

# Getting To Know Your Customers: The Emergence of CIAM

## Abstract

Ten years ago identity and access management (IAM) solutions were rarely deployed beyond the company firewall, providing permissions and access rights to enterprise resources to employees and contractors. When available, the management of customer and partner access to a generally limited set of resources was often poorly coordinated. Today, however, a very different social, technology and business environment demands that enterprises make their customers' online experience as sleek and personalized as possible. And to do this, enterprises are embracing a new breed of consumer or customer identity and access management (CIAM) solutions from their IAM vendors.

The investment and commitment to CIAM are being driven by an ever-increasing sophistication of customer expectation in terms of a 'joined up' user experience and real-time availability of relevant resources accessible anywhere, anytime and from any device. Alongside the need to protect the 'disappearing perimeter' with adequate security is measured the need to address competitive advantage and maintain customer loyalty. Boosting transparency between marketing and lines of business has the potential to deepen the customer relationship.

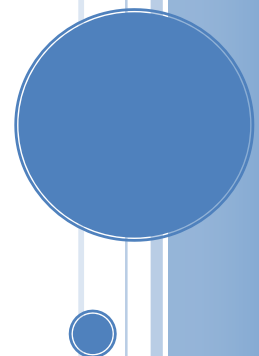
In this report, we investigate this emerging trend, what the major players are doing, and what should be the next steps for TechVision Research clients.

This report covers:

- The CIAM value proposition and business rationale for the enterprise
- Getting the balance right between enterprise IAM (EIAM) and CIAM
- TechVision Research's shortlist of CIAM vendors
- Eight steps an enterprise should take to best leverage CIAM

### Author:

David Goodman, D. Phil  
Principal Consulting Analyst  
[david@techvisionresearch.com](mailto:david@techvisionresearch.com)



## Table of Contents

Abstract.....	0
Table of Contents .....	1
Executive Summary .....	2
Introduction – Getting To Know Your Customers .....	4
Data Sources – Internal.....	6
Data Sources – External .....	7
Opportunities and Business Benefits.....	9
Know Your Customer (KYC).....	10
Marketing & Sales .....	10
Consumer/Customer Experience .....	10
Constraints & Regulations .....	11
Security.....	11
Privacy & Consent.....	11
Enterprise vs Customer IAM.....	13
Marketplace Realities.....	15
TechVision Research Vendor Shortlist.....	16
Vendor Selection Criteria .....	16
Vendor Shortlist .....	18
ForgeRock .....	20
Gigya .....	22
iWelcome .....	24
Janrain.....	25
Microsoft.....	27
Ping Identity.....	29
Corporate Readiness & Next Steps.....	31
Next Steps.....	31
Timeline .....	34
Conclusion.....	34
Glossary.....	36
About TechVision.....	37
About the Author .....	37
References .....	38
Related Reports.....	39

## Executive Summary

For most of the last 15-20 years, organizations have focussed their IAM initiatives on employees, ensuring the appropriate access and permissions are in place to carry out business securely, effectively and efficiently day-to-day. However, with the explosion in the use of the Internet for social and commercial transactions, it is not surprising that enterprises are waking up to the imperative to demonstrate a competitive user experience to their technology-savvy customers and consumers, whose expectations have been raised by their familiarity with a plethora of sophisticated, user-friendly apps on their mobile devices.

All enterprises have access to a wealth of data about their customers but in many cases either it is in disparate silos, or its potential is not being utilized effectively.

Data Types	Identity Providers	Relying Parties
<b>Personal</b>	Social media companies	Local retailers, hoteliers and travel companies; potential employers and insurance companies
<b>Financial</b>	Credit card companies (and to a lesser extent banks)	Retailers, finance companies
	Data information services (i.e. data brokers)	All enterprises
<b>Retail</b>	Retail stores	Retailers, finance companies
	Travel companies	Hotels, restaurants, rental car companies and airlines
<b>Location-based</b>	Mobile/cell phone operators	Retailers, travel companies and government agencies
	Local authorities, sensors, parking lots, garages, etc.	Most enterprises, particularly retailers and local authorities
<b>Regulatory</b>	Government agencies	Finance, airline, travel and car rental companies
	Healthcare providers	Finance companies

*Fig. 1 CIAM - relevant data types (see figure 2 below for full table)*

For competitive reasons alone, it is no longer a nice-to-have, but a business necessity to invest in providing a secure, seamless and unified customer experience across multiple channels – and the way to achieve that is through deploying the right customer IAM (CIAM) solution. The immediate benefits to the customer are to reduce friction through multiple login options and increase and improve engagement through self-service and progressive profiling. This leads to greater transaction satisfaction and the likelihood of brand loyalty along with the development of a mid- to long-term relationship. From the organization's

perspective, the upfront investment in CIAM offers faster time to market, a reduction in administrative overhead and ultimately an ongoing increase in revenue. The opportunities to get to know customers better are provided not only by cataloging preferences from their engagement history and self-provisioning but also by leveraging external sources of data, such as those available from social media. However, this has the potential to be a mixed blessing: on the one hand, it could provide highly personalized responses and service, but it may also be considered an intrusion of privacy with questions about appropriate use of data if consent is not requested. The new and upcoming privacy regulations across multiple geographical jurisdictions, each nuanced slightly differently, are a challenge for both organizations and their IDaaS providers with stiff penalties incurred for any mishandling of personal data.

Next, a decision has to be made on the appropriate technical approach. This requires achieving consensus amongst internal stakeholders, led by sales and marketing from the customer-facing LOBs, working with IT to understand the parameters of what is and is not possible, and finally reaching out to a representative group of external stakeholders. Despite the temptation and attraction of going with a home-grown solution, particularly if there is one already in place, TechVision Research's strong recommendation is to choose from among the numerous vendors offering purpose-built CIAM solutions.

This report separates the marketplace into specialist, federated or hybrid and extended enterprise IAM (EIAM) [1]. It is important to be mindful that there are significant differences in approach and functionality between CIAM and EIAM that may outweigh the decision for an organization to simply stay with their EIAM vendor. Even though it may make sense, unless the vendor is not yet able to fully respond to an organization's CIAM aspirations, it could lead to eventual frustration and dissatisfaction. As with other recent reports, TechVision Research provides a shortlist of vendors we would tell our clients about today if we were asked who to start with in the CIAM space. For further help with your CIAM strategy and the eight steps from start to rollout, TechVision Research offers strategic and practical support through its consulting services.

## Introduction – Getting To Know Your Customers

For more than ten years, vendors and system integrators have been working assiduously to develop and improve all aspects of their customers' internal identity management systems, deploying ever more sophisticated forms of access governance and provisioning. More recently, the advent of cloud-based identity or identity as a service (IDaaS) platforms has opened up a new set of opportunities for most, if not yet all, enterprise identity and access management (EIAM) vendors. It's not surprising then that attention has turned to providing the same degree of IAM functionality beyond an organizations' perimeter by extending the traditional on-premise service.

Every organization already has access to a wealth of material relating to its external stakeholders, whether they be consumers, customers or partners. Typically most of that information is stored in distinct database silos, 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. Added to which, the new, much stricter data protection and privacy regulations coming into force across multiple geographical domains carry with them the threat of heavy fines and penalties in cases where there is evidence that personal identity data is not being adequately managed or maintained. In other words, holding large volumes of poorly managed customer data is not only an administrative headache, but it is also becoming a significant potential liability to businesses and their brands.

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.

Context-based identity and identity relationship management are core elements supporting the next big evolution in both EIAM and CIAM as was highlighted in TechVision Research's *Putting Identity into Context*. The privacy constraints associated with the use of contextual data apply to CIAM just as they do to EIAM, except of course on a much larger scale. Also, there is a considerably greater degree of care required to get the appropriate level and degree of consent from customers for the use of their personal data than there is for employees. Not least the aims of a CIAM strategy are quite

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.

distinct from those of an EIAM: an EIAM continues to be focused on access and security whereas a CIAM is primarily about developing and deepening the organization's relationship with its customers. If it's not apparent today, the lessons learned from fully functional CIAM solutions – those that go beyond vendors simply mimicking EIAM – will ultimately impact the approach enterprises expect their vendors to take towards EIAM. Either way, understanding and managing the relationships defined by identity contexts is the ultimate goal of IAM. It also represents another aspect of the digital transformation of businesses alongside other macro trends such as the disappearing enterprise perimeter, the proliferation of data and business analytics, the cloudification of IT, as well as the drive to find new opportunities to understand and connect with customers.

IAM is a fundamental building block of internal or external communication, collaboration or commerce. The management of identities is also a critical part of how organizations directly interact with consumers and trading partners, using the distribution of identity data to leverage most substantive applications and processes. So, despite the continuing improvements of role or rule-based enterprise IAM solutions, the benefits of decision making supported by understanding relationships in context will be appreciated not only by IT administrators but across all departments.

The many drivers for the coming changes include the proliferation of CRM information, increasing security concerns, the geometric explosion of IoT data being generated, as well as the ubiquity of social media platforms and businesses that are built on information sharing. Also, the amount and richness of information stored at scale in the cloud are so much greater than that of any single organization. However, unlike with most EIAM systems in which its usefulness is limited, the information stored in these massive data sources can be more easily integrated with other profile data in CIAM and be used to build a rich and powerful set of applications.

The widespread use of smart devices and the availability of inexpensive broadband has led to an explosion in online commercial and social transactions. This has, in turn, produced an exponential growth in the volume and diversity of data captured, stored and analyzed, both in real time and otherwise, aided by virtually unlimited and historically cheap cloud storage. This data has created a treasure trove of highly personalized user behavioral information and the resulting insights — from online shopping habits to social media interactions — are becoming a vital asset in providing secure access to confidential data, particularly financial data.

With well-established public dependency on the Internet as well as a deepening awareness of digital security, for the consumer or end-customer, the application of profiling, particularly with the added dimension of self-service and social media feeds, will offer either a welcome higher degree of personalized service or an unwanted degree of intrusiveness. In other words, the potential business advantages and consumer convenience have to be weighed against the privacy concerns. Identity is always multi-faceted and involves many relationships that need to be considered, depending on the problem space and the solution. Most people have many aspects to their lives and may want to keep these relationships segregated in some cases or aggregated in others, depending on the circumstance and the perceived benefit. [2]

The basic rationale for undertaking a thorough CIAM strategy is that the expectations of all external stakeholders, whether contractors, partners or consumers/customers, have gone up dramatically, regarding the user experience as well as access to relevant resources. Their familiarity with apps on mobile devices has trained them to understand that easy to use, low-friction interfaces are their inalienable right. So the silos have to go, but most organizations need to start with an inventory of available data sources. Get ready to start planning!

The basic rationale for undertaking a thorough CIAM strategy is that the expectations of all external stakeholders, ... have gone up dramatically, regarding the user experience as well as access to relevant resources.

