ForgeRock®

HOW TO EVALUATE

CIAM Providers for Enterprise Capabilities

A Checklist Buyer's Guide With Essential Customer Identity

Table of Contents

The Eight Digital Transformation Trends Shaping Business and Society **3**

Falling Short: Traditional, Disparate Systems **5**

- Multiple Systems and Silos 5
- Legacy Identity and Access Management 6
- Traditional Cloud-Based IAM Solutions 7

The Way Forward: Enterprise CIAM **8**

How to Evaluate CIAM Providers for Critical Capabilities **9**

- Basic CIAM Capabilities 9
- Intermediate CIAM Capabilities 12
- Advanced CIAM Capabilities 20

ForgeRock: The Undisputed Enterprise CIAM Leader **26**

Where to Go From Here **27**

The Eight Digital Transformation Trends Shaping Business and Society

Eight digital transformation trends are actively and interdependently shaping business and society. These trends help to inform what is required of a consumer identity and access management (CIAM) platform. To survive and thrive in the pandemic era and beyond, enterprise organizations must be equipped to address each trend.

1. Disrupted. The Reinvention Economy

The pandemic disrupted everything. Now, facing economic and geo-political uncertainty, enterprise organizations are in a high-stakes game to reinvent themselves to acquire and engage customers, mitigate their losses, and future-proof their businesses.

2. Partner Ecosystems

As part of their reinvention, enterprise organizations are entering multi-party digital ecosystems to fill consumers' insatiable demand for exceptional experiences and convenience.

3. Phygital Experiences

No matter how or where consumers interact with an organization, they want a seamless experience that blends physical and digital elements.

4. Smart Devices and the Internet of Things (IoT)

In large response to phygital demands, the global consumer IoT market is projected to increase from $97.50 billion in 2020 to an estimated $188.34 billion by 2026.[1] Unfortunately, most 'things' are not secure.

5. Cybercrime, Breaches, Fraud, and Overreach

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

6. Public Opinion and Activism

Today is the age of distrust. Public opinion has taken a defensive turn. Consumers want control over their personal data and want organizations to be held accountable.

7. Privacy, Consent, and Data Regulations

In response to public demand, governments worldwide have enacted regulations concerning privacy, consent, and data. More are expected in the coming years.

8. Gen Z, Gen Alpha, and the Metaverse

Generation Z is now the largest generation, constituting 32% of the global population.[2] Behind them, Gen Alpha is under 12 years old, yet its members influence over $500 billion in purchases. Both of these generations are loyal to experiences rather than to brands. Additionally, in the coming years, Gen Z and Gen Alpha will not only play within Metaverses, they will also learn, work,, shop, and invest in them.

To learn more about the eight trends, download the paper:
The 8 Digital Transformation Trends Shaping Business and Society

1 https://www.marketdataforecast.com/market-reports/consumer-iot-market
2 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/

Gaining future-ready capabilities is critical, especially to build a resilient organization able to sense and respond to volatility and disruption.[3]

Gartner

The eight digital transformation trends are a dominant force. They necessitate that organizations be able to:

- Reinvent their business and IT strategies to handle any disruption and meet consumer demands with agility and resilience at scale
- Securely participate in multi-party digital ecosystems
- Deliver secure and frictionless omnichannel customer experiences across the physical and digital domains
- Secure IoT and manage the relationships between people and their things
- Identify and protect against cybercrime and fraud
- Adhere to privacy, consent, and data regulations and establish themselves as trustworthy brands
- Future-proof their businesses to meet generational demands

Unfortunately, the necessities above present real challenges to current organizational ecosystems.

3 Gartner, The C-Suite Guide: Accelerate Digital for Future-Ready Business. Frameworks for composable tech, empowered customers and the future of work, 2021

Falling Short: Traditional, Disparate Systems

In the context of the eight trends, enterprise organizations' aim to acquire customers faster and deliver great experiences while complying with regulations and securing their consumers and the organization. Yet, traditional IT ecosystems make achieving this problematic.

70% of respondents rated disruptive growth as critical for their companies' success, but only 13% were confident that their company could deliver on this strategic priority.[4]

Deloitte.

Therefore, as a first step towards reinvention, organizational leaders must take inventory of the current systems and processes used throughout their enterprise.

Multiple Systems and Silos

To collect, secure, and manage consumer, partner, and IoT identities and data, most organizations still use a multitude of disparate systems across varying departments.

