

WHITEPAPER



6 Reasons Duo Customers Choose BIO-key for IAM

Introduction

If your organization uses DUO, there is an opportunity to uplevel your Identity and Access Management (IAM) strategy. Many DUO customers choose the BIO-key PortalGuard solution to improve access management and identity authentication for employees, customers, students, and suppliers.

With BIO-key PortalGuard, you can:

- **Enhance Security:** Safeguard sensitive data with flexible advanced authentication methods
- **Prevent Phishing and Fraud:** Protect against cyberattacks with strong multi-factor authentication (MFA) and adaptive risk-based policies
- **Improve User Experience:** Streamline login processes with features like Single Sign-On (SSO), passwordless authentication, and personalized access portals
- **Increase User Productivity:** Enable quick access to tools and information for internal and external users
- **Support Remote Access:** Securely manage remote access, allowing users to connect from anywhere without compromising security
- **Meet Cyber Insurance Requirements:** Protect user accounts with MFA and strong password policies, or eliminate passwords altogether
- **Centralize Administration:** Simplify management with a single IAM platform to oversee user access and security policies
- **Reduce IT Costs:** Lower the burden of password resets and IT help desk calls, saving time and money
- **Scale Easily:** Adapt to organizational growth and evolving technology needs with flexible security solutions
- **Integrate Seamlessly:** Work with existing tools like DUO Security, Microsoft Entra ID, and other third-party apps to enhance your IT infrastructure

This whitepaper will explain the top 6 reasons DUO customers choose PortalGuard for IAM.

The top 6 reasons DUO customers choose BIO-key PortalGuard

Comprehensive authentication options
(15+ options including BIO-key MobileAuth™)



Reason 1:

Comprehensive Authentication Options

Multi-factor authentication (MFA) is crucial for securing access and preventing cyberattacks, but it can be challenging to provide users with effective authentication methods.

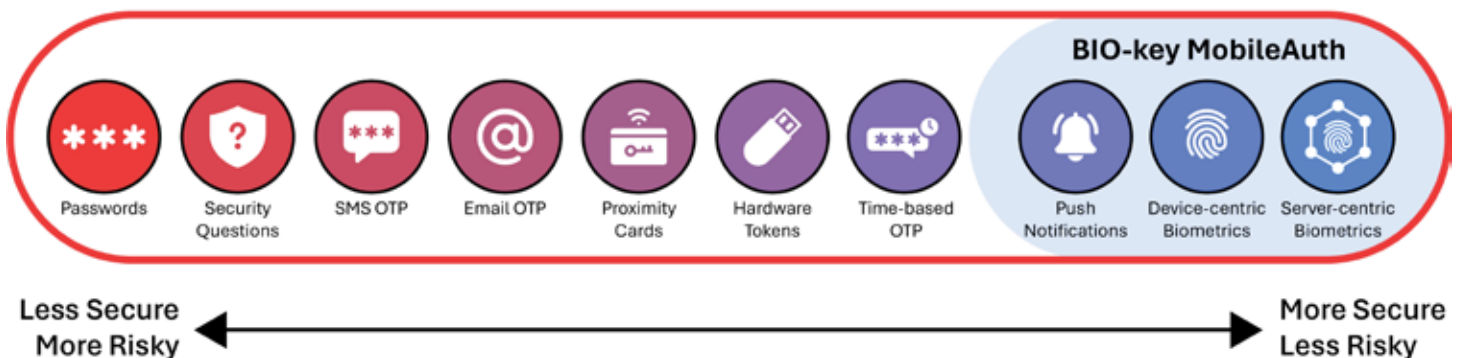
DUO Security is known for its convenient authentication solutions, yet its MFA options are somewhat limited. While DUO supports device-centric biometrics like Apple TouchID and FaceID, these methods verify the device rather than the user. This distinction can leave organizations vulnerable, particularly with the growing reliance on remote access and cloud services since the pandemic.

In contrast, BIO-key's PortalGuard solution offers over 15 authentication methods and utilizes server-centric biometrics. This approach permanently links biometric data to a user's digital identity, ensuring that only the authorized individual can authenticate.

Additionally, BIO-key's MobileAuth app enhances security by bringing advanced server-centric biometrics to any mobile device. With features like PalmPositive™ (palm scanning) and FacePositive™ (facial recognition), along with device-centric biometrics and push notifications, it provides robust two-factor authentication for all applications.

When compared to the DUO Mobile App, which primarily focuses on device authentication and time-based one-time passwords (TOTPs), BIO-key's MobileAuth app presents a more holistic solution. By directly linking biometrics to user identity, it not only strengthens security but also simplifies the authentication process. This makes it ideal for securing both individual and shared workstations, remote access, and any scenario where reliable user identification is essential.

Authentication Methods Supported by BIO-key PortalGuard



Key Benefits of PortalGuard MFA



Flexible Authentication Methods: PortalGuard supports more than 15 authentication methods, allowing organizations to choose options that fit their needs.



