

Kensington®

Chiavette di sicurezza VeriMark™ con impronta digitale

Il tuo partner fidato nell'autenticazione a
più fattori e nella cybersicurezza



Accesso Sicuro Senza Complicazioni

Le chiavi biometriche e le chiavi di sicurezza NFC stanno trasformando il modo in cui proteggiamo il nostro mondo digitale. Le chiavi biometriche offrono un'autenticazione veloce, affidabile e senza password utilizzando dati biometrici unici, rendendo quasi impossibile l'accesso non autorizzato. Le chiavi di sicurezza NFC aggiungono un ulteriore livello di comodità e flessibilità, specialmente per le persone che utilizzano sia PC che dispositivi mobili. Sono semplici da usare e spesso più economiche rispetto alle opzioni biometriche. Insieme, questi strumenti offrono una protezione forte e a più fattori che è facile da usare, altamente sicura e progettata per mantenere al sicuro le informazioni sensibili.

Domande Principali

- Qual è il **l'obiettivo principale** nel caso d'uso?
- Quali dispositivi o **browser** devono essere supportati?
- Viene utilizzato **Windows Hello** o **Windows Hello for Business** o l'autenticazione web?
- Gli utenti accedono a **uno** o **più** dispositivi?
- Più **utenti** accederanno allo **stesso dispositivo** in momenti diversi della giornata?
- Quali **servizi** vengono utilizzati?





Tendenze del Settore e Approfondimenti di Ricerca

Panorama Attuale Della Sicurezza dei Dispositivi

Kensington ha sponsorizzato uno studio, condotto dallo specialista di ricerche di mercato indipendente Vanson Bourne, su 1.000 decisori IT senior responsabili della sicurezza hardware della loro organizzazione. Una scoperta chiave è stata che l'accesso non autorizzato ai dati aziendali sui dispositivi è la principale preoccupazione per il 43% degli intervistati, seguita dal 19% che si preoccupa della perdita di dati sensibili a causa di reti domestiche insicure. Le organizzazioni si stanno sempre più rivolgendo all'autenticazione a più fattori (MFA) come difesa primaria, con il 30% degli intervistati che identificano l'autenticazione biometrica o a più fattori come critica per mitigare le minacce alla sicurezza.

Adozione Dell'autenticazione Biometrica

Un numero crescente di organizzazioni riconosce il valore delle soluzioni di sicurezza biometrica. Secondo la nostra ricerca di mercato, il 71% delle organizzazioni interpellate utilizza attualmente impronte digitali e/o chiavi di sicurezza per l'autenticazione a due fattori (2FA), mentre un ulteriore 26% prevede di implementare queste misure nel prossimo futuro. La linea VeriMark™ di Kensington esemplifica la sicurezza biometrica all'avanguardia, combinando la comodità senza password con una protezione di livello enterprise. Come leader nella sicurezza del moderno posto di lavoro, Kensington offre soluzioni conformi a TAA e GDPR che si integrano nelle infrastrutture esistenti, consentendo alle organizzazioni di affrontare efficacemente le minacce informatiche in evoluzione.

Fonte: Vanson Bourne, Ricerca sulla Sicurezza del Dispositivo, ottobre-novembre 2024

Sicurezza e Comodità Migliorate con VeriMark™ IT 2.0 e VeriMark™ Desktop 2.0



Chiavi biometriche come VeriMark™ IT 2.0 e VeriMark™ Desktop 2.0 si integrano perfettamente con Windows Hello per offrire una sicurezza migliorata e un accesso rapido e conveniente. Completamente conformi ai requisiti di Sicurezza di Accesso Migliorata (ESS) di Microsoft, combinano il riconoscimento avanzato delle impronte digitali con i più recenti standard di autenticazione di Windows. VeriMark™ IT 2.0 e Desktop 2.0 garantiscono accessi sicuri, crittografia e protezione online, ideali per proteggere dati sensibili mentre semplificano l'accesso con un semplice tocco, rendendoli perfetti per i professionisti moderni e gli ambienti IT.

