Hype Cycle for Identity and Access Management Technologies, 2021

Published 27 July 2021 - ID G00747578 - 88 min read

By Analyst(s): Tricia Phillips

Initiatives: Identity and Access Management and Fraud Detection

Security and risk management leaders can use this research to find technologies to combat complex identity-based attacks. Machine identity management and decentralized identity dominate the Peak of Inflated Expectations, while FIDO and SaaS-delivered IAM are already in the Trough of Disillusionment.

Additional Perspectives

- Summary Translation: Hype Cycle for Identity and Access Management Technologies, 2021
  (13 October 2021)

Analysis

What You Need to Know

This Hype Cycle for identity and access management (IAM) emphasizes the maturation of innovations that deliver security, risk management and business value for customer and workforce IAM. As organizations look forward to a postpandemic world, the lessons learned are fresh in the minds of security architects and operations teams. They are driving adoption of cloud-first solutions that can scale and support remote working, enable identity-first security for virtualized and legacy environments, and bring consistency and visibility to distributed identity systems, applications and users. Beyond security and operations, many organizations have had to roll out new customer-facing digital services, which have required IAM. This has driven interest in innovations like passwordless authentication and bring your own identity (BYOI), and highlighted some of the limitations of both customer identity and access management (CIAM) deployments.

This Hype Cycle provides decision-making support to IAM leaders who already have visions and roadmaps for their IAM programs, or who are in the process of redefining their roadmaps and priorities based on their organizations' security and business goals. This Hype Cycle will help IAM leaders determine which innovations (technologies and standards) can fulfill their visions and roadmaps, and which may not yet be sufficiently mature.

The Hype Cycle

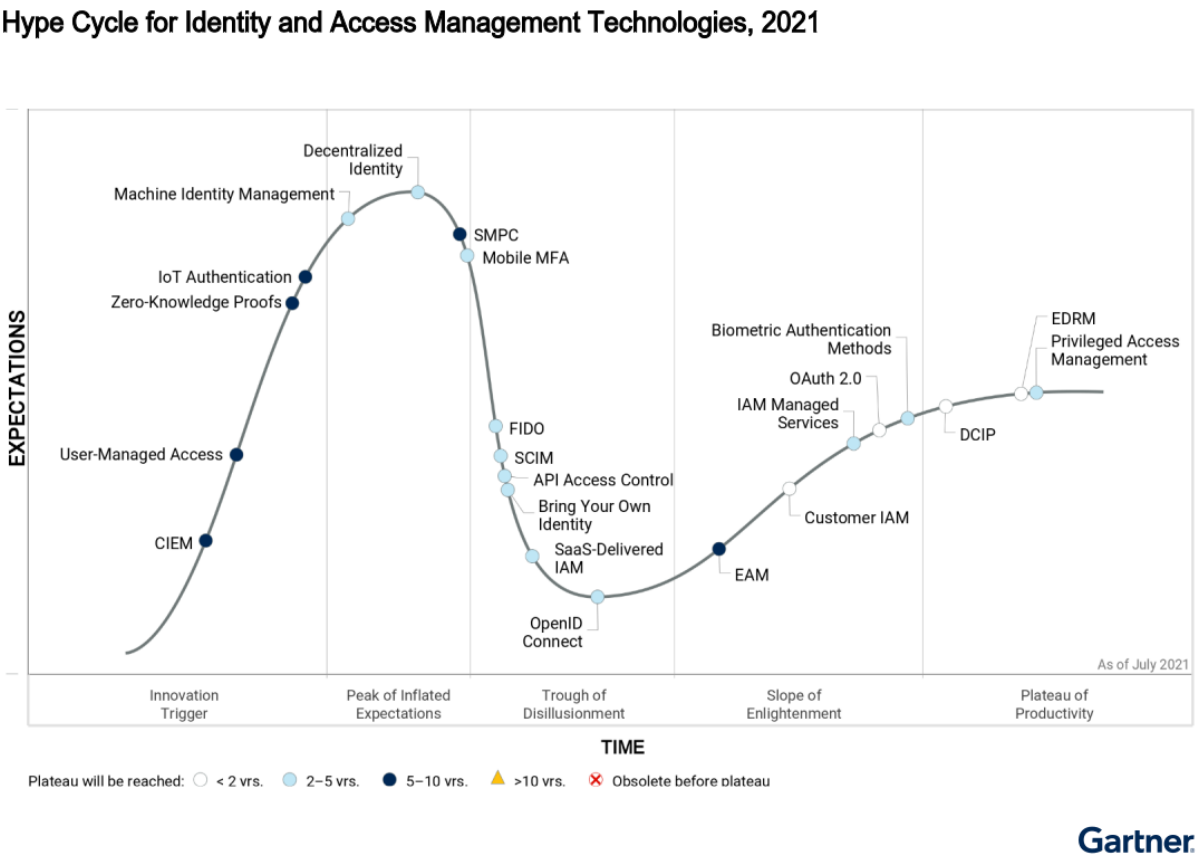
IAM is a security, risk management and business discipline. It encompasses practices, processes and technologies that manage the identities and entitlements of people, services and things, and the relationships between, and trust associated with, them. Effective IAM technologies equip IAM leaders and their teams to provide the right access for the right reasons. They thereby enable the right interactions at the right time — and with the right user experience (UX) — to help drive desired business outcomes and digital experience goals (see Success in the Digital Experience Economy Requires Connecting MX, UX, CX and EX).

The dramatic rise of remote working, combined with high-profile identity-based attacks, has resulted in an increase in deployments of multifactor authentication (MFA). While many of those deployments have used well-established MFA factors, there has also been increased focus on streamlining the UX (from anywhere) with strong, but lower-friction, user authentication and access management (AM). This has resulted in standards-based protocols like OpenID Connect (OIDC), Fast IDentity Online 2 (FIDO2) and System for Cross-Domain Identity Management (SCIM) leaping forward in adoption and appearing on more client roadmaps. These significant developments, reflected in the Hype Cycle, demonstrate that standards-focused AM tools continue to grow in importance, and support a consistent approach to diverse application architecture and user roles.

Decentralized identity and secure multiparty computation, though still at the Peak of Inflated Expectations, have moved forward. Their progress has been driven partly by the increased need for privacy preservation, as well as by the requirement for high-assurance digital identities. Secure, high-assurance, remote access to government services, banking services and other critical or high-risk interactions is now mandatory, and legacy strategies have proven insufficient, due to a lack of consumer control and the risk of fraud.

Privileged access management (PAM) adoption has moved further along the Plateau of Productivity. It is now a basic requirement, as many of the most damaging attacks of the past year have involved attacks on human and machine privileged accounts. Machine identity management has advanced to the Peak of Inflated Expectations.

Figure 1. Hype Cycle for Identity and Access Management Technologies, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for Identity and Access Management Technologies, 2021

The Priority Matrix

IAM innovations have a wide range of uses. They enable revenue-generating or cost-saving business process and UX improvements, protect against increasingly sophisticated account takeovers, facilitate secure, scalable access to critical IT resources, and support compliance and other security and risk management initiatives that increasingly need an identity-first approach.

Some technologies on this Hype Cycle, such as IAM managed services and document-centric identity proofing (DCIP), can map directly to business value through revenue enhancements or operational savings. Others, like Internet of Things (IoT) authentication and API access control have a value that is more aligned with protecting the business from security breaches than with revenue-driving activities.

The Priority Matrix reflects Gartner's view of the benefits and timeline to maturity for the entries in this Hype Cycle. It is important to interpret these benefits in light of your business priorities and the current state of your security initiatives. For example, some organizations could have detected and mitigated recent sophisticated identity-based attacks sooner if they had had a robust PAM tool in place and had made full use of it, or if DCIP had been available for account recovery scenarios (see Predicts 2021: Identity and Access Management and Fraud Detection). For other organizations, the value of implementing a low-friction biometric authentication method for customers could exceed the value of a PAM tool, due to the top-line revenue benefit, though both are categorized as being of high benefit in this Hype Cycle. Map these technologies to your own business and technology priorities to determine the right time and sequence for acquisition, integration and deployment.

Table 1: Priority Matrix for Identity and Access Management Technologies, 2021

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
	Less Than 2 Years	*2 - 5 Years*	*5 - 10 Years*	*More Than 10 Years*
Transformational		Bring Your Own Identity Decentralized Identity	SMPC	
High	Customer IAM DCIP EDRM OAuth 2.0	Biometric Authentication Methods FIDO IAM Managed Services Machine Identity Management Mobile MFA OpenID Connect Privileged Access Management SaaS-Delivered IAM	IoT Authentication	
Moderate		API Access Control SCIM	CIEM EAM Zero-Knowledge Proofs	
Low			User-Managed Access	

Source: Gartner (July 2021)

Off the Hype Cycle

X.509 hardware tokens for user authentication, having moved further along the Plateau of Productivity, have left the Hype Cycle. It is also worth noting that there is increased interest in FIDO and mobile MFA, which both embrace public-key cryptography, as used within X.509 hardware tokens.

Mobile identity has been removed as a discrete entry, as it described various innovations covered separately in this Hype Cycle, such as BYOI and mobile MFA.

5G security has been removed from this Hype Cycle, as it is covered more appropriately in Hype Cycle for the Future of CSP Network Infrastructure, 2021.

On the Rise

CIEM

Analysis By: Henrique Teixeira

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

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 IaaS. They use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges, dormant and unnecessary permissions. CIEM ideally provides enforcement and remediation of least privilege approaches.

Why This Is Important

Managing cloud infrastructure entitlements is challenging due to their rapid increase in number and complexity, further exacerbated by the multicloud, where entitlements are inconsistently defined and configured. Traditional identity governance and administration (IGA) and privileged access management (PAM) solutions have not adequately addressed the need of managing entitlements that are extremely granular and dynamic. New tools using CIEM capabilities are emerging to fill this gap.

Business Impact

CIEM offers a quicker time to value when compared to generalist tools like traditional PAM and IGA, or cloud security posture management (CSPM) to mitigate multicloud IaaS identity risks. For example:

- Managing permissions risks to prevent cloud breaches and data theft.
- DevSecOps use cases, or cases where agility and speed need to be balanced with IAM security in the cloud.
- Defining IaaS access policies, addressing auditor concerns and simplifying compliance.

- Improving existing PAM and IGA processes.

Drivers

Inquiries into Gartner on CIEM have more than doubled over the past year. Specialist CIEM vendors are growing in number and CIEM capabilities are being embedded in adjacent markets:

- Gartner projects that a stand-alone market for CIEM is not sustainable in the long term, but CIEM capabilities will persist in other tools, and the time to plateau now reflects that.
- The challenge of managing the risk of overprivileged accounts in multicloud is becoming worse, with thousands of new IaaS services and features added in the last couple of years by cloud infrastructure and platform services (CIPS) providers.
- Through 2023, Gartner estimates that at least 99% of cloud security failures will be the customer's fault.
- The vast majority of identities in IaaS are using only a small fraction of permissions granted in IaaS.
- CIEM delivers narrow, specific and efficient use cases for managing IaaS privilege risks. It has been a successful strategy, allowing predictive and prescriptive analytics techniques to be applied with reduced manual input (Quick Answer: How to Use Different Types of Identity Analytics for More Efficient IGA).
- Some CIEM vendors have started to expand their scope to include a broader identity security posture management capacity, beyond multicloud IaaS only. Extended controls include SaaS application targets, basic threat discovery, incident response and forensics. In the short term, it fills a gap that exists in traditional IAM tools as well as in CIPS and CSPM platforms.
- Some vendors even started to offer products that extend analytics-driven entitlement management to on-premises targets and cloud identity providers (IdPs).
- Traditional IGA, PAM and CSPM vendors have also been adding more CIEM capabilities.
- CIPS providers are also adding new tools to enhance entitlement management. However, these embedded tools are in different stages of maturity and do not support multicloud use cases, reinforcing the need for specialized cloud security tools that provide CIEM capabilities.

Obstacles

- Awareness about CIEM challenges and solutions: CIEM is an emerging market segment, and vendors and customers are still experiencing early challenges in understanding what CIEM can provide today, and what this segment may become in the future.
- Maturity of technologies and limited number of customer success stories.
- There is overlap of CIEM capabilities with CSPM, which may add to hesitancy and confusion when buying.
- Similar to CSPM, CIEM tools risk being subsumed into adjacent markets; however, it's no longer flagged to be obsolete before plateau.
- In terms of third-party alternatives, besides CSPM, CIEM features can be acquired through competing IGA vendors like SailPoint, Saviynt, SecurEnds, or PAM vendors, like CyberArk.
- In most cases, especially in more complex organizations with lots of legacy and on-premises resources, CIEM cannot replace full-featured IGA and PAM technologies.

