

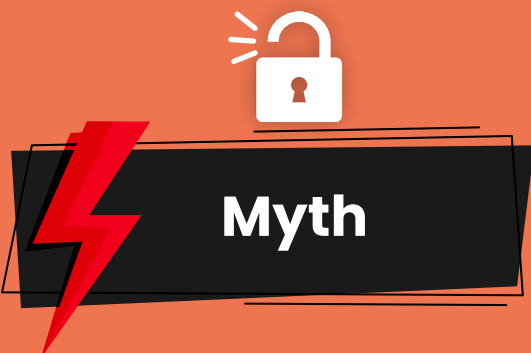


Going Passwordless?

Dispel These 5 Common Myths

With **p@\$\$w0rd\$** becoming a thing of the past, the passwordless future is seeing traction. However, the myths around the password-free approach are fogging its adoption.

Let's dispel the myths:



- A PIN and a password are the same.
- Going passwordless is less secure.
- Biometrics can be hacked or spoofed.
- Passwordless biometrics are costly.
- No password means no authentication.



- Unlike a password, a PIN is tied to the device it was set up on. Without the device, the PIN is pointless.
- Passwordless technique eliminates the use of weak passwords for better security.
- Biometrics are invoked locally on a specific device, eliminating the risk of hacking.
- One can easily deploy passwordless biometric solutions over the cloud, eliminating IT costs.
- Passwordless does not mean "no authentication." It just means that the user gets access without using a password.

With myths busted, let's go password-free.
Plot Your Path to Passwordless future with StealthLabs! [Contact us](#)