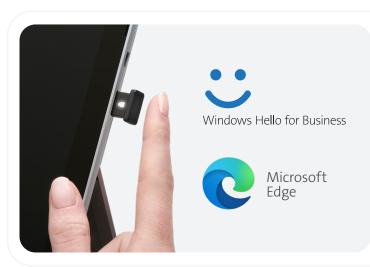# Kensington Fingerprint Readers

Why Risk It?

Recent data from Risk Based Security[1] revealed that the number of records exposed has increased to a staggering **36 billion in 2020.** There were 3,932 publicly reported breaches in the first three quarters of 2020, with the three months of Q3 adding an additional 8.3 billion records to what was already the **"worst year on record."**

While no security solution can guarantee full protection, biometrics is yet another strong link in your security chain. In addition to the inherent uniqueness of an individual's biometric data (and therefore the level of security this offers), biometrics offers a passwordless solution.

Security Where, When and How you Need It

Windows Hello for Business

Microsoft Edge

Enterprise Deployment

VeriMark IT, VeriMark Desktop and VeriMark Guard easily integrate into an existing IT infrastructure, offering passwordless login to Windows Hello, Windows Hello for Business, Microsoft Azure and other Microsoft services on Edge, making it easy for administrators to manage employee access, privileges and passwords.

TAA COMPLIANT

Government Use

VeriMark IT, Desktop and Guard can be used to support a company's cybersecurity measures, consistent with (but not limited to) privacy laws such as GDPR, BIPA and CCPA.

G Suite

Windows Hello

Dropbox   GitHub

OS Compatibility

VeriMark Guard offers maximum compatibility with web services including Google, Facebook and Microsoft (for Windows Hello, refer to VeriMark or VeriMark IT), with support for Chrome, Edge, Firefox & Safari and cross-platform OS support for Windows 10, macOS and Chrome OS as a FIDO2 security key.

Why Biometric Authentication?

As physical features such as fingerprints and pupils are so difficult to forge, biometrics is a strong security solution, though we see biometrics as part of a comprehensive security solution that might also include a password and/or physical devices such as a key, card or token.

In the workplace, biometrics can be part of a strong security protocol for access to internal systems, files, information and data. And it can be as simple as touching a finger or looking into a camera lens.

Key Questions

What is the key objective in the use case?

Is Windows Hello or Hello for Business being utilised?

What platforms or browsers need to be supported?

User accessing single device or multiple devices?
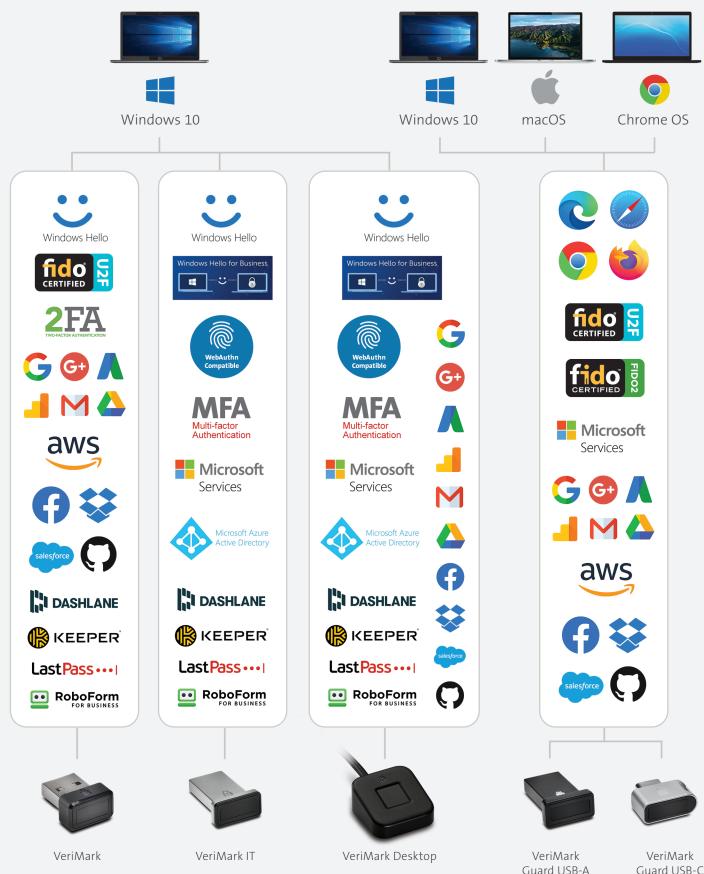
Aware of biometric reader benefits?

DID YOU KNOW?

