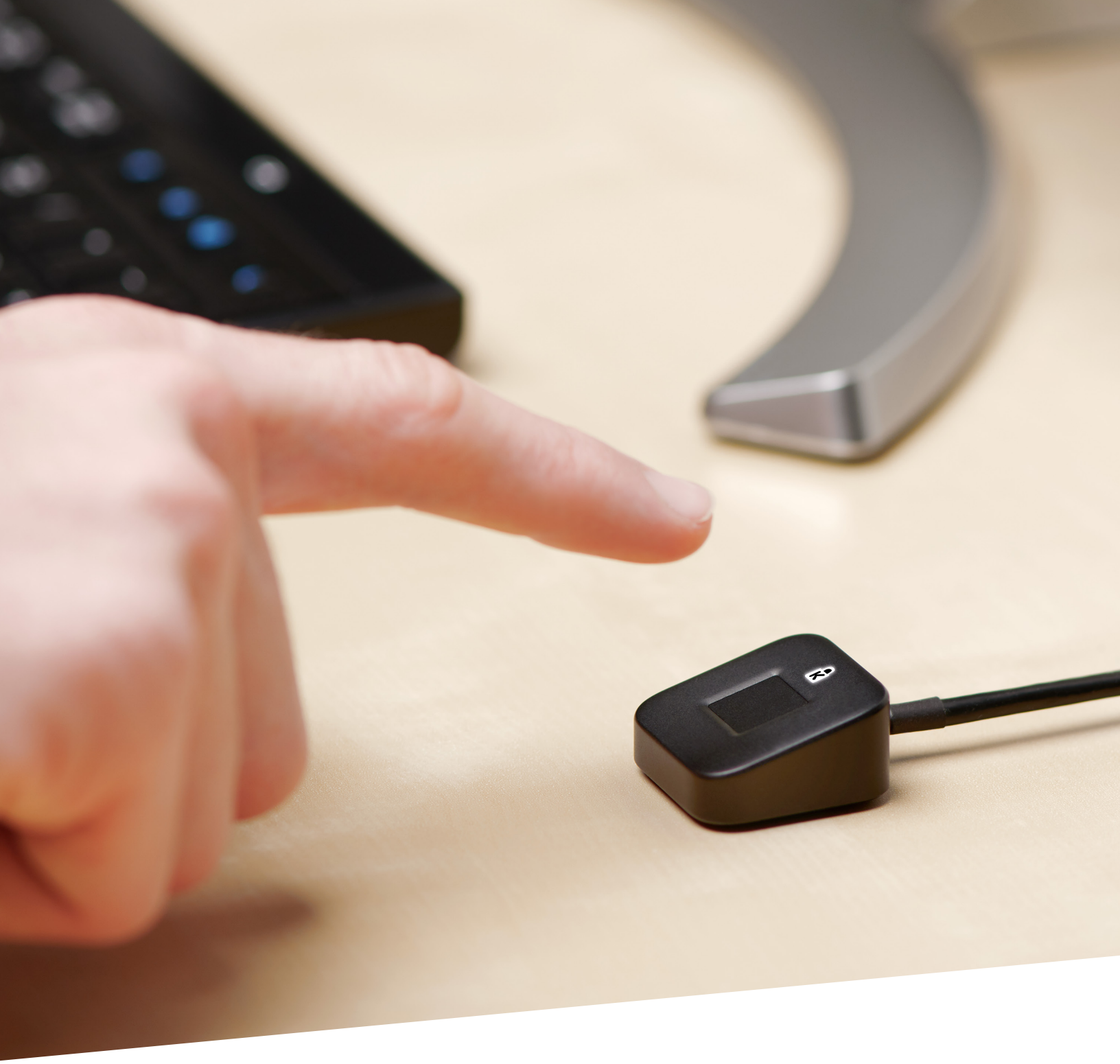
