The Guide to Trusted Digital Relationships with Customer Identity and Access Management (CIAM)

Table of Contents

Introduction

Identity is a fundamental requirement to digital growth. Businesses and organizations cannot properly take advantage of mobile, cloud, or internet of things (IoT) technologies without a scalable and repeatable digital identity strategy. Without it, they have no way to identify, engage, and build meaningful relationships with their customers— whether it be through a laptop, mobile phone, tablet, connected car, healthcare wearable, connected home device or the next great connected innovation. This guide is designed to explain the fundamentals of digital identity and how it helps you build relationships with your customers.

What is Identity Access Management (IAM)?

In its simplest form, identity and access management is the creation and administration of users, devices, and things and the rules that govern what they can do online. It answers the questions: Who (or what) are you? What can you (or it) do online?

Sounds simple, but the number of applications, devices and things involved in making these types of decisions are often quite complex. It requires taking every application and externalizing the IAM capabilities in order to centrally manage users as well as things and their sign-on and authorization policies. For some enterprises, this may comprise hundreds or thousands of digital identity-enabled apps interacting online.

What is Customer Identity Access Management (CIAM)?

As businesses transition to a digital ecosystem where their goods and services are available online and via devices, companies and governments alike are realizing that the ability to manage the digital identities of every customer, every prospect, and every citizen is fundamental to their success.

Legacy IAM was based on monolithic platforms that used static rules to make decisions. It was not designed to easily integrate with any application, to provide device-agnostic access, to handle large scale populations, or to make decisions based on consumer context. In short, traditional IAM cannot meet today's business demands.

To connect customers and citizens to relevant goods and services in the digital age, and to build trusted digital relationships with their users, businesses and governments instead require customer identity and access management (CIAM).

CIAM delivers the following capabilities:

- Eliminates departmental business silos with a common identity model company-wide
- Develops a single customer profile for each end-user
- Focuses on speed and repeatable processes
- Builds trust digital relationships with users, devices, and things
- Device-agnostic
- Context-aware
- Designed to handle internet-scale volume from hundreds of millions to billions of identities

CIAM is built for flexibility, scale, and the internet of things. It can interact with healthcare wearables, connected cars, set-top boxes, e-citizen portals, home security systems, medical devices, and whatever 'yet-to-be-invented' "thing" customers will be using in the years ahead.

At its core, CIAM uses identity to break down organizational silos and create a single, company-wide view of the customer or citizen. It uses data to build detailed individual profiles that help businesses and governments engage with their customers and citizens effectively. Understanding who these customers and citizens are empowers businesses and governments to provide improved services and more relevant goods, making for loyal customers and satisfied citizens. Businesses have the opportunity to build new revenue-driving initiatives that capitalize on this new customer data.

Key Takeaway

The evolution from identity and access management to customer-focused identity management has a name: customer identity and access management (CIAM). CIAM is equipped with unique capabilities that differ from traditional identity management requirements.

How is CIAM Strategic to Your Organization?

CIAM allows businesses to rapidly identity-enable new cloud, mobile, and IoT services in order to offer a richer, seamless customer experience across applications, devices, and internet-connected 'things.' It does this by:

- Using identity to get to know your customer. CIAM uses real-time context to create a single overview of the customer in order to offer personalized services based on real buying habits. CIAM builds lasting relationships with customers--and more importantly, trust.
- Implementing a common identity platform companywide, in order to share valuable data across the entire organization. Customer data and information is no longer siloed in different business units, but transparent across lines of business. Business units can then respond more quickly, more consistently, and more collaboratively to changing customer needs.
- Taking advantage of its modular, scalable, and flexible architecture, which facilitates repeatable business processes, accommodates millions of concurrent users and devices, and reduces typical deployment times versus legacy vendors. This allows businesses to realize revenue gains and strategic goals faster than competitors.

Businesses that can quickly establish an engaging customer experience at any time, from any place, device, or thing, will satisfy their current customers and rapidly attract new ones. These businesses will set the bar for customer engagement, and any competitor that hasn't begun implementing CIAM will not be able to provide a comparable customer experience. Those businesses will struggle to retain a loyal customer base—and they will have no chance to play catch up.

Key Takeaway

You cannot take advantage of the cloud, mobility, IoT or any other digital initiative without identity. You need to create, manage, and protect every user in order to engage with them. Therefore, identity is a fundamental requirement for a successful digital transformation.

