Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control

Published 23 November 2021 - ID G00757769 - 28 min read

By Analyst(s): Tricia Phillips, Erik Wahlstrom, Henrique Teixeira, Mary Ruddy, Michael Kelley

Initiatives: Identity and Access Management and Fraud Detection

The rapid increase in multicloud environments and distributed users has resulted in massive identity-centered security vulnerabilities. SRM leaders must combine centralized IAM controls, policies, data, and programs with empowered, decentralized and context-sensitive enforcement.

Additional Perspectives

- Summary Translation: Predicts 2022: Identity-First Security Demands Decentralized Enforcement and Centralized Control
  (14 December 2021)

Overview

Key Findings

- Identity-first security has become a core concept of many security initiatives, such as zero-trust architecture, but traditional, siloed identity and access management (IAM) staffing models and tools were not designed for this type of distributed and fast-paced development approach.
- IAM leaders need to modernize their approach to several connected but disparate identity-based use cases and business functions. However, they often find that buying separate solutions for each component can cause inefficiencies, duplication of controls and security gaps that can be exploited by attackers.
- Developer-focused organizations and microservices architectures have taken identity decisions out of the hands of formal IAM teams, who are often viewed as barriers to innovation and business-driven development initiatives.
- Customer- and citizen-facing organizations have found themselves without a scalable, privacy-preserving and high-assurance method of verifying identities and claims. This can result in staggering fraud losses, poor customer and citizen experience and increased scrutiny with regard to identity data collection, management and protection.

Recommendations

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

- Embrace the concepts of centralized control and composable, decentralized enforcement described in the cybersecurity mesh architecture (CSMA) with regard to access controls by ensuring that IAM buying decisions, solution design and implementation follow that approach.
- Enhance IAM performance and reduce risks by implementing a converged IAM platform if and when that would be more effective than separately sourced component solutions.
- Establish an extended virtual IAM fusion team that brings together stakeholders from architecture, development, operations and product alongside the core IAM team. This team will ensure that core IAM standards, policies and technologies are championed and implemented across the organization, and that IAM decisions are more firmly rooted in business and development objectives.

- Optimize customer and citizen UX, privacy, and identity assurance, and reduce fraud losses and overheads by adopting decentralized identity (DCI) and verifiable claims where they can yield improvements.

Strategic Planning Assumptions

By 2025, 70% of new access management, governance, administration and privileged access deployments will be converged identity and access management platforms.

By 2024, organizations adopting a cybersecurity mesh architecture will reduce the number and scope of security incidents and 90% of their financial impact.

By 2025 identity and access management leaders who foster interdisciplinary fusion teams will gain control of 50% more identity and access management decisions than those who do not.

By 2026, 50% of smartphone users will frequently use one or more verifiable claims stored in their decentralized identity wallet.

