The Future Of Identity And Access Management

Vision: The Identity And Access Management Playbook

by Andras Cser and Merritt Maxim

June 26, 2019

Why Read This Report

Identity and access management (IAM) capabilities are critical in the fight to protect customers from account takeover, identity theft, and privacy abuses. Business leaders, CIOs, and CISOs use IAM technologies to both engage with customers and protect them throughout their journey. These same technologies are also vital to protecting employee experience, driving both operational efficiencies and productivity. In this report, we help security pros understand how to use IAM to enable digital transformation initiatives and new business models in the next two years.

This is an update of a previously published report; Forrester reviews and updates it periodically for continued relevance and accuracy.

Key Takeaways

IAM Is An Essential Component Of Customer Security And Privacy

All business processes and applications are imbued with identities, and managing these identities is essential when it comes to protecting data. Customer-obsessed security pros need a solid grasp of IAM capabilities and must treat them as a top priority.

IAM Is Core To Driving Optimal Employee Experience

Today's tight labor market requires engaged employees, and improving employee experience (EX) is a key to driving retention. Given that many IAM technologies, especially those related to identity management, can have a direct impact on user productivity and engagement, security pros need to assess how IAM can help further existing EX initiatives.

IAM Becomes Microservices- And API-Based

Tired of clunky, monolithic IAM solutions? Then you'll be happy to learn that vendors are breaking existing platforms into microservices- and API-based offerings that can simplify integration. This lets organizations flexibly adapt to evolving business requirements, on a smaller footprint, and with faster time-to-value.

The Future Of Identity And Access Management

Vision: The Identity And Access Management Playbook

by Andras Cser and Merritt Maxim
with Stephanie Balaouras, Salvatore Schiano, Benjamin Corey, and Peggy Dostie

June 26, 2019

Table Of Contents

Related Research Documents

Forrester's Identity And Access Management Maturity Assessment

Forrester's Risk-Centric Identity And Access Management Process Framework

The Forrester Wave™: Identity Management And Governance, Q3 2018

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

You Need IAM In Your Technology Portfolio

Great customer experiences lead to higher revenue growth for your company.[1] To provide great experiences, you must invest in the technology, systems, and processes that help win, serve, and retain customers.[2] IAM is one such technology. Although it began as a collection of purely security-focused technologies, it has evolved into an essential tool for helping a firm understand and engage with customers along every step of their journey. You need IAM technologies in order to:

- **Manage customer identities, preferences, and profiles across channels and devices.** When purchasing your products and services, and through other forms of engagement, customers demand consistent, personalized, and relevant experiences across all channels. This is only possible if you can accurately verify, enroll, and identify the customer, remember their prior interactions and customer preferences, and understand their behavior in context. Remembering the customer's actions, preferences, and profile is only feasible if you centrally manage all customer identities; for example, the website of a magazine with both a print and an electronic presence needs to maintain a single record of a subscriber's delivery address, subscription expiration date, payment method, content customization, and email list preferences for all of the customer's subscriptions.[3]
- **Maintain customer privacy preferences across locations, hosting models, partners.** Customers are becoming more sensitive to and affected by how firms collect, store, and use their personally identifiable information (PII).[4] Regulations such as the EU's General Data Protection Regulation (GDPR) and Payment Services Directive (PSD2) also create greater regulatory and customer scrutiny of IAM vendor solutions that store and have to protect PII and firms that collect and use it.[5] You must manage users' identities in such a way that it also allows them to log in and manage their privacy preferences. Even more challenging, you must ensure that wherever you store, copy, or transmit that data, you: 1) protect it in transit, at rest, and in use and 2) enforce customers' privacy preferences without diminishing the potential value that businesses can extract from it or unnecessarily adding costs.
- **Provide adaptive, secure access to sensitive data for employees and partners.** Because your company's processes and products are increasingly digital, you're generating more and more data. Moreover, few companies work in isolation: You may have hundreds of third-party relationships, from suppliers, to contractors, to outsourcers, and it's your role to ensure that: 1) this data is accessible to the right, authorized owner and protected from unauthorized users and access regardless of location or hosting model and 2) authorization takes context into account.[6] IAM must tie employees, business partners, and even customers to data: An automotive manufacturer must ensure that its suppliers gain access only to the intellectual property (IP) of parts they need to deliver to the manufacturer — but no other data.[7] In addition, the rise of machine identities such as bots that may interact with customers and sensitive data also requires extending existing identity controls to cover these machine identity use cases.[8]

