THE TOP 5 REASONS YOU NEED A

Customer Identity and Access Management (CIAM) Solution

EBOOK

onelogin

Introduction

In order to stay competitive and build trusted experiences with your customers in today's hyper-connected landscape, digital transformation initiatives have climbed to the top of the list for many IT organizations. And the current COVID-19 pandemic has accelerated this trend even further. As an example, with people sheltered-in-place and unable to frequent their favorite brick-and-mortar stores, consumers have turned to online shopping in droves.

The United States, for example, has seen an increase of 63% in e-commerce activity when comparing even a week's worth of transactions in early July of 2020 to July of 2019 (pre-COVID). Some countries, such as Mexico, have seen a 200% increase over the same time period according to COVID-19 Commerce Insight. And even though the world is slowly opening up, we expect this change in consumer purchasing habits to remain for the long term.

Plus, as a result of shelter-in-place mandates, non-ecommerce consumer-facing businesses are trying to figure out how to be successful online–like restaurants, repair shops, doctor offices, government services, and more. Restaurants are providing online sites and mobile apps for ordering food to go. Repair shops are implementing online reservation systems that give you the ability to schedule a time for the repair and drop off with minimal physical interaction. Even in the world of medicine, an online presence has become crucial. "Forrester now predicts that virtual care visits will soar to more than 1 billion this year, including 900 million visits related to COVID-19." The examples are endless. Companies who do not accelerate their move online and prioritize their digital presence will simply struggle to survive.

But the more your organization focuses on developing that perfect digital customer experience, the more open you become to data breaches and hacks. You need to ensure that your consumers can log into your digital channels easily and securely.

You don't want a headline like this tied to your business- ***Nintendo: 160,000 Accounts Hacked or Sino Weibo, China's Equivalent to Twitter, exposedpersonal data from over 500 million users.***

In order to keep your customer's data safe from bad actors, you need to implement a Customer Identity and Access Management (CIAM) Solution to increase your security posture while ensuring your customer experience remains seamless.

In this ebook, we discuss five critical use cases for Customer Identity and Access Management:

- Replacing a legacy identity solution that is vulnerable to attack and is unable to meet usage demands
- Replacing an existing homegrown identity solution that is too costly and time-intensive to maintain
- Developing a brand new application or service that needs to be secured
- Securing your customer's identity and access with Multi-Factor Authentication (MFA)
- Securing your customers with an identity solution that can scale with user activity

What is a CIAM Solution?

A Customer Identity and Access Management (CIAM) platform, like OneLogin's Trusted Customer Experience (TCE), provides a secure and seamless solution to protect your customer identities from devastating breaches without sacrificing user experience. CIAM solutions control a customer's access to resources, such as an application or content. Whether your customers are purchasing a product or service, looking at educational resources, consulting with a doctor online in order to be diagnosed, or just streaming a hit musical, a CIAM solution provides a simple and secure way to register and/or reset their passwords when necessary.

The Importance of a Secure, Seamless and Customizable Login Experience

A CIAM solution provides an easy way to implement Multi-Factor Authentication (MFA). This enables your business to determine what type and how many factors you want to require when a customer logs in. Examples of common factors include an SMS text message, an email verification, a security question, etc.

Taking this concept one step further, a solution like OneLogin's TCE, leverages machine learning as a critical component to MFA. In other words, your MFA solution can learn a user's habits to determine whether or not a login attempt is high risk.

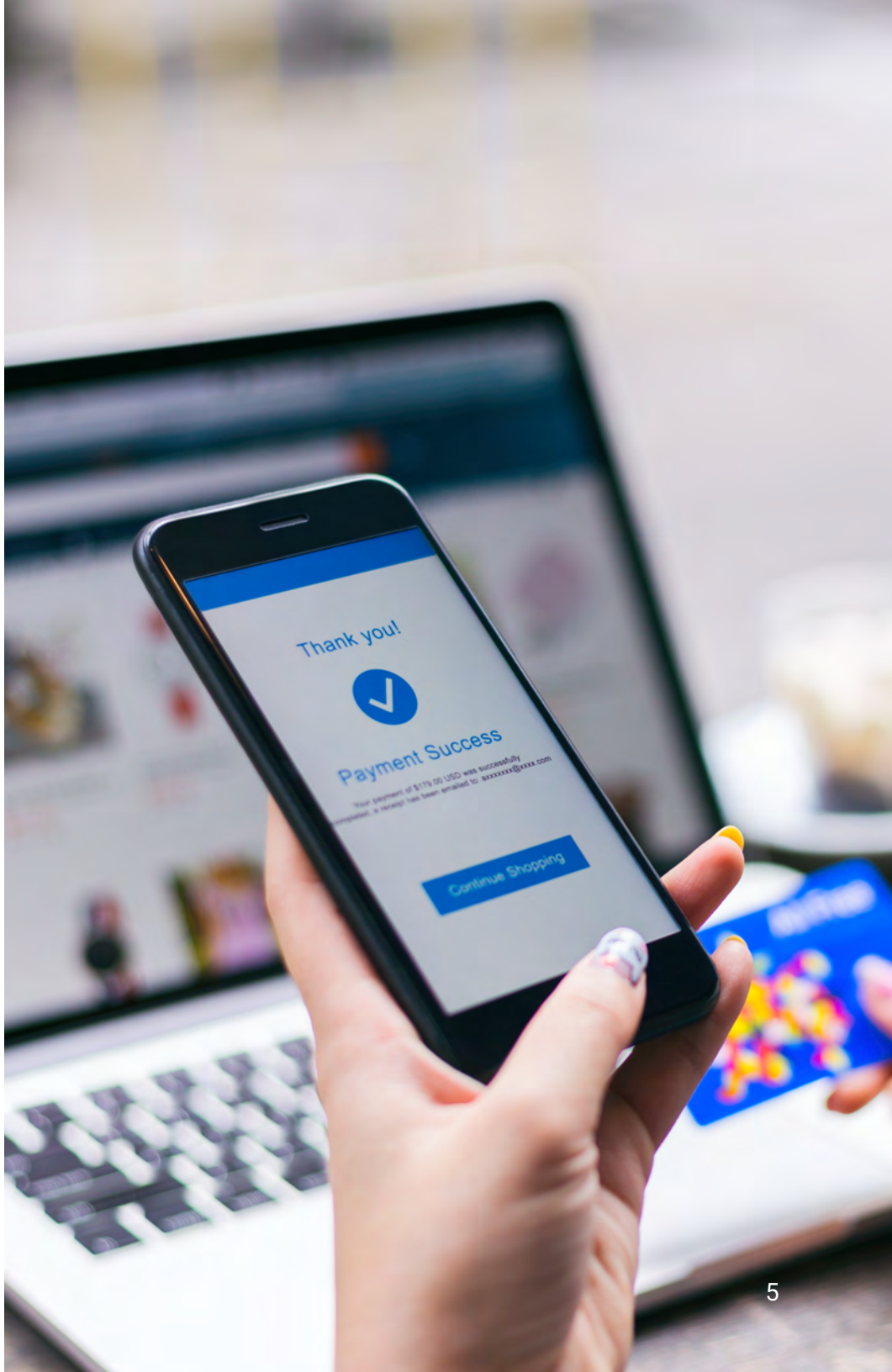
For instance, if your customer typically logs into your application from a specific IP Address and all of a sudden it appears that same customer is logging in from a completely different IP Address across the country, an adaptive MFA solution can automatically prompt the user for additional factors to verify his or her identity. Conversely, if a customer's login attempt appears very low risk, the system can remove authentication factors, making the user experience more seamless.

Additionally, your CIAM solution should also check to make sure that users aren't reusing credentials that have already been hacked and are for sale on the dark web.

Most Common CIAM Use Cases

Now that you understand what a CIAM solution, like OneLogin does, the next step is to determine what your specific needs are. Questions to ask yourself are–do you need to add an additional layer of security to your customer-facing applications to ensure that their data is safe from bad actors? Or, perhaps you have a legacy identity management solution that needs to be updated in order to secure your customers with modern security protocols? Or, maybe you are building a new application and need a seamless way to add security via API?

Let's take a look at some common CIAM use cases that may apply to your organization.



Use Case 1:

You Need to Secure Your Customer Identities Without Impacting User Experience

One of the most common reasons to implement a CIAM solution is the need to secure data and to verify the identity of your customers when they log into your system or website. This use case is based upon security concerns.

Let's take a look at this example. B. Crusher, Inc. recently paid for a security audit of their online telemedicine service and found there were a few holes in their existing legacy identity system. If their user accounts get hacked their business will be devastated, not only because users will lose confidence in B. Crusher, but they will also be in violation of a multitude of healthcare compliance regulations that they need comply with.

B. Crusher is looking for a solution that provides:

- A secure cloud directory with modern authentication options such as MFA or passwordless authentication.
- A login experience that doesn't impact customers.
- Extra security measures, such as doing a compromised credential check.
- A way to secure all endpoints and APIs.
- OIDC and SAML support to securely authenticate users against supporting applications that are integrated into the system.

By implementing a solution, like OneLogin's Trusted Customer Experience, B. Crusher, Inc. can ensure that their patients can log in securely and are prevented from using credentials that might have been hacked from another site. Plus, by leveraging a CIAM solution that uses context-aware machine learning for authentication, B. Crusher, Inc's customers can have a more seamless, passwordless user experience.

With OneLogin's TCE customers can choose what type of additional authentication factor they want to use, for example, a text message, a push notification on their phone, or even a voice call. They will not be constrained to only one choice, like email, which can sometimes be slow. Every endpoint can be secured, including their API endpoints. Most importantly, B. Crusher, Inc. doesn't have to spend time and money attempting to do all of the security "heavy lifting" themselves.

Quark and Co.

Use Case 2:

Your Homegrown Identity Solution is Too Costly and Lacks Built in Modern Security Best-Practices

This is probably one of the most common scenarios that we see. While a homegrown identity solution may have been good enough when it was initially developed, adding new features can be incredibly costly and resource intensive.

Quark and Co. has 3 million customers that use their e-commerce site to purchase Quark's Quenching Drinks. Quark and Co. got into the e-commerce game years ago and developed their own ecommerce platform, including a homegrown identity solution. Over the years, they have realized it is harder and harder to maintain their existing identity solution; they only have one administrator on staff that even understands how the system works.

They want to implement a Multi-Factor Authentication (MFA) solution that provides a variety of authentication factors. And ideally, they want to build in a passwordless option to make the login experience even easier. The cost to overhaul their existing system will be exorbitant and, with a lack of experts out there that understand the system, modifying the existing identity solution seems almost impossible. Quark and Co. needs to find an alternative fast.

To quickly solve this issue they decided to purchase a new Customer Identity and Access Management system that is less costly to maintain, less resource intensive, and comes complete with all of the modern security protocols customers expect. Plus, Quark needs to ensure that their chosen CIAM solution can migrate users quickly and easily.

Quark is looking for a solution that provides:

- A cloud directory they can rely on to securely authenticate their users.
- A quick way to migrate their users without a huge impact to user experience.
- Modern authentication options, such as different MFA factors and passwordless authentication.

OneLogin's TCE solution provides a way to quickly migrate users from your existing identity solution, so your customers' experience is not impacted. Additionally, you can take advantage of a multitude of features that can make your user experience easier, such as a choice of MFA factors, implementing a passwordless experience, or leveraging AI-powered MFA that provides a contextual way to automatically update authentication based on behavior.

THE ORION INSTITUTE
OF COSMOLOGY

Use Case 3:

A Brand New Application or Service is Being Developed and Needs to be Secured

The third use case for a CIAM solution focuses on the development of a new application and the need to secure users in a way that is seamlessly embedded in the app.

The Orion Institute of Cosmology (OIC) has been working on an online remote learning system to serve their learners. They need a user directory for their students that will not only be incredibly secure, but it also needs to be reliable. OIC needs an identity platform that can scale as their student body expands. However, OIC realizes that developing their own CIAM solution to embed in their application will be costly and time consuming to maintain since they will consistently have to protect themselves against new security threats.

They have decided to look for a CIAM solution that their developers can utilize as the identity platform for the online learning system they are already building.

OIC is looking for a solution that provides:

- A scalable and reliable cloud based user directory.
- API access management which will secure access to their API endpoints.
- Support for standard protocols like OpenID Connect (OIDC).
- Support for social sign up and sign in.

OneLogin's Trusted Customer Experience provides a strong OpenID Connect (OIDC) offering to complement your modern application development. With TCE you can integrate with the authentication systems your users might already belong to such as social media websites, Yahoo, Google, etc. Because of OneLogin's fully developed RESTful API, the platform has the ability to work with any type of digital channel you are developing. And, most importantly, OneLogin provides users with a variety of MFA choices, a self-service password reset process, and full branding functionality.

Use Case 4:

You Need to Secure Your Customer Identities Without Impacting User Experience

This use case involves migrating away from an existing identity solution. However, in contrast with our previous use cases, the migration is motivated by a recent burst in traffic to the website that the current CIAM solution was unable to handle.

Nelix, an online streaming service, has designed their streaming platform to increase resources with customer demand, but their login system was not designed to meet this requirement. Nelix recently got the exclusive rights to stream “Starington”, a popular musical, and their customers were so eager to watch it when the movie released that they all logged in at the same time and Nelix’s identity solution crashed. This obviously resulted in a lot of very angry customers. As a result, Nelix is looking for a CIAM solution that is designed to scale with their needs, thus preventing this type of outage in the future.

Nelix is looking for a solution that provides:

- Load scaling and the ability to expand or contract to meet heavier or lighter loads.
- A seamless and secure login experience for their customers.
- An easy way for developers to integrate with the existing system.

The ability to load scale is crucial in this use case. As user login activity increases the platform needs to spin up resources, like additional servers, to handle the load. Your user experience needs to be your highest priority and if they can't log onto your service trust and revenue is lost. You need a platform that meets your customer demands, won't cause outages, integrates easily, and provide the level of security that your customers need.

Use Case 5:

Find the Perfect Piece that will Fit into Your Solution

This last use case is usually driven by developers. Bok'Nor Shipping wants to keep their system secure and improve their end user experience. They have an existing identity solution that they recently developed and do not want to migrate away from it at the moment. However, they do want to implement MFA for their online package tracking system.

Bok'Nor has scoped out the cost of developing their own MFA solution in house and have determined that it would be too costly, especially because they want AI-powered adaptive authentication. Plus, they don't want to allocate any additional resources for more software or servers. Instead, Bok'Nor is looking for a cloud-based service that can easily integrate with their other cloud-based applications.

Bok'Nor is looking for a solution that provides:

- A rich set of APIs that are easy to integrate with and secure.
- A flexible set of APIs that they can customize to fit their MFA needs--in this case, adaptive authentication.
- A reliable cloud-based solution.

OneLogin's Trusted Customer Experience platform is a highly flexible, API-first CIAM solution. So instead of being stuck with out-of-the-box functionality, you can customize your solution based on your unique customer identity needs. For instance, just like Bok'Nor, you might want AI-powered authentication for a passwordless experience or maybe you want to ensure support for standard authentication protocols like OIDC or SAML. With OneLogin's platform you have the ability to choose exactly what you need.

Questions to Ask

No matter what scenario fits your use case, you need to ensure that your chosen CIAM solution covers off on several main buckets of functionality. In this section, we go over the top four functionalities you should look for and questions you should ask.

Registration and Usage

Look at how your user accounts are created:

- [ ] How are your users registering?
- [ ] How many users are you managing?
- [ ] Most importantly, how many users are actively logging in and how often are they logging in?

Storage and Security

The whole point of a CIAM solution is to ensure that your user data is secure. Ask yourself:

- [ ] Where is your user data being stored after they have registered?
- [ ] What type of data are you storing and are you meeting compliance requirements in regards to how the data is stored?
- [ ] How are your users currently authenticating in order to get access to their data?
- [ ] How are you authenticating against APIs?

Functionality Needed

Your CIAM solution should provide you with choices that fit your needs and your vision of what your consumer experience should be like. Ask yourself:

- [ ] Exactly what kind of functionality do you need?
- [ ] Do you need MFA?
- [ ] Do you want users to have a choice between multiple MFA options–such as a choice between email, SMS or, an app on their phone?
- [ ] Do you want AI-powered context aware authentication that adjusts automatically based on login risk?
- [ ] Do you want to be able to deny access to logins if they are coming from certain geographical regions or prevent users from reusing credentials that might have been compromised already?
- [ ] Do you want to integrate with other authentication directories, like Active Directory?
- [ ] Do you want users to seamlessly reset their own passwords?
- [ ] Do you want to use industry best practice and adopt standards like OpenId Connect?

Application Access

Assess how many different applications your users need to access:

- [ ] Is there just one application that your consumers need access to or are there multiple applications that they are accessing behind the scenes?
- [ ] Are these applications homegrown or are they third party applications?
- [ ] Do they support SAML or OIDC authentication?

Conclusion

Customers around the world are turning to online solutions for all their needs: retail, medicine, learning, entertainment, communication,and more. This massive migration from in-person to online interaction has been increasing over time, but with COVID-19 we are seeing an unprecedented amount of online activity.

Every company and organization needs to have a secure digital channel for customers to interact with your brand. Above all else, you need to ensure that your customers trust your business with their information and without their fear of being hacked. Remember, if a customer sees your organization's name in the headline associated with a huge data breach, you will quickly lose loyalty and revenue.

You need a CIAM solution you can trust, that is reliable, is easy for your developers to integrate with, and does not impact user experience. You want the ability to implement features such as MFA, compromised credential check, adaptive authentication, passwordless authentication, OIDC/SAML integration, and more. Developing and maintaining homegrown identity solutions to support these features is too expensive and risky. You need to find a system that can do the job for you; you need a Trusted Experience Platform.

About OneLogin

OneLogin is the identity platform for secure, scalable, and smart experiences that connect people to technology. With the OneLogin Trusted Experience Platform, customers can connect all of their applications, identify potential threats, and act quickly. Headquartered in San Francisco, CA, OneLogin secures over 2,500 customers worldwide, including Airbus, Stitch Fix, and AAA. To learn more, visit www.onelogin.com.