User Recommendations

CIEM offers a quicker time to value when compared to more traditional IAM or CSPM tools. Here are a few recommendations when evaluating CIEM capabilities and specialist tools:

- Prioritize investment into CIEM capabilities for closing gaps in CSPM and IAM when protecting hybrid and multicloud IaaS.
- Leverage CIEM in DevSecOps use cases, and infrastructure as code, leveraging its abilities to provide visibility to unnecessary privileges, and refining policies, without disrupting developer flows.
- Check if your existing vendors for IGA, PAM and CSPM offer CIEM capabilities to avoid overlap and redundancy.
- Use CIEM as part of a broader IAM strategy; it cannot replace full-featured IGA and PAM technologies, especially in organizations with lots of legacy and on-premises resources.

Sample Vendors

Authomize; Britive; CloudKnox; CyberArk; Ermetic; Obsidian; SailPoint; Saviynt; Sonrai Security; Zscaler

Gartner Recommended Reading

IAM Leaders' Guide to Identity Governance and Administration

Quick Answer: How to Use Different Types of Identity Analytics for More Efficient IGA

IAM Leaders' Guide to Privileged Access Management

Managing Privileged Access in Cloud Infrastructure

User-Managed Access

Analysis By: Michael Kelley

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

User-managed access (UMA) is a profile of the OAuth 2.0 framework that defines how individuals can control, allow, deny and delegate access to their personal digital assets, like personal data. UMA gives users the tools and autonomy to grant and revoke access to their data and assets, actions which would normally require the assistance of a system administrator.

Why This Is Important

One significant benefit of UMA over other approaches like OAuth is the ability to control access across administrative domains. This means that the resource does not have to be tightly coupled with the policy engine, which allows decentralized user access control.

Once defined and configured, users can easily temporarily share access with anyone, regardless of where that information may be, and can just as easily revoke that access, all without the assistance of IT administrators.

Business Impact

- **Healthcare:** UMA enables the private exchange of health information. For example, HEART (Health Relationship Trust) by the OpenID Foundation uses UMA, OAuth and OpenID Connect, which complies with the open standard FHIR (Fast Healthcare Interoperability Resources).
- **Privacy regulation:** UMA could enable the online customer to never relinquish control of their personal assets, but instead allow the customer to delegate granular access to an online provider for analytics, marketing data or personalization.

Drivers

- The original concept for UMA was targeted at privacy scenarios, where private — and potentially regulated — data could be controlled from an access perspective by the subject, or owner, of that data.
- UMA provides technical controls that individuals use to control access to their information, which is relevant for complying with privacy regulations, such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations bring more sophisticated requirements for the control of personal information, including the need to share specific portions of data on a time-bound basis.
- UMA will have the most bearing on customer identity and access management (CIAM) use cases, due to the emphasis on user experience (UX) and privacy preferences. However, there may be workforce applications for UMA, too.
- UMA might be helpful in multiuser account scenarios, like a family participating in a sports association. The children would have accounts and access, but the parents or guardians would have their own access, and the children would delegate control and management of access and preferences to the parents or guardians.

Obstacles

- UMA is difficult to define, and beyond minimal growth in vendor-supported and open-source implementations, adoption remains extremely limited. Successful implementations are rare.
- Use cases are still niche, which continues to delay widespread adoption.
- Competing technologies, such as delegated administration approaches, OAuth and even decentralized identity, may prove to be a better long-term approach for user privacy.
- Very few changes have occurred with UMA 2.0 specifications. It is in "recommended" status, approved by the Kantara membership.
- Beyond ForgeRock, and open-source vendors like Gluu, Red Hat and WSO2, almost no access management vendors in the market are promoting UMA.

User Recommendations

- Current identity and access management (IAM) approaches to sharing personal information require IT administrators to control authorization changes through policy. When there is a need to allow individuals to have better control for others accessing their protected information across administrative domains, IAM leaders should determine whether UMA could add needed functionality.
- Begin by modeling processes and data flows that could support these new types of user-controlled interactions and work with access management vendors on product roadmaps. Proofs of concept (POCs) will be critical, due to the lack of production implementations and proven best practices.
- IAM leaders should also weigh alternative approaches in these use cases, including OAuth, delegated administration and decentralized identity approaches.

Sample Vendors

ForgeRock; Gluu; iWelcome; Red Hat; WSO2

Gartner Recommended Reading

Solution Criteria for Access Management

Critical Capabilities for Access Management

Zero-Knowledge Proofs

Analysis By: David Mahdi, Bart Willemsen, Mark Driver

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Zero-knowledge proofs (ZKPs) are privacy-preserving messaging protocols that enable entities to prove that information available to them is correct, without the requirement to transmit or share the underlying information. Blockchain platforms have been evolving to include this privacy-oriented mechanism.

Why This Is Important

Due to cyberthreats and privacy laws, security and risk management (SRM) leaders must support use cases that enable digital business while ensuring data protection. ZKPs enable entities to prove information validity, without the requirement to transmit sensitive data. These protocols limit the requirement for mass decryption/encryption of data elements, which benefits the efficiency of the network as well as the potential adoption of blockchain-based systems.

Business Impact

ZKPs are being applied for a variety of use cases, especially in the context of authentication and transaction verification. Other use cases include payments, custody management, anti-money-laundering (AML), know your customer (KYC), consumer identity and access management (IAM), etc. With the addition of ZKPs to blockchain platforms, SRM leaders now have the potential to cover information security use cases that require confidentiality, integrity and availability (CIA).

Drivers

- Traditional data protection techniques typically focus on data in motion (i.e., transport layer security) and data-at-rest encryption. Data-at-rest encryption, as commonly implemented, does not provide strong protection from data theft and privacy disclosures. It is unable to secure data in use and data sharing scenarios.

- New use cases and maturing privacy legislation worldwide present new privacy and cybersecurity concerns that require data-in-use protection. There are also scenarios where the data itself does not need to be shared. ZKPs enable such data-in-use protection.

- Concerns about data security in several scenarios, including: collecting and retaining sensitive personal information; processing personal information in external environments such as the cloud; and information sharing.
- Privacy law violations (due to the exposure of sensitive information).
- Need for mitigation of sensitive data leakage and cyberattacks.

- Homomorphic encryption, which allows for computation on encrypted variables without revealing their values.

Obstacles

- Even with a variety of working groups (e.g., ZKProof), ZKPs remain in an emerging state. They still require a common framework for applications to leverage.
- Only a limited number of practical implementations have emerged till date.
- The variety of methodologies and the multiplicity of approaches to data management inhibit adoption. ZKPs will need to scale at the rate of blockchain transactional volumes in order to be effective.
- ZKPs require integration into applications. Downstream applications, such as CRMs and databases, will need some modification.

User Recommendations

- Work with SRM leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Be realistic with the current immaturity of ZKP solutions and approaches when evaluating ZKP benefits for privacy protection.
- Evaluate how ZKP controls may impact transaction authentication and ultimately consumers.
- Assess the impact on the broader information management strategy.
- Assess the architectural implications for using ZKP with different blockchains and distributed ledgers.

Sample Vendors

Evernym; IBM

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation

IoT Authentication

Analysis By: David Mahdi, Michael Kelley

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Internet of Things (IoT) authentication is the mechanism of establishing trust in the identity of a thing (for example, a device) interacting with other entities such as devices, applications, cloud services or gateways operating in an IoT environment. Authentication for the “things” in IoT takes into account potential resource constraints of IoT devices, the bandwidth limitations of networks they operate within and the mechanized nature of interaction among various IoT entities.

Why This Is Important

IoT solutions promise to unlock new opportunities to optimize processes or even tap into new revenue streams. Unfortunately, as these connected devices bridge the cyber and physical worlds, they open new threat vectors for bad actors. Therefore, sound IoT security coupled with strong identity in IoT devices requires strong IoT authentication, with the goal of mitigating and minimizing cyberattacks and/or other issues and vulnerabilities.

Business Impact

- IoT authentication for consumer devices can mitigate privacy issues that directly impact liability and brand reputation.
- IoT authentication can mitigate unauthorized access leading to degraded or halted performance that could directly impact productivity.
- IoT authentication for industrial devices can mitigate attacks against devices that lead to operational impacts and, potentially, safety incidents if used in a safety-critical production area.

Drivers

- IoT solutions blend the physical and digital worlds by creating cyber-physical systems (CPS), thus transforming the way we live and work.
- By 2024, growth of organization spend on overall IoT security will be roughly $4 billion — up from $2.5 billion in 2021 (Gartner 2020). As such, these investments will drive attention and spend on IoT authentication methods.
- Public key infrastructure (PKI) vendor investments and focus in this space include DigiCert, Keyfactor and Sectigo, leveraging their PKI capabilities to solve IoT authentication use cases.
- Standards helping to provide consistent approaches, and solidifying investments, viability and utility, include the following: (1) RFC 8628: OAuth 2.0 Device Authorization Grant extension; (2) the ACE working group within the Internet Engineering Task Force (IETF) is also specifying how OAuth 2.0-based authentication and authorization exchanges can be optimized for constrained devices for use over Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT) and other messaging protocols.

Obstacles

- The IoT security landscape is complex, including determining the right people, process and technology to employ due to a fragmented market, and difficulties productizing due to inconsistent device types and operating environments.
- Some authentication methods are not good candidates due to certain IoT devices that are resource-constrained with low computing power and storage capacity.
- Support of authentication methods via IoT platforms is lacking, and use-case areas such as industrial IoT (IIoT) have protocols that are still in flux, creating ongoing challenges for authentication approaches.

User Recommendations

- Catalog and establish capabilities for each category of device in its IoT network. Leverage device- and network-based contextual information to gain additional assurance.
- Evaluate and adopt authentication frameworks that support the range of device types across the IoT realms in operation.
- Make use of trusted computing techniques, such as hardware root of trust, that help to protect against physical attacks on devices and sensors, but also against the external software attacks that could enable unauthorized reading, analyzing and manipulating of software code.

Sample Vendors

DigiCert; Entrust; Keyfactor; Microsoft; Sectigo; V-Key

Gartner Recommended Reading

Solution Comparison for PKI and Certificate Management Tools

Managing Machine Identities, Secrets, Keys and Certificates

Technology Insight for X.509 Certificate Management

Market Trends: IoT Edge Device Security, 2020

At the Peak

Machine Identity Management

Analysis By: David Mahdi, Erik Wahlstrom, Felix Gaehtgens

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Machine identity management aims to establish and manage trust in the identity of a machine (hardware or software) interacting with other entities, such as devices, applications, cloud services or gateways. Specifically, machine identity management handles the life cycle of credentials used by machines. The credentials span secrets, cryptographic keys, X.509 certificates and SSH keys.

Why This Is Important

- Digital transformation has led to an explosion in the number of machines — such as workloads, code, applications and containers — that need to identify themselves and communicate with each other.
- As a result, several technology providers have built tools that can help clients discover and manage machine identities across hybrid and multicloud environments.
- Managing machine identities has become critical, as nonhuman entities are now at the leading edge of digital transformation.

Business Impact

- Security leaders need to protect the increasing volume of machine-to-machine communication that will be required to support their business needs.
- Machine identity management encompasses technologies that today remain mostly siloed (for example, secrets, X.509 certificates and keys).
- Currently machine identity management spans several technical areas (markets and vendors). Many clients are getting some (albeit limited) benefit from products that already exist.

Drivers

- Already, many organizations have more machine identities to manage than people identities. As organizations further transform to use more digital services (including hybrid and multicloud), the number of machine entities (software, devices, workloads and robotic process automation [RPA]) that need to be managed will increase even further.
- In order to offer higher-value transactions and operations, security and identity must be built in at the foundation. Machine ID management offers the ability to create a strong foundation in order to capitalize on automation and overall digital transformation.
- Hype around machine identity is increasing, and vendors serving part of the machine identity space have recently attracted new investment (some recent examples are Akeyless, AppViewX, senhasegura and Venafi).
- Some privileged access management (PAM) vendors include SSH key management, and several PAM vendors are actively adding secrets management capabilities.
- Cloud providers are also offering some key management capabilities (examples include Alibaba Cloud Key Management Service [KMS], Amazon Web Services [AWS] Key Management Service, Azure Key Vault and Google Secret Manager).
- Vendors in this space are now realizing that they need to acquire, build or partner with ancillary vendors in order to provide more holistic solutions in the machine ID space. Consequently, vendors will likely conduct M&As in order to remain competitive and capitalize on this newly forming market.
- Integrations and hybrid or multicloud single-pane-of-glass functionality are becoming more important evaluation criteria than previously expected. The aim is to help increase organization efficiency and decrease response times (that is, to improve agility).

