Making Passwordless Possible

Why your business should go passwordless, and how to give employees a frictionless login experience.

80% of breaches are still caused by weak or reused passwords, and 76% of employees experience regular password problems. When faced with the ongoing resource drain and security risks of passwords, what should IT teams do?

Why your business should go passwordless.

Eliminating passwords might seem impossible, but the right combination of technologies can remove password-related obstacles. But why should your business even consider moving beyond the password? Going passwordless offers several benefits to your organization:

Stronger security.

The risks of passwords – especially ones that are weak, reused, and poorly-managed – are well known. Nearly 80% of breaches caused by hacking feature the use of stolen credentials. When you remove passwords from the picture, you significantly reduce the possibility of a password-related breach.

Improved experience.

The average employee struggles to manage over 100 passwords, so it's no wonder that 59% of people mostly or always use the same password. Employees just want their technology to be fast and easy-to-use. Going passwordless means employees are connected to their work tools more quickly while eliminating time-wasting obstacles like lockouts, resets, and frequent password updates.

Greater control.

77% of employees use a 3rd-party cloud app without the approval or knowledge of IT and most (83%) IT professionals report employees storing company data on unsanctioned cloud services. In short, IT lacks visibility into employee access across the business and control over "Shadow IT". Technologies that replace or eliminate passwords give IT the oversight they need to make that visibility and control possible.

Lowered costs.

On average, IT security teams spend 4 hours per week on password management-related issues alone and receive 96 password-related requests per month. Legacy technologies managed and run in-house often come with a lot of overhead. Passwordless software solutions eliminate costly overhead, reduce needed manpower, and free up IT resources to focus on more value-add activities.

How to go passwordless.

Start by collecting passwords in one central place.

Part of the reason passwords continue to be such a challenge is that employees are left to manage them on their own. Start by giving employees an Enterprise Password Management (EPM) solution that captures and stores every single password in use.

Employees no longer have to worry about remembering credentials – the password manager fills them instead – and IT now has visibility into password hygiene for every login, for every user.

Passwords may not be eliminated yet, but employees must only remember one master password, so it's a big step in the right direction.

Where possible, replace passwords with other secure protocols.

Next, replace passwords with Single Sign-On (SSO). Using the secure protocol SAML 2.0, employees can then connect to their apps – whether cloud, mobile, legacy, or on-premise – without ever needing to store a password or fill a login form.

Pairing SSO with EPM ensures that employees still only have one password to remember and they can connect to many services without messing with passwords, while any credentials for form-based logins are automatically filled for them.

Eliminate passwords with stronger authentication.

The final step in achieving a passwordless experience is implementing Multifactor Authentication. Typically, Multifactor Authentication is seen as adding login steps – and it's true that one of the main goals is to add extra protection by requiring additional information (or "factors") to prove an identity.

But a modern authentication solution can combine biometric (human) factors like fingerprint ID and face scan with contextual (hidden) factors like device ID, geolocation, or IP address. These data points can be used to more accurately verify a user's identity. And, they can replace passwords, bypassing the need to enter a credential before unlocking an SSO and EPM portal or other service.

An all-in-one identity solution makes passwordless possible.

An identity solution that combines EPM, SSO, and MFA is an effective way for today's businesses to give employees a passwordless experience. Passwordless authentication means a better user experience, greater visibility and control for the IT team, stronger security across the organization, and less IT overhead. In short, it's a win-win for users and administrators.

For businesses looking to gain simple control and unified visibility across every entry point, with an intuitive access and multifactor authentication experience that works on everything from cloud and mobile apps to legacy on-premise tools, try LastPass Identity.

Learn more about unifying access and authentication with LastPass Identity:
www.lastpass.com/products/identity