BMW used ForgeRock to consolidate 20 different identity and access management systems into one ForgeRock platform in order to realize significant cost savings, improvements in time to market, scalability and compliance.[5]

For example, a marketing department may use a multitude of software solutions to collect consumer data such as geo-locations and purchase history. At the same time, IT may use a patchwork of separate systems to manage the security of departmental solutions and the data they gather, as well as the organization as a whole.

Multiple systems result in silos, and a multitude of undesirable consequences. For instance, not only do disparate systems create a non-unified, inaccurate view of customers, they make risk assessments more difficult, thereby increasing the likelihood of regulatory non-compliance. Additionally, the more access points within an organization, the more risk of breaches.

4 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
5 https://www.forgerock.com/resources/view/108814636/customer-story/bmw-motors-into-the-digital-era-with-forgerock.pdf

Legacy Identity and Access Management

In an effort to mitigate costs, many organizations have tried modifying their current employee IAM systems to meet trends and demands, rather than invest in an enterprise CIAM platform. Yet, as the pandemic's disruption made apparent, the results are less than ideal.

> **Attempting to adapt existing IAM systems that do not have the flexibility, extensibility or scalability required is a common pitfall of organisations...[6]**
>
> ComputerWeekly

Legacy IAM systems are built to support employee use cases; they are not built to secure and manage millions or billions of consumer, partner, and IoT identities – not to mention their data. Also, legacy IAM was not designed to provide effortless, omnichannel experiences; support privacy and data regulations such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), or Consumer Data Right (CDR); nor mitigate the risk of today's sophisticated cybercrime and fraud. Furthermore, legacy IAM solutions don't support modern standards, making it impossible for them to address today's intermediate to advanced consumer, partner, and IoT use cases. It is also very difficult and expensive to upgrade them – yet they must be upgraded to meet the most basic use cases, not to mention the eight trends.

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

Traditional Cloud-Based IAM Solutions

In an attempt to get the CIAM functionality they needed quickly and easily, many enterprise organizations implemented traditional cloud-based IAM solutions. These early cloud-only IAM solutions focused primarily on simplicity for small to medium sized businesses at the expense of enterprise-grade functionality and configurability. This narrow focus allowed them to quickly gain market share within a band of organizations that had simple needs.

98%

of cloud-only IAM solution early adopters cited challenges.[7]

FORRESTER®

Enterprise organizations require greater capabilities than traditional cloud-only IAM solutions can deliver. These include enterprise-grade security and configurability.

In a 2021 Forrester study, nearly all (98%) of the early adopters of traditional cloud-only IAM solutions cited challenges including:

- Failure to integrate with existing business processes
- Inability to manage identities across current applications and systems
- Lack of visibility into on-premises systems, resulting in an incomplete picture of risk and security posture

The most consistent hurdle Forrester's respondents face is the inability to map or integrate to existing processes or legacy solutions. Business processes and identity integrations vary widely across applications. Each supports different standards and protocols. And this introduces complexity for any cloud-based IAM solution that does not support the required standards, or does not offer the flexibility and extensibility required to adapt to enterprise business needs. Simply put, these traditional cloud-based IAM solutions cannot integrate seamlessly with legacy and modern applications, nor adapt to enterprise business processes.

7 https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam

The Way Forward: Enterprise CIAM

Unlike legacy IAM and traditional cloud-based IAM solutions, enterprise CIAM is the foundation for reinvention, security, and disruption. Leading organizations use it to address each of the eight trends while reducing burdens on IT resources. With enterprise CIAM, they acquire customers faster, deliver great experiences, and protect their customers and organization by:

- Reinventing their business and IT strategies to handle any disruption and meet consumer demands with agility and resilience at scale
- Securely participating in multi-party digital ecosystems
- Delivering secure and frictionless omnichannel customer experiences across the physical and digital domains
- Securing IoT and manage the relationships between people and their things
- Adhering to privacy, consent, and data regulations and establish themselves as trustworthy brands
- Identifying and protecting against cybercrime and fraud
- Future-proofing their businesses to meet generational demands

CIAM plays a significant role in helping today's digital businesses acquire and retain customers, while providing them with the necessary security features and personalization for them to engage and transact with the company.[8]

FORRESTER®

8 https://www.forrester.com/report/now-tech-customer-identity-and-access-management-ciam-q2-2020/RES160459?objectid=RES160459

How to Evaluate CIAM Providers

The following table lists key CIAM critical capabilities and attributes; what they are and why they're important; and RFP questions to ask providers. The CIAM capabilities and attributes are grouped into Basic, Intermediate, and Advanced categories representing use case complexity. Note that most large enterprise organizations have advanced requirements.

