


Evaluating Digital Identity Providers for Customer Identity and Access Management

Top Criteria, Differentiators, and Questions to Ask CIAM Providers

The Top Six Digital Transformation Trends Shaping Business and Society	2
Falling Short: Traditional, Disparate Systems	3
Multiple Systems and Silos.....	3
Traditional Identity and Access Management.....	3
Supporting the Six Trends' Customer Use Cases.....	4
The Way Forward: Digital Identity Platforms for Customer Identity and Access Management	4
Seven Basic Components for Customer Identity and Access Management.....	5
Beyond the Basics: Strategic Components for Customer Identity and Access Management.....	6
ForgeRock: Disrupting Digital Identity	12
Meet All Digital Identity Use Cases With One Simple Yet Comprehensive Platform.....	12
Gain Full Regulatory Compliance Based on Security, Privacy, and Consent.....	12
Create a Single, Organization-Wide View of the Customer.....	12
Expand Capabilities and Grow Revenue.....	12
Learn More About ForgeRock for Your Organization	12



Within the past decade, there has been an explosive combination of technology and ingenuity — culminating in six global trends that are actively and interdependently shaping business and society today. Anchored in customer experience and demand, these trends are now the landscape that organizations must navigate. To survive and thrive, organizations must be equipped to address each.

The Top Six Digital Transformation Trends Shaping Business and Society

1. The Disruptive Economy

The combination of ingenuity and technology has created a high-stakes game to capture consumer attention. This means constantly reinventing offerings to surprise and delight customers.

2. Internet of Things (IoT)

By 2020 there will be 25 billion connected 'things'. Unfortunately, most 'things' are not secure.

3. Cybercrime and over-reach

The number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting.

4. Public opinion

Public opinion has taken a defensive turn. Consumers want control of their personal data and for organizations to be held accountable.

5. Changing regulatory environment

The General Data Protection Regulation (GDPR) is the most profound regulation passed since the 1990s, changing business globally. Additional regulations (Open Banking, PSD2) have passed and more are expected to follow.

6. Gen Z and Gen Alpha

By 2020, Generation Z will become the largest consumer group in the US and Europe. Behind them, Gen Alpha already has household purchase influence.

To learn more about the six trends, download the paper: [The Top Six Digital Transformation Trends Shaping Business and Society: Why Digital Identity Platforms Are the New Imperative for Customer Identity and Access Management](#)

The six trends are a dominating force, necessitating that organizations:

- › Evolve quickly to address the latest 'disruption' and demand
- › Deliver secure, frictionless, omnichannel experiences
- › Build trusted, digital relationships across people, services, and 'things'
- › Establish themselves as a trustworthy brand
- › Support and adhere to the most advanced privacy and consent regulations (GDPR, Open Banking, PSD2)
- › Identify and protect against cybercrime

Unfortunately, the above presents real challenges to current organizational ecosystems.

Falling Short: Traditional, Disparate Systems

The need to collect data and secure the identities of customers and 'things'; adhere to regulations for privacy and control; and create delightful, seamless, and personalized customer experiences challenges current organizational ecosystems.

Therefore, in the context of the six global trends, organizational leaders must take inventory of the current systems and processes used throughout their enterprise.

Multiple Systems and Silos

To collect, secure, and manage customer identities and data, most organizations are still using a multitude of disparate systems across multiple departments. For example, a marketing department may be collecting user geo-locations and purchase history using two different software solutions. At the same time, IT uses multiple systems, such as traditional identity and access management (IAM) to secure the organization itself, along with a patchwork of other systems to keep departmental solutions and the data they gather in check.

Not only do disparate systems create an un-unified, inaccurate view of customers, they make risk assessments more difficult, increasing the likelihood of regulatory non-compliance. Additionally, the vast majority of these systems cannot secure 'things' nor their data — opening the door for breaches and hacks.

Traditional Identity and Access Management

Grounded in customer use cases, it is only within the past five years that the six global trends solidified. Within that time, most organizations have made large investments in traditional, employee-centered identity and access management (IAM) systems. As such, to address the new trends as they've appeared, many organizations have tried modifying their IAM systems. However, traditional IAM systems are built to support employee identities; they are not built to secure millions and billions of 'customers' and 'things' — nor the data they amass.