81 percent of hacking-related breaches
leveraged either **stolen** and/or **weak passwords.**

2020 Verizon Data Breach Investigations Report
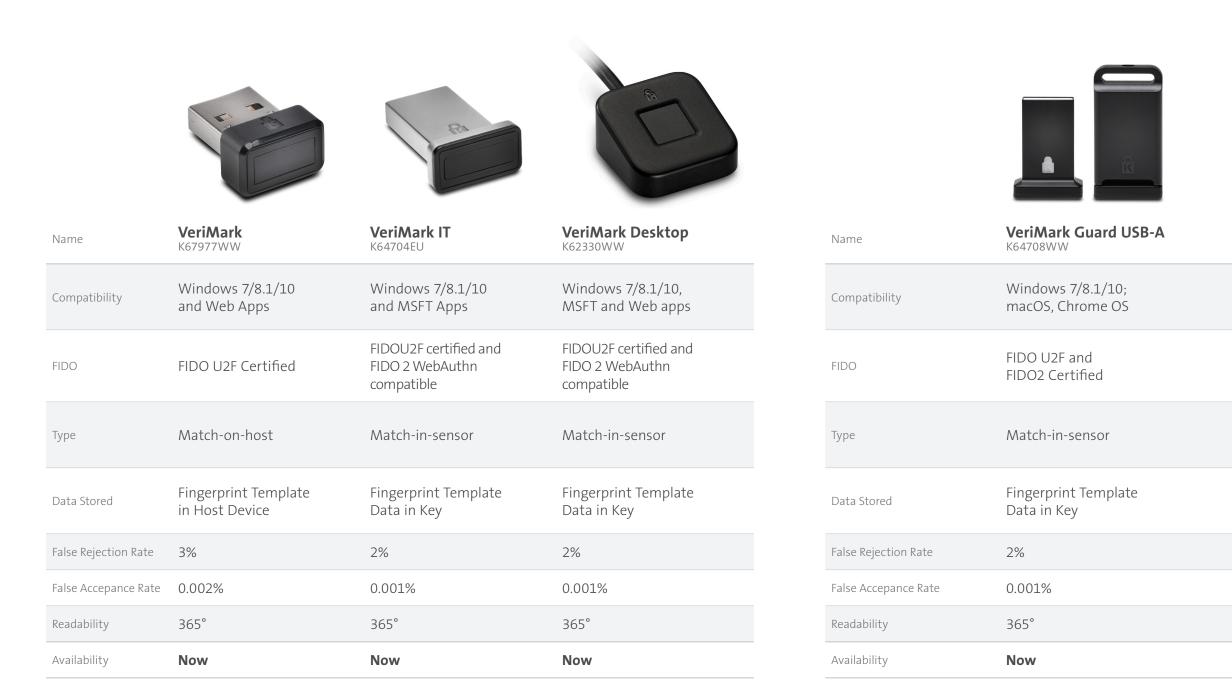
Which Fingerprint Key is Right For You?

Windows 10   Windows 10   macOS   Chrome OS

VeriMark   VeriMark IT   VeriMark Desktop   VeriMark Guard USB-A   VeriMark Guard USB-C

VeriMark Fingerprint Readers

Member of
Microsoft Intelligent
Security Association

Microsoft

Name	**VeriMark** K67977WW	**VeriMark IT** K64704EU	**VeriMark Desktop** K62330WW
Compatibility	Windows 7/8.1/10 and Web Apps	Windows 7/8.1/10 and MSFT Apps	Windows 7/8.1/10, MSFT and Web apps
FIDO	FIDO U2F Certified	FIDOU2F certified and FIDO 2 WebAuthn compatible	FIDOU2F certified and FIDO 2 WebAuthn compatible
Type	Match-on-host	Match-in-sensor	Match-in-sensor
Data Stored	Fingerprint Template in Host Device	Fingerprint Template Data in Key	Fingerprint Template Data in Key
False Rejection Rate	3%	2%	2%
False Accepance Rate	0.002%	0.001%	0.001%
Readability	365°	365°	365°
Availability	**Now**	**Now**	**Now**

Name	**VeriMark Guard USB-A** K64708WW	**VeriMark Guard USB-C** K64709WW
Compatibility	Windows 7/8.1/10; macOS, Chrome OS	Windows 7/8.1/10; macOS, Chrome OS
FIDO	FIDO U2F and FIDO2 Certified	FIDO U2F and FIDO2 Certified
Type	Match-in-sensor	Match-in-sensor
Data Stored	Fingerprint Template Data in Key	Fingerprint Template Data in Key
False Rejection Rate	2%	2%
False Accepance Rate	0.001%	0.001%
Readability	365°	365°
Availability	**Now**	**Now**