Developing a Customer IAM (CIAM) Strategy and Roadmap

Initial Publication Date: 29 July 2020

Abstract

This is the third report TechVision has released on the topic of Customer Identity and Access Management (CIAM). In our report three years ago, we characterized CIAM as an "emerging" category. Eighteen months ago, we declared that CIAM had "emerged", but now we see CIAM as maturing. We find that most large enterprises are leveraging CIAM in some way, major vendors (such as Akamai and SAP) have acquired early CIAM leaders (Janrain and Gigya) and other vendors (Okta and Ping) achieving successful IPOs.

CIAM is important and highly visible as it provides organizations with a public gateway to secure external engagement and is a critical element of any Digital Enterprise program. CIAM is often an organization's first "touch point" with a prospect and an on-going reflection of a brand. The CIAM stakes are high; get it right and you'll attract customers, drive revenue and positively representyour organization; get it wrong and your business/image will suffer.

This report offers recommended customer-centric IAM strategies, architectural approaches and pragmatic, experience-based advice. CIAM differs from traditional (internal enterprise-focused) IAM with a greater emphasis on user experience, privacy and consent management, increased scale, integration with CRM/marketing systems and a business/sales focus.

This report provides strategic and tactical recommendations for enterprises building an IAM foundation for customer/prospective customer engagement and external stakeholders in the context of business goals. This report covers:

- The enterprise CIAM value proposition, core requirements and business rationale
- Developing a CIAM strategy and action plan
- The CIAM market and vendor short list
- Recommendations and next steps

Authors:

Gary Rowe
CEO & Principal Consulting Analyst
gary@techvisionresearch.com

Doug Simmons
Principal Consulting Analyst
dsimmons@techvisionresearch.com

Table of Contents

Executive Summary

Customer IAM (CIAM) is an area every large organization should be paying attention to. It is one of the most important foundational areas organizations should be investing in to prepare to become a truly Digital Enterprise. This IAM category is rapidly evolving and is critical to building trusted customer relationships and providing requisite security and privacy protection. Enterprises are architecting customer-centric IAM solutions and vendors are developing CIAM services that are differentiated from traditional Enterprise IAM solutions.

TechVision Research recommends the use of CIAM-centric, cloud-enabled services as opposed to simply fine-tuning traditional enterprise-centric IAM products and services—at least in the short-to-intermediate term. CIAM is particularly adept at supporting key Sales and Marketing objectives including enticing and engaging prospective customers, better serving and retaining current customers and establishing trusted, secure and sustainable relationships. For example, in TechVision's recent report on the Digital Trust we describe CIAM as a core part of establishing *Mechanical Trust*.

A CIAM program, properly executed, is a conduit towards building lifetime digital customer relationships. Establishing trusted connections and building relationships that generate useful data and can be served by better customer knowledge are keys to digital business success. These digital relationships can be maintained and enhanced over time with a steady flow of updated contextual and progressive profiling-generated information that drives personalized customer offerings and improves business decisions.

CIAM is different than many infrastructure technologies in that the business benefits are so directly visible and impactful. In many cases the customer engagement process can make or break a lifetime relationship; get CIAM right and you can build a strong digital presence and business results; get it wrong and your competitive advantage can be forever lost.

In building a CIAM program, organizations should start by focusing on the customer experience and how CIAM can support the evolution of this experience throughout the suspect/prospect/customer lifecycle. Relationships to be managed may be initiated by anonymous users investigating your website and grow as offers are responded to and trust is built up. During this process data is aggregated and customer profile information naturally evolves throughout the lifetime of the relationship. This method of gaining customer insights as the customer journey evolves is characterized as progressive profiling and a key part of a strong CIAM offering.

