management
- Managing Machine Identities, Secrets, Keys and Certificates
- How Software Engineering Leaders Can Mitigate Software Supply Chain Security Risks

Empower Your Privileged Users Without Sacrificing Security

Privileged access management is a cyberdefense issue that goes beyond addressing typical compliance requirements. Privileged accounts are of interest to perpetrators because they can bypass security controls that apply to regular users. PAM controls are even more important now because more administrative tasks and vendor support must be performed remotely. Also, many organizations are struggling to balance security and user experience, especially for administrators and developers. This includes operationalizing PAM controls in support of new DevSecOps, robotic process automation and delegating privileged access for third parties.

Privileged task automation, or scripting/automation of defined privileged actions, enables security without causing privileged users inconvenience. Automation includes increasing reliability and security by removing the human element. This increases efficiency by enabling privileged tasks to be run by more administrators (with less experience) or by software agents, such as RPA. It also reduces the burden of auditing privileged activities by decreasing activities performed manually by privileged users. Some of this automation translates to real business value in terms of increased efficiency and helping the business reach strategic objectives.

Privileged task automation capability provides functions and features for automating multistep, repetitive tasks related to privileged operations that are orchestrated and/or executed over a range of systems. It uses extensible libraries of preconfigured privileged operations for common IT systems and devices. The objective is to orchestrate back and forth between different activities and ask for more information as needed while putting in guardrails by checking input against policies and settings. This is like robotic process automation for IT operation processes that require privileged access or cloud infrastructure entitlement management (CIEM) controls. Examples are delegating tasks to help desk engineers, starting/stopping cloud instances or virtual machines, or automating DevOps provisioning of different computing environments.

IAM technical professionals should:

- **Manage identities of remote privileged users and implement zero-trust access:** Create an identity for remote privileged users, as opposed to using an account that is shared by all remote users. This enables remote users to authenticate every time they intend to perform administrative tasks or privileged operations and then use a shared account which is controlled by a PAM tool. It is a good practice to establish a formal system of record for third-party support staff in a separate user directory or as a distinct domain in the identity governance and administration system. Also, IAM teams should remove any remote user persistent privileges in the PAM tool or any of the target systems. Except in limited cases such as emergency accounts, these users should be configured with the least privileges. Any privileged access should be requested and approved by system owners (e.g.,via IT service management [ITSM] or IGA processes), and just-in-time access should be established through a PAM tool. Remote users should use higher-trust authentication (e.g., MFA) to connect to the PAM tool.
- **Automate privileged tasks:** For example, the PAM solution should be able to spin up a container for each relevant IT operation process. It must also provide the container with a one-time key and the necessary data to perform the required tasks, such as the identities and devices involved. The script or code within the secure container should only ask for required keys and credentials from the PAM or pure-play secrets manager solutions. This process usually requires the container (one-time) key and data verification before requesting the actual identity's keys/credentials from the PAM tool. The goal is to reduce the complexity and errors in privileged operations and achieve higher efficiency.

- **Automate cloud infrastructure entitlement management:** CIEM tools help enterprises manage cloud access risks via administration-time controls for the governance of entitlements in hybrid and multicloud environments (IaaS). They use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges, and dormant and unnecessary permissions. CIEM ideally provides enforcement and remediation of least privilege approaches. Privileged entitlements define access to cloud resources, service access privileges and cloud management permissions. Most CIEM tools provide integrations with Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure.

Related research:

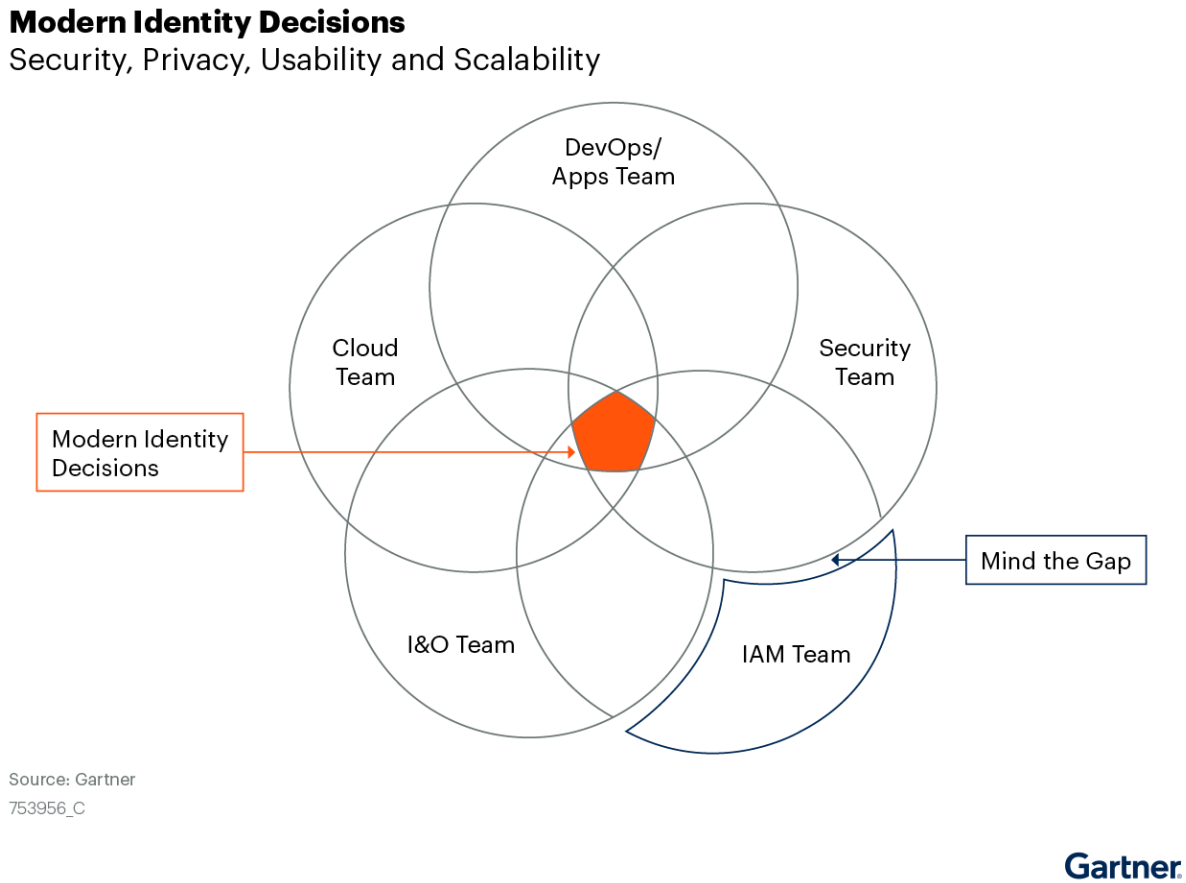
- Guidance for Privileged Access Management
- Managing Privileged Access in Cloud Infrastructure

Keys, Secrets, Certificates and Machines Will Require More Attention

The surge of the number of machines, their deployment and use in hybrid and multicloud environments, and new deployment practices are forcing organizations to reframe their IAM strategies. Machine identities are different from human identities and classified into two subgroups, one for devices and another for workloads. Devices include physical machines such as mobile phones, desktop computers, Internet of Things (IoT) and operational technology (OT) devices. Examples of workloads are containers, VMs, applications and services. A clear and refined definition of machines helps set expectations on what's included, and not included, in a phased IAM strategy. Right now, machine identity management tooling decisions such as picking a best-of-breed or an all-in-one strategy often don't receive broad enough attention in organizations. Different business units and teams have different definitions, expectations and tooling preferences. This is exacerbated by hybrid and multicloud environments.

