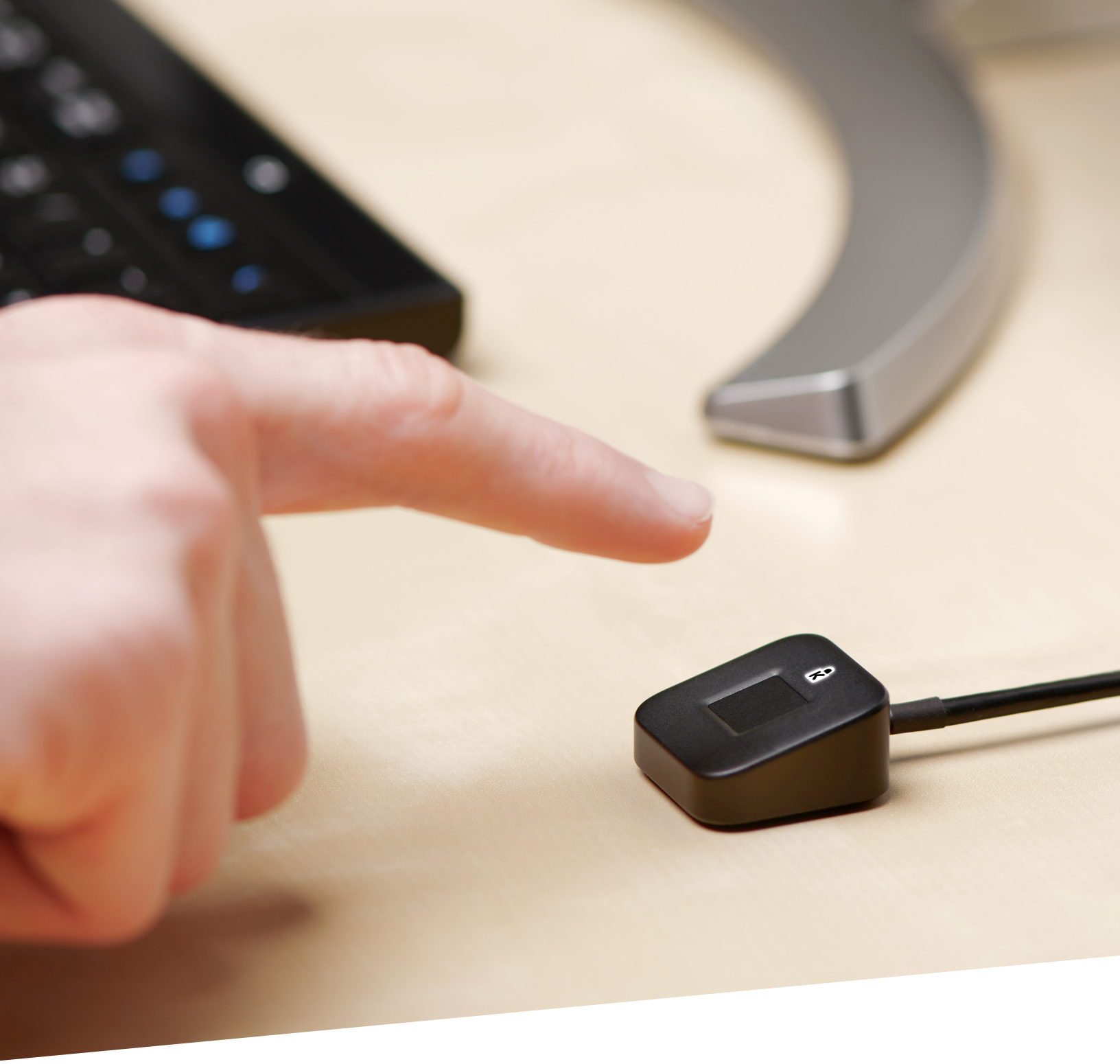