Protection Against Phishing: PortalGuard MFA offers advanced authentication methods, such as biometrics and passkeys, that are inherently resistant to phishing attacks.



Regulatory Compliance: Implementing PortalGuard MFA can help organizations meet industry regulations and compliance standards, such as GDPR, HIPAA, and PCI DSS, which often mandate strong authentication measures.



Customizable Policies: Organizations can tailor MFA policies based on user roles, locations, and risk levels, allowing for a more dynamic and responsive security approach.



Improved User Experience: The PortalGuard MFA solution integrates seamlessly with existing user workflows, minimizing disruption while enhancing security.



Centralized Management: Administrators can manage MFA settings and user access from a single platform, simplifying oversight and reducing administrative burdens.



Reduced IT Support Costs: By decreasing the likelihood of account breaches, PortalGuard MFA can lead to lower IT support costs and fewer help desk calls.



Scalability: The PortalGuard MFA solution can easily scale alongside organizational growth, accommodating more users and devices without compromising security.

Reason 2:

Passwordless with Biometrics

When it comes to biometric authentication, the two primary approaches are device-centric biometrics, as supported by Duo, and server-centric biometrics, offered by BIO-key PortalGuard. Each method has its unique strengths and considerations, impacting security, user experience, and deployment.

Device-Centric Biometric Authentication (Duo)

In device-centric biometric authentication, the biometric data (such as fingerprints or facial recognition) is stored and processed locally on the user's device. This means that authentication occurs on the device itself without sending sensitive biometric information to a central server.

Limitations:

- **Device Dependency:** Users must have their specific device to authenticate, which can create accessibility issues if the device is lost or damaged.
- **Management Complexity:** Organizations may face challenges in managing and securing multiple devices across the workforce.

Server-Centric Biometric Authentication (BIO-key PortalGuard)

Server-centric biometric authentication involves sending biometric data to a central server for verification. BIO-key PortalGuard processes and stores this data securely, allowing for a more unified management approach across an organization.

Advantages:

- **Centralized Management:** Organizations can manage biometric data and authentication policies from a single platform, simplifying administration and compliance.
- **Flexibility:** Users can authenticate from various devices, as the biometric data is not tied to a single device. This is particularly beneficial in scenarios with remote work or shared devices.
- **Enhanced Security:** Centralized storage allows for advanced security measures, including encryption and monitoring, to protect biometric data.

Reason 3:

SSO that Eliminates All App Logins

When implemented properly, Single Sign-On (SSO) eliminates the need for multiple application logins, offering secure access through a single login.

DUO Security provides SSO for cloud applications, supporting Active Directory (AD) or SAML for federated access. While DUO is SAML 2.0 IdP compliant, it requires a third-party SAML Identity Provider (IdP) such as the PortalGuard solution to complete SSO requests.

BIO-key's PortalGuard helps secure on-premises, legacy, thick client, and web applications with a single IdP. It supports various SSO methods, including WS-Federation, CAS, OAUTH, OpenID Connect, and Shibboleth SSO, ensuring users can access all applications without managing multiple passwords.

Benefits of Using PortalGuard SSO



Eliminate the need to develop and maintain your own portal.



Reduce the number of passwords users are required to remember and manage.



Implement and enforce configurable password policies.



Remove the need to manage external users' credentials.



Optionally increase security using any combination of transparent barriers.



Add stronger authentication using Two-Factor and/or Passwordless Authentication for select users or groups of users (e.g., Administrators).



Reduce password-related Help Desk calls related to password and access issues.

Reason 4:

Flexibility & Customization

BIO-key PortalGuard offers significant flexibility and customization, making it a versatile choice for organizations. Administrators can tailor security policies to meet specific needs, adjusting authentication requirements based on user roles, locations, or devices. This ensures that security levels are appropriate without hindering the user experience. Additionally, the user interface can be branded, creating a cohesive experience that reflects the organization's identity.

PortalGuard can be deployed in various environments—on-premises, cloud, or hybrid—providing adaptability to existing IT infrastructures. It seamlessly integrates with a wide range of applications, enabling organizations to enhance security without overhauling their current systems. Custom workflows, granular access controls, and adaptive authentication further allow for tailored user experiences and security measures.