## Data Sources – Internal

Every organization maintains some form of record or database relating to customers and consumers as well as partners:

- A **customer** relationship management (CRM) system that manages and analyzes interactions and commercial transactions with customers and potential customers to streamline processes, improve business relationships and ultimately drive sales. Similarly, an enterprise will have database systems to hold information about **partners**, depending on whether they are suppliers, service providers, contractors or sales channels that are designed to manage and retain the relationship by tracking transactions and other forms of interactions.
- A database that maintains **consumer** profiles, often supported by loyalty cards and the offer of a self-service portal to allow users to manage their preferences

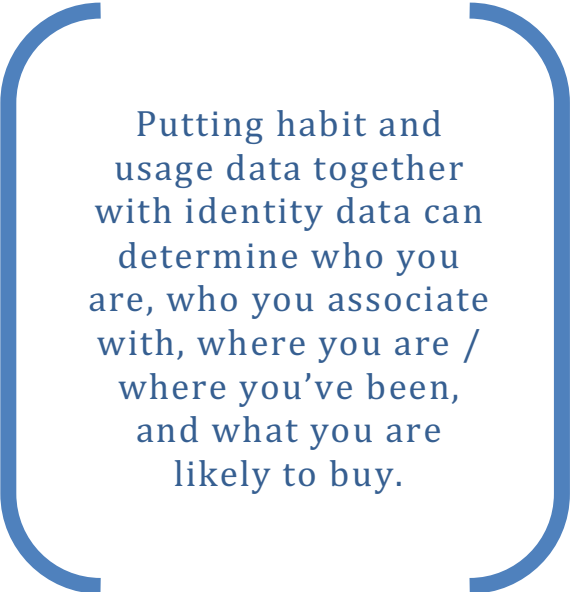


and take advantage of deals. While this gives customers a sense of ownership, most businesses already have at their disposal the wherewithal to understand their customers, based on previous buying habits. Those companies that actively propagate real-time information to returning customers, such as Amazon, do so to great effect. There is no reason why this experience cannot be extended beyond online shopping to the physical world of retail outlets, restaurants, and travel.

## Data Sources – External

As explained in *Putting Identity Into Context*, certain types of commercial enterprises, such as banks, social media, and retailers, collect relatively unregulated commercial data. This data can be mined directly (e.g., social media), acquired (e.g., retailers sell catalog subscription lists and purchasing history) or used for their purposes (e.g., banks and retailers have access to their pools of data). Other more heavily regulated sources of data, such as governmental records, certain types of geo-locational records unrelated to phones, phone records, and medical records, can augment the commercial data.

Besides the basic aspects of identity data, there are several categories of data based on habitual behavior patterns such as social, retail, travel as well as device usage. Putting habit and usage data together with identity data can determine who you are, who you associate with, where you are / where you've been, and what you are likely to buy. One of the primary goals of commercial marketing is to determine who you are, your friends and habits and to predict what you're going to want to do next and figure out how to offer it to you at a compelling price point.



Putting habit and  
usage data together  
with identity data can  
determine who you  
are, who you associate  
with, where you are /  
where you've been,  
and what you are  
likely to buy.

For an enterprise seeking to understand more about either an employee or an external stakeholder, there are external sources of identity-related information that provide the raw data for a contextualized environment.



Identity Providers	Relying Parties	Current	CIAM Usage Recommended
<b>Personal</b>			
<b>Social media companies</b>	Local retailers, hoteliers and travel companies; potential employers and insurance companies	Controversially invite their users to openly publish a daily catalogue of their thoughts, ideas, social habits and social networks, which can easily be analyzed for business purposes. For example, a person shows that they regularly travel to the same resort in Switzerland to enjoy downhill skiing.	This information will be of interest to promote competitive offers, but it will also be of interest to potential employers and insurance companies who may be concerned about a person's regular participation in a dangerous sport. Ensure your use of personal data conforms with your privacy policy and regulatory requirements such as the EU's GDPR.
<b>Financial</b>			
<b>Credit card companies (and to a lesser extent banks)</b>	Retailers, finance companies	Hold very unambiguous profiles of the time, location and type of purchasing habits of businesses and individuals and provide the clearest picture of daily activities of each as well as the overall health of their finances.	Could be a determining factor in partnering with a company, hiring someone or being sensitive to debt-related or repayment issues.
<b>Data information services (i.e. data brokers)</b>	All enterprises	Routinely perform credit checks on individuals and businesses.	Enterprises regular monitoring of partners, suppliers and consumers.
<b>Retail</b>			
<b>Retail stores</b>	Retailers, finance companies	In-store and online transaction histories combined with loyalty cards allow retailers to accumulate a wealth of information about consumer purchasing and preferences.	Provide opportunities for targeted selling and marketing campaigns.
<b>Travel companies</b>	Hotels, restaurants, rental car companies and airlines	Regularly trawl online bookings and loyalty card profiles to understand consumer travel habits and preferences.	All travel companies are able to promote desirable locations at attractive price points.
<b>Location-based</b>			
<b>Mobile/cell phone operators</b>	Retailers, travel companies and government agencies	Not only know how many phone calls and text messages subscribers have made as well as how much data they have consumed, they also have an extremely granular map of their subscribers' movements anytime, anywhere and in some cases on any device.	Highly valuable to know customers/consumers/citizens immediate locations or regular journeys that can be used for real-time decision making or targeted marketing.
<b>Local authorities, sensors, parking lots, garages etc</b>	Most enterprises, particularly retailers and local authorities	CCTV is deployed in Europe and the US in public places for surveillance purposes as a national security and law-enforcement measure as well as for traffic monitoring purposes. It is also used for protecting private and commercial premises.	Another form of location-based data with photo ID. It can be used for tracking the movement of people and 'things' – not least when they are apparently lost.
<b>Regulatory</b>			
<b>Government agencies</b>	Finance, airline, travel and car rental companies	Have direct access to formal datasets such as required for passports, identity cards, drivers' licences as well as a record of tax returns, as well as, depending on a country's attitude to information gathering and sharing, indirect access to considerably more.	Potential to considerably augment consumer identity profiles.
<b>Healthcare providers</b>	Finance companies	Maintain patient medical records which offer confidential information.	If disclosed could influence decisions relating to, for example, applications for finance or insurance premiums.

*Fig. 2 Identity Providers, Relying Parties and potential CIAM Applications*

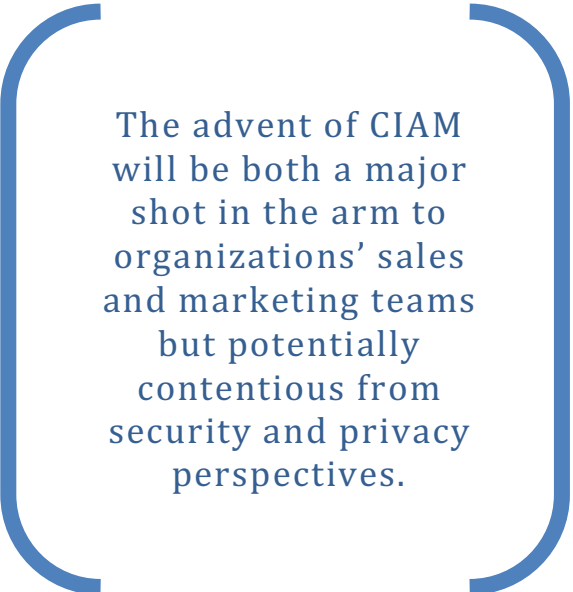
Any of the above data sources have the potential to become even more useful when federated. Depending on which jurisdiction the enterprise is based in, there are further sources of data that might be available and used for identity validation purposes. For example, based on social equality principles, in Scandinavia – Norway, Sweden, and Finland – the income and tax details of everyone, from ordinary citizens to celebrities, CEOs, and politicians, are published every year and are accessible by anyone. Compare that with the situation in the United States where, with the exception of isolated examples, such a government policy would be considered a massive betrayal of trust.

The examples above highlight the potential and impact of Internet-enabled ‘things’ that will generate a gargantuan volume of data to be analyzed and managed. Although not all of this data will be linkable to individuals, a lot may be attributable to a person’s behavior patterns and preferences. As such an enterprise IoT strategy which collects data *inter alia* from connected products the consumer has bought – a camera, a cooker, or any device with sensors – has a role to play in achieving the aims of the identity aspects of any digital transformation project.

### Opportunities and Business Benefits

The advent of CIAM will be both a major shot in the arm to organizations’ sales and marketing teams but potentially contentious from security and privacy perspectives.

It would be very easy for an organization to view CIAM as ‘simply’ an extension of their existing EIAM or CRM systems – or both. At one level, CIAM provides a similar degree of access to company resources as EIAM does. However, CIAM affords greater autonomy to customers than EIAM does for employees to manage their profiles and preferences with the promise of developing a long term relationship. It should be apparent that the same considerations should be – and in some cases are being – applied to employees in next-generation IAM systems based on contextual identity or identity relationship management.



The advent of CIAM  
will be both a major  
shot in the arm to  
organizations’ sales  
and marketing teams  
but potentially  
contentious from  
security and privacy  
perspectives.

As discussed in *Putting Identity into Context*, there are at least three potential dimensions to getting to know your customers better:

- **Consumer/Customer Validation:** To verify identities in compliance with KYC (Know Your Customer) requirements, particularly in the financial sector

- **Marketing & Sales:** To market and sell to customers better by using big data and advanced analytics to process the wealth of data available either openly or through acquisition
- **Consumer/Customer Experience:** To improve both online and real world user or customer experience by understanding and, where possible, anticipating patterns of behavior as well as general and context-based preferences

### Know Your Customer (KYC)

Originally defined in the 2001 Patriot Act, KYC requires businesses to check out who its 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 bona fide; in other words, 'real,' not on any transactional blacklist, and of low risk. One of the key drivers for a CIAM system is to be able to spot anomalous or suspicious behavior, not only at the beginning of a trading relationship but on an ongoing basis.

### Marketing & Sales

In the retail industry, all businesses and organizations benefit from knowing more about their customers or clients from a non-regulatory perspective. Most major organizations appreciate that establishing the right data relationship with customers is a key factor in sustaining a competitive edge. Behavior patterns are discernible from a variety of different input sources, such as purchasing preferences, location-based information, social media feeds, and stored general identity profiling. In fact, many businesses are either deploying some form of context-based identity management or have access to the required building blocks today to improve targeted marketing and sales promotions and initiatives. Knowing what factors are going to enhance customer confidence and trust will determine whether a brand reputation is strengthened rather than compromised. However, some of the most valuable sources of marketing and sales data come from self-described interests and usage. When someone identifies themselves online, they voluntarily give up a certain amount of data before participating in a loyalty program or even before making their first purchase.

### Consumer/Customer Experience

As an extension of the above, enterprises can cement customer loyalty by taking the opportunity to streamline and personalize users' online experience on a retail site. Or in the physical world, through a combination of secure, specialized big data analysis, similar to the above, with location-based smartphone triggers, recognizing and welcoming customers when they enter a store either to remember their buying preferences or to steer them towards profile-relevant deals or promotions.

The challenge in all three cases is to balance the availability of the opportunity with regulations concerning security, privacy and data protection.

## Constraints & Regulations

### Security

Introducing a CIAM system brings with it a new set of challenges required to balance meeting the usability expectations of customers and maintaining a high degree of security. Increasingly, the use of username and password, along with the unloved CAPTCHA challenge-response test, is giving way to the use of social network logins, federation with mostly Facebook, Twitter or LinkedIn, or biometric, generally fingerprint, authentication. Today users are accustomed to a frictionless registration process at retail sites and will show a reasonable degree of intolerance if engagement does not match other regular experience. With EIAM, traditionally employees were bound with what they were presented with and, for better or worse, had to learn to live with it, although this scenario is clearly evolving. By contrast, customers and consumers have a legally-enshrined right to complain, change their minds or simply go elsewhere to obtain what they want.