Because the IAM team is not always involved in these modern identity decisions, new organizational structures have to be put in place. The identity fabric comprises multiple types of specialized tools such as cloud and on-premises deployed secrets managers, PAM tools, key management systems, SSH key management tools, PKI, and certificate management tools. Understanding their overlap, integrations and convergence is crucial. Organizations should forge new internal cross-function alliances, depicted in Figure 6, often in the shape of virtual teams, that are tasked with establishing ownership and strategies for machines.

Figure 6. Modern Identity Decisions



Organizations should establish a cross-team strategy that sets expectations on what can be controlled, determines required skills to bridge organizational gaps and introduces the new tooling.

Planning Considerations

Raise the Bar on Key and Secrets Management

Developers move fast. They need secrets, keys and certificates, and they often deploy open-source tooling to manage them. Cloud teams promote native IaaS tools, in contrast with the IAM team, which promotes its existing tooling. Encryption keys, secrets, certificates, and the life cycle management of identifiers and the directories where machines are stored all require different tooling. There is no “single-pane of glass” across them all. This leaves organizations’ usability, security, compliance and single source of truth requirements unmet.

Organizations must raise the bar on how secrets, keys and certificates are managed. It's time to establish strategies or reinvigorate existing strategies that have failed since they were based on isolated islands of requirements and unrealistic expectations.

Organizations should:

- **Establish a fusion team:** This is a cross-functional team that gathers requirements, provides leadership, defines ownership, lays out guidance and sets reasonable expectations. Don't do this informally. Assign an official organizational team name such as the machine identity platform team or the crypto center of excellence, or roll it up under the enterprise architect board — whatever sticks for your organizations. Then empower that cross-functional team.
- **Determine the machine identities you are using:** Categorize them into two groups: devices and workloads. Devices are your mobile devices, IoT/operational technology (OT) devices and desktop computers that typically have mature tooling in place to manage their identities. Workloads are more challenging and require the introduction of new tooling. This makes it easier to lay out a phased approach and solve the organization's urgent needs.
- **Refine the key and secrets management segment of your identity fabric:** The integrations between the different modules are slowly crystallizing. For example, it's possible to integrate an existing PKI in a secrets management tool. This is a fundamental shift in thinking for how organizations pick and use security tools. Today, different business units often own, operate and promote different tools. Instead, they should start moving along the maturity ladder and thinking of the identity fabric as a co-owned platform. They should evaluate capabilities based on use cases instead of tools. A best-of-breed strategy is still a relevant and often a required strategy, but understanding where any tool sits in the identity fabric ensures better integrations to solve use-cases that span different tools. For example, applications need secrets, keys and certificates to be able to operate. One of them isn't enough. This design thinking is not only true for machine identities but for all modern identity decisions.
- **Evaluate new tools to add to your identity fabric in light of the ongoing convergence between tools, and assess the depth of support each tool provides:** Take a use-case approach to your best-of-breed versus all-in-one solution discussions. The definitions and use cases help define strategies as they rule out certain tools. Use requirements for latency, the need for centralized governance, the reach of each tool across network boundaries, organizational gaps and discovery support as foundational drivers for tooling decisions.

- **Establish a multitooling strategy for secrets management:** IAM teams often have to integrate with tools picked by other teams. Find ways, organizational as well as technical, to deal with that. Stop the bleeding by providing guidance. Also make secrets management configuration part of an app migration play book. Gartner has also observed a growing list of clients who are now forced to build their own synchronization scripts to bridge tools used by developers, IAM teams and cloud infrastructure. Instead, ask vendors for a single pane of glass and standardized provisioning protocols now, not only for your users, but also for your machines. But don't expect a grandiose enterprise solution that addresses everything just yet.

Related research:

- Managing Machine Identities, Secrets, Keys and Certificates
- Architecting an Agile and Modern Identity Infrastructure

Incorporate IAM Best Practice for Agents and Bots

Adoption of robotic process automation (RPA) is increasing rapidly. Software robots — agents — now operate in many technology environments as digital laborers that either impersonate humans or independently automate manual tasks. With their own characteristics, software robots represent a new type of digital worker entity that introduces new identity requirements. Software robots deployed by RPA tools can expose organizations to substantial security and compliance risk if the access controls on the robots are not aligned with the access controls required by the systems the robots touch. Organizations must manage software robot identities and govern their access by applying required IAM best practices.

Organizations should:

- **Extend the identity fabric's controls and capabilities to include software robots as a distinct identity type, accounting for their unique characteristics and requirements:** Define best practices and guiding principles for how to integrate RPA tools into the identity fabric.
- **Treat RPA's software robots as another workload that needs a machine identity:** In the preferably rare cases when business requirements force the RPA to impersonate a human, leverage the machine identity to check out a human identity from a credential management tool such as a PAM tool or a secrets manager tool.

- **Credential management tools must enable digital workers or software robots to securely retrieve credentials needed to perform their functions:** Credential management tools should also rotate those credentials used in RPA to ensure compliance with corporate policies and industry guidelines.
- **Discover and register software robots with a unique identity in an authoritative source to manage their life cycle, credentials and key profile attributes:** Where software robots impersonate people or use other shared accounts, employ a secrets management tool.
- **Leverage the cross-functional platform team to ensure that software robots are held accountable for their actions via their human supervisors and in compliance with corporate access control policies and business rules such as segregation of duties.**
- **Govern software robot development, deployment and access to resources by ensuring proper ownership and accountability:** Update applicable policies and software development life cycle (SDLC) processes, and use roles to carefully assign entitlements that follow the principle of least privilege. Lastly, use analytics to monitor software robot activities.

Related research:

- RPA and Managing Software Robot Identities

New Applications and APIs Will Need to Leverage the Latest IAM Development Guidelines

In today's distributed environments, where there is an imperative to evolve to and maintain a zero-trust architecture, good IAM hygiene is increasingly important. Evolving from a traditional architecture to a zero-trust architecture is a journey that can take a significant amount of time, especially for organizations with many legacy systems. Implementing a zero-trust architecture has two components. The first is to clean up any existing technical debt by connecting existing digital assets into an access management system (as part of an identity fabric) that authenticates all users and authorizes access to each application/service. The second component is ensuring that all access to new digital assets is authenticated and authorized. This second part is of great tactical importance. If an organization allows new applications to be added outside of a zero-trust architecture, then there will be no end to its technical debt. It is crucial that organizations "stop the bleeding."

Identity teams need to coordinate with other parts of the organization to provide guidance to ensure that new applications from all sources are securely developed, sourced and onboarded. This should be handled in a way that is beneficial to all concerned. For example, people licensing new SaaS apps who coordinate with IAM teams are rewarded with single sign-on to their applications. Zero-trust initiatives don't just apply to applications that were previously accessed via a traditional VPN. These initiatives also increase the importance of organizations addressing their "shadow IT" challenge. Managing shadow IT is no longer just a licensing cost savings issue. It is also a supply chain security and internal security issue.