CIAM is different in many ways from traditional IAM. The major focus within CIAM is on the customer - with an emphasis on minimizing friction and enticing engagement. This is different from employee-facing IAM in that employees are generally required to use the system as a condition of employment with an emphasis on security, compliance and provisioning. Prospects and customers may be lost forever if the registration, log-in, update process, consent management and other CIAM services are not deemed to be an intuitive, responsive and overall positive experience.

Another key area of focus in building a CIAM program is ensuring that trust is established with the proper data security, consent and privacy protection. Customers expect some control over how their data is collected, managed, stored and shared and the CIAM service needs to support this. In the era of more rigorous data protection and privacy regulations such as the General Data Protection Regulation (GDPR) in Europe, the Canada Privacy Act and the California Consumer Privacy Act of 2018 (AB 375), strong security and privacy controls and policies are necessary prerequisites for any CIAM program.

TechVision recommends that CIAM programs be considered a priority area of investment in most large enterprises given the direct business benefits and risks if customer data isn't properly managed. Digitally connecting with customers and building sustainable business relationships require a strong and flexible Customer IAM foundation. This report describes the difference between CIAM and traditional IAM, key end-user requirements, CIAM architecture considerations, design guidelines and a short-list of vendors to consider. Traditional, enterprise-focused IAM is generally not the best solution to support customer facing applications and services, while CIAM is architected to specifically support the needs of current and prospective customers while minimize external risks.

Introduction – A Customer IAM Platform

For the past 25 years, most organizations have focused the bulk of their IAM investments in support of employees and contractors. This internally focused product/service has traditionally been called Identity and Access Management (IAM) or Enterprise IAM. Most large enterprises recognize that IAM needs to be extended to broaden its reach. Digital Enterprise (often called Digital Transformation) programs are extending digital connections to include customers and external stakeholders. CIAM can optimally support these connections and relationships throughout the prospect/customer lifecycle.

In our report on CIAM three years ago, we characterized Customer IAM as an "emerging" category. In our report on CIAM 18 months ago we declared that it had "emerged". At this point we are beginning to see some maturity, increased vendor investment, broader usage and major vendors (such as Akamai and SAP) acquiring early initial CIAM leaders. We've also seen Ping and Okta go public with Okta's recent market cap at over $26 Billion. TechVision Research currently classifies CIAM as a separate and distinct Identity and Access Management category and we expect this to remain the case for the next several years. Ultimately there may be a single full-service Identity as a Service (IDaaS) platform that can handle both customers and internal users, but TechVision believes that this is a few years out…and even if there is a consolidated platform, most organizations may logically separate internal and external accounts for security, privacy protection, skill set and business continuity reasons.

> Most organizations may logically separate internal and external accounts for security, privacy protection, skill set and business continuity reasons.

CIAM reflects an expanding set of IAM requirements that are not fully accommodated by the traditional IAM solutions. The increased scale, the diverse contextual information requirements, the focus on an engaging user experience, key privacy considerations/ regulations and support for and integration with sales/marketing and business critical applications are areas of particular emphasis in CIAM. Simply put, identifying, securing, contextualizing, supporting and providing a greater focus on user experience while ensuring appropriate protection for Personally Identifiable Information (PII) is critical in supporting current and future customers.

Most enterprises that don't have a separate CIAM solution still have an IAM service that supports customers, but they are often just extensions of existing enterprise-focused IAM platforms. Customers still must be supported, so these organizations use legacy systems with different schemas (internal and external), different security processes/policies and physical separation between customer and internally facing IAM services. This can be a workable solution, but the problem over time is that traditional EIAM platforms have not been optimized for the customer experience and are not optimized for scale nor the cloud.

All enterprises have access to a growing base of customer data, but this data is often in disparate silos, not structured or just not being leveraged in an optimal way. For competitive reasons, the business benefits of providing a secure, seamless and unified customer experience across multiple channels (omni-channel experience) as part of Digital Enterprise/ Transformation programs is driving the CIAM market. The immediate benefits to the customer are to reduce friction by offering choices of interfaces, offering simplified-yet-secure login, providing self-service capabilities and relevant contextual data leading to personalization, progressive profiling and transaction efficiency. These factors lead to increased customer engagement and the likelihood of brand loyalty as long as security is maintained and privacy is respected.