Basic CIAM Capabilities

BASIC CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Federated SSO	Based on trusted 'federated' relationships between organizations, federated single sign-on (SSO) gives users, such as partners, 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. This capability is used to deliver great experiences. It addresses the Partner Ecosystems and Cybercrime trends.	• 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. This capability is used to deliver great experiences. It addresses the Phygital Experience, Gen Z and Gen Alpha, and Cybercrime trends.	• Does the provider offer social registration and authentication? • Which social networking services are included in their offering? • How does the CIAM solution administrator configure social identity verification?

BASIC CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Multi-Factor Authentication (MFA)	Multi-factor authentication (MFA) is a method of validating a user's 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). This capability is used to protect consumers and the organization. It addresses the Cybercrime and Public Opinion trends.	• 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. This capability is used to protect consumers and the organization. It addresses the Partner Ecosystems, Phygital Experiences, and Cybercrime, Public Opinion, and Privacy Data Regulations trends.	• What types of authorization methods and access controls are offered by the provider?
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. This core identity attribute is used to meet the Reinvention Economy, Partner Ecosystems, Phygital Experiences, IoT, Cybercrime, and Privacy and Data Regulation trends.	• Does the solution's identity store encrypt data both at rest and in transit? • Does the solution offer fractional and multi-master replication? • How does the identity store scale to support data from hundreds to millions of identities, including devices and 'things'? • How does the solution's identity store comply with LDAP v3 and integrate seamlessly with any directory?

BASIC CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
CIAM Platform Software As a Service (SaaS)	Maintaining and upgrading identity solutions is complex and labor intensive. With a comprehensive CIAM platform delivered as software as a service (SaaS), organizations can leverage the latest capabilities without having to be responsible for things such as hosting, maintenance, upgrades, and more. CIAM SaaS also allows IT resources to focus on other important initiatives, such as innovation. Security concerns – including data sharing and data sovereignty – are among the major reasons many large organizations have shied away from moving to a complete cloud CIAM platform. This is because many SaaS vendors combine multiple customers (tenants) into a single instance. This outmoded approach to multi-tenancy results in elevated risk because one organization's activities could impact other organizations. For this reason, the ideal CIAM SaaS platform offers full tenant isolation so data and workloads are never commingled with others. Tenant isolation also eliminates common challenges related to scaling and storing sensitive and regulated identity data in the cloud. CIAM SaaS should also provide data sovereignty and compliance, and maximum availability with individual backups. And, it should also include a high-availability architecture with transparent failover to meet strict service level agreement (SLA) requirements and tenant-specific backup and restore. This enables organizations to recover quickly and efficiently from any accidental or malicious data corruption issues. This cloud architecture model is used to acquire customers faster, deliver great experiences, and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, Cybersecurity, Public Opinion, and Privacy and Data Regulations trends.	• Does the CIAM SaaS solution offer full tenant isolation within a multi-tenant architecture? • How does the CIAM solution deliver granular data sovereignty? • How does the CIAM provider ensure data residency of identity, application, and backup data? • What is the CIAM provider's availability SLA for the identity SaaS solution? • How does the CIAM SaaS provider use industry standards used to design the data security architecture for solution? • What third-party assessments, audits, reviews or certifications have been obtained for the identity cloud solution?

