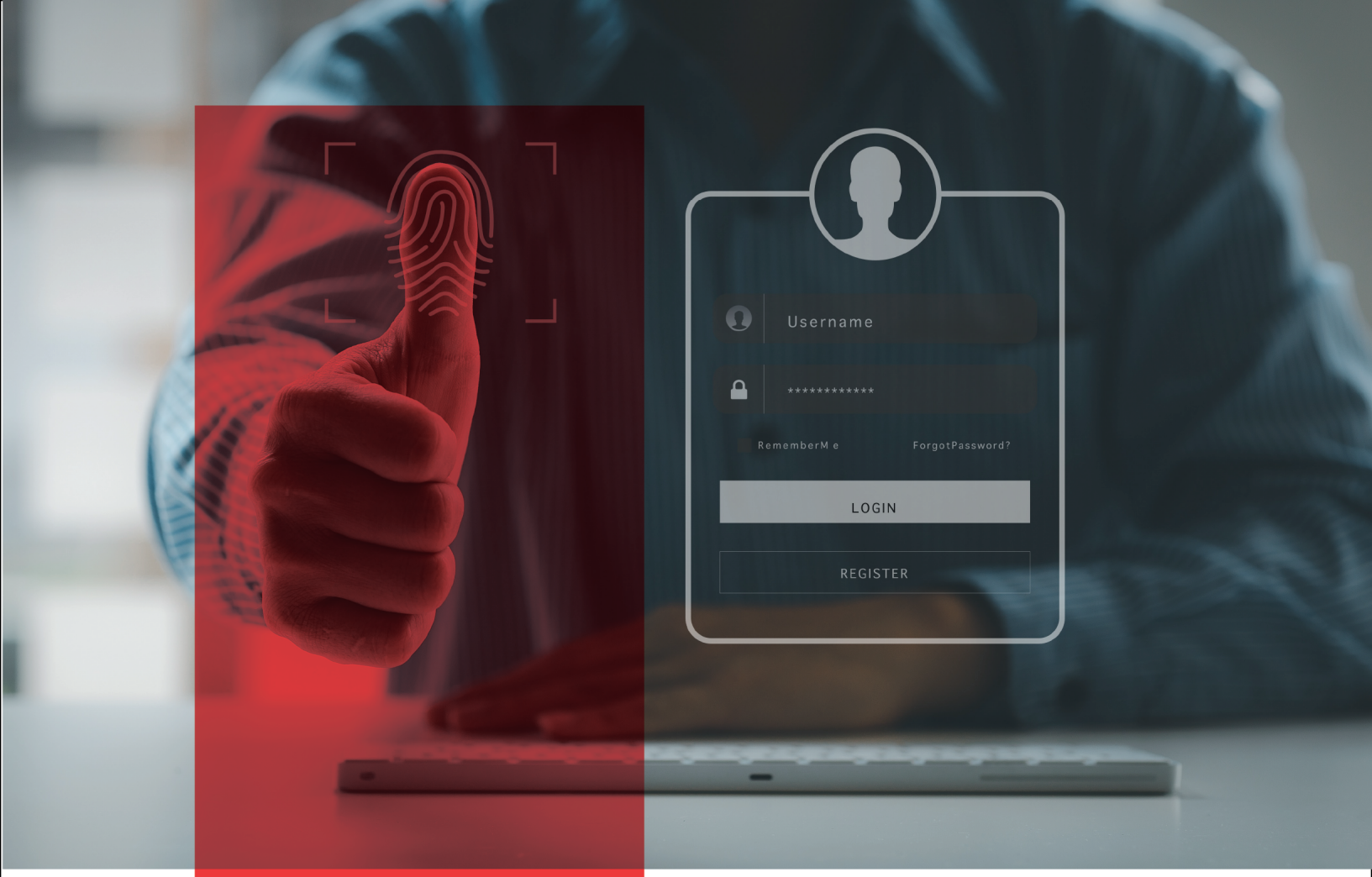


WHITEPAPER

PORTALGUARD®
A BIO-key® Solution.