- **Support seamless mobile customer experiences that engender trust.** Unlike with your own employees, you don't have the power to manage a customer's device and its contents. To support customers' mobile moments, you must build IAM into the mobile experience in such a way that it doesn't detract from their experience yet instills confidence that you're protecting them from cybercriminals and potential privacy abuses. You can engender your customers' trust in their mobile moments by how you: 1) verify and enroll users; 2) register your firm's mobile application or a third-party IoT device to use your services; 3) authenticate users for routine and high-value transactions securely; and 4) recover their password or user ID. Agile mobile application developers must repeatedly provide scalable IAM features to millions of customers — at low cost.[9]
- **Support a broad ecosystem of Zero Trust processes and technologies.** Forrester's Zero Trust model of information security and its eXtended framework (ZTX) is quickly becoming a de facto standard and design principle in every domain of security, including but not limited to network security, cloud security, data protection, and application security.[10] IAM plays an outsized role in ZTX. Providing users and devices with the least privilege necessary to perform their actions is a foundational tenet of the framework. To allow firms to transition easily to the new, identity-based perimeter of ZTX, IAM solutions must prevent overprivileging users but also pre-integrate with the main domains and components of the ZTX framework.
- **Leverage existing identity data to enhance customer relationships.** IAM solutions provide rich context and identify patterns on how users interact with your mobile application, website, call center, and corporate applications. Security professionals typically use this data to defend against cyberthreats and investigate security incidents, but now marketing and line of business (LOB) owners are asking security teams to provide trend analysis on how customers browse the site and where they struggle with registration, authentication, and self-services like password reset. Security pros, in collaboration with LOB owners, can then use this data to redesign the site and provide more-targeted offers to users or speed up the customer registration process. A thorough understanding of customers' behaviors helps with fast-tracking identity verification and enrollment of known honest and/or whitelisted customers.

IAM Must Support New Digital Business Models And Requirements

As customer-obsessed firms use digital technologies to create new sources of value for customers and to increase operational agility, vital business processes will traverse different user populations, hosting models, and access channels and devices (see Figure 1).[11] Your IAM strategy and architecture must provide the right level of controlled access from any device to any internal or external application and data resource, regardless of hosting model, for your employees and contractors (workforce IAM scenarios), business partners (partner IAM scenarios), customers (consumer and additional partner IAM scenarios), and devices (connected IAM scenarios) (see Figure 2). Connected devices and machine identities such as bots further complicate these requirements because of their huge number and types

and amount of data, all of which security teams must manage and govern. This will have an enormous impact on the interface design of IAM systems and the architecture of modern solutions that integrate with IAM systems. In the future:

- **Passwordless authentication will become the norm.** With the adoption of Trusona and Windows 10 Hello, and the proliferation of smartphone-based, connected tokens, security teams can finally start their migration away from password-only authentication. Alternatives include push notifications sent to mobile devices, biometrics (finger, face, and voice), FIDO WebAuthN, behavioral biometrics, risk-based authentication, as well as multimodal biometrics. Passwordless authentication will direct firms' attention to the initial onboarding and device registration processes that they need to enhance.
- **Behavioral biometrics will perform IDV and continuous user authentication.** Cybercriminals don't have to harvest passwords from privileged systems from endpoints; they can hack directly into a password vault or an Active Directory domain.[12] Making a one-time authentication decision based on passwords alone is no longer sufficient. You must add multifactor and behavioral and device profiling to your arsenal.[13] Use behavioral biometrics to assess user behavior for identity verification (IDV) as customers fill out forms at enrollment. Expand authentication and authorization of activity from a one-time decision at the beginning of the session into an ongoing process of establishing and monitoring user activity profiles.[14]
- **IAM will increasingly provide context to data and networks in a Zero Trust framework.** IAM systems are a pillar of Forrester's Zero Trust Model of information security and provide the enforcement framework for secure access to applications and data. In the future, IAM solutions will provide more integrated ways to embed identity data into data protection and network forensics systems. For data protection and network security, it will be important to understand whose data assets and network packets are moving across the corporate network.[15]
- **Multitarget and multimodal IAM services will support cloud and on-prem workloads.** Although cloud adoption is on the rise, legacy, on-premises user directories, applications, and processes won't go away overnight ("the definition of legacy is that it works"). Develop hybrid IAM architectures that have a track record of supporting IAM needs of on-premises, legacy applications such as HRIS and ERP with a broad set of connectors and single sign-on (SSO) integration. Since you may be reluctant to store user information and PII in the cloud, your IAM vendor must support hybrid application environments, which includes integrating with on-premises and SaaS apps, and also support deployments in multiple configurations, including an on-premises offering, a cloud IDaaS, or as a managed service (see Figure 3).[16]
- **Self-sovereign, decentralized Identity will penetrate government and healthcare.** Decentralized digital identity (DDID), also known as self-sovereign identity, is an ID verification and authentication framework that usually consists of: 1) a technology backbone (uPort, Sovrin, etc.); 2) a vertical network provider (e.g., CULedger); 3) issuers (colleges, governments, etc.) that issue credentials to users; 4) verifiers (banks, healthcare providers, etc.) that verify claims; and 5) users