Analysis

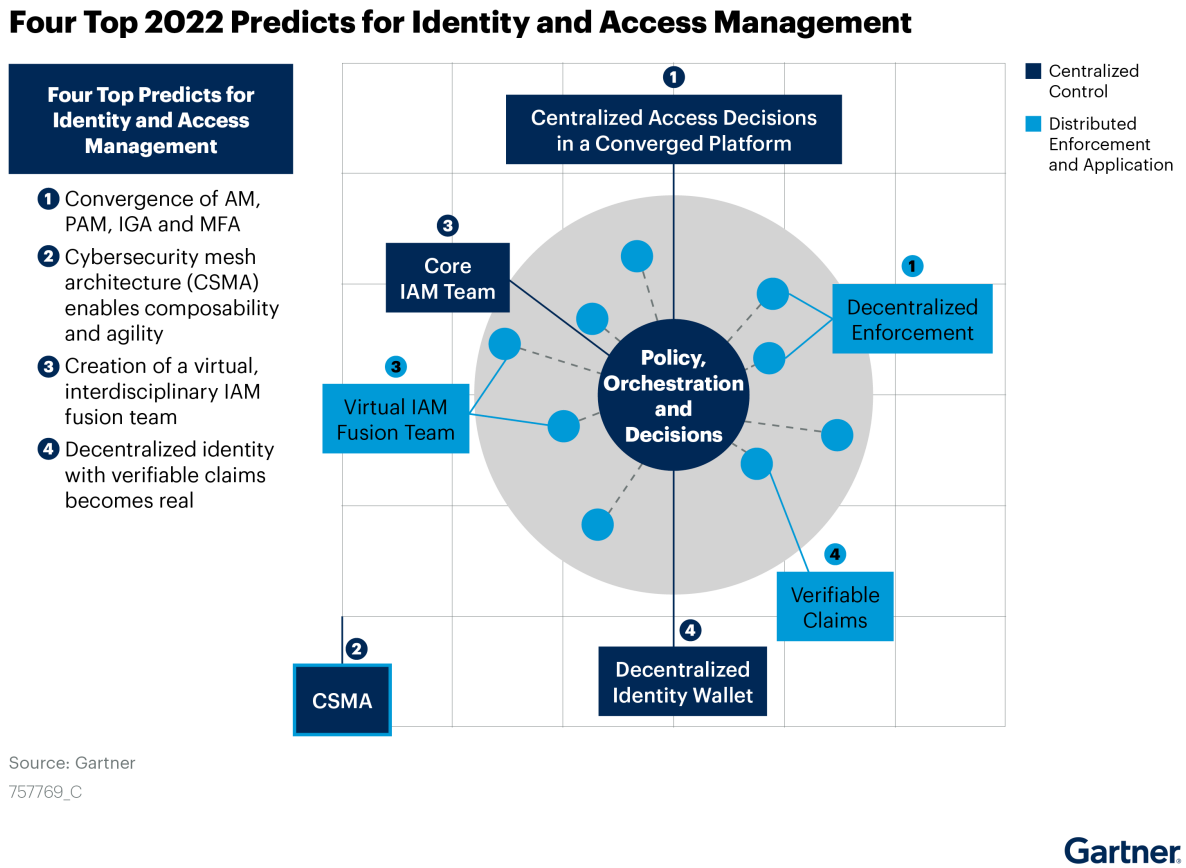
What You Need to Know

The acceleration of digital interactions as the primary method of business and government interactions is here to stay. When we reframe anywhere, anytime digital access and identity assurance as the primary objective, not the exception, and combine it with the emergence of identity-first security as the leading defense against attacks, we see that legacy IAM approaches are insufficient. The broader trend toward technological and organizational composability, which empowers those closest to the action to respond autonomously, supports the need for a fundamental change in the way IAM leaders design and enforce identity-focused solutions and policies.

Gartner sees a trend toward decentralization across IAM disciplines in everything, from the way access management decisions are enforced, to the creation of virtual IAM teams, to the manner in which an individual's identity data is shared and managed. Consolidating policies, analytics and controls in a converged, centralized architecture can prevent this decentralization from descending into fragmentation.

This overarching concept is echoed through each of the predictions highlighted in this report, and is relevant to enterprises of all sizes and industries (see Figure 1).

Figure 1. Four Top Predicts for Identity and Access Management



Strategic Planning Assumptions

By 2025, 70% of new access management, governance, administration and privileged access deployments will be converged identity and access management platforms.

Analysis by: Henrique Teixeira

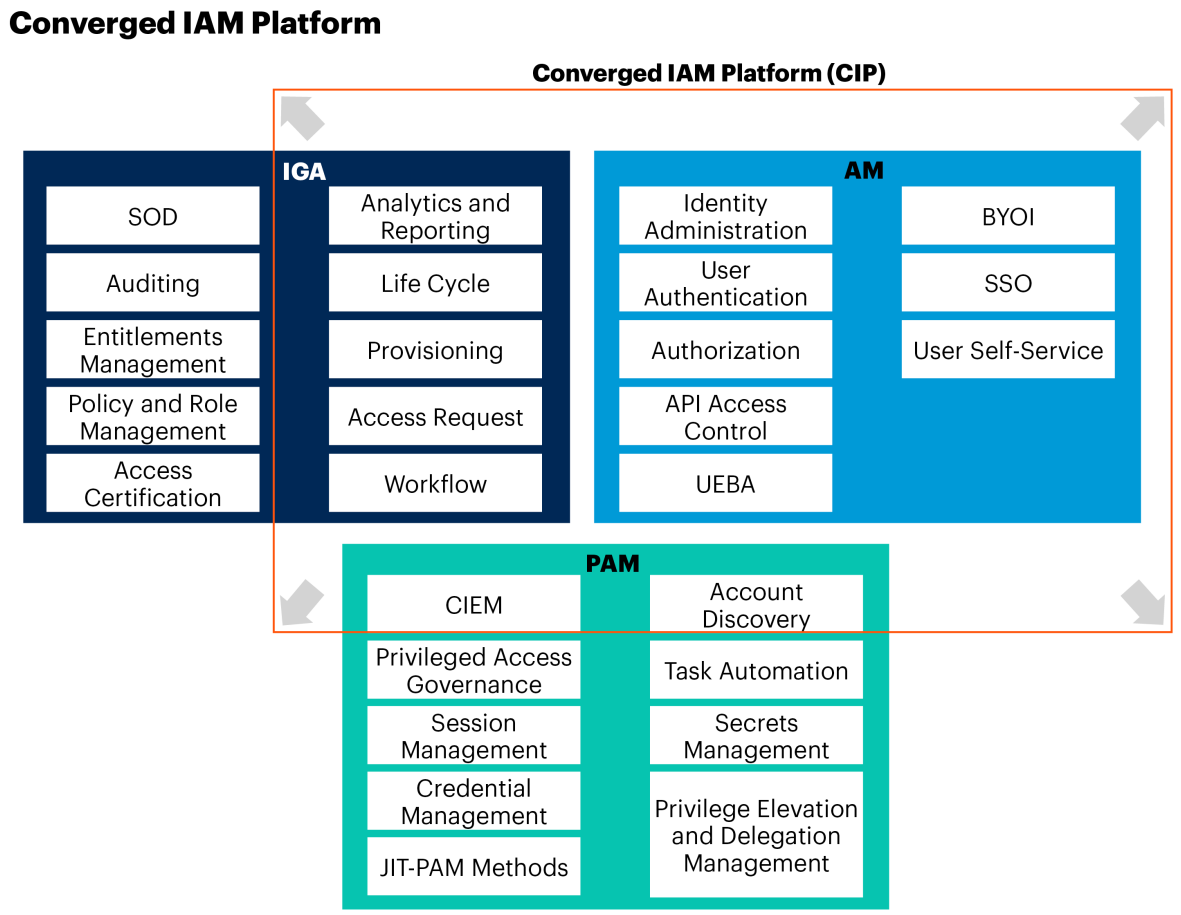
Key findings:

- More than one in four organizations are currently pursuing a cybersecurity vendor consolidation strategy. [1]

- Convergence is happening in three ways in IAM: First, vendor consolidation and innovation through mergers and acquisitions. Second, IAM use-case feature consolidation, with more vendors delivering strong unified capabilities for external, internal and developer users. Lastly, functional convergence is also ramping up, with several vendors already delivering a combination of access management (AM), identity governance and administration (IGA) and privileged access management (PAM) capabilities.