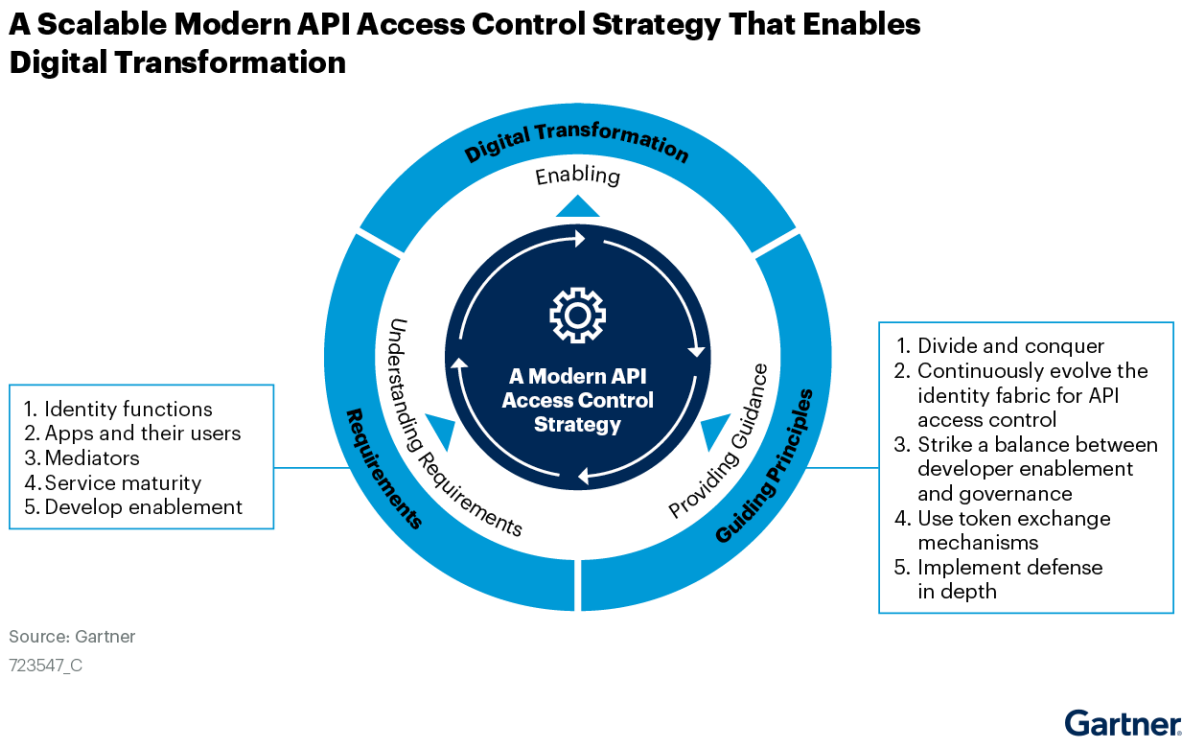
Planning Considerations

Define Best Practices for API Access Control

API access control — authentication and authorization of APIs — is a vital part of API security, together with API discovery and API threat protection. APIs are foundational for the digital transformation, and by 2019, 83% of HTTP traffic already was API requests and only 17% used traditional web applications. [4] Access management deployments must therefore expand their scope to include the protection of APIs. While doing so, it's critical to balance privacy, usability, security and scale to ensure a successful deployment. JSON Web Tokens (JWTs) have become the de facto standard for protecting modern APIs and can enable a zero-trust architecture. But that said, a single technical pattern for API access control is not sufficient for all of the types of APIs organizations must secure. To be successful, organizations must define a more inclusive API access control strategy and establish a cross-functional team that supports it.

A modern API access control strategy consists of detailed assessments of API use cases that define the requirements, a security assessment based on those requirements and the establishment of guiding principles. As depicted in Figure 7, there are five dimensions that must be used to define the requirements and five guiding principles that will stop the growth of technical debt. Applied correctly, they enable digital transformation.

Figure 7. A Scalable Modern API Access Control Strategy That Enables Digital Transformation



Organizations should:

- **Create a community of practice for APIs — an API platform team — that promotes API and API access control best practices:** Gather the right stakeholders and insights and set reasonable expectations for the strategies to be successful. This must be an ongoing effort. That team must involve practitioners such as developers, DevOps teams, cloud, security and IAM to help establish the right guardrails and API access control guidelines.
- **Divide and conquer a large and complex API access control problem into smaller solvable pieces:** Break down API access control into smaller and narrower use-case patterns that are easier to define, promote, enforce and ultimately govern. Only then is it possible to assess each API use case based on the above depicted dimensions.
- **Establish an identity fabric that supports API access control:** Tailor it for API use cases using full-featured authorization servers, externalized authorization managers and secrets managers that work in concert with mediators such as API gateways and, if necessary, other in-line proxies such as sidecars. This is in addition to API threat protection mechanisms such as web application and API protection (WAAP) tools that are also part of the cybersecurity mesh.

- **Improve developer experience by providing implementation guidance, proven libraries, and integration strategies for a hybrid and multicloud environment:** Ensure that the API platform team is represented in the developer community to ensure that the principles are implemented.

Related research:

- Architect a Modern API Access Control Strategy
- Building Authentication, Authorization and SSO Into API-Driven Apps

Integrate IAM Into Your Microservices/Container Stack

When microservices architecture and DevOps environments began, IAM tools struggled to meet the challenges of the ecosystem. Fortunately, the toolset has advanced dramatically, although it is still evolving.

Depending on an organization's level of maturity, potential actions for the coming year include:

- **Address any remaining legacy authentication issues:** Containers originally didn't have secure mechanisms for retrieving or storing credentials. Secrets management tools now have integration with container management platforms that allow the secrets manager to authenticate containers. This allows containers to "boot-strap" the required trust to retrieve the credentials needed.
- **Meet authorization demands of the applications:** API gateways are an excellent first line of defense in microservices architectures. Applying coarse-grained authorization and other security measures at the gateway reduces the threats services may encounter. Sidecar proxies capable of validating tokens and enforcing more granular policies can help to create a zero-trust architecture. This doesn't infer that the microservice will never be required to make authorization decisions because authorization is sometimes business logic that cannot be externalized.
- **Maintain a transaction's context without interfering with microservice components:** JWTs are the de facto method of passing authentication and authorization claims in a microservices architecture. However, simply passing the client access token from one service to the next, especially via a message queue, can omit important context and risks the token expiring. Create an environment where services can retrieve access tokens of their own and design a message payload that includes the important context of the original request.

The API platform team must:

- **Create guidelines of how IAM components can assist with application authentication and authorization:** An API gateway can expose internal APIs and enforce business rules and coarse-grained authorization. Sidecar proxies can enforce policies at microservices to create a zero-trust environment and externalize requirements from the services themselves. And an IdP can authenticate all components and mint the appropriate tokens.
- **Engage in a timely manner to meet evolving development team requirements:** The old model of a hardening phase at the end of a development cycle is no longer timely enough. Security needs must be architected into the solution at the same time as requirements.
- **Assist in defining strategies for least privilege and separation of duties that don't unduly compromise development functions:** Developers need environments where they can quickly change access policies to develop and test new functionality. Looser policies in development and local sandboxes should be created, whereas testing and production environments have more stringent policies.

Related research:

- Building Identity Into a Microservices Architecture
- Modern Identity and APIs: OpenID Connect, OAuth 2.0 and SCIM 2.0

Strengthen IAM Integration With SaaS

As IAM architecture becomes more sophisticated, IAM integration requirements have grown and evolved. Therefore, it is now even more important for organizations to choose applications and services developed with the latest security and modern identity standards, and plug them into their identity fabric. The move to zero-trust strategies is placing even more pressure on having good SaaS application/tool acquisition and onboarding processes.

IAM technical professionals should:

- **Improve coordination between your software acquisition teams (both central and divisional) and your IAM teams:** This will ensure alignment across the entire application life cycle.

- **Review the IAM criteria in your organization's SaaS acquisition criteria:** SaaS support for modern identity standards and best practices isn't just a single checkbox in your RFP. It's many, including SAML 2.0/OIDC 1.0, OAuth 2.0 and SCIM 2.0. Organizations must now make those IAM standards a requirement in application RFPs whenever the organization has leverage with the application provider. Many SaaS applications still don't support SCIM for life cycle management, and some still don't support a modern federation protocol. See How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria.

- **Rerationalize the approach to SSO:** Many organizations have multiple disjointed SSO tools serving workforce users.