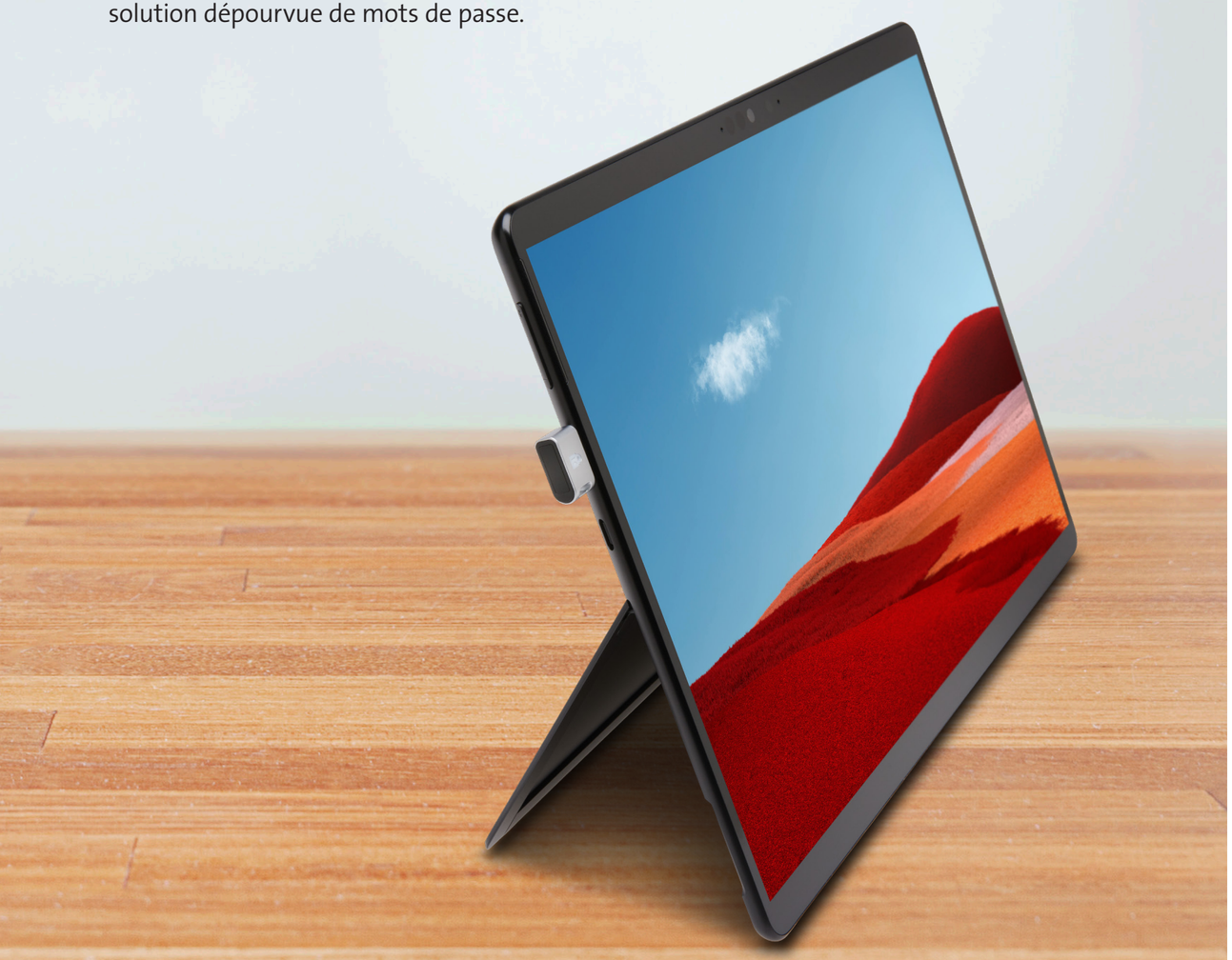


