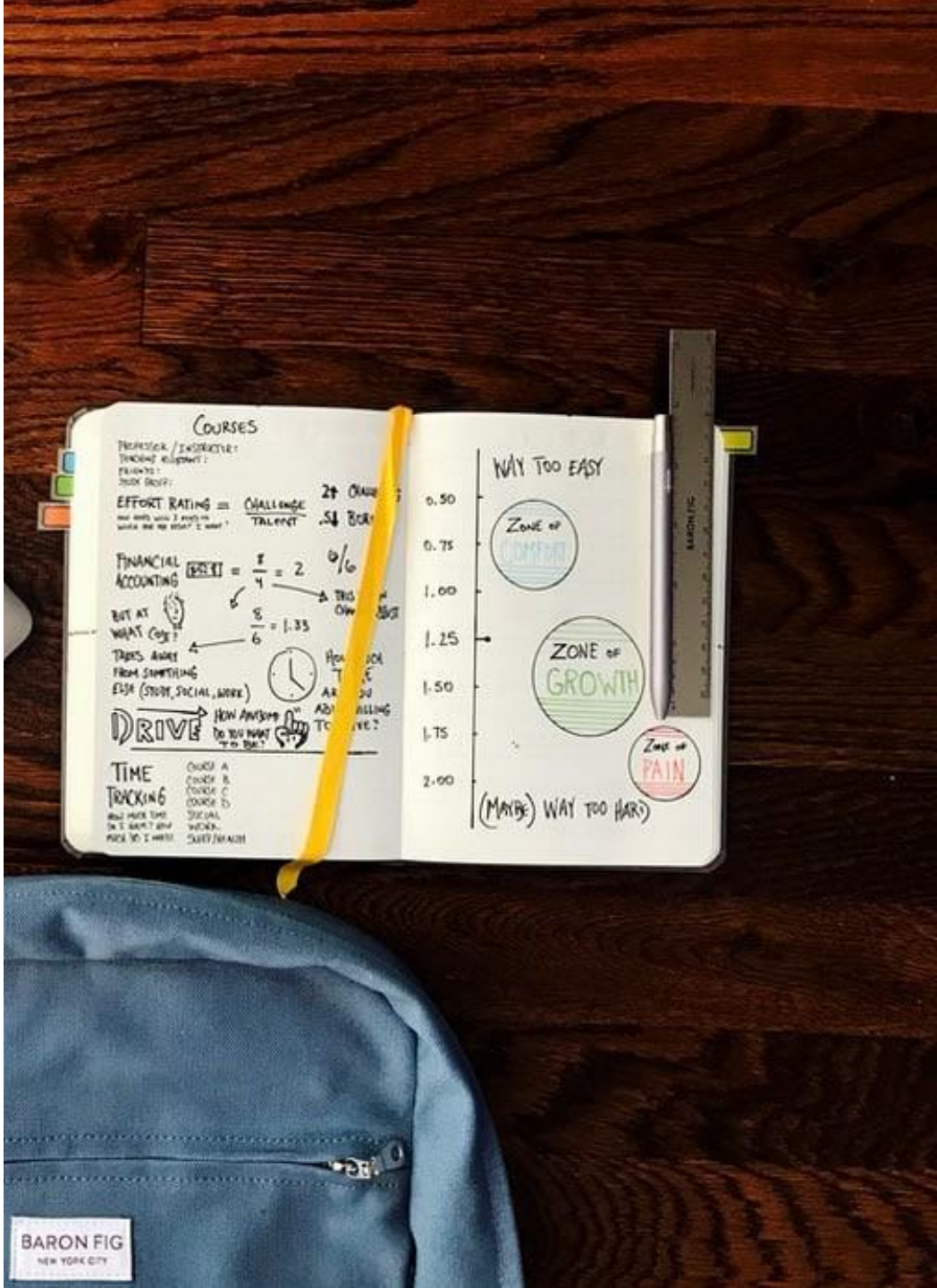
Evolving Your Cybersecurity Together

BIO-key®

Introduction

In today's landscape, CISOs and CIOs in higher education have valid concerns. The education sector is the most targeted by hackers globally, facing nearly 2,300 attacks each week. This sector not only has the highest vulnerabilities but also ranks lowest in readiness for identifying and addressing threats. These alarming statistics highlight why the 2024 EDUCAUSE Top 10 identified "Cybersecurity as a Core Competency" as the leading factor in fostering institutional resilience[1].

