Build vs. Buy?
A Guide for Customer Identity and Access Management (CIAM)

Understand the pros and cons of implementation options, ranging from in-house software development to commercial off-the-shelf solutions.
Executive Summary

Digital identity and customer profiles are at the center of every company's digital transformation. In today's markets, customer identities and the personal data associated with them are among the most critical and valuable assets of any enterprise. They are crucial for business success.

Managing these digital identities – from first registration and login to the later stages of the customer relationship – and extracting business value from the associated data are complex tasks, commonly referred to as customer identity and access management (CIAM).

When implementing the concepts, processes, and technologies needed to collect, manage, and utilize digital identity and customer data, companies have two basic choices: in-house development or buying a dedicated solution from a vendor specialized in CIAM (i.e., build vs. buy).

This paper explores the pros and cons of in-house software development versus commercial off-the-shelf solutions. Different options are considered, such as on-premises implementations, colocation, and various cloud environments.

The findings in this paper indicate that in most scenarios and for most enterprises, “buy” is preferable to “build,” and that off-the-shelf cloud-based solutions are a better choice for most companies' goals, needs, and resources. This is particularly the case when not just the initial implementation is being considered, but also the level of effort it takes to operate and maintain a solution in the long term, with continuously changing requirements dictated by technology, consumers, markets, and regulators.

Who should read this paper?

Decision-makers in both technical and nontechnical roles who need to make informed decisions on how to best implement CIAM in their organization.
CRITICALITY CONSIDERATIONS FOR IDENTITY SOLUTIONS

As a first step in exploring implementation options for identity management, including the option to build it in-house, it is useful to reflect on the overall criticality of the task: How relevant is it for the enterprise, and what business damage could arise in the case of a service interruption or malfunction?
Customer Identity as a Basic Digital Business Prerequisite

The value of profile data linked to customer identities has grown dramatically over the past decade and is one of the most crucial success factors for companies today. Customer profile data forms the foundation for analyzing, understanding, and predicting consumer behavior and customer journeys — from first contact to purchase decisions to long-term brand loyalty.

Just as important, customer data is also the prerequisite for any form of personalization, be it basic personalized marketing or real-time personalization. The latter takes customer targeting to a more sophisticated level by not only making advance decisions about what message a customer will see the next time they are contacted, but also by making automated and data-driven decisions during a live customer interaction. Real-time personalization allows adjustments to the user experience and content so that it resonates with the individual — on a website, mobile application, Internet of Things (IoT) device, or other channel.

On a more basic level, digital identities are a fundamental functional prerequisite for any online retail site or other transaction-based application where customers need to log in and be securely authenticated before they are granted access to data and services to engage in business with the company.

In simple terms, if customers cannot log in because of a glitch in the identity management system, business could stall and revenue generation could be affected. At the same time, support workloads will most likely increase, and there is potential for reputational impact from frustrated users venting on social media and in review forums.

Customer Experience Aspects: UI, Performance, and Reliability

Another crucial factor that helps determine the criticality of CIAM is the customer experience in the processes and flows for registration, account creation, login, and preference management. Apart from the actual user interface aspects (like web forms), performance and reliability are vital factors here.

Research reveals that slow load times and a sluggish user experience have a devastating impact on conversion rates. Furthermore, a study conducted by Dynatrace and T-Mobile showed that visitors viewing pages earlier in the transaction journey are more sensitive to performance issues than when viewing later pages.¹
The registration, login, and authentication processes are among the earliest engagement points in the customer journey; these stages can more easily make or break the user experience. Conversely, the deeper a customer goes into a transaction, the more patient and committed they are to completing it. Page loading time is also a ranking factor for Google search results for both desktop and mobile sites.²

**Customer Satisfaction and Support Aspects**

Of course, user experience issues can occur at any stage of the customer journey, even after successful account creation. Forgotten passwords or similar account issues may impact customer satisfaction and typically result in account abandonment, a decrease in brand loyalty and, ultimately, lost business. According to Chatbots Magazine, 91% of unsatisfied customers will not return for a repeat purchase or service.³

Additionally, support for user experience issues are costly for businesses. Statistics from contact center software provider Aspect Software estimate that the cost of a single customer service phone interaction is around $35 to $50. Even text-chat support costs around $8 to $10 per session.⁴ IBM estimates that 265 billion customer support requests are made every year, and it costs businesses a whopping $1.3 trillion to service them.⁵

---

A sluggish registration or login experience can have a devastating effect on conversion rates.