How Does CIAM Accelerate Time-To-Market?

Because CIAM is designed as a customer-facing driver of business value, these platforms must cater to speed and developer ease-of-use to match the pace of customer demands.

Traditionally, IAM systems were built by piecing together acquisitions, making for unwieldy "product suites" that were overly complex with redundant and incompatible capabilities. These products were notorious for taking years to deploy and integrate, and failure was not an uncommon result. Niche IAM players created streamlined solutions to address specific problems, but without any overarching identity solution, companies still had no way to quickly and easily deploy and utilize identity.

CIAM requires a unified identity model. The core tenant of CIAM is that identity should be exposed in a single, repeatable way that makes it easy to roll out new services. The goal behind this principle is to provide new services quickly, taking years down to months, and months down to weeks.

Key Takeaway

It's essential to have a common identity platform with a single API for developers to implement identity services at scale. It must offer repeatable processes that are easy for developers to consume, ensuring reliability, train-ability, and agility.

How does CIAM provide stronger security?

Over a billion passwords have been stolen—and counting. To protect identities, you must implement a more robust, multi-layered security model, of which CIAM is an integral part. CIAM uses contextual clues to decide whether to give access, and how much. Even with correct credentials, a login attempt from an unrecognized IP address or at an atypical time of day can trigger additional security precautions from the CIAM platform, asking security questions or prompting a push notification to a user's cell phone, for example. CIAM is so powerful because it looks at real-time information to make secure access decisions.

Key Takeaway

Your CIAM platform must support dynamic decision-making based on real-time context. Static approaches to evaluating access and authorization policies limits your ability to properly protect your most important asset—the customer.

How Does CIAM Improve Customer Engagement?

CIAM lets you build a customer identity-centered digital platform. The same digital identities can be used across our omnichannel world, so customers and citizens can interact with businesses and governments from anywhere, on any device. CIAM uses real-time context and data to personalize that experience. A sampling of examples below:

Connected Car — Your car knows who you are, and, more importantly, knows who you are not. Your husband might have different preferences for seat and mirror position, radio station, car temperature, etc. And his list of typical destinations might include the grocery store on the right hand side of the road on his commute, movie theaters equipped with IMAX 3D, and gas stations charging under $4.09 for premium. Your connected car knows these personal preferences and adjusts its seats, mirrors, radio, temperature, and GPS preferences depending on who gets into the car, because each of you has a unique identity tied to your login credentials, where personalized data can be noted, saved, and utilized by the car to cater to your needs. The benefit for the company is customer satisfaction and loyalty. The customer in turn is rewarded for this loyalty when their next car of the same make already knows all of these preferences too. Consumers are incentivized to replace vehicles faster in order to take advantage of continuous improvements in this technology, as well—much as they do now with their smart-phones. Company profits increase as customers remain loyal, make purchases more often, and opt for upgrades that allow for more personalization.

Insurance Portal — Customers often buy multiple insurance policies, from home to vehicle to life and everything in between, and each individual and vehicle and home has a separate policy. Consumers and insurance companies alike would appreciate having all of a customer's policies organized in one place, associated to their digital identity. This makes it easy for the customer to manage, buy, and make changes to

policies, as well as make payments, get quotes, and obtain documents, 24 hours a day. It also makes it easy for the company to understand and assist the customer—where they live, what policies they have, how many and at what price, etc. It opens up opportunities for the insurance company to offer additional policies the customer may be interested in, as well.

E-Government — By associating citizens with a digital ID, governments can deliver secure services to citizens and businesses so they can do things like obtain birth and death certificates, apply for schools and student loans, manage welfare services and health information, and pay parking tickets, automobile registration fees, utility bills, and taxes online, empowering citizens with quick and easy self-service— without the line! Citizens get the services they need faster, and come away from the experience feeling positive about government's role in their lives.

Set-Top Box — Your set-top box understands who is watching TV, and what your preferences are. When you log in, it can pull up your preferred shows, genres, stars, and suggest similar ones. When your kids log in, it will block certain channels, or movies with a certain age restriction. Better yet, when you walk in the door and it recognizes that your phone is on the premises (and thus that you are home) it can give the kids permission to watch certain shows, or even to turn on the TV! CIAM-enabled set-top boxes are able to deliver content to users based on the policies associated with their identities. These set-top boxes can make intelligent decisions about who is able to watch what, when, and where.

