




Connecting Identity.  
Transforming Digital Business.

A large, stylized illustration in shades of blue and teal. It depicts two business professionals, a woman on the left and a man on the right, sitting at desks and working on laptops. The background is filled with various data visualization elements: bar charts, a line graph, a pie chart, and several interlocking gears. A large, semi-transparent teal 'U' shape is overlaid on the right side of the illustration. The overall aesthetic is modern and tech-oriented.

# Customer Identity and Access Management (CIAM): Investment and ROI

---

A guide to the value of CIAM projects

## Contents

---

Introduction	3
Cost savings	3
- Avoiding a costly data breach	3
- Avoiding regulatory non-compliance fines	4
- Lowering support desk costs	4
- Increasing efficiencies	5
- Growing with your business	5
Increase revenue	5
- Retaining customers	5
- Converting new customers	6
- Creating additional revenue streams	7
Build vs Buy?	7
Why Ubisecure	8
- Analysts	8
- Deployments	9
Summary	10
Further resources	10
Get in touch	10

## Introduction

---

— READ MORE ON 'WHAT IS CIAM' [HERE](#).

Written for the budget holders, this document will help you understand the return on your Customer Identity and Access Management (CIAM) investment.

'CIAM' covers a set of capabilities that enable you to **securely, efficiently and compliantly** verify and manage customer, partner, or other external user identities in your digital services, and control user access to areas of your services. These capabilities may include self-service account credential management, single sign-on (SSO), multi-factor authentication (MFA), support for third party identity providers (IdPs) to streamline registration and login, delegated authority and many more, some of which we will use as examples throughout this document.

CIAM is a very important part of your digital infrastructure and is necessary for any organisation that deals with customer (whether consumer, business or citizen) digital identities. Let's explore the financial aspects of CIAM for your organisation and why it makes financial sense to buy a CIAM solution over building the functionality in-house.

## Cost savings

---

### AVOIDING A COSTLY DATA BREACH

---

The average cost of a data breach is now **\$3.92 million**. The staff resource for detecting and rectifying a data breach, notifying affected users, lost constructive productivity, legal fees and fines (more on fines below) all contribute to this cost.

CIAM helps prevent data breaches in multiple ways, centring around the principle that users gaining access to data are who they claim to be and only accessing what they have permission to access. There are many CIAM capabilities that enforce this principle, and whoever is leading this project for your organisation will select what your specific organisation needs in order to address the correct balance of security and user experience through your digital service(s).

One example is multi-factor authentication ([MFA](#)) – i.e. requiring more than one identifying form factor to log in to a service. [80%](#) of data breaches are caused by stolen, weak or default passwords. While the use of passwords is still commonplace, a second factor (such as biometrics, mobile phone authenticator apps, time-based one time passwords, bank IDs etc.) significantly reduces successful breaches as hackers are far less likely to be able to reproduce both identifiers.

## AVOIDING REGULATORY NON-COMPLIANCE FINES

---

Lack of compliance with regulations, such as GDPR and the more recent California Consumer Privacy Act (CCPA), can leave you with hefty fines.

Going against the GDPR could leave you with the maximum fine of €20 million or 4% of annual global turnover – whichever is greater. Google has been issued the largest fine since enforcement at [€50 million](#). Under the CCPA, fines range up to \$7,500 per record in the database, if the violation was intentional, and \$2,500 if unintentional. That's \$25-\$75 million if you have 10,000 records.

CIAM helps with regulatory compliance with capabilities enabling privacy by design. For example, self-service account management, a CIAM cornerstone, gives users easy control of their own data settings and communications preferences, which is a key requirement of both the GDPR and CCPA.

## LOWERING SUPPORT DESK COSTS

---

Offering self-service account management (for example, a 'My Account' portal) also dramatically decreases calls to your support desk for manual settings changes, e.g. password resets. And these costs certainly add up - according to [Forrester](#), large organisations spend up to \$1 million each year in staffing and infrastructure expenses to handle password resets.

Factoring in single sign-on ([SSO](#)) – a CIAM capability that removes the need for multiple login credentials for multiple services (explainer video [here](#)) – means that cost is lowered even further, as there are simply less credential-related resets necessary.

— [50%](#) OF OUR SURVEY PARTICIPANTS SAID ACHIEVING GDPR COMPLIANCE WITHOUT CIAM WOULD BE IMPOSSIBLE.

## INCREASING EFFICIENCIES

---

Many of your workflows can be made far more efficient with CIAM – both internally and with external partners and customers – taking up less staff time (so they can focus on revenue-generating activities), increasing accuracy of information communicated (leading to fewer costly errors) and keeping data secure.