---

Businesses spend $1.3 trillion a year on customer support requests — and they still lose customers.
One of Akamai’s clients, a large global retail company, estimated the average number of abandoned logins at about 200,000 per month, resulting in estimated lost sales of approximately $45 per customer per month. This — and the costs associated with customers contacting the company’s service hotline to recover their accounts — were the main drivers for this client to switch from an in-house developed identity solution to Akamai’s CIAM solution, Identity Cloud.

The company’s internal solution could not offer a self-service functionality for customers to regain access to their accounts through alternative authentication methods, such as social login, security questions, or SMS notification. The development effort to implement these features into the existing in-house solution was estimated to be higher and more risky than migrating to Akamai Identity Cloud, a commercial solution that offers these capabilities out of the box.

The cost of login failures can add up. And the cost to build self-service functionality to recover credentials can be higher than the cost of deploying Akamai Identity Cloud.
The Ability to Evolve and Innovate

What makes a successful customer experience is subject to constant change. As the digital landscape grows and new demographic cohorts enter the buyer audience, customer identity management continues to see increasingly fast-paced evolution.

This requires keeping up with new user expectations, like passwordless login, and a changing topography of customer engagement points – web, mobile, and IoT. True omnichannel support has become a necessity to satisfy modern consumer expectations, allowing customers to login anytime, from anywhere, and on any device, and experience the same or very similar navigation flows and personalization.

The identity management solution must be able to accommodate new, fast-changing requirements and trends that often are hard to predict, or it will put the business at risk of falling behind the competition. When building an in-house identity solution, significant funding, staffing, and expertise must be secured far beyond the initial implementation stage.

Compliance and Security Aspects

Customer identities are valuable assets to not just companies, but also to the individuals who own them. As more areas of our lives move into the digital realm, sensitive personal data ends up in our profile data – ranging from name, address, phone, sex, or payment information to personal preferences, shopping and browsing histories, and other behavioral data. The need for companies to secure and protect the customer data stored online has increased significantly, and regulators worldwide are reacting to this.

Regulatory compliance and security are major factors that add tremendously to the complexity and criticality of identity management. Customer data contains personally identifiable information (PII), which is subject to a broad and increasing variety of regulations and privacy laws.

These regulations vary between regions and jurisdictions, yet global businesses must ensure that their digital sites comply with all laws. Examples include the European Union’s General Data Protection Regulation (GDPR), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act of 2018 (CCPA), and other industry-specific regulations, such as the privacy laws restricting the release of medical information in the United States.
As identity data can easily be abused and exploited, it has become the main target for hacking attacks. The 2018 Cost of a Data Breach Study, conducted by IBM Security and Ponemon Institute, found that almost half of the organizations represented in that research (48 percent) identified the root cause of a data breach as a malicious or criminal attack, with an average cost of approximately $157 per breached identity record. As breaches frequently involve hundreds of thousands (or even millions) of records, the resulting cost can severely harm a company – and that’s before revenue loss associated with reputational damage and loss in customer trust is calculated.

Businesses need to apply the highest security measures, not just to protect themselves, but also their consumers. In the worst-case scenario, customers could become victims of identity theft, with potentially significant impact on their financial, professional, and personal safety, all of which have the potential to lead to liability charges and class-action lawsuits against the business.

The factors described above show that in most cases and for most companies, the overall criticality of customer identity management is extremely high.

