Hype Cycle for Identity and Access Management Technologies, 2020

Published: 16 July 2020 **ID:** G00450324

Analyst(s): Ant Allan

Several innovations make their debuts in this year's Hype Cycle, as IGA, identity proofing and phone-as-a-token authentication bid their farewells. Decentralized identity teeters at the peak. Changes along the Hype Cycle reflect shifts in interest and adoption, tracking increased digitalization.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

This document was revised on 22 July 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

This Hype Cycle for identity and access management (IAM) emphasizes advancement for innovations that have proven effective in delivering security, risk management and business value, reducing implementation and operational overheads and enhancing user experience (UX), which is becoming as important for employees as it is for customers.

Digital transformation has become a significant driver for many organizations. According to the 2019 Gartner CEO and Senior Business Executive Survey, 82% of CEOs have a digital transformation or management initiative, up from 62% in 2018.

Chances are that your enterprise has already been working on some initiatives supporting digital business transformation and optimization strategies. These may have included programs like modernization of workplace tools, migration to the cloud, integrating SaaS and on-premises applications, work-from-home initiatives, and expanding customer service channels.

In this new decade that has begun with COVID-19, customer and employee interactions are more remote, mobile, virtual and distributed, and this will become part of the fabric of society. The pandemic has suddenly accelerated the shift of work from office to home, as well as the continued movement of commerce from brick-and-mortar to digital channels.

For many enterprises, the global pandemic has compressed years-long strategic change into months, even weeks. For others, it has forced them to adopt approaches that they'd previously been cautious about.

Whatever the timescale and trajectory of the pandemic, IAM leaders will need to plan for a new normal, where the numbers of remote workers and online customers will likely fall from crisis levels but remain higher than they were in the past (industry estimates are 20% to 30%).

This Hype Cycle provides decision-making support to IAM leaders who have already created a vision and roadmap for their IAM programs based on the security and business goals of the organization and the expected value that IAM will provide. This Hype Cycle helps IAM leaders determine which innovations (technologies and standards) can fulfill their vision and roadmap and which may not yet be sufficiently mature.

The Hype Cycle

IAM is a security, risk management and business discipline, encompassing practices, processes and technologies that manage the identities and entitlements of people, services and things, and the relationships and trust among them. Effective IAM technologies equip IAM leaders and their teams to provide the right access for the right reasons, enabling the right interactions at the right time (and with the right UX), to help drive desired business outcomes and digital experience goals.

IAM innovations are spread across the maturity and hype spectrum.

Identity governance and administration (IGA), identity proofing and corroboration, and phone-as-a-token authentication were at the plateau last year and have now moved off the Hype Cycle. However, the latter two have new, specialized iterations, which debut in this Hype Cycle: document-

centric identity proofing and mobile multifactor authentication (MFA). The former continues to evolve and to have its functions incorporated into solutions such as access management and ITSM.

There is further need for more advanced tools to manage the increasing number and granularity of entitlements in hybrid and multicloud environments. Gartner projects the rapid evolution of cloud infrastructure entitlement management (CIEM), which debuts in this Hype Cycle and promises to simplify the implementation of least privilege principles by detecting and removing excessive, unnecessary privileges across these environments.

AM solutions continue to mature their ability to support OAuth2 and OpenID Connect (OIDC) and protect applications with RESTful architectures, but we now see a focus on API access control technologies that deliver additional features not available in full life cycle API management solutions. A SaaS delivery model, adaptive access control and integrated MFA capabilities are becoming commonplace in AM implementations.

PAM adoption grows further in line with increasing awareness that many security breaches stem from privileged account compromises. PAM tools help tighten control, monitor the use of privileged accounts (by both people and software), and enable DevSecOps initiatives and infrastructure as a service (IaaS) agility. PAM tools are consolidating their support for just in time (JIT) privileged access and the ability to manage finer-grained privileged access to SaaS control panels.

Fast IDentity Online (FIDO) authentication protocols shift beyond peak but are integral to the evolution of new passwordless mobile MFA options, which are climbing to the peak. Mobile identity, which made its unheralded debut in last year's Hype Cycle, also contributes to adaptive authentication and access approaches that enhance UX and resilience.

Internet of Things (IoT) authentication remains nascent, and we also see the emergence of tools that facilitate trust in a wider variety of machine identities associated with not just devices but also "machines" that enable agile development and application delivery (for example, virtual machines and containers) as well as enhancing business workflows (for example, robotic process automation [RPA] bots).

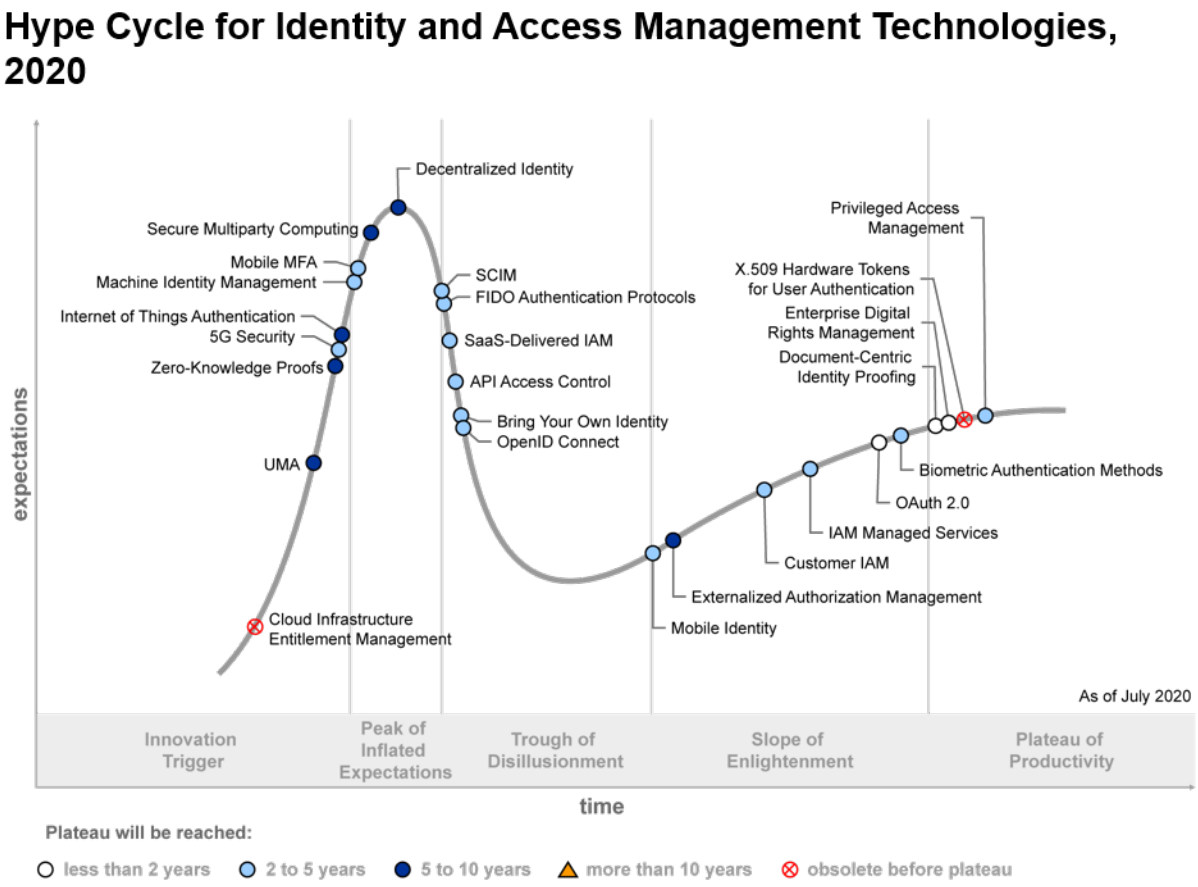
Biometric authentication methods still face barriers to movement up the slope, from privacy concerns and potential vulnerabilities to presentation and infrastructure attacks. X.509 hardware tokens for user authentication are a mature mainstream technology, but adoption is largely constrained to Windows PCs and network login in risk-averse enterprises or where mandated by regulations. Other technologies with broader applicability will render them obsolete before the plateau.

Decentralized identity now sits at the peak; however, we have extended time to plateau. Practical blockchain-based solutions were overhyped and have made less headway than expected. Furthermore, effective solutions will depend on secure (formerly "privacy-enhanced") multiparty computing and zero-knowledge proofs, which have longer timescales. Meanwhile, bring your own identity (BYOI) slides toward the trough due to inconsistent global identity offerings. User-managed access (UMA) has made some further progress with production implementations, but it is still at an early stage of adoption.

Gartner has added the following innovation profiles for the 2020 IAM Hype Cycle:

- **Cloud infrastructure entitlement management (CIEM) —** This is a new profile that reflects the emergence of specialized SaaS-delivered IAM solutions that manage entitlements in hybrid and multicloud IaaS. CIEM provides important foundational capabilities to mitigate identity risks in IaaS. However, we project that its capabilities will rather quickly be subsumed into other IAM tools, cloud security posture management (CSPM) tools or the cloud infrastructure, becoming obsolete as a stand-alone innovation.
- **Machine identity management —** This is a new profile that reflects an increased need to manage the cryptographic keys, X.509 certificates and other credentials that are used to establish trust in the identities of machines, such as IoT devices, virtual machines, containers and RPA bots.
- **Mobile multifactor authentication —** This is a new profile for a broad class of solutions that provide passwordless MFA by combining multiple (typically two) factors in a smartphone app. Among other things, they fuse phone-as-a-token authentication, FIDO authentication protocols and biometric authentication.
- **API access control —** This is a new profile that reflects an increased demand for specialized access control features for APIs that offer session management capabilities, advanced adaptive access capabilities and support for evolving identity standards, which full life cycle API management offerings like API gateways sometimes lack.
- **Document-centric identity proofing —** This profile supersedes the "identity proofing and corroboration" profile published in past Hype Cycle research. Many data-centric components of the previous profile, such as reputation and link analysis, are now considered mainstream, while others, such as knowledge-based verification (KBV), have become obsolete. The document-centric focus in this profile reflects client interest in a distinct and rapidly maturing technology. (Even though identity proofing represents only a fraction of regulatory Know Your Customer [KYC] processes, some vendors spuriously and misleadingly call this particular technology "eKYC" or "digital KYC.")

Figure 1. Hype Cycle for Identity and Access Management Technologies, 2020



Source: Gartner
ID: 450324

The Priority Matrix

IAM innovations are predominantly infrastructure technologies; however, some directly map to business value.

IAM tools such as PAM are implemented to support one or more business process improvements or compliance or other security and risk management initiatives. For this reason, many of the business benefits from adoption are indirect and are not easily made visible to the business.

The ability to enhance cybersecurity by delivering accountability and transparency of access to the business remains important, but interpretation of these needs and correlating the importance for corresponding technical investments is the challenge and responsibility of the reader.

Furthermore, IAM has a significant opportunity to deliver direct business value by enabling lower-cost, risk-managed interactions with partners and customers and by enhancing user and customer experience. Key innovations here span AM, user authentication and CIAM.

IAM leaders should focus on business and CIO imperatives where they can deliver recognized value (for example, modernization of workplace tools, migration to the cloud, integrating SaaS and on-premises applications, supporting higher volumes of remote access, and expanding customer service channels).

Innovations such as SaaS-delivered IAM routinely demonstrate impact and value, have an anticipated mainstream adoption of two to five years, and can be widely adopted without concern.

However, early phase innovations — such as secure multiparty computing, zero-knowledge proofs and decentralized identity — may be promising but have a long way to go to be proven and demand cautious evaluation against business needs. Note that secure multiparty computing is transformational but likely has a lower benefit in IAM specifically.

Figure 2. Priority Matrix for Identity and Access Management Technologies, 2020

Priority Matrix for Identity and Access Management Technologies, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational		**Bring Your Own Identity**	**Secure Multiparty Computing**	
high	**Document-Centric Identity Proofing** **Enterprise Digital Rights Management** **OAuth 2.0**	**Customer IAM** **Machine Identity Management** **Mobile MFA** **OpenID Connect** **Privileged Access Management** **SaaS-Delivered IAM**	Decentralized Identity Internet of Things Authentication	
moderate		5G Security API Access Control Biometric Authentication Methods FIDO Authentication Protocols IAM Managed Services Mobile Identity SCIM	Externalized Authorization Management UMA Zero-Knowledge Proofs	
low				

As of July 2020

Source: Gartner
ID: 450324

Off the Hype Cycle

The following technologies have been removed from the IAM Hype Cycle this year:

- **Identity governance and administration (IGA) —** The IGA market has reached the point of maturity. Mainstream IGA products and services can fulfill all the most common use cases. The basic functionality associated with core capabilities (identity life cycle, entitlements management, access requests with approval workflows, access certification campaigns, fulfillment and reporting) is delivered in a relatively consistent manner by all products and services in the market. Most large and global enterprises in mature regions have already purchased IGA (see "The Identity Governance and Administration Landscape Is Changing").
- **Identity proofing and corroboration —** The data-centric components of this profile are now considered mainstream or obsolete. Document-centric identity proofing is represented by a new profile in this Hype Cycle.
- **Phone-as-a-token authentication —** This class of authentication methods, including out-of-band (OOB) SMS, one-time-password (OTP) apps and mobile push, is now widely adopted as part of MFA implementations across the market. While some challenges remain (see "Technology Insight for Phone-as-a-Token Authentication"), the technology is mature and mobile push or OTP apps can provide most users with a robust MFA option with good UX.
- **Full life cycle API management —** This persists in several other Hype Cycles but has been replaced here by API access control.

On the Rise

Cloud Infrastructure Entitlement Management

Analysis By: Henrique Teixeira

Definition: Cloud infrastructure entitlement management (CIEM) offerings are specialized identity-centric SaaS solutions focused on managing cloud access risk via administration-time controls for the governance of entitlements in hybrid and multicloud IaaS. They typically use analytics, machine learning (ML) and other methods to detect anomalies in account entitlements, like accumulation of privileges, dormant and unnecessary entitlements. CIEM ideally provides remediation and enforcement of least privilege approaches.

