

Trusted Customer Experiences (TCE)

Deliver secure, seamless experiences for your customers

Today, businesses collect a multitude of customer data, ranging from an email address, to passwords, and other sensitive information. Protecting sensitive data is essential to building a trusted relationship with your customers. Implementing a Customer Identity and Access Management (CIAM) solution dramatically increases your security posture and ensures a seamless customer experience.

OneLogin Trusted Customer Experiences™

OneLogin Trusted Customer Experiences (TCE) provides a secure and seamless solution to protect your customer identities from devastating breaches without sacrificing user experience. Leverage a unified cloud directory to capture identities and authenticate customers via multiple methods (OIDC/SAML, Social Identity, Active Directory, and more). OneLogin TCE allows organizations to upgrade to the cloud from a homegrown or legacy system, bringing built-in single sign-on (SSO) and multi-factor authentication (MFA), without impacting end users.

KEY BENEFITS OF ONELOGIN TRUSTED CUSTOMER EXPERIENCES

Keep customer data safe from attacks

Implement modern security features, like MFA and biometrics, to prevent costly breaches that damage customers and destroy your reputation. AI-powered MFA streamlines real-time visibility into login attempts, enabling you to act quickly to address high-risk login events.

Create seamless and trusted digital experiences for customers

Ensure fast, convenient authentication so the first—and every—customer engagement is seamless. Provide a consistent, trusted login experience across all devices and applications, and eliminate friction during the sign in and registration process with passwordless authentication and Social Login.

Quickly migrate customers without interrupting the user experience

Easily implement modern security protocols without the significant investment to build in-house solutions. OneLogin works with your existing system to quickly migrate your customers without impacting their user experience.

Customize the experience with flexible APIs

Through OneLogin’s APIs, developers enjoy the flexibility needed to customize authentication requirements as they progress through the development process

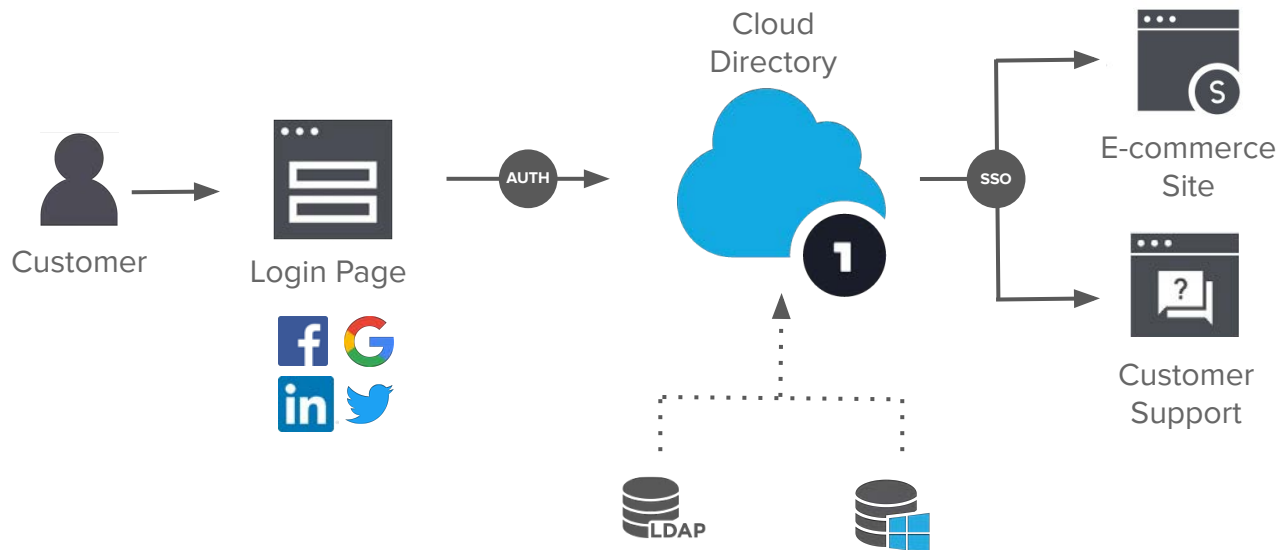
Ensure high availability & reliability at scale

Operate at the scale and speed your customers demand. When you leverage OneLogin for identity, you can feel confident in our 99.9% reliability and up-time.

“The most important things we were looking for when looking to purchase OneLogin were security and ease of use for all of our users. And we got that with OneLogin.”

TIM NALE | CIO, Bic Graphic

HOW DOES ONELOGIN TRUSTED EXPERIENCES WORK?



ONELOGIN TRUSTED CUSTOMER EXPERIENCES FUNCTIONALITY INCLUDES:

- **Cloud Directory**

OneLogin's unified cloud directory is a centralized identity store in the cloud. It can be a minimal directory that captures the necessary amount of profile data required to authenticate the customer—or enhance with data from different sources. Use it as the store for customer identities or synchronize with LDAP and Active Directory (AD) through our pre-built integrations.

- **Single Sign-On (SSO)**

OneLogin uses the SSO protocols SAML and OpenID Connect to allow customers to sign in to applications without using a password. Once authenticated, customers can access applications that have a trust relationship with OneLogin. If your online portal consists of multiple, discrete applications, customers experience a streamlined, seamless user experience.

- **Multi-Factor Authentication (MFA)**

When needed, enforce MFA for increased protection. Require customers to respond with a one-time password sent via text, push notification in the OneLogin Protect mobile app, or biometrics on their devices. Add adaptive authentication to take security to the next level by prompting customers for an additional factor when an abnormality is detected.

- **Social Login and Registration**

Easily implement Social Login and registration for your users. Allowing customers to sign in with their social identity (Facebook, Google, LinkedIn, etc.) removes friction and eliminates the need for users to create yet another password.

- **API Access Management**

Use OneLogin to authorize your requests against your APIs, enabling best security practices for protecting APIs that support single-page or native mobile applications.

- **Authentication and Administration APIs**

OneLogin's rich APIs enable developers to easily integrate OneLogin into existing applications to create secure user experiences, automate app roll out, and monitor security events.

- **Analytics**

OneLogin event webhooks are used to send login events and other user interactions to analytics tools, like SumoLogic and Splunk, for advanced threat detection.

To learn more about OneLogin TCE, visit <https://www.onelogin.com/product/ciam>