Departments involved in selecting and implementing identity solutions are advised to carefully identify and examine the factors that determine criticality in their specific case. They should also make stakeholders and decision-makers across the organization aware of their findings to ensure a common understanding and agreement. This will help in allocating the appropriate budgets, resources, and priorities needed for a successful CIAM implementation.
Selecting an Enterprise-Grade Customer Identity and Access Management (CIAM) Solution

**MUST-HAVES**

**Registration, login, and authentication** – including multi-factor authentication (where two or more credentials are requested for increased security)

**Social login** – authentication through Facebook, Google, LinkedIn, or other social media identity providers

**Single sign-on (SSO) and federated identity** – providing access to multiple sites and systems with one single login

**Access control** – the ability to implement and enforce access policies to control what customers can and cannot do on a site

**Preference management** – the ability for customers to view and edit certain preferences within their account

**Consent management** – most privacy regulations require companies to obtain explicit consent from customers before obtaining personal data, and customers must be enabled to view, modify, or revoke consent

**Omnichannel user experience** – the UI/UX (web forms, interfaces, flows) to perform the above tasks, across web, mobile, IoT, and other channels

**Data aggregation and storage** – all related customer data needs to be stored in a secure way and in compliance with data protection and privacy regulations

**Integration** with the existing landscape of CMS, CRM, ERP, marketing automation, analytics, and security information and event management (SIEM) systems

**Compliance and audit-readiness** – the ability to do all of the above while staying compliant with regulations and/or industry standards, and being able to provide proof for audits

**Scalability and reliability** – reliably execute all of the above globally at large scale and with no performance degradation during peak times, with an SLA of 99.95% uptime across multiple channels and domains, and for millions of concurrent users
BUILD VS. BUY?

Given the value and overall criticality of digital identity for the business, it seems well within reason for a company to aim for full control and completely own its fate by developing its own solution. However, given the complexities described in this paper, it is entirely possible – while often not immediately obvious – that companies overreach their capabilities and end up with customer identity solutions that fail to meet business, regulatory, or customer requirements.
Departments tasked with implementing identity management might find themselves confronted with unexpected problems; the resulting pressure may become a heavy burden on the organization’s motivation, productivity, and ability to deliver. This could result in missed deadlines, go-to-market delays, surpassed budgets, and other negative consequences.

Even if the technical implementation and operation proceed as expected, the question remains as to whether in-house development makes economic sense, considering business metrics including total cost of ownership (TCO), return on investment, or expenditure for capital. Furthermore, organizations must ensure that they are able to not only solve today’s requirements for functionality, security, availability, and scalability, but that they can evolve the solution to keep up with changing market developments.

**Reasons to Outsource**

Departments tasked with implementing identity management might find themselves confronted with unexpected problems; the resulting pressure may become a heavy burden on the organization’s motivation, productivity, and ability to deliver. This could result in missed deadlines, go-to-market delays, surpassed budgets, and other negative consequences.

Even if the technical implementation and operation proceed as expected, the question remains as to whether in-house development makes economic sense, considering business metrics including total cost of ownership (TCO), return on investment, or expenditure for capital. Furthermore, organizations must ensure that they are able to not only solve today’s requirements for functionality, security, availability, and scalability, but that they can evolve the solution to keep up with changing market developments.

**Outsourcing non-core competencies – like CIAM – offers multiple benefits.**

Even if the technical implementation and operation proceed as expected, the question remains as to whether in-house development makes economic sense, considering business metrics including total cost of ownership (TCO), return on investment, or expenditure for capital. Furthermore, organizations must ensure that they are able to not only solve today’s requirements for functionality, security, availability, and scalability, but that they can evolve the solution to keep up with changing market developments.

Last, but not least, companies will have to decide if creating and running a customer identity solution is the best use of their in-house resources.