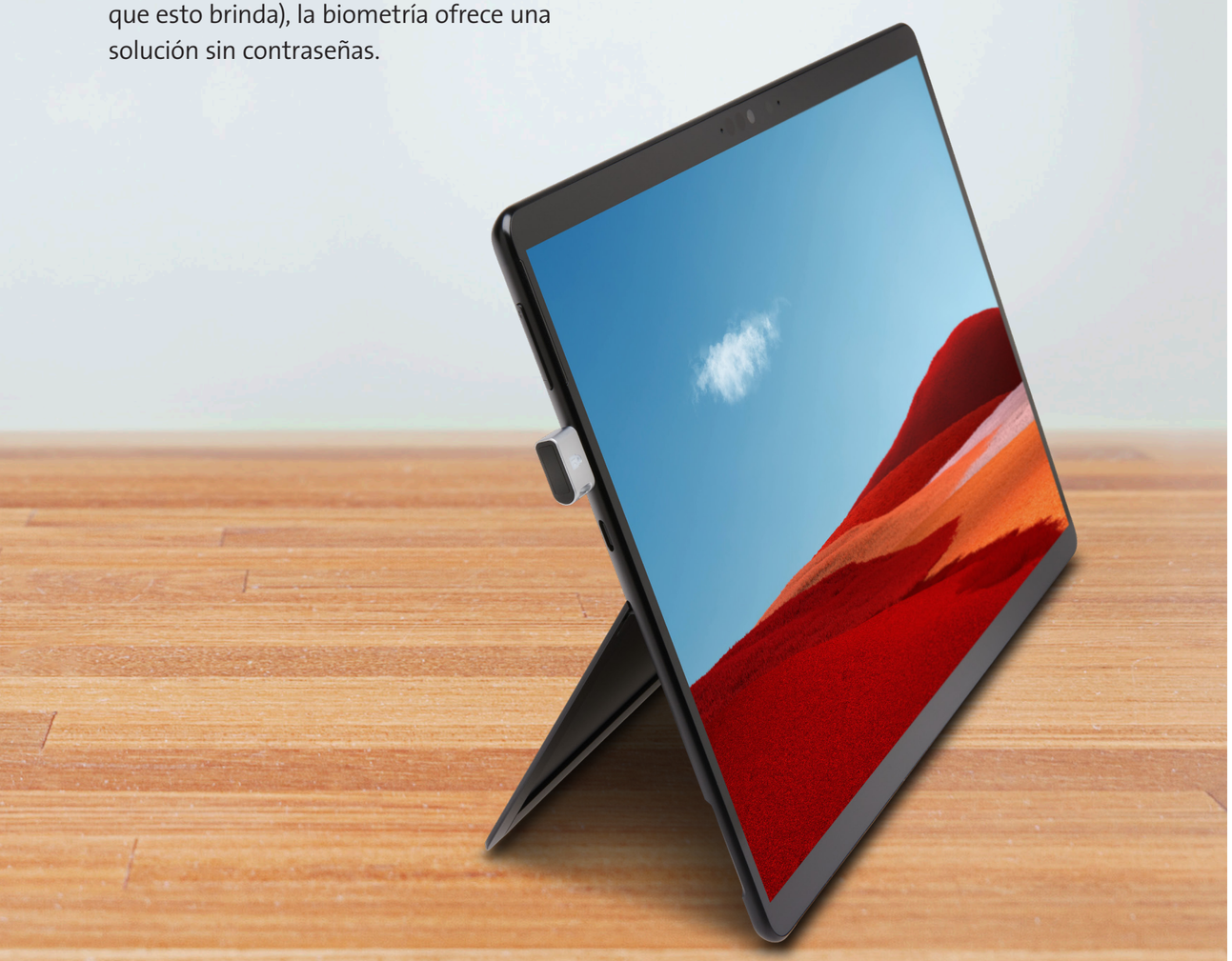