To safeguard their students, staff, and intellectual property while remaining competitive and responsive to community needs, educational institutions must invest in affordable, practical, and comprehensive identity solutions.



1. https://er.educause.edu/articles/sponsored/2024/5/cybersecurity-in-higher-education-dont-let-the-hackers-win

Challenges to Implementing Identity & Access Management (IAM)

Critical IAM controls such as multi-factor authentication (MFA) and single sign-on (SSO) can be challenging to implement.

Prevention

The U.S. national security cyber chief reports that multi-factor authentication (MFA) could **prevent 80-90% of cyberattacks**[2]. However, finding a single solution with the appropriate mix of authentication methods to support students, faculty, and staff remains a significant challenge.

Challenges

While Identity and Access Management (IAM) controls are crucial, implementing them cohesively with limited resources and budget often leads to a fragmented strategy and increased operational overhead.

Many educational institutions currently rely on multiple siloed MFA solutions—such as separate systems for mobile authenticators, push tokens, and hardware tokens—each governed by different security policies.

Similarly, Single Sign-On (SSO) implementations are often disjointed, incorporating a mix of homegrown, open-source, and commercial solutions. This fragmentation leaves critical applications unintegrated, leading to password prompts that hinder user access.

2. https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of/

Password Reset Burden

Password policies that enforce expiration and complexity requirements often lead to an increase in password reset requests from users who forget their credentials. This influx can place a significant burden on help desks, especially in the absence of self-service password reset (SSPR) capabilities. With the average cost of each password reset call reaching $70[3], this becomes a substantial financial strain for many institutions.

Staffing and Budget Challenges

In the post-COVID landscape, IT teams are still navigating the complexities of supporting new educational methods, including hybrid and remote learning platforms. While many institutions have adapted, they continue to face staffing shortages and budget constraints as they recover from the pandemic's financial impact.

As educational priorities shift, resources remain limited, making it increasingly difficult to implement comprehensive cybersecurity measures. This ongoing challenge emphasizes the need for innovative solutions to safeguard institutions in a rapidly evolving environment.

3. https://www.forrester.com/report/best-practices-selecting-deploying-and-managing-enterprise-password-managers/RES139333

Over 200 institutions, including 65+ community colleges, rely on BIO-key for their identity and access management needs.

Mendocino College
University of Denver
Butte College
Butte-Glenn Community College District
SWC
Johnston Community College
East Georgia State College
Baker University
Merced College
Ventura County Community College District
Allan Hancock College
Arcadia University
Central Carolina Community College
University of Wisconsin System
Barstow Community College
Glendale Community College
Cuesta College
Morgan State University
Oklahoma Wesleyan University
Prince George's Community College
Antelope Valley College
Coastal Carolina Community College
Eastern University
Indiana Tech
Chaffey College
Neumann University
RACC
Reading Area Community College
Herzing University
College of the Canyons
University of Arkansas Fort Smith
Cerritos College
Northeast Iowa Community College

SPOTLIGHT

Foundation for California Community Colleges (FCCC)

Since 2014, BIO-key has collaborated with the FCCC to enhance the cybersecurity posture of educational institutions.

- Trusted by over 50 colleges and districts
- Exclusive discounts available through the CollegeBuys contract
- Annual Sponsor of the CISOA Technology Summit, supporting technology leadership within the California Community College System

This partnership underscores our commitment to strengthening cybersecurity and fostering innovation in education.

FOUNDATION *for* CALIFORNIA COMMUNITY COLLEGES

Why do institutions select BIO-key?

With BIO-key, you don’t have to manage your IAM strategy alone. Our customer success team and security practitioners are experts in higher education. Think of them as part of your team because that’s exactly what they are. They’ll work with you to understand your institution's unique requirements and partner with you to take on any heavy lifting, so your IT team doesn’t have to.

Implementing BIO-key PortalGuard is a cybersecurity "quick win" as it helps you evolve your cybersecurity posture with the resources you already have.

- Single, award-winning platform aggregates and consolidates security point solutions under centralized security policies
- Widest range of options for MFA, SSO, and SSPR, including Identity-Bound Biometric options to authenticate “who you are”
- Amazing customer support that combines product know-how with IAM expertise to ensure you are getting the most out of your solution
- Affordable for any budget with special higher education pricing based on FTE Students

IAM that benefits your institution

BIO-key customers experience benefits not only for their students, faculty, staff, and IT teams but also their institution as a whole.