### Build vs. Buy?

The decision to build or buy the CIAM solution involves choosing between in-house development and outsourcing. Below are the most common options, along with associated benefits and challenges.

#### Build vs. Buy?

Whether the decision is to build or buy the CIAM solution, the company must decide where to host it. Below are the most common options, along with associated benefits and challenges.

### On-Premises Data Centers and/or Colocations

Hosting the CIAM solution in the company’s own data center involves owning and operating the physical computing and storage resources. Owning the entire infrastructure gives the company full control of the operation, down to the choice of what server models and network switches are being deployed.

On-premises data centers are often used in scenarios where the data they process are considered too sensitive to be transferred across public networks and/or where regulations prohibit data transfer outside of a private network. Local data centers might also be the only option in cases where the data volume is simply so large that transferring the data across public networks would be too slow.
However, when it comes to CIAM, typically none of the above applies. Customer-facing digital sites are connected to the Internet, and customers provide their data using public networks in the first place. While there are many strict data protection regulations that CIAM solutions need to adhere to, none of them prohibit the use of public networks. Encryption of data in transfer and in rest can—in combination with other safety means—provide adequate security. The volume of identity data can be very high, but can (and must) be handled using the Internet, because that is where the customers are and where they engage with the company's systems.

The cost and effort of owning and maintaining data center facilities is significant. This would encompass the cost of the actual data center facility, including real estate; hardware such as servers, routers, firewalls, and load balancers; air conditioning; energy; redundant electricity lines; uninterruptible power supplies; compliance with building security policies; and more. Additional costs include the staffing needed to run the infrastructure.

Businesses could opt for a colocation approach—renting parts or all of these physical resources from a third party—which offers a lower-cost entry point. However, it requires an exact definition of resources, service levels, and security and operational models to ensure a smooth collaboration between the business and the hosting facility. This adds to the administrative overhead.

Under data protection regulations such as the GDPR, companies are generally accountable for ensuring that their vendors handle personal data in full compliance. This needs to be considered when choosing colocation providers.11

All of the above efforts proliferate if the company needs multiple data centers in different regions. This is likely to be the case when serving audiences across regions or continents with a need to ensure low latency times so that the performance of the digital sites and services do not negatively impact the user experience. As discussed previously, customer dissatisfaction from unreliable or sluggish digital experiences can lead to high bounce and drop-off rates, as well as increased support costs, and can potentially impact the business.

Another primary reason to have more than one data center or colocation is the requirement of high availability. If one data center goes down for some reason, the company will need the capability to failover to another data center as part of a broader plan for business continuity and disaster recovery.

In-house CIAM solutions may require incremental data-center costs, and they can be significant.
Private Cloud
A private cloud is basically an on-premises data center or colocation using a shared-pool cloud computing approach.

Cloud environments have advantages over more traditional infrastructure. They allow for easier and faster configuration of services and rapid deployment of applications. They also work better with modern software development paradigms and technologies, such as agile development, continuous integration and delivery, DevOps, and the use of containers and microservices.

Clouds offer certain economy-of-scale benefits because their design allows for different services to share resources. However, the ability to share resources within a company is fairly limited. The private cloud infrastructure must be able to accommodate all potential traffic and workload peaks. Such peaks can be high for CIAM systems. For example, if a company runs a large and successful but seasonal marketing campaign, the number of customers who are logging in, creating accounts, and engaging on a digital site might increase many times over and reach tens of millions of concurrent users. At the same time, the amount of system-related operational data, like log and event data, will multiply as well.

The hardware resources to handle these temporary increased needs for compute power and storage must be physically available. That means they have to be owned or rented and paid for by the company, even if they sit idle for the rest of the year and drive up CapEx spending and TCO, while eating into the return on investment.

