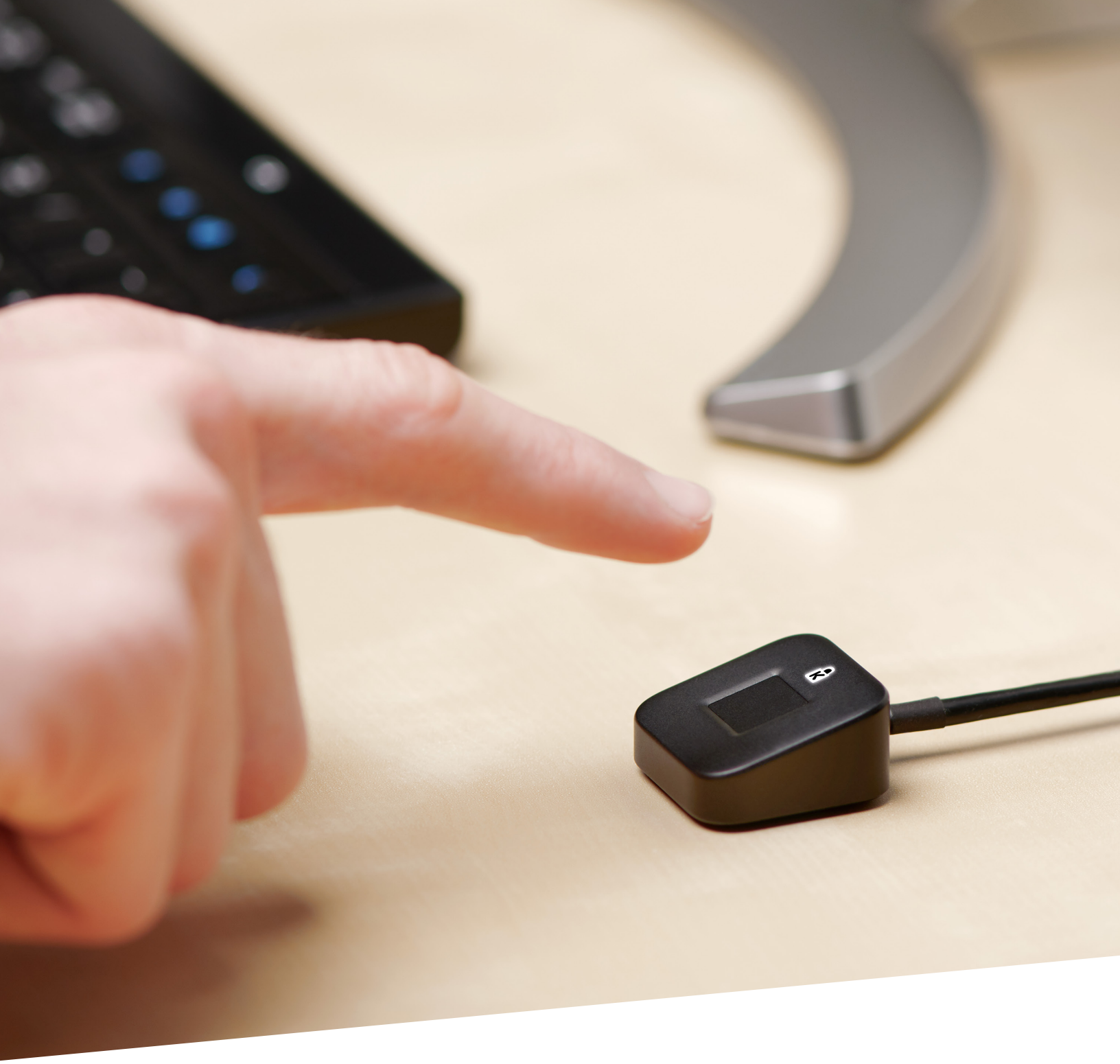