Introducing a CIAM system brings with it a new set of challenges required to balance meeting the usability expectations of customers and maintaining a high degree of security.

### Privacy & Consent

While the benefits and opportunities of the extension of IAM systems to incorporate context and relationships are extensive, there is the danger of a gradual encroachment on the dividing line between what customers and consumers are comfortable being known about them and what strays into areas of discomfort.

Alongside citizens' overwhelming social and economic dependency on the Internet has come the sobering awareness of the potentially negative or even dangerous implications of personal data falling into the wrong hands. Consequently, unsolicited profiling, particularly real-time, location or context-based, which in an ideal world would be understood as providing a highly tuned quality of service, could nevertheless be seen as highly intrusive, particularly if it merges different aspects of a person's life without due consent.

In Europe, the EU's introduction of a substantial revision to the way that it administers and regulates data protection on behalf of European citizens – General Data Protection Regulation (GDPR) – is coming into force in May 2018. Already the potential ramifications

of these changes have been felt by some of the major US technology vendors – see the recent TechVision Research report by David Goodman, “New European Privacy and Data Protection Regulations” for more detail. In particular, non-European companies will be held responsible and accountable for personal data held about European citizens. The consequences of non-compliance are severe financial penalties that can be levied by the supervisory bodies in EU Member States.

In addition, and to make matters slightly more complicated, there is new data protection and privacy legislation coming into force in other jurisdictions. For example, over the last three years, Russia has announced regulatory steps to protect its citizens’ personal data, not least a data localization law that requires personal data of Russians to stay in Russia [3]. Unsurprisingly, what is now law in Russia has similarities with GDPR but is sufficiently different to merit cautious attention. Similarly, while there may be a move away from the industry-led approach to data protection prevalent in the United States to a more federal model, compliance still will have a different flavor to that in Europe and Russia. As a result, it will be increasingly difficult for a multinational to manage adequate compliance with the various regulatory bodies, particularly if the CIAM is managed on-premise. But it is also the case if it turns out that the company’s preferred cloud service provider uses data centers outside any of the above domains. Consider customers moving from one domain to another – their opt-ins and preferences would have to be adjusted accordingly, and in some cases, their whole profile would have to be moved. The clearest resolution to what has the potential to be a daily nightmare scenario is for organizations with a portfolio of international customers, or other external stakeholders, is to establish multiple international data centers to ensure compliance.

It will be increasingly difficult for a multinational to manage adequate compliance with the various regulatory bodies, particularly if the CIAM is managed on-premise.

To achieve compliance with data protection legislation in any jurisdiction, and at the same time achieve an acceptable level of business agility, separate views on a user’s identity are not feasible: it is vital to have a unified, single view of a customer’s identity profile, opt-ins or consents, and preferences. To bring about this coherent picture, decisions, particularly those associated with regulatory compliance, but potentially others too, require stringent business rules that need to be captured, modeled and codified in systems. Juggling the constraints imposed by one jurisdiction over another places higher demands on the modeling than in most other system rollouts and may have more than GRC ramifications.



## Enterprise vs Customer IAM

Building a customer-oriented identity management system demands a significant shift in the way vendors and their clients approach the management and use of identity profiles, of not only customers and consumers, but potentially also contractors, partners, third party service providers – and even employees. 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 permissions as their design goal. As discussed in *Putting Identity into Context*, this premise which has been valid for many years is becoming outdated due to the rapidly changing nature of the relationship between the enterprise and the Internet and the boundaries between them. As TechVision Research has stated previously, the next generation of EIAM systems will stretch beyond the enterprise to the Internet, becoming borderless rather than defined by the enterprise perimeter.

Customer or consumer IAM is driven by an organization's desire to get more insight into its customers and to plant the seeds for long-term 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 B2E IAM solutions, which focus on managing employees and, in some cases partners and a new breed of B2C IAM products 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.

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.

Characteristic	Enterprise IAM	Customer/Consumer IAM
<b>Business</b>		
Purpose	Encouragement of good corporate behavior and stewardship of the enterprise mission	A closer relationship with the consumer leading to product consumption and brand loyalty
Drivers	Originally, security risk and cost reduction, on boarding efficiency; increasingly enterprise culture and employee loyalty creation	Acquisition, engagement, recommendation & retention; revenue-driven
Intelligence	Static, rules-driven intelligence; but changing with increased use of context-based identity	Dynamic, real-time, analytics-based
<b>Governance, Risk and Compliance</b>		
Access Management	Protection of information key to the enterprise	Consumers' purchased rights
Access Governance	High priority	Low priority
Policies & Permissions	LOB and CIO/IT	LOB and CIO/IT as well as customer/consumer
Privacy Compliance	Centralized policy-driven	Policy-driven as well as customer-driven and opt-in/opt-out
<b>Architecture</b>		
Adaptability	Integration with back-end systems	Dynamic schema required to support managing consent, opt-ins and preferences
Agility	Monolithic and predictable	Modular and adaptable
Architecture	SOAP	REST
Extent	Perimeter-based, enterprise-defined; but evolving to perimeter-less	Borderless, internet-scale
Network	On-premises as well as BYOD/BYOI/BYON	Cloud and on-premises
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
<b>Data</b>		
Data	Predefined by IT, stored in directories and relational databases	Derived from many sources, often using unstructured data requiring dynamic schema
Enrollment	Triggered by employer	Initiated by consumer
Profile & Preferences	HR and employee, to a degree	LOB from CRM and consumer through self-service
Provisioning	SPML, defined by CIO/IT policies	SCIM; users voluntarily register through self-service
Scope	Employees and possibly contractors	Customers/consumers; optionally employees, contractors, partners, service providers
<b>User Experience</b>		
Priority	Generally low priority, but gradually improving, driven by HR	Unified user experience is high priority, further enhanced by self-service
Personalization	Limited but changing	Considered a differentiator and a benefit by both enterprise and consumer

*Fig. 3 Enterprise Vs. Consumer IAM*



### Marketplace Realities

Most, if not all, EIAM and CRM vendors are aware of the growing demand for CIAM and the changing dynamics that impact the efficacy of their existing product sets. Some have already made strategic moves to extend their existing EIAM solutions to provide for the very different expectations of external stakeholders as well as the LOBs that support them.

Nevertheless, most vendors' changes in their product strategy are incremental, adding new functionality on top of old rather than taking a significant new direction. As such, the current marketplace is split between vendors specifically addressing internal IAM requirements and those who have focused on offering customer-facing solutions, although eventually, the differences will go away. The good news is that, if they haven't already done so, all have plans to host their next generation platforms in the cloud or, in some cases, on-premise as well, allowing the IAM system to be extended beyond the enterprise while still being able to integrate existing systems and data sources.

The market for identity management solutions that organizations should be considering can be roughly divided into three categories:

- **Specialist:** a small group of vendors who specialize in providing 'pure play' CIAM solutions which are not based on existing EIAM. Some vendors also offer EIAM solutions in particular cases, although at the moment this tends to be the exception rather than the rule.
- **Federation or Hybrid:** vendors who use federation to consolidate their approach to EIAM and CIAM without sacrificing the distinctive requirements of the one over the other. Most but not all of these vendors started with a customer/consumer focus and used federation or other technologies to cover the whole gamut of employee to consumer IAM.
- **Extended IAM:** a larger group of vendors who have adapted their existing EIAM technologies with some modifications to offer CIAM. IDaaS providers are well placed to extend their EIAM offerings for consumers with only relatively few additions or modifications, although it is reasonable to expect some vendors to strive to provide clearer delineations between EIAM and CIAM functionality in the future.