Autenticazione Forte

L'autenticazione biometrica utilizza l'impronta digitale, unica per ogni utente, rendendola un metodo di autenticazione altamente sicuro.

Basso Rischio di Dimenticare o Perdere

A differenza delle password, gli utenti non possono dimenticare o perdere i propri dati biometrici.

Accesso Veloce e Conveniente

Autenticati in pochi secondi con un semplice tocco: niente digitazione, niente problemi.

Eleva la Sicurezza Web con VeriMark™ Guard 2.1 Tramite MFA



Impronte digitali e chiavi di sicurezza come VeriMark™ Guard 2.1 sono ideali per l'autenticazione a più fattori (MFA) quando si accede a servizi web che richiedono una protezione migliorata. Come soluzione certificata FIDO®, combina la verifica biometrica o l'inserimento del PIN con l'autenticazione basata su hardware per offrire una sicurezza forte e resistente al phishing. Perfetto per piattaforme finanziarie, applicazioni aziendali o account cloud sensibili, VeriMark™ Guard 2.1 offre una robusta difesa contro il furto di credenziali mantenendo un'esperienza utente veloce e senza interruzioni.

Estremamente Sicuro

Le chiavi di sicurezza utilizzano un'autenticazione crittografica forte che è estremamente difficile da duplicare o manipolare, rendendole resistenti a phishing e attacchi di ingegneria sociale. Come dispositivi certificati FIDO2, U2F e CTAP2.1, supportano standard di sicurezza moderni e basati sull'hardware che aiutano le organizzazioni a soddisfare requisiti normativi rigorosi come HIPAA e PCI DSS.

Facile da Usare

Le chiavi di sicurezza sono semplici da usare e richiedono una configurazione minima, rendendole un'opzione conveniente per gli utenti.

Accedi alla Sicurezza di Livello Aziendale Senza Password



La chiave di sicurezza VeriMark™ NFC+ offre un modo semplice ma potente per garantire l'accesso su più dispositivi. Combinano la comodità wireless con una crittografia robusta, consentendo agli utenti di autenticarsi semplicemente toccando la chiave quando inserita, o toccando la chiave contro un lettore NFC. Queste chiavi eliminano la necessità di registrazione biometrica, rendendole perfette per postazioni di lavoro condivise o configurazioni rapide. Con tecnologia resistente al phishing e certificazione FIDO®, offrono sicurezza di livello aziendale a un prezzo conveniente, garantendo sia usabilità che conformità.

Integrazione con Windows Hello

VeriMark™ Access consente accessi rapidi a Windows senza password con una semplice configurazione della chiave per impronte digitali plug-and-play. Quando la chiave non è disponibile, l'app mobile VeriMark™ Companion funge da backup sicuro, generando un codice monouso per garantire un accesso ininterrotto. La soluzione supporta anche ambienti multi-utente che richiedono un rapido e fluido cambio di utente.

Capacità FIDO2

Certificati per FIDO2 Livello 2 e supportando CTAP2.1, queste chiavi funzionano su tutte le principali piattaforme e browser, inclusi Windows, macOS, iOS e Android. Questa chiave fornisce una soluzione scalabile e conforme per le imprese che abbracciano la sicurezza senza password.

Sicurezza in Qualunque Momento, Luogo e Condizione



Distribuzione Aziendale

I prodotti VeriMark™ sono progettati per una distribuzione aziendale scalabile, offrendo un modo semplice ed economico per implementare l'autenticazione senza password. Con una vasta compatibilità tra sistemi operativi, browser e piattaforme di identità, i prodotti VeriMark™ si integrano senza soluzione di continuità negli ambienti IT esistenti. Supportano la gestione centralizzata, soddisfano gli standard di conformità FIDO2 e del settore e forniscono sicurezza resistente al phishing senza aggiungere complessità.