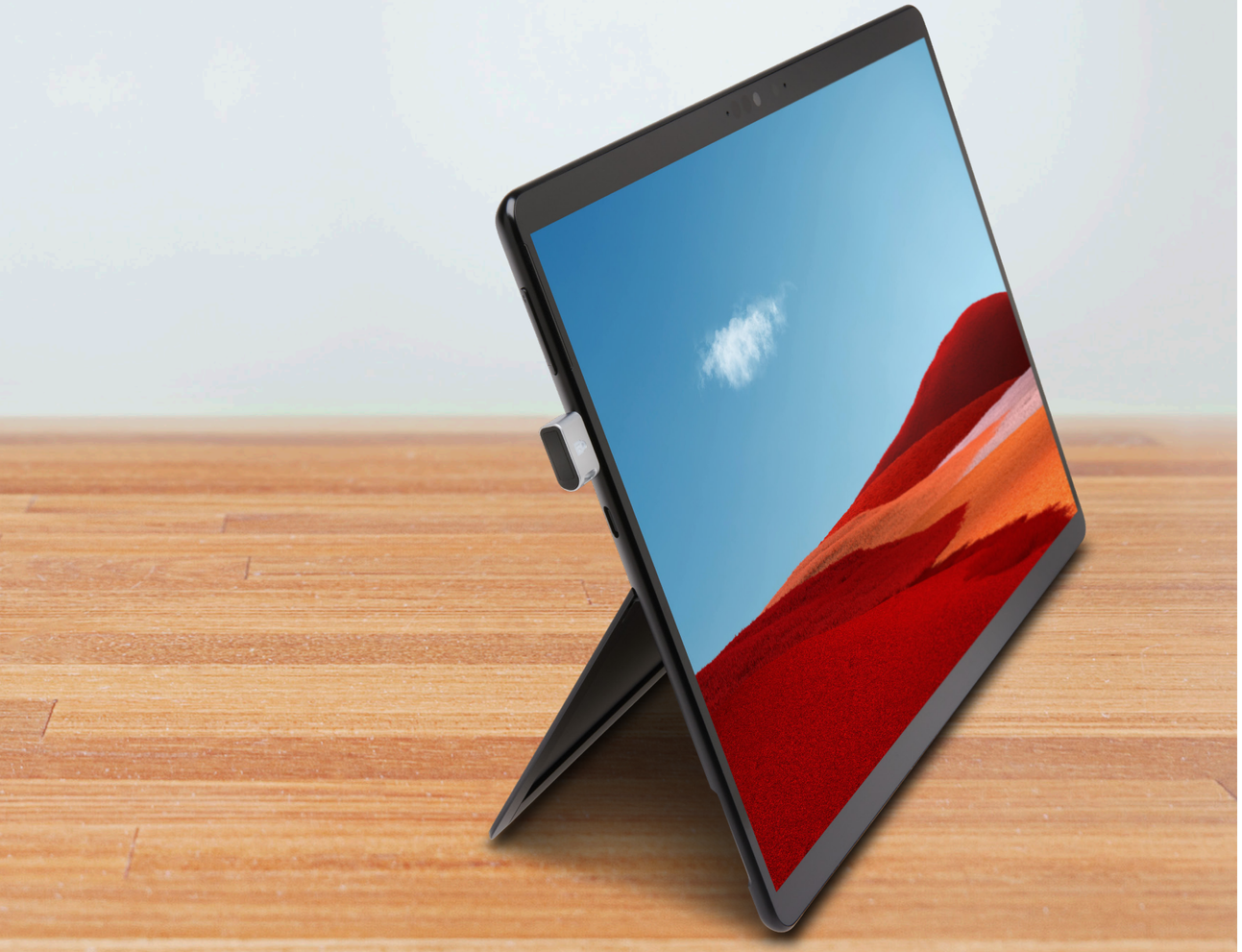