The friction reducing benefits to the customer are

- choices of interfaces,
- simplified-yet-secure login,
- self-service capabilities and personalization,
- progressive profiling and transaction efficiency.

From a business perspective, the upfront investment in CIAM offers faster time to market (immediately connecting with customers), a reduction in administrative overhead (automated, electronic processes) and ultimately, an on-going increase in revenue and client retention. But the use of CIAM and the collection and use of contextual data provides much more than just engaging the customer; the consistent use of these platforms are core business opportunities to get to know and serve customers better and more efficiently.

The challenge for both CIAM and customer data in general is that typically most customer data is stored in distinct database instances that are uncoordinated and unsynchronized, providing minimal value-added functionality. In fact, the very lack of coherence between multiple forms of Customer Relationship Management (CRM) and customer databases systems can lead to customer frustration, security vulnerabilities and lost opportunities for the organization. The right customer-facing IAM service can provide valuable profile information, preference data, consent management and other contextual information to support the integration of the right data with the right customers/prospects. In short, it can support key business goals through efficiency, accuracy and security.

Hence, it not only makes sense but it becomes a business necessity to address the issue by adopting a CIAM strategy that will give your customers' data at the very least the same level of care as that of your employees and at the same time improve their online experience.

It would be easy for an organization to view CIAM as 'simply' an extension of their existing EIAM or CRM systems – or both. At one level, CIAM does provide a similar degree of access to company resources as compared to EIAM, but CIAM requires greater usability and autonomy in managing profiles and preferences in support of developing long-term relationships and uncovering business opportunities. We'll now take a look at how CIAM is developing as a separate IAM category and how it differs from traditional, internally focused IAM.

Enterprise (traditional) IAM vs. Customer IAM

While CIAM is based on long-standing Identity Management principles originating within the enterprise, there are major differences and areas of emphasis that are driving the Customer IAM category. Key deltas include increased scale, new types contextual information/ relationships, personal data control, a high priority placed on the user experience and key privacy considerations/regulations. CIAM is optimized for customer engagement while protecting the company and the individuals engaging.

This specialized class of IAM services requires links into marketing systems, CRM systems, customer data bases and reporting systems and must handle both the scale and the imprecision in engaging with customers and prospective customers. Employees generally won't leave if there is a poor IAM user experience, but customers and potential customers need to be enticed and motivated to engage and reengage. These stakeholders are also increasingly technology-savvy and expect a fast, pleasant and secure user experience or they may simply find that experience elsewhere.

Employees generally won't leave if there is a poor IAM user experience, but customers and potential customers need to be enticed and motivated to engage and reengage.

Building a customer-oriented identity management system demands a significant shift in the way vendors and their clients approach the management and use of identities. Employees and contractors are a captive audience; they generally won't leave because of cumbersome identity registration, update, login or provisioning processes. Enterprise IAM has traditionally been confined to a predictable, often static environment, based on a set of mandated policies that, to date, have security and access control as their design goal, while often leaving the user experience as a lower priority.

Customer or consumer IAM on the other hand is driven by an organization's desire to engage prospective customers and build loyalty with existing clients. CIAM also provides more insight into its customers and plants the seeds for long-term business relationships, enabling closer online responsiveness based on behaviors and both observed and customer-provided preferences. In contrast with EIAM, CIAM is, by its very nature, open to the Internet and involves scaling to hundreds of thousands or potentially many millions of personal identities. Scale apart, there are considerable differences between the approaches taken by traditional IAM solutions, which focus on managing employees and, in some cases partners and a new breed of CIAM services intended to manage interactions and relationships with customers and consumers. The key drivers for both are radically different, driven by different parts of the business and requiring different technical solutions and architectures.