Position and Adoption Speed Justification: Managing cloud infrastructure entitlements is becoming a greater challenge due to their rapid increase in number and complexity, further exacerbated by the multicloud, where entitlements are inconsistently defined and configured. Adding to that, cloud identity entitlements are too granular and dynamic to be managed effectively by traditional identity governance and administration (IGA) and privileged access management tools (PAM) solutions, so new tools are emerging to fill this gap.

CIEM provides a subset of cloud security posture management (CSPM) capabilities (see "Innovation Insight for Cloud Security Posture Management"). However, it expands deeper into identity controls (like governance of entitlements and identity analytics, PAM and IGA process integrations, etc.),

while CSPM provides a broader security approach of controls for configuration settings, network, data storage and APIs for example. Not all CSPM vendors provide account privileges governance as part of their security controls, which is a core functionality of CIEM.

Cloud infrastructure and platform services (CIPS) providers are also adding new tools to enhance cloud infrastructure entitlement management. However, these embedded tools are in different stages of maturity and do not support multicloud use cases, reinforcing the need of specialized cloud security tools that provide CIEM capabilities.

Over the past two years, CIEM vendors are emerging as solutions for managing the risk of overprivileged accounts in modern hybrid, multicloud infrastructures. Optionally it can extend controls to SaaS applications, and provide 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.

However, a stand-alone market for CIEM is not sustainable in the long term. Similarly to the CSPM market, CIEM vendors are evolving to address a real, immediate, and significant need, but it risks being subsumed into adjacent markets. The cloud providers themselves are improving their own capabilities. In terms of third-party alternatives, besides CSPM, CIEM features are also being adopted by a few IGA vendors, like SailPoint and Saviynt.

User Advice:

- Prioritize the implementation of CIEM capabilities when protecting cloud infrastructure services. In the short term, choose either a CIEM specialist vendor, an IGA or a CSPM solution with integrated and strong CIEM capabilities. CIEM specialists are likely to offer a better cost-benefit than CSPM for organizations mostly concerned with identity-centric risks. Sign short-term contracts only as the market for specialized identity-centric cloud security evolves.
- Until IaaS (and traditional IAM) vendors offer more robust and easy to use embedded methods for the governance of entitlements across multi clouds, CIEM technologies should be used to fill that gap.
- A few CIEM vendors also offer basic threat discovery that overlaps with capabilities of some CSPM and CASB technologies. Adoption of CIEM should take in consideration other broader requirements of cloud security, in order to avoid overlap and redundancy of features.
- CIEM cannot replace full featured IGA and PAM technologies, and it should be considered as part of a broader IAM strategy. Integration points should be implemented between IGA and PAM processes, using APIs offered by CIEM vendors to facilitate integration with adjacent security and IAM systems. Continue to consistently manage the life cycle and governance of your cloud infrastructure accounts by leveraging common IGA tools and processes.
- CIEM vendors don’t yet provide out of the box integrations with all major security, IGA and PAM solutions, and vice versa. Over time, IAM and security vendors will likely build integrations with CIEM for making deployments in more established organizations more feasible, but in the meantime anticipating customized integration efforts is recommended.

- Consider leveraging CIEM capabilities from existing tools by established vendors. (e.g., Orkus acquired by SailPoint) and evaluate evolution of the market from other security vendors either acquiring or extending their offerings to include these features.

Business Impact:

- With the increased demand for multicloud architectures, CIEM will continue to offer a significant advantage over proprietary CIPS embedded technologies for governance of identity entitlements.
- CIEM tools can provide basic infrastructure functions such as audit, log, reporting, and alerting, which may be enough for smaller organizations.
- CIEM offers a potential better value for mitigating identity risks when compared to CSPM, given it's an identity-centric solution focused on entitlements management, instead of a more comprehensive, but potentially more expensive solution.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Authomize; Britive; CloudKnox Security; Ermetic; Obsidian; Polyrize; SailPoint; Saviynt; Sonraí Security

Recommended Reading: "IAM Leaders' Guide to Identity Governance and Administration"

"IAM Leaders' Guide to Privileged Access Management"

"The Identity Governance and Administration Landscape Is Changing"

"Managing Privileged Access in Cloud Infrastructures"

"Innovation Insight for Cloud Security Posture Management"

"Guide to Cloud Security Concepts"

"5 Things You Must Absolutely Get Right for Secure IaaS and PaaS"

UMA

Analysis By: Michael Kelley

Definition: User-managed access (UMA) is a profile of OAuth 2.0 that defines how individuals can control, allow, deny and delegate access to their personal data. There are five roles in UMA. There is a resource owner (an individual), a requesting party, (who needs access to the resource owner's data) and a resource server (where the resource owner's data is stored). There is also an authorization server (controls access to data on the resource server) and a client (controls interactions between resource owners and requesting parties for data access).

Position and Adoption Speed Justification: UMA enables individuals to control, allow, deny and delegate access to their own information, rather than having an administrator manage this access. Beyond minimal growth in vendor-supported and open-source implementations, adoption remains extremely limited. UMA has implementations from ForgeRock, Gluu, WSO2 and Red Hat, and there are other, less-known, implementations; however, UMA is difficult to define. Use cases are still niche, which continues to delay widespread adoption. In addition, competing technologies such as 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. The current UMA 2.0 specification has functionality to allow a resource owner to configure authorization grant rules, prior to requests being received, rather than at runtime, which was a limitation in the prior specification.

User Advice: UMA provides technical controls that individuals use to control access to their information, which is relevant for complying with privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union 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 CIAM use cases, due to the emphasis on user experience (UX) and privacy preferences. However, there will eventually be workforce applications for UMA, too.

Current identity and access management (IAM) approaches to sharing personal information require IT administrators to control authorization changes through policy. UMA puts this control back into the hands of the individual. When there is a need to allow individuals to have better control for others accessing their protected information, 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.

Business Impact: Successful UMA implementations can enable individuals to explicitly manage access policies for resources (data) they own. Without UMA, access management mechanisms controlling access to user-owned resources (such as profile data and patient data) is proprietary or is insufficient for setting up access policies before access occurs.

For example, if a patient is using a team of healthcare providers, and all providers need access to some of the patient's information during treatment, then all requesters must use the access management features of a shared healthcare system. The patient would be asked to give consent each time, for each request for access. With UMA, the patient uses a client interface to control which healthcare providers have access to which data and how long they have access, and it provides the ability to revoke that access.

UMA provides a standards-based mechanism to centrally control the orchestration of authorization grants and access flows across disparate systems.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ForgeRock; Gluu; Red Hat; WSO2

Recommended Reading: "A Systematic and Practical Approach to Optimizing Authorization Architecture"

"Evaluation Criteria for Access Management"

"Critical Capabilities for Access Management, Worldwide"

"Innovation Insight for Decentralized and Blockchain Identity Services"

Zero-Knowledge Proofs

Analysis By: David Mahdi

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

Position and Adoption Speed Justification: MIT first developed the concept of ZKP in the 1980s. In particular, the challenge was to overcome the possibility of fraudulent representation of information. Rather than just focusing on an entity (prover) who tries to persuade the receiver (verifier) that the information is accurate (either false or true), the goal is to also address the issue of a verifier learning more about the information than merely if it is accurate or not. This challenge has applicability in a wide range of use cases especially in the context of authentication and transaction verification. Other cases include payments, custody management, AML/KYC, consumer IAM, medical records, mergers and acquisitions, etc.

To operate effectively, ZKP must have completeness (of process), soundness (of information), and zero knowledge (of anything other than the proof). This challenge is highly relevant to blockchains and distributed ledgers as a core tenet of their operation is data sharing. The zero-knowledge approach is used by blockchain platforms and crypocurrencies in the form of zk-SNARKS, which are better-suited to a blockchain context due to greater efficiency and reduced need for interactivity. Hawk is an application of ZKP to smart contract domain, where the state of the computation is encrypted. An enabling cryptographic construct for ZKP is homomorphic encryption, which allows for computation on encrypted variables without revealing their values. Zcash (and its predecessor, Zerocash) is an early example of applying ZKP as an extension to the Bitcoin Protocol. In July 2016, Ethereum developers (such as Vitalik Buterin, the founder of Ethereum) worked in combination with ZKP experts to add a lightweight implementation of zk-SNARKs to the Ethereum platform, called ZoE. It is likely that future versions of Ethereum will incorporate a more robust ZKP capability. Over time, major platforms that seek to compete with Ethereum and Bitcoin will add ZKP capability as well, and its value as a point of differentiation in a crowded competitive platform landscape will diminish. Overall, ZKPs are privacy-preserving messaging protocols that enable entities to prove

that information available to both of them is correct, without the requirement to transmit or share the underlying information. Leveraging ZKPs limits the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology. Ultimately, by leveraging ZKPs, service providers, and others can reduce their reliance on honeypots of user data, to help mitigate against mass data breaches.

A challenge is that variety of methodologies and the multiplicity of types of ledgers and approaches to data management inhibits adoption. Moreover, ZKP will need to scale at the rate of DL transactional volumes in order to be effective, and this is yet to be proven.

User Advice:

- Work with security and risk management leaders to gain a deeper understanding of the nature of these controls, understanding that ZKP techniques are a paradigm shift.
- Understand how ZKP can benefit use cases that require privacy protection but be realistic with the current immaturity of ZKP solutions and approaches.
- Evaluate how such 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.

Business Impact: Most blockchain platforms today offer a number of core benefits, but namely, those of integrity and availability. And while this may benefit a number of approaches to ensure transaction and data security, confidentiality was not covered by the core of blockchain platforms. With the addition of ZKPs to blockchain platforms, security and risk management leaders now have the potential to cover information security use cases that require confidentiality, integrity and availability (CIA). Extending CIA, this also provides privacy focused security leaders with alternatives regarding privacy protection, and sensitive data minimization. Ultimately, business impact can be significant in terms of institutions and individuals being able to better protect and prove the context and details of information while simultaneously being able to maintain confidentiality. This would also limit the requirement for mass decryption and encryption of all the data elements, which has benefits for the efficiency of the network as well as the potential adoption of blockchain/distributed ledger technology.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Ethereum; Evernym; IBM; Zcash

Recommended Reading: “Market Guide for Blockchain Platforms”

“A Technical Primer for Assessing a Blockchain Platform”

“Innovation Insight for Blockchain Security”

“Cool Vendors in Blockchain Technology”

“Predicts 2019: The Ambiguous Future of Privacy”

“Cool Vendors in Privacy Management”

5G Security

Analysis By: Sylvain Fabre; Bernard Woo

Definition: 5G security is enabled by a set of 5G network mechanisms, and improves 4G security with:

- Unified authentication (4G authentication is access dependent).
- Flexible security policy for diverse use cases (versus single 4G policy).
- Encrypted transmission Subscription Permanent Identifier (SUPI) prevents International Mobile Subscriber Identity (IMSI) leakage for user privacy.

Position and Adoption Speed Justification: 5G security is not a priority in many deployments; standards won’t cover everything — implementation will hugely influence outcomes (e.g., private network versus public infrastructure). Switching on security features is up to the CSPs.

- 5G will increase number and diversity of connected objects, potential DDoS attack vectors and entry points; this also provides more telemetry for anomaly detection.
- More 5G private, dedicated networks will be deployed by enterprises (more security conscious than consumers).
- Legacy networks and devices will interconnect with 5G.
- 5G infrastructure virtualization, automation and orchestration of a service-based architecture increases exposure.
- Slicing virtual networks across shared infrastructure impacts security due to lateral movement risk, and cross-slice permeability issues.
- Wider ecosystem delivering industrial 5G use cases, with varying security competencies and credentials, make SLAs, service assurance including E2E security, challenging.
- Backward compatibility with 4G/Long Term Evolution (LTE) means some legacy security issues persist in 5G.

User Advice: Don’t rely exceedingly on network 5G security, end users will still have to continue using VPNs and identity management.

In addition, security leaders leveraging 5G, including for industries, should:

- Anticipate increased attack risk such as DDoS by improving equipment and software design of 5G network infrastructure and endpoints, and recovery procedures.
- Implement layered-DDoS defense with best of cloud scrubbing center, cloud web application firewall, bot mitigation, DNS protection, ISP and on-premises DDoS appliances. Determine effectiveness of protections from incremental add-on solutions an ISP or CDN can sell.
- Evaluate DDoS protection services from current CSP or cloud providers as a possible failover for key applications when on-premises DC is under attack.
- Initiate effective mitigation by correlating network traffic, application availability and server performance. Outages may be due to human or system error rather than attacks.
- Consider interoperability with other networks e.g., authentication of Wi-Fi devices. Ensure 5G device hardening to reduce possibility of being used as botnets.
- Segment IoT devices with different incident responses.
- Complement 5G infrastructure security with distributed anomaly detection/monitoring including edge and core slicing.
- Decide any trade-offs between secrecy, capacity, delay, quality of service (QoS), compute and energy efficiency by use case.
- Implement edge protection concepts used in application security for elasticity and focused on app-layer protection, and commonly provided via a CDN provider, SaaS or cloud provider.

Security for 5G systems encompasses need to include in network deployments:

- Cross-network layer security (e.g., between 5G macro and small cell layers)
- E2E security (e.g., managing strength of different algorithms, generating and negotiating secret keys, confidentiality protection)
- Cross-CSP 5G network domain security (e.g., in R16, several cloud service providers [CSPs] could provide slices for a given 5G service)
- Leverage user traffic integrity protection which is available now

Traffic interception may require formal and time-sensitive reporting to clients due to maturing data protection regulations.

Implement patching policies and procedures on devices used for network configuration given 5G's reliance on software.

All 5G network infrastructure vendors implement the same 3GPP standards for 5G security; however, development processes may vary; concerns about specific vendors as well as geopolitical tensions have increased procurement scrutiny around 5G infrastructure.