The requirement to have enough buffer for traffic peaks is the reason why cloud environments are usually over provisioned. Underprovisioning is dangerous, since it might lead to severe issues in user experience – from slow registration forms to total downtime. Ironically, this is most likely to occur when a service, product, or campaign is otherwise highly successful in driving traffic and sales. It is the worst time for IT to get in the way of business success.
Decision-makers need to understand that it requires significant time, effort, experience, and expertise to determine the right level of provisioning and—in general—to architect, implement, and operate a large-scale private cloud environment. It adds a significant additional layer of complex technology that will introduce many additional single points of failure if not designed and operated correctly.

Instead of using a company’s own hardware and data center facilities, a popular option to host CIAM solutions is using a public cloud vendor, like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud.

Public Cloud

Public clouds eliminate the need to own and operate data centers and hardware platforms, which are provided as services over the network instead. These platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offerings can be used to host an otherwise in-house-developed CIAM solution. If needed, public clouds can be combined with hosting parts of the infrastructure on-premises or in a colocation (hybrid cloud).

In addition to removing the overhead of owning and operating data center resources, public clouds offer major cost efficiency benefits. As the cloud infrastructure is not just used by one company, but shared among many (multitenant model), the cloud vendors can realize economies of scale to a level that is simply unachievable by an on-premises private cloud.

Additionally, most public cloud vendors offer “pay-as-you-go” pricing, where clients are only charged for services that they use and that actively utilize system resources. If an application deployed on the public cloud lies dormant because of low traffic, few or no charges will occur, while charges go up when traffic increases and the application consumes compute cycles or storage on the servers.

Home-built CIAM solutions, running on public cloud services, will not automatically inherit the cloud vendor’s own security, service, and support levels.
Calculating cloud costs compared with on-premises infrastructure

Microsoft and Amazon provide online calculators that compare TCO for configurations hosted on-premises and on their respective public clouds. At the time of this writing, Google only offers a pricing calculator that doesn’t compare TCO. There are other similar calculators available on the web as well.

All of these can only give rough estimates of the true costs. In reality, costs will be influenced by a variety of factors and need to be analyzed on a case-by-case basis.

Risk of Cloud Vendor Lock-in

The major public cloud vendors offer an increasing variety of services. This makes it tempting to go all-in with one big cloud provider, following a similar model that many CIOs chose during the era of big enterprise software deployments, as ZDNet’s Larry Dignan points out. Once companies have moved their applications and data onto one cloud platform, it can be very complicated and expensive for them to move away again. It might even prevent a company from moving to a cloud vendor that offers better pricing or more innovative technology.

A multivendor cloud strategy would reduce the risk of lock-in, but requires additional efforts and resources in the design of a CIAM solution, and means that teams must build up and maintain expertise in the technologies of different vendors.

Security, Service Level, and Support Aspects

CIAM solutions that use one of the large public clouds benefit from the significant resources that these vendors invest in the technology, infrastructure, and security of their offerings. These vendors provide 99.5% availability for many of their services, and obtain a large number of security or industry certifications.
This might lead to a false sense of “inherited” security and reliability. Any software project that is built on top of a public cloud environment will not automatically have the same levels of availability and security, and will not be covered by the certifications that the cloud vendors have obtained for their services. This is also true for CIAM solutions, whether they are in-house developments or commercial products.

Significant effort, expertise, and experience is needed to achieve the same (or better) levels of availability and security for the CIAM solution as those of the underlying cloud infrastructure.

As an example, Akamai Identity Cloud maintains and is audited or assessed for certification/compliance with a large number of assurance programs for its Identity Cloud solution, including ISO 27001:2013, ISO 27018:2014 (PII protections in the cloud), SOC 2 Type II (all five Trust Principles), HIPAA (storage of healthcare data), HITECH (transmission of healthcare data), Cloud Security Alliance (CSA star), U.S.-E.U. Privacy Shield Framework (reviewed by TRUSTe), and TRUSTe privacy program.