Intermediate CIAM Capabilities

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
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. This capability is used to deliver great experiences. It addresses the Partner Ecosystems, Phygital Experiences, and Gen Z and Gen Alpha trends.	• What self-service capabilities does the provider support and how? • How does the CIAM solution customize and theme self service journeys for different user populations?
Secure Impersonation	An organizations' representatives, such as their help desk staff, sometimes need to 'impersonate' (in a good way) a user in order to take actions on the user's behalf. The secure impersonation feature enables users to consensually hand over temporary control over their account to another party for a set period of time. To extend consumer digital services to third parties requires OAuth 2.0 token exchange support. This capability is used to deliver great experiences and to protect consumers and organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and Gen Z and Gen Alpha, Cybersecurity, Public Opinion, and Privacy and Data Regulations trends.	• Does the CIAM solution support OAuth 2.0 token exchange including a CIBA (Client-initiated Backchannel authentication) grant? • How does the provider handle end user delegation and secure impersonation use cases?
Support for a Single View of Identities	A single view of a consumer's identity organization-wide improves security, customer service, marketing initiatives, and more. For CIAM 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 of an identity organization-wide. This capability is used to deliver great experiences, and to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, Gen Z and Gen Alpha, and Cybercrime trends.	• How does the solution integrate with other systems in order to consolidate identity data silos to create a single view of the customer organization-wide? • Can the solution provide live bidirectional synchronization and reconciliation of identity attributes between data stores? • How does the CIAM solution administrator configure migration of customers from a previous CIAM solution into the vendor's CIAM solution? How does it support gradual migration? • How does the CIAM solution administrator import existing password hashes?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Availability and Scale	Scale, performance, and availability are critical in an CIAM platform because if the identity platform goes down, so will the business. It's important to have a plan for bursts/spikes 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. CIAM 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. CIAM providers should also support a variety of scale scenarios. This includes a shifting number (often in the 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. Additionally, it's important to prevent latency in micrsoervice-to-microservice access decision (east/west flows are quite prolific) in addition to support for a stateless protocol using JWT session tokens. Availability and scale are not only part of the CIAM platform itself, but also how it is hosted. See the CIAM Software as a Service section for details pertaining to cloud. These capabilities are used to acquire customers faster and deliver great experiences. Availability and scale addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and IoT trends.	When it comes to evaluation of the CIAM platform itself, and not the hosting of it, consider the following: • Does the CIAM vendor offer performance benchmarking across transactions per section, loading of identity data, syncing identity data? What's the impact if a large number of IDPs (10s, 100s, or 1000s) is required? • Can the CIAM solution 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? • Does the identity provider support session availability, stateful availability, and stateless protocols? Does the vendor support redundant servicers, load balancers, HA deployments with n-way multi-master replication? Does the solution extend horizontally in multi-tenant environments?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Open Standards Support	'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 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. This capability is used to acquire customers faster, deliver great experiences, and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, Gen Z and Gen Alpha, Cybercrime, and Privacy and Data Regulations trends.	• Does the CIAM solution support both basic and advanced open standards, including OAuth2, OpenID Connect, SAML, UMA 2.0, OAuth2 Device Flow and OAuth 2.0 Proof-of-Possession, FIDO2, WebAuthN, and CIBA?
Contextual Access	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. 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. It 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. This capability is used to deliver great experiences and secure consumers and the organization. It addresses the Reinvention Economy and Cybercrime trends.	• 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?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
No-Code Identity Orchestration	Traditional authentication and authorization methods include usernames and passwords, as well as third-party validated data elements, such as social security numbers and birthdates. Yet, in a Zero Trust security model, it is assumed that these authenticators may be compromised. Additionally, traditional methods hinder good user experience. To provide secure, effortless user journeys, a CIAM solution should provide organizations with a no-code identity orchestration tool. With a drag and drop workflow interface, the no-code tool allows administrators to easily assemble and adjust workflows for steps such as registration, authentication, authorization, self-service, etc. in the users' journeys. This capability means users will receive highly tailored and personalized user experiences across channels and brands. No-code identity orchestration also gives administrators the ability to build authentication workflows that easily configure, measure, and adjust user login journeys using digital signals including device, contextual, behavioral, user choice, analytics, and risk-based factors. Administrators can also quickly consume out-of-the box authenticators, utilize existing authenticators, and integrate with cyber security solutions. This capability is used to acquire consumers faster, deliver great experiences, and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, Gen Z and Gen Alpha, and Cybercrime trends.	• Does the solution allow registration, authorization, and authentication journeys to be easily created, viewed, and changed with no-code drag and drop functionality through workflows and trees? • How does the solution 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 and inform downstream apps of the accumulated knowledge gained during the authentication journey? • How 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? • 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? • Does the solution include transactional authorization for high-risk transactions within a session?