Kensington Lecteurs d’empreintes digitales

Pourquoi courir le risque?

Des données récentes de Risk Based Security[1] montre que le nombre de dossiers exposés a atteint pas moins de 36 milliards en 2020. 3 932 violations de données ont été divulguées publiquement lors des trois premiers trimestres de 2020. La fin du T2 marquait déjà la « pire année jamais enregistrée » quant au nombre total de dossiers exposés.

Même si aucune solution de sécurité n'assure une protection complète, la biométrie est un maillon sûr dans votre chaîne de défense. En plus du caractère unique des données biométriques d'une personne (et, par conséquent, le degré de sécurité qu'elles offrent), la biométrie est une solution dépourvue de mots de passe.

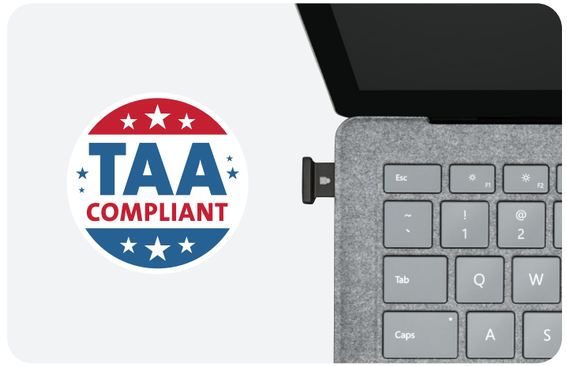


[1] *https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf*

La sécurité là où vous en avez besoin, au moment où vous en avez besoin, comme vous en avez besoin

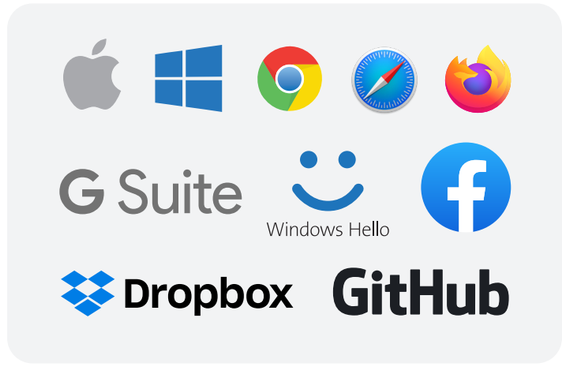
Déploiement en entreprise

Les lecteurs VeriMark IT, VeriMark Desktop et VeriMark Guard s'intègrent facilement à l'infrastructure TI actuelle, offrent l'authentification exempte de mot de passe à Windows Hello, Windows Hello Entreprise et aux autres services de Microsoft par l'entremise de Edge, et permettent au service des TI de gérer facilement les droits et les privilèges d'accès ainsi que les mots de passe des employés.



Usage gouvernemental

Les lecteurs VeriMark IT, VeriMark Desktop et VeriMark Guard peuvent contribuer à la mise en œuvre des mesures de cybersécurité d'une société conformément aux lois protégeant la vie privée, notamment le RGPD, la BIPA et la CCPA.



Compatibilité avec les systèmes d'exploitation

Le lecteur Verimark Guard assure une compatibilité maximale avec les services Web, dont Google, Facebook et Microsoft (pour Windows Hello, reportez-vous aux lecteurs VeriMark ou VeriMark IT) et la prise en charge de Chrome, Edge, Firefox et Safari. À titre de clé de sécurité FIDO2, il procure aussi une compatibilité multiplateforme avec les systèmes d'exploitation Win10, mac et Chrome.

Pourquoi choisir l'authentification biométrique?

Les caractéristiques physiques, comme les empreintes digitales et les pupilles, sont difficiles à falsifier; la biométrie procure donc une solution très sécuritaire. À notre avis, elle vient compléter une solution sécuritaire incluant par exemple un mot de passe et un appareil physique, comme une clé, une carte ou un jeton.

En milieu de travail, la biométrie s'inscrit parfois dans un protocole de sécurité rigoureux pour accéder à des systèmes internes, des fichiers, des renseignements et des données. Il peut s'agir simplement de poser un doigt ou de regarder dans la lentille d'une caméra.

Questions principales

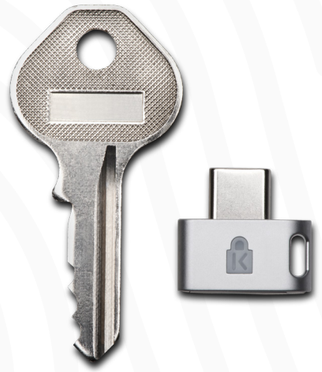
Quel est le principal objectif du cas d'utilisation?

Le service Windows Hello ou Windows Hello Entreprise est-il utilisé?

Quels sont les plateformes ou navigateurs devant être pris en charge?

L'utilisateur peut-il accéder à un seul périphérique ou à plusieurs périphériques?

Connaissez-vous les avantages que procurent les lecteurs biométriques?