Obstacles

- Most machine identities and credentials are fragmented and require distinct solutions to manage them. Examples are secrets management, and public key infrastructure. It is not feasible for any organization to manage all machine identities with only one technology.

- There is only a partial convergence of tools. Many tools have different approaches with regards to user interfaces, integrations, discovery and reporting capabilities.
- There is a confusion around the definition of machine identities, exacerbated by vendors providing their own interpretation and messaging. This makes selecting the right tooling very difficult.
- Different teams — such as DevOps, security, identity access management (IAM) and infrastructure and operations (I&O) — have different needs and tool preferences. A cross-team strategy becomes critical to help balance expectations around centralized governance and operational functionality.

User Recommendations

- Determine the overall interdependence of machine identities by establishing discovery processes. Evaluate a mix of multiple tools that can provide insight.
- For certificates, use full life cycle management and discovery-centric tools to audit the number of deployed machine identities, and to identify the potential risks from expiry and overall compliance. Choose full life cycle machine identity management solutions to drive automation when dealing with large, complex, multivendor certificate environments — especially with multiple certificate-based enterprise use cases such as mobile and the IoT.
- For secrets, use free discovery tools from PAM vendors and leverage a configuration management database (CMDB). Track authentication events to find machine accounts. Use secrets management functions from specialized tools, PAM tools and cloud providers. Refrain from signing multiyear deals. Competition is increasing and Gartner expects prices for secrets management products to come down.

Sample Vendors

Akeyless; Amazon Web Services; AppViewX; CyberArk; Entrust; Google; HashiCorp; Keyfactor; Microsoft; senhasegura; Venafi

Gartner Recommended Reading

Managing Machine Identities, Secrets, Keys and Certificates

Technology Insight for X.509 Certificate Management

Decentralized Identity

Analysis By: David Mahdi, Michael Kelley

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Decentralized identity (DCI) leverages technologies such as blockchain or other distributed ledger technologies (DLTs) to allow an entity to create and control its own digital identity. Thus, it provides an alternative to centralized IAM architectures by establishing trust in identities and resilience within the overall system, with little reliance on centralized arbiters or identity stores.

Why This Is Important

Isolated digital identities will not scale with the needs of digital business. Online and mobile identities continue to be in a fragmented state due to service providers (banks, retailers, social networks, etc.) forcing consumers to create individual identities for each and every service. DCI offers an alternative approach that does not have the security, privacy and usability issues associated with traditional, fragmented, digital identity approaches.

Business Impact

With DCI, users gain control of their identities and data, enabling service providers to interact with users with greater speed and confidence. Currently, providers typically hoard identity information about users. Leveraging DCI, identity and service providers will be able to increase security and access convenience for end users, while reducing exposure to data breaches and potential privacy compliance violations.

Drivers

- **Vendor investments in DCI:** Due to the ubiquity and influence of vendors investing in this space, there is high potential to drive the DCI market forward. Significant investments have been made by IBM and Microsoft. Other major developments in this space include the acquisition of ShoCard by Ping Identity, and funding received by vendors such as 1Kosmos and InfoCert.
- **Investments in BYOI:** Including investments in overall BYOI could also act as a precursor to DCI adoption. E.g., Microsoft enabling "external identities" with Azure Active Directory (Azure AD).
- **Client and overall market interest in DCI:** Interest is increasing due to attractive elements such as the ability to enable new digital business opportunities while maintaining client privacy. For example, using DCI to share verified claims, such as age/income, without the need to expose sensitive personal data.
- **Standards enabling consistency:** Standards are currently emerging, led by entities such as the World Wide Web Consortium (W3C) and Decentralized Identity Foundation (DIF), to create a consistent approach to DCI. These standards will help propel this technology forward.

Obstacles

- Despite a lot of promise and hype, adoption is slow due to lack of progress and inaction by most large ecosystem players, CIAM vendors and various IDPs including governments.
- Standards are still in the development stage.
- Lack of core DLT/blockchain performance, interoperability, scalability and maturity.
- Lack of clear security standards for DLTs, such as crypto-agility, wallet standards/adoption and security.
- Lack of production-level solutions, which prevents some organizations from deploying due to concerns of having to "rip and replace" in the near future when the solutions stabilize.

User Recommendations

- Deliver attainable use cases as POCs, such as a DCI solution focused on business partners (i.e., limited deployments, low in scale). Plan for, but don't rush, long-term, large-scale initiatives such as consortium and/or DCI interoperable global identity.
- Leverage market vendors, such as IBM, Microsoft or Ping Identity, to understand the possibilities and potential of DCI.
- Be cautious of overoptimistic vendor claims. Evaluate the technical security aspects of blockchain platforms under consideration. In particular, examine vendor plans for support of standards, such as W3C and DIF.

Sample Vendors

1Kosmos; Evernym; Finema; IBM; InfoCert; Microsoft; Ping Identity; SecureKey

Gartner Recommended Reading

Guidance for Decentralized Identity and Verifiable Claims

SMPC

Analysis By: David Mahdi, Bart Willemsen, Brian Lowans

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Secure multiparty computation (SMPC) is a method of distributed computing and cryptography that enables entities (applications, individuals, organizations or devices) to work with data while keeping data or encryption keys in a protected state. Specifically, SMPC allows multiple entities to share insights while keeping data confidential from each other.

Why This Is Important

Security and risk management (SRM) leaders struggle to achieve a balance between data security and privacy when processing (personal) data. This is further complicated by regulations and overall business objectives. Historically, data protection has focused mainly on two states: securing data at rest and in transit. However, SMPC-based methods introduce data protection in use. This is a new paradigm to the arsenal of security methods and enhances traditional security approaches.

Business Impact

Due to their reliance on data for AI-based decision making and the sharing of insight from those decisions between multiple parties, SRM leaders need privacy-enhanced approaches to protect data amid a landscape of maturing data protection regulations. SMPC allows for the secure enablement of business, enabling organizations to leverage their data while addressing security and privacy concerns.

Drivers

- Traditional data-at-rest encryption, as commonly implemented, does not provide strong protection from data theft and privacy disclosures. It is unable to secure data in use and data sharing scenarios.
- SMPC-enabled data security allows for the protection of data while in use; thus providing SRM leaders with another data protection technique, which can be applied to new and existing use cases (such as multiparty data sharing).
- New use cases such as big data analytics, artificial intelligence (AI) or machine learning (ML) model training, present new privacy and cybersecurity concerns that require data-in-use protection.
- Concerns about data security in several scenarios, including collecting and retaining sensitive personal information, are driving SMPC adoption.
- Relative to other privacy protection methods, such as homomorphic encryption, SMPC can be much faster.
- SMPC helps ease fear of privacy law violations (due to the exposure of sensitive information).
- SMPC enables mitigation of sensitive data leakage, and overall reduction and mitigation of cyberattacks.

Obstacles

- SMPC algorithms can be latency-sensitive. As such, performance in some cases might not meet client requirements or expectations.
- Although considerable academic research has been conducted on SMPC, relatively limited number of practical implementations have emerged so far.
- When compared to existing techniques (such as cryptography based on hardware-generated and stored keys), clients could have potential issues with audits, especially if they have to adhere to standards like Federal Information Processing Standards (FIPS) certifications.

User Recommendations

- Work with developers/architects to establish a high-level position on SMPC relevance and a vision for future adoption (including POCs).
- Evaluate use cases such as: cloud computing, focusing on confidentiality with data in a cloud environment; privacy-enhancing (personal) data analytics initiatives; cryptographic key protection, including encryption key management initiatives (i.e., for protection of data at rest); secure and private data mining for data and analytics use cases, including data lake security; blockchain security (wallet protection, and/or quorum-based multisignature operations).

Sample Vendors

Baffle; Cybernetica; Inpher; IXUP; LiveRamp; Nth Party; Sepior; Snowflake (CryptoNumerics); Unbound Security; Ziroh Labs

Gartner Recommended Reading

Achieving Data Security Through Privacy-Enhanced Computation Techniques

Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation

Mobile MFA

Analysis By: Ant Allan

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Mobile multifactor authentication (MFA) provides passwordless identity corroboration by combining multiple (typically two) factors in a smartphone app. Possession of the phone provides the first factor, with the app typically using one or more of the following modes: one-time password (OTP), mobile push, X.509, and Fast IDentity Online (FIDO) authentication protocols. The additional factor may be a biometric trait or a local PIN. Biometric authentication may be device-native or proprietary.

Why This Is Important

User authentication is fundamental to identity-first security. It must provide sufficient credence in an identity claim to bring account takeover (ATO) and other digital-identity risks within an organization's risk tolerance. Unlike many mainstream MFA approaches, mobile MFA eliminates legacy passwords as an authentication factor, thus improving security and user experience (UX).

Business Impact

Identity and access management (IAM) and other security leaders across all industry verticals and geographies can benefit from investment in mobile MFA, which:

- Inherits the UX and total cost of ownership (TCO) benefits of mainstream phone-as-a-token authentication.
- Eliminates legacy passwords as an authentication factor, with security and further UX benefits.
- Can provide mobile-centric biometric authentication, enabling adoption of biometric methods across multiple use cases.

Drivers

- The imperative to avoid the vulnerabilities, risks and user frustration associated with legacy passwords that provide one of the authentication factors in the majority of legacy MFA solutions.
- The broad success of mainstream phone-as-a-token authentication over the past 15 years and the consequent interest in smartphones as a platform for passwordless authentication.
- Increasing commercial availability of mobile MFA. Among the varieties of passwordless authentication, those most often labeled “passwordless” by vendors are mobile MFA methods: (1) Mobile MFA methods are often modifications of vendors’ mainstream phone-as-a-token modes (especially mobile push), with a choice between a local PIN and a (typically, device-native) biometric trait as the additional factor that replaces the legacy password; (2) Newer vendors have come to market with obligate mobile MFA methods (i.e., where there’s no option of not using the additional factor on the phone). Some of these vendors have built on a mobile push architecture; others may incorporate X.509 or **FIDO authentication protocols,** especially FIDO2. In this case, using a proprietary, third-party biometric method is more common.
- Increasing interest in using **biometric authentication** for improved trust and accountability: (1) Mobile-centric biometric authentication — implementing biometric authentication via smartphone apps, regardless of the endpoint device — provides more consistency in UX and the technical implementation, as well as a lower TCO than maintaining discrete solutions for different use cases; (2) Furthermore, this approach can implement local comparison and matching, potentially avoiding the risks of centrally stored biometric data for multichannel implementations.

Obstacles

- In common with mainstream phone-as-a-token authentication, the main obstacle is that not everyone can or wants to use a phone for authentication: (1) Smartphones might not be allowed in some environments (e.g., contact centers, oil rigs); (2) Not everyone will have a suitable phone (with penetration varying by geography); (3) Not everyone will want to have yet another app on their personal phones, especially if they feel an employer might be collecting location and usage data via the app.
- Some mobile MFA tools might not readily support all use cases: (1) Mainstream phone-as-a-token methods integrate well with legacy remote access tools and with SaaS applications, typically via access management (AM) tools, but integration in other use cases, especially PC and network login, is often fragile. Mobile MFA based on these methods inherits the same limitations; (2) Mobile MFA based on X.509 and, especially, FIDO2 offers potentially broader support.

User Recommendations

- Use mobile MFA with mobile push and OTP as an evolution of phone-as-a-token deployments. OTP hardware tokens are ready alternatives to mainstream phone-as-a-token methods. However, a passwordless alternative is elusive.
- Use mobile MFA with X.509 for Windows PC and network login. Legacy PIN-protected X.509 hardware tokens remain viable when mobile MFA cannot be used.
- Evaluate mobile MFA with FIDO2 for Windows 10 login and for SaaS and other application access. FIDO2 security keys are the alternatives here.
- Choose full multiprotocol mobile MFA to cohesively support multiple use cases and to facilitate migration to FIDO2.
- Support legacy use cases (e.g., some VPNs) that still demand a password via mobile MFA that can function as a single factor or consider relaxing password rules.
- Favor mobile MFA in mobile use cases, with third-party biometric methods, for better trust and accountability. Enhance UX by providing a choice of two or more modes, such as face/fingerprint, face/voice, face/palm.