5G network infrastructure requires more antennas, promoting sharing with different CSPs or utility providers, or multitenant scenarios. It needs the review and update of hardware protection

protocols, including physical measures to address recent increases in vandalism based on fake news.

Embed privacy-protective features into endpoint/IoT devices to manage potential privacy risks.

Plan for lower security context anytime your 5G devices connect to a legacy 3G or 4G network.

Business Impact: Increased controls could impact QoS, increase latency and lower data rate due to traffic encryption overhead.

Guaranteed security levels may enable 5G use in more demanding use cases, using other improvements, like:

- Home control feature enables network to verify device location when the device is in a visited network, preventing spoofing attacks on device locations involving false signaling messages to request device identifier and location, and then intercept ongoing communications.
- 5G mitigation against bidding down attacks prevents a fake base station from making UEs believe that the BTS ("IMSI catcher") does not support a specific security feature and use a previous mobile network technology.
- Flexible security policies and other chargeable features such as slice as a service, QoS SLAs for latency etc. in 5G allow premium pricing.
- 5G security adds value for CSPs but may be adding complexity for business users.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Ericsson; Huawei; Intel; Mobileum; Netcracker; Nokia; VIAVI Solutions

Recommended Reading: "Market Trends: Strategies Communications Service Providers Can Use to Address Key 5G Security Challenges"

"Reduce Privacy Risks When Using 5G Products and Services"

"Market Guide for Mobile Threat Defense"

"Protecting Web Applications and APIs From Exploits and Abuse"

Internet of Things Authentication

Analysis By: David Mahdi; Michael Kelley

Definition: Internet of Things (IoT) authentication is the mechanism of establishing trust in the identity of a thing (device, etc.) 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.

Position and Adoption Speed Justification: The diversity of devices and their different capabilities result in a market that is in a state of flux. In the IoT authentication space there is a lot of innovation, in areas such as new provisioning flows, and new software and hardware platform support for full life cycle handling of credentials. Unfortunately, many IoT devices lack physical integrity protection due to device manufacturers' poor track record on security (see "IoT Security Primer: Challenges and Emerging Practices"). In addition, IoT devices can be resource-constrained with low computing power and storage capacity. Some authentication methods are not good candidates due to their significant bandwidth and computational requirements. Furthermore, use cases (consumer IoT and IIoT), bring another filter of requirements and constraints that IoT devices must support and account for. Complicating these matters further is that with use case areas such as IIoT have protocols that are still in flux, creating ongoing challenges for authentication approaches.

There is a growing need to evaluate and streamline the methods adopted for device and service authentication over constrained IoT networks. This includes three potential classes of IoT devices (similar to IETF RFC 7228 on Terminology for Constrained-Node Networks):

- Class 0 (minimal) devices have little or no hardware capacity to sustain software that might be required for authentication.
- Class 1 (moderate) devices have a limited capacity ("headless devices") for cryptographic key generation/storage or software agents but vary from type to type.
- Class 2 (full function) devices have authentication capabilities similar to mobile phones and are capable of sustaining authentication functionality used today.

Standard authentication techniques, such as public-key methods, can be adopted to serve IoT use cases. For example:

- Public-key certificates often leverage elliptic curve cryptography algorithms and optimized template formats to meet the needs of smaller devices. These methods apply to Class 2 and Class 3 devices.
- RFC 8628: OAuth 2.0 Device Authorization Grant extension enables devices with no browsers, or unconstrained devices (i.e., Class 1) aid in the bootstrapping of IoT devices.
- The ACE working group within 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.

While still emerging, blockchain-based methods promise an alternative approach to ensuring device integrity and availability. Blockchain could also act as a mechanism for the secure delivery of cryptographic keys.

User Advice: Security and risk management leaders focused on IAM and IoT security must:

- Catalog and establish identity assurance requirements and capabilities for each category of devices in their IoT network. Leverage device- and network-based contextual information to gain additional assurance.
- Evaluate and adopt a centralized authentication framework that supports the range of device types (Class 0, 1 or 2) within and across the IoT realms in operation.
- Understand assurance requirements as Class 2 devices identify and authenticate users. Most user authentication methods, like device-based public-key or biometric methods (such as fingerprint) meet assurance objectives but often do not scale to the needs of IoT implementations.
- Make use of trusted computing techniques, such as Trusted Execution Environment (TEE) or Hardware Root of Trust (HRoT), 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 elements on the devices.
- Know when to inspect and adapt, and when to inspect and adopt when assessing and architecting identity into IoT devices. In many brownfield cases the devices can't be secured and instead need to be protected with other mechanisms such as gateways, software defined networks or even physical security.

Business Impact: As IoT finds widespread applicability, ensuring the identity and integrity of entities connected to each other by means of reliable authentication and control mechanisms is crucial. The constrained nature of many IoT devices opens new attack vectors and vulnerabilities using the security threats that apply to IP-based networks. These vulnerabilities could be exploited to introduce a range of threats targeted at compromising security and performance of IoT devices. Custom IoT implementations across multiple devices and IoT realms in industries such as healthcare, logistics and supply chain, smart homes, smart grids, automotive transportation, and retail will benefit from emerging IoT authentication standards. Ultimately, overtime, IoT authentication will eventually have a strong influence on the IoT architectures and security controls in other industries at the enterprise level.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Amazon Web Services (AWS); Device Authority; DigiCert; Entrust Datacard; Infineon Technologies; Intel; Keyfactor; Microsoft; PrimeKey; Sectigo

Recommended Reading: "Architecting Identity for the Edge of IoT Innovations"

"IoT Security Primer: Challenges and Emerging Practices"

At the Peak

Machine Identity Management

Analysis By: David Mahdi

Definition: Machine identity management aims to establish and manage trust in the identity of a machine (mobile devices and IoT devices and workloads such as applications and containers) 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.

Position and Adoption Speed Justification: Machines, such as devices and workloads (i.e., applications and containers), are being leveraged at an increased rate due to the growing trends related to digital business and digital transformation. Traditional methods of identifying and managing machine identities has led to the proliferation of siloed processes and tools. Many of these tools do not scale and interoperate with modern cloud environments. As a result, several technology providers are starting to build tools that can help clients discover and manage machine identities across hybrid and multicloud environments.

In addition, over the past year, Gartner witnessed an increasing number of clients reposition enterprise X.509 certificate management with the overall notion of machine identity management. And enterprisewide machine identity management strategy is needed to support digital transformation in modern IT environments.

Machine identity management approaches handle the discovery and life cycle management of the credentials used by machines. This can include leveraging secrets, keys, X.509 certificates and other cryptographic materials that are used to strongly identify nonhuman entities (“machines”) such as:

Workloads:

- Containers
- Virtual Machines
- Application credentials such as a database key and credentials used by RPA/bots
- Services such as web servers/websites
- Code signing operations and certificates

Devices:

- OT/IoT devices
- Mobile devices
- Desktops

User Advice: Security and risk management leaders focused on IAM and security must:

- Determine the overall usage and dependency of machine identities. Initiating a discovery process (by leveraging tools) can help provide SRM and IAM leaders with insight into their environment from a machine identity perspective.
- Furthermore, use full life cycle management or discovery-centric tools to audit the number of deployed machine identities; and to identify the potential risks from expiry and overall compliance. (See "Technology Insight for X.509 Certificate Management.")
- Choose full life cycle machine identity management solutions to drive intelligent automation when dealing with large, complex, multivendor certificate environments — especially when dealing with multiple certificate-based enterprise use cases such as mobile and the IoT.
- SRM leaders charged with securing virtual, containerized systems can use machine identity management tools with built-in integrations (such as HashiCorp, and Kubernetes) to secure these environments
- Ensure that machine identity management operations include the practice of crypto-agility (see "Better Safe Than Sorry: Prepare for Crypto-Agility") and align with the overall cybersecurity incident response plan.

Business Impact: As environments become more digital and cloud-enabled, security leaders will need to ensure that they can manage the increase in volume and velocity of machine identities that will be required to support their digital business needs. Machines, such as servers, cloud environments, RPA, and applications all require digital identities. These digital identities will allow SRM leaders to apply the most appropriate security policy to manage and control all of these entities.

Machine identity management encompasses a number of technologies, that today remain mostly siloed (i.e., X.509 Certificate management, SSH key management, as well as secrets and other crypto-key management). In addition, many of these areas remain overly complex, as they delve into highly technical areas. SRM leaders can ensure that they have aligned their approaches accordingly by repositioning overly technical PKI, or crypto-key management projects with "machine identity management" that is tied to digital business criticality. Overall, this is to ensure that nontechnical business leaders understand that cryptography and machine identities is critical infrastructure for digital business and, therefore, requires attention and investment. By attaching the notion of cryptography to a higher-level issue like digital business, the aim for security leaders is to increase their overall success in establishing a center of excellence for cryptography in their organization.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Amazon Web Services (AWS); AppViewX; CyberArk; HashiCorp; Keyfactor; Microsoft; Scytale; Sectigo; SSH; Venafi

Recommended Reading: "Technology Insight for X.509 Certificate Management"

"Better Safe Than Sorry: Preparing for Crypto-Agility"

"Best Practices for Privileged Access Management Through the Four Pillars of PAM"

"Managing Secrets and Privileged Access in an Agile, DevOps Environment"

Mobile MFA

Analysis By: Ant Allan

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 protocols: one-time password (OTP), mobile push, X.509, and Fast IDentity Online (FIDO) Universal Authentication Framework (UAF) or FIDO2. The additional factor may be a biometric trait or a local PIN. Biometric authentication may be native to the device or a custom method.

Position and Adoption Speed Justification: Mobile MFA methods were subsumed within the discussion of phone-as-a-token authentication in past Hype Cycle research. We now see increasing client interest and vendor investment in these methods in their own right.

Gartner clients are increasingly seeking "passwordless" authentication methods to improve user experience (UX) by eliminating passwords from the user journey or enhance security by eliminating centrally stored passwords, which are a honey pot for attackers.

Thus, there is increasing hype around a variety of passwordless methods that are commercially available. Those most often labeled "passwordless" by vendors are mobile MFA methods and these will be dominant in many use cases.

Mobile MFA methods are often modifications of established vendors' legacy phone-as-a-token modes (especially mobile push) that would ordinarily be added to legacy passwords to provide MFA. In mobile MFA the additional factor on the phone replaces the password.

Here, the vendors typically offer a choice between a local PIN and a biometric trait as the additional factor, but the latter is often restricted to device-native biometric authentication.

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 a FIDO authentication protocol. In this case, the additional choice of using a proprietary, third-party biometric method is more common.

The adoption of mobile MFA of either pedigree remains nascent.

User Advice: Mobile MFA can be used to support access from any endpoint device, including the phone itself.

Evaluate mobile MFA supporting mobile push and OTP as an evolution of investments in phone-as-a-token methods, in the same use cases (typically remote access to corporate networks and access to SaaS applications).

Similar to legacy phone-as-a-token methods, mobile MFA is potentially limited by the availability of smartphones among the target population, and their willingness to use a personal device "for work" and by any operational restrictions on the use of phones.

OTP hardware tokens can readily be used as alternatives to legacy phone-as-a-token methods; however, an alternative passwordless option is elusive. Biometric-enabled OTP tokens are rare. FIDO2 security keys offer an alternative in some use cases in the near term.

Some mobile MFA implementations can also support Windows PC and network login, but typically rely on a vendor-supplied credential provider that must be implemented across all corporate and bring your own device (BYOD) PCs. Support for macOS is less common.

Evaluate mobile MFA supporting X.509 authentication as an alternative to PIN-protected smart cards or USB tokens for "interactive smartcard login" to Windows PCs and networks. Here, the smartphone effectively functions as a contactless smart card via Bluetooth or NFC.

Legacy X.509 hardware tokens remain alternatives when mobile MFA cannot be used.

Evaluate mobile MFA supporting FIDO2 as a FIDO2 external authenticator as an alternative to hardware FIDO2 security keys for access to applications via a Web-Authentication-compliant browser. We project that Windows 10 login will support this option too.

FIDO2 security keys remain alternatives when mobile MFA cannot be used.

"Full" multiprotocol mobile MFA that includes FIDO2 is still in the offing. When available, choose this to support multiple use cases in a cohesive way, with similar UX, and to facilitate transition from legacy protocols (e.g., OTP, mobile push and X.509) to FIDO2 during the next two to three years. FIDO2 will provide a consistent UX independent of phone connectivity.

Some legacy use cases (e.g., some virtual private networks [VPNs]) that require MFA integration via RADIUS or Lightweight Directory Access Protocol (LDAP) will not readily support passwordless. To support these cases, choose mobile MFA that can function as an additional single factor or consider relaxing password rules.

In mobile use cases, favor mobile MFA that uses proprietary, third-party biometric methods, because these offer higher levels of trust and accountability than device-native biometric methods that give enterprises no control over enrollment or configuration.

Favor methods that provide a choice of two or more biometric modes, such as face/fingerprint, face/voice, face/palm. This provides better UX across a range of environmental situations.

Business Impact: Mobile MFA enables passwordless MFA in a variety of use cases with multiprotocol implementations being able to support multiple use cases in a cohesive way. It

provides a consistent way of using biometric authentication ("mobile-centric biometric authentication").

It extends the benefits of legacy phone-as-a-token authentication by further improving UX (through the elimination of passwords) and support for more use cases (without clunky integration for Windows PC and network login).

Enterprises benefit by potentially lower total cost of ownership (TCO), compared with maintaining discrete solutions for different use cases and users benefit from a more consistent UX. However, alternatives must still be used for those who cannot or will not use smartphones for personal or operational reasons.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Forticode; HYPR; Microsoft Azure; Secret Double Octopus (SDO); SecureAuth; Trusona; Veridium; Whykeykeysoft

Recommended Reading: "Technology Insight for Phone-as-a-Token Authentication"

"Technology Insight for Biometric Authentication"

"Passwordless Authentication Is Here and There, but Not Everywhere"

Secure Multiparty Computing

Analysis By: David Mahdi; Bart Willemsen; Brian Lowans

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

Position and Adoption Speed Justification: With increasing demands of privacy protection and adequate, contextualized security controls, security and risk management (SRM) leaders struggle to achieve balance between data protection requirements and business objectives. Regulations focused on privacy and data protection further complicate the processing of (personal) data.

