Kensington Lecteurs d’empreintes digitales

Pourquoi prendre des risques ?

Une récente étude de Risk Based Security[1] a révélé que le nombre d'enregistrements exposés a augmenté pour atteindre le chiffre vertigineux de 36 milliards en 2020. Quelque 3932 violations de données ont été rendues publiques au cours des trois premiers trimestres de 2020. Fin juin, il s'agissait déjà « la plus mauvaise année jamais écoulée » compte tenu du nombre de données exposées.

Bien qu'aucune solution de sécurité ne puisse garantir une protection totale, la biométrie reste une maille supplémentaire solide dans votre chaîne de sécurité. En plus du caractère unique des données biométriques d'un individu (et par conséquent du niveau de sécurité proposé), la biométrie permet une solution sans mot de passe.

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

La sécurité où, quand et comme vous le souhaitez !

Déploiement en entreprise

VeriMark IT, VeriMark Desktop et VeriMark Guard s'intègrent facilement dans une infrastructure IT existante : Ils rendent possible une connexion sans mot de passe à Windows Hello, Windows Hello for Business, Microsoft Azure et à d'autres services Microsoft sur Edge et permettent au service informatique de gérer sans difficulté les accès, privilèges et mots de passe des employés.

Conforme aux normes en vigueur

VeriMark IT, Desktop et Guard peuvent être utilisés parmi les mesures de lutte contre la cybercriminalité d'une entreprise conformément (mais sans se limiter) aux réglementations sur la confidentialité des données (RGPD, BIPA, CCPA, etc.).

Compatibilité avec les OS

VeriMark Guard offre une compatibilité maximale avec des services web tels que Google, Facebook et Microsoft (pour Windows Hello, voir la clé VeriMark ou VeriMark IT), il prend en charge Chrome, Edge, Firefox et Safari et offre une prise en charge inter-plateformes pour Windows 10, Mac OS et Chrome OS comme une clé de sécurité FIDO2.

Pourquoi une authentification biométrique ?

Tout simplement parce que les caractéristiques physiques telles que les empreintes digitales ou les pupilles sont particulièrement difficiles à contrefaire. Pour nous, elle doit être considérée comme une composante d'une solution complète, comprenant aussi des mots de passe et/ou une solution physique comme une clé, une carte ou un badge.

Sur le lieu de travail, la biométrie peut faire partie d'un protocole de sécurité puissant qui restreint l'accès aux systèmes, fichiers, informations et données internes. Mais l'appliquer peut être aussi simple que de placer un doigt sur un capteur ou regarder l'objectif d'un appareil photo.

Questions clés

Quel est mon principal objectif ?

Windows Hello ou Hello for Business est-il sollicité ?

Quelles plateformes ou quels navigateurs doivent être reconnus ?

Les utilisateurs accèdent-ils à un seul ou plusieurs appareils ?

Quels sont les avantages d'un lecteur biométrique ?

LE SAVIEZ-VOUS ?

81 % des violations par piratage ont exploité des mots de passe volés et/ou trop faibles.

Rapport d'enquête Verizon 2020 sur les violations de données

Quelle clé à empreintes digitales pour vos besoins ?

Lecteurs d'empreintes digitales VeriMark

LE SAVIEZ-VOUS ?

L'authentification multifacteurs (MFA) permet de bloquer 99,9% des piratages de comptes d'entreprise.

Etude de Microsoft, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Nom	**VeriMark** K67977WW	**VeriMark IT** K64704EU	**VeriMark Desktop** K62330WW
Compatibilité	Windows 7/8.1/10 & applications Web	Windows 7/8.1/10 & Applications Microsoft	Windows 7/8.1/10; Applications Microsoft & Web
FIDO	Certifié FIDO U2F	Certifié FIDOU2F et compatible FIDO 2 Web Authn	Certifié FIDO U2F et compatible FIDO 2 Web Authn
Type	Match-on-Host (Correspondance hôte)	Match-in-Sensor (Correspondance capteur)	Match-in-Sensor (Correspondance capteur)
Données stockées	Le modèle d'empreintes digitales est stocké dans l'appareil hôte	Le modèle d'empreintes digitales est stocké dans la clé	Le modèle d'empreintes digitales est stocké dans la clé
False Rejection Rate (Taux de faux rejet)	3%	2%	2%
False Acceptance Rate (Taux de fausse acceptation)	0,002%	0,001%	0,001%
Lisibilité	365 degrés	365 degrés	365 degrés
Disponibilité	**Dès maintenant**	**Dès maintenant**	**Dès maintenant**

Nom	**VeriMark Guard USB-A** K64708WW	**VeriMark Guard USB-C** K64709WW
Compatibilité	Windows 7/8.1/10 ; Mac OS; Chrome OS	Windows 7/8.1/10 ; Mac OS; Chrome OS
FIDO	Certifié FIDO U2F & FIDO 2	Certifié FIDO U2F & FIDO 2
Type	Match-in-Sensor (Correspondance capteur)	Match-in-Sensor (Correspondance capteur)
Données stockées	Le modèle d'empreintes digitales est stocké dans la clé	Le modèle d'empreintes digitales est stocké dans la clé
False Rejection Rate (Taux de faux rejet)	2%	2%
False Acceptance Rate (Taux de fausse acceptation)	0,001%	0,001%
Lisibilité	365 degrés	365 degrés
Disponibilité	**Dès maintenant**	**Dès maintenant**

POUR TOUTE INFORMATION COMPLÉMENTAIRE, ÉCRIVEZ À

contact@kensington.com