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Passwordless Authentication	The average user has more than 90 accounts. Remembering passwords is hard, which is why more than 50% of users have reused passwords across multiple websites. Additionally, creating passwords that rely on personal information makes accounts vulnerable to attacks. Using a password management system is one way to deal with the password problem, but some of these services themselves are vulnerable. Leading CIAM platforms enable organizations to design secure and seamless login journeys without the need for passwords, called Passwordless Authentication. Some CIAM solutions also eliminate the need for usernames. Passwordless Authentication reduces an organization's attack surface by virtually eliminating credential theft arising from phishing attacks, password reuse, credential stuffing, keyloggers, and more. This capability is used to deliver great experiences and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, Gen Z and Gen Alpha, Cybercrime, and Public Opinion trends.	• How does the CIAM solution enable an administrator to add Passwordless Authentication to a user's authentication journey? What steps does the administrator need to take? • Can the CIAM provider's Passwordless Authentication solution be used for both initial login and step-up authentication, including transactional authorization? • Does the CIAM solution include Usernameless Authentication?
Fraud Mitigation	While no single solution can address all aspects of online fraud, a combination of security infrastructure and CIAM features can detect credential theft, privileged account misuse, and transaction fraud. To predict whether fraud is likely requires context. CIAM platforms should enable organizations to design user journeys that detect anomalies both before and after the user authenticates. Fraud and threat signals include a user's location, IP address, device type, whether the device is jailbroken or rooted, operating system, browser type, user profile attributes, device cookie, last login, request header, time of day, and device fingerprint. Additional signals after authentication include the number of authentication attempts, the time of day, and the distance between the user's computer and their MFA factor. CIAM solutions can also integrate with third-party technologies to further mitigate the risk and cost of fraud. This capability is used to protect consumers and the organization. It addresses the Cybercrime and Public Opinion trends.	• How does the CIAM solution pull together fraud and threat signals to infuse context into a session before a user authenticates? • How does the solution capture and store additional signals after authentication to inform downstream applications? • Can the CIAM solution add a Google reCAPTCHA node into a registration journey to require user input and reduce automated/bot attacks? • How does the CIAM solution enable step-up authentication and transactional authorization for transactions occurring outside of the normal device, location, or behavioral context of a user? • Does the CIAM solution score user sessions with a high, medium, or low level of suspicion, and send users with a high risk to a honeypot version of their intended target?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Login Analytics and Decision Logic	The only way to continuously improve and secure the customer journey is to have data-driven insight. As part of identity orchestration, user login analytics offer metrics and timers that analyze end-user interactions and their devices across all channels and lines of business. CIAM 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 login 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. This capability is used to acquire customers faster, deliver great experiences, and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and Gen Z and Gen Alpha trends.	• Does the solution evaluate whether logins result in increased abandoned shopping carts? • Does the solution assess average time for call-outs to fraud systems? • Does the solution monitor performance of Service Level Agreements that impact login journeys? • Does the solution determine if shorter login journeys result in fewer help desk calls?
Progressive Profiling	Rather than asking your users to fill out extensive registration forms, you can implement progressive profiling, a technique to collect user information as users interact with your system, on your website or application. For example, you might collect just the user's name, email, and password on initial sign-up. At a later point in time, you might ask for the name of their company and their title. This capability is used to acquire customers faster and deliver great experiences. It addresses the Phygital Experiences and Gen Z and Gen Alpha trends.	• Does the solution support progressive profiling across the customer journey and lifecycle? • How does the CIAM solution administrator configure progressive profiling? • How does the CIAM solution administrator configure reports for supporting alternative (A/B) testing (e.g.: how does the registration abandonment improve with a change to registration pages)? • How does the CIAM solution administrator configure support for early stage accounts (unauthenticated, unregistered users)?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Business Systems Integration	CIAM platforms are an important part of a solution ecosystem that stores customer identities and performs 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. CIAM platforms should have the ability to integrate and connect with these systems 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. This capability is used to acquire customers faster and deliver great experiences. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and Gen Z and Gen Alpha trends.	• For greater personalization and an omnichannel experience, how 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? • How does the CIAM solution administrator configure the CIAM solution to integrate with a CRM solution (e.g. Salesforce)?
Privacy by Design and Consent Mechanisms	Privacy regulations such as GDPR mandate that users have control over their personal data, including privacy, security, and usage preferences. For global and regional compliance, it is imperative that CIAM 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 connected things. Importantly, the user interface of the privacy and control mechanism should be intuitive and friendly. This capability is used to deliver great experiences and protect consumers and the organization. It addresses the Public Opinion and Privacy and Data Regulations trends.	• Does the solution support a privacy and consent framework based on the UMA 2.0 standard? • How does the solution provide users with fine-grained controls to share and audit data about themselves, their devices and connected things? • How does the solution support "the right to be forgotten" that adheres to regulations such as GDPR? • How does the CIAM solution administrator configure multiple versions of consent documents and forcing customers to accept these versions?