- **Improve security across your institution** – Reduce cyber risk by implementing consistent security policies across all systems, platforms, applications and devices to enforce stronger security, including multi-factor authentication.
- **Simplify the lives of students, faculty, and staff with a modern login experience** - Enable users to easily access systems, regardless of where they are, what time it is and what devices they are using.
- **Improve the efficiency and efficacy of security teams** – Centralized administration helps streamline critical aspects of managing identities, authentication, and authorization.
- **Maintain regulatory compliance and meet cyber insurance requirements** - Prove where and how user credentials are used and demonstrate that data is protected with the proper controls.
- **Increase business agility** – Support new services and systems your institution implements with SSO and centralized policy management, to quickly secure access to these systems without creating additional security silos.
- **Lower Management and IT Costs** – Streamlined password management minimizes the frequency of password reset requests, easing the workload for help desk staff and administrators. This allows them to allocate more time to high-priority tasks instead of routine issues. By adopting a single, integrated Identity as a Service (IDaaS) solution, organizations can reduce costs by consolidating disparate systems and diminishing or even eliminating the need for on-premises infrastructure.

BIO-key PortalGuard®

An award-winning platform to secure Access for students, faculty, and staff.

Multi-Factor Authentication (MFA)

Wide range of authentication methods for flexible and powerful identity security

Identity-Bound Biometrics™

Biometric authentication for the highest levels of integrity and convenience

Single Sign-On (SSO)

Reduce password prompts and secure access to all apps from a single IdP

MobileAuth™

Multi-factor authentication app that offers Identity-Bound Biometric authentication options and push tokens

Self-Service Password Reset (SSPR)

Reduce password-related IT support calls by up to 95%

Hardware Devices

Offer a variety of hardware devices including Microsoft-qualified Windows Hello USB fingerprint scanners & FIDO-key hardware tokens

Deployment Options

PortalGuard can be deployed on-premises, in your cloud, or as Identity-as-a-Service (IDaaS) platform in AWS.

BIG INNOVATION 2024

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

G2 High Performer FALL 2024

G2 Momentum Leader FALL 2024

G2 Highest User Adoption FALL 2024

G2 Best Meets Requirements FALL 2024

G2 Easiest To Use FALL 2024

G2 Easiest To Do Business With FALL 2024

G2 Best Support FALL 2024

Flexible Multi-Factor Authentication (MFA)

Secure all access & keep your institution safe

Aggregate and consolidate all your authentication methods under centrally managed security policies.

- Wide range of out-of-the box authentication methods
- Easily integrate existing solutions (e.g., DUO Security, Yubikey, & MS Authenticator)
- Supports contextual authentication & passwordless approaches
- Users can select the authentication option(s) that work for them
- Granular security policies configured down to the group, OU, or individual
- Secures browser and desktop logins

Security Questions

SMS OTP

Email OTP

Mobile Authenticator App

Push Notifications

FIDO2 / WebAuthn (Hardware Tokens)

WEB-key (Identity-Bound Biometrics)

MobileAuth (Identity-Bound Biometrics)