who store their digitally signed claims in their digital wallets. DDID will allow for an exponential boost to trust networks and use cases, such as IDV and authentication, as well as user profile management.[17]

FIGURE 1 IAM Must Serve Managed Application Hosting Models, User Populations, And Endpoint Variety

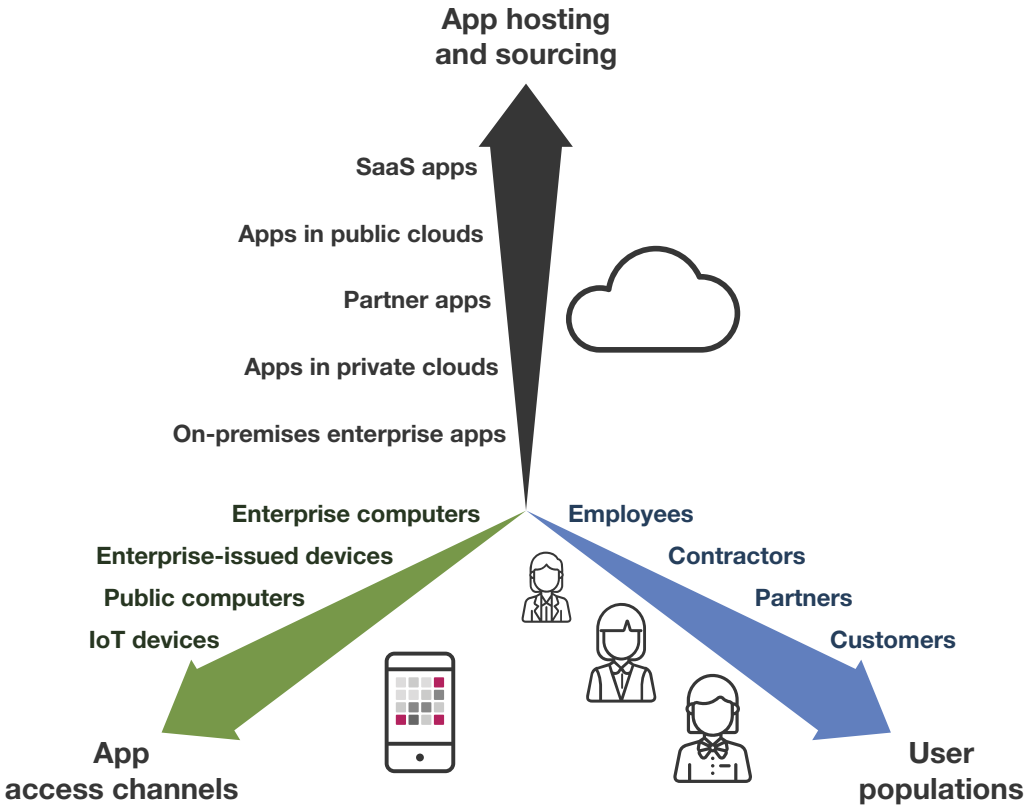

FIGURE 2 Microservices- And API-Based IAM Reference Architecture

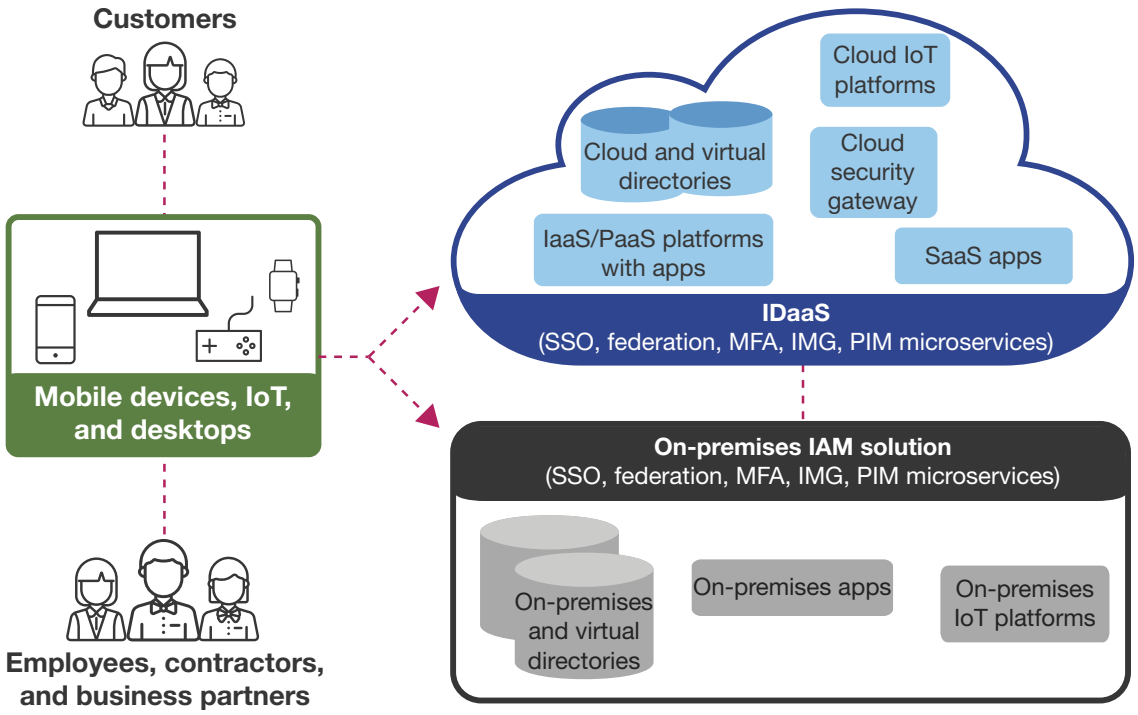

FIGURE 3 Characteristics Of The Multimodal IAM Service Delivery Framework

Supported target applications	Hosting model: on-premises IAM	Hosting model: cloud-based (IDaaS) IAM
On-premises managed applications	Legacy but still important for large organizations. Supports complex workflows. Essential when you can't move identity data to the cloud.	Emerging trend: ability to support on-premises applications with authentication, provisioning, and access governance
Cloud-based managed applications (running on IaaS/PaaS or SaaS)	Difficult area, as most on-premises IAM vendors neglected delivering services to cloud apps	The DNA of IDaaS services but often with very limited functionality in provisioning and governance

Workforce IAM: Support Employee, Contractor Access With Context-Based Identity Views

To achieve digital operational excellence, you must ensure that your extended workforce can easily and seamlessly access authorized on-premises and cloud apps. These apps can be employee- or customer-facing; for instance, a help desk worker must be able to mimic a banking customer in an external-facing online banking application. To achieve better security and improve the operational efficiency and cost of compliance, S&R pros must develop IAM architectures and select vendor solutions that:

- **Encapsulate data and its protection with data identity.** If you want to avoid data loss, you must track data identity. Data identity is metadata about that data itself — such as who created the data, who has access to it, and who can delete it — embedded into the data asset. It's a crucial component of a secure, Zero Trust environment. Data identity can also carry information about data usage patterns. This means that hackers can still leverage metadata, even if it's encrypted, to understand specific user activity. Managing data identity and tying it to employee access rights in the IAM system helps prevent data loss and reduces the threat surface of the firm. This means assigning data access privileges to employees throughout their identity life cycle and including data assets (unstructured and structured) into every quarterly or annual access certification campaign.
