

Unlock the benefits of biometrics for password security

Grow your remote workforce without compromising security by incorporating VeriMark™ Guard with Azure Active Directory into your identity verification protocols.

Kensington®



Member of
Microsoft Intelligent
Security Association



Table of Contents

- How vulnerable is your organization to the growing risk of a data breach? 3
 - With Azure AD Identity, use biometric verification to enhance security, streamline access, and protect against scams and cyberthreats 3
 - Strike a balance between security and convenience with VeriMark and Azure AD 3
- Enhanced security protocols 4
- Streamlined passwordless access 5
- Fraud-resistant verification 6
- What are people saying about Kensington VeriMark solutions? 7
- A simple solution for effective protection 7

How vulnerable is your organization to the growing risk of a data breach?

With Azure AD Identity, use biometric verification to enhance security, streamline access, and protect against scams and cyberthreats.

Password-based security and maintenance puts a burden on both end users and IT admins. While two-factor authentication adds a layer of security to identity verification, traditional unencrypted SMS verification is not fraud-proof and leaves an organization open to SIM swapping, weak passwords, or phishing attacks that make you vulnerable to a data breach. Data breaches can disrupt business and result in lost revenue, regulatory fines, and put your reputation at risk.

273% increased data breaches in Q1 of 2020 over 2019.¹

64% more reported breaches and exposed records compared to 2019.²

Over 80% of hacking-related breaches involve brute force or the use of lost or stolen credentials.³

Strike a balance between security and convenience with VeriMark Guard and Azure AD



Enhanced security protocols

Revamp your authentication methods by incorporating biometric data that is unique to the individual.



Streamlined access

Empower remote employees to securely work from anywhere and access company applications.



Fraud-resistant verification

Decrease IT expenses, comply with major privacy laws and regulations, and gain peace of mind with biometric security.

Tap-and-Go support

One biometric security key for many services

Multifactor and 2nd factor authentication

Eliminate password phishing

Self-configuration and easy deployment

FIDO U2F and FIDO2 certified



Enhanced security protocols

To adequately protect business and consumer accounts, biometrics is the one element no one can forge or duplicate.

Passwords are a hassle, and they are no longer a secure form of authentication. Organizations can simultaneously eliminate passwords altogether, as well as less secure SMS two-factor authentication, by embracing the power of biometric data within Azure AD multi-factor authentication. VeriMark biometric fingerprint keys integrate seamlessly with your Azure AD account and increases your sign-in security.

Streamlined passwordless access

Empower remote employees to securely work from anywhere with biometric authentication.

Eliminate the hassle of passwords. Offer your employees a seamless user experience when they log into company applications. Reduce friction with multi-factor authentication that can be as simple as a touch of a finger. In the workplace, biometrics can be part of a strong security protocol for access to internal systems, files, information, and data. Leverage encrypted biometric data to ensure only the right person is authenticating.

Fraud-resistant verification

Why risk it?