- Convergence is starting with AM (see Figure 2). AM is the most commonly deployed IAM technology among organizations (43% on-premises, 33% SaaS). All prominent AM vendors have already added "light" IGA capabilities in the past year and a half, including at least basic identity administration features. Some have also added cloud infrastructure entitlement management (CIEM) and basic PAM capabilities.

Figure 2. Converged IAM Platform



Source: Gartner
757769_C

Gartner

- Moving forward we will also see more fraud detection and identity-proofing capabilities converging into converged IAM platforms (CIPs) as well.
- IAM convergence is happening in the cloud. The top reason organizations planning to replace AM have wanted to do so is because they want to adopt a SaaS solution. SaaS adoption of AM is growing steadily, and will surpass on-premises deployments by early 2022.
- A SaaS-delivered, CIP is the preferred adoption method for IGA, AM and PAM. IGA is the top candidate for technology replacement for a SaaS-delivered CIP in the preference of surveyed organizations (59% of responses), followed closely by AM and PAM.
- More than half of Gartner surveyed customers believe it is more important for IAM products to fulfill all of their requirements in terms of capabilities than price or delivery model.
- Some organizations, especially those with complex IAM requirements, will still prefer best-of-breed solutions, but that is becoming the exception, not the mainstream rule. Some of these organizations are also choosing specialist IAM tools (like B2B customer identity and access management [CIAM] specialists) to deliver features that are not mature in CIPs.

Market implications:

- The biggest benefit of CIPs is to cast a wider net of identity controls across IAM domains, providing a more efficient, comprehensive risk mitigation strategy than individual IAM modules working alone. A single cloud-delivered CIP offers streamlined identity data and context to be shared among many applications and services in multiple locations. A CIP could provide multiple IAM services that enable parts of an identity fabric in a cybersecurity mesh architecture (CSMA). Converging identity data and other identity threat signals is crucial to preventing the type of sophisticated identity attacks that have been on the rise. These attacks rely on lateral movement, unauthorized privilege escalation and golden ticket attacks, which enable the attacker to generate Kerberos tickets with arbitrary privileges for any account in the active directory (AD).

- The alternative to a CIP is to buy individual IAM modules and build integrations between them. However, these integration projects rely on synchronization agents, connectors and APIs, and often redundant repositories of identity data. They also use different consoles for operation and administration. Services to deploy this type of integration are not trivial, and will require training and support for different types of tools. Lastly, the context about identity threats is harder to obtain this way.
- Midsize enterprises (MSEs) with more basic IAM needs have helped a lot with the popularization of CIPs. Given the maturity of some IAM markets like IGA and AM, and the complexity of deploying and managing some best-of-breed solutions, purchase behavior is changing. Via a simplified way to consume IAM controls via SaaS, CIP enables MSEs to achieve acceptable levels of risk mitigation. It is easier to deliver (and consume) a multifunctional platform as a service than as consolidated server software.
- Cost is still an important factor for market adoption of CIPs, but it is not the main factor. An improved risk posture, through a more comprehensive solution, is the main reason why CIPs are becoming popular. Organizations are demanding a broad spectrum of identity risk mitigation capabilities.
- While CIPs mature and evolve, the IAM market will continue to see the emergence of new categories of specialized IAM modules. These focus on delivering “easy-to-use” identity-first security controls, such as CIEM, to complement potential gaps in defense in depth of the current generation of CIPs.

Recommendations:

- Start an IAM convergence strategy in 2022 by planning to consolidate the management of external and internal identity use cases. Evaluate the possibility of using the same vendor for both use cases.
- If you have successfully implemented a SaaS-delivered AM solution, but have struggled to obtain good results with past PAM and IGA deployments due to complexity, explore that AM vendor’s converged IGA and PAM functionalities to find an adequate fit.
- If your organization is an MSE, or if you haven’t yet started to plan an IAM strategy, consider starting with a CIP.

- If you have more advanced needs for PAM and IGA, keep an eye on market development in the AM space, but invest in best-of-breed tools for now. For example, add IGA and PAM to mitigate the risk of inappropriate access, making sure those adjacent platforms can at least be integrated with AM to enable centralized authentication.
- If possible, start small, with a limited set of capabilities of a CIP, by prioritizing less complex IAM use cases that are aligned with your roadmap. “Grow with the vendor” by adding new capabilities as they become available. Be careful to check frequently (every quarter) that the vendor’s roadmap continues to align with yours.
- Evaluate whether additional enriched features provided by specialized IAM modules (like CIEM, analytics, orchestration, access certification) can close the gaps in the current generation of CIPs.