The goal is to get to one integrated SSO system per user constituency that can mediate access to all of the generations of applications the organization uses.

Note that this doesn't necessarily mean using one access management tool. It may involve federating (chaining) multiple AM tools. This approach is also facilitated by deploying newer, more flexible IAM systems that enable access to multiple generations of applications in multiple locations.

- **Create and sustain a process in your IAM program to ensure that new applications and services are appropriately brought under standardized IAM control in a timely fashion:** This can include creating IAM program policies for which IdP should be used to integrate various types of new applications (e.g., workforce administrative applications, sensitive workforce operational technology and customer applications). This is particularly important when an organization is transitioning from one IdP vendor to another. Policies are also needed for how to handle provisioning of applications.

- **Be wary of creating unnecessary dependencies:** High availability is key for SSO systems. Therefore, many organizations with sensitive operational technology (including some manufacturers, utilities, hospitals, banks and government agencies) continue to run some on-premises IAM for critical infrastructure use cases, even if they also use IAM as SaaS for other business systems.

- **Avoid giving third-party tools excessive privileges:** This has been a common problem in a number of publicized breaches. Restrict privileged access to and by Tier 0 systems.

- **As organizations consume third-party APIs in SaaS products or within partner environments, it's important to establish mechanisms to discover them and ensure their security and health:** These are often business-critical APIs, but API access control strategies have to be adapted to the existing APIs more than the other way around. IGA, access management support for identity federation, certificate management tools, secrets management support for vaulting and adding access control to legacy credentials are all tools in play here to establish control over the access.
- **Revisit, and strengthen if necessary, your ongoing processes for discovering "shadow-IT" applications:** The risk of using SaaS, whose access is not controlled by IAM systems, is now a security issue, not just a user experience or license cost management issue.

Related research:

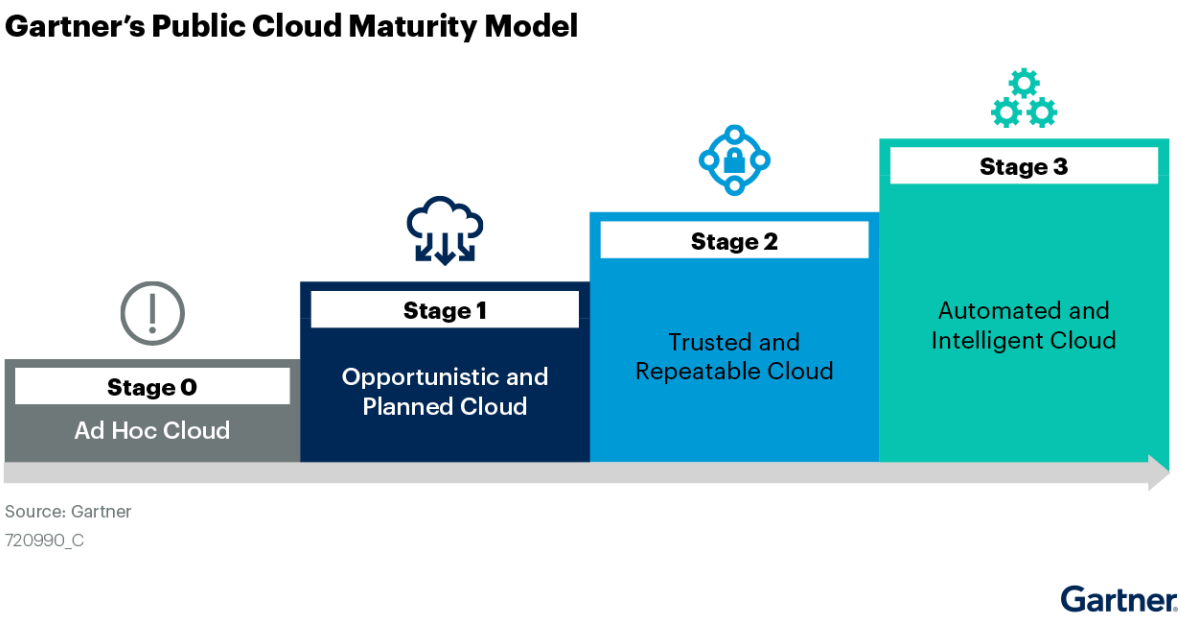
- How to Evaluate SaaS Providers and Solutions by Developing RFP Criteria
- Architecting an Agile and Modern Identity Infrastructure

Hybrid Cloud and Multicloud Will Drive Ongoing IAM Architecture Maintenance/Evolution

Computing is becoming even more decentralized. Not only are many organizations operating in hybrid (cloud and on-premises) mode, 92% of organizations are operating in a multicloud environment. [5] Secure, efficient decentralized computing requires a composable Identity fabric that enables any user or machine to access any authorized digital asset/service regardless of where the user or service is located. As organizations leverage more cloud resources, many are realizing they need to refactor their use of IAM to protect cloud assets. Organizations need to layer on more advanced analytics to protect these resources.

Organizations are overwhelmed. They have too many objects, IAM policies, processes and procedures to manage in too many places. As IAM requirements become more complex and distributed, an organization's IAM architecture must continue to evolve in order for it to securely and resiliently support the organization's ever-changing demands. As shown in Figure 8, in order to mature, organizations should deploy higher levels of intelligent automation using IAM tools that leverage machine learning.

Figure 8. Gartner's Public Cloud Maturity Model



This includes automation not only of simpler processes, but also advanced automation of the creation and management of IAM policies themselves as IAM systems evolve to be more autonomous (hyperautomation). IAM deployments also must mature to have fewer, more integrated dashboards so that IAM professionals have a "single pane of glass" with which to protect digital assets.

Now that many organizations and vendors have experience operating in hybrid multicloud environments, additional best practices for cloud maturity are emerging. These can include:

- Improving access control and governance of their growing cloud assets using advanced analytics for use cases such as risk-based access request and access certification, smart role modeling, and cloud infrastructure entitlement management (CIEM)
- Rerationalizing the use of IaaS-/PaaS-specific IAM features and increasing the use of multicloud IAM tools where possible
- Removing unnecessary duplication of user directories

In the excitement of moving more services and IAM tools to the cloud, it is important to continue to evolve and practice IAM best practices.

Related research:

- Advance Through Public Cloud Adoption Maturity

Planning Considerations

Reassess Risk Areas and Apply Compensating Controls: PAM, IGA, CIEM

As organizations move more digital assets to decentralized multicloud environments and operate in a hybrid IT environment, it is crucial that they add and mature automated compensating controls. Manual control processes are no longer adequate when an organization is developing/running many services in a multicloud environment and has an uncountable number of continuously changing service endpoints.

The runtime goal is for all users (both standard end users and privileged users) to be authenticated (using risk-based factors) and for access to every resource to be authorized via an access policy, regardless of the generation of technology. The admin-time goal is to always know who has access to what and to ensure that a least-privileged approach is used to grant entitlements. The processes to accomplish these two goals must be able to operate effectively independent of where the digital assets or users are located today.

Most organizations will need to evolve their IAM infrastructure to operate in a decentralized environment. This requires a gradual implementation of a cybersecurity mesh architecture, relying on:

- An identity fabric approach to break identity silos
- Policy management and orchestration to enhance metadata quality
- Federated learning to enhance machine learning models and identity analytics

In the context of cybersecurity mesh, we assume some form of IGA and PAM is in place. If not, deployment of IGA and PAM key capabilities should be prioritized. Specific priorities for 2022 will vary depending on an organization's existing level of cloud maturity.

