Password problems exist. Almost three-quarters (73%) of IT admins say their organization requires a password reset every three months or more, and 92% require a reset at least every six months. As a result of this rotating plethora of credentials, almost one-third (31%) of help desk tickets are password-related.

Breaches, breaches everywhere

Slightly more than one-third (35%) of IT admins have experienced a business breach in the past 2 years. It’s no longer a matter of if but when your business will be exposed.

Your business already has...

The right strategy in mind. IT admins are early adopters and forward thinkers. For more than half of IT admins (57%), passwordless technology is on the roadmap for their businesses.

Why go passwordless?

Removing password-related barriers allows employees to quickly access the applications and credentials they need most. Simple access encourages usage and increases employee adoption, ultimately improving overall password hygiene. You can set even stronger master password requirements since end users won’t need it to gain access to the vault.

How does passwordless work?

Users gain passwordless access to the LastPass vault using the LastPass Authenticator app to set up and verify the trusted device. The authenticator then replaces the master password.

Passwordless still includes passwords — for now. Master passwords will be used to register a LastPass account and other security-related account changes.

It’s time to envision a world without passwords

In general, IT admins would feel more relaxed and secure if they were able to adopt passwordless technology.

Don’t compromise security for simplicity when you can have both.

Your business is better protected from cyber risk when employees use secure authentication methods to access their vault rather than weak or reused passwords.

You can set even stronger master password requirements since end users won’t need it to gain access to the vault.