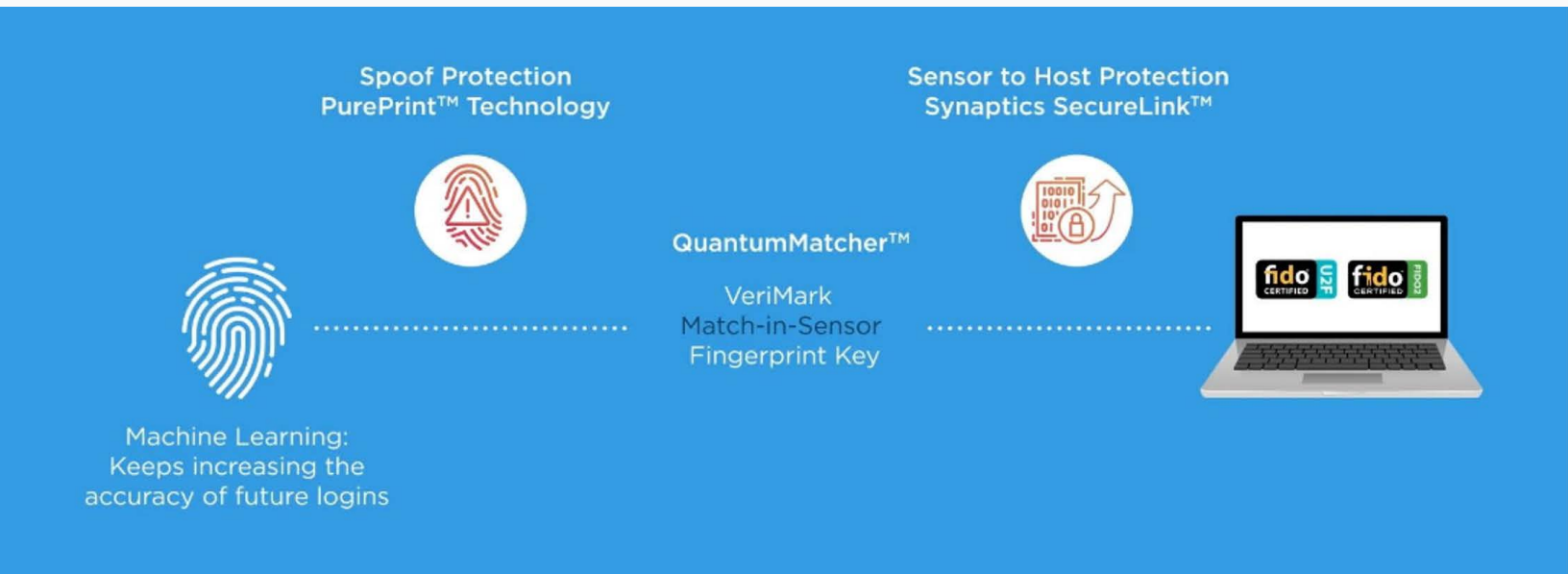
Benefit from technology to minimize the risk of fraud and gain peace of mind with VeriMark biometric fingerprint keys that provide strong authentication resistant to phishing and other common attacks. By minimizing the risk, rest assured your IT department can conserve resources and your organization will remain fully compliant with major privacy laws and regulations.

ACCESS COMPANY RESOURCES BY LOGGING IN TO AZURE AD WITH A TOUCH OF YOUR FINGER

Kensington Fingerprint sensors feature Synaptics' SentryPoint technology, offering Quantum Matcher with PurePrint anti-spoof technology. PurePrint examines fingerprint images using unique artificial intelligence technology to distinguish between fake and actual fingers.

Secure fingerprint sensor with end-to-end security

Provides strong authentication, resistant to phishing and other common attacks.



What are people saying about Kensington VeriMark solutions?

MBREVIEWS

"Kensington VeriMark IT is one step ahead of most of its competitors, featuring a match-in sensor for improved security, the ability to use one USB key for multiple computers (and services). The sensor has proven to be very fast and accurate. So, if you need an extra layer of security to your company or your personal computer, the Kensington VeriMark IT fingerprint key is one of the best solutions available right now."

THE GADGETEER

"The concept of having a portable hardware device/key that adds a layer of security and includes the benefit of not storing passwords on the computer is great."

NERD TECHY

"The Kensington VeriMark Guard is compatible with most modern operating systems. It supports use on Windows machines, macOS machines, and iOS smartphones. It's compatible with the Chrome, Edge, Firefox, and Safari browsers right out of the box. It's plug and play, so you don't have to follow any complex setup procedures to get it working."

A simple solution for effective protection

The threat of identity fraud is ever-present and increasing.

Biometric verification provides organizations double the security around identity with the added benefits of convenience and scalability. Kensington's systems are highly flexible and replace traditional password systems by removing the need for tedious password resets and password-related risks. The use of biometrics can replace traditional multi-factor authentication, allowing organizations to maximize their Microsoft technology investments and provide a future-proof, fraud-resistant solution that integrates seamlessly with Azure AD.



Kensington®



¹ 2020 Data Breaches Identity Force

² Risk-Based Security

³ Verizon 2020 Data Breach Investigations Report

© Copyright 2021 Kensington Computer Products Group and Microsoft Corporation. All rights reserved.

Member of
Microsoft Intelligent
Security Association