Traditional IAM uses static rules to make decisions. It was not designed to address the six global trends, such as to easily provide omnichannel experiences, secure 'things' and their data, create personalized experiences based on consumer context, enable users to control privacy, consent, and erasure over their data, or support regulations such as GDPR, Open Banking, and PSD2.

Rather than sewing multiple systems together and modifying traditional IAM to address the six global trends and prepare for the future, organizations must deploy an all-encompassing and purpose-built digital identity management solution.

Attempting to adapt existing IAM systems that do not have the flexibility, extensibility or scalability required is a common pitfall of organizations...

- ComputerWeekly

<https://www.computerweekly.com/news/450429018/Consumer-identity-management-will-benefit-business>

The Way Forward: Digital Identity Platforms for Customer Identity and Access Management

Unlike traditional IAM, and even traditional customer identity and access management (CIAM) systems, which are built only for specific use cases, digital identity management platforms are designed to secure and manage identities and data of every kind (employees, customers, devices, and 'things').

As such, they are implemented as a single, all-encompassing identity and access management solution across an organization for all use cases — employees, customers, devices, and 'things'.

Supporting the Six Trends' Customer Use Cases

In terms of the customer use cases defined by the six trends, the most advanced digital identity platforms must enable organizations to:

- › Personalize customer experiences, build relationships and deliver omnichannel experiences
- › Secure and connect billions of customer and IoT identities and data
- › Facilitate security, analytics, privacy, and control
- › Authenticate and authorize billions of logins and transactions daily
- › Support and adhere to regulations (GDPR, HIPAA, Open Banking, PSD2)
- › Integrate with other systems, such as marketing automation systems
- › Easily scale to meet demands and requirements
- › Identify and protect against fraudulent or malicious activities

With their all-encompassing, purpose-built capabilities, digital identity management platforms serve as the backbone of the secure, seamless, personalized, and privacy-minded digital ecosystem that customers demand.



Seven Basic Components for Customer Identity and Access Management

Behind the scenes, digital identity management platforms are now the enablers of both business and everyday life. Yet, platforms vary in their components and capabilities. The following are the seven basic components of digital identity management platforms needed to begin to address the six global trends.

To help evaluate providers for each component, RFP questions are also provided. For ForgeRock answers to the questions, read the [Comparing Digital Identity Providers for Customer Identity and Access Management Workbook](#). RFP questions by the healthcare, automotive and new mobility, retail, telecommunications, public sector and financial services industries are available in separate workbooks.

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Federated SSO	Based on trusted relationships between organizations, federated single sign-on (SSO) gives users secure access to those organizations' web properties and applications using a single account, hence single sign-on. Federated SSO uses open standards such as OAuth, WS-Federation, WS-Trust, OpenID Connect and SAML to pass authentication tokens between the organizations' identity providers.	Does the provider offer federated single sign-on based on open standards such as OAuth, WS-Federation, WS-Trust, OIDC and SAML?
Social Registration and Authentication	As a form of single sign-on (SSO), social registration and authentication allows users to register and authenticate quickly and easily using their existing information from a social networking service, such as Google or Facebook.	Does the provider offer social registration and authentication? Which social networking services are included in their offering?
Multi-Factor Authentication	Multi-factor authentication (MFA) is a method of validating a users identity through multiple authentication mechanisms. Authentication mechanisms include something the user knows, something the user has, and something the user is. For example, access is only granted after a user enters their password (what the user knows) and a numeric code sent by text to their phone (something the user has).	Does the provider offer multi-factor authentication? What authentication mechanisms do they offer?
Authorization	As part of access control within a digital identity solution, authorization is the function of determining if a user has permission to access a specified resource(s), such as a website(s), record(s), document(s), and so on.	What types of authorization methods and access controls are offered by the provider?
Self-Service	'Self-service' refers to allowing users to manage their accounts on their own rather than relying on an organization's support staff. Examples of self-service include managing login preferences, password management, updating contact information, requesting support, and so on. Self-service not only reduces support costs, it also improves user experience and customer engagement.	Does the provider offer self-service? What self-service capabilities does the provider support?

