

Passwordless: What it is (and why it's critical)

The frequency and severity of cyberattacks continue to be alarming – and costly. The good news? Passwordless authentication makes it much harder for cybercriminals to gain access through phishing, stolen credentials, and brute force attacks. Passwordless access also enhances operational efficiencies, especially amid growing requirements by IT and security teams for longer character passwords. Here's a snapshot of what it involves, and why it's so vital for organizations.

What it's about

Simply put, passwordless is focused on eliminating passwords for end users, and replacing them with more secure, user-friendly authentication methods. **In a nutshell, it's about simultaneously enhancing data security and reducing digital access friction for users**, especially those who may log in and out of systems and applications many times each day.



Each day

A user may log in and out of systems and applications many times each day.

Use cases

A big challenge faced by many industries is the complex range of use cases and devices users interact with on a day-to-day basis. That can include shared mobile devices and shared virtual desktops – plus cloud and legacy apps.

Passwordless authentication methods

More secure, user-friendly alternatives to passwords include badge tap, facial recognition, push notification to phone, fingerprint, and phishing-resistant FIDO passkeys. PIN can be used as a second factor. Passwordless authentication should use a combination of two factors as a sound security practice. Yet, it's important to note that not all methods are appropriate for every use case, so combinations must be selected according to use case and user needs.



Setting priorities

Getting to passwordless starts with prioritizing use cases, apps, and user populations to target for initial passwordless rollouts, and then phasing in the new authentication methods based on the greatest opportunity for benefits where systems can support them. Also essential to success is a change management strategy sharply focused on achieving user buy-in and adoption.

Want to know more? [Visit our website](#) for information and insight on authentication solutions.