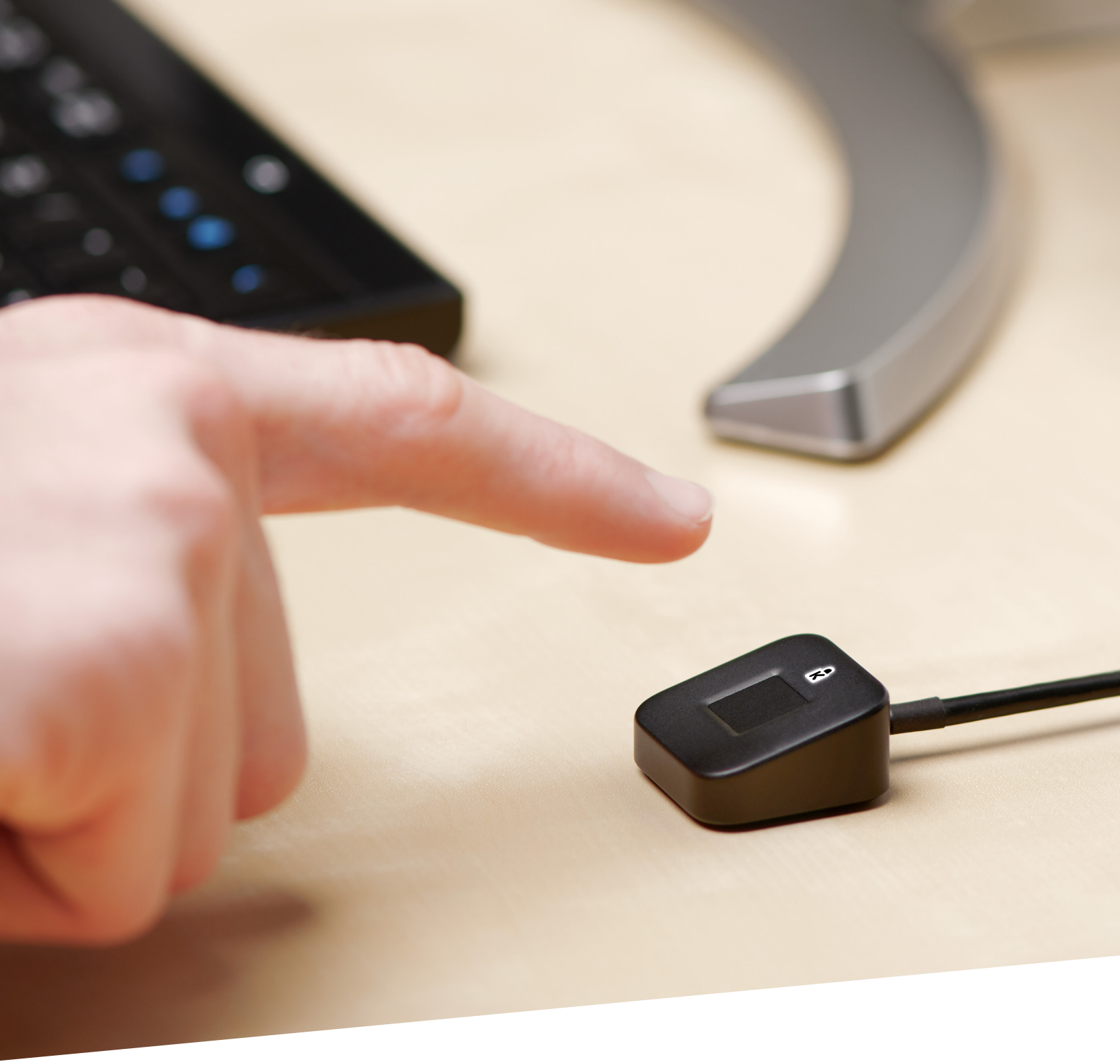