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Identity Store	As part of Directory Services , an identity store is a repository for the attribution data of identities. Stored identity data should be encrypted both while at rest and in transit. Also, as a best practice, it is good to have an embeddable repository that can easily share real-time customer, device, and user identity data across multiple environments. Additionally, from a hosting perspective, identity stores should include high availability, performance, and security. Also, the identity store should be fully compliant with LDAP v3 and should integrate seamlessly with any directory.	<p>Does the solution's identity store encrypt data both at rest and in transit?</p> <p>Does the solution offer fractional and multi-master replication?</p> <p>Can the identity store scale to support data from hundreds to millions of identities, including devices and 'things'?</p> <p>Does the solution's identity store comply with LDAP v3 and integrate seamlessly with any directory?</p>
Support for a Single View of Identities	A single view of a customer (an identity) organization-wide improves security, customer service, marketing initiatives, and more. For digital identity platforms to support 'a single view of identities', they must have the ability to integrate with other systems and consolidate multiple customer data silos in order to create a single view organization-wide.	<p>Can the solution integrate with other systems in order to consolidate identity data silos to create a single view of the customer organization-wide?</p> <p>Can the solution provide live bidirectional synchronization and reconciliation of identity attributes between data stores?</p>

Beyond the Basics: Strategic Components for Customer Identity and Access Management

To do their job well, digital identity platforms should go 'beyond the basics' and contain strategic technology components designed to not only address the current six global trends, but those to come. The following are the strategic components digital identity platforms must provide in order to meet today's six global trends and beyond.

To help evaluate providers for each component, questions are provided. Download [Compare Digital Identity Providers for CIAM: A Workbook](#) for ForgeRock's answers to the questions. For questions by the healthcare, automotive and new mobility, retail, telecommunications, public sector and financial services industries, read the industry [workbooks](#).

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Availability and Scale	<p>It is important to ensure that a user's access and session remains uninterrupted should something happen, such as a server going down. Digital identity providers should support both 'service availability' and 'session availability'. Service availability ensures users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down.</p> <p>Digital identity providers should also support a variety of scale scenarios. This includes a shifting number (often millions) of users, devices, and things that need to be stored in a database, as well as changing frequencies and lengths of simultaneous and concurrent sessions. Support for a stateless protocol using JWT session tokens is also advisable.</p>	<p>Does the solution scale elastically?</p> <p>For example, does it have the ability to scale the identity registration, authentication, and authorization service by many orders of magnitude to respond to predicted peaks, such as during a high profile event, or unpredicted events such as trending content demand or social media activities?</p>

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Open Standards Support	<p>Open standards are established, uniform technical norms used by developers. Each standard has specified capabilities and functionality. Identity security relies on the OAuth2, OpenID Connect, and SAML standards. Going beyond these basic identity standards, leading digital identity providers are integrating standards that are needed to support the six global trends, such as UMA 2.0, which allows users to securely share access to personal data with a third-party. Other advanced standards include OAuth 2.0 Proof-of-Possession, which ensures that the presenter of a bearer token is the real and original token owner, and OAuth2 Device Flow, which is designed for client devices that have limited user interfaces.</p>	<p>Does the solution support both basic and advanced open standards, such as OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow and OAuth 2.0 Proof-of-Possession?</p>
Zero Trust Security	<p>The Zero Trust Security model is based on the idea that no network, individual, 'thing', or device can be trusted.</p> <p>Digital identity platforms should be able determine whether an entity requesting an action is authorized to do so, and if they have proven they are the entity they claim to be with a sufficient level of assurance based on the risk of the specific action.</p> <p>Within a Zero Trust Security model, every action taken must be properly authenticated and authorized. To do this, authentication and authorization decisions leverage contextual information and become risk-based rather than binary, taking into consideration a rich set of information.</p>	<p>Does the solution provide a Zero Trust Security and CARTA model of risk and/or value-based authentication (Adaptive Authentication), enabling people, devices, things, and applications to have different levels of credentials to authenticate against a common Identity store?</p>
Distributed Scope Design with Least Privileged Access	<p>Scopes enable the principle of 'least privileged access'. This means only granting access that is essential to perform an intended purpose. For example, customers are only permitted to access the exact information and resources necessary for a particular and legitimate purpose.</p> <p>A first step towards achieving this fine-grained authorization is developing a mechanism to 'distribute' and assign strongly-typed scopes to applications, API endpoints, and other protected resources. Scopes must then be coupled with real-time context at policy-enforcing gates throughout the identity ecosystem. Scopes for fine-grained, actionable rules that can be used to make authorization decisions should also be applied.</p>	<p>Can the solution enable the principle of 'least privileged access' to only grant access that is essential to perform an intended purpose?</p>
Contextual Access	<p>Most identity solutions only protect at the initial authentication. To ensure the authenticity of users, devices, 'things', and services at all times and mitigate risk whenever an anomaly is detected, even during existing sessions, contextual access should be applied.</p> <p>As part of Next Gen AuthX, contextual access builds context-based intelligence into policies to assess risk and protect resources at the time of access as well as at any point during a digital session. Contextual access applies fine-grained authorization policies, adaptive risk, multi-factor authentication, and push authorization, yet only requires these stronger authentication mechanisms when necessary to make it easier for users while maintaining system security.</p>	<p>Does the solution leverage contextual authentication and authorization factors at any point during a session to assess risk—invoking stronger authentication mechanisms only when necessary by evaluating who the user is and their context?</p>