IAM technical professionals should:

- **Prepare for implementing a consistent identity fabric** by establishing robust processes to discover, evaluate and manage the growing number of identities and entitlements across all environments. Risk is increasing as the ability to create accounts and entitlements outside formalized IT processes grows. PAM, IGA and CIEM tools have varying discovery features that leverage APIs. Examples include discovery of accounts in cloud infrastructure resources, DevOps tools and operational technology (OT) environments. Gartner recommends a continuous discovery approach through integration with SIEM solutions and the event-monitoring tools from cloud platforms. PAM tools also offer integration with configuration management database and asset tracking tools to discover new resources and associated accounts. This should also include tools to do a robust discovery process for keys, secrets and certificates. This will help the organization prepare for and respond to incidents and outages, as well as to aid in cryptoagility. Many attack chains include lateral movement enabled by compromised keys and keystores.

- **Implement a consistent identity analytics and intelligence capability** by deploying CIEM offerings to ensure that access to cloud infrastructure endpoints is actively controlled. Cloud accounts and entitlements are the fastest-growing area where access is often not based on least privilege and is subject to greater risk of misuse. Organizations restricting the use of native cloud endpoints to a single IaaS provider may be able to use a cloud-native tool. Organizations operating in a hybrid and multicloud IaaS environment should deploy a consolidated CIEM tool that supports multiple cloud providers. CIEM tools use analytics and machine learning (ML) to detect anomalies in account entitlements, such as dormant and excessive entitlements. CIEM solutions are also beginning to provide remediation and enforcement of least privilege approaches. Organizations should also evaluate existing tools, such as cloud security posture management and cloud-native application protection platforms, to determine their ability to meet their CIEM requirements.

- **Prioritize opportunities to implement policy management and orchestration capability** by integrating IGA, PAM and CIEM solutions for consistent management and governance of identities and entitlements across all environments. PAM and IGA integration is essential in securing and managing access to on-premises and cloud environments, where long-standing privileged accounts still exist. Establish common governance and administration processes and controls for privileged and nonprivileged identities across all environments, particularly cloud infrastructures.

- **Manage and accurately access risk in distributed environments by orchestrating IAM tools to operate as an integrated identity fabric.** Organizations gain synergies by extending IAM tools across multicloud, hybrid cloud and private cloud environments to perform critical governance functions such as access certifications and SOD checking, particularly for high-risk applications. Leverage IGA solutions to conduct risk analysis processes to facilitate triage and prioritization. Modern IGA solutions provide a more comprehensive risk evaluation to assess and prioritize account risk. Smaller organizations may find that they can leverage ITSM and newer lightweight IGA offerings. This may include extended integration with security technologies such as CASB and ZTNA. This ensures that adaptive access control and access monitoring can be properly implemented.

Related research:

- Managing Privileged Access in Cloud Infrastructure
- Guidance for Privileged Access Management
- Evaluation Criteria for Privileged Access Management

Rearchitect the Use of General and IaaS-/PaaS-Specific IAM in Multicloud Environments

Most organizations have already adopted multiple public cloud providers for different applications and use cases. Some organizations have done so as part of a strategy to access best-of-breed services. Others have done so unintentionally, through uncoordinated cloud adoption strategies or through mergers and acquisitions.

Organizations often choose a primary cloud provider where they run most of their workloads while selecting a secondary or tertiary (and so on) provider for specific unique functionality. Most organizations have at least one application that spans multiple clouds. And some look to multicloud computing for improved disaster recovery and business continuity management (“redundant multicloud”).

This variety of usage patterns and intrinsic complexity of individual public clouds makes unified IAM for multicloud computing challenging. Respondents in a recent Gartner survey identified increased security risks (46%) and operational complexity (45%) as top challenges related to working with multiple cloud providers. [6]

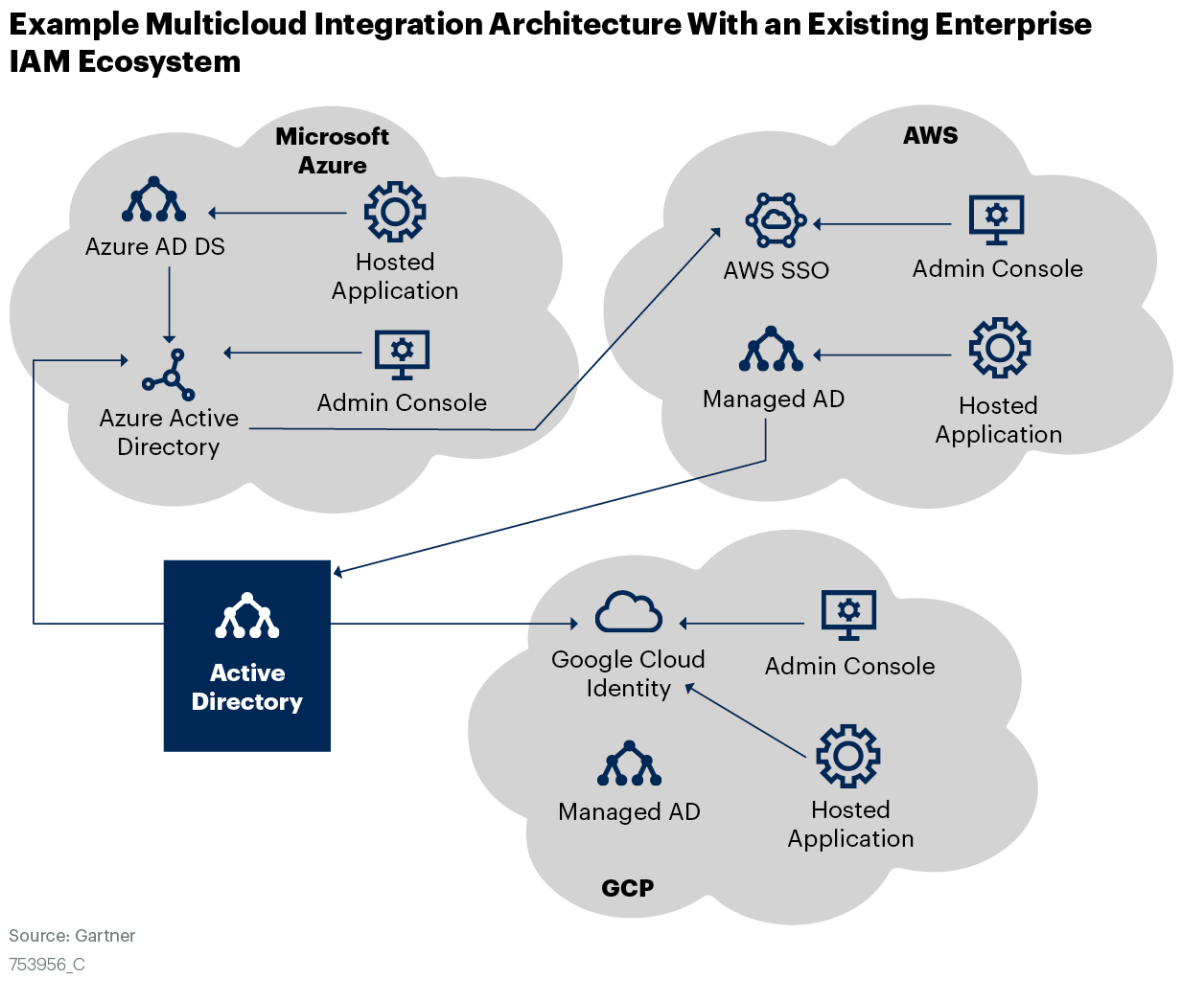
Best practices for overall IAM architecture in multicloud environments are still emerging. Creating a “single pane of glass” for managing all aspects of identity in such an environment is currently impractical. However, implementing a single overarching framework for multicloud IAM that centralizes some functions but leaves room for native tools is both achievable and desirable.