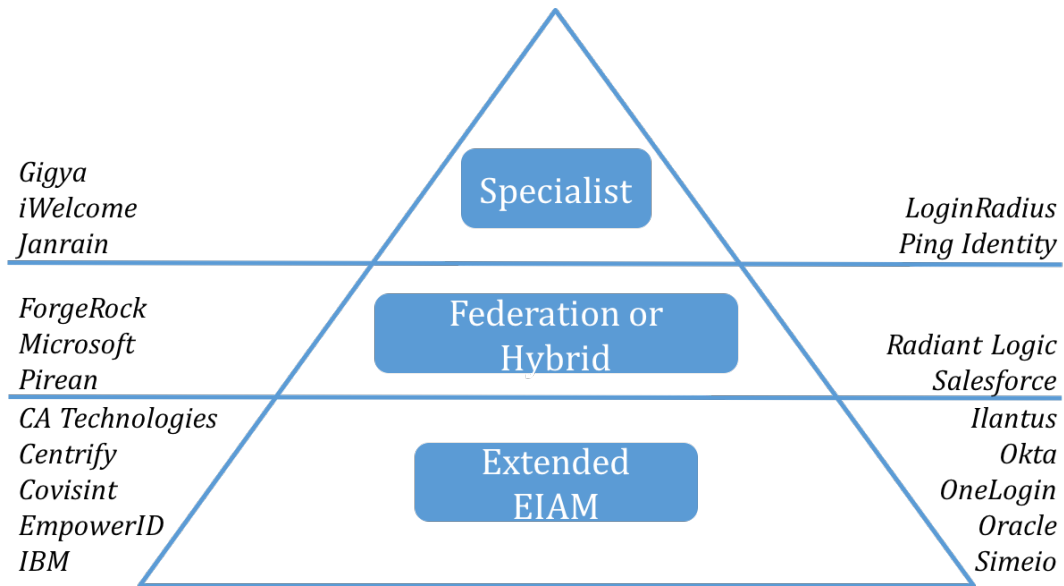


Fig. 4 Three levels of CIAM offerings

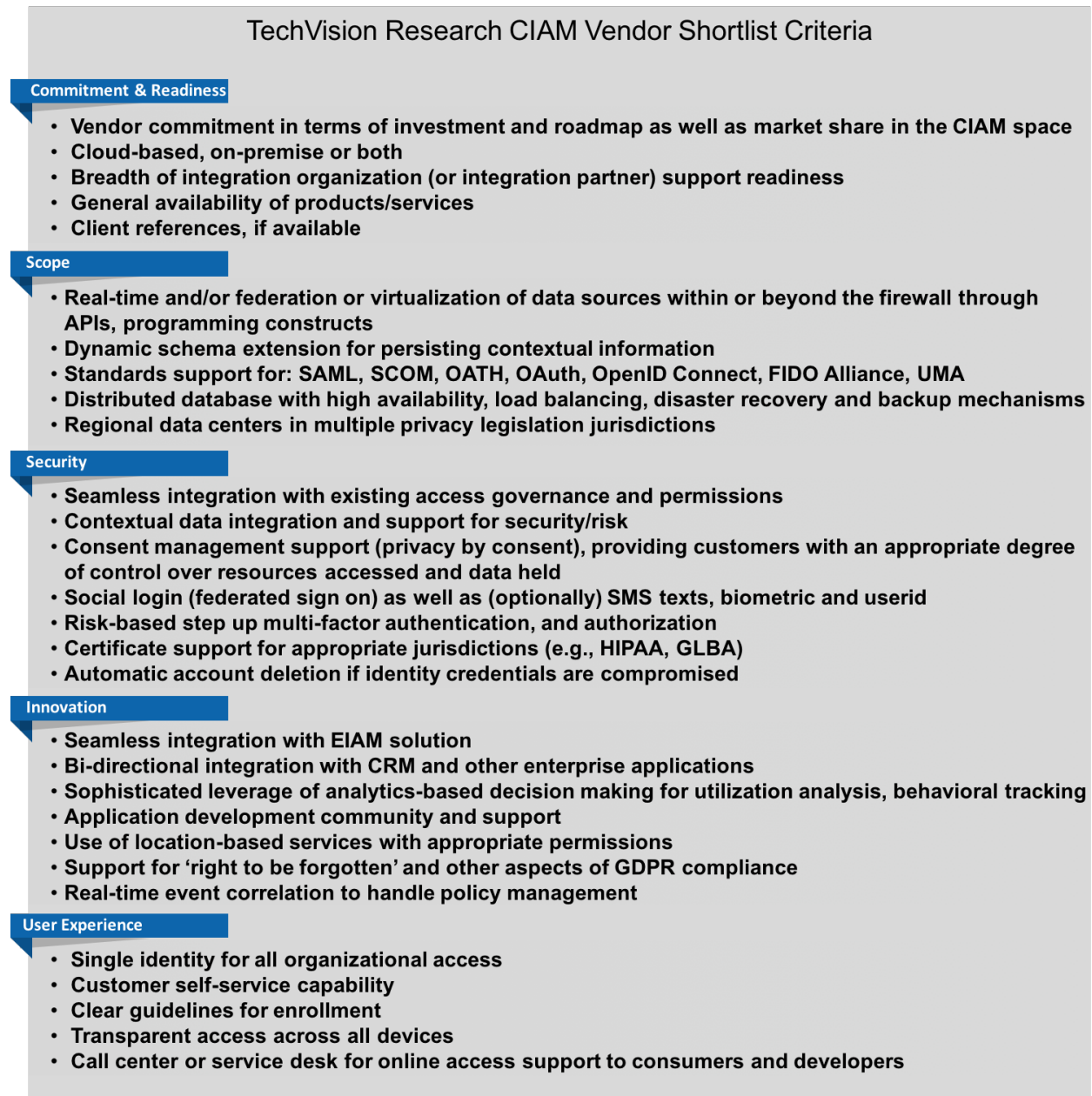
## TechVision Research Vendor Shortlist

### Vendor Selection Criteria

Although organizations and vendors have been looking at Customer IAM for several years, the market for specialist solutions is not yet mature and the CIAM landscape is still dominated by Enterprise IAM vendors either partnering (IBM, SailPoint) or offering cloud-based solutions that are not fundamentally different from their EIAM offerings. It is questionable how effectively these solutions can offer the level of user experience expected as well as handle customer profiles and access requests. On the other hand, from an administrative perspective, being able to manage both EIAM and CIAM with the same interface is clearly an attractive proposition.

Another approach would be to build an in-house solution or to extend a home-grown partial solution. While this may initially appear to be the most attractive way forward and one that requires the least initial capital outlay, it is TechVision Research's opinion that it is fraught with risk and would eventually become a logistical and commercial liability. Amongst the potential pitfalls going forward would be achieving the right levels of access and security, managing data protection and passwords, supporting API standards and keeping up with demands for increases in speed and scale as the system grows.

Below is the TechVision Research recommended checklist based on our observations in the marketplace from both vendors and user organizations. As this is a specific area of focus within the identity management market, it doesn't necessarily mean that the vendors selected on our shortlist are the best overall identity management providers, but it does mean that these are the vendors that we believe have strong offerings specific to consumer-oriented identity services.



*Fig. 5 Vendor Selection Criteria*

### Vendor Shortlist

The list of vendors providing IAM and CIAM solutions and services today is considerable. As this is an emerging market, traditional EIAM vendors are already offering cloud-based services with probably the majority evaluating requirements and making design decisions for CIAM. The vendors in this space represent a range of different approaches to many of the same problems associated with protecting physical and data assets, both within a firewall as well as in the cloud, for employees or customers.

Bearing in mind that this is a specific area of focus within the identity management market, the list below is a representative but certainly not exhaustive sample of companies that TechVision Research believes have strong offerings specific to consumer identity services. This doesn't necessarily mean that the vendors selected on our shortlist are the best overall identity management providers or the only vendors to consider in the CIAM space. Think of this shortlist as representing the vendors TechVision Research would tell our consulting clients today if we were asked who to start with in evaluating CIAM vendors.

### TechVision Research CIAM Vendor Shortlist

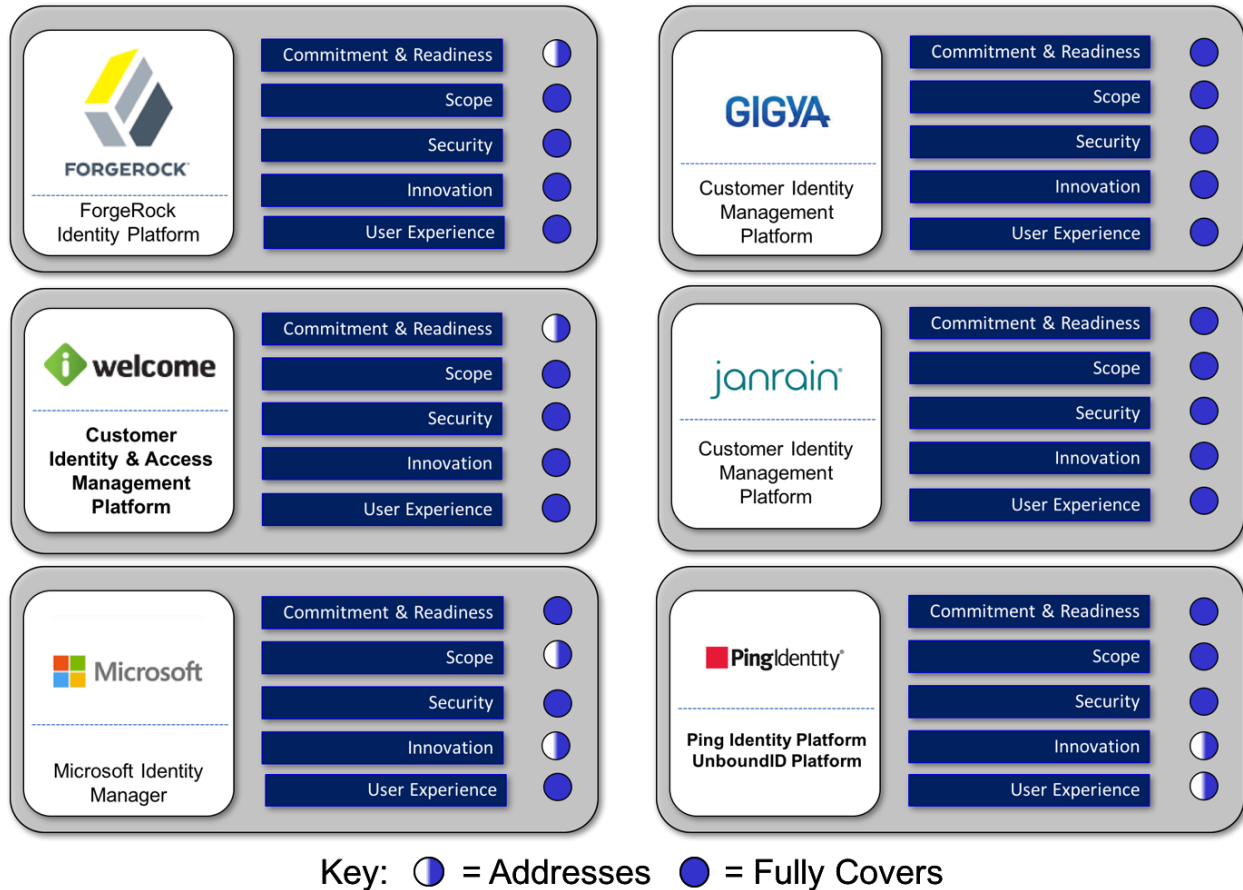


Fig. 6 TechVision Research CIAM Vendor Shortlist

In characterizing how and why vendors are on this shortlist, our primary considerations were how information is integrated (connectors, synchronization, meta-directories, virtualization), how effectively contextual information is used, the sophistication of the relationships that are being managed and the accessibility of information to users.

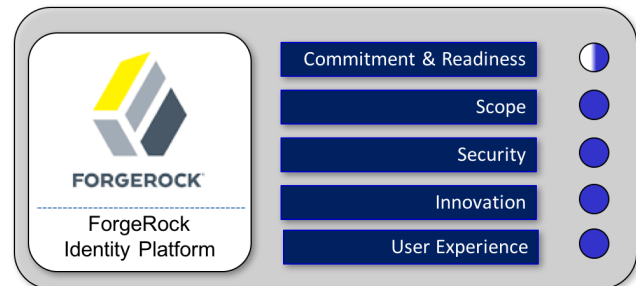
**Gigya** and **Janrain** were advantaged in having developed products specifically with CIAM in mind. Likewise, **Ping Identity** who would have been candidates for inclusion anyway recently acquired UnboundID, who for some time had focused on CIAM. **Microsoft**, whose Azure cloud service is used by most enterprises, is included because of the depth of its supporting product portfolio and its extensive customer base and support services. **ForgeRock**'s claim is to having focused a holistic identity relationship management strategy across the whole enterprise ecosystem from employees to customers to devices. Although **iWelcome** primarily only serves the European market, the company has focused on developing a CIAM solution with broad and diverse functionality.

At this point, the TechVision Research shortlist comprises the following six CIAM vendors. We'll provide a brief background on each vendor and a brief description of their solution.

## ForgeRock

### Background

Although the company was founded in 2010, its product base is considerably more mature as most of the founders came from Sun Microsystems. Headquartered in San Francisco with ten offices worldwide and over 350 employees, ForgeRock has over 450 customers in more than 30 countries.



### Shortlist Rationale

The ForgeRock Identity Platform consists of a series of modules built from open source projects, and is an identity administration and provisioning solution focused on managing relationships. The company achieves this by building dynamic, context-based relationship management systems that span consumers, partners, customers, employees, and devices, generating millions of relationships. This will eventually become billions when the identities associated with 'things' in the IoT create new relationships and integrate with existing ones.