Kensington Lectores de huellas digitales

¿Por qué arriesgarse?

En los datos recientes de Risk Based Security[1] se reveló que el número de registros expuestos ha aumentado hasta la cifra asombrosa 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.

Si bien no existe ninguna solución de seguridad que pueda garantizar una protección total, la biometría constituye otro eslabón resistente en su cadena de seguridad. Además de la singularidad inherente de los datos biométricos de una persona (y, por lo tanto, del nivel de seguridad que esto brinda), la biometría ofrece una solución sin contraseñas.

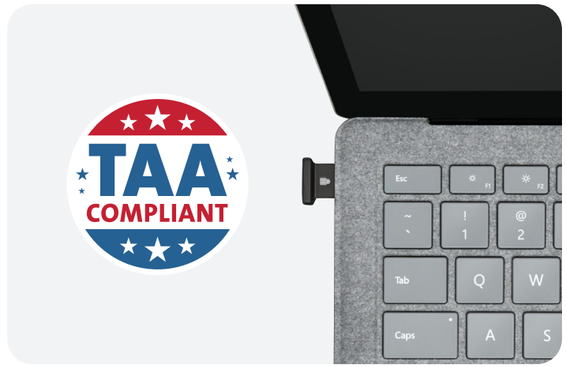


[1] *https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf*

Seguridad donde, cuando y como la necesita

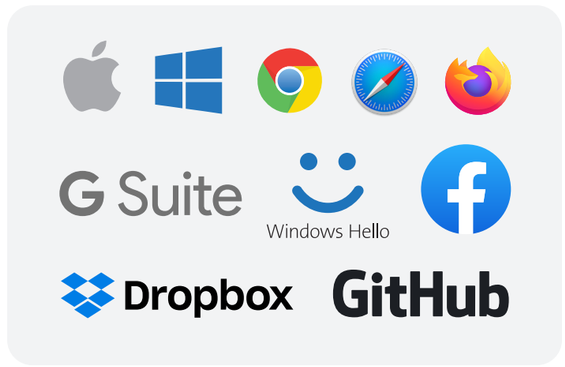
Uso empresarial

Las llaves VeriMark para TI, VeriMark para escritorio y VeriMark Guard se integran fácilmente en la infraestructura informática existente, ofrece la posibilidad de iniciar sesión sin contraseñas en Windows Hello, Windows Hello para empresas, Microsoft Azure y otros servicios de Microsoft Edge, y le permite al equipo de TI gestionar fácilmente las contraseñas, los privilegios y el acceso de los empleados.



Uso gubernamental

VeriMark para TI, para escritorio y Guard cumplen con la TAA y se pueden usar para respaldar las medidas de ciberseguridad de una empresa de acuerdo con (pero sin limitarse a) leyes de privacidad, como el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad de Información Biométrica (BIPA) y la Ley de Privacidad del Consumidor de California (CCPA).



Compatibilidad con OS

VeriMark Guard ofrece máxima compatibilidad con los servicios web, como Google, Facebook y Microsoft (para Windows Hello, consultar VeriMark o VeriMark para TI), compatible con Chrome, Edge, Firefox y Safari, y con sistemas operativos de múltiples plataformas para Win10, mac OS y Chrome OS como llave de seguridad FIDO2.

¿Por qué autenticación biométrica?

Debido a que las características físicas como las huellas digitales y las pupilas son tan difíciles de falsificar, la biometría constituye una buena solución de seguridad. Sin embargo, consideramos que la biometría es solo una parte de una solución de seguridad integral que también puede incluir una contraseña o un dispositivo físico, como una llave, una tarjeta o una ficha.

En el lugar de trabajo, la biometría puede formar parte de un buen protocolo de seguridad para autorizar el acceso a sistemas internos, archivos, información y datos. Y puede consistir en algo tan simple como tocar con un dedo o mirar al lente de una cámara.

Preguntas clave:

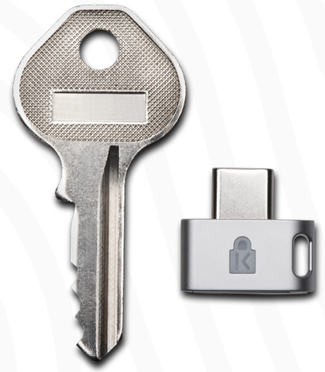
¿Cuál es el objetivo clave en el caso de uso?

¿Se está usando Windows Hello o Hello para empresas?

¿Qué plataformas o navegadores deben ser compatibles?

¿El usuario accede a un solo dispositivo o a varios?

¿Conoce las ventajas del lector biométrico?