INTERMEDIATE CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Data Residency	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. To address the GDPR concept of data residency, CIAM 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. This capability is used to protect consumers and the organization. It addresses the Public Opinion and Privacy and Data Regulations trends.	• Does the solution support data residency? • How does the CIAM solution administrator configure data residency for different geographies (i.e. storing data in correct regions, honoring data privacy globally)?
API First Model	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. This model is used to acquire consumers faster and deliver great experiences. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and IoT trends.	• Does the provider use an API first development model to create one common REST API framework across the entire platform? • How does the CIAM solution provide a single, common method to invoke any identity service?
Strong Partner Ecosystem	To address the eight trends and more, the strongest CIAM 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, CIAM providers must have a strong ecosystem of respected consultancy, technology, and integration partners. This ecosystem should include pre-built, tested, and always updated integrations ready to be easily utilized. This attribute is used to acquire customers faster, deliver great experiences, and to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, IoT, Gen Z and Gen Alpha, Cybersecurity, and Privacy and Data Regulations trends.	• Does the provider have a strong ecosystem of respected consultancy, technology, and integration partners? • How many of the partner integrations are pre-built, tested, and always updated? • Are the partner integrations included as part of the CIAM platform without additional charge?

Advanced CIAM Capabilities

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
AI and ML-Powered Threat Detection	Cybercriminals are becoming more sophisticated, leading to an increase in cyberthreats, such as account takeover. Account takeover (ATO) occurs when a bad actor gains unauthorized access to a user's digital identity account. ATO is often the source of data breaches, theft, and other fraudulent activities that lead to lost revenue, damaged brand reputation, and significant mitigation costs. To provide legitimate customers with the seamless, secure access experiences they demand, enterprise organizations require a modern security solution that removes unwanted friction while strengthening security. An AI and ML powered threat protection solution helps to prevent account takeover and fraud at the identity perimeter by treating each login request differently based on a risk score. This enables organizations to fast-track trusted users with options like passwordless authentication, while stopping attackers.	• Does the CIAM provider offer a threat detection solution that leverages artificial intelligence (AI) and machine learning (ML)? • How does the AI-powered solution prevent known threats? • How does the AI-powered solution prevent emerging or unknown threats? • Does the AI-powered solution require custom integration? • What type of enterprise-wide threat visibility does the AI-powered solution provide? • Does the AI-powered solution support a multi-layered intelligence security approach? • Does the AI-powered solution support no-code access orchestration? • Does the AI-powered solution support enterprise-grade scalability?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Flexibility for UI	The user interface (UI) for things like login boxes, profile pages, password reset interfaces, and so on, are an important part of a CIAM strategy that supports ease-of-use as part of a great digital experience. CIAM UI's should be folded into an organization's overarching corporate UI strategy. It is natural for such strategies to evolve. This attribute is used to acquire customers faster and deliver great experiences. It addresses the Reinvention Economy, Phygital Experiences, and Gen Z and Gen Alpha trends.	• Can the CIAM solution allow organizations to build a bespoke UI, meaning the ability to call REST APIs? • How does the CIAM solution use SDKs to more easily embed identity? • Does the CIAM platform include flexible hosted UI options?
Multi-Brand / Omnichannel / Cross-Channel (UI Theming)	Each user is unique and must be treated accordingly. An organization with multiple brands or channels (such as branches) needs to recognize each user and give them a personalized experience, directing them to the appropriately branded access experience. Additionally, organizations within multi-party ecosystems with partners need to manage different business units or groups of users within their identity hierarchy separately and discretely. They may need to extend some privileges to partners to better manage their end customers (B2B2C). A CIAM solution should include multi-brand UI theming that enables organizations to define unique journeys that connect users with the appropriate channel or brand. It should also support hierarchical tiers of users and delegated administrators. This capability is used to acquire customers faster and deliver great experiences. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, and Gen Z and Gen Alpha trends.	• How does the CIAM solution customize end user UI themes? • Can the CIAM solution dynamically select a theme based on a language input? • Can the CIAM solution detect the organization of which user is a member and then present a themed interface that matches the organization? • Can the CIAM solution detect that the user has visual impairment and switch to a high contrast theme?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Hierarchical, Multi-Brand, and Complex Organization Design	Most enterprise organizations create a hierarchy of departments or Lines of Business (LOB) to fit their needs around how they structure their business (e.g. multiple brands). These hierarchies inform how they then delegate administration as well as access rights to users within those organizations. The hierarchical, multi-brand, and complex organization design feature gives enterprises the flexibility to set up unique identity and access management configurations, like password policies and access permissions, for different audiences. It does this by allowing for the creation of hierarchical tiers of users and delegated administrators so organizations can set up and manage discrete groups of users to meet their business requirements. Hierarchies can be nested within other hierarchies as needed. Owners and admins are assigned to each hierarchy, who have the ability to manage the fine-grained access and authorization privileges of the users within their tier. An administrator of one organization might have full access to the users within that organization, but no access to the users in an adjacent organization. This empowers each admin in the hierarchy to make the changes they need to accommodate the security, usability, and convenience needs of their users. This approach saves organizations time and money by allowing them to consolidate multiple identity types into a single system. This capability is used to acquire customers faster, deliver great experiences, and to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, and Cybersecurity trends.	