Basic Component	Description	Questions for Digital Identity and CIAM Providers
<p>Next Generation AuthX (Authentication and Authorization)</p>	<p>Traditional authentication and authorization methods include usernames and passwords, as well as third-party validated data elements, such as social security numbers and birthdates. However, in a Zero Trust model, it is assumed that these authenticators may be compromised.</p> <p>Therefore, digital identity providers should offer Next Generation AuthX consisting of continuous assessment for authorization and authentication. This includes transactional authorization and authentication, which requires users to perform actions and provide additional factors, often multiple times, for each high-risk transaction within a session.</p> <p>Authentication trees are an integral part of Next Gen AuthX. As a visual, drag and drop workflow, authentication trees allow administrators to easily configure, measure, and adjust login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. With an intuitive drag-and drop interface, administrators can also quickly consume out-of-the box authenticators, utilize existing authenticators, and integrate with cyber security solutions.</p>	<p>Can the solution easily configure, measure, and adjust authentication journeys using factors and digital signals (context, risk, behavior, choice, analytics) to not only determine risk, but to improve the user experience</p> <p>and inform downstream apps of the accumulated knowledge gained during the authentication journey?</p> <p>Does the solution pre-identify a user's digital signal such as location, IP address, device type, operating system, browser type, and more before a username is even collected?</p> <p>Does the solution provide OOB authenticators, the ability to custom build authenticators, and have rapid integration with third-party authentication, fraud, and risk providers in a centralized place?</p> <p>Does the solution allow authorization and authentication workflows to be easily viewed, created, and changed with drag and drop functionality through workflows and trees?</p> <p>Does the solution include transactional authorization for high-risk transactions within a session?</p>
<p>Log In Analytics and Decision Logic</p>	<p>The only way to continuously improve and secure the customer journey is to have data-driven insight. As part of Next Generation AuthX, user login analytics offer metrics and timers that analyze end-user interactions and their devices across all channels and lines of business. Digital identity platforms should therefore be able to monitor performance of third party fraud and analysis services that impact login journeys. Platforms should also allow administrators to optimize the customer journey with contextual and behavioral analytics that investigate what devices and browsers people use, where people log in from, the length of login journeys across the user population, and more. From this, organizations can discover correlations between existing login methods to improve customer adoption rates.</p>	<p>Does the solution evaluate whether logins result in increased abandoned shopping carts?</p> <p>Does the solution assess average time for call-outs to fraud systems?</p> <p>Does the solution monitor performance of Service Level Agreements that impact login journeys?</p> <p>Does the solution determine if shorter login journeys result in fewer help desk calls?</p>
<p>Progressive Profiling</p>	<p>Rather than asking users to fill out extensive registration forms, identity administrators can implement progressive profiling, a technique to collect user information as users interact with the system, on a website or application. For example, organizations can collect just the user's name, email, and password on initial signup. At a later point in time, the user's company and title may be requested.</p>	<p>Does the solution support progressive profiling across the customer journey and lifecycle?</p>