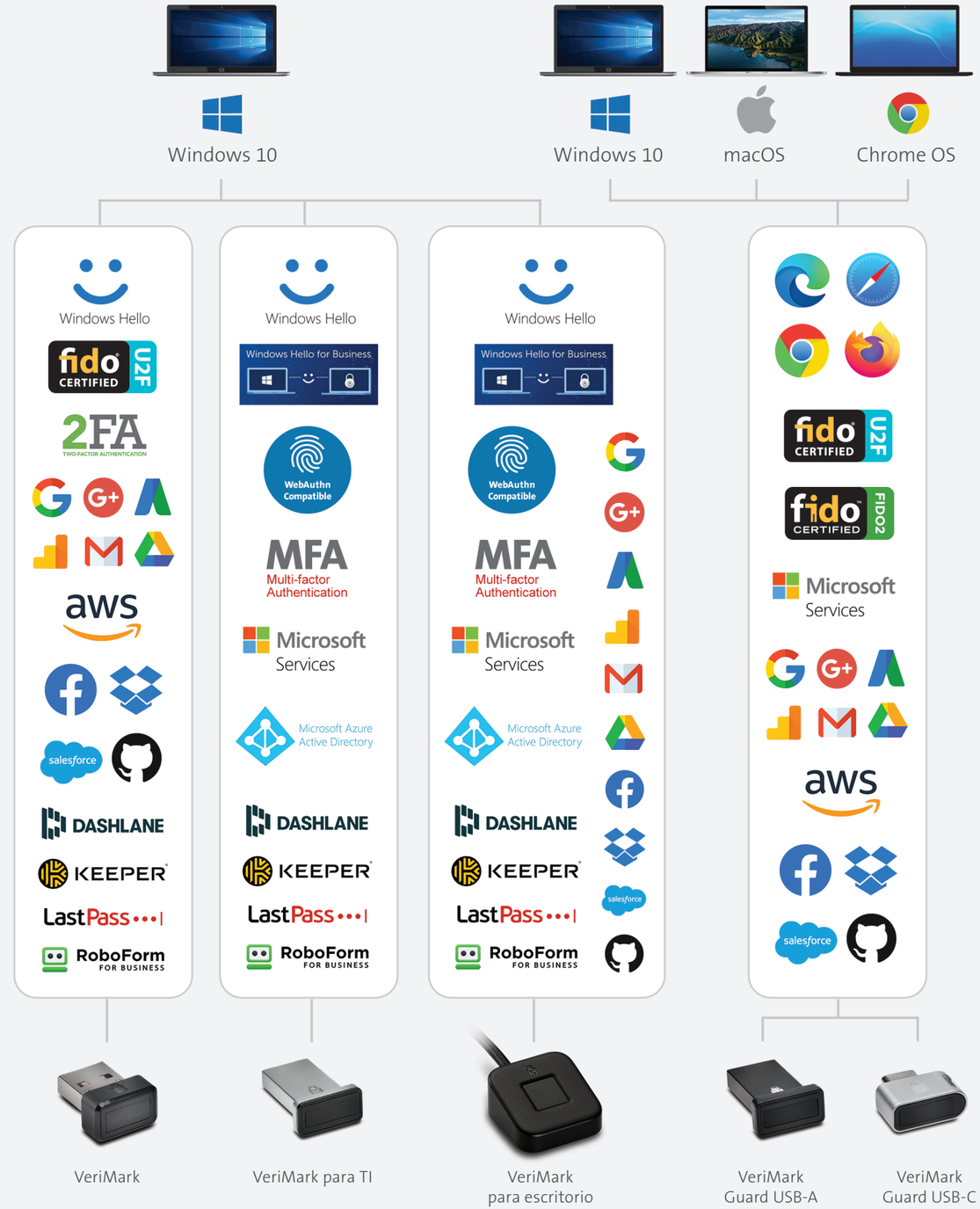


¿SABÍA QUE...?

el 81 % de las infracciones relacionadas con la piratería aprovecharon contraseñas robadas o poco seguras.

Informe sobre Investigaciones de Filtraciones de Datos de Verizon de 2020

¿Qué llave de huella digital es adecuada para usted?



Lectores de huellas digitales de VeriMark

¿SABÍA QUE...?