Stricter data protection and privacy regulations supported by the threat of heavy fines and penalties are also increasing the stakes for better organizing, managing and protecting customer data. Marketing systems, CRM and CIAM services house large volumes or personal information - if customer data isn't properly managed it isn't just an administrative headache, it can also become a significant potential liability to businesses and their brands. This (privacy/data protection) is an issue with IAM systems supporting employees, but customer data presents more expansive risks.

While a small number of vendors offer CIAM-only solutions, most of the EIAM market leaders are extending their B2E portfolio to address the requirements of Business to Customer (B2C) to affect the convergence addressed in this document. Others, however, will continue to differentiate between the two – at least for the time being – often partnering with a specialist vendor for CIAM. As we'll describe later in this report, we are beginning to see vendors (e.g., Ping, Microsoft, ForgeRock, Okta) offering a core IAM service with different views or configurations for customer engagement.

The following table provides a summary of the more important differentiators between CIAM and EIAM requirements and characteristics. These deltas as well as the increasing investment in the CIAM area (by both the vendors and their customers) are driving the movement towards purpose-specific CIAM service offerings.

Characteristic	Enterprise IAM	Customer/Consumer IAM
Business		
Purpose	Platform for employee engagement and the encouragement/enforcement of good corporate behavior	Platform for discovery and development of a relationship with the customer to drive consumption, brand loyalty and revenue
Drivers	Security risk and cost reduction, employee productivity, on- boarding and off-boarding efficiency	Acquisition, engagement, recommendation & retention; revenue-driven
Intelligence	Static, rules-driven intelligence; but changing with increased use of contextual awareness	Dynamic, real-time, analytics-based; Progressive profiling, personalized, frictionless security based on analytics
Governance, Risk and Compliance		
Access Management	Information protection and appropriate access is key to the enterprise	Dynamically balance ease of use/engagement against risks
Access Governance	High priority	Low-to-medium priority, transaction value-based
Policies & Permissions	CIO/IT/CISO with perhaps some input from LOBs	LOB/Marketing and CIO/IT/CISO as well as (increasingly) the customer directly
Privacy Compliance	Centralized policy-driven with further controls for regulatory compliance; Implicit consent	Policy-driven as well as customer-driven and opt-in/opt-out and explicit consent management. Protection of PII is key as is privacy regulation compliance
Architecture		
Adaptability	Integration with back-end systems such as HR and Active Directory, with growing SaaS integration	Dynamic schema required to support managing consent, opt-ins and preferences; Integration with CRM and customer reporting solutions
Agility	Traditionally monolithic and predictable	Modular and adaptable
Architecture	SOAP/REST, principally desktop/laptop centered	REST, often "mobile device first"
Extent	Perimeter-based, enterprise-defined; but evolving to perimeter-less	Borderless, inclusive, internet-scale
Network	On-premise, moving to cloud/hybrid as well as BYOD/BYOI/BYON	Mobile and cloud-first; on-premise/hybrid if necessary
Performance	Higher latency using captive IDs, primarily for security	Lower latency for frictionless user experience, taking account of busy hours (evenings and weekends)
Scalability	Tens or hundreds of thousands, relatively stable size	Hundreds of thousands or millions, sometimes expanding with Sales & Marketing campaigns