Key aspects of flexibility and customization include:



Tailored Security Policies
based on user roles and contexts



Custom Workflows for access requests and user management



Diverse Authentication Options
including biometrics and tokens



Granular Access Control
to limit permissions effectively



Customizable User Interface
to reflect organizational branding



Adaptive Authentication
based on contextual factors



Flexible Deployment Options:
on-premises, cloud, or hybrid



Scalability to accommodate growth and changing needs



Seamless Integration with existing applications and systems



API Access for further customization and integration

Reason 5:

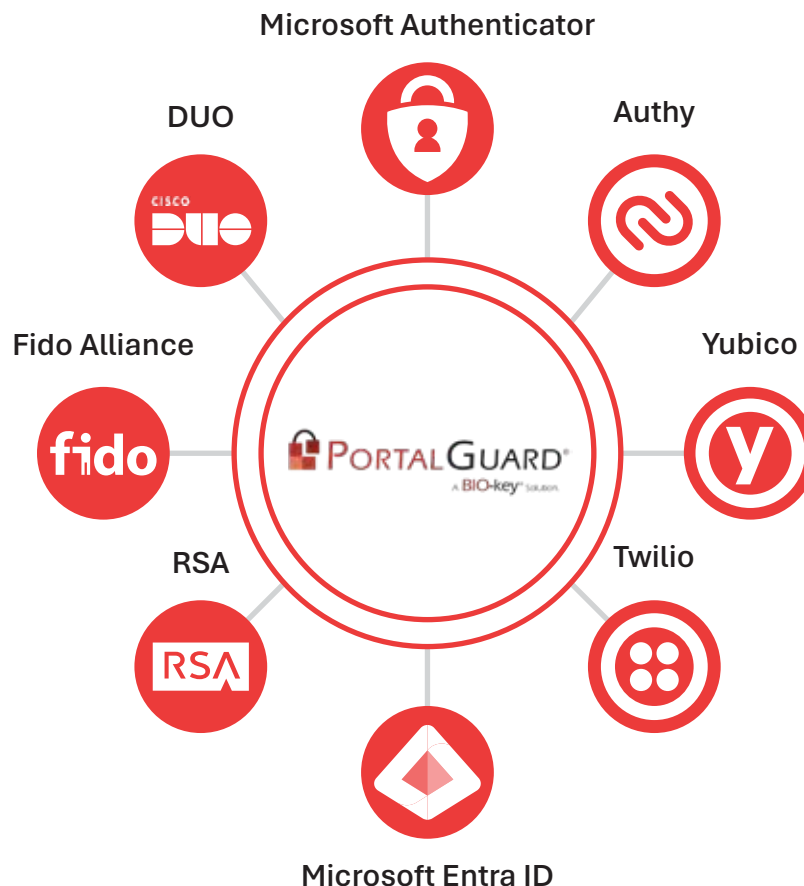
Secure Authentication for External Identities

A complete Identity and Access Management (IAM) solution should easily secure access for all identities —employees, customers, students, and suppliers. DUO Security primarily supports internal workforce identities, leading customers to adopt multiple overlapping solutions for different access needs.

PortalGuard can streamline this by integrating multiple IAM solutions, including DUO, into one platform. It supports both workforce and customer identities (Customer IAM or CIAM), offering key features that DUO lacks, such as:

- User self-registration workflows
- Directory support beyond Active Directory
- Fully customizable user interface (UI) and user experience (UX)

While DUO allows only limited UI customization, PortalGuard enables customers to fully brand their login screens and SSO portals to create a modern user experience.




Reason 6:

Affordable with High-Quality Support


PortalGuard offers clear and straightforward pricing, bundling all its features into a competitive rate based on the number of users. This contrasts with DUO's complex a la carte pricing model, making PortalGuard easier to budget with a lower total cost of ownership and faster ROI. In fact, PortalGuard was recognized as having the Best ROI for MFA by G2 customer reviews in Summer 2024, achieving an above-average return on investment in just 18 months—significantly faster than the industry average.

Furthermore, PortalGuard is supported by a team of IAM experts, ensuring high-quality customer service. Larger vendors like DUO can be challenging for IT teams to reach, leaving them without timely solutions.



CJ O.
Network Administrator
Mid-Market (51-1000 emp.)

Validated Reviewer ✓
Verified Current User ✓
Review source: G2 invite on behalf of seller
Incentivized Review



★★★★★ Aug 15, 2024 (Original May 30, 2024) 🗨️

"the experience has been good, support good, technology good, no complaints, no hiccups."

What do you like best about PortalGuard?

The technology is good and the support is even better; I've had good support experiences from all of the people I've worked with at PortalGuard since our rollout a couple of years ago - I've had lots of time working with support getting help setting up new connections or sorting out an issue here or there and it has been a great relationship that we plan to continue.



Verified User in Automotive ⓘ
Mid-Market (51-1000 emp.)

Validated Reviewer ✓
Verified Current User ✓
Review source: G2 invite on behalf of seller
Incentivized Review



★★★★★ Mar 01, 2024

"Excellent Product"

What do you like best about PortalGuard?

It's less expensive than its true competitors, and it allows us to stay compliant with all the new FTC regulations. The team really works with you to make sure that the solution works best for your environment. Their support team implemented the solution quickly and it integrated with our environment very easily. The support staff is patient and thorough. When we had a problem (of our own making) they stayed on task until it was resolved. If there's a feature you need, they'll sincerely consider it. In our case, they even saw the value of the feature we requested and added it for everyone (you're welcome!). Everyone in our organization has to use MFA daily, and when we calculated the the labor/time savings of the feature they added, it amounted to over \$4M saved yearly!

More reviews on G2