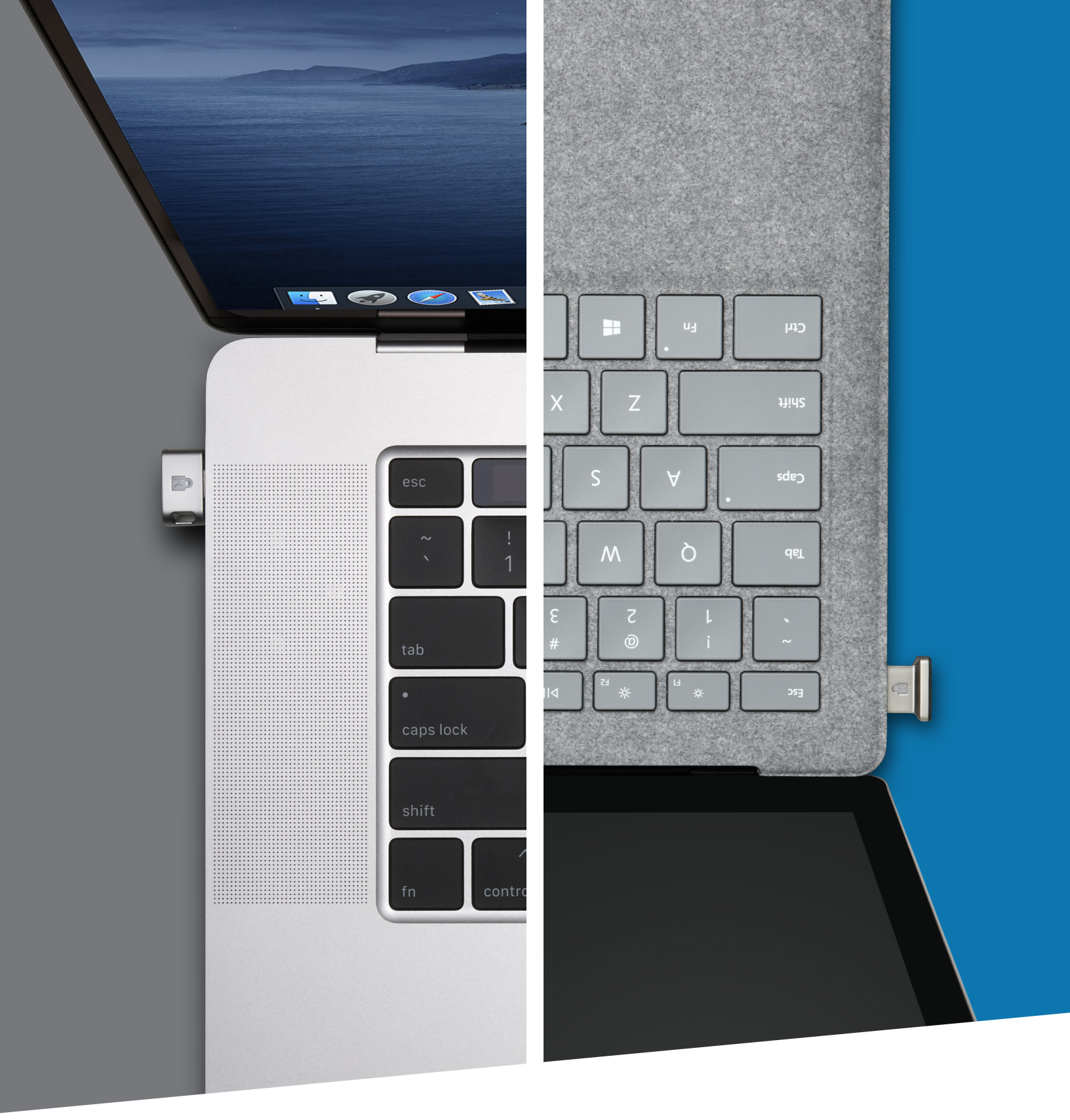
La autenticación de múltiples factores (MFA) bloquea hasta un asombroso 99,9 % de los hackeos de cuentas empresariales

Microsoft Study, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Nombre	**VeriMark** K67977WW	**VeriMark para TI** K64704WW	**VeriMark para escritorio** 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
FIDO	Certificado FIDO U2F	Certificado FIDOU2F y compatible con FIDO 2 Web Authn	Certificado FIDOU2F y compatible con FIDO 2 Web Authn
Tipo	Match-on-Host	Match-in-Sensor	Match-in-Sensor
Datos almacenados	Plantilla de huellas digitales en el dispositivo Host	Datos de la plantilla de huellas digitales en la llave	Datos de la plantilla de huellas digitales en la llave
Tasa de falso rechazo	3%	2%	2%
Tasa de falsa aceptación	0,002%	0,001%	0,001%
Legibilidad	365 grados	365 grados	365 grados
Disponibilidad	**Ahora**	**Ahora**	**Ahora**

Nombre	**VeriMark Guard USB-A** K64708WW	**VeriMark Guard USB-C** K64709WW
Compatibilidad	Windows 7/8.1/10; Mac OS; Chrome OS	Windows 7/8.1/10; Mac OS; Chrome OS
FIDO	Certificado FIDO U2F y FIDO 2	Certificado FIDO U2F y FIDO 2
Tipo	Match-in-Sensor	Match-in-Sensor
Datos almacenados	Datos de la plantilla de huellas digitales en la llave	Datos de la plantilla de huellas digitales en la llave
Tasa de falso rechazo	2%	2%
Tasa de falsa aceptación	0,001%	0,001%
Legibilidad	365 grados	365 grados
Disponibilidad	**Ahora**	**Ahora**



PARA OBTENER MÁS INFORMACIÓN, COMUNÍQUESE A LA SIGUIENTE DIRECCIÓN DE CORREO ELECTRÓNICO:

sales@kensington.com