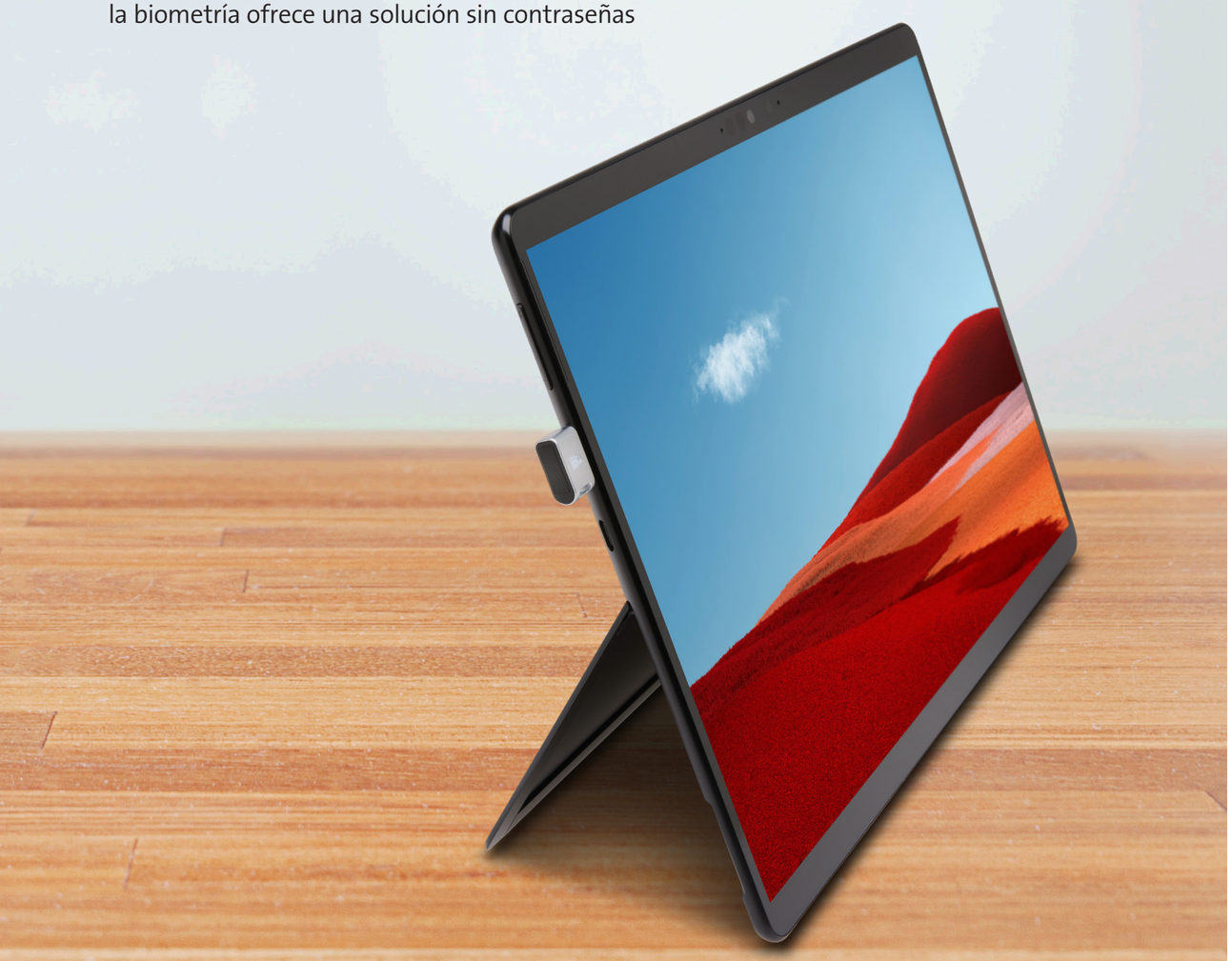