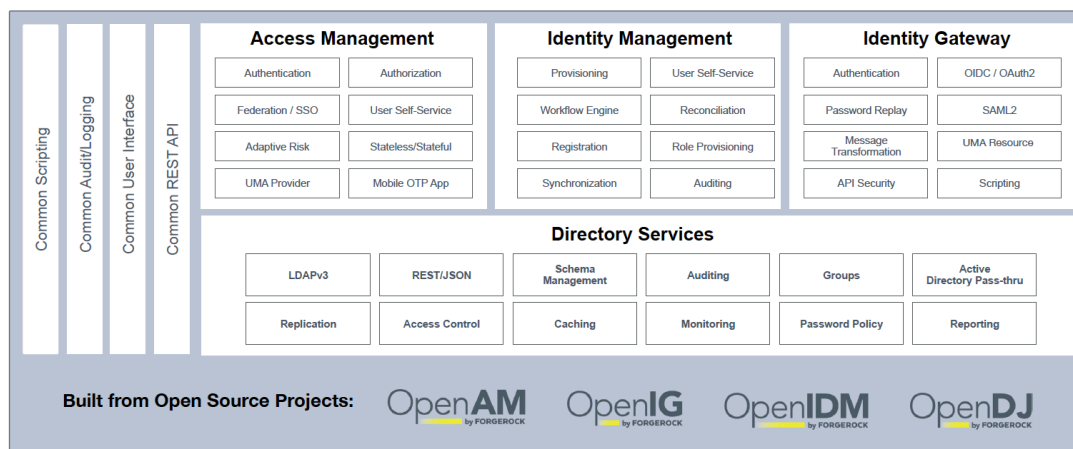
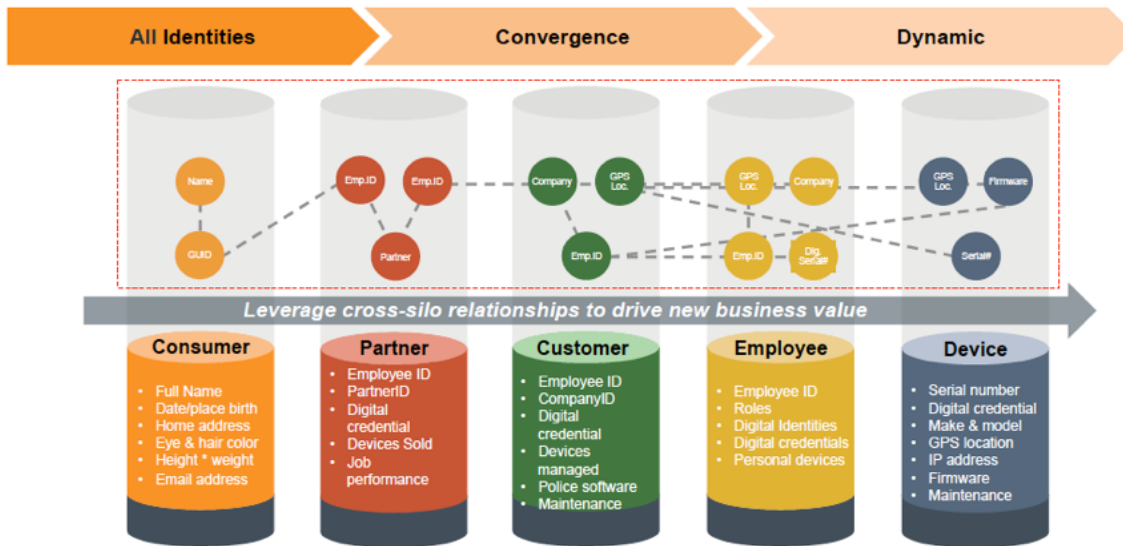


Fig. 7 The ForgeRock Identity Platform





*Fig. 8 ForgeRock's approach to architecting the relationship layer*

ForgeRock is one of the leaders in driving the development and uptake of UMA (User-Managed Access) and IRM (identity relationship management) which they use to integrate additional consent-driven, privacy-based concepts into their relationship management offerings. The company emphasizes the synergies between context, control, choice and respect in applying UMA to deliver privacy as well as the importance of moving from XAML and LDAP to graph databases to get fine-grained context-based dynamic access control.

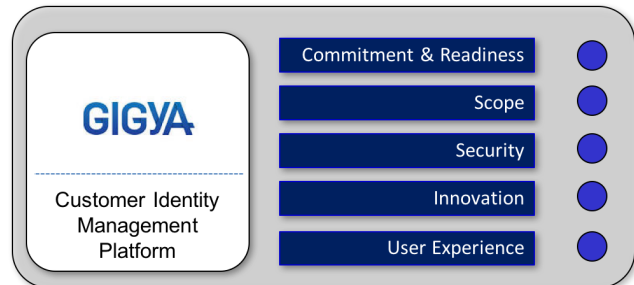
As such ForgeRock provides a holistic IAM solution for all types of identities across the whole enterprise and beyond on a single unified platform. Their approach to privacy and consent ticks the appropriate boxes regarding compliance with GDPR and other data protection regulations. Unlike other vendors in this space, ForgeRock is not an IDaaS provider.



## Gigya

### Background

Founded in 2006 in Tel Aviv, Gigya is today headquartered in Mountain View, California with seven offices worldwide. Gigya has over 325 employees and more than 700 enterprise customers in 46 countries deploying the company's Customer Identity Management Suite.



### Shortlist Rationale

The company's founders saw the potential to link business sites on the Internet with the rapid growth of social networking, in terms of combining data from both to provide better and more accurate data to the benefit of businesses and their customers. Gigya started in business as a SaaS provider and saw the opportunity to popularize the use of social logins. From there the company went on to design the current, subscription-based IDaaS service with the complex requirements of managing consumer identity profiles including unstructured social and mobile data, across multiple devices and platforms, with privacy and security in mind.

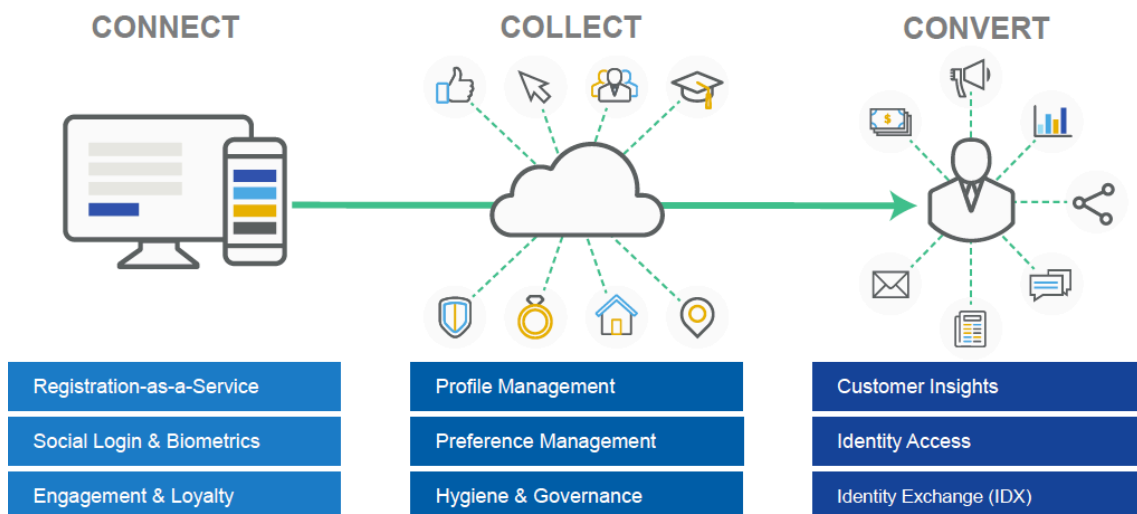


Fig. 9 Gigya's Customer Identity Management Platform

Gigya provides risk-based and multi-factor authentication with an out-of-band (email or mobile) option, support for SAML 2.0, and federated authentication for partners using OpenID Connect. The company offers a dynamic schema directory service and provides tools for end-users to input and manage their interests and preferences that Gigya's

customers can then, with user consent, collect, aggregate and analyze to provide a bigger picture of their consumers and thereby develop a deeper relationship with them. Gigya's social media analytics tools enable customers to visualize and cross segment their users' demographics, interests, social behavior, influence and revenue-generating activity. In addition, Gigya facilitates customer services' platforms to be adapted and customized to take account of information synched with social media and preferences data to improve and personalize consumers' real-time interaction.

The company's CIAM offering is based on a purpose-built home-grown database that caters for both structured and unstructured data and has the capacity to support 100 million identities.

Gigya has four data centers worldwide with a fifth coming soon to address regional privacy compliance regulations. The company also partners with IBM.

## Gigya Platform Overview

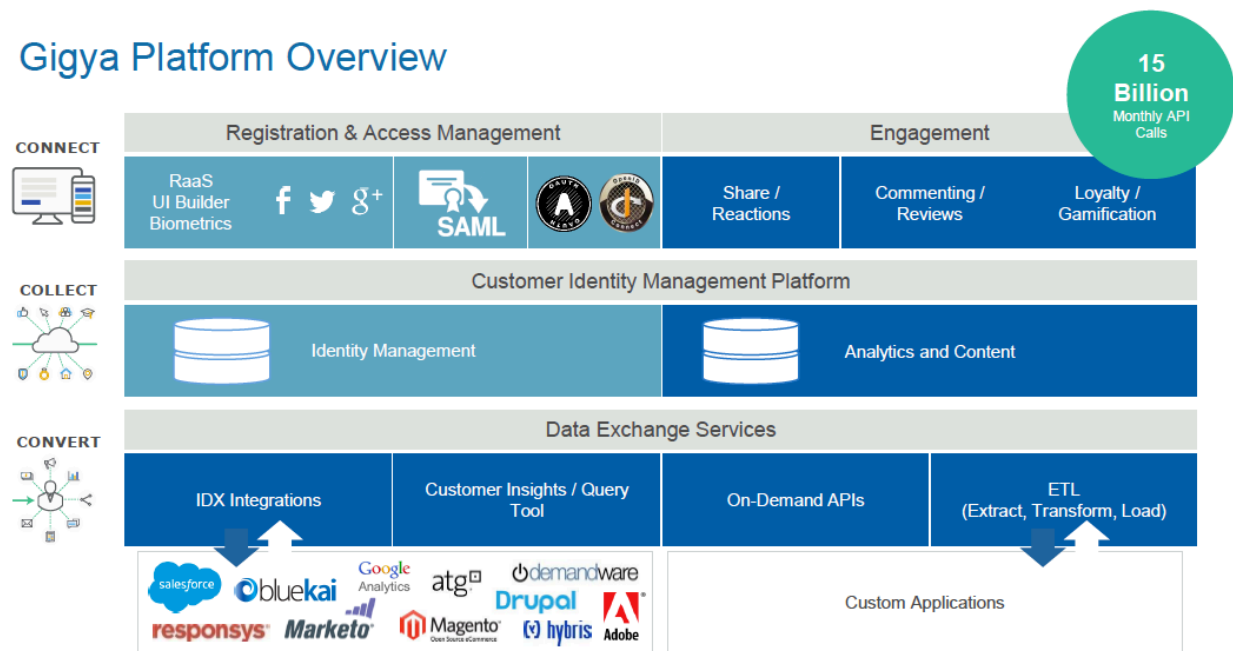
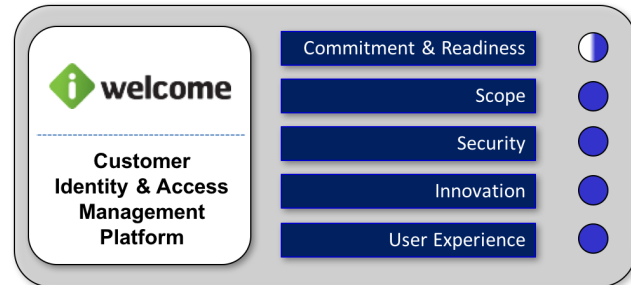


Fig. 10 Gigya Platform Overview

## iWelcome

### Background

iWelcome is an IDaaS provider, based in Amersfoort, The Netherlands, and is the only European-based company on the shortlist with access to 13 data centers in nine different European countries. iWelcome has 65 employees and at present its customer base is in Europe.