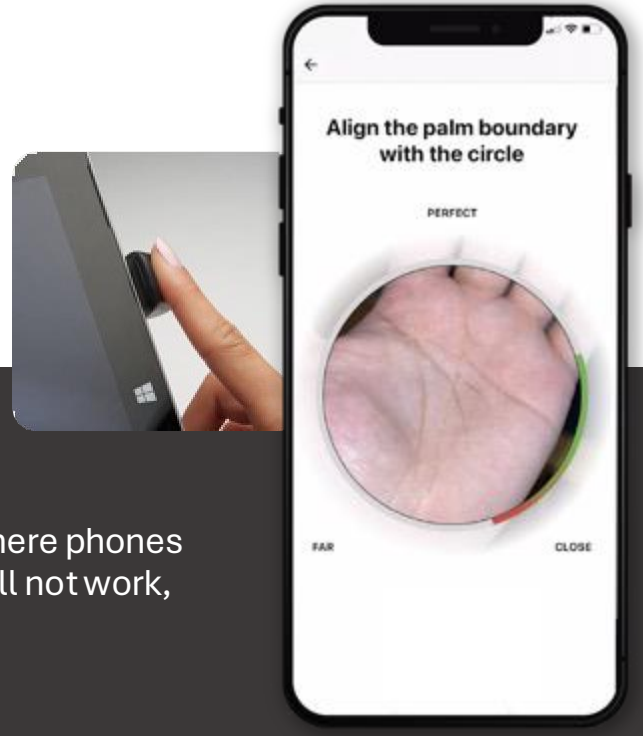
Integrated Device-based Biometrics

Proximity Cards

Complete your MFA with Identity-Bound Biometrics

Identity-Bound Biometrics (IBB) offer the highest level of integrity by binding a biometric to the user's digital identity.

- Centrally stored biometrics
- Non-reversible hashed biometric data
- Strict session management
- Captured on fingerprint scanners or via BIO-key MobileAuth™



Cannot be handed over, shared, forgotten, or stolen

Perfect for situations where phones and hardware tokens will not work, are not reliable, or safe

Enterprise-controlled enrollment

Affordable and easy to implement

SSO to eliminate passwords and SSPR to reduce help desk calls

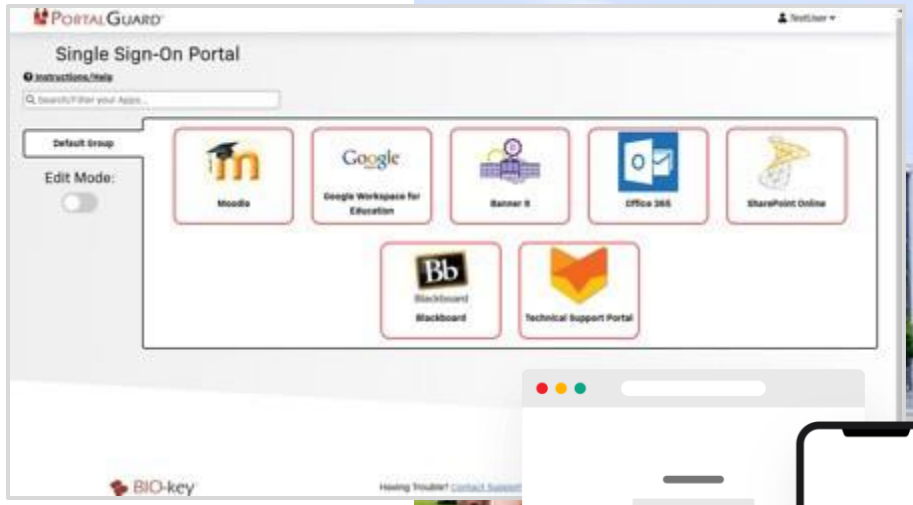
Customers using PortalGuard's Single Sign-On and Self-Service Password Reset (SSPR) capabilities reduce help desk calls by 95% or more.