In the context of multicloud identity architecture, Gartner strongly recommends that organizations avoid identity silos in the cloud. With few exceptions (for instance, related to privileged access), users should be able to use a single identity to access cloud services. Figure 9 provides an example of integration between Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure and a typical organization’s enterprise Active Directory facilitating access to the respective platforms’ management consoles and API-based services.

Organizations should extend their centralized SaaS-delivered access management solution to simplify user access to multiple public cloud providers. Market-leading CIPS provide integrations with popular SaaS AM tools. Some CIPS (IBM, Microsoft and Oracle) also have their own strong offerings in that space. A standard AM tool can provide modern identity features (for example, multifactor authentication, adaptive access and API access controls) and unified UX for end users.

For legacy applications, organizations can adopt managed AD services, available from AWS, Google and Microsoft (see Figure 9). These vendors support AD forest trusts for integration with on-premises Active Directory, and some integrate their managed AD with their platform’s centralized identity service.

Figure 9. Example Multicloud Integration Architecture With an Existing Enterprise IAM Ecosystem



In addition to implementing a unified identity architecture, organizations should:

- Where possible, extend their existing IGA controls and processes to include resources hosted in public clouds. Leading IGA vendors support integration with popular CIPS.
- Evaluate third-party cloud security posture management (CSPM) and CIEM tools as needed to augment built-in functionality provided by CIPS vendors. CIEM is especially important for organizations operating in multicloud environments.

- Deploy a PAM solution to protect public cloud access by administrators. Privileged access encompasses management functions in cloud platforms as well as administrative access to workloads such as hosted virtual machines, applications and databases. Market-leading full-feature PAM vendors and some lightweight PAM vendors support these use cases.
- Carefully evaluate exceptions and special cases where a centralized tool may not deliver sufficient value and built-in functionality should be given priority. For example, it's not uncommon to manage coarse-grained entitlements centrally and leave fine-grained entitlements to individual services.
- Assess platform as a service (PaaS) IAM services from individual public clouds for their value beyond the cloud that offers them. For example, CIPS-provided secret vaults, certificate managers and API gateways can be deployed in cloud-to-cloud and ground-to-cloud scenarios.

Related research:

- Solution Comparison for the IAM Capabilities in Amazon Web Services, Google Cloud Platform and Microsoft Azure
- Innovation Insight for Multicloud Computing
- Implementing Governance for Public Cloud IaaS and PaaS
- 5 Things You Must Absolutely Get Right for Secure IaaS and PaaS

Evolve Your Enterprise Active Directory — and Keep It Secure

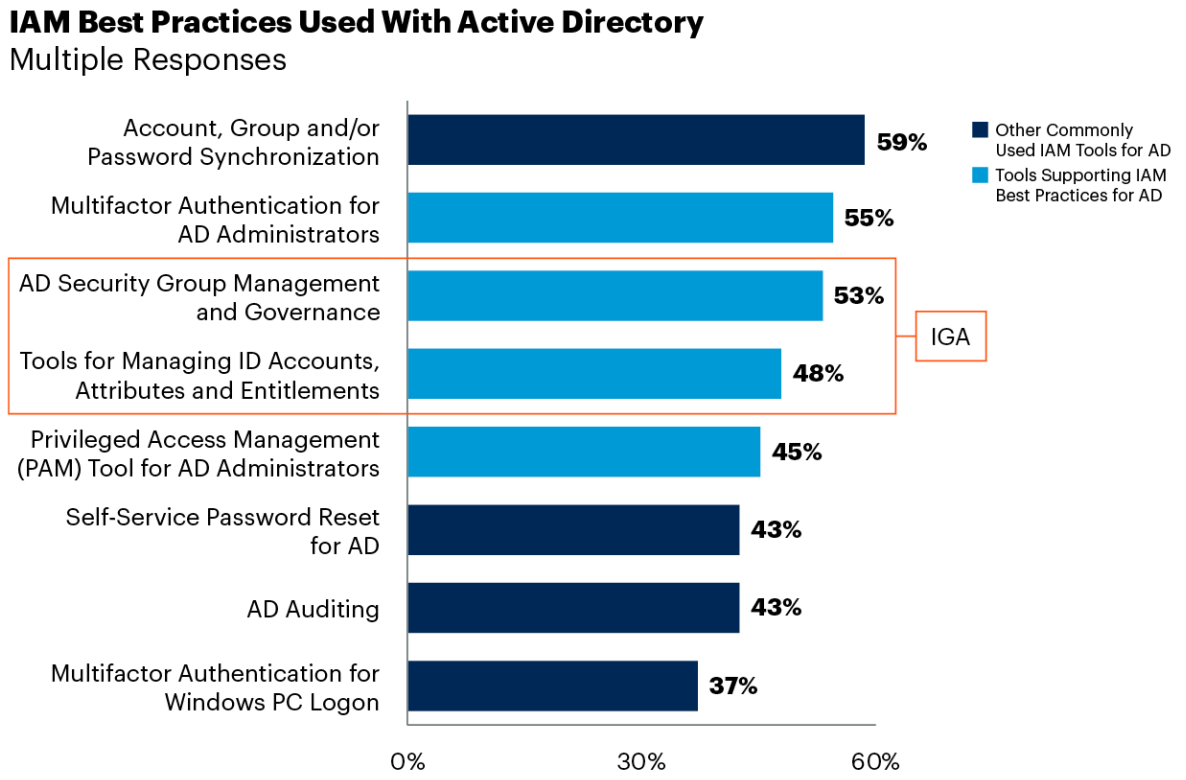
Gartner estimates that more than 90% of organizations worldwide use Active Directory as their enterprise directory. Created from 1999 to 2000 to address the needs of Windows-centric environments, it lacks support for many requirements driven by new enterprise imperatives — notably those related to cloud, remote and mobile access. It's a legacy technology. In a recent Gartner survey, 67% of respondents indicated that they are using a hybrid enterprise directory. This combines an on-premises Active Directory implementation with a SaaS-delivered access management service, a directory-as-a-service or a managed AD service provided by a CIPS platform. [7] Further, many organizations hybridize their AD in various ways, thereby chipping away some of the functionality historically delivered through AD to:

- Enable modern IAM for AD-protected applications using cloud services' SSO capabilities, proxies supporting nonstandard applications, and password vaulting and forwarding.
- Leverage cloud services for managing primary identities for some user constituencies, such as frontline workers, contractors and temporary workers.
- Use a cloud identity service as an identity hub for accessing all SaaS applications.
- Enable user authentication to non-Windows systems using cloud services instead of implementing an Active Directory bridge that connects macOS, UNIX and Linux systems to on-premises AD.
- Migrate applications still relying on Kerberos, LDAP and NTLM to the cloud and integrate them with customer- or platform-managed AD services.
- Offload management of Windows devices to a cloud-based service.

Although hybrid Active Directory is now the norm, few organizations made the leap and replaced AD with a cloud-based identity service. This means that AD remains an essential system for a vast majority of organizations. Active Directory's critical nature was brought into stark relief by the 2017 NotPetya attack against Maersk, the world's largest container shipping company. The malware encrypted the company's AD domain controllers and brought all its systems to a standstill for several days.

Like many centralized systems, AD concentrates risk. The more applications and services depend on it, the bigger the blast radius from interruptions and security incidents. Yet, according to the Gartner 2021 The Future of Active Directory Survey, [7] only about 50% of organizations implement core IAM best practices for their AD including, IGA tooling, privileged access management and MFA for administrators (see Figure 10).

Figure 10. IAM Best Practices Used With Active Directory



Smaller, recently formed organizations, those with simple IT needs and those who have already moved significant parts of their operations to the cloud should:

- Evaluate replacing Active Directory with a cloud-based identity service.