5 Reasons Microsoft Customers Choose BIO-key for Identity

Introduction

The correct identity management solution can be a game-changer for your organization – and many Microsoft customers are realizing this. In the following analysis, we discuss the 5 reasons Microsoft customers are going with BIO-key for identity.

1. User-First Product Design

BIO-key has been focused on identity security since day one. We build and design all products from the ground up to be user-centric. Our unified IAM platform, PortalGuard, can be easily configured to meet your security requirements – not the other way around. Here are five key ways BIO-key customers benefit from our fundamental user-first approach to product design:

IDaaS, on-premises, private cloud and hybrid options for deployment

Consolidation of disparate policies under a single security policy

Easy integration into existing tech stacks – no ripping or replacing

Self-service enrollment for users and highly configurable policy management for admins

Detailed reporting and audit reports of all login activity to meet security and compliance requirements

Lastly, while all BIO-key products and solutions are built to make deployment and use as easy as possible for both administrators and end-users alike, implementation is fully supported by an expert technical team. Learn how this software and business intelligence company had BIO-key's PortalGuard fully deployed in less than two months – half the time the company had anticipated.

2. Compatibility with Microsoft Products

BIO-key provides digital identity solutions that connect customers' Microsoft and non-Microsoft infrastructures. Together, we make Office 365 and Azure AD easier, more secure, and more productive. If you have existing Microsoft products, we can integrate easily. Tight integration enhances security and user experience while reducing TCO via vendor consolidation, including the following:

Microsoft 365

MS Authenticator app

Windows OS

Windows Hello

Active Directory

Kerberos apps

Azure Active Directory

However, the fluid and seamless relationship between BIO-key and Microsoft products does not end there. From hardware – like USB scanners and devices – to software applications, the ease of integration remains consistent:

Microsoft-Qualified USB Scanners: Use out of the box with Windows Hello and Windows Hello for Business, or for use with our Identity and Access Management (IAM) solutions, as one of many supported brands of scanners.

On-Premises Apps: Integrate via Kerberos SSO and tackle legacy or thick applications that don't support modern SSO and Identity management.

Fluid User Management Policies: Leverage Microsoft Active Directory policies, groups, and organizational units (OUs) through BIO-key's user management policies.

Microsoft Suite of Products & Solutions: Seamless compatibility with Microsoft 365, Windows OS, Active Directory, Azure Active Directory, MS Authenticator app, Windows Hello, and Kerberos apps.

Windows Server Security: Secure your Windows server with PG Desktop via Credential Provider and support for RDP and VDI implementations.

Windows Device Support: BIO-key's PortalGuard platform supports identity management and advanced authentication for Microsoft devices, such as the Surface family of tablets.

BIO-key's one-of-kind passkey authentication solution, Passkey:YOU, leverages the FIDO standard's newest capabilities to allow a user to authenticate to any software or service relying party with only a touch of a finger USB scanner attached to a Windows workstation. Moreover, various Microsoft-qualified Windows Hello USB scanners can be used out of the box with Windows Hello and Windows Hello for Business.