Related research:

Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?

Innovation Insight for Cloud Infrastructure Entitlement Management

Magic Quadrant for Access Management

The Identity Governance and Administration Landscape Is Changing

Buyer’s Guide for Access Management

Buyers’ Guide for Privileged Access Management

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

By 2024, organizations adopting a cybersecurity mesh architecture will reduce the number and scope of security incidents and 90% of their financial impact.

Analysis by: Mary Ruddy

Key findings:

- Evolving a more secure, resilient, composable and distributed IAM infrastructure is now mission-critical for all organizations to keep up with ever-changing threats and business demands.
- Attackers do not distinguish between tool and technology boundaries, and neither should defenders. Therefore, organizations must compose their security and IAM tools in a more integrated cohesive fashion to increase operational efficiency and effectiveness.
- Many of the most disruptive (expensive) security incidents involve lateral movement that can be constrained by proper use of IAM tools, including PAM, IGA, AM and MFA. These tools use continuous adaptive access to provide identity threat detection and restrict access to users that have been authenticated and authorized to a sufficient level of trust.
- Many breaches are caused by security and identity tools that have been misconfigured, not fully configured or whose configurations are out of date. It is no longer realistic for organizations to rely on manually setting and maintaining all of their access policies. This is especially true for distributed organizations operating in a multicloud environment or engaging in software development. There are too many services that need protection to or from too many endpoints and users, all of which are frequently changing. Organizations must use risk-based identity analytics to increase their levels of IAM tool automation.
- Enterprises are placing a premium on IAM tools that are easy to operate and enable the elimination of unnecessary tool overlap.
- Many IAM deployments are overly fragmented (siloed for the wrong reasons), leading to gaps in effectiveness and increasing the attack surface of the enterprise.
- Zero-trust architecture requires authorizing access to each application, service or digital asset. End users are authenticated with a level of trust appropriate to the access they need, with single sign-on (SSO) brokering that single authenticated identity to each authorized application. Also, as part of continuous adaptive access, there is the possibility of dynamically modifying that level of trust ("continuous adaptive trust"). There is renewed emphasis on enabling SSO and continuous adaptive access for all of an organization's applications across all generations of application technology as part of zero-trust initiatives.
- The cost of a breach that is not quickly detected and remediated can grow exponentially over time.

Market implications:

CSMA is an evolutionary approach that will require the enhancement of security and identity tools, as well as changes in how organizations select and deploy those tools. A CSMA can both reduce the chance of a breach and the "blast radius" of a breach, if one occurs.

CSMA provides several foundational security services, including an identity fabric. The identity fabric layer is a distributed identity framework that supports all of the general IAM functions. IAM tools must evolve to be more composable, enabling deeper integrations, more IAM tool interoperability and consolidated operations management with other security tools in the mesh. This will require more consistent application of existing identity and security standards, as well as the adoption of emerging standards. For example, authorization policy is highly fragmented in many organizations today. IAM deployments would benefit from the standardization of access policy across tools. Emerging standards, such as open policy agent (OPA) and the nascent identity query language (IDQL), are designed to facilitate consolidated policy administration while enabling distributed policy enforcement as part of an identity fabric.

IAM vendor product managers may architect their identity tools to operate stand-alone, but they also must enable their offerings to be more composable. This in turn enables the tools to interoperate as part of an identity fabric that forms the backbone of CSMA. For example, an API gateway vendor enabling their API gateway to work with third-party AM tools to be able to leverage existing identities and their entitlements instead of requiring organizations to establish new islands of identities in the API gateways. Gartner has observed security and identity vendors adding integrations to more IAM tools for some time now. Vendors must do more, and combating the growth of IAM operational complexity should be higher on their priority lists. Enterprises are placing a premium on IAM tools that are easy to operate and enable the elimination of unnecessary tool overlap.

The emergence of CSMA is closely related to the trend for IAM convergence (see above prediction). Likewise, IAM capabilities deployed to protect new APIs may need to interoperate with an SSO solution that provides workforce access to legacy web apps. This provides employees with a unified access experience, regardless of the technology used to build the applications they use.

CSMA enables secure centralized operation and oversight in a world of decentralized IT. CSMA provides a multipronged approach to reduce the financial impact of security incidents, which includes the following elements:

- Reducing the chance of unauthorized access, especially by compromised credentials.
- Reducing the attack surface. The potential damage from any compromised credential is minimized by deploying advanced analytics to create and maintain least privilege configurations.
- Reducing the duration that an attacker has access by using machine learning analytics to continuously look for anomalies in access and access policies.

These factors combine to provide a multiplicative effect.

Recommendations:

- Choose IAM tools that are able to deeply interoperate as part of a CSMA deployment. That is, give priority to tools that promote composability within the identity fabric. For example, demand that your SaaS vendor support OpenID Connect and SCIM; insist that your IAM vendors support identity federation with MFA or support pluggable MFA directly through established industry standards (RADIUS, LDAP, proxy with header injection, pluggable auth. module on Linux, WebAuthn, etc.).
- Rearrange your organization's IAM roadmap to align with CSMA best practices.
- Raise the priority of moving to a zero-trust architecture by defining a journey to zero-trust for your organization that details:
    - Identity interoperability criteria when licensing new software to stop adding to technical debt.
    - IAM best practices when developing new software.
    - Priorities for enabling authorization when accessing existing applications (remediate existing technical debt).
- Deploy more intelligent, continuous adaptive access.
- Protect the keys to your IAM kingdom by revisiting how you secure your foundational IAM components, such as secrets managers or Active Directory. Such components should not be operating in isolation, but should be protected as part of a broader CSMA.