- **Leverage machine learning to intercept anomalous access requests and patterns.** In an identity management and governance (IMG) solution that draws static user information from a user directory, you can know and enforce what a user has access to.[18] However, this information is fairly static and doesn't identify threats when a user suddenly requests access to 10 times as many apps as they have in the past or accesses orders of magnitude more records in a CRM system than other users in their peer group. IMG tools offer identity analytics that provides the behavioral insight to reviewers on how a user requested, obtained, and used entitlements. IMG platforms also tie into threat and identity breach (e.g., stolen user name/password) databases to increase accuracy of their ID analytics.[19]
- **Feed cyberthreat and identity intelligence data into IAM platforms.** Protecting against threats in the vacuum of your siloed environment will only offer partial and insufficient defenses against hacks and breaches. Forrester expects that, to keep adversaries out, IAM vendors will offer expanded capabilities for integrating and analyzing a range of identity analytics data, such as which IP addresses, device fingerprints, user name and password combinations, and sites hackers have used.[20]
- **Build identity federation across internal user stores and applications.** In a modern enterprise, user directories exist for every application and line of business, but each application requires attribute values from other internal applications' user directories. In the case of mergers or acquisitions or for other political reasons, user directory consolidation or redesign may not be feasible. To limit identity sprawl, you need to design user stores on directory platforms that support internal and external identity federation and maintain trust relationships and synchronization

between on-premises and cloud-based user directories.[21] These new-generation user stores must provide direct tools, such as mapping relationships between identities, for investigating cyberthreats.

