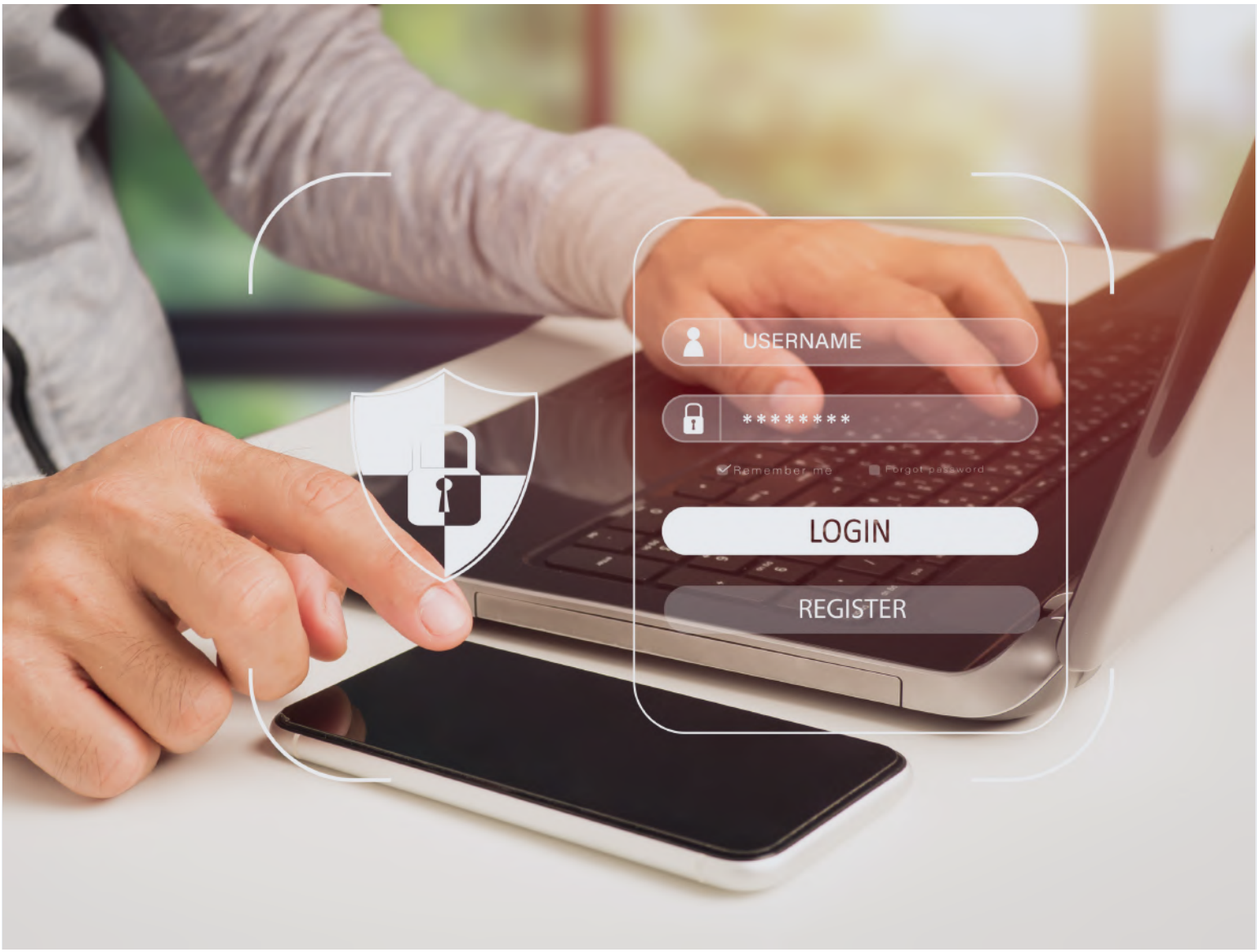
OPTIMAL IdM
Identity & Access Management

THE BEST THING

You Can Do for Your Customers That They'll Never Notice

Transform Access into a Competitive Advantage with Customer Identity Access Management



Background:

Your employees are a captive audience. You want them to have a good user experience, but nobody's going to quit because they don't like logging into the corporate network.

Your customers are another story. If logging in is too slow or cumbersome, if the signup process doesn't instill confidence, if a lack of self-service features forces customers to open a ticket every time they want to make a change, or if they have to re-authenticate every time they switch devices, they will take their business to a company that gives them the experience they desire.