Historically, data protection has focused mainly on two states: securing data at rest and in transit. However, with SMPC-based methods and key splitting, it is possible to employ data protection in use. Data protection in use introduces a new paradigm to the arsenal of security methods and enhances traditional security approaches. The application of SMPC extends to combating data residency concerns, for example, balancing a single-point-of-failure risk regarding a cloud service provider's environment. SMPC can empower cloud key management with the ability to "split"

cryptographic keys in a manner such that it ensures protection and privacy in the cloud. Most importantly, it facilitates data sharing for analytics in a protected state, across multiple contributors.

User Advice: SMPC-based solutions offer new methods to ensure scalable, private and secure data processing and sharing. With SMPC just starting to become a reality from a product and solution perspective, a number of new vendors are solving data security and privacy use cases with SMPC-based technology, often in combination with other capabilities. Use cases include:

- Cloud computing (confidentiality with data in a cloud environment)
- Privacy-preserved (personal) data analytics
- Encryption key management
- Cryptographic key protection
- Scalable software-defined hardware security modules (virtual HSMs)
- Secure and private data mining
- IoT security
- Blockchain security
- Analytics of data using proprietary algorithms

Data management strategies that include SMPC-based approaches enable secure and private sharing and analytics of data. For example, an organization that aims to extract value from customer data but has to adhere to strict privacy laws can maintain information value to extract insights while ensuring that the data is kept in an unidentifiable state. SRM leaders should work with developers/architects to establish a high-level position on its relevance and a vision for the future adoption.

Furthermore, trust in the SMPC algorithm(s) and their respective security posture are crucial to SMPC's effectiveness as a privacy-preserving technology. SRM leaders must continue to gain insight into the technology development to provide trust-invoking transparency.

Business Impact: As organizations face ongoing pressure to ensure that their data is secure and private throughout the data life cycle, SRM leaders will need sustainable, effective and efficient ways to comply and treat risk.

SMPC, while known to academia for a few decades now, is only now starting to become commercially viable.

As volumes of both structured and unstructured data continue to grow, SRM leaders will need scalable, privacy-centric approaches to protect data amid a landscape of maturing data protection regulations. This is particularly important in areas such as cloud, Internet of Things and data mining or monetization.

SMPC can alleviate privacy concerns in the areas of big data analytics, machine learning (ML) and artificial intelligence (AI). SMPC helps SRM and data and analytics leaders to benefit from data insights that are derived from ML and AI while keeping the data secure and private. As ML and AI

mature, SMPC will need to account for performance issues with specific algorithms such as recursive algorithms. Overall, SMPC allows for the secure enablement of business, enabling organizations to leverage their data while mitigating security and privacy concerns.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Baffle; CryptoNumerics; Cybernetica; DataFleets; Inpher; Unbound Tech

Recommended Reading: "The State of Privacy and Personal Data Protection, 2019-2020"

Decentralized Identity

Analysis By: David Mahdi; Michael Kelley

Definition: Decentralized identity services leverage technologies such as blockchain or other decentralized ledger technologies (DLTs) to decentralize an identity system by distributing it across a large number of nodes or participants. Thus, they provide an alternative to siloed legacy IAM architectures by establishing trust in identities and resiliency within the overall system, with little reliance on centralized arbiters or identity stores.

Position and Adoption Speed Justification: Decentralized identity (DID) differs from traditional IAM approaches due to the concept of centralized, versus decentralized, generation and storage of identities. Traditional IAM approaches, storing identity and entitlement data in central authoritative sources can be problematic from the perspectives of liability, security, scalability, reliability and privacy.

A decentralized approach minimizes these problems due to its core architecture being decentralized, distributed and transparent. It has the potential to increase trust, scale and resiliency, possibly with a more equitable and efficient economic model.

Standards are currently emerging, and at a fast rate. However, the market will take time to reach a steady state. However, development and innovation are increasing at a rapid pace, actively supported by financial and government institutions. On the standards front, the WC3 group, along with the decentralized identity foundation, (DIF), have created open standards which DID vendors can use to align their technology and vision with the rest of the market. In addition, the recently launched Trust over IP (ToIP), offers some promise in the area of standardization as well (see "Guidance for Decentralized Identity and Verifiable Claims").

A growing number of IAM approaches are reflecting blockchain-based enhancements including bring your own identity (BYOI) and decentralized identity. Mid 2019 and early into 2020, saw new entrants into the space such as Mastercard, Microsoft, Ping Identity (acquired ShoCard March 2020) Workday (acquired TrustedKey August 2019). Implementations are still primarily in POC, however, initiatives are gaining traction (such as Verified.Me in Canada).

Decentralized identity now sits at the peak; however, we have extended time to plateau. Practical blockchain-based solutions were overhyped and have made less headway than expected. Furthermore, effective solutions will depend on secure (formerly "privacy-enhanced") multiparty computing and zero-knowledge proofs, which have longer timescales.

User Advice: IAM leaders should familiarize themselves with decentralized identity through early stage research. In doing so, leaders can gain insight into new ideas and approaches that may be relevant. Ultimately, leaders must base all planning decisions on a clear understanding of the core differences between decentralized identity and traditional IAM approaches. A number of new and well-established vendors are experimenting with IAM applications in areas such as:

- Identity registration and verification.
- Ensuring integrity of devices (including things in the IoT).
- Enabling identity data sharing while preserving privacy ("consent control").
- Mitigating trust and transparency issues by using the distributed/decentralized model.
- Enhancing the ability to handle identities, attributes and relationships at massive scale.
- Enabling bring your own identity and/or self-sovereign identity. (Self-sovereign identity is another description for decentralized identity, or user managed identity; see "Blockchain: Evolving Decentralized Identity Design").

IT leaders with an interest in decentralized identity approaches must recognize that leveraging this technology today requires proofs of concept to learn about the technology and, ultimately, the new business models and identity ecosystem that can be realized. Leveraging in market vendors, such as Microsoft, Workday, InfoCert, or IBM, is one option to understand the possibilities of decentralized identity applied to their use case(s). Customer identity and access management, (CIAM) use cases in particular offer potential for a DID approach.

Business Impact: Ultimately, with decentralized identity, users gain control of their identities and related attributes (i.e., personal information such as address, age and credentials), and service providers will be able to onboard and interact with users with greater speed and confidence. This is in contrast to many online services today, where digital identity and access are siloed, and service providers are forced to horde identity information about users. This has led to data breaches and other security and privacy issues. In the age of GDPR and privacy-conscious consumers, service providers will need to reevaluate their stance on the identity data they store. By leveraging decentralized identity, service providers could liberate themselves from storing sensitive data, instead relying upon assertions generated by identity providers.

Leveraging decentralized identity has the potential to allow service providers to increase security and convenience of access for end users, all while reducing exposure to data breaches and potential privacy compliance violations.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: 1Kosmos; Evernym; Hyperledger; IBM; InfoCert; Microsoft; Ping Identity; SecureKey; Sovrin; Trusted Key

Recommended Reading: "Innovation Insight for Decentralized and Blockchain Identity Services"

"Innovation Insight for Bring Your Own Identity"

"Guidance for Decentralized Identity and Verifiable Claims"

"Top 10 Strategic Technology Trends for 2020: Practical Blockchain"

FIDO Authentication Protocols

Analysis By: Ant Allan; Tricia Phillips

Definition: The three Fast IDentity Online (FIDO) authentication protocols published by the FIDO Alliance are:

- Universal Authentication Framework (UAF), enabling passwordless authentication via a method local to a person's device.
- Universal Second Factor (U2F), enabling the use of a hardware token or other device as a second factor.
- Client to Authenticator Protocol (CTAP), new in FIDO2, enabling a FIDO-enabled device to authenticate a user accessing an application via a Web Authentication (WebAuthn) enabled web browser on another device.

Position and Adoption Speed Justification: Device manufacturers and authentication providers continue to invest in FIDO-compliant products. Native support of FIDO2-based authentication in Windows 10 through Windows Hello for Business has driven broader interest in FIDO for workforce use cases.

Google, Microsoft and, most recently, Apple's involvement in the FIDO Alliance, along with W3C's support for the FIDO2 protocol, sustain the hype. However, while UAF and U2F have been adopted by some prominent companies worldwide, FIDO2 is still nascent, and client interest tends to focus on different benefits from those espoused by the FIDO Alliance.

UAF reflects the FIDO Alliance's original aim to offer a consistent "passwordless" user experience via a "universal" authenticator that can be used to access multiple services from different providers. However, most client interest has focused on discrete implementations of local biometric authentication in mobile use cases, where UAF can greatly reduce integration efforts, and this focus on UAF (rather than FIDO2) persists.

FIDO2 CTAP supersedes U2F in providing a standardized way of implementing MFA, as well as passwordless authentication with just a FIDO2 security key. Client interest in U2F had focused on

ways of supporting hardware tokens, typically complementing other methods (such as mobile push), but legacy OTP tokens remain more popular in this situation. Microsoft's support for FIDO2 security keys for passwordless Windows 10 login has yet to drive significant client interest.

User Advice: Carefully evaluate the potential benefits of the FIDO2 authentication protocol across each use case in the enterprise compared to wholly proprietary alternatives, especially its better protection against man-in-the-middle attacks. FIDO2-compliant solutions may not provide the optimal approach across multiple use cases.

A FIDO2 internal or external authenticator embeds one or more private keys, each dedicated to one online account and thus provides what is essentially a multifactor software cryptographic token. However, the confidence that FIDO2 authentication provides depends on the "gesture" used: At minimum, with a weak local password or PIN, FIDO2 authentication can provide higher confidence than legacy passwords. Prefer FIDO2-compliant products enforcing the use of stronger local authentication methods, such as third-party biometric modes.

Choose FIDO2 as a way of alleviating the risks of continued use of centralized passwords. However, while many phones and some PCs have native UAF support, it will still be some time before FIDO2 compliant products are ubiquitous. Seek proprietary implementations by MFA providers that offer more granular control over how FIDO2 is consumed.

FIDO2 security keys with a PIN or biometric authentication option can provide passwordless MFA, but using FIDO2-compliant smartphones as an external authenticator offers the convenience of phone-as-a-token authentication and constitutes another option for passwordless mobile MFA.

Consider FIDO2 as a way of standardizing and simplifying implementation of biometric authentication in mobile apps. UAF is still widely used in this case, but FIDO2 enables broader benefits, such as passwordless mobile MFA for access from a PC or other device with a WebAuthn compliant browser. However, multidevice/multichannel deployments may be better served by a biometric authentication architecture with centralized data storage, comparison and matching.

Seek certified products. The FIDO Alliance now offers certification for FIDO authenticators and FIDO servers, as well as biometric certification, through third-party labs, that includes ISO/IEC 30107-3:2017 conformant testing of presentation attack detection or "liveness testing."

Consider FIDO2 options as complementary to existing MFA options and plan incremental migration to a FIDO2-centric architecture over the next few years as opportunities arise. Lean on incumbent providers tosupport your strategy and conduct POCs with new, FIDO2-centric vendors to accelerate adoption.

Business Impact: Adoption and use of FIDO2 devices with WebAuthn-enabled browsers lag market availability, so the possibility of universal passwordless authentication to consumer-facing applications is still some way off.

FIDO2 (or UAF) can simplify deployment of local biometric authentication in mobile and web channels. This is still where we've seen the biggest business impact to date.

In enterprise workforce use cases, as enterprises shift to using access management (AM) tools as the platform of choice for MFA, and as AM tools become FIDO2-compliant, we will see wider adoption of FIDO2 tokens and smartphone apps as an alternative to existing X.509 smart cards, OTP hardware tokens and proprietary phone-as-a-token methods, especially where passwordless MFA is sought.

WHfB is FIDO2-based and can therefore be used to enable authentication to any FIDO2-compliant application, as well as corporate networks. Within Azure AD Premium Conditional Access, WHfB-login from an AD-joined PC confers "trusted device" status to the PC, potentially avoiding the need to use an additional MFA method for access to SaaS applications.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Dot Origin (Key-ID); FEITIAN Technologies; Google; HYPR; Nok Nok; OctatcO; Raonsecure; Samsung SDS; Synaptics; Yubico

Recommended Reading: "Market Guide for User Authentication"

"Technology Insight for Phone-as-a-Token Authentication"

SCIM

Analysis By: Henrique Teixeira

Definition: The System for Cross-Domain Identity Management (SCIM) specifications provide a protocol, schema definition and APIs 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, things and 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.

Position and Adoption Speed Justification: Development for the SCIM specifications began in 2011 and the current version 2.0 was released as IETF RFC in 2015 for managing identity resources such as users, things and groups using application-level, REST/JavaScript Object Notation (JSON).

Most identity and access management (IAM) vendors that provide user provisioning capabilities have adopted SCIM. SCIM support by SaaS vendors continues to grow, and smaller vendors are perceiving the benefit of supporting the standard as an entry point for selling to large organizations.

Since last year, some good progress has been observed in the use of SCIM in provisioning gateways and identity synchronization brokers. Aquera and Radiant Logic are leveraging these approaches respectively. Since last year, Acquera extended partnerships with Omada, Oracle, Okta, Microsoft and JumpCloud in order to leverage its SCIM gateway as one more option for those

identity providers to connect with organizations target systems (over 3,000 apps are supported). Radiant Logic offers an updated cloud identity connector to Microsoft Azure AD, Salesforce, Google Directory, Okta, Workday and others. 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.

