BIO-key®

Data Sheet
Passwordless Solutions

The time to go passwordless is now! Don't wait any longer to secure all of your user groups with the right level of security.

BIO-key offers a suite of passwordless authentication solutions designed to enhance security, improve user experience, and reduce operational costs. By leveraging advanced biometric technologies, BIO-key enables organizations to transition seamlessly to a passwordless environment, eliminating the vulnerabilities associated with traditional password systems.

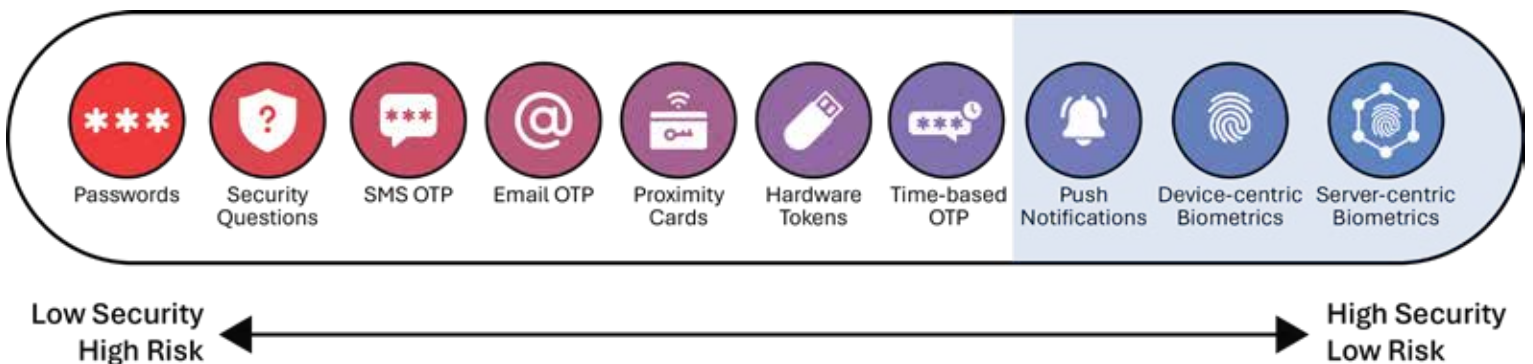## Key Benefits of Passwordless Authentication

Enhanced Security: Utilizes advanced authentication methods, including biometrics and secure tokens, to eliminate password vulnerabilities and mitigate risks related to stolen, shared, or forgotten passwords.

Improved User Experience: Users can authenticate quickly without the frustration of password management, leading to higher employee satisfaction and improved output.

Cost Efficiency: Reduces IT support costs by minimizing expenses related to password resets and management, allowing IT resources to focus on critical business initiatives.

Passwords | Security Questions | SMS OTP | Email OTP | Proximity Cards | Hardware Tokens | Time-based OTP | Push Notifications | Device-centric Biometrics | Server-centric Biometrics

Low Security High Risk ← → High Security Low Risk

Transitioning to a passwordless environment is an ongoing journey. BIO-key supports this process with the PortalGuard platform, a unified identity and access management (IAM) solution that simplifies the implementation and management of passwordless authentication for desktop and web applications. BIO-key PortalGuard supports all the authentication methods displayed above, including high-security, low-risk options like push notifications, device-centric biometrics, and server-centric biometrics.

BIO-key Options for Passwordless

WEB-key
(Biometrics Software)

An advanced biometrics management platform that establishes a unique identity for users.

Features:

- Advanced fingerprint scanning technology
- Achieved the highest independently-tested & verified NIST benchmarks for fingerprint identification speed and accuracy

Use Case: Ideal for businesses looking for a secure and user-friendly authentication solution for roving users and shared workstations

Passkey:YOU
(Biometric Passkey)

A FIDO-certified solution that replaces mobile phones and hardware tokens for authentication.

Features:

- Tap a badge on compatible readers
- Use fingerprint scanners connected to any Windows workstation

Use Case: Ideal for organizations that want convenient and secure access without the hassle or cost of purchasing authentication hardware for every user

MobileAuth App

A versatile app that provides users with multiple authentication options.

Features:

- Choose from push notifications, phone-based biometrics, or advanced biometrics
- Designed to combat phishing threats effectively

Use Case: Ideal for organizations with remote teams that prioritize security while offering users the flexibility to choose their preferred method

FIDO-key Security Keys

Compact physical security keys that enhance authentication strategies.

Features:

- Supports FIDO2 and WebAuthn standards
- Plug-and-play functionality for easy integration with Microsoft Windows, macOS, and Linux

Use Case: Suitable for organizations looking to implement a physical authentication method in their security protocols