It is typically neither feasible, nor economically reasonable, to obtain this level of certified and audited security and compliance with an in-house-built solution.
Leveraging Free/Open Source Software (FOSS): Basics and Common Mistakes

Most organizations will heavily rely on using free/open source software (FOSS) when building their own CIAM solution. Almost every infrastructure and application stack today utilizes a variety of components based on FOSS governed by a license that allows companies to obtain, share, and modify the source code. Prominent examples include the Linux operating system, the Apache web server, and OpenSSL (a toolkit for secure data encryption). The development of FOSS is most often associated with an open community of contributors and a community-based vetting process that determines which contributions and modifications to the code will become part of the main source tree.

It is important to keep these basics in mind when evaluating if a particular FOSS component is a viable choice for an enterprise-grade, in-house project. DevOps teams often focus only on the actual functionality and quality of a FOSS component: Does it do what we need and does it do it well? For these criteria, many FOSS components will pass the evaluation with flying colors. Some of the most feature-rich, highest-quality, and most widely used software projects are being developed as FOSS.

However, there are common misconceptions about FOSS that can lead to incorrect assumptions about the effort and costs associated with using FOSS components as part of the application or infrastructure stack within a larger commercial project. These misconceptions are related to the basic nature of free software described above.

“Free Software” Does Not Mean Free of Costs

While one can typically download and use the software free of charge, running FOSS components still requires effort and resources that come at a cost. In fact, the term “free” was never supposed to mean free of costs, as Richard Stallman of the Free Software Foundation explained: “Free software means software that respects users’ freedom and community. Roughly, it means that the users have the freedom to run, copy, distribute, study, change, and improve the software. Thus, free software is a matter of liberty, not price. To understand the concept, you should think of free as in free speech, not as in free beer.”[14]
The Community Will Not Do All Development and Bug-Fixing for You

One of the strengths of the community-based development model is that it frees software projects from being driven by the interest of only one or very few individuals. The developer community has the freedom to break compatibility between releases, radically change APIs, interfaces, or data structures, and drop or add functionality at any time — all without being slowed down by the needs of large commercial users for whom such changes might be difficult to stomach and expensive to implement.

While this agility allows for amazingly fast innovation cycles, it can turn out to be problematic if the company using the FOSS components is actually a large commercial user who needs to put significant resources into the roll out and testing of updates and new versions of components that make up the application stack. If the community decides to introduce a major code change that breaks compatibility with other parts of the application, then the cost and effort to rework (potentially re-architect) the stack can be significant. If such a change is introduced as part of a critical security fix, the company might not even have the option to wait to implement the update — unless it accepts the risk of leaving sites and customer data vulnerable for the time being.

While it might be acceptable not to upgrade to every new version of a FOSS component, skipping community-provided code patches and version upgrades for too long almost always leads to a point when urgent security and/or other bug fixes cannot be applied to the older version.

License Compliance

At the time of this writing, there are 83 different open source licenses that have been approved by the Open Source Initiative, and there are literally hundreds of other licenses that are unapproved by the organization. Companies using FOSS components must ensure compliance with these licenses and understand the obligations and — especially if they redistribute the open source software — possible implications on their own intellectual property.

Open Source Projects Might Change Direction or Even Cease to Exist

Open source projects can change for a variety of reasons. The community might decide to take the project in a new direction because the needs and requirements that initially motivated the development have changed. Disagreement on direction, technology, or licensing within the community sometimes leads to a divide, resulting in the creation of a new project and a fork in the source code. An example specific to identity management software are the OpenDS and OpenSSO projects, which were originally created by Sun Microsystems, then became the basis for a commercial offering by ForgeRock, and, after a license change, went through a fork and split of the community.
Buy Options

Traditional IAM Solutions

There are two types of dedicated commercial identity solutions:

- **Traditional identity access and management (IAM)**
- **Customer identity access and management (CIAM)**

It is a common misconception that the technology required for CIAM is the same as that for traditional IAM. Traditional IAM solutions – also called enterprise, employee, or workforce IAM – are the IT systems that ensure that only the workforce or known business partners of a company can access the corporate network and its resources.