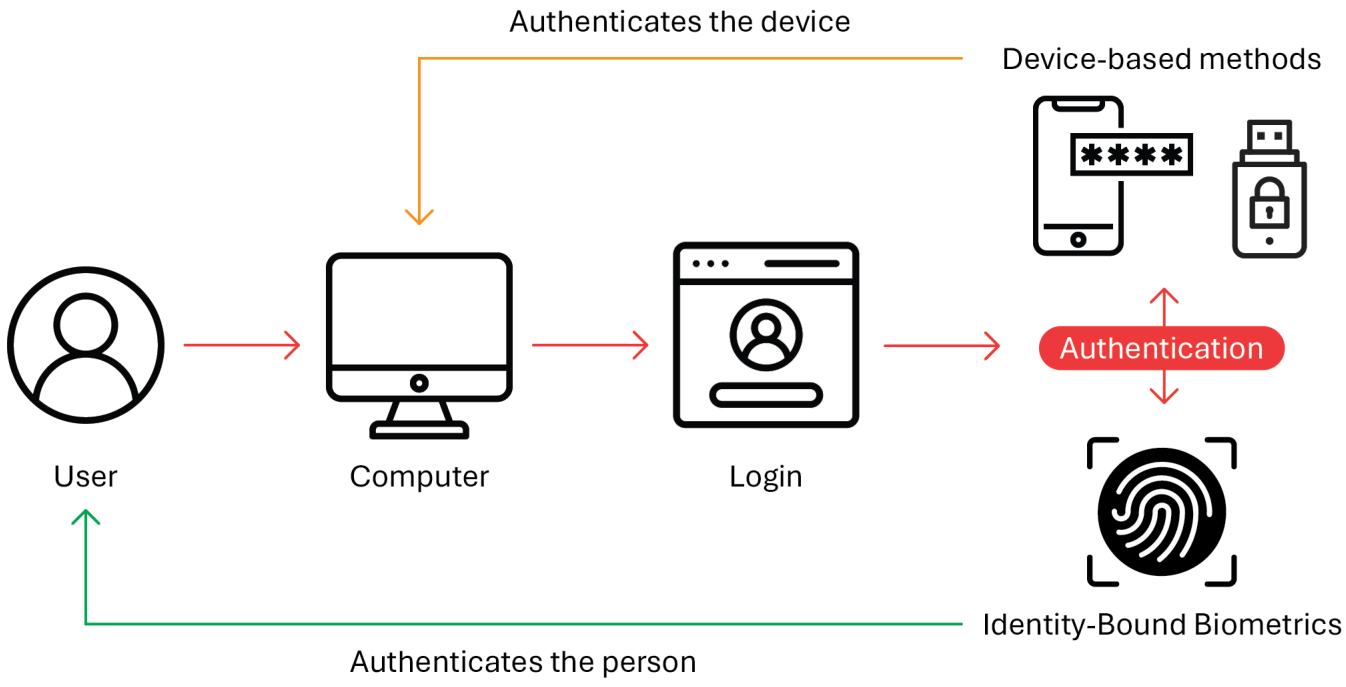
3. Robust Biometric Authentication (Identity-Bound Biometrics)

With 81% of data breaches involving compromised credentials and 91% of phishing attacks targeting user credentials, it's no shock that organizations of all sizes and industries are questioning password-based authentication. "What you know" authentication factors – like passwords – and "what you have" factors, like hardware tokens, are vulnerable to phishing and other cyberattacks. However, the third factor, "what you are," – biometrics – is not susceptible to these attacks.

BIO-key's Identity-Bound Biometrics was built with identity security as a priority: it is the only biometrics authentication solution that genuinely verifies the actual identity of the individual requesting access – not just authenticating an approved device or token. With IBB, customers can add an extra layer of security when and where needed.

In today's world, which is rapidly shifting towards passwordless authentication, Identity-Bound Biometrics enhances passwordless even further, requiring no phones or hardware tokens. With the touch of a finger on a fingerprint reader or a palm scan using BIO-key's mobile app – MobileAuth – approved users can authenticate securely and conveniently.

Moreover, IBB is a part of BIO-key's unified IAM platform, PortalGuard, where you can access a suite of powerful, easy-to-use IAM solutions that address critical business use cases.



4. More Authentication Method Options & Flexibility

No two organizations are the same regarding security needs, priorities, and requirements. Even within a single business, various user groups may need to authenticate differently. On their own, Azure and Office365 can be limiting in authentication choices, like requiring the use of their own app or outdated SMS OTPs.

Today, organizations and end-users alike need more flexibility from their identity partners – something that BIO-key offers in abundance. When it comes to workforce productivity apps, many customers opt for Microsoft – and rightfully so. However, when it comes to Identity, BIO-key has been focused on it since day one – it's in our DNA. That's why we've built our IAM platform, PortalGuard, with 17 authentication options to fit any need and use case.