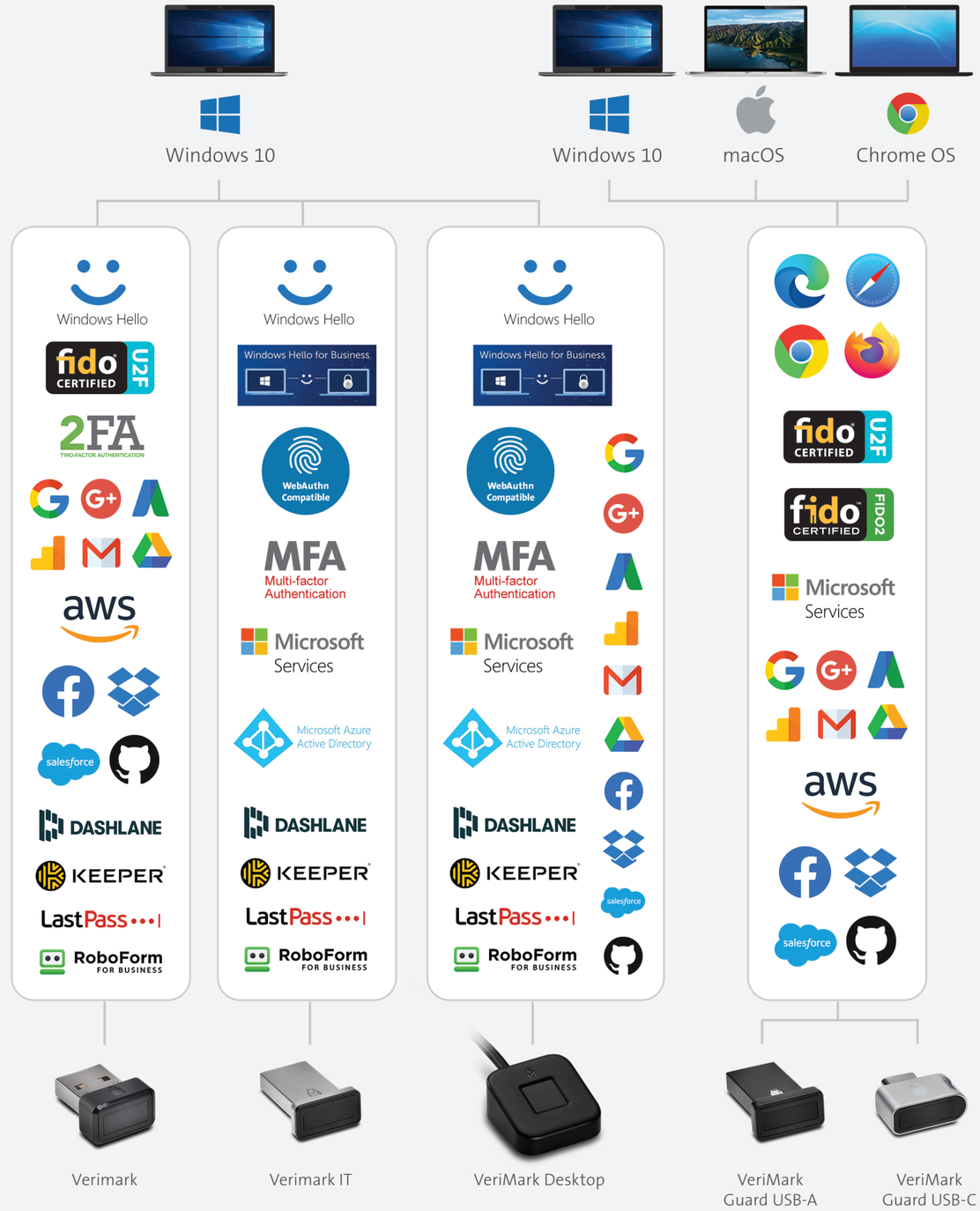


LE SAVIEZ-VOUS?

81 pour cent des failles résultant d'un piratage ont été facilitées par des mots de passe volés ou peu complexes.

Rapport d'enquête sur les violations de données de Verizon en 2020

Quel lecteur d'empreintes digitales vous convient?



Lecteurs d’empreintes digitales VeriMark

LE SAVIEZ-VOUS?