Let's take [Delegated Authority](#) for example – a CIAM capability that enables users to delegate the right to use digital services on their behalf (explainer video [here](#)). This reduces the need for internal admin-heavy workflows by enabling your external users to delegate authority themselves, within your defined parameters. For instance, a telco may use Delegated Authority for family mobile contracts, whereby a parent could authorise their family members' access to appropriate areas of its online service themselves, again reducing your support desk burden.

## GROWING WITH YOUR BUSINESS

---

If you're trying to make an internal IAM solution fit for external use cases, it could be holding your business back rather than supporting vital growth workflows.

We've all experienced technology that frustrates rather than facilitates processes; if this sounds like your IAM solution there are many financial incentives to upgrade to specialised CIAM. The key thing to remember is that modern CIAM solutions with flexible functionality can be scaled as your business grows and adapts to changing environments, like support for the sudden shift to remote working with the COVID-19 pandemic, making them more future-proof than legacy IAM solutions.

## Increase revenue

---

### RETAINING CUSTOMERS

---

A great customer experience (CX) is absolutely essential to both protecting your existing revenue and winning new customers to drive new revenue.

→ [89%](#) of companies see customer experience as a key factor in driving customer loyalty and retention.

→ It costs 5 times as much to attract a new customer than to retain an existing one.

And CIAM is a key enabler to a great experience with your digital service – check out our white paper on this subject [here](#).

One example is single sign-on (SSO) – again, a CIAM capability that removes the need for multiple login credentials for multiple services, meaning that your customers only need to sign in once to gain access to all applications that they have the right to access. This is a clear CX win as customers don't need to waste time and effort logging in to each separate service. It also increases average revenue per user (ARPU) by making it easier for existing customers to use your complementary products and services without tedious re-registration.

## CONVERTING NEW CUSTOMERS

---

And it's not just retaining existing customers, winning new customers is also facilitated by CIAM.

Firstly, by streamlining your sign up and onboarding journey you ensure that users don't get frustrated with clunky technology and workflows, who may then go to your competitors for the service instead. [45%](#) of users give up if the registration process is too hard. For example, CIAM offers support for third party identity providers, like Google, Facebook, Bank IDs and other federated digital identities. Building in the ability for customers to use an existing identity helps your marketing organisation understand who they are dealing with and makes it very easy for new customers to simply click to register – reducing form filling fatigue and abandonment.

Secondly, CIAM can be leveraged to increase the accuracy of your CRM data. With capabilities such as self-service account management, user data is kept current by the user themselves, making it far more accurate than Sales/Marketing-led CRMs. By integrating the two, you avoid identity silos and leverage the ongoing accuracy of CIAM data for progressive profiling. And Marketing and Sales teams rely on accurate CRM data for efficient operations and personalised outreach, as key steps to a successful customer conversion strategy.

**For these reasons, your CIAM investment should be considered a part of your CX and marketing budget, not just your IT budget.**

## CREATING ADDITIONAL REVENUE STREAMS

---

Federation, another CIAM capability, allows organisations to build links between their own services and external third parties' services.

Large, trusted organisations have the potential to deliver federated trust services based on their identity directories, for the benefit of the members of those directories. This enables revenue streams from third party service providers whilst simultaneously raising awareness of federated brands.

For example, a bank or telecoms provider may already invest in strong KYC assurance practices. Federation would enable them to become an identity provider for other (paying) organisations – think 'log in with my bank ID'.

## Build vs Buy?

---

You might be wondering if your in-house developers could build this functionality themselves, rather than buying the solution from a vendor.

Throughout our many years of working in CIAM, we've seen repeatedly that building a CIAM solution in-house very often doesn't live up to expectations, for example by overrunning on both time and budget. The reality is that CIAM is complex and anyone attempting to build and maintain a CIAM system should have extensive expertise in its technologies and standards (e.g. OpenID Connect, OAuth 2.0, SAML, etc.). Even if you do have these skills in-house, can you be sure that they will not leave the company?

For such a vital part of your IT infrastructure, it is far less risky to buy your CIAM solution from a vendor with this expertise already built in. Buying CIAM means the time and cost of implementation and maintenance will be much easier to predict, and issues like regulatory compliance and security will have been proven with the same technology many times before.

Many successful businesses build their applications by plugging in specialist third-party APIs to facilitate complex operations for core services like payment, communications, & identity management. Best practice now sees organisations using APIs (including identity APIs provided by CIAM) to facilitate their unique digital proposition. This frees up your developers to focus on your core business proposition, creating real value rather than trying to reinvent the wheel in-house.