Kensington Lectores de huellas dactilares

¿Por qué jugársela?

Datos recientes de Risk Based Security[1] muestran que el número de registros expuestos ha aumentado a la sorprendente cifra de 36 000 millones en 2020. En los tres primeros trimestres de 2020 se produjeron 3932 infracciones notificadas públicamente. Al final del segundo trimestre, ya era el “peor año registrado” en términos del número total registros expuestos.

Aunque no existe ninguna solución de seguridad que pueda garantizar una completa protección, la biometría es otro eslabón importante en la cadena de seguridad. Además del carácter único inherente de los datos biométricos de un individuo (y el nivel de seguridad que esto ofrece), la biometría ofrece una solución sin contraseñas

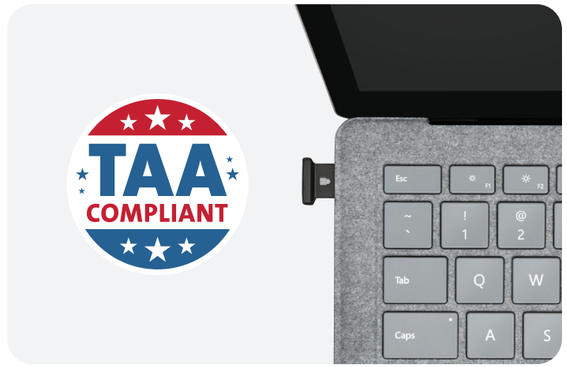


[1] *https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf*

Seguridad donde, cuando y como la necesite

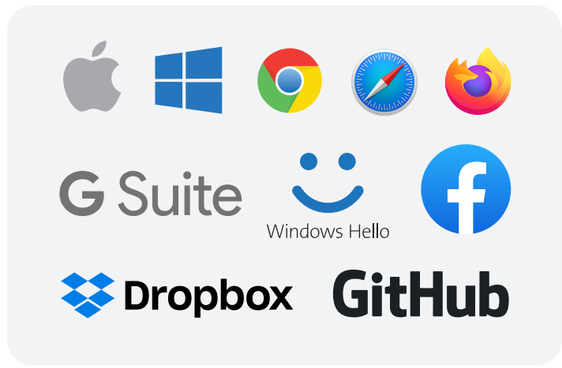
Despliegue para empresas

VeriMark IT, VeriMark Desktop y VeriMark Guard se integran de manera fácil en una infraestructura informática existente, ofrecen un inicio de sesión sin contraseña para Windows Hello, Windows Hello para empresas, Microsoft Azure y otros servicios de Microsoft en Edge, y hacen que sea fácil para los equipos de TI gestionar el acceso de los empleados y sus privilegios y contraseñas.



Uso gubernamental

VeriMark IT, Desktop y Guard pueden utilizarse para respaldar las medidas de ciberseguridad de una empresa de acuerdo con (y sin limitarse a) las leyes de privacidad, como RGPD, BIPA y CCPA.



Compatibilidad con iOS

Verimark Guard ofrece máxima compatibilidad con servicios web como Google, Facebook y Microsoft (para Windows Hello, consulte VeriMark o VeriMark IT), admite Chrome, Edge, Firefox y Safari, y ofrece compatibilidad con sistemas operativos de diversas plataformas para Win10, macOS y Chrome OS como clave de seguridad FIDO2.

¿Por qué usar la autenticación biométrica?

Debido a que las características físicas como la huella dactilar y la pupila son mucho más difíciles de falsificar, la biometría es una solución de seguridad sólida, aunque sea una parte de una solución de seguridad completa que puede incluir además una contraseña o un dispositivo en físico como una llave, tarjeta o ficha.

En el lugar de trabajo, la biometría puede ser parte de un protocolo de seguridad sólido para acceder a sistemas, archivos, información y datos internos. Y es tan fácil como tocar con el dedo o mirar en la lente de una cámara.

Preguntas principales

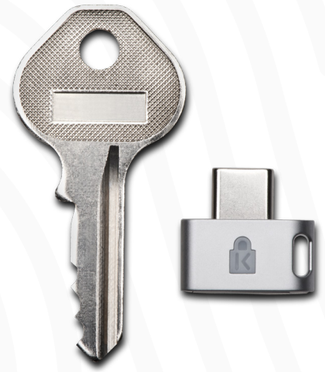
¿Cuál es el objetivo clave en el caso de uso?

¿Se utiliza Windows Hello o Hello para empresas?

¿Qué plataformas o navegadores se admiten?

¿El usuario accede a uno o varios dispositivos?

¿Conoce las ventajas de los lectores biométricos?