Kensington Lettori di impronte digitali

Perché rischiare?

Dati recenti raccolti da Risk Based Security[1] hanno rivelato che il numero di filre esposti è aumentato, raggiungendo la cifra impressionante di 36 miliardi nel 2020. Sono state segnalate pubblicamente 3.932 violazioni nei primi tre trimestri del 2020. Alla fine del secondo trimestre, il 2020 era già considerato “il peggiore anno in assoluto” in termini di numero totale di dati esposti.

Benché nessuna soluzione possa garantire una protezione totale, la biometria è un anello molto importante nella catena della sicurezza. Oltre all'unicità intrinseca dei dati biometrici di ciascuna persona (e, di conseguenza, il livello di sicurezza offerto), la biometria consente di attuare soluzioni senza password.

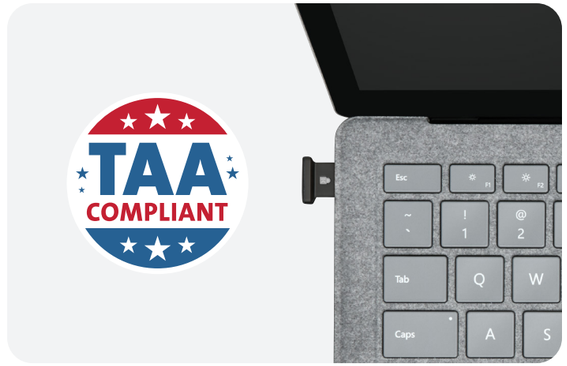


[1] *https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf*

Sicurezza in qualunque momento, luogo e condizione

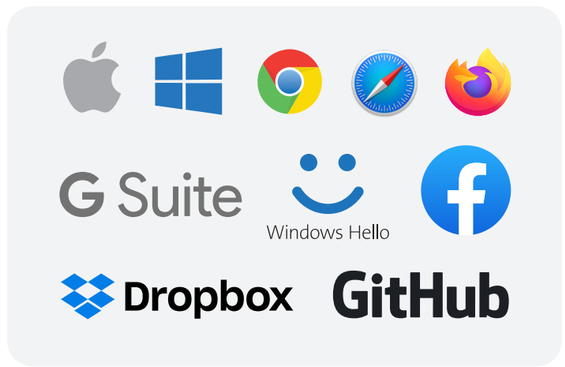
Distribuzione aziendale

Le chiavette VeriMark per il settore IT, VeriMark Desktop e VeriMark Guard si integrano facilmente nell'infrastruttura IT esistente, offrendo l'accesso senza password a Windows Hello, Windows Hello for Business, Microsoft Azure e agli altri servizi Microsoft su Edge, e facilitano la gestione di accessi, privilegi e password per il settore IT.



Utilizzo nelle infrastrutture governative

Le chiavette VeriMark per il settore IT, Desktop e Guard possono essere utilizzate per supportare le misure di sicurezza informatica di un’azienda coerenti con (ma non limitate a) le leggi sulla privacy come SDPR, BIPA e CCPA.



Sistemi operativi compatibili

La chiavetta VeriMark Guard offre la massima compatibilità con i servizi Web, tra cui Google, Facebook e Microsoft (per Windows Hello, fare riferimento a VeriMark o VeriMark IT), con supporto per Chrome, Edge, Firefox e Safari e supporto OS multipiattaforma per Win10, macOS e Chrome OS come chiave di sicurezza FIDO2.

Perché affidarsi all'autenticazione biometrica?

Poiché è estremamente difficoltoso falsificare caratteristiche fisiche come le impronte digitali e le pupille, la biometria rappresenta una soluzione per la sicurezza estremamente affidabile, anche per soluzioni complete che possono comprendere, in aggiunta, l'utilizzo di una password e/o di dispositivi fisici come una chiave, una card o un token.

Negli ambienti di lavoro, la biometria può essere utilizzata in solidi protocolli di sicurezza per l'accesso a sistemi, file, informazioni e dati interni all'azienda, semplicemente toccando un lettore di impronte digitali o guardando la lente di una fotocamera.

Domande principali

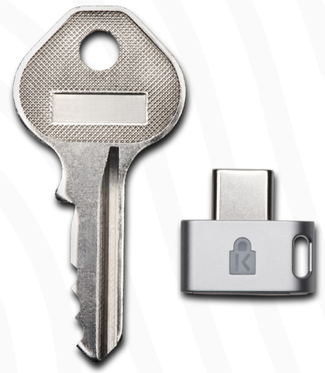
Qual è l'obiettivo principale nel caso d'uso?

Si utilizzano Windows Hello o Hello for Business?

Quali piattaforme o browser devono essere supportati?

Gli utenti hanno accesso a uno o più dispositivi?

Si è a conoscenza dei vantaggi dei lettori biometrici?

