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.

An April 2025 Gartner Analyst report "IAM Leader's Guide to User Authentication Fundamentals" highlighted the struggles of many companies when adopting passwordless authentication. They struggle because mainstream passwordless approaches require users to carry phones and tokens, or they cannot be digitally identified. These "what you have" approaches fail to account for user resistance to security that gets in the way of doing their job. Passwordless can't be considered in a vacuum.

BIO-key offers a uniquely different take on passwordless authentication, and our approach has quietly been adopted by many of the most discriminating buyers of authentication and security products in the world. Rather than burdening users with something else to keep track of, BIO-key achieves the highest levels of security while streamlining user authentication journeys, so users love it. BIO-key offers a suite of passwordless authentication solutions designed to enhance security, improve user experience, and reduce operational costs.

By leveraging unique Identity-Bound, not device-bound, biometric technologies, BIO-key enables organizations to transition seamlessly to a passwordless environment, replacing passwords with a simple touch of a users' finger at any device in the enterprise.

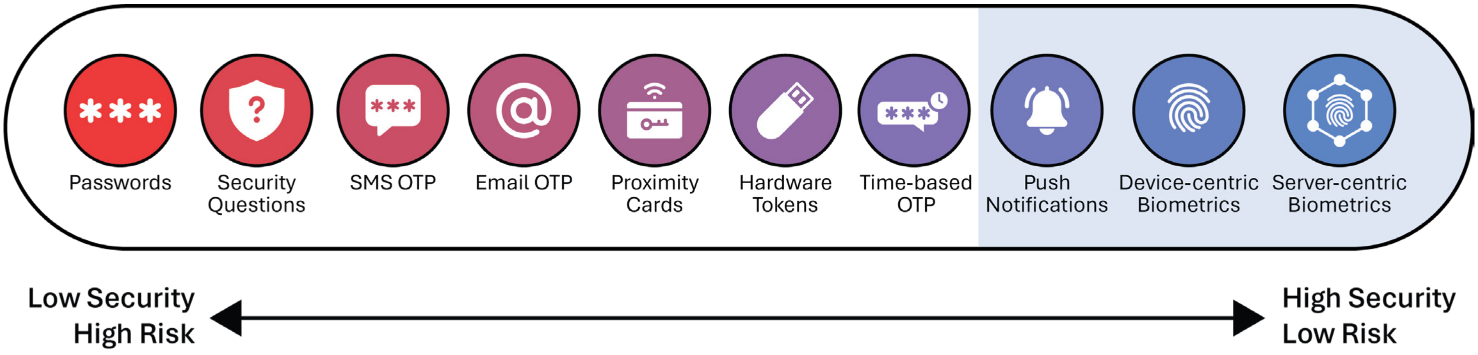
Key Benefits of BIO-key's Passwordless Approach

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

UX **Improved User Experience:** Users can authenticate quickly without the frustration of retrieving a phone or token, leading to higher employee satisfaction and improved efficiency.

Cost Efficiency: Avoids unnecessary purchases of multiple FIDO hardware tokens per non-phone users. Avoids labor law liability for compensating employees for personal phone use.

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

Passkey:YOU
Biometric (or Door-badge) secured managed passkey

A FIDO-certified solution that replaces mobile phones and hardware tokens with a credential your users already have —their finger or their door badge —for authentication to any relying party—whether an existing Entra, Okta, Ping or Duo platform or applications that accept FIDO2 authentication.

Features:

FIDO2 passkeys unlocked by

- ✓ Touching a fingerprint scanner at any Windows workstation
- ✓ Tapping a badge on compatible readers

Use Case:

Manufacturing shop floor, Retail, Call Center, Healthcare. Ideal for organizations that want convenient and secure access without the hassle or cost of purchasing authentication hardware for every user.

PortalGuard

A versatile IdP that provides users with SSO (SAML, OIDC, OAuth) and multiple MFA authentication options including passwordless Fingerprint, Face and Palm scanning.

Passwordless Features:

- ✓ Choose from push notifications, phone-based biometrics (Palm Scan or Selfie), or advanced biometrics on workstations via USB fingerprint scanners.
- ✓ Designed to combat phishing threats effectively while making sign in easier for users.

Use Case:

Ideal for organizations in the market for a full IdP, or who want more authentication options as a third-party authentication module for Entra, Okta, Ping.