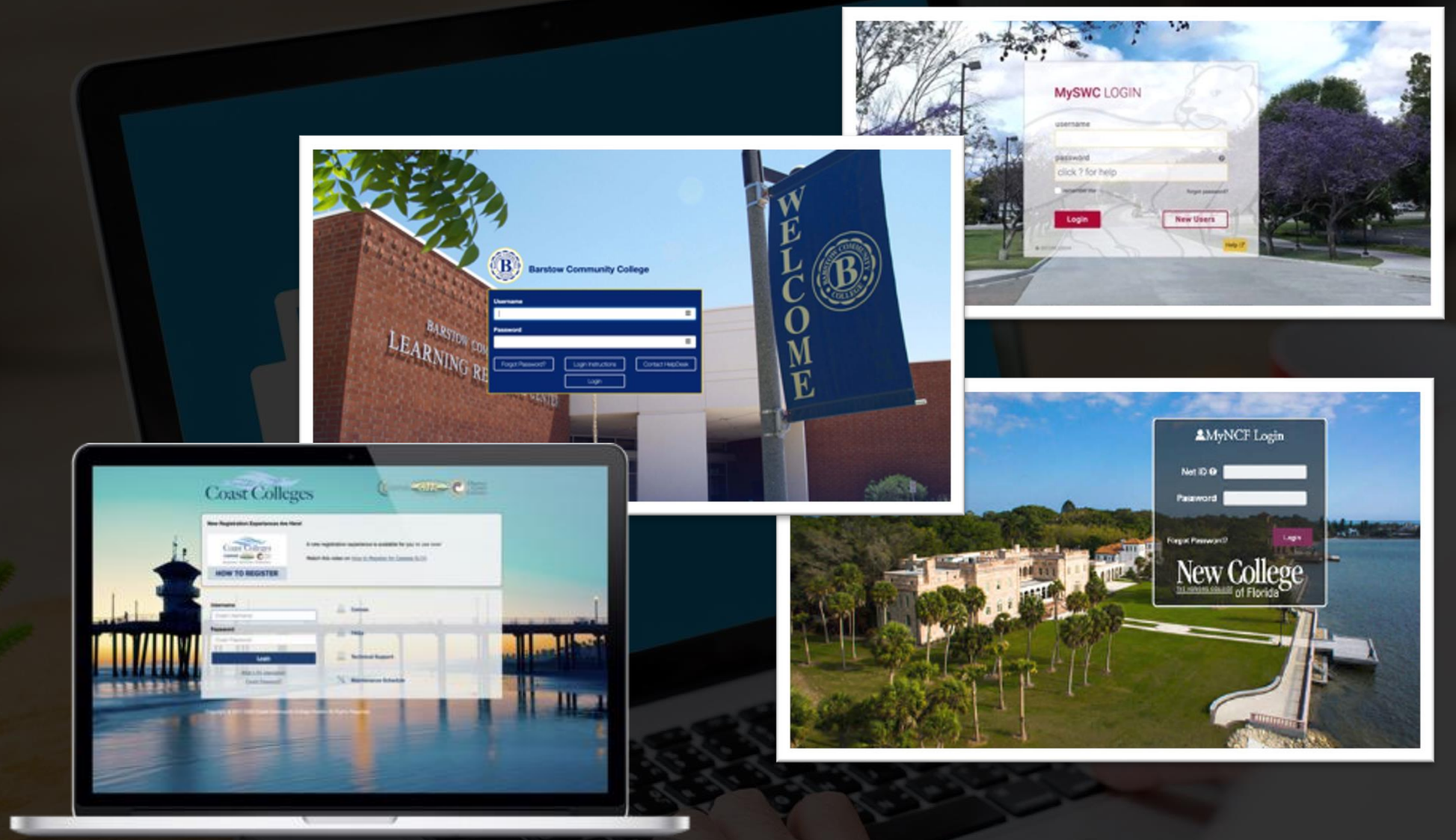
Single Sign-On (SSO)

- Protect on-premises and web applications from a single Identity Provider (IdP)
- Supported standards include SAML 2.0, Shibboleth, WS-Federation, OAuth 2.0, OpenID Connect 1.0, CAS 3.0+

Self-Service Password Reset (SSPR)

- Supports password reset, account unlock, password expiration, password & username recovery, and offline password recovery
- Available for browser & desktop/OS logins





Fully customizable UX for a modern, branded login experience that students, faculty, and staff will love.

Want to learn more?

Contact the BIO-key Team

Here are some resources to help you learn more about cybersecurity, BIO-key's solutions, and how institutions are currently implementing them. For additional materials, feel free to explore our online Resource Center.

- WHITEPAPER: Cybersecurity in Education
- WEBINAR: The Future of IAM for Education: How Colleges are Combating the Increase in Cyberattacks
- WEBINAR: NICC's Journey to a Secure Student Experience
- DATA SHEET: BIO-key PortalGuard
- COMPETITIVE: 5 Reasons DUO Security Customers Choose PortalGuard
- CASE STUDY: Contra Costa Community College District
- CASE STUDY: Southwestern Community College District

About BIO-key International

BIO-key International is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that enable convenient and secure access to devices, information, applications, and high-value transactions.

BIO-key offers the simplicity and flexibility required to secure the modern digital experience for on-prem and remote users, while easing the burden on IT teams.

BIO-key PortalGuard is a fully unified Identity-as-a-Service (IDaaS) platform with industry-leading biometric authentication options, single sign-on, multi-factor authentication, adaptive authentication, and self-service password reset.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery, strong partner relationships, and low TCO.

More information is available at:
https://www.bio-key.com/

Learn More:
https://www.bio-key.com/expertise-in-education/

BIO-key®