### Shortlist Rationale

iWelcome is unusual in that, having started as an IDaaS and invested in providing a comprehensive CIAM solution, they later extended the functionality, but with a different approach, to deal with the requirements of EIAM. Hence, customers are able to benefit from a single platform that supports both forms of IAM together.

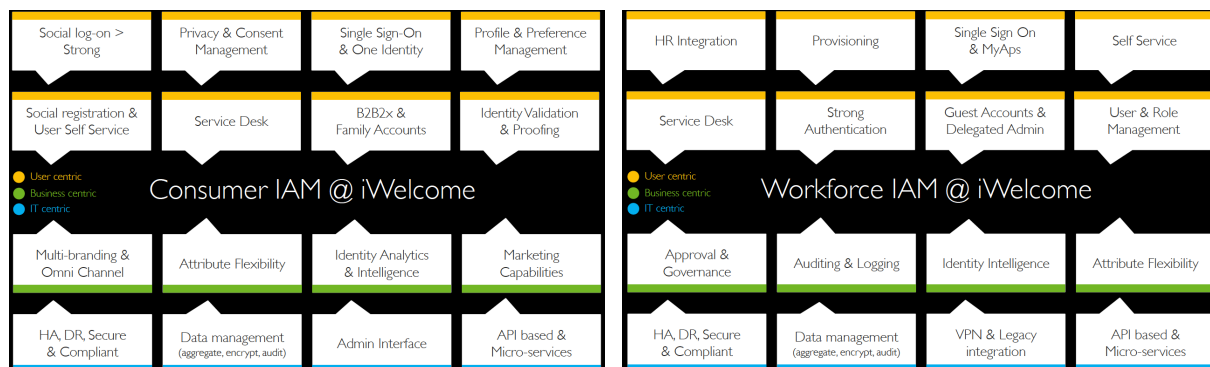


Fig. 11 A direct comparison of iWelcome's Consumer and Workforce IAM functionality

The iWelcome platform uses the open source OpenAM and OpenDJ (originally from ForgeRock), Apache Syncope for identity management services, Elastic, Logstash and Kibana for reporting, ConnId for its identity connector framework and Interoute as its IaaS. Its functional architecture is delivered through micro-services which provide continuous delivery and agility enabling quick response times to new opportunities. iWelcome is focused on enterprise rather than mid-size companies and is strictly a private cloud service, i.e., it does not offer multi-tenancy, based on the company's understanding that businesses are extremely sensitive about flexibility and security.

Being European in its outlook, iWelcome recognizes the importance of incorporating GDPR compliance parameters into its product. This in part is achieved by creating, for every attribute, metadata containing details of consent stored in an instance of MongoDB [4].

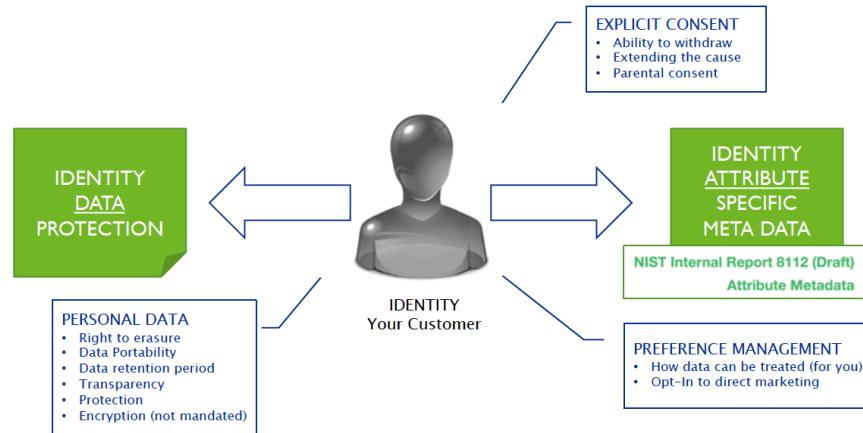


Fig. 12 The customer identity as the central point

## Janrain

### Background

Janrain is based in Portland, Oregon where it started in 2002 and has offices in Redwood City, London, and Paris. The company has 120 employees and has 1500 clients across multiple verticals in 65 countries. Janrain's technology is a customer profile management solution and evolved from the first social login product which came in 2009 with CIAM arriving a year or two later.



### Shortlist Rationale

The Janrain Customer Identity Management Platform is based on the Janrain Identity Cloud and started from the simple premise that the proliferation of username and passwords on the web was becoming untenable. This in turn led to the company pioneering the use of social logins. Janrain's CIAM platform provides organizations with a unified view of their customers across all devices by collecting accurate customer profile data as an aid to personalized marketing. The platform includes social login, registration, customer profile data storage, customer segments, customer insights, single sign-on, and engagement.

In addition to an extensive application development community of over 50,000 installs, Janrain has partnered with AWS since 2006 and uses Amazon's RDS (relational database

service) as its backend database. The company also OEMs its technology to Google, IBM, Twitter and Salesforce to manage authentication processes.

Janrain uses six data centers across the world to provide latency as well as local regulation compliance, with five more coming on stream in 1Q 2017 to align with AWS.

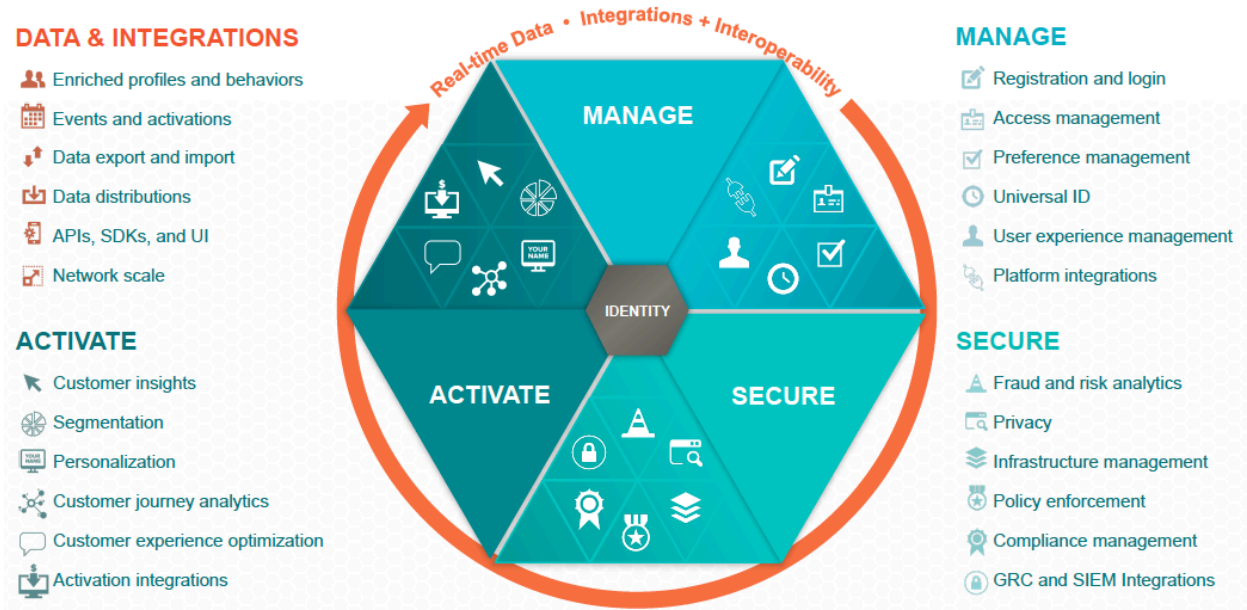


Fig. 13 Janrain Identity Overview

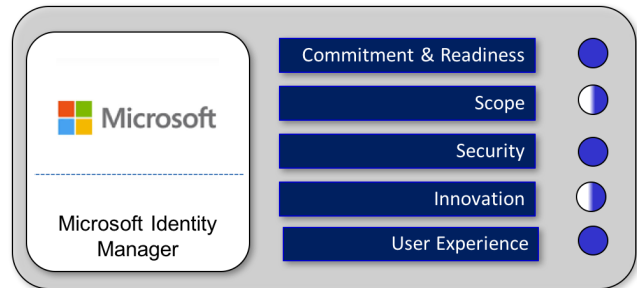


Fig. 14 Janrain solution overview

## Microsoft

### Background

Microsoft was founded in 1975 and is worth approximately \$85 billion with about 114,000 employees worldwide and millions of customers across all verticals in most countries of the world. Microsoft has been a leader in enterprise directory services with Active Directory and has extended this platform to its Azure cloud service, which has 600 million users and 1.3 billion enterprise and 13 billion authentication sign-ins daily.



### Shortlist Rationale

Microsoft's CIAM, also referred to as Azure Active Directory (AAD) B2C, is driven by its new Identity Execution Engine (IEE), an open, third-party identity development platform that allows customers to model and build their cloud-based trust frameworks. The IEE has been designed to cover the requirements of B2B, B2E as well as IoT and allows applications to exist in a multi-IdP environment as a multi-purpose claims exchange. The multi-platform extensible policy framework includes integrating third party identity or attribute providers and directories as well as support for OpenID Connect, OAuth 1.0 and 2.0, SAML 2.0 and WS-Federation. Identities are created and deleted in one or more external systems such as on-premises AD or HR systems. The identities are then synchronized into the cloud using

AAD Connect or Microsoft Identity Manager – and continue to remain in sync. Alternatively, identities can be provisioned externally and integrated with third-party governance systems.

Azure AD B2C Basic is a pay-as-you-go consumption-based service.

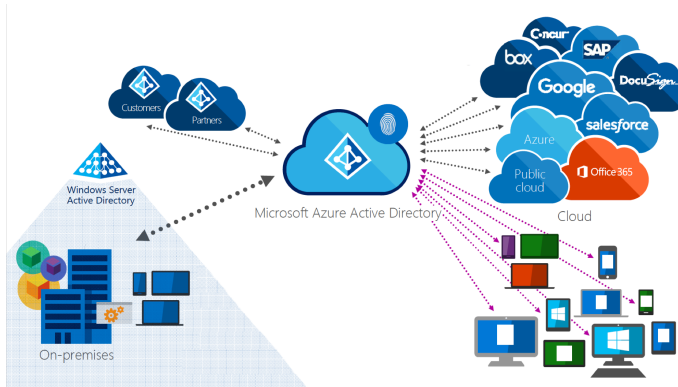


Fig. 15 Microsoft Azure Active Directory

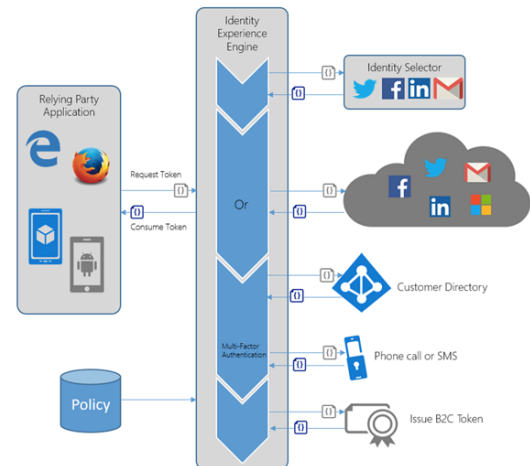


Fig. 16 Identity Experience Engine

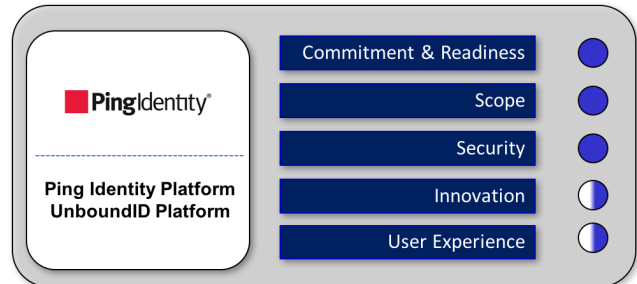
The acquisition of LinkedIn that closed in December 2016 opens up new opportunities for Microsoft's customer-facing strategy going forward. According to Microsoft EVP Cloud and Enterprise, Scott Guthrie, talking about LinkedIn, *"The insight you get from a sales reps' or customer service reps' inbox with Exchange and what we have in Office 365, the insight you get from someone's calendar, and even with Skype all of their phone and voice communications and IM traffic, you take all that together and have a cloud that can do deep insight and analytics and machine learning and AI on top of that. You create the ultimate selling tool, the ultimate customer support tool in the industry because you have so much insight that can assist a sales rep or assist a customer service rep that no one other vendor can provide."* [5]



## Ping Identity

### Background

Founded in 2002, Ping Identity has its headquarters in Denver, offices in Boston, San Francisco, Halifax, Vancouver, London and Israel with sales outlets in EMEA and APAC, has over 350 employees and more than 1,500 customers, 300 partners and 12 system integrators worldwide.