Identity isn't getting any easier *Customer Identity Access Management (CIAM)* **is a specialized form of** *Identity Access Management (IAM)* **that is purpose-built to solve the unique challenges associated with customer-facing systems.**

CIAM addresses issues around customer expectations, performance and scalability, customer data integration, fraud prevention, and security. Unlike IAM, which is internally focused, CIAM is designed from the ground up to please customers and control access in a way that is transparent, customizable, and secure.

Why CIAM?

An enterprise has a limited number of users, usually maxing out below 300,000. A retailer, on the other hand, may have millions of users who log in from multiple devices. Providing access at this scale requires a different approach than traditional IAM.

Many companies are still using IAM solutions to provide access to their customers. This is a missed opportunity. While IAM is great for provisioning users, managing access rights, and performing other security-related functions, it doesn't deliver the level of self-service capabilities expected by customers, incorporate anti-fraud capabilities, or integrate with the variety of systems a retailer, government agency, SaaS, or other consumer-facing organization needs to orchestrate the sophisticated user experience customers expect today.

Some companies that recognize the need for CIAM have built proprietary solutions in-house. But homegrown CIAM tends to be riddled with security gaps, for several reasons: first, developers are not security experts. Second, the threat landscape evolves at a breakneck pace that is impossible for anyone other than devoted security professionals to keep up with. And third, companies relying on homegrown solutions are not likely to conduct penetration tests and vulnerability scans with the frequency or depth that they should. In addition, maintaining a homegrown solution requires staff that possesses deep knowledge of the discipline, and these people are hard to attract and retain.

As digital transformations push security and operational functions to the cloud, it is logical to extend that business model to include identity access management as a whole and CIAM in particular. Cloud-based CIAM relieves businesses of the need to update their software, fortify their solution against new threats, worry about building and securing API connections, and the many other tasks associated with controlling access when the userbase is unknown, large, and dynamic.

What's Important to Your Customer?

CIAM isn't really about password management or access security. It's about how a customer makes a purchase, and how they feel about the company they are buying from.

Customers want a frictionless experience that they don't have to think about. If they switch from their laptop to their phone to their car's onboard technology mid-purchase, they expect their session to be persistent. If they are transferred to a third-party service during a session, they want their authentication and profile information to travel with them. They want to change their own account details without having to contact tech support, and they expect every transaction to be fast and reliable at any time of the day or night. They feel good about companies that meet these expectations and are eager to do business with them again. And people who are happy with a business tell an average of nine people about their positive experience – while unhappy customers tell 16 people about a negative experience.

A customer journey involves many systems: order fulfillment, customer feedback, payment processing, etc. A CIAM should integrate with these systems but should also allow the business to control how the information it shares with third party providers and even with separate internal systems. For example, if a retailer's CIAM offers single sign-on (SSO), the retailer should be able to configure which customer information will travel with the SSO.

The future of CIAM is moving toward dynamic profiling. Retailers want a lot of information about their customers, but customers want to start shopping. Asking for too much information upfront can drive a customer away.

Dynamic profiling is a way to incrementally gather more information about a customer throughout their relationship with the retailer. For instance, a new customer might receive a welcome email that asks them for their mobile number and explains why this information will make the customer's experience better. The next time the customer visits the site, they may see a banner that asks for a thumbnail photo or for feedback on a new feature. The more information the retailer has, the more personalization they can deliver, and the more insights they can gain about their customer base.

73%

of customers say a good experience is key to brand loyalty.

-PWC

84%

of companies that improve their customer experience report and increase in revenue.

-IT World Canada

57%

of consumers rate control over which of their private data is shared as the most improtant factor in choosing who to do business with.

- EY Global Consumer Privacy Study 2020

AI-Powered Threat Detection and Blocking

The OptimalCloud™ uses AI, a machine-based learning system, to continuously detect and block hacking attempts on public-facing websites. Businesses can block IP addresses and entire geographic regions and can view hacking attempts against their organizations at any time through their dashboards. The information collected by the OptimalCloud CIAM is useful in forensic investigation and litigation.

This data can also automatically be shared with SIEMs to enrich the feeds to the security stack, and events like user profile changes can automatically be shared with other internal systems using the OptimalCloud's rich API library. Optimal IdM also maintains a massive library of vulnerabilities that is used to keep the OptimalCloud CIAM up to date on the latest threats.

Fight Fraud

When security teams think about access, they think about preventing unauthorized access. When consumer-facing businesses think about access, they also must think about fraud. The retail industry has a continuing problem with fraud detection, so much so that the cost of fraud is priced into their business models. CIAM helps prevent fraud by continuously authenticating users across multiple sessions and providing insights that can be used to detect patterns common to fraudsters.