User Advice:

- Where native provisioning connectors are not available, leverage SCIM to simplify provisioning and reconciliation with target systems, thus replacing custom or proprietary connectors with SCIM connectors provided by IGA tools.
- Consider SCIM as part of a broader fulfillment strategy including indirect methods, like ITSM and RPA integrations.
- Leverage SCIM gateways and identity synchronization brokers (like Aquera and Radiant Logic) to simplify your account fulfillment objectives when out of the box connectors are not available. These gateways and proxies can translate SCIM into the proprietary protocol or format used by target systems for greater interoperability, including adding indirect fulfillment methods — thus extending the choice of connectors available.
- SaaS and application developers must continue to embrace SCIM to lessen organizations' burden of manually handling the life cycle or maintain a vast set of connectors.
- Enterprise buyers (and IAM vendors) must continue to push laggard SaaS vendors that have not yet adopted the standard to do so. Tell your application vendors to support SCIM, pointing to the need for integration with enterprise and cloud IAM systems.
- Standardize on SCIM for provisioning when deploying or developing new applications or refactoring applications.

Business Impact:

- SCIM can be used to reduce the costs and time for administering identities across identity management boundaries. 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. SCIM's part is to help establish and standardize the communications and identity data exchange between two different applications.
- Traditional IGA tools use proprietary connectors to perform CRUD operations. User provisioning is not a problem for large SaaS applications with wide connector support from IAM vendors. However, it is an issue for the smaller, less commonly used applications. Ideally, when both provisioning and target systems support SCIM, provisioning is supported out of the box. If only the provisioning system supports SCIM, then generic SCIM connectors, gateways and brokers can be used by enterprise organizations for protocol translation and allow for wider interoperability and choice.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Aquera; IBM; Microsoft; Okta; Oracle; Ping; Radiant Logic; SailPoint; Salesforce; WSO2

Recommended Reading: "IAM Leaders' Guide to Identity Governance and Administration"

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

"Modernizing IGA Architecture for the Digital Enterprise"

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

"Architecting an Agile and Modern Identity Infrastructure"

Sliding Into the Trough

SaaS-Delivered IAM

Analysis By: Michael Kelley; Abhyuday Data

Definition: SaaS-delivered IAM has been trending up in the market as clients seek an alternative to software-delivered tools as well as the related infrastructure and people costs that accompany that approach. Up until recently, IAM SaaS offerings have seen the strongest growth in adoption in access management (AM), and authentication functionality. But now many other elements of IAM, like identity governance and administration (IGA) and privileged access management (PAM), are increasingly being offered through SaaS delivery models.

Position and Adoption Speed Justification: Driven by digital transformation initiatives, SaaS adoption for IAM services continues to grow. There are many organizations who require a hybrid approach due to a large portfolio of legacy applications, and these environments will require more effort to migrate entirely to SaaS, which will delay universal adoption. However, the majority of customers worldwide appear to be prioritizing SaaS approaches over software.

SaaS-delivered AM and authentication capabilities are very mature, with many organizations comfortable consuming multifactor authentication (MFA) as a SaaS offering. SaaS-delivered IGA is not yet mainstream, and not every IGA vendor offers it, however, Gartner has noticed a marked acceleration in client purchasing. PAM capabilities are still primarily being delivered via software, and in some instances are still bound to purpose-built appliances. However, several PAM vendors have started to offer SaaS-delivered options, and the ratio of SaaS-based PAM solutions is growing quickly for new purchases.

User Advice:

- Identify the 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.
- Evaluate the ability to use a SaaS-based IAM solution to resolve conflicts over duplicate IAM implementations. A SaaS-based platform augments these solutions by providing standardization and consolidation for all apps and users.
- For organizations that manage frequent acquisition and divestiture activities, leverage the agility of SaaS-based IAM solutions and quicker time to completion compared to software-delivered solutions.
- When considering new IAM purchases, use a responsibility and cost comparison framework to ensure appropriate comparisons between software and SaaS-delivered IAM implementations.
- Capture a more complete picture of the costs for software delivered tools by; auditing and documenting people and IT asset costs for owning and managing IT infrastructure, documenting project related costs for software upgrades, and audit and document ongoing support costs and planned obsolescence, which drives investment in new IT infrastructure. These costs can be used when evaluating transition and subscription fees for SaaS-delivered IAM platforms.
- For hybrid approaches, organizations required to maintain both software and SaaS tools based on application requirements, take a cloud first approach and consider software solutions as exceptions.
- If not already consuming MFA from SaaS, begin there, followed by access management, both of which are mature in adoption. Consider migrating PAM next, and consider IGA migrations last, due to the complexity of software implementations.

Business Impact: Organizations are using SaaS to fill gaps in enterprise IAM portfolios, IAM staffing functions and to achieve faster time to value. IAM staff can potentially be redirected to other areas. SaaS provides standard, consistent IAM functions to support both internal and cloud-based applications and users for multiple lines of business with disparate IAM infrastructures inside an enterprise.

SaaS is proven in authentication with SaaS representing the default choice in over 90% of the cases, as well as in AM and customer IAM (CIAM) use cases, in addition to growing PAM and IGA offerings. Popular SaaS offerings from a single vendor may not be able to replace functionally deep and broadly implemented IAM solutions in all organizations, but SaaS may be used to supplement those implementations, and to provide a bridge for digital transformation initiatives, some convergence between AM, IGA, and PAM in SaaS tools has been observed in the market.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Cisco-Duo Security; Entrust Datacard; Microsoft; Okta; OneLogin; Oracle; Ping Identity; SailPoint; Saviynt

Recommended Reading: "How to Choose Between Software and SaaS Delivery Models for Identity and Access Management"

"Predicts 2020: Identity and Access Management"

API Access Control

Analysis By: Henrique Teixeira; Michael Kelley

Definition: API access control is a subset of API security capabilities that enables authentication and authorization of API targets. API targets may include web and mobile applications and microservices. API access control is typically achieved with centralized policy management and the creation of security access tokens, with the support for OAuth 2.0, OpenID Connect (OIDC) and JSON Web Tokens (JWT) for protecting user-present and machine-to-machine scenarios.

Position and Adoption Speed Justification: API access control has grown in importance, as organizations have evolved their application architectures toward mobile apps, API clients and back-end services thus requiring more sophisticated authentication and authorization controls to APIs and microservices.

API security has traditionally been a domain of full life cycle API management offerings like API gateways (see "Magic Quadrant for Full Life Cycle API Management"). However, while API gateways provide more than access control functions (such as throttling and bot detection), they lack the session management capabilities, advanced adaptive access and support for evolving identity standards, which are features that AM tools provide. This lack of advanced IAM capabilities of API gateways 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 and OIDC as industry standards widely adopted by the vast majority of AM and API security vendors. Customer IAM is another big driver for recent API access control demand when developing more sophisticated privacy and consent management controls based on those protocols.

User Advice:

- When a mix of user-present and machine-to-machine access to API targets is needed, organizations should use AM products' deep support for OAuth 2.0, connections to repositories and the centralization of authorization policies along with API gateways for their complementary features. In other words, organizations should not engage in API-based apps development without both API gateway and API access control capabilities.
- Cost containment strategies for API access control should take in consideration AM tools that provide converged IAM features for APIs, and at least some "lightweight" API gateway capabilities such as traffic throttling to mitigate denial of service attacks. See the API target

enablement sections of " "Critical Capabilities for Access Management, Worldwide" for more details.

- Proprietary methods for API access control (like custom code using shared databases) should be phased out and replaced with standards-based supported API access control mechanisms: OIDC, OAuth 2.0 and JWT.
- API security now benefits from increased awareness and product feature coverage. However, application leaders must create and implement an effective API security strategy that looks beyond just API access controls, and also include other API threat protection controls, such as API traffic anomaly detection.
- API access control strategies should also take into consideration developer staff training and enablement, including education on how to apply standards to govern changes in the claims of security access tokens.
- Deploy policy enforcement points for API access control as close as possible to the service being protected. This will enable better efficiency of resources, like high-performance and nonblocking execution and defense in depth (at both microservices and other traditional network API endpoints).

Business Impact:

- API access control and API threat protection are both necessary elements of API security. API access control means controlling which applications and people can access APIs, while API threat protection means detecting and blocking attacks on APIs. Organizations need both.
- API access control plays a role in both workforce and customer IAM use cases. Customer data protection, consent management and data privacy strategies in modern applications will require API access controls for all user populations.
- API access control has a direct impact on application development training. It includes alignment between IAM and security experts for adoption of best practices for API access controls and threat protection respectively.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Amazon Web Services; Broadcom; Cloudentity; Curity; ForgeRock; IBM; Micro Focus; Microsoft; Okta; Ping Identity

Recommended Reading: "Critical Capabilities for Access Management, Worldwide"

"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"

Bring Your Own Identity

Analysis By: David Mahdi; Felix Gaehtgens

Definition: Bring your own identity (BYOI) is the concept of allowing users to select and use an external (third-party) digital identity, such as a social identity (Facebook, VK, WeChat, etc.) or a higher-assurance identity (such as a bank identity, or a government eID) to assert their identity in order to access multiple digital services. Service providers 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.

Position and Adoption Speed Justification: BYOI consists of several mechanisms and technologies, each with their own level of adoption and maturity. Social identities are well established and have been the most commonly used type of digital ID with BYOI; however, this mechanism comes with issues regarding privacy as the use of social identities leaves a digital "bread crumb" (log of activity) with social media providers, and have a relatively low assurance of identity, as many social media providers do not perform identity proofing when establishing user credentials.

The year 2019-2020 has seen much progress in comparison to earlier years. The EU electronic IDentification, Authentication and trust Services (eIDAS) regulation established minimum identity assurance requirements and mandated interoperability by 28 September 2018. Organizations delivering public digital services in an EU member state must now recognize electronic identification from all EU member states, and EU Trusted Service Providers can enable users to sign legal documents using digital signatures. In Canada, SecureKey launched Verified.Me, in addition to the already established Concierge service. WeChat was chosen to deliver an electronic eID in Guangzhou, China in late 2018, with expansion to other provinces in 2019.

Financial institutions also forged ahead with interoperable digital identities. In the Nordics, partnerships between the government and financial institutions are already established. Capital One's Identity Services was launched in 2017 and expanded, including through acquisitions of technology. Mastercard announced a consumer-centric model for digital identity in 2019. Other tech titans such as Apple announced and launched "Sign in With Apple" in 2019, which leverages Apple digital identities.

Furthermore, new and innovative approaches to decentralize identity also known as "blockchain identity" and "self-sovereign identity" are spawning a lively mix of startups and industry consortia, and large technology providers are also investing in this area.

User Advice: Recognize that the proliferation of siloed, noninteroperable digital identities will not scale with the needs of digital business. Determine how to take value from, or in some cases, contribute to, the BYOI landscape. Especially for B2C or G2C initiatives, there are 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. BYOI can alleviate this.
- Honeypot for identity credentials and personal information: Mitigate risks here by enabling customer and other users to rely on BYOI. However, by not considering BYOI, full responsibility for identity and credential exposure remains with the enterprise.

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.

Determine the overall model of the approach to consumer access: Will you accept other methods for BYOI (i.e., accept third-party identities)? Will you be a third-party IdP, that will offer identities for consumption by other organizations?

Business Impact: BYOI offers the potential to leverage outside identities to help reduce friction and to increase adoption, security and overall end-user satisfaction. Exploiting higher trust BYOI for customer registration potentially avoids the cost of doing your own identity proofing, as can relying on high assurance iDPs to perform appropriate risk assessment and MFA at authentication, lowering the barrier to new business models that require higher levels of identity assurance. This can cause some transformational impacts on certain industries, especially in the era of digital business.

Many organizations have made significant investment in their IAM approach and to retain the customer, and therefore have established themselves as custodians of digital identity. However, only a small number of these organizations will likely be able to monetize their existing client basis by becoming a third-party IdP. Key decision points that can motivate a move in this direction include:

- Monetization of identity attributes
- Brand loyalty
- User demographics
- Security and privacy concerns

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon; Apple; Evernym; Facebook; ForgeRock; Google; Microsoft; SecureKey; Signicat; Twitter

Recommended Reading: “Innovation Insight for Bring Your Own Identity”

"Innovation Insight for Decentralized and Blockchain Identity"

"Cool Vendors in Blockchain Technology"

OpenID Connect

Analysis By: Henrique Teixeira

Definition: OpenID Connect (OIDC) is an identity layer on top of the OAuth 2.0 protocol that enables web services to outsource identity authentication and authorization 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.

Position and Adoption Speed Justification: 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. There is ongoing and 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 multiparty federation work (OpenID Connect Federation) and the OIDC profile for SCIM services, which client applications may use to discover availability of and register for, and access, SCIM services.

Nearly all access management (AM) vendors already support parts of the specification. 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.

The list of SaaS applications supporting OIDC is growing, however, its growth is slower and has a smaller market penetration than SAML. Gartner estimates that less than 15% of SaaS applications support OIDC. However, there is an increase in interest in the protocol, and it's poised to replace SAML for new applications. 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 in line with Gartner's continuous adaptive risk and trust assessment (CARTA) principles will accelerate its time to achieve plateau and become mainstream.

User Advice: We recommend:

- RESTful approaches are increasingly favored for new development and implementations. Give preference to OIDC over SAML as it provides better support for consent management and is more lightweight. Use OIDC for modern application "greenfield" developments, especially when target resources include APIs.
- Mobile network providers, finance, government and healthcare institutions should evaluate OIDC for its industry applicability defined in recent drafts from working groups like: The MODRNA, Financial API (FAPI), iGov and HEART working groups, respectively.

- Where there's a mix of new applications that need OIDC support, as well as older applications that need SAML or proprietary access techniques, leverage an AM tool that supports multiple protocols and can do translation among protocols and security token formats.
- Tell application vendors to increase support to OIDC, pointing to the need for integration with enterprise and cloud IAM systems, providing an alternative to SAML especially when a more lightweight method is expected for both authentication and authorization to services.
- Some AM and SaaS application vendors still do not support all of the OIDC specification extensions, due to the fact extensions to the standard continue to be defined and refined (i.e., best practices for the implementation of implicit authentication flows, which are being revisited). If that is the case, organizations should press IAM and SaaS application vendors to prioritize the adoption of at least the core portions of the standard.

Business Impact: OIDC provides the tools for enabling improved user experiences, by adding convenience (lightweight authentication and authorization) and control (fine grained consent management, for example). It reduces the data entry burden on users registering with and revisiting service providers, and it provides single sign-on and federation support for modern apps as well.