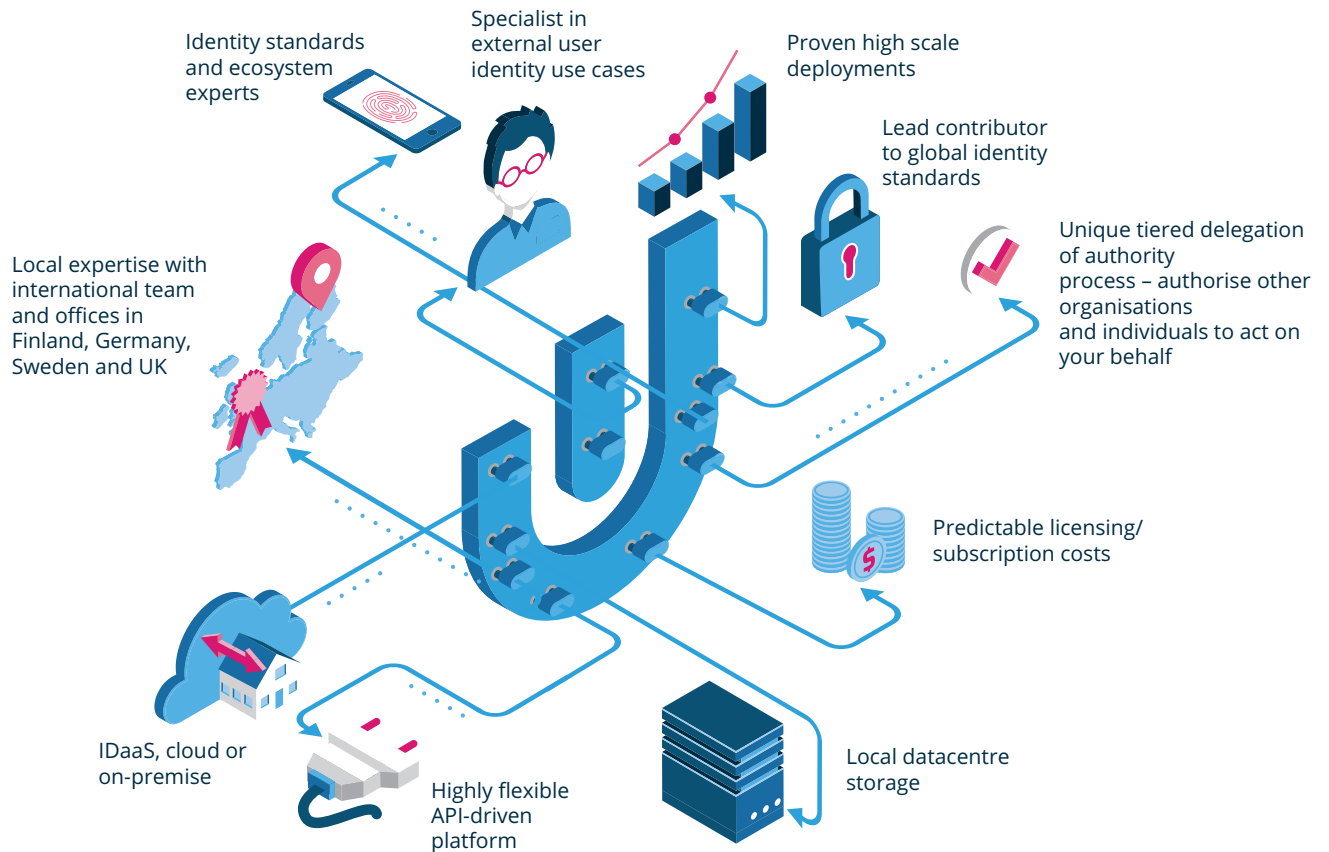
[— DOWNLOAD THIS WHITE PAPER FOR A FULL BUILD VS BUY: CIAM RUN-THROUGH HERE.](#)

## Why Ubisecure

Ubisecure has been helping enterprises securely and effectively manage digital identities and identity-based user experience since our beginnings in 2002, helping organisations use CIAM to become more efficient and drive revenue.

For example, the Finnish government deployed a nationwide identity management system to enable the strong identification of individuals and organisations, based on Ubisecure’s Identity Platform. This resulted in a [99%](#) reduction in the cost of citizen interactions by moving to an online service vs. a physical point of service.

Ubisecure is also a member and community contributor for the industry associations shaping the identity management ecosystem, and has won multiple awards for its solution deployments.



### ANALYSTS

[KuppingerCole](#), in its 2019 Leadership Compass, identified Ubisecure in the follow categories: Identity APIs (challenger); Access Management and Federation (challenger); Consumer Authentication (one to watch) and CIAM platforms (one





to watch). It has also rated Ubisecure positive across the board in security, functionality, integration, interoperability and usability.