Traditional IAM is usually well established, leading some companies to make the misguided assumption that, “because we have this technology in-house already, it can’t be that hard to extend it to our customers.” At the root of this approach is a drastic underestimation of the differences between workforce IAM and customer IAM, and the complexity of managing customer identities for a business’s public-facing digital properties. CIAM has disparate – and far more challenging – requirements than workforce IAM; as a result, repurposing workforce IAM solutions can be a problematic approach.

As traditional IAM is designed to facilitate employee access to internal systems, it cannot provide insights into who a user is. In fact, identity is assumed, and advanced data like the actions a user takes and what influences their journey and behavior within the digital sphere cannot be tracked. But businesses require these types of data insights to understand their customers and compete in the digital market space.

From a security perspective, this assumption of identity poses a risk. IAM system users are known employees of the company, and access is typically determined by HR or IT. Conversely, applications or programs that employ CIAM solutions – where unknown users register themselves over the Internet – cannot and should not assume identity. Bad actors can create fraudulent accounts relatively easily, and even users without malicious intentions can use fake data to register. The identity management system must be able to account for this difference.
Another crucial difference between traditional IAM and CIAM systems is the ability to scale. At even the largest corporations, workforce IAM systems might be charged with administering up to tens of thousands of employee identities. But high-volume brands must handle tens — or even hundreds — of millions of customer accounts simultaneously.

**Customer IAM Solutions**

Dedicated CIAM platforms, like Akamai Identity Cloud, are architected from the ground up to handle customer identities on a very large scale and provide companies with maximum value from customer profile data.

CIAM solutions also enable seamless and frictionless customer experiences so that tasks like login, authentication, or preference management don’t impede activity and drive consumers toward the competition. CIAM technologies also address the critical need to secure personal data across public networks, as well as enable global businesses to comply with varied and frequently changing privacy regulations.

**On-Premises**

Similar to the “build” options, commercial CIAM solutions are available that can run on a company’s own hardware in on-premises data centers. This option eliminates the need to develop the actual CIAM functionality, but the costs and efforts associated with owning and operating hardware and facilities as discussed above remain. It also does not solve the problems of business continuity/disaster recovery, reliability, and potential performance and latency issues that stem from not having enough physical data centers for failover and distribution of traffic.

**Hosted (Pseudo-Cloud) CIAM**

Choosing a commercial CIAM solution that is cloud-based enables companies to eliminate these efforts and further reduce complexity. Companies should take a close look at exactly what it means when a vendor claims to be cloud-based and to offer identity as a service (IDaaS), a term often used in conjunction with these offerings.

Engineering teams built Akamai Identity Cloud from the ground up to handle customer identities on a very large scale, and make sure companies could get the maximum value from customer profile data.
Many CIAM solutions have their roots in traditional IAM; the original architecture of these solutions is often that of a traditional monolithic application that companies need to install and operate on their own hardware on-premises.

In order to “cloudify” these solutions, many vendors simply choose to host them on a server in the cloud. While this concept has one advantage – it allows the software to run on-premises as well as on private and public clouds – it also means that the inherent architecture of the CIAM solution is not capable of taking full advantage of a modern cloud environment. This approach will fall short on capabilities like elastic scaling to accommodate traffic peaks or quick failover between instances and regions.

These “pseudo-cloud” solutions also usually can’t fully utilize the economic benefits of shared resources in a cloud. Their architecture is not designed to run in a highly modularized and distributed multitenant environment. They typically duplicate many functional components that would be shared in software that is natively architected for the cloud.

**Cloud-Based (Cloud-Native) CIAM**

CIAM solutions that were designed and architected to run in a modern cloud are much better suited to take full advantage of the environment’s shared resource model and economies of scale. They frequently cannot be deployed on-premises in a private cloud environment.

This “cloud-native” model eliminates the need for companies to provide hardware and data center resources or to worry about the choice of a cloud provider. It also allows for a high level of efficiency and optimization.