As interoperable implementations increase, OIDC allows 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.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Auth0; ForgeRock; Gluu; Google; IBM; Idaptive; Microsoft; Okta; Ping; Salesforce

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"

"Single Sign-On in Native Apps and Modern Web Apps"

"Solution Comparison for OAuth-Based Access Management Capabilities of Nine Vendors"

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

Mobile Identity

Analysis By: Rob Smith; Ant Allan

Definition: Mobile identity supports the trusted identification of the devices people use to access the corporate network, cloud resources or other assets, as well as the users themselves. Mobile

identity is typically a capability of mobility management tools, rather than a discrete solution. It puts public-key credentials (a digital certificate and keys) on the device. It supports the recognition of corporate-authorized devices and adds confidence to user identity claims.

Position and Adoption Speed Justification: Enterprises increasingly look to defend against phishing and other account takeover (ATO) attacks, especially for users connecting remotely and from mobile devices. This generally drives investment in multifactor authentication (MFA) solutions. However, at the same time, enterprises are looking to improve user experience (UX), especially in the context of employee experience (EX) in the digital workplace. Thus, there is a strong focus on methods that enhance authentication, without adding additional friction and eroding UX, which is where mobile identity adds value. Mobile identity based on X.509 credentials increases the confidence in device ownership and elevates trust during authentication steps, compared with noncryptographic methods for endpoint device identification. This is a cornerstone of zero-trust network access (ZTNA), for example.

Mobile identity is well-established in most enterprises that have implemented unified endpoint management (UEM) or mobile device management (MDM) tools. This enables enterprises to allow access to corporate networks, without having to invoke orthodox MFA every time.

In addition, some vendors such as Microsoft and VMware bundle access management (AM) capabilities (e.g., single sign-on [SSO] and authorization) with their UEM tools, enabling tighter integration of mobile identity in a broader access context. AM tools are typically able to consume mobile identity as part of evolving adaptive access approaches.

User Advice: Exploit mobile identity as a way to recognize when a corporate-authorized device is being used to access the corporate network and as a way of increasing confidence in the identity of the user. In conjunction with UEM/MDM policies that enforce a passcode policy or use of device-native biometric authentication (e.g., Apple Touch ID), mobile identity might provide sufficient confidence for baseline (lower risk) access. However, take a risk-averse approach and combine mobile identity with legacy passwords or other orthodox authentication methods when a higher level of trust is required.

Consider investment in PKI tools offering certificate services that can integrate with most modern UEM and MDM tools, or work directly with the mobile devices.

As part of a broader authentication and access strategy, use mobile identity as an input to AM tools as a potential way of skipping MFA prompts to improve UX. For example, in Microsoft Azure AD Premium, a Microsoft Intune managed device is a “trusted device” that can satisfy the strong authentication requirements of a conditional access policy without an explicit MFA challenge to the user. (MFA would still be required when enrolling a new device or when accessing assets from untrusted devices.)

Explore more-generic tools that implement more-robust software cryptographic tokens (which always include user certificates, rather than device certificates) on managed or unmanaged devices. These include proprietary solutions, from vendors such as Beyond Identity or Entrust Datacard, and Fast IDentity Online (FIDO) 2 authenticators (see “FIDO Authentication Protocols” in “Hype Cycle for

Identity and Access Management Technologies, 2020"). Note that FIDO protocols also establish device identity, as the credentials are unique to each combination of relying party, user and device.

Prefer mobile identity implementations (or alternative cryptographic tokens) that embed keys in a trusted execution environment (TEE) or secure enclave on the device.

Business Impact: In some circumstances, mobile identity can enable passwordless access to corporate networks for users employing corporate-authorized devices. More generally, it provides additional confidence in a claimed user identity. It can enable access without the friction of orthodox MFA, especially when integrated with AM tools implementing adaptive authentication in line with continuous and adaptive risk and trust assessment (CARTA) principles. In general, the net benefit is enhanced UX, improving EX for remote work among other use cases.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: BlackBerry; Citrix; DigiCert; Entrust Datacard; IBM (MaaS360); Microsoft; MobileIron; Okta; Sectigo; VMware

Recommended Reading: "Magic Quadrant for Unified Endpoint Management Tools"

"Market Guide for Zero Trust Network Access"

"Passwordless Authentication Is Here and There, but Not Everywhere"

"Transform User Authentication With a CARTA Approach to Identity Corroboration"

Climbing the Slope

Externalized Authorization Management

Analysis By: Felix Gaehtgens

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 can implement multiple authorization methodologies, including attribute-based/role based access control (ABAC/RBAC).

Position and Adoption Speed Justification: EAM is often deployed tactically to target specific off-the-shelf applications (such as Microsoft SharePoint, Dynamics 365 or SAP applications). Strategic deployments of EAM focus on providing an authorization framework for custom software development efforts.

Organizations also look into EAM to support opening up legacy systems through API gateways. Furthermore, compliance continues to be a key driver for EAM — an example being General Data Protection Regulation (GDPR), which requires organizations to support more-granular data access authorization. During the past year, this question came up in inquiries about customer identity and access management (CIAM), especially for the enablement of more dynamic authorization requirements and adaptive access to customer data. 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.

Because they need to be tightly integrated, EAM implementations are still rare, compared with coarse-grained authorization provided by access management (AM) tools, the integration of which is much looser and simpler.

The prevalent standard for EAM policies is the Extensible Access Control Markup Language (XACML). There has also been progress in standardizing a REST/JSON profile for XACML. Apart from XACML, proprietary policy mechanisms also exist:

- The emerging Next Generation Access Control (NGAC) specification and its reference implementation broaden runtime authorization architecture options, as part of a standard methodology as defined by ANSI and the International Committee for Information Technology Standards (INCITS).
- The Open Policy Agent (OPA) is starting to be used for orchestrating policy over infrastructure and applications, including container management systems, such as Kubernetes.

User Advice: Seek opportunities to use EAM to establish an authorization framework that is external to applications and systems and provide a consistent way of defining and enforcing authorization policies.

Use EAM should to remove custom authorization code for decision and enforcement from homegrown applications and move it into an easier-to-maintain, consistent framework for centralized policy management. Policy decisions are based on a variety of inputs, using a combination of attributes and rules, and can protect a variety of objects, such as transactions, webpages, files and database objects.

Use EAM when externalized and centralized fine-grained authorization across a variety of applications is desired. Developer buy-in is essential. When evaluating EAM solutions, conduct evaluations against two sets of requirements: policy management services and policy runtime services (decision and enforcement). Policy management can usually be consolidated and potentially centralized. Runtime services are still fragmented by integration patterns:

- Near-natural language (NNL) policy authoring and policy conversion tools can translate simple policies to various machine-readable policy formats, such as JSON or XACML.
- When looking to define centralized authorization policies for infrastructure (systems, containers), evaluate the communities and vendors emerging around Open Policy Agent.

- When looking to retrofit existing applications with EAM, look at specialized solutions that cover their immediate needs by integrating into native entitlement systems, but can also provide standardized authorization methods (typically XACML support) for future developments.
- When considering EAM, explore adjacent product areas, such as API gateways and AM tools implementing adaptive access to extend the scope of authorization and enhance the overall security posture.
- Mandate robust management of attributes and data that is used in policy evaluation, because EAM requires it.

Business Impact: EAM is a long-term investment in an architecture for granular control of application and data access. Its use in business applications and data systems can significantly change the consistency, flexibility and granularity of authorization, resulting in better access control, audit and compliance results over a broader set of infrastructure, applications, services, transactions and data. Doing so can help developers focus on delivering functionality and outsource access decisions made by the EAM tool.

EAM investments return the most value when:

- Implementations are focused and often constrained to a set of related business functions
- Strong governance is in place for data and entitlements are used as input to access decisions
- There is continued commitment to policy change management

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Axiomatics; Cyberinc; ForgeRock; Ionic Security; Jericho Systems; NextLabs; ObjectSecurity; PlainID; Styra; WSO2

Recommended Reading: "Improving Runtime Authorization Maturity"

"Decision Point for Selecting Runtime Authorization Architecture Patterns"

"A Systematic and Practical Approach to Optimizing Authorization Architecture"

Customer IAM

Analysis By: Michael Kelley; Henrique Teixeira

Definition: Customer identity and access management (CIAM) manages identity, authentication and authorization for customer access. CIAM is necessary for public-facing applications that require customers to register identities and create and use accounts.

Key CIAM features include:

- Self-service for registration (password, profile and consent management; progressive profiling)
- Authentication and authorization into applications
- Identity repositories
- Reporting and analytics
- APIs and SDKs for mobile applications
- Bring your own identity (BYOI)

Position and Adoption Speed Justification: 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, password management and BYOI integration options.

From GDPR in the EU, to LGPD in Brazil, to CCPA 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, highlights the increased need to provide consumer 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, but native functionality for online fraud prevention, and preference and consent management are not yet fully developed.

User Advice: While there are some IT organizations that know how to build capabilities that get the online user experience "right," many organizations run very lean, and lack the skills and knowledge to develop an outstanding online customer experience. Our advice is to:

- Avoid developing CIAM capabilities that vendors can offer out of the box by acquiring commercially available CIAM solutions that: (1) are aligned to your strategy and staff expertise, and (2) provide a strong IAM infrastructure that supports native integrations for expansions. Significant business value is driven through marketing, sales and CRM integrations with CIAM.
- Use the intelligence provided by identity analytics and reporting features provided by CIAM products to dynamically discover and respond to ever-changing customer preferences and requirements.
- Develop a privacy strategy for customer identities, including choosing a CIAM vendor who has demonstrated the ability to meet the rising bar of privacy for customers. Pair CIAM capabilities with a consent and preference management tool for advanced functionality to strengthen the ability to comply with privacy regulations. And in financial services and retail industries, work with fraud leaders to augment CIAM with online fraud prevention tools.

Business Impact: In a world of near-instant gratification, the online portals of any business are the face of that business. Much like proprietors of the past coached their employees to greet customers walking in the front door with a smile, the modern web portal and mobile application have become

the embodiment of that first impression for digital businesses. CIAM products are core to creating the outstanding user experience so necessary for success in online commerce and digital business.

There are other business benefits of adopting CIAM solutions. The first is optimization and efficiency — homegrown CIAM solutions can be a drain on developer and IT resources, both for support and for creating modern functionality. Second is the acquisition of knowledge for complying with privacy regulations. 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.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Akamai; Auth0; ForgeRock; LoginRadius; Microsoft; Okta; OneLogin; Ping Identity; Salesforce; SAP

Recommended Reading: "Technology Insight for Customer Identity and Access Management"

"Key Features for Customer Identity and Access Management"

"Critical Capabilities for Access Management"

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

IAM Managed Services

Analysis By: Kevin Kampman

Definition: Identity and access management (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 software vendors or IAM professional services firms. IT outsourcing firms have also provided these services in the form of staff augmentation, supplying personnel to perform engineering and operational functions as part of their clients' IAM teams.

Position and Adoption Speed Justification: Interest in IAM managed services exists among organizations seeking alternative models for managing their IAM functions. The main driver of interest is the difficulty organizations face in attracting, training and retaining personnel with the right skills to manage and support IAM operations. New entrants adopting IAM, particularly in midsize enterprises, and organizations replacing their existing IAM due to modernization are challenged to meet skilled resource demands. An additional driver is the need for round-the-clock support for global IAM deployments. IAM managed services have become 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.

Offering IAM managed services is attractive for IAM professional services firms because it provides opportunities for annuitized streams of revenue. IAM managed services are frequently provided as staff augmentation, but more full-service variants are a top area of investment for IAM professional services firms. In these firms, methodologies and packaged solutions are being developed in an effort to make the services more attractive, profitable and inexpensive. Managed services will compete with and perhaps complement self-managed cloud-architected IAM technologies. These have a more straightforward adoption model but may still require support when organizations lack their own skilled resources.

User Advice: IAM managed services exist in a niche 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 is sufficiently 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. Combinations of IAM functions are often aggregated by services firms to provide a more 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 increasingly split between product and managed services firms. Identity governance and administration (IGA) and privileged access management (PAM) have seen growth in the number of cloud-architected solutions made available and IGA often requires managed services support due to their complexity.

Some IAM managed service providers continue to support 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.

Organizations interested in IAM managed services may initially consider such services to be a transitional move toward delivery of their IAM services using cloud-architected models. Start by looking for 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. Consider 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.

When utilizing IAM managed services, keep track of the evolution of supported services toward commoditization, at which point such services may be transitioned to more cost-effective SaaS-delivered IAM.

Business Impact: Managed services have the potential to provide businesses with a cost-effective way to:

- Extend support coverage beyond normal working hours
- Help address staffing problems or shortages

- Gain access to experts that can optimize IAM deployments
- Ensure continuous support for on-premises and cloud IAM by delegating it to a third-party provider

The ultimate benefit derived from IAM managed services is greater flexibility in support of business operations. For organizations needing highly customized IAM solutions with extensive support for on-premises systems, IAM managed services can provide a midterm solution to staffing and management issues until better options are available through SaaS models.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Accenture; Cognizant; Deloitte; EY; Identropy; IDMWORKS; Infosys; Novacoast; Simeio Solutions; Tata Consultancy Services (TCS)

Recommended Reading: "Best Practices for Engaging With Identity and Access Management Professional Services Firms"

"Market Guide for IAM Professional Services, Worldwide"

"Toolkit: Selecting IAM Professional Services"

OAuth 2.0

Analysis By: Abhyuday Data

Definition: OAuth 2.0 is an authorization framework that delegates access rights to applications and services. OAuth 2.0 defines an authorization server that issues tokens to applications, which then make authorized API calls to the resource server by sending the received tokens. The resource server then validates, authorizes or rejects the access tokens.