Basic Component	Description	Questions for Digital Identity and CIAM Providers
System Integrations	<p>Identity platforms are an important part of a solution ecosystem that store customer identities and perform data collection and analytics. This ecosystem includes Identity and Access Management (IAM), Mobile Device Management (MDM) systems, Customer Relationship Management (CRM) systems, and marketing automation systems. Unfortunately, most of these ecosystems result in fragmented views of the customer. Advanced digital identity platforms have the ability to integrate and connect with the systems listed above to create a single view of the customer organization-wide. This aggregated data provides a much more robust data-set with which to engage customers, such as using location data from the security system and using it for more customized marketing.</p>	<p>For greater personalization and an omnichannel experience, does the solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of the customer organization-wide?</p>
Privacy by Design and Consent Mechanisms	<p>GDPR mandates that users have control over their personal data, including privacy, security, and usage preferences. For global and regional compliance, it is imperative that digital identity platforms include Privacy by Design and Consent mechanisms based on the UMA 2.0 standard as well as integrate with other software that help meet regulatory requirements. Such mechanisms provide users with fine-grained controls to share and audit data about themselves, their devices and 'things'. A Consent Receipt feature to track user consent is also mandatory for a compliance-ready digital identity platform. Importantly, the user interface of the privacy and control mechanism should be intuitive and friendly.</p>	<p>Does the solution support a privacy and consent framework based on the UMA 2.0 standard?</p> <p>Can the solution provide users with fine-grained controls to share and audit data about themselves, their devices and 'things'?</p> <p>Does the solution include a Consent Receipt feature?</p> <p>Does the solution support "the right to be forgotten" that adheres to regulations such as GDPR?</p>
Data Residency	<p>Data residency and data sovereignty are related concepts covering the legalities of where user data resides, and the legal authority over the data, regardless of where it resides. Generally, data residency requires that a citizen's personal data be collected, stored, and processed only within their country's borders.</p> <p>To address the GDPR concept of data residency, digital identity providers should enable privacy-bound user data storage and fractional replication of personal data. This allows the processing of user data that is context-sensitive to a particular jurisdiction.</p>	<p>Does the solution support data residency by enabling privacy-bound user data storage and fractional replication of personal data?</p>
Data Aggregation of People, Things, and Their Relationships	<p>To create secure, personalized, omnichannel experiences, digital identity providers must allow organizations to aggregate relational data between people and their 'things' to create a highly comprehensive, single view of the customer. This is achieved by meeting several technical requirements, including establishing a common customer data model, connecting a broad range of data sources, implementing simple synchronization and reconciliation logic, and allowing access to customer data in an appropriate format.</p> <p>Importantly, with billions of digital relationships to support and manage, the most future-looking digital identity providers are developing Identity Graph Engines. These relationship-focused engines represent and query complex and interconnected webs of identity relationships that cross organizations, systems, people, services, devices, business agreements, and more.</p>	<p>Does the solution include identity relationship modelling at a granular level (parents, children, friends, and so on) for identity management between those relationships?</p>

