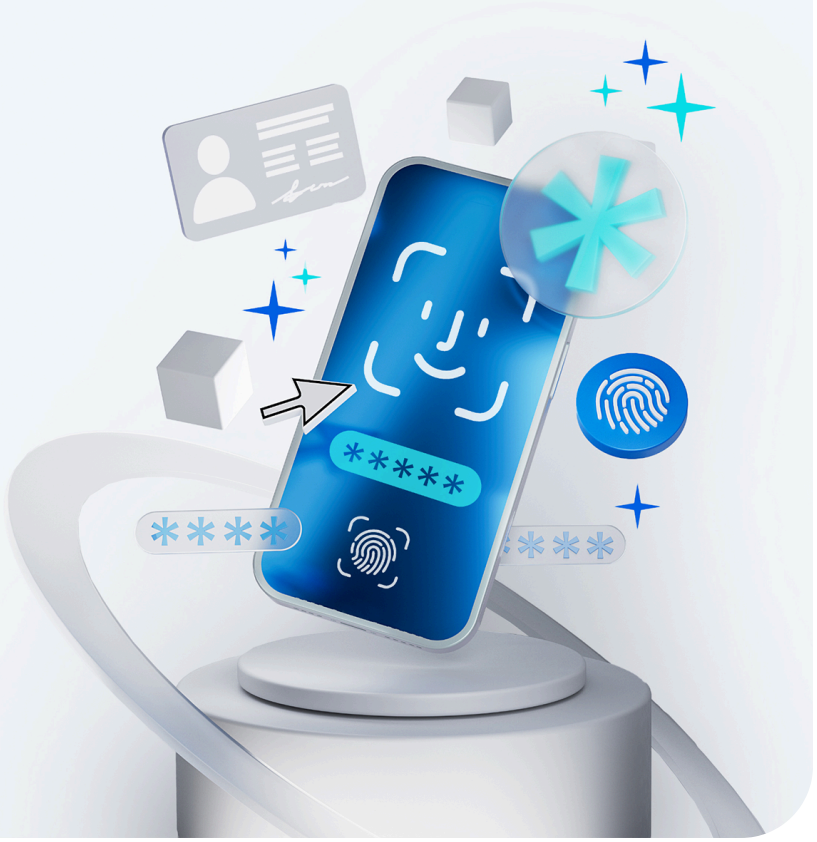
bitwarden



BITWARDEN SECURITY PERSPECTIVES

Passwordless Authentication

What you need to know

What exactly is passwordless authentication?

Passwordless Authentication refers to a range of sophisticated login methods that move beyond traditional passwords. Instead, they leverage biometrics, physical security devices, or software-centric cryptographic keys known as passkeys. Passkeys are a particularly popular approach. These use public-key cryptography.

54%

of people familiar with passkeys consider them to be more convenient than passwords, and 53% believe they offer greater security.

Source: Fidoalliance.org

How does password management fit in here?

Modern password management platforms securely generate, store, and synchronize passkeys according to FIDO2 and WebAuthn standards. This simplifies user access across devices while easing the transition away from traditional passwords. Specific features to look for:

- **Secure feneration and storage**: automatically creates and securely stores cryptographic keys.
- **Cross-device synchronization**: ensures consistent access across multiple user devices.
- **Biometric integration**: supports Face ID, Touch ID, Windows Hello, and Android Biometrics.
- **Legacy system compatibility**: manages traditional passwords alongside passkeys.
- **Phishing protection**: prevents credential exposure through domain-specific credential autofill.

Together, these features help maximize the effectiveness of Passwordless Authentication. They also make it easier for everyone within an organization to get on board with newer, more secure technology.

How passwordless authentication keeps today's businesses safer

By eliminating traditional password vulnerabilities, Passwordless Authentication strengthens cybersecurity while reducing associated risks and costs. It can also drive significant improvements in user experience, compliance, and operational efficiency. These newer approaches offer many business benefits:

- **Enhanced security**: mitigate phishing, credential stuffing, and brute-force attacks.
- **Improved user experience**: streamline authentication using either biometric or device-based methods.
- **Reduced IT costs**: minimize password resets and related support requests.

In this article

- **Compliance assurance**: support regulatory compliance for ISO 27001, GDPR, SOC 2, HIPAA, and PCI DSS.
- **Efficient onboarding/offboarding**: simplify employee transitions without password vulnerability issues.
- **Remote work security**: provide secure authentication from anywhere.
- **Competitive advantage**: demonstrate proactive cybersecurity leadership.

Passwordless Authentication offers a powerful way for businesses and organizations to reduce security risks, improve efficiency, and streamline access.

How Bitwarden supports passwordless suthentication

Bitwarden helps businesses transition to Passwordless Authentication by securely managing passkeys through a robust integrated platform. This comprehensive set of security features, access controls, and management tools includes:

- **Passwordless SSO**: devices that have been designated as trusted are able to authenticate and login with Single Sign-On without entering a password.
- **Comprehensive passkey support**: provides secure passkey generation, management, and synchronization.
- **Biometric unlock**: vaults that have timed-out and locked can be quickly unlocked with a fingerprint or facial recognition.
- **FIDO2/WebAuthn integration**: ensures secure, phishing-resistant domain-bound authentication and multifactor authentication.
- **Flexible Deployment**: supports cloud-based and self-hosted environments to address specific business needs.
- **Emergency access and decovery**: quickly provides secure recovery options and fallback mechanisms to reduce downtime if a device storing passkeys is lost or damaged.
- **Audit and compliance monitoring**: maintains detailed logs that track passkey usage, logins, and access attempts for compliance adherence.
- **Multi-factor authentication (MFA)**: integrates additional authentication layers for even stronger security.

The bottom line

By adopting Bitwarden for passwordless and passkey authentication, businesses of any size can enhance security, improve employee experience, and reduce the burden of password management. And they can do it all while ensuring seamless compatibility with both modern and legacy systems.

Bitwarden offers both cloud and self-hosted deployment options. So even those organizations held to the world's most stringent security and compliance standards can benefit from today's most advanced authentication tools. Just one more reason Bitwarden is regarded as the most trusted name in password management.

What makes Bitwarden stand out from the pack?

Passkeys, biometrics, and trusted devices represent the future of information security. Most Bitwarden users already enjoy a password-free experience today; using automatic password generation and autofill lets Bitwarden do all of the work.

Bitwarden remains on the leading edge for passwordless authentication in these areas:

- Passwordless login options, including the popular Login with SSO and trusted devices. Since 2020, Bitwarden has provided more SSO integrations than any competitor in the password management space, offering users greater choice.
- Universal passkey support. This includes managing passkeys for 3rd party applications, using a passkey as 2FA for Bitwarden, and logging into Bitwarden via passkey.
- Biometric unlock options, including face and fingerprint recognition.
- For companies looking to implement passkey infrastructure, Bitwarden offers solutions with Passwordless.dev.