Sample Vendors

1Kosmos; Entrust; HYPR; IDmelon Technologies; Microsoft; Secret Double Octopus; Trusona; TruU; Veridium

Gartner Recommended Reading

Innovation Insight for Many Flavors of Authentication Token

Passwordless Authentication Is Here and There, but Not Everywhere

Technology Insight for Biometric Authentication

IAM Leaders' Guide to User Authentication

Sliding into the Trough

FIDO

Analysis By: Ant Allan, Tricia Phillips

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

The three Fast IDentity Online (FIDO) authentication protocols published by the FIDO Alliance combine public-key credentials in a hardware or software authenticator with a local "gesture" (e.g., a PIN or a biometric method). The majority of new FIDO deployments use FIDO2, which includes enabling the W3C Web Authentication web standard. FIDO2 software authenticators can be installed on endpoint devices; FIDO2 security keys and FIDO2-enabled smartphones provide a "roaming" alternative.

Why This Is Important

User authentication is fundamental to identity-first security. It must provide sufficient confidence in an identity claim to bring account takeover (ATO) and other digital-identity risks within an organization's risk tolerance. Passwords are notoriously weak, elevating risk, even when used as an element of multifactor authentication (MFA). FIDO authentication protocols, particularly FIDO2, can provide passwordless MFA in a consistent way across multiple use cases for both employees and customers.

Business Impact

Identity and access management (IAM) and other security leaders across all industry verticals and geographies can benefit from adopting FIDO authentication protocols, which can:

- Provide passwordless multifactor authentication (MFA) in multiple employee and some customer use cases.
- Improve trust and user experience (UX) and ensure a more consistent UX across different use cases.
- Simplify the adoption of biometric authentication for improved accountability in some use cases.

Drivers

- The imperative to avoid the vulnerabilities, risks and user frustration associated with legacy passwords drives interest in passwordless authentication, the original premise of the FIDO Alliance.
- The integration and extension of earlier, discrete FIDO protocols in FIDO2 to create a FIDO Authentication standard for platforms such as the web and native operating systems.
- Increasing support for FIDO2 among major vendors including Google, Microsoft and (to a lesser degree) Apple: (1) Google, along with Yubico, has been a strong advocate of FIDO security keys, laying the foundations for FIDO2. FIDO2 support in Android enables any phone running Android 7+ to be used as a "roaming" authenticator; (2) Microsoft Windows Hello and Windows Hello for Business (WHfB) provide FIDO2 authenticators for Windows 10, enabling passwordless login to PCs via a biometric method or local PIN. Windows Hello enables login to FIDO2-enabled websites and WHfB enables login to corporate AD networks and to cloud environments via Azure AD Premium; (3) FIDO2 "roaming" authenticators can be used for Windows 10 login and natively within Azure AD Premium; (4) FIDO2 support in Apple Safari in iOS and macOS enables Touch ID and Face ID for web logins; (5) Web Authentication support in Google Chrome, Mozilla Firefox, Microsoft Edge and Apple Safari.
- Increasing support for FIDO2 among access management (AM) vendors such as CyberArk, ForgeRock, Okta, OneLogin and Ping Identity.
- Increased market availability of FIDO2 security keys from a variety of vendors. FIDO2 security keys with embedded fingerprint sensors enable biometric authentication as an alternative to a PIN: (1) Relatively few vendors offer FIDO2-enabled smartphone apps. Nevertheless, Gartner projects that this will emerge as the most popular approach, given the success of phone-as-a-token authentication over the past 15 years. Leading vendors with mobile push apps are likely to add FIDO2 support in the coming year, which will accelerate movement to the plateau.

Obstacles

- For employees: Lack of FIDO2 support in legacy use cases such as VPNs, privileged access management (PAM) tools and traditional data-center applications: (1) This limitation for VPNs and PAMs disappears where these tools can be federated with a FIDO2-enabled identity provider (an AM tool or similar); (2) Some AM vendors' and third-party tools (e.g., "access gateways") can extend the reach of AM tools to legacy apps.

- For customers: Lack of device-native FIDO2 capability and the need for “roaming” authenticators (smartphone apps or hardware keys).
- Constraints on biometric authentication architectures: (1) FIDO2 can use device-native biometric methods or third-party methods implemented wholly on the device. By design, this enhances privacy by ensuring that the user’s biometric data never leaves the device; (2) However, a centralized biometric architecture might be required to support multichannel use of biometric authentication and integration with document-centric identity proofing tools.

User Recommendations

- Prefer FIDO2 as the strategic approach for passwordless MFA, especially in employee use cases: (1) Prepare for strategic investments in FIDO2 for passwordless MFA in the medium term. Seek near-term opportunities in discrete use cases; (2) Choose certified proprietary tools with granular control over how FIDO2 is consumed and what “gestures” can be used (e.g., third-party biometric modes); (3) Devices with native FIDO2 support might be OK in some use cases, but it will be some time before these will be ubiquitous; (4) Be cautious about continued investment in legacy tokens. Favor vendors that provide a migration path to FIDO2.
- Weigh the benefits of using FIDO2 as a way to simplify the implementation of third-party biometric methods against the need to support multiple channels and integration with identity proofing tools: (1) Using a smartphone as a “roaming” FIDO2 authenticator with third-party biometric methods (with FIDO-certified presentation attack detection capability) might be a happy medium.

Sample Vendors

FEITIAN Technologies; Google; Hypersecu Information Systems; IDmelon Technologies; LoginID; Microsoft; Nok Nok Labs; Thales; TrustKey Solutions; Yubico

Gartner Recommended Reading

Innovation Insight for Many Flavors of Authentication Token

IAM Leaders’ Guide to User Authentication

SCIM

Analysis By: Henrique Teixeira

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

The System for Cross-Domain Identity Management (SCIM) specifications provide a protocol, schema definition and extension model for provisioning and managing identity data in cloud/hybrid applications and services. The protocol supports create, read, update and delete (CRUD) operations of identity resources, such as users, groups and custom resource extensions. SCIM is not a complete solution for full life cycle management but defines the interfaces and formats for identity provisioning.

Why This Is Important

SCIM helps establish and standardize the communications and identity data exchange between two different applications. SCIM is a very popular starting point for basic user provisioning to cloud-based targets, given its broad adoption by identity access management (IAM) vendors and ease of deployment due to standardization. It is easier and less expensive than other API or custom developed provisioning adapter approaches.

Business Impact

SCIM can be used to reduce the costs and time for administering identities across identity management boundaries. It is applicable in the following situations:

- General IAM use cases where provisioning to SaaS applications, or where any API friendly system is required
- Merger and acquisitions, or when coexistence of multiple identity providers and identity sources are required
- Identity data synchronization and consolidation use cases, including but not limited to CIAM

Drivers

Development for the SCIM specifications began in 2011 and the current 2.0 version was released as IETF RFC in 2015 for managing identity resources such as users and groups using application-level, REST/JavaScript Object Notation (JSON). The key trends and developments driving hype around this innovation are:

- Interest groups have discussed enhancing the protocol to offer extended capabilities like PAM process integrations, use SCIM to read privileged data, and read and modify the access rights to privileged data (ACLs).
- SCIM has established itself as the minimum viable product for user provisioning. The vast majority of IAM vendors that provide some life cycle or user provisioning capability have adopted SCIM.
- Some IAM vendors offer SCIM agents that are installed on-premises to support legacy protocols such as LDAP, and the agents translate it into SCIM for when it's communicating back to the SaaS-delivered IAM platform.
- Organizations looking to implement IGA or life cycle management processes are including SCIM as a mandatory requirement.
- SCIM support by SaaS applications continues to grow, and smaller SaaS vendors are perceiving the benefit of supporting the standard as an entry point for selling to large organizations.
- In the last couple of years, some good progress continues to be observed in the use of SCIM in provisioning gateways and identity synchronization brokers. Aquera and Radiant Logic are both leveraging these approaches.
- The number of SaaS vendors that have exposed any type of identity administration API is also growing, which at least opens a path for IAM integration using customized SCIM-based connectors.

Obstacles

- SCIM has passed the Peak of Inflated Expectations, and as more organizations adopt SCIM as a solution for provisioning to SaaS applications, more of its limitations start to show.
- Organizations still are not familiar enough with SCIM so custom APIs are still deployed instead.
- SCIM defines some standard attribute definitions and relies on extensions for a large portion of use cases. Not all implementations of SCIM currently support the extensions.
- In general, SCIM functionality is limited when compared with proprietary native connectors.

- SCIM does not solve the problem of integrating with less commonly used applications that will not have a native connector available for provisioning, and neither offer support to SCIM. Custom code will still be necessary, even when developing an adapter using SCIM standard in those cases.
- SCIM must be combined with the type of capabilities that IGA solutions provide to handle the full life cycle of identities with workflows and identity reconciliation.

User Recommendations

- Where native provisioning connectors are not available, leverage SCIM to simplify provisioning and reconciliation with target systems that support the protocol.
- Choose SCIM as the new framework if you are replacing custom developed connectors.
- Use SCIM as a basis to develop future adapters.
- Utilize SCIM as part of a broader fulfillment strategy including indirect methods, like ITSM and RPA.
- Leverage SCIM gateways and identity synchronization brokers (like Aquera and Radiant Logic) to simplify account fulfillment objectives. These gateways and proxies can translate SCIM into the proprietary protocol or format used by target systems for greater interoperability.
- SaaS and application developers must continue to embrace SCIM to lessen organizations' burden of manually handling many custom connectors.
- Enterprise buyers (and IAM vendors) must tell application vendors to support SCIM, pointing to the need for integration with enterprise and cloud IAM systems.

Sample Vendors

Aquera; Curity; Kapstone Provisioning Gateway; Microsoft; Okta; One Identity Starling Connect; Radiant Logic; SailPoint; Salesforce; UNIFY Solutions

Gartner Recommended Reading

IAM Leaders' Guide to Identity Governance and Administration

Modern Identity and APIs: OpenID Connect, OAuth 2.0 and SCIM 2.0

Architecting an Agile and Modern Identity Infrastructure

API Access Control

Analysis By: Henrique Teixeira, Michael Kelley

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

API access control is a big part of the API security capabilities that enable authentication and authorization of API targets. At minimum, it involves an OAuth 2.0 authorization server, which supports and implements consent, handles scope to claim mappings, and is capable of issuing customizable and self-contained JSON Web Tokens (JWTs) to web servers, mobile apps, modern web apps and services used for accessing API targets.

Why This Is Important

API access control has grown in importance. Over the past year, there was a 300% increase in IAM discussions related to APIs. Organizations have evolved their application architectures toward mobile apps, API clients and back-end services, all of which require more sophisticated authentication and authorization controls to APIs and microservices.

Business Impact

API access control capabilities are important in the following scenarios:

- Developer use cases, offering libraries, out-of-the-box integrations, as well as best practices examples for access controls in APIs.
- Enabling user-present and machine-to-machine access to API targets.
- Workforce and customer IAM use cases, including customer data protection, consent management and data privacy strategies in modern applications.
- Architecture standardization with central access controls for APIs.

Drivers

The market has been maturing and access management and API security vendors have added more robust capabilities for API access controls. The key trends and developments driving hype around this innovation are:

- Beyond OAuth 2.0 authorization servers, other functionalities are starting to become more popular in API scenarios, like libraries, sidecars or out-of-the-box integrations with APIs and API mediators to centralize authentication and authorization decisions to the authorization server.
- Developer self-service capabilities are also increasing in demand, for managing apps and services and support for flows such as: OAuth mTLS, JWT and SAML grant types, the device flow, token exchange, introspection and revocation. They also provide strong and agile cryptographic mechanisms for signing tokens.
- Modern applications and service patterns (like service mesh) are extensively adopting JWTs as an authentication mechanism. JWTs are becoming the de facto standard to convey authorization information and claims about users and services.
- The lack of advanced IAM capabilities of API gateways (like session management, advanced adaptive access and support for evolving identity standards) has led to an increased demand for specialized access control features for APIs, either delivered by AM and other IAM and API security specialist tools.
- API access control adoption has benefited from the popularity of OAuth 2.0 as an industry standard as it is widely adopted by the vast majority of AM and API security vendors.
- Customer IAM is another big driver for more recent API access control demand when developing more sophisticated privacy and consent management controls based on those standards.
- API security now benefits from increased awareness and product feature coverage.

Obstacles

API access control is increasing in importance and should be a mandatory piece of API security strategies. However there are still obstacles to mainstream adoption, including:

- Lack of application development alignment with IAM strategies. Time to market is seen as more important than basic API protection in those situations.
- Lack of developer and security staff training in IAM best practices.
- Proprietary methods for API access control are still in use (like custom code using shared databases).

- Belief that API gateways are enough for enabling and securely running API-based applications.
- Lack of tooling that enables scaling access controls to thousands of APIs and services.

