Kensington Fingerprint Keys

Warum das Risiko eingehen?

Den neuesten Untersuchungen von Risk Based Security[1] zufolge, ist die Zahl der preisgegebenen Datensätze im Jahr 2020 auf unglaubliche 36 Milliarden angestiegen. In den ersten drei Quartalen des Jahres 2020 gab es 3.932 offiziell gemeldete Datenschutzverletzungen. Ende des zweiten Quartals war es bereits das “schlimmste Jahr in der Geschichte”, hinsichtlich des Missbrauchs vertraulicher Daten.

Wenngleich keine Sicherheitslösung einen hundertprozentigen Schutz garantieren kann, bietet die Biometrie doch ein weiteres starkes Glied in Ihrer Sicherheitskette. Neben der inhärenten Einzigartigkeit der biometrischen Daten einer Person (und dem damit verbundenen Sicherheitsgrad) bietet die Biometrie eine passwortlose Lösung.

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

Sicherheit wo, wann und wie Sie sie brauchen

Unternehmenslösung

VeriMark™ IT, VeriMark™ Desktop und VeriMark™ Guard lassen sich problemlos in eine bestehende IT-Infrastruktur integrieren, bieten eine passwortlose Anmeldung bei Windows Hello, Windows Hello for Business, Microsoft Azure und anderen Microsoft-Diensten auf Edge und erleichtern der IT-Abteilung die Verwaltung von Mitarbeiterzugängen, Berechtigungen und Passwörtern.

Lösung für staatliche Behörden

Verimark™ IT, Desktop und Guard können zur Unterstützung der Cybersicherheitsmaßnahmen eines Unternehmens eingesetzt werden, die mit Datenschutzgesetzen wie DSGVO, BIPA und CCPA übereinstimmen (jedoch nicht darauf beschränkt sind).

OS-Kompatibilität

Der Verimark™ Guard bietet maximale Kompatibilität mit Webdiensten wie Google, Facebook und Microsoft (für Windows Hello siehe VeriMark oder VeriMark IT), mit Unterstützung für Chrome, Edge, Firefox und Safari und plattformübergreifender Betriebssystemunterstützung für Win10, macOS und Chrome OS als FIDO2-Sicherheitsschlüssel.

Warum biometrische Authentifizierung?

Da physische Merkmale wie Fingerabdrücke und Pupillen so schwer zu fälschen sind, ist die biometrische Authentifizierung eine sichere Lösung. Dabei sehen wir die biometrische Authentifizierung als Teil einer umfassenden Sicherheitslösung, die auch ein Passwort und/oder physische Geräte wie Schlüssel, Karten oder Token umfassen kann.

Am Arbeitsplatz kann die biometrische Authentifizierung Teil eines strengen Sicherheitsprotokolls für den Zugang zu internen Systemen, Dateien, Informationen und Daten sein. Und das kann so einfach sein wie die Berührung eines Fingers oder der Blick in ein Kameraobjektiv.

Schlüsselfragen

Was ist das Hauptziel im Anwendungsfall?

Wird Windows Hello oder Hello for Business verwendet?

Welche Plattformen oder Browser müssen unterstützt werden?

Greift der Anwender auf ein einzelnes Gerät oder auf mehrere Geräte zu?

Kennen Sie die Vorteile biometrischer Lesegeräte?

SCHON GEWUSST?

81 Prozent der Datenschutzverletzungen durch Hacker wurden durch gestohlene und/oder schwache Passwörter verursacht.

2020 Verizon Data Breach Investigations Report

Welcher Fingerprint Key ist der richtige für Sie?

VeriMark™ Fingeprint Keys

SCHON GEWUSST?

Multifaktor-Authentifizierung (MFA) blockiert beeindruckende 99,9 % der Hacks von Unternehmenskonten.

Microsoft Studie, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Produktname	VeriMark™	VeriMark™ IT	VeriMark™ Desktop
Kompatibilität	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 zertifiziert	FIDO U2F zertifiziert und FIDO 2 WebAuthn-kompatibel	FIDO U2F zertifiziert und FIDO 2 WebAuthn-kompatibel
Typ	Match-on-Host	Match-in-Sensor	Match-in-Sensor
Speicherort	Fingerprint wird im Host-Gerät (z.B. Laptop) gespeichert	Fingerprint wird im Schlüssel gespeichert	Fingerprint wird im Schlüssel gespeichert
Falsch-Zurückweisungsrate (FRR)	3%	2%	2%
Falsch-Akzeptanzrate (FAR)	0,002%	0,001%	0,001%
Lesbarkeit	365 Grad	365 Grad	365 Grad
Verfügbarkeit	**Lieferbar**	**Lieferbar**	**Lieferbar**

Produktname	VeriMark™ Guard USB-A	VeriMark™ Guard USB-C
Kompatibilität	Windows 7/8.1/10; macOS; Chrome OS	Windows 7/8.1/10; macOS; Chrome OS
FIDO	FIDO U2F & FIDO 2 zertifiziert	FIDO U2F & FIDO 2 zertifiziert
Typ	Match-in-Sensor	Match-in-Sensor
Speicherort	Fingerprint im Schlüssel gespeichert	Fingerprint im Schlüssel gespeichert
Falsch-Zurückweisungsrate (FRR)	2%	2%
Falsch-Akzeptanzrate (FAR)	0,001%	0,001%
Lesbarkeit	365 Grad	365 Grad
Verfügbarkeit	**Lieferbar**	**Lieferbar**

WEITERE INFORMATIONEN ERHALTEN SIE UNTER:

sales.dach@kensington.com