Position and Adoption Speed Justification: The OAuth specification was originally developed to enable users to grant others access to their web-based information without divulging passwords. However, OAuth 2.0 has evolved to support many more use cases and is needed to support the increasing requirements for multiparty interactions, native web and mobile applications usage, and API services proliferation. OAuth 2.0 can protect APIs and services from any type of application. This includes native applications, JavaScript-based applications running in web browsers, services or web applications by shifting the complexity from the client to resource server communication into client to authorization server communication.

OAuth 2.0 is an evolving framework and is standardized under the Internet Engineering Task Force (IETF). All access management (AM) tools support OAuth 2.0 to handle multiple use cases. OAuth 2.0 is commonly used to protect new RESTful APIs and services, particularly when interactions involve human users. OAuth 2.0 is a more-secure alternative than users providing their passwords

to third-party apps. The U.K.'s Open Banking Standard supports OAuth 2.0 authentication framework as a standard to meet PSD2 requirements.

OAuth 2.0 provides an important underpinning for the future of authentication and authorization services. OpenID Connect (OIDC) is an identity layer built on top of the OAuth 2.0 protocol that enables web services to outsource identity authentication and authorization to a third party. Authorization server, the epicenter of the OAuth2.0 framework provides authentication, authorizes access, handles consent, and, ultimately, creates tokens and facilitates OIDC interactions. OAuth 2.0 also has built-in capabilities to handle privacy and can enable impersonation, delegation and obfuscation of personally identifying information (PII) when needed. OAuth 2.0 and its derivative standards are fundamental in API access control techniques used in AM, API security and API gateway technologies.

User Advice:

- Continue to use and deploy OAuth 2.0 to abstract authorization, balance security, privacy, usability and scale when building and deploying your applications and services.
- Prioritize evaluating OAuth roadmaps for AM and API gateway tools.
- Leverage newer capabilities intended to better secure OAuth 2.0 interactions, such as token exchange, proof of possession 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.

Business Impact: The OAuth 2.0 framework helps IAM leaders streamline authentication and authorization decisions to target applications. OAuth 2.0 is a relevant method of supporting authorization and authentication for web, mobile and single-page apps; APIs; microservices; and Internet of Things (IoT) use cases. OAuth 2.0 authorization framework uses token formats, such as JavaScript Object Notation Web Token (JWT), which is digitally authenticated and trusted to transfer data between various parties and enables flexible deployment of OAuth.

Using OAuth 2.0 for authenticating multiple API services and applications, in public and private settings, improves an organization's internal architecture where JWT works as bearer tokens to make implementations easier. To comply with the growing adoption of privacy regulations, end users can allow or deny access to their data. It's also possible to limit the amount of personally identifying information (PII) that's sent to services and applications using OAuth 2.0 framework.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Sample Vendors: Akamai Technologies; Auth0; ForgeRock; IBM; Microsoft; Okta; OneLogin; Oracle; Ping Identity; SAP

Recommended Reading: "Magic Quadrant for Access Management"

"Critical Capabilities for Access Management"

"IAM Leaders' Guide to Access Management"

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

"Solution Comparison for OAuth-Based Access Management Capabilities of Nine Vendors"

Biometric Authentication Methods

Analysis By: Ant Allan; Tricia Phillips

Definition: Biometric authentication methods use unique morphological or behavioral traits to corroborate a person's claim to an identity previously established to enable access to an electronic or digital asset. A biometric authentication method is typically used in one-to-one comparison mode (biometric verification) to support an implicit or explicit identity claim. Rarely, a method is used in one-to-many search mode (biometric identification): the person simply presents a biometric trait and the system determines the identity from a range of candidates.

Position and Adoption Speed Justification: Biometric authentication is increasingly used across a variety of use cases, especially in mobile banking and, more recently, in enterprises rolling out Windows 10 with Hello for Business. Drivers for adoption are improved user experience (UX) and increased trust and accountability. However, concerns about privacy and presentation attacks inhibit forward movement and still create disillusionment with these technologies.

Usability and reliability issues with fingerprint modes have inhibited adoption for workforce use cases and negatively influence buyers' attitudes toward all modes, client interest has continued to grow due to Microsoft's support for face and other modes in Windows Hello for Business.

Vendors increasingly support Fast IDentity Online (FIDO) authentication protocols that can simplify implementation through standardization. W3C Web Authentication browser support for FIDO2 will likely speed up adoption and increase penetration over the next two years.

Clients' privacy concerns tend to focus on data security issues, but the main hurdle is privacy regulations' demand to be able to justify the use of biometric methods. Clients also worry about biometric methods' vulnerability to presentation attacks and other potential compromises even though these are far less likely than password compromises.

User Advice: Biometric methods are a viable alternative or adjunct to passwords and tokens across a variety of use cases. However, trust, TCO and UX vary between modes, and their viability varies by use case. Biometric methods can provide greater individual accountability than alternatives and should be favored when this is paramount.

The utility of biometric authentication depends on effective presentation attack detection (PAD) or liveness testing. Carefully evaluate vendor claims and favor methods tested in conformance with

ISO/IEC 30107-3:2017. However, successful presentation attacks are rare. Evaluate how vendors can mitigate replay and injection attacks, which are more scalable and thus a more significant risk.

As with any authentication method, poor exception handling (in the event that the biometric method is unavailable) and identity recovery processes give attackers an easier path to account takeover.

Most modes can provide better UX for most people than nonbiometric alternatives, and this benefit is particularly relevant to mobile use cases. Banks commonly integrate device-native modes in mobile banking apps, but third-party face and voice are emerging as the modes of choice. Favor modes that can make use of standard inputs (camera and microphone) and offer multiple benefits over device-native methods.

Consider migrating to biometric authentication for Windows PC and network access but recognize the limitations of Windows Hello for Business (e.g., biometric methods cannot be mandated). Evaluate vendors that offer broader endpoint and use-case support and choice of biometric modes, including those that combine biometric modes with phone-as-a-token methods for mobile multifactor authentication.

Weigh the pros and cons of local vs. centralized data storage; comparison and matching; and PAD. Favor centralized architectures:

- To more readily support multiple digital (and other) channels and devices and, especially in banking, to exploit biometric data captured during identity proofing.
- To provide more direct control over data security, PAD and functional integrity.

Architectures differ in the effort needed to comply with privacy regulations, but the architectural choices cannot avoid the general justification requirements set out in the EU General Data Protection Regulation (GDPR) and similar privacy mandates.

Business Impact: Because biometric traits cannot easily be shared, biometric methods with effective PAD and functional integrity can provide increased trust and accountability over other credential-based methods. They also provide improved UX for most people.

Biometric methods suit mobile use cases, where users — especially retail customers — resist having to use any kind of discrete token. Biometric methods may be integrated within mobile apps (as they are in mobile banking), apps for mobile push authentication and so on.

Biometric methods can be used for PC and network login. Proprietary solutions offer broader endpoint and use-case support and choice of biometric modes and thus provide more value than device-native biometric methods supported by Windows Hello for Business.

Active and passive voice modes, which are increasingly used in contact centers as a welcome alternative to the abysmal standards of knowledge-based verification (KBV), are a natural fit for virtual personal assistant (VPAs or “smart speakers”).

In addition to the methods represented by this profile, passive behavioral modes (keyboard, gesture and handling dynamics) provide additional recognition signals that can add significant value to

analytics-based tools, including online fraud detection (OFD) tools, elevating trust and improving UX by reducing false positives (i.e., bogus fraud alerts). In this context, these modes can also provide bot detection.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Auraya Systems; FaceTec; iProov; ImageWare Systems; Keyless Technologies; OneVisage; SensibleVision

Recommended Reading: "Best Practices for Selecting New User Authentication Methods"

"Technology Insight for Biometric Authentication"

"Technology Insight for Phone-as-a-Token Authentication"

"Market Guide for User Authentication"

"Predicts 2019: Identity and Access Management"

Entering the Plateau

Document-Centric Identity Proofing

Analysis By: Akif Khan; Jonathan Care

Definition: Document-centric identity proofing brings an identity claim in an online (browser or mobile app) interaction within organizational risk tolerance by:

- Capturing an image of a photo identity document and determining there are no signs of tampering or forging.
- Capturing and analyzing images or a video clip of the person claiming the identity to determine the claimant is present and, by comparing against the document photo, the legitimate bearer of the document. Biometric comparison is typical, but comparison may be done by human specialists.

Position and Adoption Speed Justification: Identity proofing within the online environment continues to grow in importance as digital transformation in regulated industries, such as financial services, takes place. The increased need for remote onboarding has been accelerated by the COVID-19 pandemic.

The continued stream of large-scale breaches of customer data provides a profitable source of identity data which fraudsters use to exploit traditional data-centric identity proofing methods. This has further increased Gartner client interest in document-centric proofing methods as a means to increase the barrier for those wishing to deceive the identity proofing process.

This profile supersedes the Identity Proofing and Corroboration profile published in past Hype Cycle research. The data-centric components of the previous profile are now considered mainstream. The document-centric focus in this profile reflects client interest in a distinct and maturing technology.

User Advice: Despite the seemingly automated nature of the document assessment process, the vast majority of vendors use a combination of algorithms and manual processes. In the first instance, the algorithms attempt to determine the authenticity of the document against the vendor's document libraries. If it is not possible to achieve the required levels of confidence, then manual review is used. Explore this point with vendors to ensure response times can meet requirements and that scalability is possible.

Recognize that the vendors in this space do not typically compare documents against any external sources. Checks consist of comparing document images against internally held libraries. In this context, the vendors are providing a digital version of a bank clerk or bartender physically inspecting a document and checking a person's likeness. Some vendors have connected to third parties to offer know your customer (KYC) and anti-money-laundering (AML) checks and Gartner recommends assessing such vendors.

Interrogate vendors regarding detection rates for the document types that will be most relevant to your requirements. A vendor may excel in detecting forged U.S. passports but be less accurate with U.K. driving licenses, for example.

Require the vendor to carry out presentation attack detection (PAD) during capture of the facial image to obtain confidence that the claimant of the identity is present. Some vendors rely on NIST-certified third-party functionality, others develop their own capability. The approach to PAD will influence the UX, and evidence should be sought of efficacy as well impact on abandonment rates.

Business Impact: Document-centric identity proofing can provide key a component of the KYC customer identification procedures required in regulated industries such as banking or gambling. It does not constitute the entirety of the KYC process, though, and should not be mistaken for doing so even when vendors describe it as "eKYC."

For many other account creation use cases, such as in e-commerce where proof of identity is not required, the "ID plus selfie" process would be considered overkill and an inconvenience.

Finally, the "ID plus selfie" process can be used 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, thus avoiding the need to provision and manage authentication credentials. However, the potentially poorer UX makes it a less attractive alternative in lower-risk events (e.g., initial login).

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Acuant; Authenteq; IDmission; Jumio; Mitek; Onfido; Trulioo

Recommended Reading: "Market Guide for Identity Proofing and Corroboration"

Enterprise Digital Rights Management

Analysis By: Steve Riley

Definition: Enterprise digital rights management (EDRM) is a set of discrete technologies that is used to apply mandatory access and usage control on unstructured data such as emails, office and CAD documents. EDRM combines cryptography with identity services and policies to restrict if and how data can be accessed and used (e.g., cut, pasted, printed, viewed, deleted, edited and/or forwarded). EDRM content is typically accessed via client applications that natively support EDRM, an EDRM endpoint agent, plug-ins, wrappers, web browsers or secure viewers.

Position and Adoption Speed Justification: EDRM solutions have been available in one form or another since the 1990s. Although the technology is elegant and the value of EDRM is sound, it is complex and impacts end-user workflows. The progress observed over the last few years focused on making a narrow set of use cases more user friendly and to enhance the integration with other technologies. While Gartner continues to see a steady increase in EDRM interest due in part to the loss of control associated with SaaS adoption and the erosion of trust in the ability of partners to effectively secure data per nondisclosure agreements, we have not seen a matching increase in operational deployments. The reasons for this are a lack of standardization and overall solution complexity.

Early adopters focused on intellectual property protection and data privacy — especially among financial services, pharmaceutical and product development/engineering firms — have initiated pilots and some rollouts of EDRM that are focused on specific business units, workgroups or processes. Few global organizations have large-scale deployments in actual use, but the increased exposure of Microsoft's Azure Information Protection has brought about some change, at least among organization committed to Microsoft infrastructure and services.

Lack of even a market/industry standard continues to make it difficult for the technology to be integrated in a broader set of applications and cloud services, limiting its usability and reach. Ongoing complexity issues regarding internal- and external-facing deployments, user experience, technology limitations and costs impact market growth and further limit its practical applications. If standardization does not happen, it is entirely possible that this technology will reach the Plateau of Productivity with relatively broad adoption but yet very narrow applications.

Additional analysis by Mario De Boer.

User Advice: Consider EDRM as a precision protection mechanism knowing that it requires significant planning, and ongoing solution management and user training during deployment. EDRM combines three security technology services (cryptography, identity and access control, and usage control) in a single solution. Expect that implementation challenges typically associated with each of these will also be present with EDRM deployments.

Although very attractive in terms of capabilities, EDRM can be complex and impractical to solve generic data protection issues. Organizations should focus on well-defined use cases where

alternative technologies (e.g., DLP, CASB, device or file level encryption, access control, watermarking, etc.) are ineffective or cannot be deployed.

EDRM policy management can be complex and has been a consistent source of failure in the past when left in the hands of the users. Orchestrate EDRM with data classification, data loss prevention (DLP) and cloud access security broker (CASB) tools, and leverage integrations with file repositories and business applications to allow the automation and consistent enablement of EDRM, and help prevent user mistakes or unsupported experimentation.

Think through the full life cycle of the data across all applications expected to process it, including security applications expected to inspect the content, indexing services to enable searching, discovery processes, and long-term retention/archiving applications. EDRM deployments across this diversity of applications can present significant integration challenges because of key management, policy enforcement and architecture support issues. These problems can be minimized by limited deployments to small workgroups or communities of interest dealing with sensitive data that has a short lifetime (typically less than 12 to 18 months).