Ping Identity was recently acquired for \$600 million by a private equity firm, Vista Equity Partners, which appears to be investing substantially in the company, not least with the acquisition of UnboundID the following month.

### Shortlist Rationale

Ping Identity had already been in the CIAM market for several years when in July 2016 they acquired, for an undisclosed amount, Austin-based UnboundID, a vendor whose portfolio included a market-leading CIAM solution. According to Andre Durand, Ping Identity CEO, *"Delivering a personalized and consistent customer experience across all channels is core to many digital transformation initiatives."* The company's stated aim in making the purchase was *"to help enterprises improve customer engagement"* and *"to accelerate digital enterprise transformation initiatives and improve how companies acquire, engage, manage and retain customers across all channels and devices."* [6]

Prior to the acquisition, the Ping Identity Platform supported multi-factor authentication, single sign-on and secure access – essentially those capabilities available for Ping Identity's EIAM solution. These have been augmented in the combined offering to include UnboundID's scalable customer data management layer (designed to be telco strength), multiple authentication methods, including social login, SMS texts, biometrics and others as well as its customer preference, privacy, and profile management functionality. The Ping Identity CIAM has support for most open standards as well as security certification for HIPAA, FERC/NER, GLBS, PCI-DSS, and others.

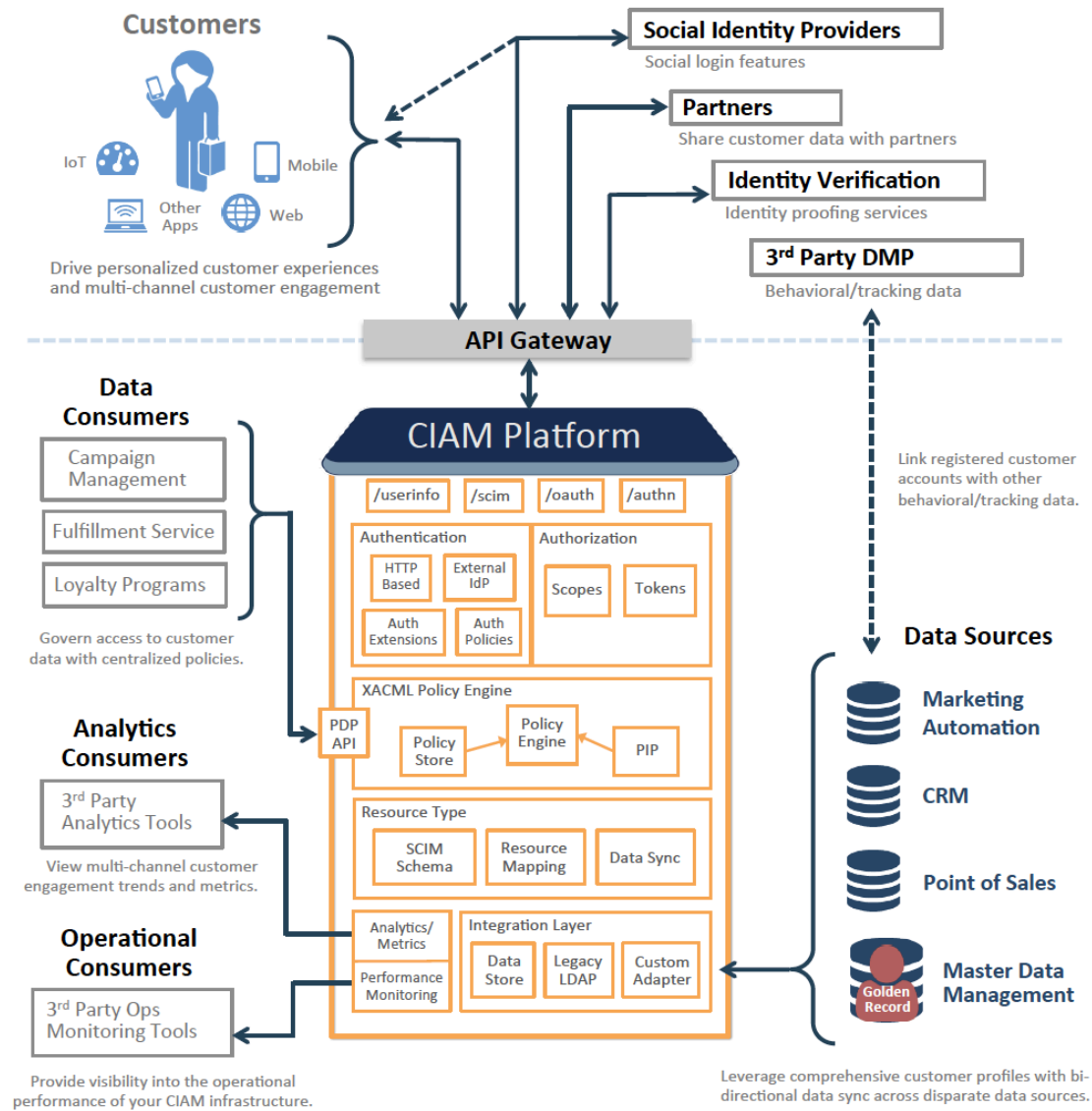


Fig. 17 Ping Identity's UnboundID CIAM Reference Architecture

## Corporate Readiness & Next Steps

It would be surprising if organizations were not excited about the possibilities of developing a sustained relationship with their customers and retaining their loyalty as well as improving secure access to data assets. Their challenge is matching that ambition with the reality of their existing infrastructure and what is available from their preferred vendors over the coming two-three years. Whatever the limitations of such solutions, a vendor-bought solution is infinitely preferable to relying on a home-grown solution, even if ultimately, that decision is likely to be predicated on either price or time to deployment.

The other factors which play into making the decision to move ahead are scope and priority. Much depends on whether enhancing customer visibility is considered a higher priority than improving access security. Equally important is whether a linkage between internal and external stakeholders is a job that can wait.

## Next Steps

There are eight steps that can be taken now to align your business with what we believe should be the future direction of your approach to customer identity and access management. Note that these steps and timeframes will vary based on the size and complexity of your organization, legacy systems and the overall state of your identity management and data infrastructure.

Step	Action	Responsible	Elapsed Time
1	Business Case Strategy	LOB	3-6 months
2	Consultation	LOB/CIO/CISO/CPO	3-4 months
3	System Review	LOB/CIO	3-4 months
4	Design	LOB/CIO	3-4 months
5	Technology Choices	CIO/LOB	3-4 months
6	Education & Awareness	LOB/Customers	4-6 months
7	Rollout	CIO	6-9 months
8	Awareness	LOB	9-12 months

*Fig. 18 Eight step process to CIAM*

### STEP 1: BUSINESS CASE STRATEGY

The first step is to build a business case with sales and marketing to transform the organization's relationship with its customers by, on the one hand, allowing them access to sensitive data and other resources while at the same time opening up a channel for greater familiarization. The discussion should address scope, determine priorities, outline budget availability and desired timelines with a set of outputs resulting in a clear, high-level strategy that addresses all the external-facing demands and expectations.

## STEP 2: CONSULTATION

The next stage is to take your findings to a wider internal group of stakeholders who include:

- The CIO to get an understanding of the potential infrastructure implications of the CIAM strategy on increased network usage and requirements for hardware and software
- The CISO to assess potential areas of security concerns from data breaches and cyber-attacks.
- The CPO or data protection officer to ensure that what is planned is aligned with privacy legislation, either national or international (such as GDPR if any EU citizens are involved).
- External stakeholders should also be consulted about the proposed new system's features and associated benefits, including the provision of the right to manage at least some of their personal data through a self-service center. A collaborative approach, leveraging external perspectives and experience, has the potential for mutually beneficial outcomes rather than making partners or consumers aware after the fact that data about them is being collected, analyzed and used.

It should be assumed that the various policies that have been put in place should be reviewed at least every three months.

## STEP 3: SYSTEM REVIEW

Review your CRM systems and other customer data repositories to determine if they provide the level of CIAM required to improve the experience clients and users are having of your online and real world portals. The chances are that your current CRM will not offer either the performance or all the up to the minute detail required to deliver optimal customer experience. It should also be apparent that CIAM systems have very different design goals compared with those of internal IAM solutions. Notably, these are:

- **Usability:** a key value and return for companies' investments is to attract new customers and maintain loyalty by offering ease of use, convenience, and enhanced security
- **Customer Experience:** to dramatically improve customer experience by being able to personalize their preferences through self-service portals which would also provide control over privacy and data sharing settings
- **Scalability:** to perform at a vastly different scale to accommodate millions of persons and 'things' and to demonstrate real-time response times, especially at times of usage spikes or surges during peak periods

CIAM is gaining traction in the market with vendors making moves to consolidate their product portfolios.

#### STEP 4: DESIGN

Whatever the compromises reached between the consensus group in Step 2, the first task of the CIAM system design is to identify the identity profiles required to address the applications to be offered to customers and ensure that it aligns with the existing CRM system, but also anticipating future expansion. In addition, it will improve the usability and acceptance of the project if the system allows social logins – using Facebook, Twitter or LinkedIn – for basic access to back-end systems.

It is essential that identity structures are universal across the CIAM system but at the same time provide enough scope for different stakeholder LOBs to make their own choices. The system should also give customers the opportunity to update some aspects of their profile and add new information through a self-service portal that will then require some degree of post-validation on the submitted data, either against a fixed set of criteria or in real-time using context-based analytics.

It is also important to plan for a seamless multi-channel (or omnichannel) customer experience as well as to build in support for application developers and to allow sufficient time for the integration of key applications prior to rollout.

#### STEP 5: TECHNOLOGY CHOICES

The choice of vendor for the new CIAM software will generally be predicated on the recommendation of your preferred or existing EIAM vendor. Not all EIAM companies offer a CIAM solution, but may partner with a pure play CIAM vendor with whom there is no perceived competitive conflict.