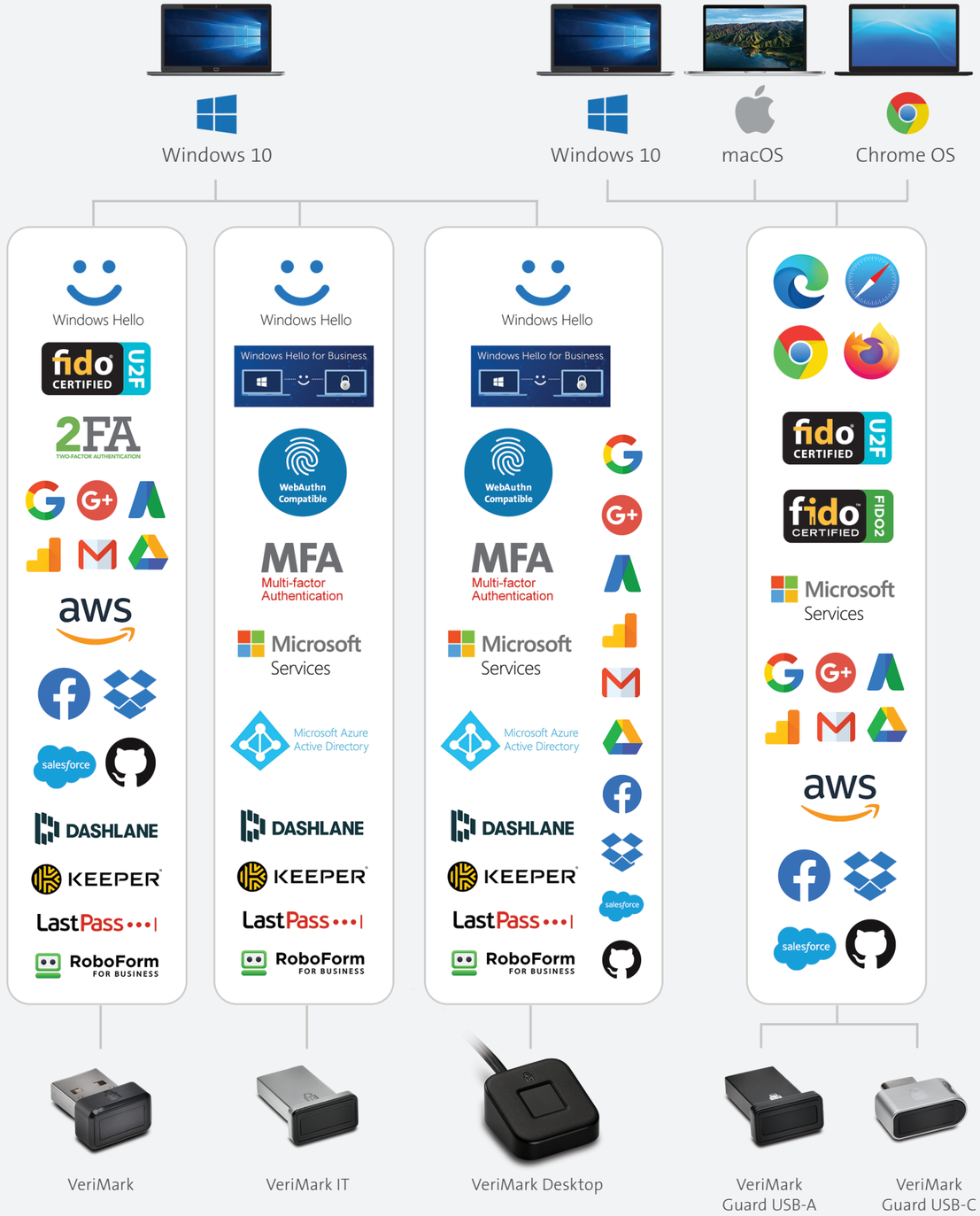


¿SABÍA QUE...?

El 81 % de las infracciones relacionadas con los ataques informáticos aprovecharon contraseñas robadas o poco seguras.

Informe de investigación sobre infracciones en la seguridad de los datos en 2020 de Verizon

¿Qué llave de huella digital es adecuada para usted?



Lectores de huellas dactilares VeriMark

¿SABÍA QUE...?