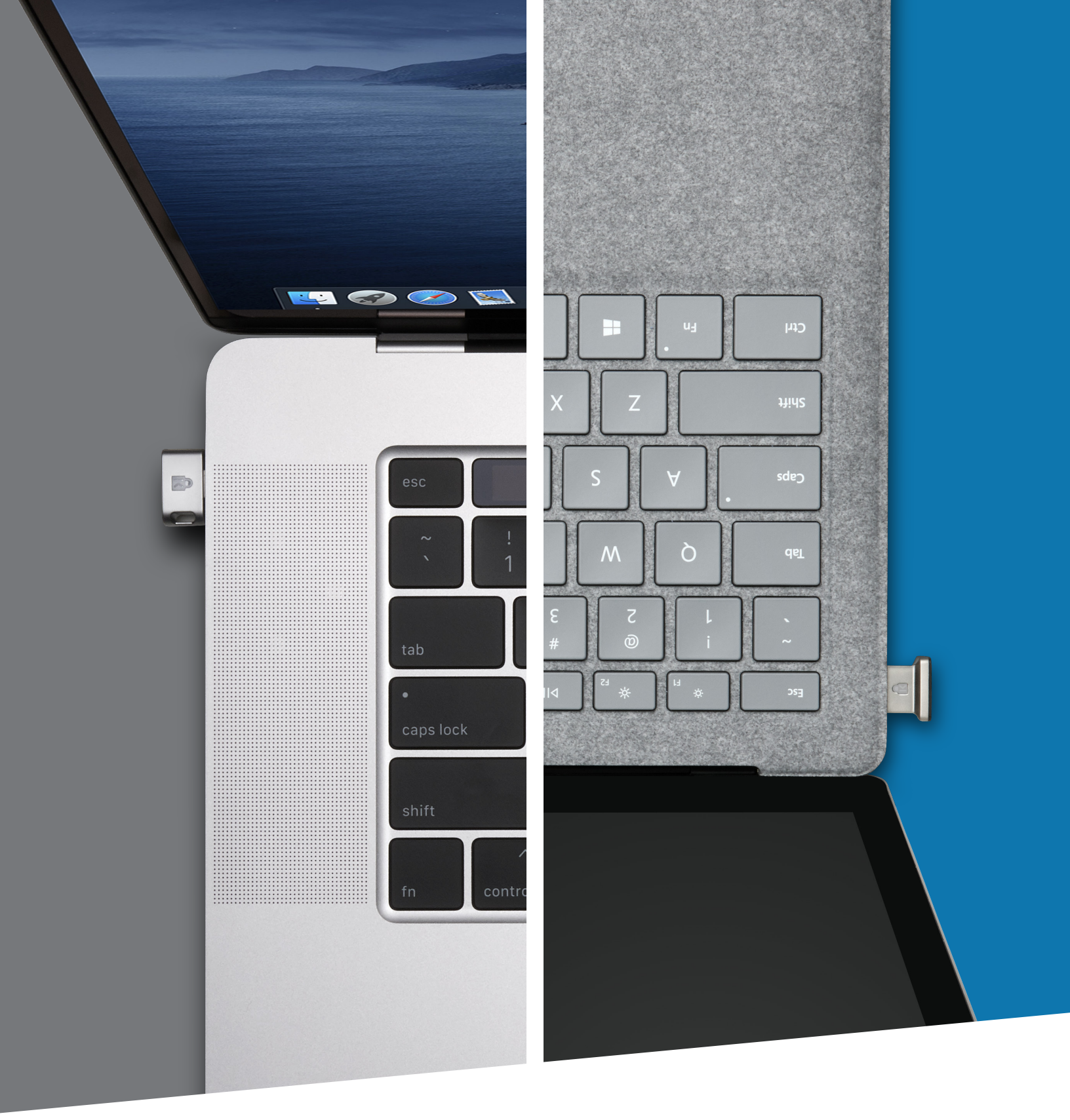
L’authentification multifacteur (AMF) empêche pas moins de 99,9 % des tentatives de piratage de comptes en entreprise.

Étude de Microsoft, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Nom	**Verimark** K67977WW	**Verimark IT** K64704WW	**VeriMark Desktop** K62330WW
Compatibilité	Windows 7/8.1/10 et applications Web	Windows 7/8.1/10 et applications MSFT	Windows 7/8.1/10 et applications Web et MSFT
FIDO	Certification de FIDO U2F	Certification FIDOU2F et compatibilité FIDO2 Web Authn	Certification FIDOU2F et compatibilité FIDO2 Web Authn
Type	Correspondance hôte	Correspondance capteur	Correspondance capteur
Données stockées	Modèle d’empreintes digitales dans l’appareil hôte	Données du modèle d’empreintes digitales stockées dans le lecteur	Données du modèle d’empreintes digitales stockées dans le lecteur
Taux de rejets erronés	3%	2%	2%
Taux d’acceptations erronées	0,002%	0,001%	0,001%
Lisibilité	365 degrés	365 degrés	365 degrés
Disponibilité	**Maintenant**	**Maintenant**	**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	Certification de FIDO U2F et de FIDO 2	Certification de FIDO U2F et de FIDO 2
Type	Correspondance capteur	Correspondance capteur
Données stockées	Modèle d’empreintes digitales Données stockées dans le lecteur	Modèle d’empreintes digitales Données stockées dans le lecteur
Taux de rejets erronés	2%	2%
Taux d’acceptations erronées	0,001%	0,001%
Lisibilité	365 degrés	365 degrés
Disponibilité	**Maintenant**	**Maintenant**



POUR DE PLUS AMPLES RENSEIGNEMENTS :

sales@kensington.com