[Read KuppingerCole's full report on Ubisecure's Identity Platform here.](#)

KuppingerCole analysts also awarded Ubisecure the Best Consumer Identity Project alongside our customer, Telia Company, at the European Identity & Cloud Awards 2019.

## DEPLOYMENTS

Ubisecure's Identity Platform can be deployed in a subscription (billed monthly) or a perpetual license (one-time capital investment) model. While the majority of our customers are trending towards a subscription model, we also support a perpetual license with our private cloud and on-premises deployments.

The deployments are summarised in the diagram below, showing 'who manages what' under an IDaaS, private cloud (Identity Cloud) and on-premises (Identity Server) deployment.

— IF YOU NEED ANY FURTHER EXPLANATION OR HELP COMPARING THE DEPLOYMENT MODELS, DO NOT HESITATE TO [CONTACT US.](#)

UBISECURE IDENTITY PLATFORM		
IDaaS	IDENTITY CLOUD	IDENTITY SERVER
Software-as-a-Service	Platform-as-a-Service	On-Premises
Applications	Applications	Applications
Data	Data	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
O/S	O/S	O/S
Virtualisation	Virtualisation	Virtualisation
Servers	Servers	Servers
Storage	Storage	Storage
Networking	Networking	Networking
EXTERNALLY MANAGED		INTERNALLY MANAGED

## Summary

---

CIAM can help you save costs by:

- Avoiding a costly data breach
- Avoiding regulatory non-compliance fines
- Lowering support desk costs
- Increasing operational efficiencies throughout your business
- Growing with your business, rather than holding it back

CIAM can help you increase your revenue by:

- Retaining customers and increasing upsell potential/average revenue per customer (ARPC) with an exceptional customer experience
- Converting new customers with easier sign-up and better sales and marketing intelligence
- Creating additional revenue streams

It is almost always less risky, and more cost-effective in the long term, to utilise an existing proven, and well supported CIAM solution versus building it in-house.

Ubisecure will help you achieve CIAM excellence, as it has done for other organisations across multiple verticals for almost two decades.

Which Identity Platform deployment method you choose (IDaaS, cloud or on-premises) will depend on your individual requirements. Ubisecure offers all three.

## Further resources

---

Case Study – [the Finnish government's nationwide identity solution \(Katso\)](#)

White Paper – [Build vs Buy: CIAM](#)

White Paper – [CIAM for Customer Experience and Marketing](#)

Report – [Ubisecure Identity Platform by KuppingerCole April 2019](#)

**Find more resources and case studies [here](#).**

## Get in touch

---

If you have any questions about your IAM investment, Ubisecure is happy to help.

[sales@ubisecure.com](mailto:sales@ubisecure.com)

[www.ubisecure.com/contact](http://www.ubisecure.com/contact)

## About Ubisecure

Ubisecure provides feature-rich customer identity management software and services to help companies reduce identity data breach risk, improve operational efficiencies, and improve user experience.

The company provides a powerful Identity Platform, deployed as IDaaS, Cloud, or on-premises software. The platform consists of productised Customer Identity & Access Management (CIAM) middleware and API tooling to enable single digital identity benefits across multiple applications. Capabilities include enabling complex authorisation and delegation workflows, single sign-on (SSO), frictionless multi-factor authentication (MFA), user identity management, and pre-established connections to dozens of third-party identity providers (social, mobile, and verified).

Ubisecure's Right to Represent is a representation governance solution offering a fast and easy way to assert and verify an individual's mandated rights to electronically represent their company, including financial, signatory, or other authority. Ubisecure's widely used Delegated Authority solution allows individuals and organisations to manage which users and organisations can act on their behalf to dramatically reduce costly, time consuming and delay-prone manual workflows.

Ubisecure is accredited by the GLEIF to issue Legal Entity Identifiers (LEI) under its RapidLEI brand. RapidLEI is a cloud-based service that automates the issuance and registration of these highly assured organisation identifiers.



[www.ubisecure.com](http://www.ubisecure.com)  
[sales@ubisecure.com](mailto:sales@ubisecure.com)

### UBISECURE UK

The Granary, Hermitage Court  
Hermitage Lane, Maidstone  
Kent, ME16 9NT, UK

### UBISECURE FINLAND

Vaisalantie 2  
FI- Espoo, 02130  
Finland

### UBISECURE SWEDEN

Blekhölmstorget 30 F  
111 64 Stockholm  
Sweden

### UBISECURE DACH

Franz-Joseph-Str. 11  
80801 Munich  
Germany