› **Tweak application-level authorization based on context and activity.** While access certification processes reduce separation of duties violations and improve the company's general security posture, employees often view it as unnecessary and a major drag on productivity. To reduce the burden of IMG processes such as access recertification, leading multinational banks and financial services firms are deploying second-generation externalized authorization solutions that can dynamically tune authorization policy decisions in apps at runtime. They do this based on: 1) context, such as device fingerprint or geolocation of the accessing device, and 2) activity, such as what the user has looked at in the application or other sensitive applications today.[22] A promising technique is to create a prize point value for a resource for access and mandating that a user's running tally of authorization points match that of the accessed resource.

Partner IAM: Support Secure Partner Access With Cloud-Based Identity Services

Today's digital business relies on a growing number of business partners to deliver product, services, and new engagement models to its ultimate end customers. And those partners need to have controlled access to systems and data in your application ecosystem. An insurance carrier must provide extensive IAM services to the employees of all the independent insurance agencies it works with. Our clients tell us that their most important partner requirements for IAM in the next two to three years include the ability to:

› **Natively support relationship management.** Static representation of organizations and users doesn't communicate what they can access or how dangerous their activity is. An employee sponsoring a business partner's employee or administering to a business partner's organization means that the user directory and IAM solution must be relationship-aware; it must be able to quickly highlight relationships (and potential conflicts) and trending graphs and reports to administrators. For example, an independent business advisor partner of a bank may belong to multiple business partner organizations, which can cause separation of duties violations that only an IAM system with identity relationship management can detect.

› **Adopt IDaaS for fast federation services.** Although vertical-specific alliances have existed for a long time (e.g., Covisint in automotive and Exostar in aerospace/defense and pharma), IDaaS providers (such as Azure, Okta, OneLogin, and Ping Identity) now offer out-of-the-box federation hubs that let clients act as both identity providers and relying parties to each other in a controlled fashion. Forrester expects that, to alleviate the legal pain of contract sprawl in a growing multilateral federation ecosystem, IDaaS vendors will offer productized partner IAM services that offer the legal framework for entity (organization) and identity verification, access, and forensics. This will help streamline the process for providing seamless federated access for an employee of an IDaaS client supplier to an IDaaS client manufacturer's applications and data. DDID will likely become the infrastructural foundation for these federation services.

› **Make PIM-as-a-service available to partners and DevOps.** Companies require outsourcers to have VPN access to the company's network as well as access to the privileged identity management (PIM) vault and on-premises systems for administration. This process is not scalable, and administrators' activities are hard to track, leaving your data exposed. You need to ensure that your outsourced system administrators and business partners can easily gain authorized and monitored access to all your on-premises and cloud systems. In a containerized environment, DevOps also needs to have PIM support (secrets management, app-to-app credential management) to securely move away from hardcoded storage of sensitive credentials or storage based on an in-house solution.

Consumer IAM: Expand Customer Functionality Beyond Security

Digital businesses focus on delivering enhanced digital experiences that add value in the context of their customers' needs. S&R pros realize that customer IAM (CIAM) projects can't succeed without close collaboration across security, marketing, and business teams.[23] S&R pros evaluating CIAM must:

› **Provide customer profile management, not just security.** Traditionally, CIAM solutions have been focused on security-only and minimal identity management capabilities — registration, enrollment, authentication, and password and user ID recovery — but have not provided extensive profile management, versioned customer consent, terms and conditions acceptance, or master data management functionality. As digital channels become the dominant form of interacting with your customers, you have to ensure that your customer identity portal can expand the identity's scope from security-only attributes to managing the entire customer journey, including marketing preferences. It must also provide additional identity context that other downstream business applications can consume to support features such as personalization and recommendations. This is even more important as GDPR and privacy regulations mature.[24]

› **Ensure that reliable IDV covers businesses and relationships.** Using IDV methods based on credit file header or public records has been the foundation of IDV, but it has fragmented and lost the trust of firms and customers in the past three to four years.[25] It's easier than ever for hackers to gain access to anyone's credit file and social media footprint and answer knowledge-based IDV and authentication questions. New ways to verify identities have to be based on: 1) decentralized identity networks (e.g., Evernym, SecureKey, etc.); 2) a blend of non-self-asserted data (e.g., credit, lien, phone numbers, and device reputation stored as pointers on private and public blockchains); and 3) self-asserted data in social media (AKA digital exhaust).

