TechVision RESEARCH

Developing a Customer IAM (CIAM) Strategy and Roadmap

Initial Publication Date: 12 November 2018

Abstract

A few years ago, TechVision released our research report on the "emerging" Customer Identity and Access Management (CIAM) market. Today CIAM is no longer emerging; it has "emerged" as most large enterprises are developing distinct customer-centric IAM strategies, architectures and programs. CIAM has several differences from traditional (internal enterprise-focused) IAM including a greater emphasis on ease of use, privacy and consent management, customer-centric data security and integration with CRM, marketing systems and key sales/business initiatives.

CIAM provides a gateway to the customer and is one of the most important elements of any Digital Transformation program. CIAM is often the first "touch point" an organization has with a prospect and is an on-going reflection of a brand. Get CIAM right and you will attract customers, drive revenue and represent your organization in the best light; get it wrong and your business will suffer.

In this report, we provide a foundation for enterprises looking to build an IAM foundation to support the engagement of customers, prospective customers and external stakeholders in the context of business goals.

This report covers:

- The CIAM value proposition and business rationale for the enterprise
- 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

David Goodman
Principal Consulting Analyst
David@techvisionresearch.com

TechVision RESEARCH

Table of Contents

Executive Summary

Customer IAM (CIAM) is an area every large organization should be paying attention to. This relatively new IAM category is rapidly evolving and is critical to building trusted customer relationships. 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 services; not just fine tuning traditional IAM products and services. Key areas of focus within CIAM include supporting key Sales and Marketing objectives including enticing and engaging prospective customers, better serving and retaining current customers and establishing a trusted, secure and sustainable relationship.

Simply put, 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 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 and provisioning. Prospects and customers may be lost forever if the registration, log-in, update process, data protection and other CIAM services are not deemed to be a 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 GDPR in Europe, the Canada Privacy Act and the California Consumer Privacy Act of 2018 (AB 375), strong security and privacy controls are necessary prerequisites for any CIAM program.

TechVision recommends that CIAM programs be considered an investment priority 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 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 IAM is generally not the best solution to support customer facing applications and services, while CIAM is architected to support the needs of your customers and minimize external risks.

Introduction – A Platform for Customer IAM

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 Transformation programs are extending digital connections to include customers and external stakeholders. CIAM can optimally support these connections and relationships.

In our previous report on CIAM a few years ago, we characterized Customer IAM as an "emerging" category. At this point we believe CIAM has "emerged". TechVision Research currently classifies CIAM as a separate and distinct Identity and Access Management category. An indication of the development of this space is that many of our clients have major initiatives focused on specifically on CIAM, whereas a few years ago Customer IAM was often just an extension of the incumbent (generally employee-centric IAM) Identity and Access Management service to accommodate customers. There are vendors and service providers that specifically focus on Customer IAM. TechVision also surveyed enterprise IAM decision makers and found an increasing percentage of large organizations were funding or planned to invest in CIAM-centric programs. So the stage is set and the right for CIAM to enter a rapid-growth track.

The movement to CIAM reflects an expanding set of IAM requirements that are not fully accommodated by 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 currently have some separation of IAM services that support customers and services to support employees, but they are often just bolted onto existing enterprise-focused IAM platforms. Using legacy systems with different schemas (between internal and external), different security processes/policies and physical separation between customer and internally facing IAM services has been the status quo, but customers and LOB leaders are demanding more. The problem is that general purpose (internally-facing) platforms have not been optimized for the customer experience and are often on-premise only offerings.

These enterprise IAM limitations have led to the development of specialized IAM services that integrate with marketing systems, CRM systems, customer/prospect data bases and reporting systems and can handle the scale and uncertainty in engaging with customers and prospective customers. These external customer "stakeholders" are increasingly technology-savvy and expect a fast, pleasant and secure user experience or they may simply find that experience from your competition.

All enterprises have access to a wealth of data about their customers, but this data is often in disparate silos 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) is driving the CIAM market. The immediate benefits to the customer are to reduce friction by offering choices of interfaces, offering simplified login, providing self-service capabilities and relevant contextual data leading to personalization 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.