• How does the CIAM solution support unique identity and access management configurations for different hierarchies or lines of business (LOBs)? • How does the CIAM solution administrator set up the CIAM solution to support multiple brands or online properties of the same parent client organization? Demonstrate account linking. • How does the CIAM solution administrator create a new organization for the purposes of multi-tenancy (this is typically a requirement when an MSSP or a very large organization uses the CIAM solution and needs to ensure that certain admins only have admin privileges for certain client or internal organizations)?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Zero Trust Security	The Zero Trust Security model is based on the idea that no network, individual, 'thing', or device can be trusted. CIAM 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. 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. This capability is used to deliver great experiences and to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, and Cybercrime trends.	• Does the solution provide a Zero Trust Security and CARTA model of risk and/or value-based authentication (Adaptive Authentication)? • How does it enable people, devices, things, and applications to have different levels of credentials to authenticate against a common Identity store? • How does the CIAM solution administrator configure risk assessment using high risk device attributes (Including but not limited to jailbreaking, malware, emulators, disabled JavaScript, stolen cookies from another session)? • How does the CIAM solution administrator configure risk scores used to drive authentication policies (e.g.: customer is logging in from a rogue country, customer is logging in from a brand-new device, customer logins show implausible travel, etc.)? What kinds of own and third party threat feeds (bad IP addresses, etc.) are available in the CIAM solution? • How does the CIAM solution administrator configure protection of customers against credential stuffing and password spraying attacks?
Distributed Scope Design with Least Privileged Access	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. 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. This capability is used to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, and Cybercrime trends.	• How does the solution enable the principle of 'least privileged access' to only grant access that is essential to perform an intended purpose? • How can the CIAM solution grant scopes to different groups of users based on their organizational structure (location, reporting hierarchy, lines of business)?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Data Aggregation of People, Things, and Their Relationships	To create secure, personalized, omnichannel experiences, CIAM providers must allow organizations to aggregate relational data between people and their IoT 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. This capability is used to deliver great experiences and protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, Phygital Experiences, IoT, Gen Z and Gen Alpha, and Cybercrime trends.	• Does the solution include identity relationship modelling at a granular level (parents, children, friends, IoT, and so on) for identity management between those relationships?
Edge Security	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. 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. 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. This capability is used to deliver great experiences and protect consumers and the organization. It addresses the Reinvention Economy, Phygital Experiences, IoT, and Cybercrime trends.	• 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? • Does the solution use Message Brokers secure IoT protocols, such as MQTT, to HTTPS to make authentication and authorization for the IoT device and data possible?
Legacy App Support	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 modern identity system is an important feature of CIAM platforms. This is done through an Identity Gateway, which allows both legacy and modern systems and applications to talk to one another fluidly and securely. This capability is used to deliver great experiences. It addresses the Reinvention Economy trend.	• Does the solution have the ability to connect and extend to legacy systems and apps through an Identity Gateway? • How does the CIAM provider's Identity Gateway integrate with legacy applications that are not built to work with access management or single sign on (SSO) solutions? • How does the CIAM provider's Identity Gateway enable secure integration between legacy and modern applications?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
DevOps Friendly Architecture and Microservices	DevOps enables software development and deployment to run in a continuous cycle, allowing organizations to roll out new capabilities faster by reducing time to production. CIAM 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. 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. These capabilities are used to acquire customers faster and deliver great experiences. They address the Reinvention Economy trend.	• How does the solution support modern deployment DevOps approaches with containerisation and orchestration technologies such as Docker and Kubernetes? • How does the CIAM solution secure microservices? • How does the CIAM solution scale horizontally and vertically?
Serverless Architecture Patterns	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. 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. This capability is used to reduce costs and to address the Reinvention Economy trend.	• Does the solution support serverless architecture patterns? • Does the solution support three-tier web application pattern (REST, GraphQL), ETL (extract, transform, load) patterns such as FanOut, Big data patterns (such as MapReduce) and Automation and deployment patterns (such as CI/CD)?