› **Work with commoditized MFA-as-a-service; replace SMS OTP with push notification.** Multifactor authentication (MFA) has become the de facto protection for step-up authentication. MFA-as-a-service (e.g., Google Authenticator and Symantec VIP) continues to become commoditized and easier to integrate. Because malware can take control of a mobile phone's SMS text message inbox and act as a man-in-the-middle attacker, use of SMS text-message-based one-time passwords will decrease in the future, and vendors will replace them with biometrics (all

modalities from finger, face, and voice to behavioral), push notification to mobile applications, and software tokens.[26] Continued promotion of new biometric modalities such as the facial recognition feature in the extended iPhone X product line will further help drive customer use of biometrics, especially for consumer IAM interactions.

- **Track user behaviors to provide continuous authentication and authorization.** Up to now, authentication has been a one-time-only decision based on the credentials that the user presented. This led to easy, undetected account takeovers. S&R pros deploying CIAM platforms need to ensure that authentication and authorization in client-facing apps is ongoing: If a user behaves nicely, they can continue to access the site and transact with it. To determine if a user is who they claim to be, the site or system needs to read signals from the user's interaction and navigational activity to build a normalcy baseline profile, then detect and alert on any anomaly from the baseline.[27] If the anomaly points to fraud, the access control system should terminate the session or require additional step-up authentication from the user.
- **Use wearables for MFA and stronger device-to-human relationships.** With the mobile device becoming a standard way to access accounts, bank online, and perform other high-value transactions, delivering push notifications or obtaining a one-time password on a mobile device is not out-of-band and entirely secure. S&R professionals need to build and acquire IAM solutions that support wearable devices like smart watches as a second factor authenticator, maybe even coupled with biometric MFA such as heart rate, gait, and sensor data.

Connected Device IAM: Manage People, Apps, Systems, And Connected Device Access

Forrester expects that by 2021 the number of managed IoT devices will exceed 100 billion.[28] To prevent security breaches, security pros need to manage not only people, apps, and systems but also connected devices, both as actors and as endpoints in the IAM universe. This could range from smart speakers such as Alexa and Google Home to other sensors or connected devices. To secure their enterprise- and customer-facing IoT populations, S&R professionals must be able to:[29]

- **Massively scale user and object stores.** One of the most daunting challenges of IoT security is dealing with the scale of connected devices. Imagine, for example, the number of devices that just one hotel chain will create as it installs sensors on every door or window of every hotel property it owns. Today's large-scale LDAP directories can manage hundreds of millions of user objects but are largely unprepared to handle static and relational information of hundreds of billions of objects. In the next 18 to 24 months, you must upgrade your directory infrastructure to a much more scalable user and object store, such as node.js, USSignal, or Wasabi.
- **Source an IAM system that handles people, apps, systems, and devices.** The original concept of IAM was to manage how an identity (human or program) can gain access to a system (application or data). IoT adds a new dimension; you now need an IAM system with a natively built-in concept of devices as: 1) actors; 2) target systems; and 3) data containers. Only then can you appropriately manage registration and access to and from IoT devices.

- **Perform device-to-device authentication at scale.** When devices talk to each other, you have to ensure that communication only happens between authorized parties and on authorized pathways. The initial step here is authenticating one device to another. Clearly, old fashioned paradigms, such as authentication based on a password or key phrase, will not be practical here for a large number of devices. Instead, you will have to source an automated certificate management solution that is capable of automated certificate life-cycle management across multiple devices.
- **Manage identity within an evolving device ownership paradigm.** Traditional IAM has generally relied on a one-to-one relationship, as in one user with one mobile device and one mobile app. IoT deployments complicate this model considerably, with both many-to-many relationships (as in multiple household devices used by multiple family members) or with change in ownership (such as a connected device that is resold on a secondary market). This different dynamic of ownership and identity in IoT places a real premium on solutions that can effectively manage this dynamic, which could include capabilities such as delegated authorization (to manage usage by a household) as well as user-centric privacy controls (to enable deletion and resetting of a device profile upon change in ownership).
- **Manage consent in IoT environments easily and explicitly.** Custom-built, one-off user data usage consent and authorization solutions will not work here — they stall under the sheer number of devices they have to manage and the access rights on each of those devices. Enter user-managed access (UMA), which provides an OpenID Connect profile to standardize authorization on IoT devices and IoT security management planes that device manufacturers may provide.[30] For example, home automation vendors can use UMA to provide a delegation framework that allows a homeowner to temporarily allow a cable TV technician to open a home's garage door but not the front door. Forrester recommends that S&R pros look at IoT IAM platforms that explicitly support UMA and provide native measures for protecting data on IoT-connected devices.