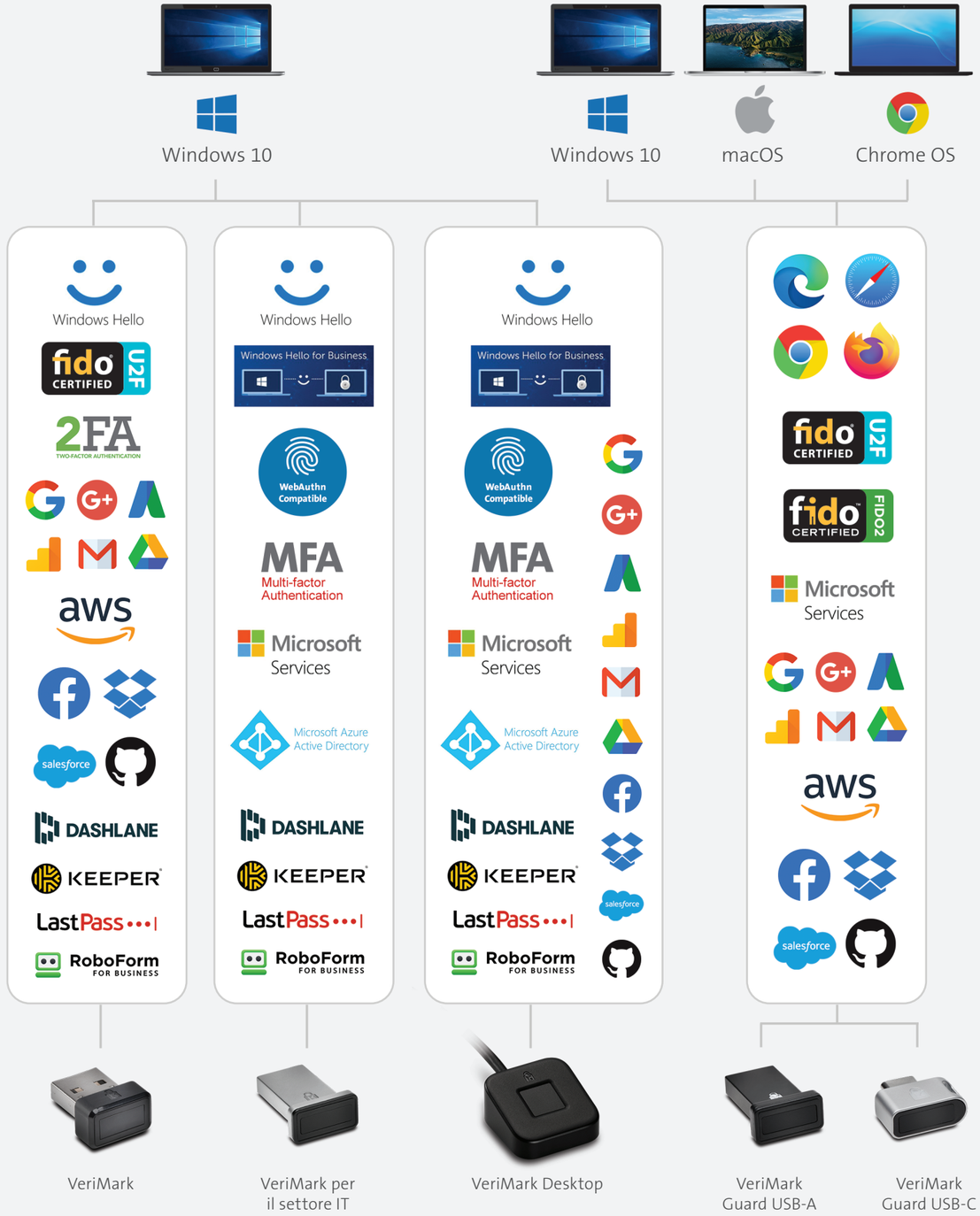


LO SAPEVI?

L'81% delle violazioni da parte di hacker hanno sfruttato password rubate e/o deboli.

Verizon 2020 Data Breach Investigations Report

Quale chiavetta con lettore di impronte digitali è la più adatta per te?



Lettori di impronte digitali VeriMark

LO SAPEVI?