Related research:

2022 Planning Guide for Identity and Access Management

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

By 2025 identity and access management leaders who foster interdisciplinary fusion teams will gain control of 50% more identity and access management decisions than those who do not.

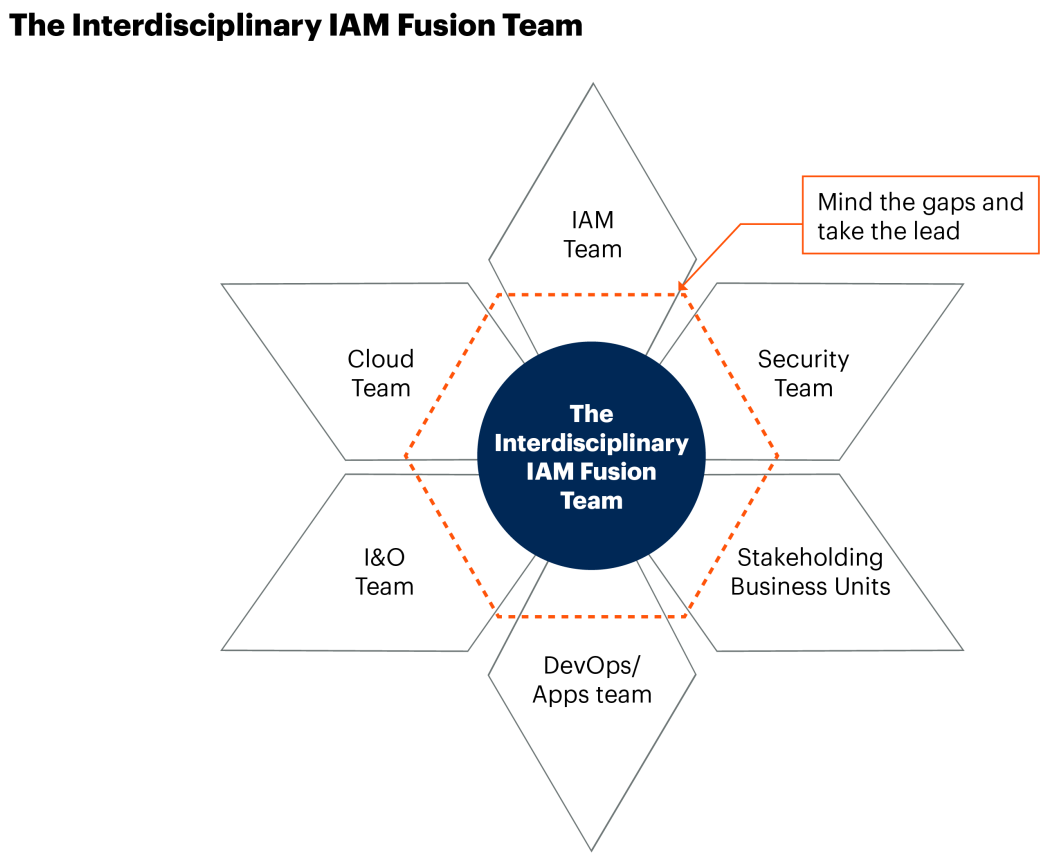
Analysis by: Erik Wahlstrom

Key findings:

- Clients report in conversations with Gartner that their IAM teams lack influence over IAM decisions, and that other business units within the organization have many, often conflicting, objectives not met by the team. There is a gap between the IAM team and business initiatives that needs to be bridged to ensure that the organization's security, usability, privacy and scale requirements can be met.
- Organizational buy-in and stakeholder inclusion have always been vital for a successful IAM program. That said, IAM team success has historically been defined as meeting compliance requirements, more than establishing an IAM program that provides an efficient and scalable foundation that meets real business enablement needs.
- Hybrid and multicloud environments, a lack of traditional perimeter protection mechanisms, zero-trust strategies, the management of new human and machine constituencies and the need for highly technical and detailed guidance require interdisciplinary skills. There is an accelerated increase in the number of use cases and processes that must be met, and finding IAM people with all of the necessary skills is extremely difficult. Organizations are reaching a turning point when a single IAM team's skill, insights and influence cannot span enough tools, processes and use cases.
- The many tools that compose the organization's evolving identity fabric, part of the CSMA as defined above, are owned, maintained and used by not one, but many different business units. Identity use cases must now span multiple tools, and must therefore also involve the active engagement of individuals outside the formal IAM team.

- Organizations must find a way to make sure the right influence and guidance are available where and when IAM decisions are made. It is no longer enough to have a centralized reactive governance team. A more proactive, matrixed and decentralized team must be formed.
- IAM teams must find ways to evolve into an interdisciplinary IAM fusion team, as depicted in Figure 3. This is a community of practice that bridges gaps, establishes ownership of use cases that cross traditional tooling siloes and establishes ownership of the evolving identity fabric. While doing so, provide tailored guidance in the form of play books, working together with the business units that make IAM decisions outside of the IAM team's control. Guidance can then be enforced by IAM fusion team participants who are also members of the business units making the decisions.