Velocity	Corporate or LOB requirements for on-boarding, often slow and methodical	Internet speed with risk awareness
Data		
Data	Predefined by IT, stored in directories and relational databases	Derived from many sources, often using unstructured data requiring dynamic schema and progressive profiling, increasingly adding IoT devices and data
Enrollment	Triggered by employer	Initiated by consumer or through registration invitation link
Profile & Preferences	HR and employee with limited scope	LOB from CRM and consumer through self-service, with personalization a key to long-term engagement
Provisioning	HR-driven, defined by CIO/IT policies	Users voluntarily register through self-service or registration invitation link, define desired interactions
Scope	Employees, contractors, consultants and sometimes partners	Customers/prospects/consumers; optionally employees, contractors, partners, service providers who are also customers (e.g., Retail employees)
User Experience		
User Experience Priority	Generally low priority, but gradually improving, driven by more by non-security focused departments, such as HR or Engineering	Unified user experience is high priority, further enhanced by self-service, fast response time and simple registration
Personalization	Limited but beginning to add personalization/birth rights, largely driven by HR	Considered a differentiator and a benefit to both enterprise Marketing-focused LOBs and consumers

Table 1: Enterprise IAM vs. Customer IAM Comparison

CIAM Opportunities and Business Benefits

One of the areas TechVision spends a lot of time covering is the new digital world enterprises are facing and this world is accelerating at unprecedented speed in the wake of the COVID-19 global lockdown. We believe that organizations aren't just transforming, they are becoming Digital Enterprises. The transformation is on-going and pervasive as the Digital Enterprise is evolving to better enable the way we do business. One of the most critical factors towards securing and managing this new digital reality is a robust and inclusive Identity Management foundation. And the most visible part of this IAM foundation is how organizations engage their customers via CIAM.

The business benefit that CIAM brings is so much more direct than other "infrastructure" services; CIAM allows an enterprise to better connect with and better understand customers and prospective customers by observing their activity and collecting data while on their website(s). If this is done right and supported by other services, there can be a positive impact on revenue and customer satisfaction; it is hard to make such a strong claim with other infrastructure technologies. CIAM, done right, drives revenue growth by connecting with customers, responsibly collecting data and using the insights from that data to acquire, retain and grow customer revenue and loyalty.

Functional areas that drive CIAM-based business benefits fit into almost every element of external relationships, but IT, Marketing, Sales, Legal and a variety of LOBs benefit directly from a strong CIAM program. The most visible area of CIAM is Sales/Marketing given their involvement in engaging, analyzing and selling and we'll discuss these direct benefits next.

CIAM is all about engaging current and future customers and it can be a game changer for enterprise sales and marketing teams by efficiently improving connections and insights at scale. Marketing is all about is understanding and categorizing a target market and understanding user preferences, buying patterns, intent and influencers. CIAM and the Digital Enterprise together provide a wide range of connections and generate data to be analyzed at scale to increase insights, brand loyalty and, ultimately sales.

But remember, collecting customer data can also increase enterprise risk as regulatory controls increase in volume and complexity. Collecting data without consent or in amounts deemed excessive can damage trusted relationships and can also create legal and regulatory risks. The good news is that proactively and transparently addressing the security and privacy challenges (like clear and simple privacy policies, implementing Privacy By Design…) can also build customer loyalty and is a foundational principle in good CIAM programs. Customer connections and building relationships supported by CIAM is a major business benefit as long as you maintain the trust your customers and prospective customers are implicitly offering by engaging with you.

A key component of the Digital Enterprise is getting to know your customer and prospective customers better and CIAM is perfectly positioned to support this. The principles of Know Your Customer (KYC) require businesses to verify who their clients are and specifically determine that they are neither laundering money nor engaged in fraud, not involved in terrorist activities or any form of illicit trafficking and are anti-bribery compliant. Although KYC is mandated for the banking and finance community, enterprises of all sizes engaged in any financial transaction have a need to know that their customers are legitimate; in other words, 'they are who they say they are', not on any transactional blacklist, and of low or accepted risk. One of the key capabilities of CIAM services is to identify anomalous or suspicious behavior, not only at the beginning of a customer relationship but throughout the full customer lifecycle.

Most organizations benefit from improving their knowledge of targeted customers and prospects. Behavior patterns are discernible from a variety of different input sources, such as purchasing preferences, location-based information, social media feeds, and data collected/verified from identity profiling. CIAM services, often in combination with Marketing systems and CRM services, can provide insights to business leaders (Marketing, Sales, LOB executives) about customer trends, leads generated, conversion rates by market segment, cross-selling opportunities and, of course projected and actual sales results.