Business Impact: EDRM technologies protect against intellectual property loss, and against inappropriate or unintended disclosure of proprietary or confidential enterprise information and can allow data owners to audit and adjust access to specific data wherever it resides. It is one of the only approaches to retain control of unstructured data transferred to business partners in secure collaboration use cases.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Sample Vendors: Adobe; Fasoo; Intralinks; Iconic Security; Microsoft; NextLabs; SealPath; Seclore; Vaultize; Vera

Recommended Reading: “How to Select the Right Enterprise Digital Rights Management Solution”

“Succeed With Enterprise Digital Rights Management, Five Steps at a Time”

“How to Secure a Content Collaboration Environment”

“Market Guide for Information-Centric Endpoint and Mobile Protection”

“How to Implement Enterprise Digital Rights Management to Control Unstructured Data”

X.509 Hardware Tokens for User Authentication

Analysis By: David Mahdi

Definition: X.509 hardware tokens are tokens carrying X.509 public-key infrastructure (PKI) credentials primarily for user authentication. Typical form factors are smart cards (either contact or

contactless) or USB tokens that embed the same kinds of chips. Multifactor X.509 smart tokens — PIN-protected or (very rarely) biometric-enabled — provide high trust.

Position and Adoption Speed Justification: The most common use case for X.509 hardware tokens is Windows PC and network login. They remain the most technically mature and most widely implemented alternative to passwords. But overall adoption is low due to complexity.

In addition, adoption is low since it is seldom the case that all users need the high trust these tokens can provide. Furthermore, provisioning and managing these tokens are relatively expensive, and user experience (UX) is poor. Gartner sees increasing interest in alternatives that give better trade-offs among trust, cost and UX.

More significant barriers to adoption in remote access and, especially, mobile use cases persist and signal the technology's obsolescence before the Plateau of Productivity. Gartner sees a majority of clients seeking alternatives for these use cases — for example, phone-as-a-token methods and, for mobile, biometric methods and FIDO2-based options. The technology will likely persist in the long term only if mandated by regulations. Gartner has already seen U.S. military and various other agencies seeking alternatives to DoD CACs/PIV cards.

User Advice: Evaluate the benefits of these tokens against the needs of each use case where:

- There is a clear need for high-trust login to Windows PCs, networks and sensitive applications.
- There is a clear need for other PKI-based security services such as digital signature.
- Their use is demanded by legislation or regulations (for example, eIDAS or Homeland Security Presidential Directive [HSPD] 12).

Although X.509 smart cards can extend to support both physical and logical access (becoming common), existing building access cards can be used in the same way (albeit with lower trust).

X.509 smart tokens are not a good first choice in remote access or mobile use cases because:

- Problems with smart card readers and middleware are hard to resolve remotely, impacting user productivity.
- Support is dependent on the mobile OS. Mobile-compatible readers incur a sometimes-prohibitive additional cost and add bulk to the device, reducing UX.

Use alternative methods if you have the freedom to do so. Among these alternatives are X.509 software tokens (user certificates or "soft certs") on the endpoint device. These tokens can be held in a secure element (such as a trusted platform module [TPM]) to provide a virtual smart card for protection against credential theft. However, these options offer lower trust than having the credentials in a discrete physical token. Clients should be aware that additional components such as middleware may be required to leverage devices such as TPMs and other types of secure elements.

Nascent Bluetooth LE tokens holding X.509 credentials might provide an alternative that can be easily used with any endpoint device.

Although still nascent, Microsoft Windows 10 deployments with Windows Hello for Business (WHfB) allow for other authentication options (such as biometric methods) that could act as alternatives to X.509 smart tokens. In essence, WHfB leverages private keys generated and stored in the local Trusted Platform Module (TPM), in certificate trust mode; this approach mimics a smart card, by using local hardware combined with a local biometric (i.e., face, or fingerprint). WHfB, also supports various other authentication methods. In addition, FIDO tokens (i.e., Google Titan Security Keys or YubiKey from Yubico) offer alternatives to traditional X.509 smart tokens as well.

Note that X.509 tokens can be used as bearers of other authentication mechanisms, such as to hold user biometric references for biometric authentication or as one-time password tokens.

Business Impact: X.509 tokens provide high-trust user authentication, especially for Microsoft Windows PCs and networks, and can support multiple additional functions (for example, enabling encryption, digital signatures).

However, the complexity of the necessary infrastructure and the associated support costs may be barriers. And X.509 tokens have the most positive impact where there is a clear need for high levels of trust or a need to provide other X.509 services such as digital signatures.

Moreover, issues around remote access and the increasing use of smartphones and tablets for accessing corporate networks and systems will continue to limit the impact of X.509 tokens and drive buyers to consider alternatives. Note that problems with personal identity verification (PIV) cards in these use cases among U.S. federal agencies have been the main drivers for derived PIV credentials (see NIST publication "Guidelines for Derived Personal Identity Verification [PIV] Credentials").

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: Entrust Datacard; Giesecke+Devrient; Google; KOBIL Systems; Microsoft; Yubico

Recommended Reading: "Market Guide for User Authentication"

"Technology Insight for Public-Key Authentication Tokens"

"IAM Leader's Guide to User Authentication"

Privileged Access Management

Analysis By: Felix Gaehtgens; Michael Kelley

Definition: Privileged access management (PAM) tools help organizations provide secure privileged access to critical assets and meet compliance requirements by managing and monitoring privileged account activity. 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 and audit privileged access sessions.

Position and Adoption Speed Justification: Interest in PAM tools continues to grow, with many organizations identifying PAM as a top 10 security control. PAM tools are mature for legacy use cases, but they continue to evolve, along with adoption of better practices from enterprises, with regards to just-in-time privileged access, zero standing privileges, secrets management and cloud use cases. For this reason, the position of PAM tools in this years' Hype Cycle continues to advance, but it will take more than two years to reach the Plateau of Productivity. PAM tools are increasingly used to secure remote privileged access scenarios. Some clients also use PAM tools to secure operational technology and industrial control systems. Securing privileged access to IaaS and PaaS is maturing, and vendors are offering SaaS-based PAM capabilities. Additionally, vendors in the PAM market have developed tools to answer the challenge of managing access and secrets in highly dynamic environments such as DevSecOps and containers, with several secrets management products available today.

User Advice: PAM tools enforce the privileged operations model for your organization:

- Plan for a roadmap that emphasizes a risk-based approach to prioritize the most risky types of accounts, or most critical assets. Plan for just-in-time privileged access and zero standing privileges.
- Get alignment from PAM users on any necessary changes to working practices. Without this, users will attempt to bypass or subvert the tools. Political boundaries and turf mentalities in organizations will prevent comprehensive utilization of PAM practices and erode security.
- Scrutinize offerings from multiple vendors; pricing for tools is converging into bundled offerings but varies in licensing metrics (per user/per asset/per session). Tools from multiple vendors can be integrated in a best-of-breed approach.
- Ensure that administrative accounts for network devices, hypervisors, IaaS, PaaS and SaaS are within scope as well.
- Determine which delivery model works best for your organization: hardware appliance, VM, SaaS or deployed into IaaS environments.
- Account for all privileged access, whether that access is human-based or software-based. For example, do not overlook service and software accounts — they are a considerable source of security and operational risk.
- Failover, disaster recovery planning and emergency access are crucial for success; ensure that your solution is highly available.
- Integrate PAM tools SIEM for logging, IGA for life cycle management, and change management/ ITSM tools for tighter access control. CMDB and ITSM tools can also help drive account discovery.

- Automate privileged tasks as much as possible to eliminate the need for full operating-system-level privileged access by people and to enable automated privileged tasks to be executed by lesser skilled personnel.

Business Impact: Privileged access is high risk and many breaches can be attributed to privileged access misuse, stolen privileged credentials or hijacked privileged accounts. A PAM tool can mitigate the risk arising from the existence of privileged accounts, while the attack surface presented by privileged accounts is reduced by working toward zero standing privileges, the highest form of just in time (JIT) PAM access. PAM tools provide robust and granular control, transparency, scalability, and more accountability for privileged access compared to manual controls and custom or generic tools. Particularly, they offer the following benefits:

- Mitigate risks and achieve visibility of privileged operations and account use.
- Enable privileged access only when it is necessary — according to the principle of least privilege.
- Allow remote privileged access, including to third parties.
- New approaches to PAM include a focus on JIT privileged access, further reducing standing privileged access and getting closer to the principle of least privilege.
- Mitigate risks associated with malware targeting privileged accounts.
- Eliminate hard-coded passwords in application code, scripts and configuration files.
- Enable a forensic review of privileged access activity.
- Provide real-time monitoring, auditing and alerting of privileged activities.
- Manage credentials for DevSecOps toolchain and containers.
- Provide delegation for automated privileged tasks, which help significantly increase IT staff efficiency and reduce operating costs.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ARCON; BeyondTrust; Centrify; CyberArk; Hitachi ID Systems; One Identity; senhasegura; Symantec; Thycotic; WALLIX

Recommended Reading: “Magic Quadrant for Privileged Access Management”

“Critical Capabilities for Privileged Access Management”

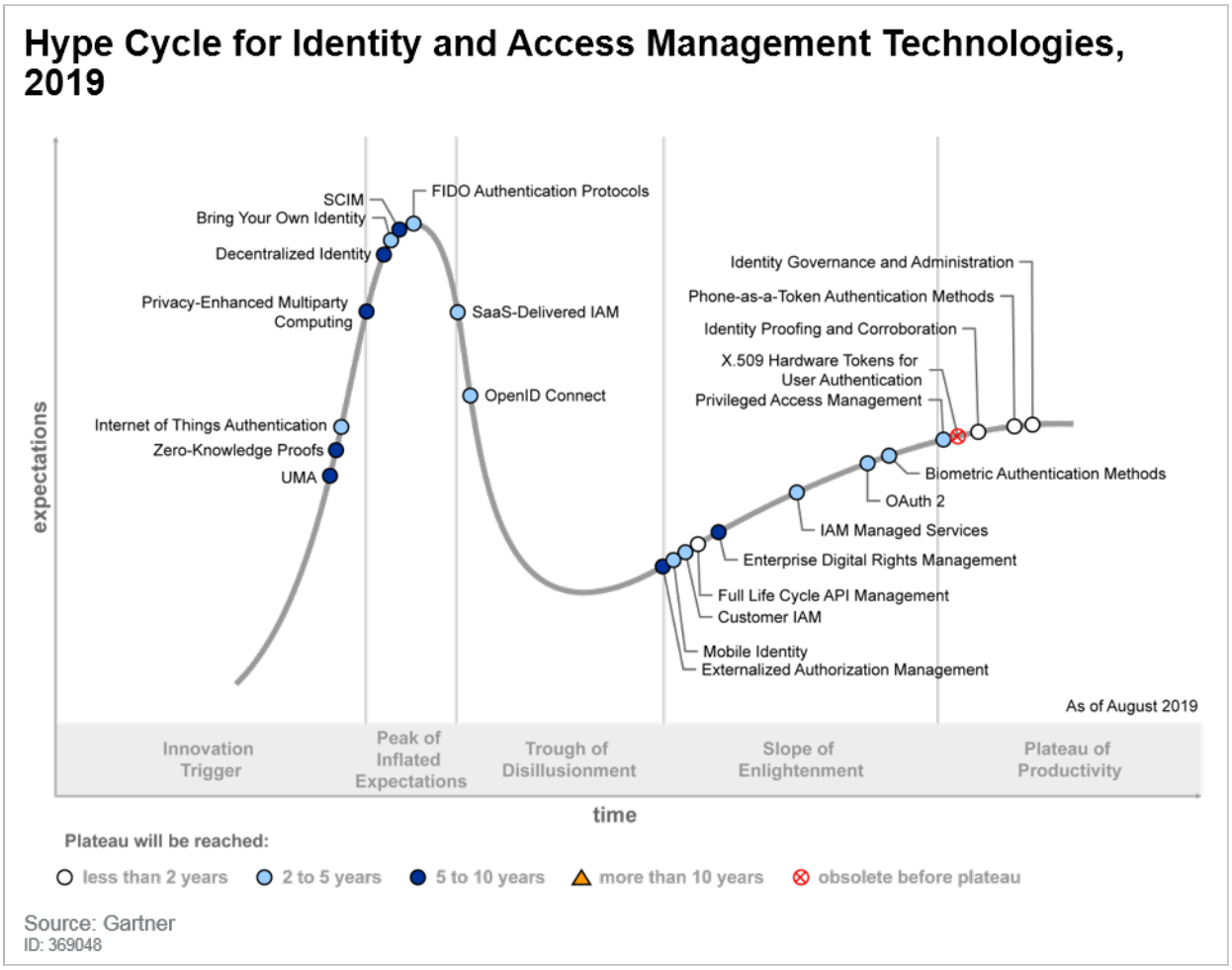
“Best Practices for Privileged Access Management Through the Four Pillars of PAM”

“IAM Leaders’ Guide to Privileged Access Management”

“Remove Standing Privileges Through a Just-in-Time PAM Approach”

Appendixes

Figure 3. Hype Cycle for Identity and Access Management Technologies, 2019



Source: Gartner
ID: 369048

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press 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 technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology 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 technology'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 technology 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 technology to reach the Plateau of Productivity.

Source: Gartner (July 2020)

Table 2. 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 2020)

Table 3. Maturity Levels

Maturity Level	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 2020)

Gartner Recommended Reading

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

Understanding Gartner's Hype Cycles

Magic Quadrant for Identity Governance and Administration

Magic Quadrant for Access Management

Magic Quadrant for Privileged Access Management

Market Guide for User Authentication

Market Guide for Identity Proofing and Corroboration

Technology Insight for Customer Identity and Access Management

Innovation Insight for Bring Your Own Identity

Innovation Insight for Decentralized and Blockchain Identity Services

Identity and Access Management and Fraud Detection Primer for 2020

Evidence

This research was developed using Gartner client interactions and secondary research.

More on This Topic

This is part of two in-depth collections of research. See the collections:

- 2020 Hype Cycle Special Report: Innovation as Strategy
- IAM Leaders' Guide to User Authentication

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp