The Top Four Things to Look for in a Customer Identity and Access Management (CIAM) Solution

onelogin
by ONE IDENTITY

Introduction

No one wants their company to make headlines like “80,000 Company X Accounts Compromised in the Latest Breach” or “Three Billion Company Y Accounts Stolen in the Past Year.”

Whether your company has an ecommerce website, most organizations have online resources, such as a website or applications, that customers need to log in to. And unfortunately, it is through insecure access or poor password hygiene that credentials are stolen and company data is breached.

In a world where threat actors are constantly trying to exploit vulnerabilities, you need to ensure that your customer online experience is secure. By providing a way to authenticate with Multi-Factor Authentication (MFA), and a simple and speedy way to reset passwords, you can protect both your organization and your customer’s data. How can you do this quickly and without depleting your budget? Let us introduce you to Customer Identity and Access Management (CIAM).

What is Customer Identity and Access Management (CIAM)?

Customer Identity and Access Management (CIAM) is the perfect answer to this problem. A CIAM solution focuses on managing customer identities and controlling customer access to a company’s online IT resources for customer interaction.

CIAM solutions provide all the functionality that you might find in your traditional AM platform through Application Programming Interfaces (APIs) that your developers can integrate into their code. As a result, your developers can focus on coding business critical applications instead of spending time developing homegrown secure login solutions, integrating MFA, and making sure users can reset their passwords. Your developers want to spend time innovating your product, not coding password reset emails.

Leveraging a CIAM solution helps ensure your company doesn’t end up in a series of breached credentials headlines. So, what should you look for in purchasing a CIAM solution? At One Identity, we believe our OneLogin CIAM solution needs to be:

- Simple
- Secure
- Reliable
- API-first

onelogin by ONE IDENTITY

Simple

A great customer experience drives growth, revenue and customer retention. Your CIAM solution should make the user experience as simple as possible for every touch point -- from registration, to password reset and beyond. When assessing a CIAM solution for ease-of-use, consider the following:

Self-service password reset/password-forget process

Your customers should be able to manage their passwords without help desk. Involving your help desk costs your company money and can cause frustration on the user's end. Although many companies do have an automated password-reset process, they are often slow and rely on email as the primary way of validating the user by providing them a link to a password reset page.

Unfortunately, password-reset emails are often slow and end up tagged as SPAM. When this happens, your customer can quickly become frustrated, abandon their cart, and still call your help desk.

A CIAM solution, like OneLogin by One Identity, **supports a self-service password reset process and provides a variety of authentication options** - not just email. For example, with OneLogin, you have multiple options such as voice, SMS and one-time password verification methods.

Secure

Security is the primary focus when it comes to managing customer identity. Your CIAM platform needs to provide secure login access and ensure that threat actors are unable to impersonate your users, and get access to individual accounts and corporate data. Your CIAM solution must have the following security features:

Multi-Factor Authentication (MFA)

Over the years, Multi-Factor Authentication (MFA) has become necessary to prevent threat actors from accessing user accounts. Adding the additional factor into the login process, such as a One-Time Password (OTP) or a fingerprint, helps ensure that it is your user logging in and not someone using compromised credentials. A CIAM solution should support MFA and provide various options for additional authentication factors, giving users and developers a choice that works for them. For example, some users might prefer a text message over email for receiving their OTP, or a developer might want to require a fingerprint for a specific app.

AI-Powered Authentication

One of the drawbacks of requiring MFA is that it can make the login process more cumbersome for customers. Users get frustrated when they have to go through too many steps to do something as simple as logging into an app. But your business also needs to ensure that those logins are secure. Adaptive MFA can solve this problem by learning about a user's typical behavior patterns: where they log in from, the time of day, the browser they use, etc., and suppress MFA if a user is following her typical patterns. By choosing a CIAM solution that provides AI-powered MFA, you can feel confident that your application is secure without your customer being burdened.

OneLogin has taken Adaptive MFA, also known as Adaptive Authentication, one step further with **SmartFactor Authentication™**. SmartFactor Authentication leverages AI to automatically provide several different options that are based on tracking typical user behavior. Our Vigilance AI engine tracks the user's behavior patterns and assigns that behavior a risk score based on how closely that user is tracking to her typical behavioral patterns. In fact, if the engine detects that your user behavior is outside the bounds of typical usage, SmartFactor can flat out deny the user access, adding an extra level of contextual security. Conversely, if your customer displays typical behavior and the risk score is low enough, that user may not be prompted for additional authentication factors - making the user experience seamless.

onelogin by ONE IDENTITY

Compromised Credentials Check

Many customers reuse the same username and password for multiple websites and applications. Unfortunately, this means that if one of those apps is breached, then those credentials are now out on the market for threat actors to find and use. A CIAM solution should provide a way to prevent customers from even using these compromised credentials in the first place, thus preventing this type of attack.

As an example, OneLogin keeps up a database of compromised credentials that have been made available by black-hat hackers. When a user sets their initial password, or even when a user resets their password, OneLogin compares the username and password combination to those in the database. If a username or password comes up on the breached credentials list, your customer will be unable to reuse that password. This prevents those with malicious intent from getting into the system by using the compromised credentials. Combining this feature with MFA provides an even higher level of security.

Compliance Standards

A CIAM solution should put security and compliance standards above all else. When you choose your CIAM solution, make sure that the system meets international, federal and state laws, as well as various government regulations.

OneLogin works diligently to make sure its platform is compliant with the various security and compliance standards that have been established in various industries and public institutions.

Reliable

A CIAM solution provides a crucial service to your customers and must be available when needed and respond swiftly to incoming requests. Make sure that your CIAM solution provides the following:

Reliability and Uptime

It is business-critical that your web application or mobile app is available to your users, even if some sort of outage occurs. If your app is down when a customer needs access, that customer will most likely go elsewhere. Any sort of outage can cost the company money, so developers need to know that the CIAM solution they choose provides the same, if not higher, standards of reliability. If your goal is 99-percent availability, then you would want your CIAM solution to aim for 99-percent uptime.

Our platform can withstand multiple regional disasters. Databases are not only backed up, but they are also replicated across regions. Because the database is replicated to several locations, your organization can rely on OneLogin.

Scalability

If your business booms (think Black Friday for an ecommerce website) and your application or website is accessed by hundreds of thousands, if not millions of customers, your CIAM solution must be able to scale as your customers increase. If they are unable to log into your application or website to make a purchase, you will lose customer loyalty and revenue.

onelogin by ONE IDENTITY

API-First

Because a CIAM solution needs to be embedded in your application, look for vendors who have an API-first approach to their product so your developers can customize the integration.

Flexibility through APIs

When looking for a CIAM solution, your developers are often an important stakeholder on the decision team because they are the ones building your applications and ensuring a seamless customer experience. When the development team is looking for a CIAM solution, they want a vendor that has taken an API-first approach to their product. An API-first approach means that priority in development of the platform goes to the APIs to ensure the APIs are consistent and reusable.

Our engineers work across product teams to ensure that all new functionality is developed with an API-first mindset. Often functionality is released before it is available in the main UI. This can ensure that your developers have time to test the functionality.

Developers Love CIAM Solutions!

Developers love CIAM solutions and you want to keep your developers happy. Developers want to focus on the functionality of the app. They do not want to worry about keeping up-todate with the latest Multi-Factor Authentication options. They want to do what they do best – develop innovative applications. They want a CIAM solution that provides a simple, secure and reliable login experience for customers.

Conclusion

Everyday it seems there's another headline reporting customer data breaches. When hackers steal credentials of users from one site they can make other sites vulnerable since many users reuse the same credentials for multiple sites. This makes features like MFA and Compromised Credential checks crucial in protecting your users' data. Developing and supporting these extra layers of security can be time consuming and costly. Now is the time to find a CIAM solution that you can trust to provide a simple and secure login experience to your customers.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500 million identities for more than 11,000 organizations worldwide.
For more information, visit www.oneidentity.com.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

eBook-OneLogin-CIAM-US-PG-74856

onelogin
by ONE IDENTITY