Correlating customer patterns/usage data with identity data can provide insights as to who the customer is, with whom they associate, and what they are likely to buy. The primary goals of present day commercial digital marketing are to determine who you are, who your friends are, and your habits in order to predict what you're going to want next and figure out how to offer it to you at a compelling price point. CIAM services combined with the right privacy controls can enhance customer confidence and trust that is critical in determining if the brand reputation is strengthened rather than compromised.

> Correlating customer patterns/usage data with identity data can provide insights as to who the customer is, with whom they associate, and what they are likely to buy.

Some of the most valuable sources of marketing and sales data comes from customer self-interest and usage. When someone identifies himself or herself online, they voluntarily give up a certain amount of data before participating in a loyalty program or even before making their first purchase. The more confidence this individual has in the brand and the privacy protection, the more complete and genuine the responses, will generally be. For example, if a consumer doesn't trust the brand, doesn't like the digital experience, isn't confident as to how the data generated will be used or shared, then the data they provide (if they provide any data) may not be accurate or complete. This is a critical business area that can be supported by the right CIAM infrastructure.

It is important to understand that CIAM is a critical element of an externally facing Digital Enterprise program, but only a piece of the puzzle. While CIAM helps to identify and contribute to decisions concerning appropriate access, these services do not replace marketing automation or CRM systems. They integrate with and augment these systems to help organizations get maximum business value out them. We'll next net out some of the key Customer IAM requirements we typically find and recommend in working with large organizations.

About TechVision

World-class research requires world-class consulting analysts and our team is just that. Gaining value from research also means having access to research. All TechVision Research licenses are enterprise licenses; this means everyone that needs access to content can have access to content. We know major technology initiatives involve many different skill sets across an organization and limiting content to a few can compromise the effectiveness of the team and the success of the initiative. Our research leverages our team's in-depth knowledge as well as their real-world consulting experience. We combine great analyst skills with real world client experiences to provide a deep and balanced perspective.

TechVision Consulting builds off our research with specific projects to help organizations better understand, architect, select, build, and deploy infrastructure technologies. Our well-rounded experience and strong analytical skills help us separate the "hype" from the reality. This provides organizations with a deeper understanding of the full scope of vendor capabilities, product life cycles, and a basis for making more informed decisions. We also support vendors in areas such as product and strategy reviews and assessments, requirement analysis, target market assessment, technology trend analysis, go-to-market plan assessment, and gap analysis.

TechVision Updates will provide regular updates on the latest developments with respect to the issues addressed in this report.

About the Authors

Gary Rowe is a seasoned technology analyst, consultant, advisor, executive and entrepreneur. Mr. Rowe helped architect, build and sell two companies and has been on the forefront the standardization and business application of core infrastructure technologies over the past 35 years. Core areas of focus include identity and access management, blockchain, Internet of Things, cloud computing, security/risk management, privacy, innovation, AI, new IT/business models and organizational strategies.

He was President of Burton Group from 1999 to 2010, the leading technology infrastructure research and consulting firm. Mr. Rowe grew Burton to over $30+ million in revenue on a self-funded basis, sold Burton to Gartner in 2010 and supported the acquisition as Burton President (now Gartner for Technical Professionals) at Gartner.

Doug Simmons brings more than 25 years of experience in IT security, risk management and identity and access management (IAM). He focuses on IT security, risk management and IAM. Doug holds a double major in Computer Science and Business Administration.

While leading consulting at Burton Group for 10 years and security, and identity management consulting at Gartner for 5 years, Doug has performed hundreds of engagements for large enterprise clients in multiple vertical industries including financial services, health care, higher education, federal and state government, manufacturing, aerospace, energy, utilities and critical infrastructure.