BUYER'S GUIDE:

CUSTOMER IDENTITY & ACCESS MANAGEMENT (CIAM)

SHIFTING MARKETPLACE

Over the last few years, there's been a major shift in requirements for enterprises managing customer identities. This shift comes from analysts who, as of 2015, have recognized customer identity and access management (CIAM) as its own distinct space with its own distinct requirements. But it's also driven by a more demanding competitive landscape where customer experience is the battleground on which market share is won and lost.

Customers today are hyper-connected and are adopting new patterns of engagement that spread their customer journeys across multiple channels. Each interaction point must have a cohesive customer experience, be secure and adhere to customer privacy and consent regulations.

CIAM business drivers span across teams from line of business to marketing to technical and security, and their requirements are just as diverse. Finding the right CIAM solution takes cross-functional collaboration and diverse capabilities from a comprehensive CIAM platform.

DEFINING CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM)

Recently, there's been a tremendous increase in the quantity (and quality) of solutions aimed specifically at solving the challenges posed by CIAM. The industry as a whole is recognizing that trying to treat customer identities as a simple extension of existing enterprise identity solutions simply won't work. CIAM if fundamentally different from employee IAM in several ways:

1. **Business Drivers** - Employee IAM business drivers include reducing risk and improving efficiencies, while CIAM business drivers revolve around increasing customer engagement and revenue.
2. **Scale** - Enterprises may have tens of thousands of employees in the largest of cases, but even moderate customer deployments can have millions of customers and billions of attributes.
3. **Registration** - Employees are provisioned and HR guides the process. Customers register themselves.
4. **Privacy** - Customers have strict privacy regulations, like GDPR, that employees don't. Violations can cause brand damage, lost customer trust and hefty fines.
5. **Service-level Requirements** - While service-level requirements are often high for employees, they're extremely high and even more important for customers. Customers won't tolerate lags and outages, whereas employees have little choice.

At its most basic level, CIAM solutions need to provide capabilities to solve for three major aspects of customer interactions with your brand that include:

1. **Access** - Enterprises must be able to securely let customers into their digital properties through authentication and registration capabilities. These capabilities should be consistent across channels and contain features that streamline the process, like social login.
2. **Recognition** - Enterprises must be able to recognize their customers once they're authenticated, no matter which channel or app they use to sign on. This includes giving the right customers access to the right content, and utilizing a unified profile that's accessible to all applications to personalize customer experiences across channels.
3. **Protection** - Enterprises must protect their customers from breach and be good stewards of customer data. That means implementing secure authentication and registration best practices including contextual multi-factor authentication (MFA) that balances security and convenience, securing the API/application layer with access control and session management, and securing customer data through data access governance, data encryption in every state and more.

Enterprises need to be able to address these fundamental categories of CIAM with a high-performance solution that can handle extreme scale.

DEFINE BUSINESS OBJECTIVES

Defining your business objectives up front will narrow your focus and ensure that you're looking at the right solutions. The top business challenges typically driving the need for CIAM solutions are:

1. **Digital Business Transformation** - It's becoming more and more common for enterprises to have digital business initiatives that aim to transform the ways customers interact with their brand. CIAM enables secure, consistent multi-channel customer experiences that can help transform the way enterprises conduct digital business.
2. **Increasing Security Threats** - The scale and frequency of data breaches are increasing. As a result, breach prevention is becoming a high priority for IT and security teams. Through end-to-end security geared specifically for customer identities, CIAM solutions can drastically reduce the risk of data breaches.
3. **Privacy Regulatory Compliance** - With strict privacy regulations that vary by region, industry, company and even from person to person, meeting customer privacy regulations can seem like a daunting task. CIAM solutions provide centralized data access governance policies and other capabilities to ensure that customer data sharing consent, regional data storage and other privacy mandates are met.
4. **Development and Delivery of Mobile Applications** - Launching a new application can often be a catalyst for providing a consistent customer experience across channels. This can help enterprises lay a foundation and introduce scale, performance, security, single sign-on, social login and other CIAM capabilities into an enterprise.

Though these are some of the most common business drivers, others that require scale, performance, security and other CIAM capabilities may also exist. These might include mergers and acquisitions, Internet of things (IoT) adoption or others.

TOP THREE BEST PRACTICES FOR CIAM IMPLEMENTATION

1. **Balance Customer Experience and Security** - This requires close collaboration between line of business/marketing and IT/Infosec teams. This collaboration will ensure that security team requirements as well as line of business usability standards are met.
2. **Engineer for Scale** - Focus not only on total number of users, but on peak usage scenarios that can sometimes be unexpected. Peak usage outages can be the most costly. Ensure that whatever solution you're looking at is priced for consumer use and works at consumer speed (>1 sec response times don't cut it with consumer apps).
3. **Plan for Multi-channel** - Whether you call it multi-channel or omnichannel, your customers are already engaging with you across many channels. Anticipate how your CIAM solution will facilitate and maintain consistency during multi-channel customer journeys.