ADVANCED CIAM CAPABILITY	WHAT IT IS AND WHY IT'S IMPORTANT	QUESTIONS TO ASK CIAM PROVIDERS
Multi-Cloud and Hybrid-Cloud	Multi-cloud environments have become popular 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. 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. CIAM platforms should include flexible consumption options that include multi-cloud and hybrid-cloud deployments. These consumption options are used to support the Reinvention Economy trend.	• How can the solution be deployed within any cloud environment, including multi-cloud, bring-your-own-cloud, or hybrid cloud? • Does it include a highly available and production-ready configuration? • How is the CIAM provider's solution licensed to support a hybrid-cloud model?
System Auditing and Analytics	System auditing and analytics capabilities are mission-critical functions. CIAM platforms 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 should 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. This capability is used to protect consumers and the organization. It addresses the Reinvention Economy, Partner Ecosystems, IoT, Cybercrime, and Privacy and Data Regulations trends.	• Is the solution able to conduct audits for system security, troubleshooting, usage analytics, and regulatory compliance? • Can the solution also support a wide range of monitoring and logging capabilities?

ForgeRock: The Undisputed Enterprise CIAM Leader

As the undisputed CIAM leader, ForgeRock helps enterprise organizations like yours address the eight digital transformation trends to acquire customers faster, deliver great experiences, and protect customers and the organization. With ForgeRock, you can do business better with the industry's only enterprise-grade, full-suite, AI-driven platform purpose-built for all identities and any cloud.

"In April 2020, we introduced BBC Bitesize, a website that provides parents and students with free videos, step-by-step guides, activities, and quizzes by level and subject. We relaunched the service within weeks and saw three million people use the service on launch day, with zero downtime."

Matt Gres, Director of Platform

BBC

FORRESTER®

LEADER

Forrester Wave™ Customer Identity and Access Management, Q4 2022

Gartner

HIGHEST SCORE

Gartner® Critical Capabilities for External Access Management and Application Development, 2022

kuppingercole ANALYSTS

OVERALL LEADER

KuppingerCole Leadership Compass, Customer Identity and Access Management, 2022

"At Philips, we're on a mission to improve people's lives and to empower people to take better care of themselves and others. With ForgeRock, we are able to design innovative data-sharing and consent technologies into our HealthSuiteDigital Platform that make it possible to foster consumer and patient trust."

Jeroen Tas,
Chief Innovation and Strategy Officer

PHILIPS

Global enterprise organizations drive growth and revenue with ForgeRock Enterprise CIAM. Join the ForgeRock community and support your unique reinvention initiatives to meet not only today's trends, but also tomorrow's.

Where to Go From Here

Learn more about ForgeRock and CIAM

- **Read** how HSBC delivers secure, personalized user experiences for more than 30 million customers in 36 countries
- **Watch** the ForgeRock and Deloitte webinar: *Four Technologies for Designing Captivating Digital CIAM Journeys*
- **Contact** sales to schedule a conversation and demo

"Now is the time to migrate to cloud, leverage AI, and take advantage of next-generation infrastructure; the architecture enterprises build today will determine their future."[9]

accenture

Independent Third-Party Resources

Read these analyst reports to learn why ForgeRock is the enterprise CIAM leader:

- **Forrester Total Economic Impact™ Study** of ForgeRock Customer Identity and Access Management
- **The Forrester Wave™:** Customer Identity and Access Management, 2020
- **Gartner®** Critical Capabilities for Access Management, 2021
- **KuppingerCole Leadership Compass:** CIAM Platforms, 2020

- For CIAM Market and Technology Training and Advisory, visit **The Cyber Hut**.

9 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf

About ForgeRock

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that 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 1300 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 headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com**.

Follow Us

ForgeRock