Figure 3. The Interdisciplinary IAM Fusion Team



Source: Gartner
757769_C

Gartner

Market implications:

The establishment of a matrixed IAM fusion team enables an organization to better balance security, privacy, usability and scale and make better-informed identity decisions.

- The team can support growth and improve scalability by having more feet firmly on the ground in the different teams and business units. Only representatives of teams that are closely attached and have a deep understanding of the projects at hand can enforce guidance at the right place and the right time.
- Short deadlines and, from an IAM perspective, the uncontrolled, raw speed of the digital transformation within an organization are often sources of unsecure systems and redundant investments and efforts. The team can improve security by ensuring that the right guiding principles and tooling support are proactively established to solve each team's evolving requirements.
- An identity fabric, as defined above, will eventually enable any human or machine to safely and conveniently access any application or service from any device anywhere. Today, an organization's identity tools consists of a loosely connected IAM infrastructure with islands of tools that solve individual IAM use cases. Deeper integrations between the tools are now required to start forming the fabric. The IAM fusion team can meet the organizational demands for usability and privacy by breaking down silos and enforcing deeper integration and usage of existing tooling in the identity fabric as it is formed.

Recommendations:

- Converge teams that make IAM decisions. See early results and start taking back control over IAM decisions by establishing an interdisciplinary IAM fusion team, a community of practice that defines guidance and both owns and operates the evolving identity fabric.
- Let an IAM leader lead the IAM fusion team. Other team participants should come from teams that often make identity decisions. For example, application and DevOps teams, security teams, infrastructure and operations (I&O) teams, cloud teams and other business units.
- Forge closer bonds with security, cloud, I&O, developers and DevOps teams. Expand the team as use cases require it in order to include more boots on the ground in different business units that make identity decisions.

- Provide guidance within the team so that they become a scalable foundation for better-informed IAM decisions across the organization. Define guidance and policies, and establish ownership of tools and their integrations.
- Set expectations. Developing guidance takes time. Don't expect the team to have all the answers at once. Continually work to provide guidance and calibration on the most business-critical use cases. Pay extra attention to greenfield deployments, where the right guidance will prevent bad implementations and thereby stop the bleeding.
- Take a use case, rather than a tooling, approach to identity. The use cases define the identity requirements, the tooling needed and therefore the composition of the team involved in the decisions.

Related research:

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

2022 Planning Guide for Identity and Access Management

A Successful IAM Program Begins With a Vision

Guide to Initiating and Running an Effective IAM Program

By 2026, 50% of smartphone users will frequently use one or more verifiable claims stored in their decentralized identity wallet.

Analysis by: Michael Kelley

Key findings:

- A number of governments or governmental authorities are both investigating and experimenting with decentralized identity (DCI) approaches. Among others, Germany has a number of DCI POCs underway, and the government of Ontario, Canada has announced a plan to use DCI to facilitate citizens' digital interactions with the Canadian government. [2] Employment and Social Development Canada (ESDC) has adopted Verified.Me to provide Canadian citizens the ability to verify their identity when signing up for government services. [3] Finally, the European Union has defined how DCI will work within member states, enabling DCI vendors to build to their use case. [4]

- While we do not expect COVID-19 vaccination passports to be universal, this is another important use case which has gained traction in parts of the world. Companies including Civic, OnFido and 1Kosmos have worked with governments and standards organizations to promote the adoption of DCI for health status credentials in the form of verifiable claims. IBM is offering the IBM Digital Health Pass, a DCI approach to health credentials, to a number of major airlines. [5] The COVID-19 Credentials Initiative (CCI) is another example of organizations working to use DCI to represent health status as a verifiable claim (VC). [6]

- We see continued investment in DCI approaches by IAM vendors, including access management (AM) vendors like Microsoft and Ping Identity, and DCI infrastructure providers like IBM and Sovrin. Many vendors are working to find use cases that bring early benefits like identity proofing, authentication, and potentially fraud prevention, as they build out infrastructure and tools for the use of verifiable claims on a wider scale.

- Banking and finance continue to offer viable use cases for high-assurance customer identity corroboration and interactions, potentially lowering the incidents and magnitude of fraud. Verified.Me works with account holders at regional banks in Canada to use high-assurance identity information from the banks to provide higher-assurance interactions for service providers who can accept Verified.Me credentials.

- Online retailers will begin offering the ability to use VCs to conduct online transactions as an alternative to creating unique, site-specific accounts, or to using less secure, less private social media accounts. In at least one case, DCI is being used for physical access for shopping at unmanned convenience stores. [7]

- Standards for DCI continue to be a concern. Each DCI vendor is typically building out their own trust framework and DLT (distributed ledger technology) architecture, leaving the ability to interact with other DCI vendors a risk. Standards for components like wallets are moving slowly, with over 40 wallet standards currently in the mix. DIF, W3C, TrustoverIP and other organizations are working quickly on definitions and adoption of standards, but a lack of interoperability may continue to delay widespread adoption.

- Several billion citizens worldwide do not have access to a verifiable electronic identity, which is needed to provide access to credit or banking services. This population is known as “unbanked” or “underbanked.” These citizens are found all over the world, mainly in developing regions of the world, but also in developed countries. Companies like BankQu, Tykn, Kiva, Bloom ID and others are attempting to help solve this global problem by helping these communities to establish identities through DCI approaches and allowing a VC to serve as proof of their identity.