It's most likely that the new CIAM software will be cloud-based. The better solutions will also provide integration with EIAM and access to on-premises enterprise applications such as Office365 and CRM systems.

#### STEP 6: EDUCATION

Just as the new system is being rolled out, it is important to update the internal stakeholders of the progress of the project, especially the customer support team, aligned with what was discussed in Step 2. Particularly for the sales and marketing teams, it is crucial that the details of what is going to be offered to customers are made as clear as possible so that news of the initiative is communicated positively and effectively. As part of the same exercise, the LOB is responsible for ensuring that the key messages get across to customers and any other external stakeholders during the course of the rollout.

#### STEP 7: ROLLOUT

Once everyone is on board with the logistical developments and the decision to proceed with the CIAM system is made, the actual rollout will take between six to nine months. Given the very nature of CIAM solutions, this estimate is contingent on the scope of the project as well as on the level and tenor of feedback obtained from external stakeholders.

In the case of very large deployments, fully on-boarding all consumers could well take longer.

#### STEP 8: AWARENESS

Once the new system is in place and the button to go 'live' has been pushed, it is vital to the long term success of the initiative to keep your customers engaged – without overwhelming them – over an extended period after the system is up and running.

#### Timeline

TechVision's Principal Consulting Analyst team has worked with literally hundreds of Global 2000 organizations helping to develop their strategies, architecture, vendor selection, deployment planning and lifecycle management. The following timeline and our recommendations draw on this perspective. From start to finish, it is realistic to estimate an elapsed period of *at least* ten months to begin a production roll out and between 15-24 months to accomplish all the steps prior to the longer term awareness activity.

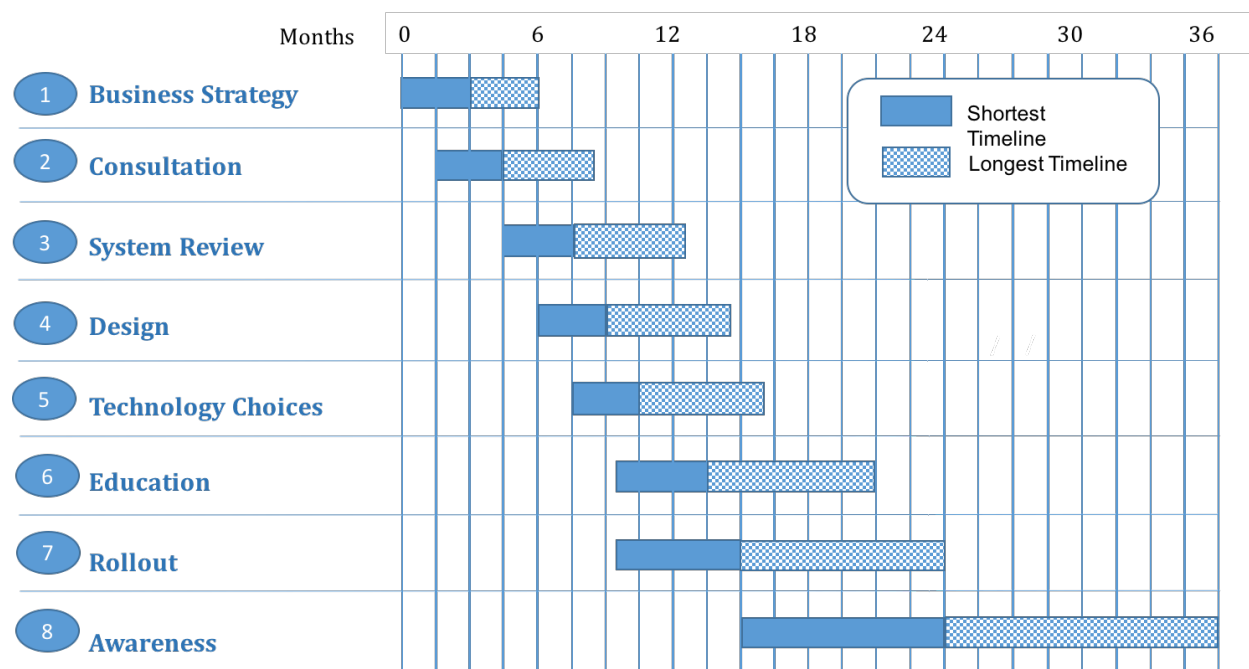


Fig. 19 Eight step timeline

#### Conclusion

It is apparent that most organizations, whether commercial or otherwise, are recognizing the need to store, analyze, manage and present their customers' data in a more sophisticated and user-friendly way than they would perhaps have thought have doing five-ten years ago. The gradual transition from on-premises facilities to the cloud has

opened up a world of possibilities, as is apparent from the number of EIAM vendors who are extending the reach of their solutions.

However, it should be apparent from this report, that the purpose and the drivers behind building a CIAM are very different from those informing the strategies for an EIAM. The one is driven by the business need for enterprises to better understand their customers and/or consumers by building a relationship that can be developed and enhanced over time with the purpose, simply put, of selling more products. Whereas the other is largely predicated on the requirement to allow employees, and in some cases contractors and partners, an appropriate level of access to the data assets required – no more and no less – for them to make their expected level of contribution to the smooth operation of the business on a daily basis.

Not surprisingly, there are – or at least there should be – considerable differences of approach in the design and execution of CIAMs and EIAMs, with a far greater emphasis placed on meeting and satisfying consumer's real-time expectations. Although it is a little trite to point out that customers can pick and choose who they buy from based on a single online experience whereas employees realistically have little or no choice however often they use their employer's EIAM system, the argument holds some grains of truth. What is fascinating to observe is that with the gradual disappearance of the enterprise perimeter due to the emergence of cloud services and BYOD/BYOI/BYON, the differences between CIAM and EIAM are contracting. More and more IDaaS vendors – but not all – are offering credible IAM services for the enterprise *and* the consumer, although the level of functionality in no way matches that of the CIAM specialists. It is also apparent that the experience of catering for the application of IAM for consumers is already having a positive effect on EIAM solutions, a trend which is likely to continue.

For enterprises contemplating on embarking on a CIAM initiative, however basic an extended EIAM solution may appear, it is still a better investment of time and resource than attempting to develop a home-grown solution. As attractive and tempting as it might be to custom-build a CIAM specifically to the unique requirements of your enterprise, it is highly unlikely to be as responsive or 'future proof' to new standards and interfaces as those of vendors who make it their business to keep up with industry trends and changes.

Not that many years ago having a dedicated CIAM system would have appeared like an expensive nice-to-have; today it is a business necessity. With careful planning and appropriate levels of support from both internal and external stakeholders, you'll be very pleasantly surprised at the benefits you'll reap from the results. TechVision Research is well-positioned to provide assistance in making such a project work, and we would be delighted to hear from you.



## Glossary

AAD	Azure Active Directory
AD	Active Directory
AWS	Amazon Web Services
B2B	Business-to-Business
B2C	Business-to-Customer
B2E	Business-to-Employee
BYOD	Bring Your Own Device
BYOI	Bring Your Own Identity
BYON	Bring Your Own Network
CIAM	Customer Identity and Access Management
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CRM	Customer Relationship Management
EIAM	Enterprise Identity and Access Management
EU	European Union
FERC	Federal Energy Research Commission
GDPR	General Data Protection Regulation
GLBA	Graham-Leach-Bliley Act
GRC	Governance, Risk and Compliance
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IDaaS	Identity as a Service
IdP	Identity Provider
IEE	Identity Execution Engine
KYC	Know Your Customer
LDAP	Lightweight Directory Access Protocol
LOB	Line of Business
REST	Representational State Transfer
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SOAP	Simple Object Access Protocol
SPML	Service Provisioning Markup Language
SQL	Structured Query Language

## 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 it. 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 when they carry out a product and strategy review and assessment, a requirement analysis, a target market assessment, a technology trend analysis, a go-to-market plan assessment, or a gap analysis.

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

## About the Author

David has over 25 years of experience in senior identity management positions in Europe and the US. He led two prominent pioneering EC-funded projects then worked for IBM, firstly with Lotus and later Tivoli. 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. He has worked as a technology analyst and consulted with some of the largest companies in Europe and the US. He has broad insights across the European privacy/regulatory environment, European clients and vendors. David is currently based in Scotland.



## References

- [1] The acronym used throughout this report for traditional IAM is EIAM, which can be understood as enterprise or employee IAM. The same concept may also be found referred to as 'workforce IAM'. Likewise, CIAM can represent either customer or consumer IAM. To add to the potential confusion, the Identity Management Institute uses CIAM to refer to a Certified Identity and Access Manager - <http://www.identitymanagementinstitute.org/ciam/>
- [2] Going forward the new initiatives that are seeking to provide a blockchain-based IAM infrastructure or eco-system share the same vision. ... *eliminating the need for a centralized identity data repository, self-sovereign user created and managed identities can be realized affording the owner complete control over how their identities are distributed and the extent of personal content that is made public.* TechVision Research's Blockchain-based Identity Management, Doug Simmons and Gary Rowe, October 2016, p.27 and *passim*.
- [3] On January 13, 2016, the Russian Data Protection Authority (*Roscommandzor*) released its plan for audits this year to assess compliance with Russia's data localization law, which became effective on September 1, 2015. The localization law requires companies to store the personal data of Russians in databases located in Russia. The audit plan indicates that the *Roscommandzor* will audit large, multinational companies doing business in numerous jurisdictions and processing the personal data of Russian citizens. Source: <https://www.huntonprivacyblog.com/2016/01/28/russian-data-protection-authority-releases-2016-audit-plan-for-localization-law/>
- [4] This is based on NIST Internal Report 8112 (Draft): Attribute Metadata, Paul A. Grassi, Ellen M. Nadeau, Applied CyberSecurity Division, Information Technology Laboratory and Ryan J. Galluzzo, Abhiraj T. Dinh, Deloitte & Touche LLP, July 2016
- [5] Source: <https://www.microsoft.com/en-us/Investor/events/FY-2017/Deutsche-Bank-Technology-Conference-09132016?EventID=175256>
- [6] Press Release, August 2, 2016, "Ping Identity Acquires UnboundID to Deliver the Leading Customer Identity and Access Management Solution". Source: <http://www.businesswire.com/news/home/20160802005781/en/Ping-Identity-Acquires-UnboundID-Deliver-Leading-Customer>

## Related Reports

The following reports might be helpful in your continued exploration of this domain:

### **Reports that explore Identity and Access Management:**

- [1] Putting Identity into Context – Next Generation IAM, by David Goodman.
- [2] The Future of Identity Management, by Gary Rowe, Doug Simmons, David Goodman, and Bill Bonney.
- [3] Blockchain-based Identity Management, by Doug Simmons and Gary Rowe.

### **Reports that explore data, its categorization, management, technical handling, and use:**

- [4] Fixing the Fundamentals: The Business Blueprint, by Noreen Kendle.
- [5] IoT as a Security Risk Amplifier and Mitigation Strategies, by Bill Bonney and Scott David.

### **Also by David Goodman**

- [6] New European Privacy and Data Protection Regulations – Compliance or Consequences, by David Goodman.
- [7] Opportunities in Europe with Electronic Identification and Trust Services, by David Goodman.