Fraud and security are often separate departments entirely, with fraud focused on loss prevention and security focused on network security. For instance, in the banking industry, fraud prevention officers work on internal fraud issues around procurement, contract rigging, etc. They do work with external issues such as identity theft but typically this effort is focused on new customers. The authentication of existing customers tends to be the responsibility of the cybersecurity team.

Breaking down these silos can help prevent fraud and separate friendly fraud from true fraud. For instance, the data collected by the CIAM can be used to determine if the potential fraudster is customer or is a malicious actor from outside. This knowledge can shorten the investigation cycle and free up the fraud prevention team to work on other initiatives. Likewise, if the cybersecurity team can put the data captured by the CIAM into the central fraud system, the ROI on CIAM will be greater and more insights can be gleaned that will help a business reduce its losses and build more fraud-resistant systems moving forward.

CIAM can detect fraud in several ways. Behavioral biometrics, for example, allow businesses to look beyond credentials to gather data about how a user is interacting with a retailer's systems. A piece of code embedded in a webpage or mobile app records the ways a user interacts with the interface, such as how a user is typing, if they're using a mouse or a trackpad, how quickly they are moving the cursor across a screen, how they are clicking on buttons, and even the angle at which they are hitting keys on their keyboards. This information can be used to detect whether the user who logs in is always the same user, if a session was hijacked by a fraudster after legitimate credentials were entered, or if a synthetic user attack is underway. A synthetic user attack is a type of fraud in which criminals combine real and fake information, such as names, addresses, and dates of birth, to fabricate a fictional identity that they use to make purchases, resulting in $20 billion in losses to US financial institutions in 2020.

Synthetic identity fraud cost US financial services businesses $20 billion in 2020.

-Dark Reading

Voice identification is an emerging type of adaptive authentication that can identify a customer in less than 2 seconds and can also pick up on audio artifacts, such as background noise, to determine the likelihood that a customer is who they say they are. Checks can be conducted continuously on both live and IVR calls throughout a session to determine if a call has been hijacked, for instance by noticing if the caller's voice seems to become synthetic or if the device the caller is using has suddenly changed. This technology that uses machine learning and deep neural networks is transparent to the customer and is unlimited in the number of concurrent sessions it can monitor.

How the OptimalCloud CIAM Helps Prevent Fraud

When customers self-register, the OptimalCloud CIAM looks for known fraudulent IP addresses and email addresses. Businesses can block geographic regions and integrate their OptimalCloud CIAM solution with Lexis/Nexis (or similar services) for identity verification. And if an IP address is unexpected, the OptimalCloud CIAM can force multi-factor authentication and notify the customer by email as well.

Solve the Password Problem

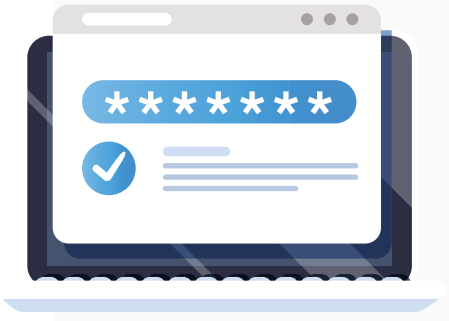
Passwords continue to present challenges. Customers are particularly prone to re-using passwords when they register with consumer-facing sites because they are not that worried about anyone seeing their shopping history, while businesses relying on homegrown identity access management may not be encrypting their passwords, may not be encrypting them properly, or may be storing them in databases – all highly risky practices.

Passwords should not be reversible. A reversible password is encrypted, but the encryption can be easily decrypted. From a hacker's point of view, a reversible password is as easily stolen as a password stored in clear text.

CIAMs that offer passwordless authentication deliver an even higher level of security. Passwordless authentication replaces or augments passwords with other authentication methods, ideally allowing customers to choose which methods they prefer. The most popular passwordless methods include:

One-time passwords (OTP) are unique codes sent to a customer's phone or voicemail. They are typically used as part of a multi-factor authentication (MFA) process in conjunction with a traditional password. OTPs may be sent to a user's device via text message, in which case the customer must enter the code into a login screen, or the OTP process may require the customer to open an authentication app to access the code, which they can then confirm directly from the app. The app may be a commercial solution, such as those offered by Google and Microsoft, or it may be proprietary to the retailer, such as Adobe Account Access.

Time-based One-Time Passwords (TOTP) are OTPs that expire within a specific amount of time. The CIAM should provide businesses with the



Biometrics and Device Authentication: Biometrics authenticate users on their mobile devices through fingerprints or Face ID. This method matches the user to the device itself, rather than matching the user to the resources the device is accessing. The retailer's system recognizes the device, the device recognizes the user, and the retailer's system trusts the device to handle the authentication on its behalf. Because the biometrics are stored on the device and never on a central server, this type of authentication makes a large scale attack impossible.