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Identity at the Edge	<p>As discussed earlier, most IoT 'things' are not secure. Identity at the Edge secures devices and the data they collect with Edge Controllers and Identity Message Brokers.</p> <p>Edge Controllers secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks.</p> <p>Many IoT 'things' use non-secure protocols such as MQTT to identify themselves and send and receive information. Identity Message Brokers secure such protocols by translating MQTT, and other protocols, to HTTPS and making authentication and authorization for the devices and data possible.</p>	<p>Does the solution use Edge Controllers to secure IoT identities and their associated credentials in order to be trusted and usable across numerous connected ecosystems to prevent man-in-the-middle and other types of attacks?</p>
API First Model	<p>The API First Model is a developer-centric method of creating a solution. Within this model, a provider first creates the API and then builds the platform around it. This results in less complexity for external developers and organizations. For ease of use, scalability, and flexibility, digital identity providers should apply this API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service. The result should be a simple and secure way to extend identity to all realms, including social, mobile, cloud, and IoT.</p>	<p>For greater personalization and an omnichannel experience, does the solution integrate with other systems and enable the consolidation of multiple identity silos to create a single view of the customer organization-wide?</p>
System Integrations	<p>Identity platforms are an important part of a solution ecosystem that store customer identities and perform data collection and analytics. This ecosystem includes Identity and Access Management (IAM), Mobile Device Management (MDM) systems, Customer Relationship Management (CRM) systems, and marketing automation systems. Unfortunately, most of these ecosystems result in fragmented views of the customer. Advanced digital identity platforms have the ability to integrate and connect with the systems listed above to create a single view of the customer organization-wide. This aggregated data provides a much more robust data-set with which to engage customers, such as using location data from the security system and using it for more customized marketing.</p>	<p>Does the provider use an API first development model to create one common REST API framework across the entire platform to provide a single, common method to invoke any identity service?</p>
Legacy App Support	<p>Most organizations contain a great number of legacy systems and applications. Many of these store customer data and credentials, yet have limited or no built-in capabilities for user registration, authentication, authorization, or federation. Therefore, the ability to connect and extend to legacy systems and apps with a contemporary identity system is an important feature of digital identity platforms. This is done through an Identity Gateway, which allows both legacy and contemporary systems and applications to talk to one another fluidly and securely.</p>	<p>Does the solution have the ability to connect and extend to legacy systems and apps through an Identity Gateway?</p>
DevOps Friendly Architecture and Micro-services	<p>DevOps enables software development and deployment to run in a continuous cycle, allowing organizations to rollout new capabilities faster by reducing time to production. Digital identity providers should provide a DevOps friendly architecture with the ability to leverage DevOps tools, such as automating and orchestrating push-button deployment and continuous delivery. They should also use containerized images for rapid automation, with Docker support, as well as have an intelligent architecture that separates configuration from binaries to easily leverage version control for DevOps artifacts. Additionally, digital identity providers should provide command-line tools for remote configuration.</p> <p>Microservices is another important development method that focuses on building and deploying applications as groups of modular, composable services within an application. The benefit of microservices is the ability to singularly modify a service without impacting the others.</p>	<p>Does the solution support modern deployment DevOps approaches with containerisation and orchestration technologies such as Docker and Kubernetes?</p> <p>Is the solution built within a microservices architecture?</p>

Basic Component	Description	Questions for Digital Identity and CIAM Providers
Serverless Architecture and Patterns	<p>As discussed in the Availability and Scale section, organizations need to account for a variety of scale scenarios, such as millions of concurrent and simultaneous sessions. To do this cost effectively, leading digital identity providers support Serverless Architecture Patterns.</p> <p>Serverless Architecture allows servers to not only spin up and down as needed, but for data-center leasing terms to be based on the size of memory used on a server as well as the length of time that it was used. This method eliminates the need for developers to manage large quantities of servers that are only used periodically for peak load times.</p>	<p>Does the solution support serverless architecture patterns?</p> <p>Does the solution support three-tier web application pattern (REST), ETL (extract, transform, load) patterns, and Automation and deployment patterns (such as CI/CD)?</p>
Multi-Cloud and Hybrid-Cloud Support	<p>Multi-cloud environments have become a recent trend due to their increased flexibility, availability, and scalability. These environments allow organizations to eliminate vendor lock-in and speed time-to-market while reducing complexity and saving time and money.</p> <p>Hybrid environments include both on-premise and cloud environments. Cloud environments support needs at scale, while on-premises environments are advised to store sensitive data for better security. The advantage of hybrid environments is the flexibility to support any deployment, anywhere, at any time.</p>	<p>Can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud, within minutes for millions of identities?</p>
Identity Platform as a Service (PaaS)	<p>Maintaining and upgrading identity solutions is complex and labor intensive. With a true identity platform as a service (Identity PaaS), organizations can consume a comprehensive identity platform offering without having to be responsible for things such as hosting, maintenance, upgrades, and more. Further, when the Identity PaaS uses the same code base as the software version, organizations gain the flexibility to consume and deploy identity solutions throughout the enterprise as needed and at scale. These benefits and more allow IT resources to focus on other important initiatives, such as innovation and modernization.</p>	<p>Does the provider offer their entire identity platform as a service (PaaS)?</p> <p>Do the provider's as-a-service and software offerings share the same code base?</p>
System Auditing and Analytics	<p>System auditing and analytics capabilities are mission-critical functions. Digital identity platform must be able to conduct audits for system security, troubleshooting, usage analytics and regulatory compliance. They should also support a wide range of monitoring and logging capabilities. Audit logs ought to gather operational information about events occurring within a deployment to track processes and security data, including authentication mechanisms, system access, user and administrator activity, error messages, and configuration changes. Additionally, digital identity platforms must provide auditing and analytics for the systems they work with, such as partner systems.</p>	<p>Is the solution able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance?</p> <p>Can the solution also support a wide range of monitoring and logging capabilities?</p>
Strong Partner Ecosystem	<p>To address the six trends and more, the strongest digital identity solutions are those that work well with a wide variety of other technologies, software, and industry leaders in order to solve the unique goals of each organization. As such, digital identity providers must have a strong ecosystem of respected consultancy, technology, and integrations partners. Further, this partner ecosystem should be designed to immediately and easily support today's needs, as well as be a source of collaboration and innovation for the future.</p>	<p>Does the provider have a strong ecosystem of respected consultancy, technology, and integrations partners?</p>

