Kensington Vingerafdruklezers

Waarom het risico lopen?

Recente gegevens van Risk Based Security[1] lieten zien dat het aantal blootgestelde records in 2020 is toegenomen tot een ongelooflijke 36 miljard. In de eerste drie kwartalen van 2020 hebben 3932 openbaar gemaakte datalekken plaatsgevonden. Tegen het einde van het tweede kwartaal was al het “slechtste jaar ooit” in termen van het totale aantal blootgestelde records.

Hoewel geen enkele beveiligingsoplossing volledige bescherming kan garanderen, vormt biometrie een extra sterke schakel in uw beveiligingsketen. Biometrische gegevens bieden niet alleen een uniek beveiligingsniveau omdat deze voor elke persoon uniek zijn, maar biometrie verstrekt ook een oplossing zonder wachtwoorden.

[1] *https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf*

Beveiliging waar, wanneer en zoals u het nodig heeft

Zakelijke implementatie

VeriMark IT, VeriMark Desktop en VeriMark Guard kunnen eenvoudig in een bestaande IT-infrastructuur worden geïntegreerd, bieden aanmelding zonder wachtwoord voor Windows Hello, Windows Hello for Business, Microsoft Azure en andere Microsoft-services op Edge en maken het eenvoudig voor IT om toegang, toestemmingen en wachtwoorden van werknemers te beheren.

Gebruik door de overheid

Verimark IT, Desktop en Guard kunnen worden gebruikt ter ondersteuning van de cyberbeveiligingsmaatregelen van een bedrijf die consistent zijn met (maar niet beperkt tot) privacywetten zoals AVG, BIPA en CCPA.

Compatibiliteit met besturingssystemen

De Verimark Guard biedt maximale compatibiliteit met internetdiensten als Google, Facebook en Microsoft (raadpleeg VeriMark of VeriMark IT voor Windows Hello), met ondersteuning voor Chrome, Edge, Firefox en Safari, en platformoverkoepelende besturingssysteemondersteuning voor Win10, mac OS en Chrome OS als een FIDO2-beveiligingssleutel.

Waarom biometrische authenticatie?

Omdat fysieke kenmerken zoals vingerafdrukken en pupillen zo moeilijk te vervalsen zijn, biedt biometrie een sterke beveiliging. Toch zien we biometrie voornamelijk als onderdeel van een complete beveiligingsoplossing, met mogelijk ook een wachtwoord en/of fysieke hulpmiddelen zoals een sleutel, kaart of token.

Op het werk kan biometrie onderdeel uitmaken van een krachtig beveiligingsprotocol voor toegang tot interne systemen, bestanden, informatie en gegevens. En het kan zo eenvoudig zijn als iets met een vinger aanraken of in een cameralens kijken.

Belangrijke vragen

Wat is het belangrijkste doel bij de praktijktoepassing?

Wordt Windows Hello of Hello for Business gebruikt?

Welke platforms of browsers moeten worden ondersteund?

Hebben gebruikers toegang tot één of meerdere apparaten?

Zijn de voordelen van biometrische lezers bekend?

WIST U DAT?

Bij 81 procent van alle datalekken via hacking werd gebruikgemaakt van gestolen en/of zwakke wachtwoorden.

2020 Verizon Data Breach Investigations Report

Welke vingerafdruksleutel is geschikt voor u?

VeriMark Fingerprint Readers

WIST U DAT?

Multifactorauthenticatie (MFA) maar liefst 99,9% van de hacks op zakelijke accounts tegenhoudt

Microsoft-onderzoek, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Naam	**VeriMark** K67977WW	**VeriMark IT** K64704EU	**VeriMark Desktop** K62330WW
Compatibiliteit	Windows 7/8.1/10 & Web Apps	Windows 7/8.1/10 & MSFT-apps	Windows 7/8.1/10; MSFT- & web-apps
FIDO	FIDO U2F-gecertificeerd	FIDO U2F-gecertificeerd en compatibel met FIDO 2 Web Authn	FIDO U2F-gecertificeerd en compatibel met FIDO 2 Web Authn
Type	Match-on-host	Match-in-sensor	Match-in-sensor
Opgeslagen gegevens	Vingerafdruksjabloon op hostapparaat	Vingerafdruksjabloon op sleutel	Vingerafdruksjabloon op sleutel
False Rejection Rate (Onterechte weigeringsfrequentie)	3%	2%	2%
False Acceptance Rate (Onterechte acceptatiefrequentie)	0,002%	0,001%	0,001%
Leesbaarheid	365 graden	365 graden	365 graden
Beschikbaarheid	**Nu**	**Nu**	**Nu**

Naam	**VeriMark Guard USB-A** K64708WW	**VeriMark Guard USB-C** K64709WW
Compatibiliteit	Windows 7/8.1/10; Mac OS; Chrome OS	Windows 7/8.1/10; Mac OS; Chrome OS
FIDO	FIDO U2F- & FIDO 2-gecertificeerd	FIDO U2F- & FIDO 2-gecertificeerd
Type	Match-in-sensor	Match-in-sensor
Opgeslagen gegevens	Vingerafdruksjabloon Gegevens op sleutel	Vingerafdruksjabloon Gegevens op sleutel
False Rejection Rate (Onterechte weigeringsfrequentie)	2%	2%
False Acceptance Rate (Onterechte acceptatiefrequentie)	0,001%	0,001%
Leesbaarheid	365 graden	365 graden
Beschikbaarheid	**Nu**	**Nu**

NEEM VOOR MEER INFORMATIE CONTACT OP VIA:

sales@kensington.com