What It Means

Growing Demand For IAM Will Drive New Entrants And Innovation

IAM has always been a complex area of security because of the need to integrate people, devices, systems, and processes. The challenges that firms face in different scenarios, from workforce, to consumer, to IoT, exacerbated by the landslide changes required by the GDPR, ensure that IAM vendors can't sit idle. Forrester envisions an IAM market in the next 18 to 24 months in which:

- **IAM suites become loosely coupled, microservices-based offerings.** Gone are the days of the classic IAM suite that offers all IAM functionality and requires the client to install everything. Loosely coupled, API-based, IAM microservices-oriented solutions will replace today's IAM behemoths. Even non-IAM Zero Trust vendors will adopt this API-centric, microservices-based approach to help ease implementation efforts. In response, it's highly likely that IAM vendors will

consolidate. Modern architectures, such as Okta and OneLogin, will lead the way here; incumbent IAM suites vendors, such as CA Technologies/Broadcom, IBM, Micro Focus, One Identity, Oracle, and RSA Security, need to evolve their IAM suites into much smaller, cloud-based, loosely coupled, and more-granular offerings — from both technical and pricing perspectives.

- **IDaaS becomes a viable alternative for all IAM services and adds identity analytics.** Today's IDaaS solutions are primarily about SSO, MFA, access policies, and simple access request management and SCIM-based provisioning to cloud apps. In the next 18 to 24 months, we will see IDaaS vendors, such as Centrify, Okta, OneLogin, and SailPoint Technologies, encompass full IMG functionality (including complex access request management, deep, visual workflow and attribute-based provisioning to on-premises apps and access recertification, and PIM) and extended all-around support for not just cloud applications but legacy, on-premises apps as well. Legacy IAM suites vendors (CA Technologies, IBM, Micro Focus, One Identity, and Oracle) will either fade into oblivion or continue to build bridge IDaaS solutions that allow their existing install base clients to use on-prem IAM solutions to manage cloud workloads (SaaS and IaaS apps).
- **Consumer IDaaS spawns a new class of customer management services.** Moving way beyond traditional security and IAM features, and built-for-privacy, CIAM will overlap with business intelligence, master data management, profile management, and marketing applications to form a new class of purpose-built, customer management platforms. These platforms from vendors such as Auth0, ForgeRock, Janrain, LoginRadius, Salesforce, and SAP (Gigya) will largely be available as SaaS offerings (customer management-as-a-service) but also deployable as on-premises solutions. Gradual, slow, and context-sensitive user registration that understands use cases and does not force users to unnecessarily disclose more information than necessary for registration will contribute to improved experiences as well as improved PII data protection and regulatory compliance.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

Companies Interviewed For This Report

Auth0
BeyondTrust
CA Technologies
Centrify
CyberArk
ForgeRock
IBM
Identity Automation
iWelcome
Micro Focus
NextLabs
Nok Nok
Okta
One Identity

OpenText (Covisint)	Simeio
Oracle	Stormpath
Ping Identity	Thycotic
RSA Security	Trusona
SailPoint Technologies	Tuebora
SecureKey	Twilio

Endnotes

[1] See the Forrester report "How Customer Experience Drives Business Growth, 2018."

[2] See the Forrester report "Use BT Road Maps To Drive Strategic Portfolio Management."

[3] See the Forrester report "Top Consumer Authentication Pitfalls To Avoid."

[4] Source: Janna Herron and Adam Shell, "Freezing your credit is free in all states under a new law following Equifax breach," USA Today, September 21, 2018 (https://www.usatoday.com/story/money/2018/09/21/equifax-free-credit-freeze-new-law/1377815002/) and Glenn Fleishman, "Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes, New Report Says," Fortune, September 8, 2018 (http://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/).

