BIO-key®

Data Sheet

PortalGuard

Simplifying Access Management to Put You Back in Control

PortalGuard is a single, unified Identity and Access Management (IAM) platform that provides cutting-edge solutions to a range of use cases and business initiatives. It is the only one to offer business-critical products — like multi-factor authentication and single sign-on — powered by the security of Identity-Bound Biometrics.

The PortalGuard Advantage: How It Helps Your Organization

- Securing Access: Remote & On-premises
- Eliminating Passwords
- Reducing Overhead for the IT Team
- Simplified Access for Users
- Meeting Compliance & Cyber Insurance Requirements

Unrivaled Flexibility & Personalization

PortalGuard can be deployed and configured to meet specific needs. SaaS, on-premises, and private cloud options make PortalGuard easy to deploy and supports nearly every cloud authentication federation standard, all major directories, and a wide variety of authentication methods.

Key Features & Capabilities

Multi-Factor Authentication

- Flexibility to choose from a wide range of authentication methods across all three main categories of factors:
  - Something you know (security question, PIN)
  - Something you have (mobile authenticator, hardware token, proximity card)
  - Something you are (biometrics, such as a fingerprint, face or palm scan)
- Our detailed overview of PortalGuard MFA, specifically, offers the full list of supported factors.
- Ability to consolidate existing authentication methods by aggregating everything under a single security policy in PortalGuard without the need to rip and replace.
- Robust security capabilities to support secure login in any scenario, including both hybrid environments and the desktop with PortalGuard Desktop.

info@bio-key.com www.bio-key.com

BIO-key®

Identity-Bound Biometrics

- Powerful, secure biometric authentication that verifies the actual person – not just a device or credentials.
- Inherent cloud-readiness allows for deployment via public or private cloud.
- Multiple authentication methods are supported to give all users flexible options, including:
  - Software: BIO-key MobileAuth, the one-of-a-kind MFA mobile app that utilizes secure facial recognition and palm scanning.
  - Hardware: Microsoft-qualified Windows Hello USB scanners that can be used out of the box with Windows Hello and Windows Hello for Business, or for use with our IAM solutions as one of many supported brands of scanners.
- Supports passwordless authentication without the need for phones or hardware tokens.

Single Sign-On

- PortalGuard SSO Concierge™ eliminates the additional login and seamlessly passes credentials to thick client applications on the user's behalf, improving productivity for users and the IT team.
- Protected by PortalGuard MFA, inducing Identity-Bound Biometrics (IBB), to give users authentication that they do not need to remember or physically possess, while also providing the highest levels of security.
- PortalGuard SSO supports modern identity federation standards to help meet requirements for all user access scenarios, including SAML 2.0, OAuth 2.0, OpenID Connect 1.0, and CAS 3.0+.
- Kerberos SSO offers a "true SSO" experience for users on domain-joined workstations. With PortalGuard's MFA capabilities, users can be given a passwordless desktop login experience and avoid additional password prompts.

MobileAuth

- One-of-a-kind, easy-to-use MFA app that requires no additional hardware.
- Supports multi-factor authentication and single sign-on solutions to streamline secure logins.
- Offers multiple, convenient authentication methods to eliminate the need for multiple vendors. These methods include:
  - Facial recognition
  - Palm scanning
  - Push tokens
  - Local biometrics
- Biometric authentication methods are powered by Identity-Bound Biometrics to ensure that the actual person is being authenticated.

Self-Service Password Reset

- Functions seamlessly across all points of access, for both browser-based access and via the desktop with PortalGuard Desktop.
- All SSPR actions can be completed from any browser or the desktop while users are both online and offline.
- PortalGuard SSPR streamlines IT teams' time and resources by providing easy-to-use administration, including:
  - Real-time auditing dashboard
  - Help Desk console
  - Verbal authentication
- Multi-factor authentication support enhances the security level of PortalGuard SSO by ensuring only the user can reset the password at a moment's notice with their choice of verification method.

info@bio-key.com www.bio-key.com

BIO-key®

PortalGuard Desktop

- PortalGuard Desktop can be installed on your workstations as an optional client-side component to secure logins from both the browser and desktop.
- Works with both on-premises and cloud/IDaaS deployments of PortalGuard.
- Provides true multi-factor authentication for both Microsoft and Mac desktops – even requiring MFA when unlocking the device, itself.
- Supports a wide range of authentication factors:
  - MobileAuth
  - Mobile App TOTP (Google Authenticator, Authy)
  - SMS and Email OTP
  - YubiKey OTP
  - Printed / Backup codes
  - Help Desk generated
  - HOTP tokens
  - Duo Push

Why PortalGuard?

Single, unified IAM platform so you can consolidate your IAM solutions and lower TCO

Identity-Bound Biometrics that go beyond device biometrics and verify the person

Support for hybrid environments and desktop login to secure all access scenarios

Customer IAM (CIAM) is fully supported with flexible options including self-registration and account management, self-service password reset, and multi-factor authentication

Affordable & simple to budget with pricing that is easy to understand, without any unexpected licensing or integration costs

Critical Business Use Cases

- Passwordless Authentication
- Adaptive Authentication
- Remote Access + Workforce
- Shared Workstations + Roving User Access
- Customer IAM
- Cyber Insurance

info@bio-key.com www.bio-key.com