ForgeRock: Disrupting Digital Identity

Identified as an customer identity and access management (CIAM) platform [Overall Leader by KuppingerCole](#) and one of the [most visionary access management provider by Gartner](#), the ForgeRock Identity Platform is the disrupter of digital identity.

Meet All Digital Identity Use Cases With One Simple Yet Comprehensive Platform

The ForgeRock Identity Platform is a flexible, unified solution that can be implemented across an organization for all use cases — employees, customers, devices, and ‘things’. The ForgeRock Identity Platform consists of access management, user-managed access, identity management, directory services, edge security, and an identity gateway. The full platform can be consumed as a service (PaaS) or deployed in minutes within any cloud environment, including multi-cloud and hybrid-cloud, for millions of identities. Importantly, the ForgeRock Identity Platform is the only solution on the market able to address all components of the six global trends and beyond.

Gain Full Regulatory Compliance Based on Security, Privacy, and Consent

The mission of ForgeRock is to create solutions that empower people through trusted digital relationships. With security, privacy, and consent as a top priority, ForgeRock was the first provider to deliver a comprehensive, interactive Profile and Privacy Dashboard for GDPR compliance. As such, ForgeRock is one of the only digital identity providers with the ability to address GDPR and the right to delete/erase personal data. ForgeRock also fully supports other regulations such as PSD2 and Open Banking.

Create a Single, Organization-Wide View of the Customer

ForgeRock offers the first solution on the market to model relationships across billions of users, devices, ‘things’, and cloud/microservices. This allows organizations to tie digital identities together, so a person, their connected things, and all the services they use are consolidated into a single user profile. Further, the ForgeRock Identity Platform uses real-time data and situational context to personalize and protect the customer experience.

Expand Capabilities and Grow Revenue

With ForgeRock, organizations gain the most comprehensive view of users across all digital channels as well as the ability to provide the personalized omnichannel experiences customers demand. Further, with one of the most sophisticated IoT security and support offerings on the market, ForgeRock enables organizations to utilize IoT with confidence. All of these capabilities and many more translate into increased opportunities to grow revenue.

Learn More About ForgeRock for Your Organization

As a leading provider, ForgeRock is designed to support the six global trends, secure the enterprise, build customer trust and loyalty, and grow business opportunities and revenue today and well into the future. Contact us to learn how ForgeRock can help your organization.

<https://www.forgerock.com/resources/view/64540906/analyst-report/kuppingercole-leadership-compass-ciam-2017.pdf>
<https://go.forgerock.com/Gartner-2018-Gartner-Magic-Quadrant-for-Access-Management-Report.html>

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.



Follow Us