**Architecture Matters**

Even for cloud-native solutions, you should have the vendor explain the details of its architecture; how it achieves scalability, reliability, and security; what availability is offered as part of its SLA; and what actual availability has been achieved over the last 12 to 36 months.

Consider this example: In 2016 in Australia, a massive storm system that ran from Brisbane to the NSW South Coast lead to a weekend of widespread flooding and coastal erosion. The data centers that host a public cloud vendor’s regional servers were affected, and as a result, many of their cloud services went down and impacted customers.
An Akamai client in Australia, one of the region’s largest B2C brands, uses this public cloud vendor to run a majority of their customer-facing sites, and the outage heavily affected their systems. While the cloud vendor recovered after about six hours, it took the client several days until its own sites were fully restored.

One of the services that wasn’t substantially impacted by the storm was Akamai Identity Cloud. What allowed Akamai to recover quickly and without data loss was its cloud-native architecture that is built with maximum global availability in mind.

Identity Cloud automatically initiated a failover to other geographical regions to take over and reroute the traffic accordingly. It not only switched to a backup region, but also declared other still-functioning regions as further fallbacks in case of a failure of the backup system. The client’s customer identity data was already available in the failover regions as part of Akamai’s regular data backup procedure.

Akamai Identity Cloud is designed to maintain functionality and still meet performance SLAs even in the case of catastrophic failures that bring down data centers and power in multiple regions at the same time. Failover scenarios and data backups between regions are tested on a regular basis, and their functionality is confirmed by an independent auditor.

As a result of the Australian storm incident, the client asked Akamai for guidance in the redesign of its systems to prevent similar future incidents from occurring.

The Importance of Geographic Diversity

When a massive storm took out a public cloud vendor’s data centers in southern Australia, Akamai Identity Cloud quickly got back up and running – with no data loss.
Conclusion

Commercial CIAM solutions have a few significant advantages over in-house IT departments that attempt to build a solution on their own. From global availability and scale to guaranteed SLAs and security certifications – the competency, resources, and ongoing research and development that come with utilizing third-party vendors mean that your IT team can focus efforts on other key business initiatives.

CIAM solutions that are architected to utilize the capabilities of a modern cloud to share resources, provide elastic scale, and enable multiregion failover and disaster recovery offer IDaaS with a wealth of features – and at security levels that are frequently hard to match with in-house developments. At the same time, they eliminate the need to own and operate data center facilities and hardware.

While do-it-yourself identity management might seem doable, there is substantial risk of underestimating effort, underfunding, and a lack of long-term internal resources and expertise to support, maintain, and evolve the solution to meet changing market requirements and consumer expectations. Commercial CIAM vendors are in a better position to keep up with changes dictated by technology, consumers, markets, and regulators, simply because the vendors need to evolve their services to keep their offerings competitive and relevant.

In most cases, the “buy” option is more recommendable than the “build” alternative, while cloud-native, off-the-shelf identity management solutions are a better choice for most companies’ goals, needs, and resources. That said, companies should evaluate their options based on their individual situation to determine which path is the best for their particular case.

For more information, visit akamai.com/ciam or read our "Buyer's Checklist: Top 10 Considerations in Selecting a CIAM Solution."

SOURCES
9) Improving IT Project Outcomes by Systematically Managing and Hedging Risk. IDC report by Dana Wiklund and Joseph C. Pucciarelli.
11) GDPR, Art. 22: “Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union.”
12) Microsoft: Total Cost of Ownership (TCO) Calculator; AWS: Total Cost of Ownership (TCO) Calculator
13) https://www.zdnet.com/article/enterprises-learning-to-love-cloud-lock-in-too-is-it-different-this-time/
15) Open Source Initiative: Licenses by Name, https://opensource.org/licenses/alphabetical
16) http://www.timeforafork.com/

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone — and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 05/19.