Market implications:

The promise of DCI is to tackle the issues of privacy, assurance and pseudonymity in a different way, offering benefits to stakeholders across the digital identity value chain and disrupting traditional, centralized approaches to managing identity data.

In terms of privacy, DCI uses decentralized computing, which ultimately uses verifiable claims built on the concept of zero-knowledge proofs and claims (see Hype Cycle for Blockchain, 2021). These enable individuals to verify claims (i.e., requests for information) with the principle of least privilege applied to information. The requestor, typically a service provider, receives only the absolute minimum required amount of information (for example, only a “yes/no”) to satisfy the request for information.

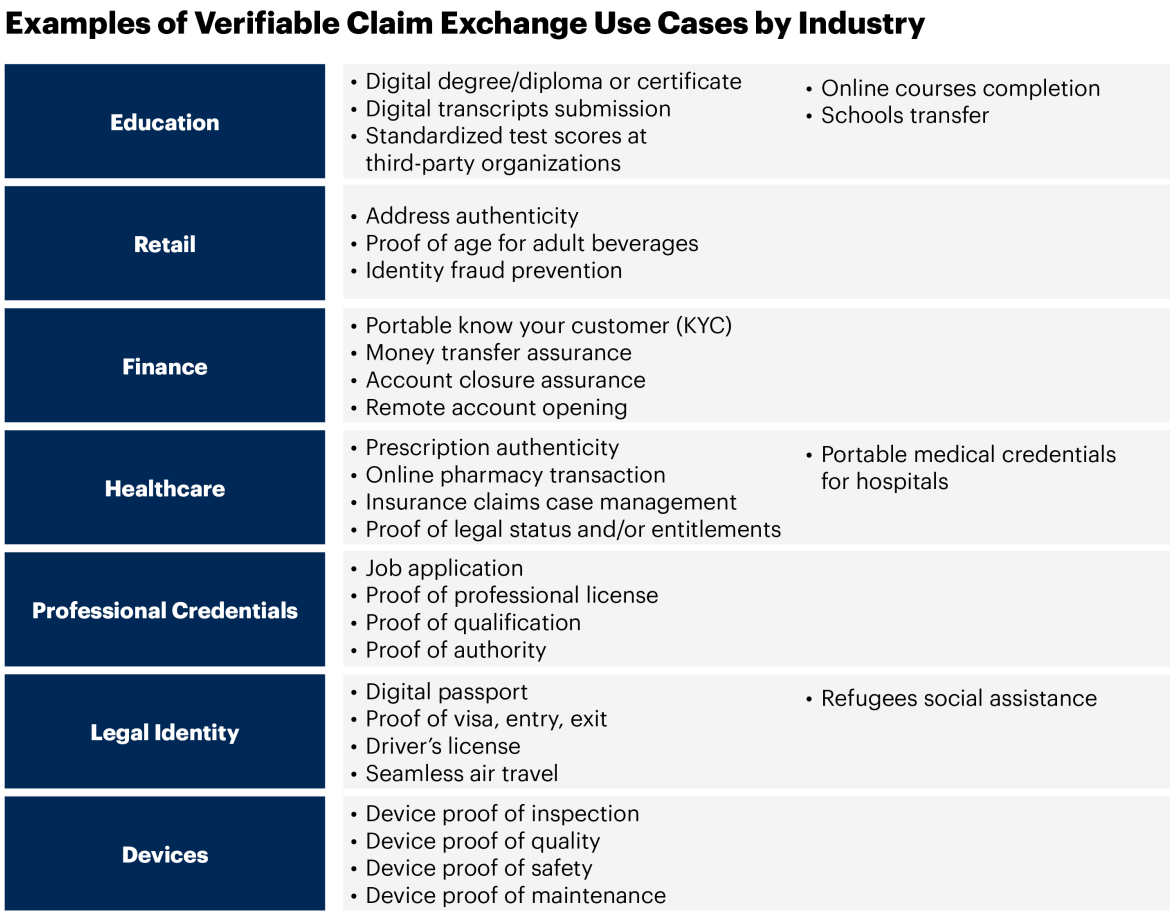
“Assurance” refers to determining that a person is the genuine owner of the real-world identity that they are claiming. Identity proofing has already happened in the process of establishing that identity within the DCI network, which may have involved validating and verifying credentials from a variety of issuers. Organizations that typically need to conduct identity proofing can theoretically “outsource” that task to the DCI network. This means that identity proofing for employees, customers or contingent workers (who are identity-invisible) can be established to an acceptable level of certainty.

“Pseudonymity” means that there is an electronic representation of a person, but organizations that have a relationship with the person have no way of tracking it back to a real-world identity, nor would they need to.

The benefits of the decentralized identity approach as outlined above offer control and efficiencies not yet seen in the market for digital identity. It may be years before the full benefits of DCI are realized. However, governments and service providers, such as banks or employers, in addition to customers, are already beginning to experiment with DCI as a means to address the limitations inherent to centralized approaches to digital identity management.

Various types of information can take the form of a verifiable claim (see Figure 4).