Social Media Sign-On lets users sign on with the credentials they've already established with a social media platform. Social sign-on relieves friction at the point of registration and leads to far fewer failed login attempts. It also can provide retailers and their marketing teams with a great deal of information about their customers, such as demographics and interests, which can then be used to deliver a more personalized experience. However, the success of social sign-on is largely dependent on the age of the customer base, with older customers less likely to use it due to concerns around privacy and data sharing.

OptimalCloud CIAM Makes Passwords Unhackable

Passwords on the OptimalCloud CIAM cannot be hacked because they're not reversible. We can't even access them ourselves.

Businesses can mix and match from many authentication approaches, including device authentication using FIDO2, social sign-on, OTP, TOTP, and of course, SSO and MFA. Customers get the experience they desire, and they change their authentication preferences at any time.

Learn to Love an Unexpected Influx

Traditional IAM handles known levels of scale. There may be a bump in activity on Monday mornings or the end of each quarter, but the spikes are predictable and have an upper limit. Consumer-based businesses lack the luxury of such predictability. While a company may expect a massive surge around Black Friday, it cannot know for certain just how large that surge will be. And some surges are completely unexpected, such as when a popular social media influencer links to the brand and a few million of their followers click on the link. That should be a good thing, but if it causes the system to crash, it's a disaster.

A CIAM must be able to accommodate large unexpected spikes of users without any lag or outages. Spikes are handled by scaling vertically or horizontally. Vertical scaling adds more computational power to the servers handling authentication, while horizontal scaling adds more servers. CIAM systems only experience peak loads in short time periods, a matter of days or – more typically – hours. In between those bursts, the systems are not called upon and resources are wasted. Businesses running CIAM in-house must bear the cost of this idle time, as well as the cost of spinning up servers and allocating the expertise necessary to make that happen. Cloud-based CIAM takes that load off the business and shifts it to the solution provider, whose core business is making sure that authentication is executed with speed, accuracy, and security.

Failover and redundancy are also essential to a successful customer experience, as well as to ensure business continuity. A CIAM should have data centers located near the customer base and be able to provide duplicate services in multiple locations.

The OptimalCloud CIAM Is Priced on Scale, Not Usage

Your cost depends on the number of servers or data centers you are using at the current moment, not the number of users you expect over the billing period. This saves you money because you only pay for the services you use.

Not sure what your needs are? OptimalCloud CIAM experts can make recommendations based on your current use, predicted growth, and expected logins per day. You get data centers that are located near your users and can locate them in the way that best supports disaster recovery and business continuity for your unique business model.

Your CIAM Checklist

Customer-Facing Must-Haves

- [ ] Allow customers to self-register
- [ ] Allow customers self-service capabilities
- [ ] Allow customers to manage consent and preferences
- [ ] Offer single sign-on, multi-factor authentication out of the box
- [ ] Offer passwordless authentication out of the box
- [ ] Enable seamless, frictionless customer privacy and consent management

Technology Must-Haves

- [ ] Integrate with identity verification (IDV) solutions
- [ ] Integrate with the security stack
- [ ] Integrate with non-synchronizing virtual directories
- [ ] Ease management with a single pane of glass
- [ ] Scale to large numbers of users in both technology and price
- [ ] Enable customization so the solution fits the business instead forcing the business to fit the solution

Contact us at info@optimalidm.com or learn more at www.optimalidm.com
WHITEPAPER

Getting Started with the OptimalCloud CIAM

The OptimalCloud CIAM is a fully managed systems for all customers. You never have to worry about managing, deploying, and updating servers and software – that's all handled for you. Just let us know how many servers you want and what your business rules are. Even if you have a complicated environment, you can still be up and running at a speed that will surprise you.

You can set up SSO on your own or choose to have the experts at Optimal IdM do it for you. And you can customize your OptimalCloud CIAM solution as much as you wish, either through self-service via your dashboard or with the help of our customization team. The OptimalCloud CIAM is flexible enough to meet your needs, a capability that other CIAM providers do not deliver.

The OptimalCloud CIAM also offers the industry's only non-synchronizing virtual directory. This means you can access more customer identity data in real-time, no matter where the data exists, without having to set up a separate master database. Instead, you store your customer identity data however you like: in SQL, multiple AD forests, ADLDS, ADAM, LDAP, and more. You and your customers get immediate and safe access to query, find, and edit information directly – no data migration necessary.

Give your customers a seamless, omnichannel, secure authentication experience today. They won't notice how frictionless their authentication experience was – and that's exactly what you want.

Book Your Demo Now

at sales@optimalidm.com