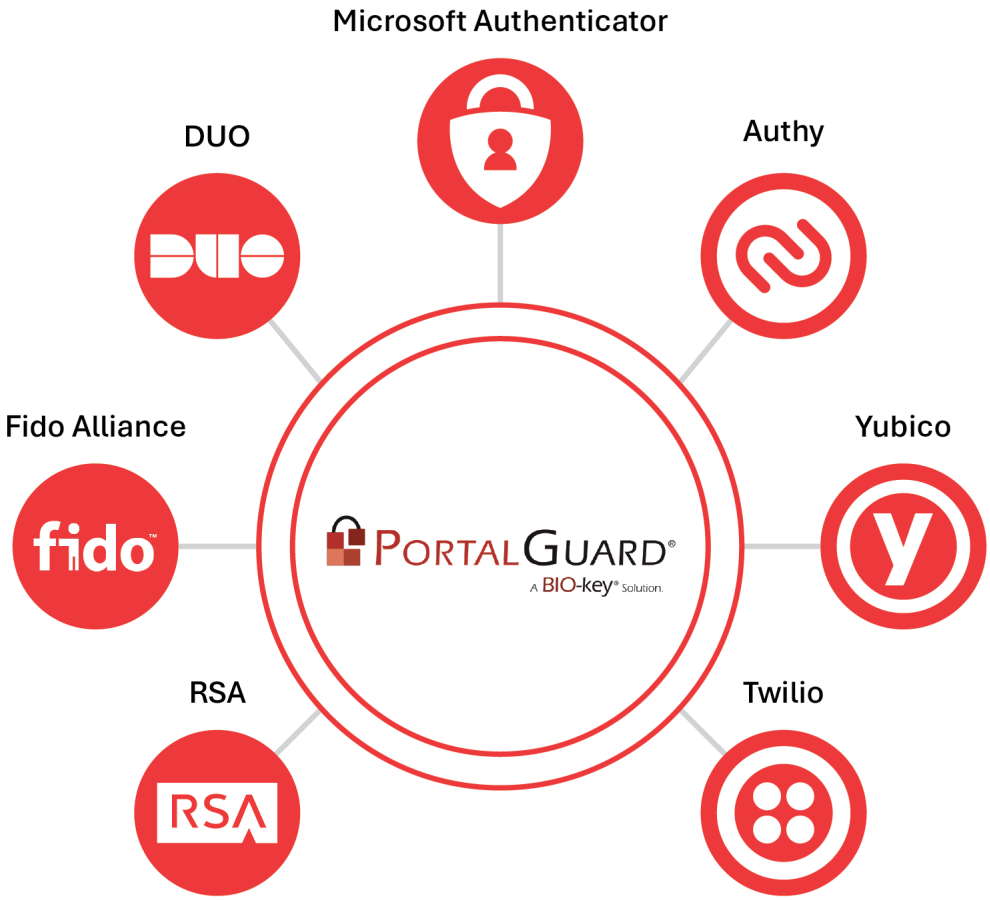
Explore the eBook "Understand How to Choose the Right Authentication Method" for an in-depth analysis.

Solution Priority	Authentication Method
Highest Security	› WEB-key IBB › MobileAuth IBB
Easiest to Implement	› Mobile Authenticator App › MobileAuth IBB
Does not require a smartphone	› WEB-key IBB › FIDO2 WebAuthn › Security Questions
Secure Third-Party/Supplier Access	› Mobile Authenticator App › MobileAuth IBB
Secure Remote Access (VPN)	› Push Notifications › Mobile Authenticator App › MobileAuth IBB › WEB-key IBB
Secure a Shared Workstation	› WEB-key IBB

5. Open, Platform-Based Approach to 3rd-Party Integrations

If you go with Microsoft for Identity and/or Security, chances are you'll need to use all the products from their tech stack. That means MS Defender for AV, MS Sentinel for SIEM, and Azure for MFA. BIO-key, however, lets you mix and match with existing solutions you may already have in place – like authenticator apps from MS and DUO.

Going with BIO-key for Identity means that you have the freedom to enhance the PortalGuard solution with integrations from our highly regarded partners:



Don't fall victim to vendor lock-in. Discover the valuable benefits of flexibility and personalization offered by BIO-key's integrated ecosystem.