[5] You should seek proof from your IAM vendor that the IAM solution it offers has been designed with privacy in mind, stores its own internal data securely, and meets your regulatory compliance requirements when securing access to your business applications. This is an area where in-house solutions struggle most, as often these solutions were initially implemented in the shortest possible time, with minimal resources to meet simple requirements, and then grew significantly without truly being transformed to protect data and help with compliance. See the Forrester report "Best Practices: Customer And Employee Authentication" and see the Forrester report "The Future Of Cybersecurity And Privacy: Defeat The Data Economy's Demons."

[6] See the Forrester report "Assess Your Digital Risk Protection Maturity" and see the Forrester report "The Forrester New Wave™: Digital Risk Protection, Q3 2018."

[7] For more on the automotive attack surface, see the Forrester report "How To Secure Connected And Autonomous Vehicles."

[8] See the Forrester report "Top Trends Shaping Identity Management And Governance, 2019."

[9] See the Forrester report "Define A Compelling Strategy To Secure And Protect Mobile Moments" and see the Forrester report "Best Practices: Securing IoT Deployments."

[10] See the Forrester report "The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018" and see the Forrester report "Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model."

[11] See the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[12] For more information on pass-the-hash Kerberos attacks, read the SANS report. Source: Bashar Ewaida, "Pass-the-hash attacks: Tools and Mitigation," SANS Institute, January 21, 2010 (https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283).

[13] NIST has been advocating for the deprecation SMS text message-based MFA, as malware can take over the SMS text message inbox of a mobile device, making man-in-the-middle attacks much easier. NIST advises companies to move to push-based notifications to mobile applications — which is not always possible in countries where mobile internet is not as ubiquitous as it is in North America or Western Europe.

In June 2018, the systems of social network website Reddit were breached through an exploit of SMS-based 2FA. Source: "We had a security incident. Here's what you need to know," Reddit, August 1, 2018 (https://www.reddit.com/r/announcements/comments/93qnm5/we_had_a_security_incident_heres_what_you_need_to/).

[14] See the Forrester report "Best Practices: Behavioral Biometrics."

[15] See the Forrester report "Future-Proof Your Digital Business With Zero Trust Security."

[16] See the Forrester report "The Forrester Wave™: Identity-As-A-Service, Q4 2017."

[17] See the Forrester report "Decentralized Digital Identity: A Primer."

[18] IMG solutions include CA Identity Manager, IBM Security Identity Governance and Intelligence, and Oracle Identity Analytics.

[19] See the Forrester report "The Forrester Wave™: Identity Management And Governance, Q3 2018."

[20] See the Forrester report "Vendor Landscape: Security User Behavior Analytics (SUBA)" and see the Forrester report "The Forrester Wave™: Security Analytics Platforms, Q3 2018."

[21] Despite rapid growth in the identity-as-a-service (IDaaS) market, many security and risk (S&R) pros still rely on an existing on-premises Microsoft Active Directory (AD) to support their IDaaS offerings. While this hybrid approach enables them to realize IDaaS value quickly without significant changes to their directory infrastructure, it doesn't provide the full benefits of cloud-optimized identity architecture. See the Forrester report "Brief: Active Directory In The Cloud Is A Reality" and see the Forrester report "The State Of Microsoft Active Directory 2018."

[22] For example, if you are in your home office location, you can have write access to 1,000 records in the CRM system a day, but if you are in a rogue country, you can only have read access to 10 records.

[23] For more information on CIAM, see the Forrester report "Q&A: 10 Questions To Ask Before Deploying Customer Identity And Access Management."

[24] See the Forrester report "Top Trends That Will Shape CIAM In 2018 And Beyond" and see the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[25] See the Forrester report "Top Trends Shaping Identity Verification (IDV) In 2018."

[26] Interviewees report that fingerprint, facial, and voiceprint MFA authentication using the FIDO specification are the modalities gaining traction quickest with mobile application developers as well as with LOB managers who are seeking ways to simplify the online authentication experience. See the Forrester report "Now Tech: Authentication Management Solutions, Q3 2018."

[27] See the Forrester report "Secure The Rise Of Intelligent Agents" and see the Forrester report "Best Practices: Maximize The Business Value Of Biometrics."

[28] In the coming months and years, identity and access management (IAM) for IoT will become an important security pillar. See the Forrester report "Vendor Landscape: Identity And Access Management Solutions For The Internet Of Things."

[29] See the Forrester report "The IoT Attack Surface Transcends The Digital-Physical Divide."

[30] Source: Eve Maler, Maciej Machulak, and Domenico Catalano, "User-Managed Access (UMA) Profile of OAuth 2.0," Kantara Initiative, April 4, 2015 (https://docs.kantarainitiative.org/uma/rec-uma-core-v1_0.html).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.