Organizations with a significant legacy application portfolio should:

- Continue to hybridize Active Directory to take advantage of emerging user and device management capabilities available in the cloud.
- Beef up IAM controls *for* and *in* Active Directory in line with published Gartner recommendations.

- Evaluate Active Directory threat detection and response tools to mitigate identity-based attacks against AD.

Related research:

- Implement IAM Best Practices for Your Active Directory
- Active Directory in Transition: Gartner Survey Results and Analysis
- Emerging Technologies and Trends Impact Radar: Security

Identity Governance and Administration Functions Will Evolve to Enable Decentralized Architecture

The accelerated pace of digitalization and cloud adoption continue to have a deep and lasting impact on IGA capabilities by expanding traditional requirements to include support for:

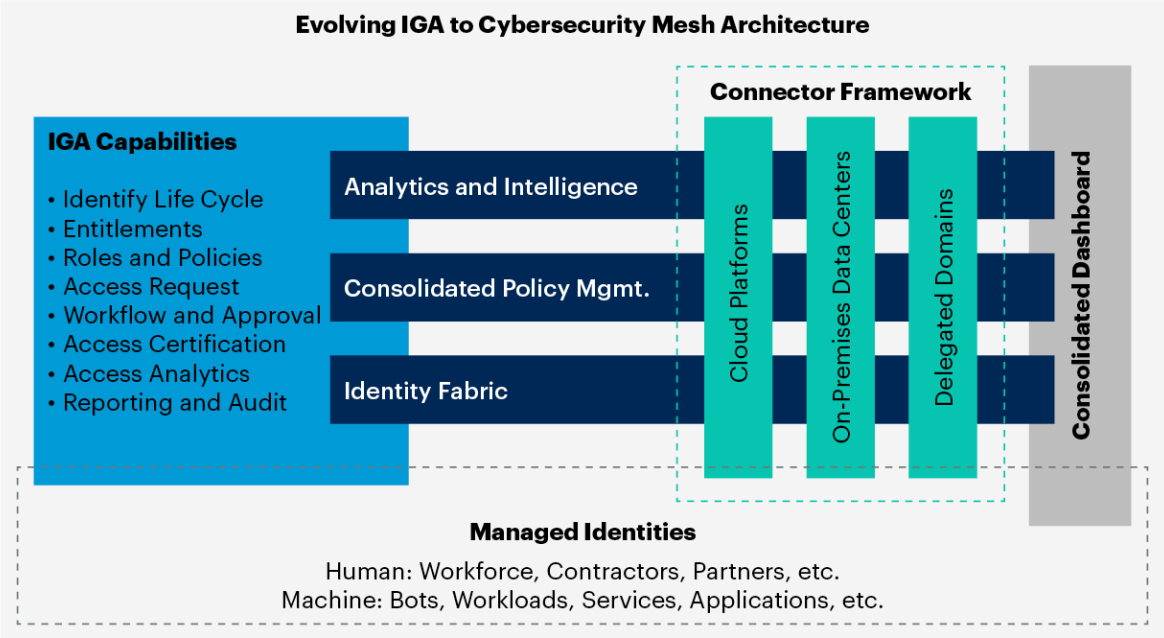
- Identities in hybrid IT environments including multiple data centers and cloud providers
- Identities in multiple cloud platforms including IaaS (e.g., AWS, Microsoft Azure, GCP, Oracle and IBM), PaaS (e.g., Kubernetes) and SaaS (e.g., Workday, SAP, ServiceNow, Snowflake and Salesforce) cloud platforms
- Inferring access pattern and policies as well as policy management and orchestration for more complex admin-time authorization use cases (across more granular resources in different platforms and environments)
- Seamless integration across business entities (B2B) and more complex relationships
- Flexible workforce and workplace including partners/contractors and gig staff working remotely
- Developer-centric automation processes such as DevSecOps pipelines
- Machine identities: Devices and workloads such as software robots and IoT devices, applications and services
- Higher pace of business activities and more autonomy for business units that require complex delegation of administrative tasks

- Alternate IGA approaches for small and midsize enterprises with less complexity and IT resources

These additional requirements drive the need for evolving IGA capabilities to align with a Cybersecurity Mesh Architecture (CSMA). This evolution involves establishing an identity fabric using a standards-based connector framework across multiple computing environments, better management and orchestration of access policies, and powerful analytics and intelligence to provide required visibility for digital automation scenarios. These capabilities, together with more versatile cybersecurity dashboards, enhance organizations' cyberdefense posture (see Figure 11).

Figure 11. Cybersecurity Mesh: Identity Governance and Administration

Cybersecurity Mesh: Identity Governance and Administration



Source: Gartner
753956_C

Gartner

Planning Considerations

Extend IGA for All Entities and Domains Via Identity Fabric and Policy Orchestration

The identity fabric approach is a game changer for IGA that forces organizations to rethink their IAM architecture. The new architecture is designed for distributed computing and enables more consistent access governance across the domains that the identity fabric protects, such as on-premises and various cloud providers. This approach allows centralized and decentralized IGA functions through identity orchestration solutions for multicloud and hybrid IT while maintaining an enterprisewide consolidated dashboard. For example, policy orchestration allows IAM teams to define policies in one place but translate and distribute them to each domain/platform as required. From the complexity perspective, the identity fabric and its related IGA functions are more elaborate for a large, regulated organization than for smaller organizations. For example, many small organizations may take a minimalist approach, preferring to leverage platform capabilities (e.g., Azure Active Directory and its IGA functions) or other tools they already have, such as ITSM IGA functions (e.g., ServiceNow function in conjunction with Clear Skye).

IAM teams should strive to extend IGA capabilities to govern access for all services across all identity fabric domains for all entities (i.e., human and machine entities). In order to achieve that, organizations should plan for the following changes:

- **Embrace standardized services, in place of proprietary connectors and non-standard integrations, to implement identity life cycle management (ILM):** These changes further emphasize the importance of migrating to modern IGA platforms that support ILM events across multiple domains using standards-based connectors, such as System for Cross-Domain Identity Management (SCIM) connectors. SCIM 2.0 standardizes user provisioning and managing identity data in cloud/hybrid applications and services and eliminates custom connectors. SCIM provisioning gateways (such as Acquera), which transform SCIM requests to another format, can be included as a key building block to implement an identity fabric. SCIM gateways convert SCIM requests into REST-based API calls, SOAP API calls, SQL commands, LDAP commands or SDK library calls to manage identities across hybrid IT infrastructure.

- **Implement synchronization of metadata, like entitlements and policies, to govern admin-time access controls across multiple domains:** As applications and services are distributed across multiple domains, governance gets more challenging. Organizations should plan on extending IGA capabilities for managing admin time access policies and distributing them across various domains. Because the metadata formats differ among different domains, an identity fabric should support conversion of the metadata to the relevant formats before it is distributed. Also, IAM teams should plan on integrating identity changes and workflows with IGA fulfillment engines so that access changes, across multiple domains, are automatically provisioned. Relying on manual tasks to complete the steps will involve collaboration with multiple domain owners, thus increasing the chances for human error, resulting in identity information getting out of sync.
- **Secure hybrid domains by integrating IGA with CIEM:** Organizations should plan on integrating IGA and CIEM tools to extend governance to multicloud and private cloud environments. Some vendors offering IGA now also have CIEM capabilities. The latest advancements with IGA tools provide capabilities to detect overentitlement with hybrid environments to mitigate risk. Smaller organizations may leverage niche providers that provide advanced analytics capabilities to recommend entitlement cleanup.

Relevant research:

- Managing Privileged Access in Cloud Infrastructure

Leverage Cloud Identity Analytics for Continuous Governance

Traditional IGA tools are dependent on metadata and constructs (e.g., policy, roles, entitlements and assets) that usually remain as static configuration in the face of an increasingly changing IT environment. Modern IGA capabilities should be more dynamic and adapt to user and application changes quickly. A key area is automated decision making to maintain least privilege access for identities. Organizations should plan on adding machine learning capabilities and other advanced analytics as a key step toward addressing these challenges.