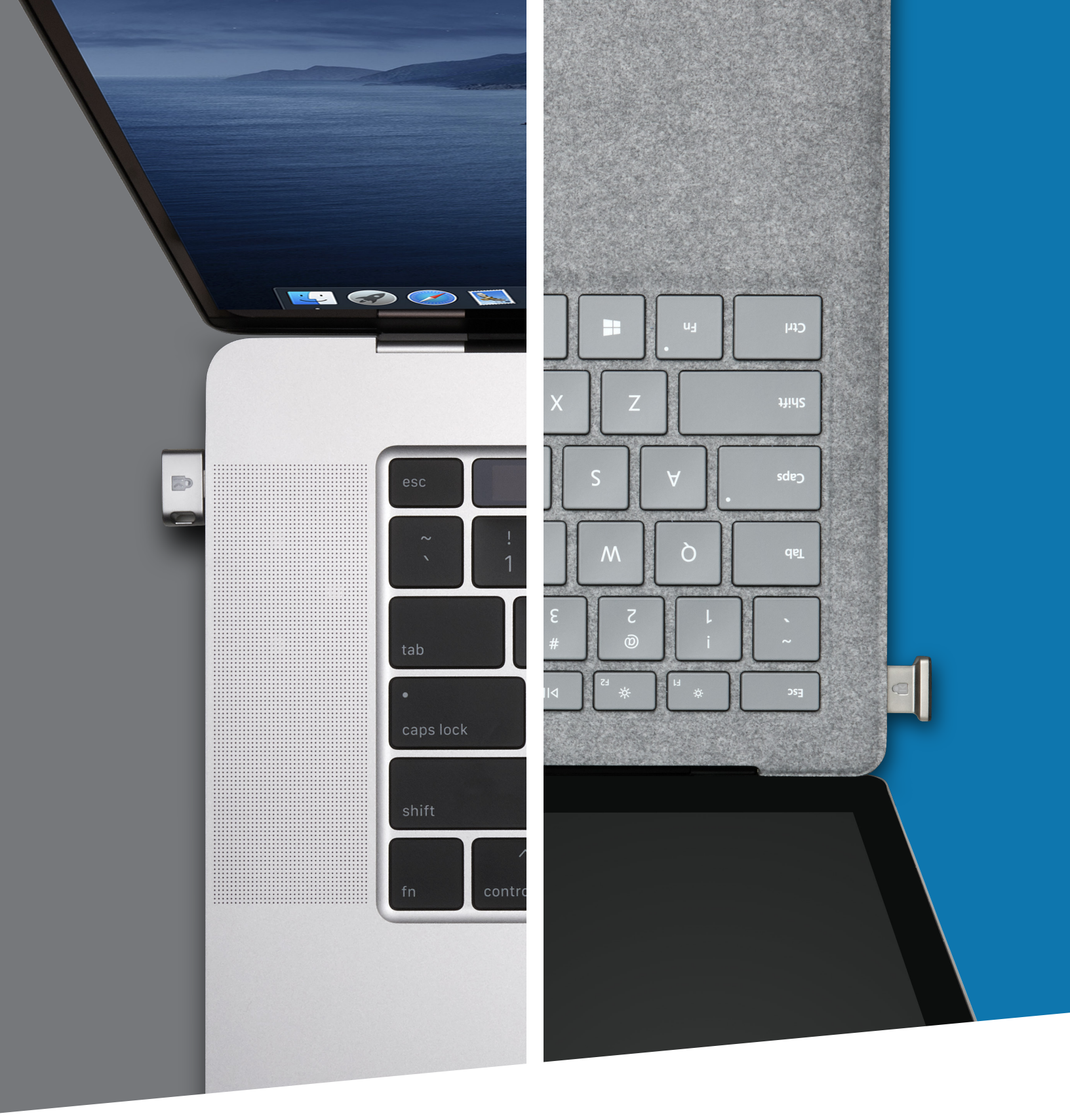
L'autenticazione a più fattori (MFA) blocca fino al 99,9% degli attacchi agli account aziendali

Microsoft Study, 2019

Member of
Microsoft Intelligent Security Association
Microsoft

Nome	VeriMark K67977WW	VeriMark per il settore IT K64704EU	VeriMark Desktop K62330WW
Compatibilità	Windows 7/8.1/10 e app Web	Windows 7/8.1/10 e app MSFT	Windows 7/8.1/10 e app MSFT e Web
FIDO	Certificazione FIDO U2F	Certificazione FIDO U2F e compatibile con Autenticazione Web FIDO 2	Certificazione FIDO U2F e compatibile con Autenticazione Web FIDO 2
Tipo	Match-on-Host	Match-in-Sensor	Match-in-Sensor
Dati archiviati	Dispositivo modello impronte digitali in host	Dati del modello impronte digitali nella chiavetta	Dati del modello impronte digitali nella chiavetta
False Rejection Rate (FRR)	3%	2%	2%
False Acceptance Rate (FAR)	0,002%	0,001%	0,001%
Leggibilità	365 gradi	365 gradi	365 gradi
Disponibilità	**Immediata**	**Immediata**	**Immediata**

Nome	VeriMark Guard USB-A K64708WW	VeriMark Guard USB-C K64709WW
Compatibilità	Windows 7/8.1/10; Mac OS; Chrome OS	Windows 7/8.1/10; Mac OS; Chrome OS
FIDO	FIDO U2F e certificazione FIDO 2	FIDO U2F e certificazione FIDO 2
Tipo	Match-in-Sensor	Match-in-Sensor
Dati archiviati	Dati del modello impronte digitali nella chiavetta	Dati del modello impronte digitali nella chiavetta
False Rejection Rate (FRR)	2%	2%
False Acceptance Rate (FAR)	0,001%	0,001%
Leggibilità	365 gradi	365 gradi
Disponibilità	**Immediata**	**Immediata**



PER ULTERIORI INFORMAZIONI, CONTATTARE:

sales@kensington.com