Wearables — Whether it's your watch connecting to your credit card details at the coffee shop so you can forgo the wallet, your shoes syncing to your laptop after your hike so you can view your workout data over time, or your hat streaming your favorite music app on your chilly walk to work, CIAM can deliver new applications to anything that can be an application platform. We have a lot of choices when it comes to our gear, and our digital gear options will continue to increase. If we want to be connected, CIAM will provide ways for us to receive any application or service on our device of choice—whether or not we're wearing it.

Key Takeaway

CIAM can connect to any device with an internet connection, whether that's a phone, a watch, a thermostat, a fridge, a car, or a shoe. Essentially, anything that can be connected, will be connected, and therefore must be identity-enabled. Your CIAM platform needs to be able to deliver identity services to any thing.

How Does CIAM Support Privacy?

Organizations have struggled to handle customer data well. For many companies, business needs and customer needs are at odds. The business wants to collect and use customer data liberally, while customers would prefer to provide minimal data and keep it well-controlled. Striking a balance between these two needs is a difficult endeavor, and helps explain why the EU General Data Protection Regulation (GDPR) was created. It provides a framework to make consumers aware of exactly how their data is handled. With growing data volume and new IoT data sources (from personal GPS devices to health trackers and more), customers need to know where their data is going and that it's protected.

Fortunately, CIAM was designed from the ground up for large-scale, consumer-facing deployments. A good CIAM platform can help companies follow GDPR regulations. It can also ensure that customers never have to wonder whether their data is being shared. It should give them direct control over who gets access to what data and when, and the ability to review their data, update it as necessary, and remove it when appropriate. Companies will need to successfully navigate this transition to customer data empowerment not just to voluntarily build trust with their customers, but to support other emerging privacy regulations as well.

Key Takeaway

An identity solution must offer a customer profile that gives users a single place to view and manage their profile data, no matter where it is stored, and a comprehensive set of customer data privacy capabilities.

Can CIAM Support Large-Scale Populations?

CIAM is designed to support millions of concurrent users, because it is designed for internet-scale. CIAM platforms are built to accommodate customers and citizens, not merely employees, so it is by nature built for high traffic and high volume.

Key Takeaway

Legacy IAM platforms were designed for employees on business premises, and cannot stand up to current and future consumer demands. CIAM platforms are designed to accommodate internet scale and a variety of devices, with customer ease of use in mind.

What's the Best Way to Evaluate an CIAM Solution?

In order to evaluate a potential CIAM solution effectively, you should make sure it meets the requirements listed below. Potential vendors should clearly outline how the solution will work to meet each of your requirements. Finally, you should test the solution. A thorough evaluation up front will save you years of toil and trouble later.

It is important to beware of the pre-fab demo some vendors will pitch. You'll want to see a real, live POC. Anyone can claim a modular, lightweight, flexible stack, but if it takes 20 engineers 20 days to simply install the software, the proof is in the pudding. If you don't understand how the solution will work for you, proceed with caution until you do.

Key Takeaway
To help you in your buying process, make sure the following boxes are check-marked before committing to a CIAM solution. Some companies offering customer-facing identity suites have not built a CIAM platform, and are instead repurposing a legacy IAM solution that is incapable of building trusted digital relationships between users, devices, and things. If the solution meets the requirements below, it is a genuine CIAM platform, ready and able to solve your customer-facing identity needs.

Customer Identity Management Evaluation Checklist

- ☐ **Was it designed for customers and citizens, or employees?**
- ☐ **Can it secure the identities of your users, devices, and connected things, and manage relationships formed between them?**
- ☐ **Is it context-aware?**
- ☐ **Can it enable customer-facing services?**
- ☐ **Can it produce a uniform customer profile across business units?**
- ☐ **Is it device-agnostic?**
- ☐ **Does it address emerging privacy regulations, like GDPR, with support for user privacy standards?**
- ☐ **Is time to market weeks to months, or months to years?**
- ☐ **Is it highly scalable?**
- ☐ **Are processes repeatable, so you can roll out new services without starting from scratch each time?**

About ForgeRock

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

Get free downloads at www.forgerock.com and follow us @ForgeRock