From a business perspective, the upfront investment in CIAM offers faster time to market, a reduction in administrative overhead 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 so much more than just engaging the customer; there are opportunities to get to know and serve customers better and more efficiently.

CIAM systems need to also accommodate the wealth of data relating to external stakeholders that may include prospects, customers or partners. Typically most of that information is stored in distinct database instances is uncoordinated and unsynchronized, providing minimal value-added functionality to either the customer or the organization. In fact, the very lack of coherence between systems can lead to customer frustration and lost opportunities for the organization. The right customer facing IAM service can provide valuable profile information, preference data, consent management and other supporting information to support the integration of the right data with the right customers/prospects.

In short, it can support key business goals.

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 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 autonomy in managing profiles and preferences in support of of developing long-term relationships and uncovering business opportunities. We'll now take a look at how CIAM is developing into 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 some major differences that are driving the emergence of this new category of IAM. Key deltas that have emerged as we extend the reach of IAM to external users include increased scale, new types contextual information/relationships, personal data control, a high priority placed on the user experience and key privacy considerations/regulations. Simply put, enterprises need a platform that is optimized for consumer engagement.

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 can be controlled (to a degree), 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 can be controlled (to a degree), 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. The most fundamental difference is that employees 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. By contrast with EIAM, CIAM is, by its very nature, open to the Internet and involves scaling to hundreds of thousands or potentially 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 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 is an issue with IAM systems supporting employees, but customer data presents new types of risks.

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.

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 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.

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 stand-alone CIAM service offerings.

Characteristic	Enterprise IAM	Customer/Consumer IAM
Business		
Purpose	Platform for employee engagement and the encouragement/enforcement of good corporate behavior	A closer relationship with the consumer leading to product consumption and brand loyalty
Drivers	Security risk and cost reduction, 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
Governance, Risk and Compliance		
Access Management	Information protection and appropriate access is key to the enterprise	Balance ease of use/engagement against risks
Access Governance	High priority	Low-to-medium priority
Policies & Permissions	CIO/IT/CISO with perhaps some input from LOBs	LOB/Marketing and CIO/IT/CISO as well as the customer directly
Privacy Compliance	Centralized policy-driven with further controls for regulatory compliance	Policy-driven as well as customer-driven and opt-in/opt-out and associated 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	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	REST
Extent	Perimeter-based, enterprise-defined; but evolving to perimeter-less	Borderless, internet-scale
Network	On-premises as well as BYOD/BYOI/BYON	Mobile and cloud-first; on-premise if necessary
Performance	High latency using captive IDs, primarily for security	Low latency for frictionless user experience, taking account of busy hours (evenings and weekends)
Scalability	Tens or hundreds of thousands	Hundreds of thousands or millions
Velocity	LOB requirements for on-boarding	Internet speed

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
Enrolment	Triggered by employer	Initiated by consumer
Profile & Preferences	HR and employee, to a degree	LOB from CRM and consumer through self-service
Provisioning	HR-driven, defined by CIO/IT policies	Users voluntarily register through self-service
Scope	Employees and contractors	Customers/consumers; optionally employees, contractors, partners, service providers
User Experience		
User Experience Priority	Generally low priority, but gradually improving, driven by CISO	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

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 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.

David Goodman has over 25 years experience in senior identity management positions in Europe and the US. He led two prominent pioneering EC-funded identity/security projects while working for IBM, firstly with Lotus in the Notes/Domino product management team and later with Tivoli's security division. He has led several start-ups in the identity space and spent eight years in senior product management roles for telecom providers Apertio, Nokia Siemens Networks and Ericsson.

His work has included database and directory services technologies and architecture, meta-directory services, role management and role-based access controls, digital certificates and PKI. More recently he has been engaged in privacy and trust services, cloud services, big data analytics and the Internet of Things.

He has worked as a technology analyst and consulted with some of the largest companies in Europe and the US. He has particular insights in the European privacy/regulatory environment, European clients and vendors. For 13 years he was chairman of EEMA, the leading European identity and security membership association.