PITFALLS TO AVOID

1. Partial solutions (e.g., MFA but no data layer security, SSO but no profile unification)
2. Complex, disjointed stack of software to meet CIAM requirements
3. DIY projects that seem simple at first, but end up costing more time and money when considering security, privacy, authentication and the long list of associated best practices

CIAM VENDOR SELECTION GUIDELINES

- Experience and references
- Financial viability and market stability
- Scope of services/completeness of solution
  - Identity management implementation experience
  - Managed services experience
- Proven implementations with extreme scale and performancey
- End-to-end security that spans authentication, application/API and data layers
- Standards-based solutions that are extensible and future-proof
- Ability to deploy in any environment (on-premises, cloud, hybrid)

SOLUTION CHECKLIST

FUNCTIONAL CONSIDERATIONS

Authentication Layer Requirements

EVALUATION CRITERIA	IMPORTANCE
Does the vendor have federated SSO capabilities?	Federated SSO ensures that customers have a consistent login experience, with common credentials, across digital properties.
Does the vendor provide social login?	Allowing customers to use existing identities (such as Facebook or Google) to authenticate with your brand can streamline user experiences during registration and authentication. It's also important for users to be able to link and unlink social accounts after they've registered.
Does the vendor support self-service account management?	Once registered, customers need self-service capabilities to manage, add, update, or delete their own data.
Does the vendor include registration best practices such as account recovery and centrally managed password policies?	It's important for CIAM vendors to include best practices like password reset and centralized password policies for added security.
Does the vendor support risk-based, contextual MFA?	Requiring users to provide second authentication factors (e.g., SMS, biometrics) isn't one-size-fits-all. Requiring second factors must be risk-based and consider the user's device context, the resource they're attempting to access, the type of transaction they're performing, or other contextual factors.
Can the vendor embed MFA into your own mobile app?	The ability to turn your mobile app into a secure second factor gives your customers an MFA option that is both more secure and convenient than SMS or Email MFA.

FUNCTIONAL CONSIDERATIONS

Application/API Layer Requirements

EVALUATION CRITERIA	IMPORTANCE
Can the vendor provide fine-grained access control to applications and APIs?	It's important to be able to centrally manage access control to specific URLs and APIs. Vendors should also provide centralized contextual access control policies.
Does the vendor provide preference management capabilities?	Enterprises need to provide customers with the ability to explicitly define preferences, which should be stored in a unified customer profile to facilitate consistent, personalized experiences across channels.
Does the vendor provide session management and single logout?	Enterprises that provide several channels and applications need the ability to offer single logout for all applications to enhance both security and convenience to customers.

FUNCTIONAL CONSIDERATIONS

Data Layer Requirements

EVALUATION CRITERIA	IMPORTANCE
Does the vendor provide a secure, scalable directory solution?	When storing customer identity and profile data, security, scale and performance are all important. It's vital to ensure that vendors provide a directory that is secure and can store millions of identities and billions of attributes. Make sure there are customer references to support the scale you need.
Can the vendor's directory store unstructured data?	The data you'll want to collect about your customers may be diverse and included unstructured data like browser fingerprints. It's important to be able to easily store that data in your customer directory.

FUNCTIONAL CONSIDERATIONS

Data Layer Requirements

EVALUATION CRITERIA	IMPORTANCE
Is the vendor's directory accessible via REST APIs?	The customer and profile data within a directory needs to be accessible through developer-friendly REST APIs so it can be easily accessed by existing apps and speed time to market for new apps.
Does the vendor provide real-time, bidirectional data synchronization capabilities?	Real-time, bidirectional data synchronization can help create a unified customer profile (in a CIAM directory) from disparate identity data silos, even if there's a need to maintain other identity repositories. It can also help facilitate zero-downtime, risk-free data migrations to a unified customer directory.
Does the vendor support fine-grained data access governance to meet privacy regulations?	Privacy regulations are diverse and requirements vary from person to person. CIAM solutions must contain centrally managed privacy policies that enforce customer consent and govern data sharing on an attribute-by-attribute level to all internal and external applications.
Does the vendor encrypt data at every state and implement other data layer security best practices?	Customer data breaches can be devastating to a brand's reputation. For that reason, it's important to ensure that customer data is encrypted in every state–at rest, in motion and in use–and subject to other best practices such as active and passive alerts, and tamper-evident logging.

FUNCTIONAL CONSIDERATIONS

Platform Requirements

EVALUATION CRITERIA	IMPORTANCE
Is the vendor's platform built on open standards?	It's important for CIAM platforms to utilize open standards such as SAML, SCIM, OAuth2 and OpenID Connect. This ensures extensibility and versatility of the CIAM solution.
Does the vendor support strong, end-to-end security at every layer?	It's important that CIAM vendors provide strong security during authentication, at the application/API layer and at the data layer.
Can the vendor handle extreme scale and performance and have a track record of success to support it?	Vendors must be able to support millions of stored identities and billions of attributes, even in peak usage scenarios with hundreds of thousands of concurrent users. They must have proven track records of success achieving 99.99999% availability and millisecond latency.
Does the vendor provide customizable reference applications and pre-built UIs.	Enterprises almost always want to completely customize user interfaces, but vendors that provide pre-built assets and UIs allow customers to speed time to market for new applications.

VENDOR EVALUATION & SELECTION

After you've defined all of your requirements, you'll want to organize them in a way that makes it easy to evaluate how each vendor stacks up. A Sheets or Excel spreadsheet works well. Create rows for each of your final criteria, organized by core stakeholder requirements as we've done above.

Next, add columns for each vendor you want to evaluate. Rate each vendor on how well they meet your criteria using a point-based rating system like this:

0 = Does not meet requirement
1 = Very limited support for requirement
2 = Partially meets requirement
3 = Meets or exceeds requirement

Using this system, you rate each vendor from 0-3 on each of the criteria. Then tally each vendor's totals. The vendor with the highest total score is also the vendor that best meets your requirements.

Want additional guidance on choosing the right CIAM solution for your enterprise?
Read our whitepaper:
Getting Customer IAM Right.

#3061(rev) | 02.18 | v03