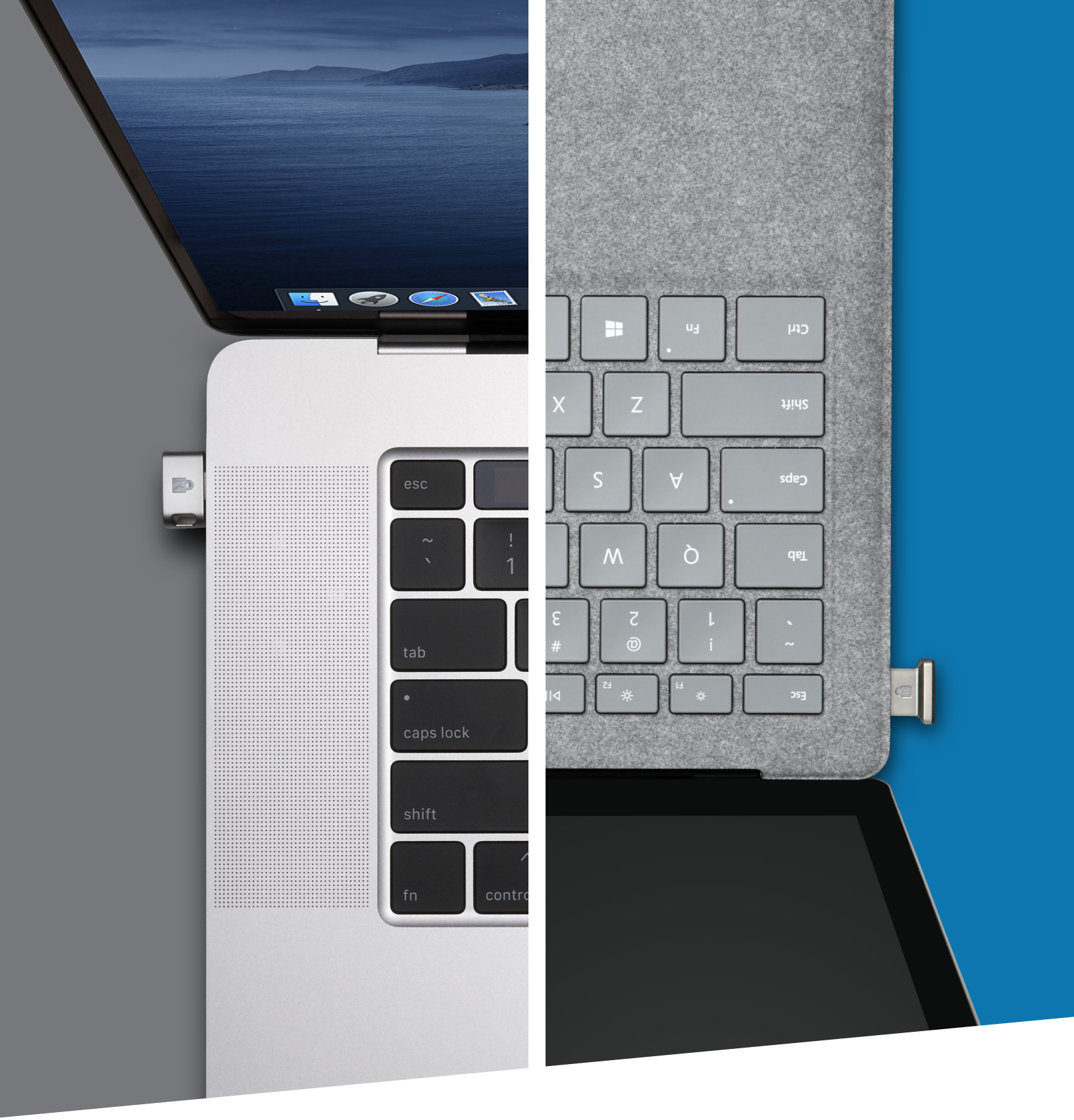
La autenticación multifactor (MFA) bloquea hasta un asombroso 99,9 % de los ataques informáticos a cuentas empresariales

Estudio de Microsoft de 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Nombre	**VeriMark** K67977WW	**VeriMark IT** K64704EU	**VeriMark Desktop** K62330WW
Compatibilidad	Windows 7/8.1/10 y aplicaciones web	Windows 7/8.1/10 y aplicaciones MSFT	Windows 7/8.1/10 y aplicaciones MSFT y web
FIDO	Certificación U2F de FIDO	Certificación U2F de FIDO y compatibilidad con la autenticación web de FIDO 2	Certificación U2F de FIDO y compatibilidad con la autenticación web de FIDO 2
Tipo	Coincidencia en host	Coincidencia en sensor	Coincidencia en sensor
Datos almacenados	Plantilla de huellas dactilares en dispositivo host	Datos de la plantilla de huellas dactilares en la llave	Datos de la plantilla de huellas dactilares en la llave
Tasa de falso rechazo	3%	2%	2%
Tasa de falsa aceptación	0,002%	0,001%	0,001%
Facilidad de lectura	365 grados	365 grados	365 grados
Disponibilidad	**Disponible actualmente**	**Disponible actualmente**	**Disponible actualmente**

Nombre	**VeriMark Guard USB-A** K64708WW	**VeriMark Guard USB-C** K64709WW
Compatibilidad	Windows 7/8.1/10, Mac OS y Chrome OS	Windows 7/8.1/10, Mac OS y Chrome OS
FIDO	Certificación U2F de FIDO y FIDO 2	Certificación U2F de FIDO y FIDO 2
Tipo	Coincidencia en sensor	Coincidencia en sensor
Datos almacenados	Plantilla de huellas dactilares Datos en la llave	Plantilla de huellas dactilares Datos en la llave
Tasa de falso rechazo	2%	2%
Tasa de falsa aceptación	0,001%	0,001%
Facilidad de lectura	365 grados	365 grados
Disponibilidad	**Disponible actualmente**	**Disponible actualmente**



PARA OBTENER MÁS INFORMACIÓN, PÓNGASE EN CONTACTO CON:

sales@kensington.com