User Recommendations

- Use API access control (to control which applications and people can access APIs) alongside API threat protection (to detect and block attacks on APIs).
- Approach API-based app development with both API threat protection services (such as WAFs) and DDOS protection as well as advanced API access control capabilities.
- InvestigateAM tools that provide converged IAM features for APIs, and at least some "lightweight" API gateway capabilities such as token validation services and centralized authorization, for example.
- Phase out proprietary methods for API access control.
- Create and implement an effective API security strategy that looks beyond just API threat protection and that also includes API access controls.
- Provide IAM training for developer and security staff, highlighting API access control.
- Deploy API access control enforcement points as close as possible to the service being protected. This will enable defense in depth.

Sample Vendors

Amazon Web Services; Auth0; Authlete; Cloudentity; Curity; ForgeRock; IBM; Microsoft; Okta; Ping Identity

Gartner Recommended Reading

Critical Capabilities for Access Management

API Security: What You Need to Do to Protect Your APIs

Critical Capabilities for Full Life Cycle API Management

Modern Identity and APIs: OpenID Connect, OAuth 2.0 and SCIM 2.0

Building Authentication, Authorization and SSO Into API-Driven Apps G00390369

Bring Your Own Identity

Analysis By: David Mahdi, Felix Gaehtgens

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Bring your own identity (BYOI) is the concept of allowing users to select and use a third-party digital identity, such as a social (Facebook, for example) or a higher-assurance identity (such as a bank or government ID) to access multiple digital services. Service providers/relying parties can be enabled to trust these external digital IDs for purposes of authentication and access to digital services, but also for sharing of identity attributes such as name and address.

Why This Is Important

BYOI is the concept of allowing users to select and use an external digital identity, such as a social identity (such as LinkedIn) or a higher-assurance identity (such as a bank ID) to assert their identity in order to streamline account registration and access digital services. Service providers can trust these digital IDs, rather than forcing the user to create a new identity, for authentication and access to, but also for sharing of identity attributes such as name and address.

Business Impact

BYOI leverages outside identities to help reduce friction and increase adoption of online services. Exploiting higher-trust BYOI for customer registration (including with identity attribute sharing) potentially avoids or lowers the costs of identity proofing or know your customer (KYC) processes. High-assurance IDPs can be used to perform appropriate risk assessment and authentication, lowering the barrier to new business models that require higher levels of identity assurance.

Drivers

Aspects driving BYOI forward are, but are not limited to:

- Vendor investment focus and enablement of BYOI: (1) Microsoft enabling “external identities” with Azure AD; (2) Support from a variety of CIAM and IAM vendors, such as ForgeRock; (3) ID.me raising $100 Million in funds.
- Identity provider investments and focus: (1) Capital One, offering APIs for BYOI functions (that is allowing service providers to use their functionality); (2) Large ecosystem vendors such as Apple, Amazon and Google.
- Client and overall market interest in BYOI due to attractive elements: (1) Reducing registration/login friction for consumers and users(where the consumer selects a BYOI to interact with the service provider); (2) Increase in Service usage and Brand loyalty: Through continued usage of an IdPs digital identity, users are periodically exposed to the IdPs brand. This can increase client loyalty. For example, using a Bank ID a various service provider digital services; the digital identity becomes critical to the daily life of the consumer/client; (3) Enabling new digital business opportunities: Monetization of identity attributes: i.e., generating transactions fees (in fiat or crypto-tokens) through enabling use cases such as Identity verification through generation of verifiable claims (see decentralized identity).

Obstacles

Social identities, while useful for a variety of use cases, do not meet security and trust standards that many organizations require, especially for regulated industries (such as finance and healthcare). Privacy concerns also persevere, with many IDPs able to track where users log in.

As a result, the combined notion of all identity types, and their various assurance levels, places BYOI in the Trough of Disillusionment.

Some of the obstacles that impede current market adoption and maturity include:

- Lack of accessibility.
- Availability of medium- and high-trust identities.
- Perception of risk (concern of service providers losing visibility and/or control of their relationships with clients).

User Recommendations

Determine how to take value from, or in some cases, contribute to, the BYOI landscape. For B2C or G2C initiatives, there are also some potential risks that can arise from not leveraging BYOI such as:

- Loss of customers: Carefully determine how the friction of using legacy approaches reduces customer experience (CX) and thus customer retention.
- Focus on reducing friction by leveraging common BYOI uses such as account registration and login. Creating a great CX can offset risks of diluting the brand and the loss of ownership of the customer journey.
- Ensure the level of trust provided by the identity provider (IdP) matches the level of risk, or the identity provider provides trust elevation to bridge any gap.

Sample Vendors

Apple; Facebook; ForgeRock; Google; ID.me; Microsoft; SecureKey; Signicat; Twitter

Gartner Recommended Reading

Innovation Insight for Bring Your Own Identity

Innovation Insight for Decentralized and Blockchain Identity Services

Cool Vendors in Blockchain Technology

Top Trends in Government for 2021: Citizen Digital Identity

SaaS-Delivered IAM

Analysis By: Abhyuday Data

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

SaaS-delivered IAM, also known as identity and access management as a service (IDaaS) or IAM as a service, is the subset of IAM tools characterized by delivery as SaaS (rather than on-premises or IaaS-hosted software). The tools can provide functionality from any of the core IAM markets — identity governance and administration (IGA), privileged access management (PAM), access management (AM) and user authentication — singly or in combination.

Why This Is Important

The expansion of remote work has greatly accelerated the widespread adoption of SaaS-delivered IAM services; these services are increasingly being used to effectively drive organizations' digital transformation initiatives. The benefits of IAM SaaS offerings include better economics, especially for scaling up or down quickly with reduced operational costs; better reliability; and quicker time to value for new features and functionality.

Business Impact

- SaaS-delivered IAM helps organizations to fill gaps in enterprise IAM portfolios and IAM staffing functions and to achieve faster time to value with reduced reliance on infrastructure.
- SaaS provides standard, consistent IAM functions to support both internal and cloud-based applications.
- Organizations that require a hybrid approach due to a large portfolio of legacy applications will require more effort to migrate entirely to SaaS, which might delay universal adoption.

Drivers

The SaaS delivery model is proven in authentication, representing the default choice in over 90% of cases. This model is also widely adopted in AM and customer IAM (CIAM) use cases, in addition to growing PAM and IGA offerings. The key trends and developments driving the widespread adoption of IAM SaaS offerings are:

- Reduced fear of the perceived risk of SaaS-delivered IAM solutions (availability, security) in favor of the benefits
- Need for effective, quicker time to value and scalable IAM controls to provide secure access to on-premises and cloud applications

- Evolution of matured SaaS-delivered IAM offerings, frequent, easy-to-consume functional upgrades, reduced operational requirements, increased buyer comfort with SaaS-delivered IAM, and significant marketing and sales initiatives from established vendors
- Simpler licensing for SaaS IAM tools (an IAM leader only needing to expand the enterprise's subscription to cover the new pool of remote/standard users)
- Shortage of staff with the skill sets required for software-delivered IAM deployments, including consultants and system integrators (SIs) with these skills
- Converged IAM functionalities, with AM vendors offering robust authentication along with light IGA and PAM functionalities
- Better agility and shorter time to completion than software-delivered IAM, which is particularly important for organizations that manage frequent acquisition and divestiture activities
- Higher total cost of ownership with software-delivered IAM deployments, which includes auditing and documenting people and IT asset costs for owning and managing IT infrastructure, documenting project-related costs for software upgrades, and ongoing support costs and planned obsolescence
- Popular SaaS offerings from a single vendor that may not be able to completely replace broad implemented IAM solutions in all organizations, but that can be used to supplement those solutions and drive digital business initiatives

Obstacles

- Perceived risks of data residency and data security in cloud infrastructures to adhere to regional privacy regulations like GDPR in Europe and CCPA in California
- Other regulatory and legal restrictions pertaining to particular geographies that prohibit the use of SaaS services
- Legacy infrastructure and complex hybrid environments of organizations requiring them to maintain both software and SaaS IAM tools
- Complexity of software implementations for IGA and PAM, which restrains organizations from adoption of SaaS-delivered IAM controls
- Reduced ability to customize
- Risks associated with credential (password) security, especially password vaulting and forwarding of identity data
- Risks associated with service availability and business continuity

User Recommendations

- Identify key business drivers for your IAM vision, which benefit from SaaS-delivered IAM: faster time to value, more reliable and available services, mitigation of staffing concerns for software deployments, and lower cost of ownership.
- Begin with consuming MFA from SaaS if you're not already, followed by AM; both are mature in delivery and adoption. You might migrate PAM next, and IGA last, due to complexity of software implementations.
- Use a responsibility and cost comparison framework for new IAM purchases to ensure appropriate comparisons between software and SaaS-delivered IAM implementations.
- Take a cloud-first approach where application requirements demand a hybrid approach, and think of software solutions as exceptions.
- Evaluate augmenting duplicated software-delivered IAM implementations caused due to mergers and acquisitions with SaaS-delivered IAM solutions to provide standardization and consolidation for all apps and users.

Sample Vendors

Cisco (Duo Security); CyberArk; ForgeRock; Microsoft; Okta; OneLogin; Oracle; Ping Identity; SailPoint; Saviynt

Gartner Recommended Reading

How to Choose Between Software and SaaS Delivery Models for Identity and Access Management

Buyer's Guide for Access Management

Buyers' Guide for Privileged Access Management

Buyer's Guide for IGA: Top 4 Elements of a Successful RFP

OpenID Connect

Analysis By: Henrique Teixeira

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

OpenID Connect (OIDC) is an identity layer on top of the OAuth 2.0 protocol that enables web services to externalize authentication and authorization functions to a third party. It allows clients of all types, including web-based, mobile and JavaScript clients, to corroborate the identity of an end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user in an interoperable and JSON/REST-like manner.

Why This Is Important

OIDC's promise is that it will meet the needs of organizations looking to authenticate users accessing resources via browsers or APIs. It also uses a more lightweight JSON and RESTful approach than XML-based standards, such as SAML and WS-Federation.

Business Impact

OIDC offers a more modern and efficient alternative to SAML. Its biggest benefits are:

- Improving user experiences through lightweight authentication and authorization and fine-grained consent management.
- Reducing the data entry burden during user registration, and providing single sign-on and federation support for modern apps.
- Improving discovery, defining where a user should authenticate (i.e., through webfinger). Also, better support for key discovery.
- Improving connection maintenance.

Drivers

- RESTful approaches like OIDC are increasingly favored for new development and implementations. There is an increase in interest in the protocol, and it has replaced SAML in terms of preference for new applications.
- Version 14 of the draft for the OIDC federation specification was published in April 2021.
- OIDC has successfully proven to allow identity interactions to be conducted more seamlessly and with less friction for developers than XML-based standards, such as SAML, or purely proprietary implementations, and with greater security than earlier versions of OpenID.
- Finance, government and healthcare institutions can benefit from its increasing work to profile OIDC specifications to support and be fine-tuned to be used by industry verticals.
- Other drafts in the work include the shared risk signals and identity assurance working groups, as well as the OIDC profile for SCIM services, which client applications may use to discover availability of and register for, and access, SCIM services.
- All access management (AM) vendors Gartner surveyed for the latest Magic Quadrant for Access Management provide support for OIDC. Dozens of organizations like Microsoft, Google, Salesforce, PayPal, Red Hat, VMware and Verizon have products or services that have been certified against server conformance profiles of OIDC.
- OIDC is the protocol of choice for “greenfield” scenarios. The benefit the protocol will have on API access controls, privacy regulation, consent management, step-up authentication, compliance and implementation of adaptive access will accelerate its time to achieve plateau and become mainstream.

Obstacles

- The list of SaaS applications supporting OIDC continues to grow; however, its growth is slower and has a smaller market penetration than SAML. Gartner estimates that less than 15% of SaaS applications support OIDC.
- Some AM and SaaS application vendors still do not support all of the OIDC specification extensions because extensions to the standard continue to be defined and refined (i.e., best practices for the implementation of implicit authentication flows are being revisited).

User Recommendations

- Give preference to OIDC over SAML. Use OIDC for modern application “greenfield” developments.Finance, government and healthcare institutions should evaluate OIDC for its industry applicability defined in drafts from working groups.
- Leverage an AM tool that supports multiple protocols and can do translation among protocols, especially between SAML and OIDC, and other proprietary security token formats.
- Ask application vendors to increase support to OIDC, providing an alternative to SAML for both authentication and authorization to services. Prioritize the adoption of at least the core portions of the standard.
- Use OIDC for user authentication, not for machine identities like services and devices.
- Don’t use OIDC for protecting APIs behind an API gateway. Use JWTs for that.