Figure 4. Examples of Verifiable Claim Exchange Use Cases by Industry



Recommendations:

- Service providers, such as online retailers, should expand bring-your-own-identity approaches to include DCI, using DCI to establish identity and trust, dramatically cutting the time needed to establish an account through the use of a VC.
- Governments should explore options to apply DCI for citizen identification and services. This includes the ability to issue VCs to and for citizens and residents. In addition, governments can define how DCI will work within their country, defining standards for wallets, claims, interoperability with other trust fabrics, etc.

- Corporations should expand the use of VCs to extend the reach of identity-proofing capabilities in both internal and external access use cases by adding emerging DCI features from their IAM providers to their onboarding workflows. Allowing new applicants to use VCs to represent themselves to the organization can reduce the effort, costs and risk involved in the identity-proofing process, while increasing the potential pool of applicants as DCI gains traction.
- Choose a business case based on your goals and requirements to justify investment in DCI and VCs. Some examples include:
  - Opportunity cost — The benefits of DCI, privacy, security, high assurance, etc. may enable a reduction in spending on existing elements which are focused on securing these benefits in other ways.
  - Efficiency — The ability to do things in a better, more efficient and timesaving way. For example, using DCI may reduce onboarding time for consumers for e-commerce sites, allowing companies to reduce abandonment rates and improve the customer experience.
  - Uniformity — For example, in government use cases, the ability to provide all citizens with equal standing and equal access to government services through high-assurance and reliable identities. Alternatively, using a master ID that can facilitate participation in government services, but which could also provide the ability to check into a hotel, buy a concert ticket, share personal health information, etc.
  - Solving significant social challenges like the unbanked/underbanked problem.

Related research:

Innovation Insight for Decentralized Identity and Verifiable Claims

Guidance for Decentralized Identity and Verifiable Claims

Market Guide for Identity Proofing and Affirmation

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Government Insight: Citizen Digital Identity Trends Provide Growth Opportunities

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

Predictions are one part art, one part science, and thus, some are on track, and some end up being way off base. This year, we find ourselves without any meaningful predictions with a due date of 2021. Perhaps we somehow anticipated that it would be a year of recovery and planning (or more likely, it was just an oddity of the timelines previously selected). We will have predictions for IAM and fraud prevention that will reach maturity in 2022, so next year we will provide analysis of those that hit the mark, and those that were way off target.

Evidence

[1] Top Security and Risk Management Trends 2021

[2] Ontario's Digital ID: Technology and Standards, Ontario.ca.

[3] Employment and Social Development Canada (ESDC) Adopts Verified.Me, Streamlining the Digital Identity Verification Process of Canadians Registering With My Service Canada, Verified.Me.

[4] High-Level Scope (ESSIF), European Commission.

[5] More Than 450 Airlines Can Now Use IBM's Blockchain-Based Vaccine Passport, Quartz.

[6] Immunity Credentials Using Self-Sovereign Identity for Combating COVID-19 Pandemic, U.S. National Library of Medicine.

[7] Coinplug, HP Retail Launch Blockchain Decentralized Identity App to Access Unmanned Stores in Korea, Ledger Insights.

Gartner's 2020 Security and IAM Solution Adoption Trend Survey

This study was conducted to learn what security solutions organizations are benefiting from, and what factors affect their choices and preferences when procuring such solutions. The research was conducted online from March through April 2020 among 405 respondents from North America, Western Europe and Asia/Pacific. Companies from different industries were screened for annual revenue of less than $500 million. Respondents were required to be at the manager level or above (excluding C-suite), and to have a primary involvement and responsibility for risk management within their organizations. The study was developed collaboratively by Gartner analysts and the primary research team.

Gartner asked respondents: “What IAM technologies does your organization have today or plan to have in the future?” Out of 400 respondents (excluding those who answered “don’t know”), 43% chose “AM — deployed on-premises.” “AM — SaaS” accounted for 33% of the answers out of 392 respondents (excluding those who answered “don’t know”).

Gartner asked respondents: “If your organization is planning to replace [x] technology, please indicate the closest description of its reason for doing so.” Of the 233 respondents to select AM, 30% of them answered: “Replacing the incumbent solution with a SaaS-delivered solution.”

Gartner asked respondents: “If your organization is planning to replace [x] technology, please indicate the closest description of its reason for doing so.” The total of respondents selecting SaaS-delivered and converged IAM platforms for IGA was 59%, for AM — 55%, and for PAM — 50%.

Gartner asked respondents: “If you were to choose a new IAM product, what would be more important to you?” Of the 405 respondents, 52% answered: “Completeness: Full feature set, the IAM product(s) must be able to fulfill all our requirements.” The second most popular answer (27%) was “Price: A cheaper broader (bundled) product that offers multiple IAM functions, although it may not fulfill all of your requirements.”

Recommended by the Authors

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

2022 Planning Guide for Identity and Access Management

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

Innovation Insight for Decentralized Identity and Verifiable Claims

Guidance for Decentralized Identity and Verifiable Claims

Market Guide for Identity Proofing and Affirmation

Three Critical Use Cases for Privacy-Enhancing Computation Techniques

Magic Quadrant for Access Management

Innovation Insight for Cloud Infrastructure Entitlement Management

A Successful IAM Program Begins With a Vision

Guide to Initiating and Running an Effective IAM Program