Organizations have traditionally used identity analytics for limited use cases, such as role modeling or analyzing historical data to calculate risk scores. Continued innovations with advanced analytics that enable IGA to be more autonomous make it very compelling for organizations to add products and services that put analytics at the center of IGA. One example is using a machine-learning-enabled IGA system to automatically fulfill an access request if the risk of the request was low enough. The latest advancements in identity analytics can predict the expected behavior of an identity population and initiate a remediation action to address behavior anomalies, thus reducing overall risk for the organizations. Automated policy and role management is another area where machine learning plays a major role in automating updates to role models.

Core capabilities, such as identity life cycle management, entitlements management, access requests, workflows, access certification and auditing, are delivered in a consistent manner by many IGA vendors. Thus, identity analytics remains as a key differentiator among full-featured IGA vendors. Organizations that plan on migrating to new IGA platforms should plan to evaluate the latest advancements in analytics when comparing IGA vendors.

IAM technical professional should:

- **Extend IGA capabilities with identity analytics to achieve autonomous governance:** Organizations should plan on implementing autonomous governance by leveraging predictive and prescriptive analytics features from IGA vendors. Predictive governance leverages machine learning and analytics to recommend user actions. For example, predictive analytics can recommend to an end user the set of entitlements that they may request based on peer group analysis. Prescriptive analytics enhances that by automatically executing the recommended actions. For example, an access request that is identified to be low risk, based on the requested entitlement and the requestor's profile, can be automatically approved.

- **Leverage identity analytics to detect user access anomalies:** Before planning for advanced governance capabilities, such as autonomous governance, organizations should implement processes to address user access anomalies. High-risk issues, such as overentitlement and unused accounts, can be addressed with usage analytics and peer group analysis. Unused entitlements and accounts can be detected by checking actual usage logs, while overentitlement can be identified by comparing users with their peers. Please note that such cleanup activities should be performed using automated tooling on a continuous basis and not as a one-time activity.

- **Automate role modeling using advanced analytics:** IGA policy and role modeling has traditionally been planned around the earlier stages of IGA implementation. The resulting model gets outdated over time due to business and technical changes. Organizations should leverage the latest advancements with leading IGA vendors and niche vendors to dynamically update the role model and update the assignment rules. The latest advancements use machine learning algorithms to identify new candidate roles and optimize the existing role model. Organizations should plan on updating their IGA role model periodically to keep up with the changes. Gartner recommends using a collaborative role modeling process. Conduct workshops and involve business and technical stakeholders when the role model is first designed or when there are major business events, such as mergers and divestitures, or technical changes, such as migrating ERP systems to cloud.

Related research:

- Modern Approaches to Identity Governance and Administration Role Modeling
- Modernizing IAM Architecture With Machine Learning

Setting Priorities

Specific IAM priorities vary based on your current level of IAM maturity, industry and user constituencies. Most organizations do not have the staff or budget to follow every suggested planning consideration, especially at a time when many organizations are more cost sensitive. Organizations should use the following priority-setting framework when planning for the upcoming year:

- **Triage remaining high-exposure risk areas and basic access controls first:** Reassess the organization's biggest risks/opportunities associated with each of the pillars of IAM — AM, IGA and PAM — to identify must-do action items. For example, if your organization is not yet using some type of MFA for its various categories of end users or PAM for remote privileged administrators, then rolling these out is an imperative. If you have outgrown a manual IGA "system," smarter IGA offerings now include enough automating analytics to make them practical for more organizations. In some organizations, one or more point solutions, rather than a complete IGA solution, may be the best fit.

- **Multiply the impact of IAM by operating IAM as an ongoing integrated program (not just a series of unrelated projects) that manages overall IAM architecture as an enabling resource:** This has long been a best practice, but as IAM operations become more complex and IAM tools become more intelligent and share more data, it has become even more important to rationalize your overall IAM architecture. For many organizations, this will include evaluating whether the organizations' IAM tools are flexible enough to support the organization's transforming requirements. Gartner is observing higher levels of both tool replacement/consolidation initiatives and initiatives to better leverage existing tool licenses. Organizations should choose vendors that can interoperate because an identity fabric is part of an integrated cybersecurity mesh architecture. In today's decentralized environment, organizations should make changes that reduce unnecessary IAM silos and streamline IAM operations.

- **Take a more active approach to broadening IAM engagement with non-IAM stakeholders:** Now that IAM mediates access to almost all of an organization's interactions, it is even more important for IAM to deeply engage with other functions in the organization, especially revenue impacting and security teams. IAM teams need to move beyond superficial coordination to better understand the goals of their colleagues in other functions so that they can effectively engage in joint problem solving to address new opportunities and threats.

- **Focus on the needs of all end users and machines:** No matter where an organization is on the IAM technology maturity curve, it is always important to review priorities with all of the human and machine users in mind. The form of an IAM program and architecture must follow the needs of the organization and its users. In times of rapid change, one of the most leveraged actions is to focus on improving user experience for administrative users and to deploy more self-service and automated capabilities so that IAM administration is handled in a timely fashion.

Evidence

[1] When used to describe software technology, the term fabric refers to a flexible, fine-grained, mesh. It is not a reference to clothing. A fabric is something that is composed of parts, or the basic structure of a thing. It evolved from the Latin word fabricari, which means to make or build something.

[2] Avoid the Top 9 Pitfalls of Implementing MFA

[3] New Research: How Effective Is Basic Account Hygiene at Preventing Hijacking, Google.

[4] State of the Internet/Security: Retail Attacks and API Traffic, Akamai.

[5] Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report, McAfee Enterprise, page 13.

[6] Gartner's 2020 Cloud End User Buying Behavior study was conducted to understand how technology leaders approach buying, renewing and using cloud technology.

The research was conducted online from July through August 2020 among 850 respondents from midsize and larger ($100M+ in revenue) organizations in the U.S., Canada, U.K., Germany, Australia and India. Industries surveyed include energy, financial services, government, healthcare, insurance, manufacturing, retail and utilities. All organizations were required to currently have cloud deployed.

Respondents were involved, either as decision makers or decision advisors, in new purchases, contract renewals or contract reviews for one of the following cloud types in the past 3 years:

- Public cloud infrastructure (IaaS)
- Public cloud platform (PaaS)
- Public cloud software (SaaS)
- Private cloud infrastructure
- Hybrid cloud infrastructure
- Multicloud infrastructure

Respondents were also required to work in IT-focused roles, with a small subset of procurement respondents.

- The study was developed collaboratively by Gartner analysts and the Primary Research Team

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed

[7] The 2021 The Future of Active Directory Survey was conducted online from 13 April to 18 April 2021 with 119 participants. 57 were members from Gartner's IT & Business Leaders Research Circle — a Gartner-managed panel — and 62 were from an external sample.

Respondents were qualified based on their knowledge of current and planned usage, strategy or roadmap for identity and access management (IAM) and Active Directory, other enterprise directories, or cloud-based identity services.

Document Revision History

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

2016 Planning Guide for Identity and Access Management - 2 October 2015

Recommended by the Authors

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

Top Strategic Technology Trends for 2021: Cybersecurity Mesh

Top Strategic Technology Trends for 2021: Total Experience

Quick Answer: How Do Access Management and Zero Trust Network Access Tools Work Together?

Client Question Video: How Can We Architect Our IAM to Be More Adaptive?

Transform User Authentication With a CARTA Approach to Identity Corroboration

Market Guide for Identity Proofing and Affirmation