Sample Vendors

Auth0; Cloudentity; ForgeRock; Gluu; Google; IBM; IdentityServer; Microsoft; Okta; Ping Identity

Gartner Recommended Reading

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

IAM Leaders’ Guide to Access Management

Critical Capabilities for Access Management

Building Authentication, Authorization and SSO Into API-Driven Apps

Climbing the Slope

EAM

Analysis By: Felix Gaehtgens

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Externalized authorization management (EAM) provides runtime controls — including policy management, policy enforcement, and decision modeling — for fine-grained authorization to infrastructure, applications, services, transactions and data. EAM is also sometimes referred to as “dynamic authorization.” EAM solutions usually offer a centralized policy server and can implement multiple authorization methodologies, including attribute-based/role-based access control (ABAC/RBAC).

Why This Is Important

EAM delivers security and lower maintenance due to a tighter, integrated and standardized common policy mechanism (what is allowed, and under which circumstances, for example). EAM defines and orchestrates authorization policies across different applications, systems and services (instead of having to define policies separately for every one of them). It can add fine-grained runtime authorization to DevOps tools, cloud resources, microservices and applications.

Business Impact

EAM is a long-term investment in an architecture for granular control of application and data access:

- Its use in applications and data systems can significantly change the consistency, flexibility and granularity of authorization.
- It results in better access control, audit and compliance results over a broader set of infrastructure, applications, services, transactions and data.
- It helps developers save time by focusing on delivering functionality while outsourcing access decisions to the EAM tool.

Drivers

EAM was a niche technology for the last decade, where it was used predominantly in large and complex environments that feature significant custom development. Its use case focused on providing a runtime authorization layer across multiple components or applications. Attribute-based access control (ABAC) was another driver for its adoption, with its capability to use dynamic runtime attributes and additional context rather than the more limited and static role-based access control (RBAC).

Typical examples of strategic deployments are in healthcare, airline ticketing systems, banking systems, or supporting trading or supply chain systems that consist of a large number of custom-developed components into which EAM can be integrated.

EAM was also used by organizations to provide more fine-grained access control consistently over distinct applications such as Microsoft Dynamics 365, SAP, or SharePoint that supported integration with EAM tools through proprietary mechanisms.

In recent years, EAM has become more popular, and importantly, more accessible because of several drivers:

- Compliance continues to be a key driver for EAM — an example being privacy regulation such as CCPR, GDPR, and LGPD, which require organizations to support more-granular data access authorization. Much of this is in combination with customer identity and access management (CIAM) initiatives.
- While the predominant standard for EAM has been the Extensible Access Control Markup Language (XACML), nowadays much traction happens around the Open Policy Agent. It supports out-of-the-box integrations for policy enforcement with many common components in cloud-native and DevOps architectures.

Additionally, recent acquisitions in the space have happened:

- Ping Identity acquired Symphonic Software in late 2020.
- Twilio acquired Ionic Security in 2021.

Obstacles

- Externalized authorization requires thoughtful planning from the design phase. Retrofitting dynamic authorization into existing applications is difficult. This is because often, applications spread authorization functions to many places within the code. Many commercial off-the-shelf applications do not offer APIs for authorization to be externalized in a plug-in manner. Instead, integration external authorization can only be loosely coupled: translation of policies into a set of entitlements, and creating tokens with those entitlement combinations for users accessing the applications.
- For developers to fully embrace EAM and be productive, they will require an easy-to-use self-service interface for policy design and testing. EAM has a learning curve and associated complexity.
- EAM requires strong governance to be in place for data and entitlements that are used as input to access decisions. Consequently, data quality has a direct impact on the viability of data-driven ABAC rules.

User Recommendations

- Use EAM to replace custom authorization code for decision and enforcement from homegrown applications with an easier-to-maintain, consistent framework for centralized policy management.
- Socialize your plans and set solid foundations for EAM by offering self-service functions and ensuring buy-in from developers.
- When evaluating EAM solutions, conduct evaluations against two sets of requirements: policy management services and policy runtime services (decision and enforcement).
- When looking to retrofit existing applications with EAM, choose tools that cover immediate needs by integrating with security tokens that deliver entitlement, but also provide standardized authorization methods (typically XACML and/or OPA support) for future developments.
- Mandate robust management of attributes and data that is used in policy evaluation, because EAM requires it.
- Explore integration with API gateways and AM tools to extend the scope of authorization and enhance the overall security posture.

Sample Vendors

Axiomatics; ForgeRock; Jericho Systems; NextLabs; ObjectSecurity; Ping Identity; PlainID; Styra; WSO2

Gartner Recommended Reading

Architecting Modern Policy-Based Runtime Authorization

Guidance for Modernizing Authorization Architecture

Customer IAM

Analysis By: Michael Kelley, Henrique Teixeira

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Customer identity and access management (CIAM) tools manage identity, authentication and authorization for external identity use cases. Functionality includes self-service capabilities, adaptive access, SSO and bring your own identity (BYOI). CIAM vendors also offer identity governance, analytics and reporting through identity repositories, and APIs and SDKs for mobile applications. Optionally, vendors may offer fraud detection and privacy features.

Why This Is Important

In a world where user interactions with any business are increasingly digital, CIAM is the glue that builds and keeps those relationships. CIAM is necessary for public-facing applications that require users to register identities and create accounts. It facilitates good digital experiences and ensures security and compliance of those interactions. Privacy regulations and increased dependence on remote interactions have intensified the importance of CIAM to businesses and their customers.

Business Impact

CIAM can improve user experience (UX), security and compliance in the following use cases:

- B2C: Online shopping, banking, insurance and financial services

- B2B: Partner collaboration, supply chain activities, manufacturers selling to retailers or insurers selling services through brokers
- G2C: Public sector and government portals targeting citizens looking to interact with government entities
- Gig economy: Temporary worker access

Drivers

- UX — By 2021, 86% of organizations will compete on the basis of UX; in industries with very little competitive differentiation between products and services, the online experience becomes the differentiation. In addition to existing and longtime online e-commerce services, suppliers of services normally purchased in person are now providing them online.
- Privacy regulation — From GDPR in the EU, to LGPD in Brazil, to CCPA and CPRA in California, growth in privacy regulation is driving growth in CIAM adoption. The need to comply with privacy regulations, from collecting consent to managing the need to be forgotten, is a primary component in providing customer protections across all online businesses. These developments have moved CIAM further along the Hype Cycle based on increased adoption in the market and maturing IAM functionality. While CIAM vendors and software can't comply with privacy regulation on behalf of an organization, they can provide the necessary technical mechanisms to enable an effective compliance program.
- Buy versus build — Organizations are adopting more commercially available CIAM technologies, and there is growing preference for buying versus building. Some key elements of CIAM for CX include lightweight marketing functions, customer analytics, insights and customer engagement features. CIAM improves CX with adaptive access control, self-service profile and password management, and BYOI integration options.
- Economics — For many companies, the cost of maintaining a homegrown CIAM tool, with the added complexity of fraud and privacy, has become more expensive compared to commercial offerings.
- CIAM-only vendors are slowly being squeezed out of the market by multiconstituency vendors, especially as the native CIAM capabilities of those vendors have grown.

Obstacles

- While CIAM tools are very capable in identity administration and access management capabilities, native functionality for online fraud prevention and preference and consent management is not yet mature, or even included in most commercial CIAM tools.
- While we see the CIAM market expanding quickly, only 40% of organizations currently have a CIAM tool. Many of these, either driven by the desire to control the platform or facing organizational challenges, still support a homegrown CIAM tool.
- Many customers are continuing to manage vendor and business partner identities using internal and manual processes, ignoring the ability of CIAM tools to manage B2B relationships.
- Acquisitions are prevalent in this market, sometimes causing confusion about vendor choice and potentially hindering growth. CyberArk purchased Idaptive in 2020, and Okta purchased Auth0 in 2021; we expect that activity to continue as more vendors work to capture a larger percentage of the growing CIAM market.

User Recommendations

- Don’t develop CIAM capabilities that vendors can offer out of the box. Prioritize adoption of a commercially available CIAM tool, as it can bind different processes related to identity administration, access management, fraud detection, identity governance and directory services in a single platform.
- Capture the significant business value driven through marketing, sales and CRM integrations with CIAM as the focal point.
- Use the intelligence provided by CIAM tools’ identity analytics and reporting features to dynamically discover and respond to customer preferences and requirements.
- Develop a privacy strategy for customers. If your requirements are light, CIAM tools’ native consent and preference management capabilities may be sufficient; otherwise, pair CIAM capabilities with a consent and preference management tool for advanced functionality.
- Work with fraud leaders to augment CIAM with online fraud detection tools in industries like healthcare, financial services and retail.

Sample Vendors

Akamai; ForgeRock; LoginRadius; Microsoft; Okta (Auth0); OneLogin; Ping Identity; SAP

Gartner Recommended Reading

Technology Insight for Customer Identity and Access Management

Top Trends in Customer IAM Solution Design

Critical Capabilities for Access Management

Buyer's Guide for Access Management

IAM Managed Services

Analysis By: Kevin Kampman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

IAM managed services provide outsourced operations management, support and maintenance for IAM technologies. These services are provided typically as an extension of system integration services delivered by IAM solution vendors or IAM professional services firms. IT outsourcing firms also provide these services in the form of staff augmentation, supplying personnel to perform engineering and operational functions as part of their clients' IAM teams.

Why This Is Important

IAM managed services have become a viable alternative for developing and maintaining the various IAM functions in organizations. Cross-application visibility, vendor interaction, experienced resources and operational improvements are several of the attractions of this alternative, in addition to accelerated project realization.

Business Impact

Managed services provide a cost-effective way to:

- Gain support outside of working hours.
- Address staffing shortages.

- Access IAM deployment experts.
- Delegate continuous support to a third-party provider.

The key benefit from IAM managed services is greater flexibility supporting business operations. For organizations with highly customized IAM solutions, IAM managed services provide a solution to staffing issues either through out-sourced or SaaS models.

Drivers

- IAM managed services address the difficulty organizations face in attracting, training and retaining personnel with the right skills to deploy and manage IAM solutions. New leaders tasked to adopt IAM, particularly in midsize enterprises and organizations replacing their existing IAM are challenged to source skilled resources.
- It satisfies the need for round-the-clock support for global IAM deployments. IAM managed services are a realistic option for organizations without the ability or desire to directly staff these functions. This demand will follow digital transformation initiatives and will be timed as organizations increase their adoption.
- It fills the gap between traditional operational support models for on-premises and SaaS IAM solutions, facilitating the evolution of IAM technologies from complex on-premises deployments toward commoditization. Once an IAM technology becomes commoditized through repetition of common deployment and integration patterns, it becomes feasible for services firms familiar with particular vendors to deliver some aspects of that technology through a hosted model.
- It provides a uniform and economical approach. Cloud-architected IAM solutions such as single sign-on (SSO) and coarse-grained administration for cloud applications have become commoditized, and support is split between product vendors and managed services firms. Identity governance and administration (IGA) and privileged access management (PAM) have seen growth in the available cloud-architected solutions, however IGA solutions often require managed services support due to their complexity.
- Continuing support for complex on-premises access management deployments for customers. In addition, these firms and newcomers are now providing support for customers' adoption of PAM and IGA technologies for cloud, hybrid or on-premises deployments.

Obstacles

- Client adoption will be challenged by confidentiality and performance expectations. IAM managers will need to become more skilled in monitoring requirements and performance expectations in addition to developing and managing service-level agreements and change management.
- IAM vendors maintain their competitive edge through the release of new features as well as acquisition of other vendors. Clients and service firms must anticipate that as advances and business conditions change, their relationship is structured to allow for mutually beneficial adaptations.
- Responsibility for expansion of its offerings will fall to the managed service provider, who in turn needs to inform its clients about additions and improvements.
- Managed services business models will be constrained by vendors and their sales motion, licensing models and established client relationships.

User Recommendations

- Catalog use cases for transitioning to delivery of IAM services using cloud-architected models or to leverage the flexibility and agility that an MSP offers.
- Identify vendors that have developed methodologies for specific products that extend to required applications, supported by repeatable processes that can be delivered remotely from an operations center. This operations center offers monitoring and proactive support for activities like integration, patching and issue resolution.
- Establish long-term contracts where solutions are stable, and evaluate providers and their solution sets based on the convenience and applicability of solutions. Relationships with managed service providers may help to augment adoption of SaaS solutions.
- Track the evolution of supported services toward commoditization when utilizing IAM managed services, as such services may transition to a SaaS-delivered IAM directly or remain with the MSP.

Sample Vendors

Accenture; Capgemini; Clango; Computacenter; IDMWORKS; Optiv Security; Simeio; Tata Consultancy Services; Wipro

Gartner Recommended Reading

Best Practices for Engaging With Identity and Access Management Professional Services FirmsToolkit: Selecting IAM Professional Services

OAuth 2.0

Analysis By: Abhyuday Data

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

OAuth 2.0 is an authorization framework that is designed to protect APIs and services accessed from any type of application. The applications (clients) can be native applications, browser-based, JavaScript-based applications, services or web applications. OAuth 2.0 defines an authorization server that issues tokens to clients, which then make authorized API calls to the resource server (services) with these tokens. The resource server then validates, authorizes or rejects the access tokens.

Why This Is Important

OAuth 2.0 is an authorization framework and the underpinning for other identity protocols like OpenID Connect (OIDC). OAuth 2.0 enables organizations to instantly, and at scale, handle authentication and authorization to and from applications and services, and is commonly used to protect RESTful APIs and services. OAuth 2.0 also has built-in capabilities to handle privacy and can enable impersonation, delegation, consent and obfuscation of personally identifying information (PII) when needed.

Business Impact

OAuth 2.0 authorization framework helps IAM leaders streamline authentication and authorization decisions for web, mobile and single-page apps; APIs; microservices; and Internet of Things (IoT) use cases. OAuth 2.0 uses token formats, such as JSON Web Token (JWT), which is digitally authenticated, encrypted and trusted to transfer data between various parties. Use of OAuth 2.0 improves an organization's internal architecture where JWT works as bearer tokens to make implementations easier.

Drivers

- OAuth 2.0 and its derivative standards are fundamental in API access control techniques used in access management (AM), API security and API gateway technologies.
- There is a need to support authentication and authorization decisions for modern targets like web apps, mobile and single-page apps; APIs; microservices; and IoT devices.
- Legacy identity protocols, like Kerberos and API keys, cannot meet the security, privacy, usability and scalability requirements for modern target applications and services.
- There is the need to improve an organization's internal authentication and authorization architecture to make implementations easier and deployments flexible.
- There is the need to enable privacy-preserving authentication and authorization and comply with the growing adoption of regional yet global privacy regulations where end users can allow or deny access to their data.
- All AM vendors Gartner surveyed for the latest Magic Quadrant for Access Management provide support for core OAuth 2.0. The support of OAuth 2.0 and other modern identity protocols lays down a foundation of success for broader AM programs.

Obstacles

OAuth 2.0 faces some minor challenges in mainstream adoption:

- OAuth 2.0 adds more complexity than legacy protocols like Kerberos do. Along with that, OAuth 2.0 is an evolving framework, and, in some cases, there are no best practices clearly yet defined for specific use cases. Gartner clients frequently ask about the usage of OAuth flows, tokens to be used and storage of credentials.
- Many organizations still possess legacy systems where technologies like Kerberos, certificates, API keys or just username and passwords will continue to be adopted and deployed by organizations, often regrettably, until the day the last legacy system that requires them is decommissioned.

User Recommendations

- Continue to use and deploy OAuth 2.0 to abstract authorization, and balance security, privacy, usability and scalability. OAuth 2.0 and, specifically, the use of the JWT token format have become the standard to implement access control for applications and services.
- Prioritize evaluating OAuth roadmaps for AM, API security and API gateway tools. OAuth 2.0 is a framework, not a single protocol. OAuth 2.0 is constantly evolving to solve new use cases and scenarios.
- Use the right flow for the right type of application. A native application, a service and a single page web application have different security capabilities and must be treated differently.
- Leverage newer capabilities intended to better secure OAuth 2.0 interactions, such as token exchange, Mutual-TLS (MTLS) client authentication and Proof Key for Code Exchange (PKCE).
- Use the OIDC specifications that are built on top of OAuth 2.0 to define more granular and controlled access across different domains for user authentications.

Sample Vendors

Akamai; ForgeRock; IBM; Keycloak; Microsoft; Okta; Oracle; Ping Identity; SAP

Gartner Recommended Reading

IAM Leaders' Guide to Access Management

Buyer's Guide for Access Management

Modern Identity and APIs: OpenID Connect, OAuth 2.0 and SCIM 2.0

Building Authentication, Authorization and SSO Into API-Driven Apps

Biometric Authentication Methods

Analysis By: Ant Allan, Tricia Phillips

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Biometric authentication methods use unique morphological or behavioral traits to corroborate a person's claim to an identity previously established for access to an electronic or digital asset. A biometric authentication method typically uses a one-to-one comparison ("verification") to support an identity claim. Rarely, a method uses a one-to-many search ("identification"): The person simply presents a biometric trait and the system finds one or more candidate matches from a larger population.

Why This Is Important

User authentication is fundamental to identity-first security. It must provide sufficient credence in an identity claim to bring account takeover (ATO) and other digital-identity risks within an organization's risk tolerance. Unlike other types of authentication credential, biometric traits are inherent to a person. Thus they cannot easily be shared or stolen and potentially free the person from having to remember a password or carry a token.

Business Impact

Identity and access management (IAM), fraud and other security leaders across all industry verticals and geographies can benefit from investment in biometric authentication methods, which can:

- Be adopted in a wide range of use cases for employee and customer authentication
- Be used alone or as an element of multifactor authentication (MFA)
- Enable passwordless authentication
- Improve trust and accountability
- Improve user experience (UX)

Drivers

- Ubiquity of device-native biometric methods in smartphones and increasing availability of this in other endpoint devices, including Microsoft's support for face and other modes in Windows Hello for Business in Windows 10. This in turn drives interest in third-party biometric methods that can make use of standard inputs (camera and microphone). These offer organizations greater control over configuration, enrollment, choice of modes, consistency across devices and channels, and improved customer trust.
- Increasing interest in, and successful deployments of, passwordless authentication, as a way to avoid the vulnerabilities, risks and frustration that passwords engender, including: (1) embedding device-native or third-party methods in customer-facing mobile apps, especially in banking; (2) proprietary passwordless **mobile MFA** tools that incorporate device-native or third-party methods within a smartphone app; and (3) **Fast IDentity Online (FIDO) authentication protocols,** especially FIDO2 (although FIDO doesn't demand the use of biometric methods).
- Increasing adoption of **document-centric identity proofing** for customer onboarding and a desire to leverage biometric face recognition data for customer authentication and identity recovery across multiple channels. This also extends to employee authentication, especially for gig workers. This specifically drives interest in third-party methods with centralized architectures.
- Successful use of voice recognition in contact centers as a welcome alternative to knowledge-based verification (KBV), which people often find frustrating and attackers readily defeat (and thus it provides very little confidence in an identity). Voice recognition is also a natural fit for virtual personal assistant (VPA or "smart speaker") use cases.

Obstacles

The following issues may deter adoption, especially regarding third-party methods rather than device-native methods:

- Usability and reliability vary across modes, populations and use cases, limiting the success with any single technology.
- Demographic bias, especially in methods using machine learning, can discriminate against certain groups, impairing security as well as UX.

- As biometric traits cannot be “reset,” effective biometric methods must corroborate genuine human presence; thus, presentation attack detection (PAD; i.e., “liveness testing”) is essential. However, some PAD techniques can add friction, leading to poorer UX.
- Concerns about replay and injection attacks, which are more scalable than presentation attacks and likely present a greater risk.
- Privacy laws are seen as a barrier, but compliance really only adds some bureaucratic hurdles. Data security controls are seen as a major obstacle but are only prudent anyway.
- Some people might view the use of biometric methods as creepy.

User Recommendations

- Use biometric methods (solely or as an element of MFA) as a way of achieving passwordless authentication.
- Prefer third-party methods over device-native methods for improved trust and accountability (including robust enrollment), multichannel support, and (for face) integration with document-centric identity proofing.
- Choose tools that reflect both the diversity of and personal preferences among the target population.
- Choose tools that demonstrate genuine human presence. Carefully evaluate vendor claims and favor methods tested in conformance with ISO/IEC 30107-3:2017. Be wary of PAD techniques that add friction and potentially erode UX benefits.
- Evaluate how vendors can mitigate replay and injection attacks.
- Reduce privacy concerns by paying full attention to nontechnical regulatory requirements as well as architectural and data security issues. Be open and transparent about how the data is used.

Sample Vendors

Auraya Systems; Aware; Daon; FaceTec; Fujitsu; IDEMIA; iProov; Ipsidy; Nuance; Veridas

Gartner Recommended Reading

Technology Insight for Biometric Authentication

Market Guide for Identity Proofing and Affirmation

IAM Leaders' Guide to User Authentication

Entering the Plateau

DCIP

Analysis By: Akif Khan, Jonathan Care

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Document-centric identity proofing (DCIP) involves capturing an image of a photo identity document and checking for signs of tampering or forging. In addition, capture and analysis of a photo or video clip of the person determines genuine presence. Finally, comparison of the photo with the one in the document determines if the person is the legitimate document bearer. Optionally, data can be extracted via OCR or from the document's chip using NFC.

Why This Is Important

Establishing confidence in identity is the foundation of many digital interactions involving customers or employees. While that need has been persistent, the need for high-assurance, remote identity proofing has become even stronger as a result of the COVID-19 pandemic. Put simply, document-centric identity proofing allows organizations to have confidence in who is on the other end of that digital interaction.

Business Impact

DCIP can be a key enabler of remote employee or customer interactions where a high level of assurance in the claimed identity is needed for fraud prevention or compliance purposes.

These use cases can include onboarding or account creation, account recovery scenarios, or to elevate trust during a high-risk activity, such as a large funds transfer. This can be an alternative to using an orthodox credential-based authentication method for such events.

Drivers

- The relentless pursuit of digital transformation has led to the majority of businesses offering the ability to register for services online. This trend is most apparent in financial services, in which the regulation related to KYC demands high confidence in a customer's identity. The COVID-19 pandemic further accelerated this trend when, in the face of local bank branches being closed, the digital channel became the only medium through which new customers could be onboarded.
- The move to remote working also created a need for remote identity proofing. In a world where a person could apply for a job, be interviewed, land the job and then start work without ever meeting their employer face-to-face, organizations needed to adapt their process. Showing your passport to HR on your first day in the office is no longer a possibility.
- The convergence of identity proofing and authentication presents opportunities to leverage document-centric identity proofing beyond the point of registration. The process can be deployed to establish confidence in identity at high risk events such as credential recovery. Alternatively, the selfie data obtained during the identity proofing process can be used as an authentication credential, enabling features such as "login via selfie." This results in a tight coupling between the authentication event and identity proofing event.
- The increasing obsolescence of data-centric techniques that rely on a user entering PII data which is then checked against sources such as credit bureaus, electoral rolls or, in some regions, government databases. In the face of continual breaches of data, it is prudent to assume that all PII data is known to everyone.

Obstacles

- With usage costs as high as several dollars per event, the technology can be prohibitive for many use cases. Outside of regulated industries where such costs are accepted to maintain compliance, difficult decisions need to be made in which cost is balanced against the tolerable level of confidence in a user's identity.
- The user experience of taking a picture of an identity document and then taking a selfie is considered too onerous by some. Questions persist about dropout rates. It also cannot be assumed that everyone has a smartphone or front-facing webcam and can engage in the process in the first place.

- Concerns persist regarding demographic bias in the face recognition process. Some vendors are transparent about their performance in this respect. Other vendors are more opaque, resulting in suspicion filling the void. Many organizations, focusing on both ethics and averting brand damage, rightly want to ensure that the identity proofing process is fair across race, age and gender.

User Recommendations

- Assess whether document-centric identity proofing is required for your use case(s). This can be done by asking stakeholders this critical question: "In addition to seeking evidence that the real-world identity exists, is it a requirement to have a high level of assurance that the rightful claimant of that identity is genuinely present in the digital interaction?"
- Manage a carefully considered vendor selection process by following the guidance in Buyer's Guide for Identity Proofing.
- Future-proof your identity proofing and onboarding process by leveraging an orchestration solution, to deliver the integration, with your chosen document-centric identity proofing vendor. This allows you to also easily use additional vendors for data-centric affirmation, fraud detection or AML checks as required.
- Recognize that while document-centric identity proofing can be a key pillar of a mandated KYC process, it does not constitute the entirety of that process, even when vendors describe it as "eKYC."

Sample Vendors

Acuant; ADVANCE.AI; AuthenticID; IDmission; Intellicheck; Jumio; MiTek; Onfido; ReadID; ZOLOZ

Gartner Recommended Reading

Buyer's Guide for Identity Proofing

Market Guide for Identity Proofing and Affirmation

EDRM

Analysis By: Ravisha Chugh, Mario de Boer

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Enterprise digital rights management (EDRM) is a technology used to apply mandatory access and usage control on unstructured data such as email messages, office documents and CAD diagrams. EDRM combines cryptography with identity policies to restrict if and how data can be accessed and used. EDRM-protected content is typically accessed via applications that natively support EDRM, an EDRM endpoint agent, plug-ins, wrappers, web browsers or secure viewers.

Why This Is Important

EDRM, also known as information rights management (IRM) provides persistent protection of data. The main objective of EDRM is protecting sensitive data, which can be met by several alternative technologies. EDRM is often deployed in a context where it makes sense to implement adjacent technologies for slightly varying use cases. It makes perfect sense to combine products, such as to have a classification or DLP product apply EDRM protection on detection of sensitive content.

Business Impact

- EDRM can safeguard intellectual property from loss, protect against inappropriate or unintended disclosure of proprietary or confidential enterprise information, and allow data owners to audit and adjust access to specific data wherever it resides.
- EDRM can be used to retain control of unstructured data transferred to business partners in secure collaboration scenarios.

Drivers

- Intellectual property protection and data privacy are important especially among financial services, pharmaceutical and product development/engineering firms.
- The rise of Microsoft's Azure Information Protection (AIP) has changed the market's dynamics. Most of the Office 365 plans have also included a form of Rights Management Services (RMS), and AIP combines RMS capabilities with a mechanism for applying sensitivity labels to content. AIP has significantly raised awareness for and interest in EDRM.

Obstacles

- EDRM policy management can be complex and may result in failure of projects.
- EDRM deployments can be used to limit complexity, but doing so may not realize all use cases for EDRM in the organization.
- Deploying EDRM without understanding how in-scope data is used and moves inside and outside of the organization for the full data life cycle will have a high likelihood of failure.
- Many organizations cannot define scenarios and use cases well enough to warrant a successful EDRM deployment.
- EDRM is difficult to deploy at large scale. Dependency on endpoints and applications is one reason, but this is trumped by overly ambitious deployments and scope without proper planning.

User Recommendations

- Evaluate EDRM as a persistent protection mechanism only when its benefits outweigh its significant planning, ongoing management and user training demands.
- Focus only on well-defined scenarios in which the content must protect itself regardless of where it is stored — for example, local copies of documents saved to unmanaged devices. For such scenarios, alternative/adjacent technologies (e.g., DLP, CASB, watermarking, etc.) are ineffective or cannot be deployed.
- Combine EDRM with data classification, and integrate EDRM with file repositories and business applications to achieve automatic and consistent policy enforcement.
- Assess the full life cycle of protected content across all forms of processing, including inspection, indexing, discovery, and retention/archiving.
- Address the cultural changes you introduce. EDRM may impact many common workflows for all users in your organization. Help users with training, mature classification tools and processes.

Sample Vendors

Adobe; Fasoo; HelpSystems; Ionic Security; Micro Focus; Microsoft; NextLabs; SealPath; Seclore; SECUDEe

Gartner Recommended Reading

How to Implement Enterprise Digital Rights Management to Control Unstructured Data

Market Guide for Enterprise Data Loss Prevention

Addressing 6 Common Use Cases for Unstructured Data Security

Privileged Access Management

Analysis By: Felix Gaehtgens, Michael Kelley

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Privileged access management (PAM) tools help organizations secure privileged (i.e., administrative) access to critical assets and meet compliance requirements. PAM tools offer features that: discover and manage privileged accounts and keys on systems, devices and applications; automatically randomize, manage and vault passwords and other keys; control access to privileged accounts, including shared and emergency accounts; isolate, monitor, record, audit and analyze privileged access sessions.

Why This Is Important

Privileged access is risky by nature: many breaches can be attributed to privileged access misuse, stolen privileged credentials or hijacked privileged accounts. Privileged accounts require elevated security because they can often bypass security controls that other users are subject to, and could be leveraged to gain further access. Yet, many organizations lack maturity in properly managing privileged access. PAM technology exists to manage the risk and offer controls for this type of access.

Business Impact

PAM tools can:

- Minimize the risk arising from privileged accounts and access.
- Detect and prevent unauthorized use of privileged access.

- Reduce the overall attack surface.
- Allow robust and granular control, transparency, scalability and more accountability for privileged access compared to manual controls and custom or generic tools.
- Manage machine identities.

These functions help organizations instill good security hygiene and meet audit and compliance requirements.

Drivers

- Interest in PAM tools continues to grow, with many organizations identifying PAM as a top 10 security control.
- The growing number of cyberattacks involving misuse of privileged access continues to fuel the adoption of PAM tools.
- While PAM adoption is mature and mainstream for medium to large organizations, smaller organizations are quickly catching up. Overall, for small organizations, PAM shows signs of early mainstream adoption.
- Support for legacy use cases such as brokering privileged access to individual (often shared) privileged accounts is mature.
- Newer use cases such as just-in-time privileged access and zero standing access are gaining traction with organizations, and many vendors are adding functionality.
- Remote privileged access has been a significant driver of adoption even before the COVID-19 pandemic, but the pandemic has further fueled emphasis of this use case.
- Adoption of machine identity management use cases is premainstream. PAM tools can address some of these use cases natively, but not all. Vendor activity is bringing new stand-alone tools to market for secrets management.
- PAM tools are increasingly adopted within industries that have significant operational technology (OT) and industrial control system (ICS) footprints to secure that type of infrastructure.
- Use cases around managing privileged access in IaaS are leading to a new class of tools called cloud infrastructure entitlement management (CIEM).

Obstacles

Privileged access is found everywhere in an organization, however:

- Many organizations start PAM initiatives with a reduced scope and without a roadmap for broader and more difficult, but essential, aspects such as machine identity management.
- Some organizations do not take advantage of more advanced just-in-time and zero standing privilege processes — a “business as usual” approach does not adequately address privileged risk.
- Additionally, some vendors focus on selling only initial PAM capabilities, or on immediate buyer needs such as privileged remote access. The functional maturity of PAM solutions available on the market thus differs significantly.

PAM for the cloud has additional needs that some vendors struggle with, such as:

- The delivery as a distributed hybrid model, that not all PAM vendors can easily comply with.
- Some traditional licensing models (per target) are also not prepared for dynamic infrastructure with fluctuating numbers of target systems.

User Recommendations

- Create a new operational model for privileged access that includes just-in-time privileged access and zero standing privileges. Involve users in the planning for changes to process and working practices.
- Avoid overlooking machine identities such as service and software accounts — they are a considerable source of security and operational risk.
- Implement a continuous discovery and onboarding mechanism for privileged accounts - including machine IDs.
- Record all privileged activity and establish audit capability by leveraging analytics and creating procedures on when and how activity will be manually reviewed.
- Ensure that administrative accounts for network devices, hypervisors, IaaS, PaaS and SaaS are within scope as well.
- Ensure that your solution is highly available as failover, disaster recovery planning and emergency access are crucial for success.
- Integrate PAM tools with SIEM for logging, IGA for life cycle management, and change management/ITSM tools for tighter access control.

Gartner Recommended Reading

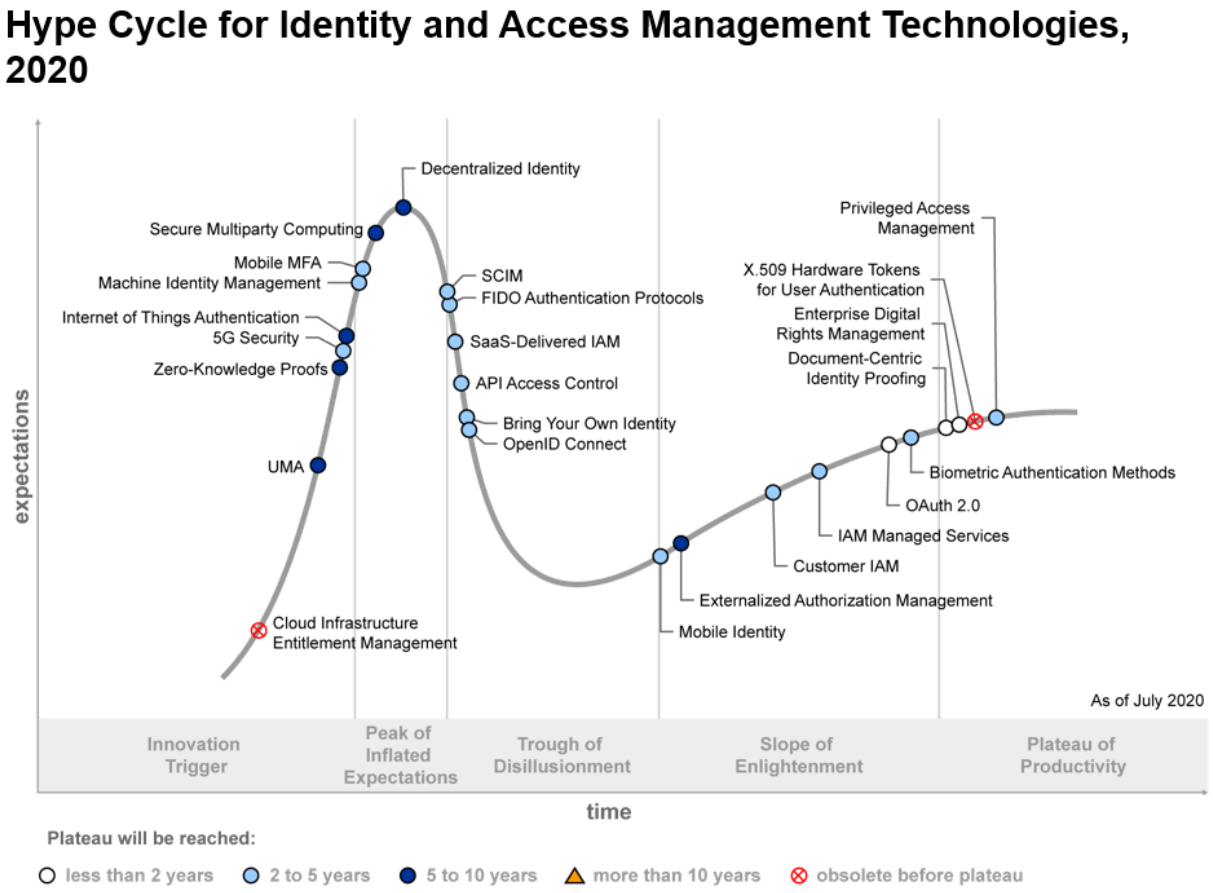
IAM Leaders' Guide to Privileged Access Management

Buyers' Guide for Privileged Access Management

Magic Quadrant for Privileged Access ManagementCritical Capabilities for Privileged Access Management

Appendixes

Figure 2. Hype Cycle for Identity and Access Management Technologies, 2020



Source: Gartner (July 2020)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2021) (required)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2021)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	*Status*	*Products/Vendors*
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2021)

Document Revision History

Hype Cycle for Identity and Access Management Technologies, 2020 - 16 July 2020

Hype Cycle for Identity and Access Management Technologies, 2019 - 2 August 2019

Hype Cycle for Identity and Access Management Technologies, 2018 - 13 July 2018

Hype Cycle for Identity and Access Management Technologies, 2017 - 5 July 2017

Hype Cycle for Identity and Access Management Technologies, 2016 - 6 July 2016

Hype Cycle for Identity and Access Management Technologies, 2015 - 6 July 2015

Hype Cycle for Identity and Access Management Technologies, 2014 - 15 July 2014

Hype Cycle for Identity and Access Management Technologies, 2013 - 23 July 2013

Hype Cycle for Identity and Access Management Technologies, 2012 - 23 July 2012

Hype Cycle for Identity and Access Management Technologies, 2011 - 13 July 2011

Hype Cycle for Identity and Access Management Technologies, 2010 - 19 July 2010

Hype Cycle for Identity and Access Management Technologies, 2009 - 16 July 2009

Hype Cycle for Identity and Access Management Technologies, 2008 - 30 June 2008

Hype Cycle for Identity and Access Management Technologies, 2007 - 21 June 2007

Hype Cycle for Identity and Access Management Technologies, 2006 - 22 June 2006

Recommended by the Author

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

Understanding Gartner's Hype Cycles

Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

IAM Leaders' Guide to User Authentication

IAM Leaders' Guide to Privileged Access Management

IAM Leaders' Guide to Access Management

IAM Leaders' Guide to Identity Governance and Administration

Table 1: Priority Matrix for Identity and Access Management Technologies, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Bring Your Own Identity Decentralized Identity	SMPC	
High	Customer IAM DCIP EDRM OAuth 2.0	Biometric Authentication Methods FIDO IAM Managed Services Machine Identity Management Mobile MFA OpenID Connect Privileged Access Management SaaS-Delivered IAM	IoT Authentication	
Moderate		API Access Control SCIM	CIEM EAM Zero-Knowledge Proofs	
Low			User-Managed Access	

Source: Gartner (July 2021)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase	Definition

Source: Gartner (July 2021) (required)

Table 3: Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2021)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2021)