Supporta la Conformità al GDPR

Può essere utilizzata per supportare le misure di sicurezza informatica conformi a leggi e regolamenti sulla privacy quali GDPR, BIPA e CCPA, ma non limitate ad essi.

Compatibilità

Le chiavi di impronta digitale e di sicurezza VeriMark™ sono progettate per una vasta compatibilità, offrendo un'autenticazione sicura e senza password su più piattaforme e servizi. Questa funzionalità multiplatforma rende VeriMark™ una soluzione ideale per aziende e individui che cercano una sicurezza forte e resistente al phishing senza sacrificare la comodità.

Punti di Forza Fondamentali delle Chiavi di Sicurezza con Impronta Digitale



Controllo Accessi Biometrici

Il vantaggio principale è che il possesso della chiave da solo non è sufficiente, l'impronta digitale dell'utente deve corrispondere. Questo riduce drasticamente il rischio nel caso in cui la chiave venga persa o rubata. Solo i registrati possono attivare la risposta crittografica della chiave.

MFA Integrato in un Dispositivo

Una chiave per impronte digitali combina qualcosa che sei (verifica biometrica) con qualcosa che hai (un dispositivo di sicurezza fisico). In pratica, questo consente alla scansione dell'impronta di servire come passaggio di verifica dell'utente, eliminando la necessità di un PIN o di una password separati al login. Questo crea un'esperienza di accesso semplificata in cui un'azione sblocca sia la chiave che autentica, pur mantenendo più fattori di autenticazione forte.

Comodità e Velocità per L'Utente

Per molti, utilizzare un'impronta digitale è più veloce e conveniente rispetto a digitare password o prendere un telefono per un codice OTP. Con una chiave ben progettata, la scansione dell'impronta è quasi istantanea.

Feedback Visivo/Tattile

Le chiavi biometriche spesso forniscono un po' di feedback (come un indicatore LED) quando un'impronta digitale viene accettata, il che può ispirare fiducia. Sapere che la chiave ti verifica attivamente aggiunge un senso di sicurezza.

Principali Vantaggi delle Chiavi Biometriche VeriMark™

Sicurezza Biometrica: Solo gli utenti registrati possono accedere.

Accesso Veloce: Touch and go—nessuna digitazione richiesta.

Resistente al Phishing: Autenticazione basata su hardware.

Portatile: Utilizzabile su più dispositivi.

Regolamentare: Supporta il GDPR ed è conforme al TAA.



Punti di Forza Fondamentali delle Chiavi di Sicurezza USB NFC



Compatibilità Tra Dispositivi

Il grande vantaggio delle chiavi abilitate NFC è che funzionano senza problemi sia con PC che con dispositivi mobili. Puoi inserire la chiave nelle porte USB standard e toccarla su telefoni o tablet tramite NFC per autenticarti senza fili.

Facilità D'Uso su Dispositivi Mobili

Utilizzare una chiave di sicurezza su un telefono può essere complicato se il telefono non ha una porta USB disponibile o ha una custodia, ma NFC risolve questo problema. Toccare la chiave sul telefono è veloce e intuitivo e comunica su una distanza molto breve (entro pochi centimetri), il che è conveniente e sicuro (difficile da intercettare).

Ottimo per Utenti Condivisi o A Rotazione

Le chiavi NFC non memorizzano impronte digitali né richiedono una configurazione biometrica individuale, rendendole perfette per ambienti in cui più persone necessitano di accesso, come team in prima linea, laboratori per studenti, o linee di produzione.

Sicurezza Elevata

Le chiavi NFC mantengono lo stesso alto livello di sicurezza crittografica delle altre chiavi hardware. L'NFC stesso è progettato per comunicazioni a corto raggio, il che limita notevolmente il rischio di intercettazione (un attaccante dovrebbe essere fisicamente a pochi centimetri durante l'uso).

Principali Vantaggi delle Chiavi di Sicurezza NFC+ VeriMark™

Interfaccia Doppia: Funziona sia con USB che con NFC per un accesso flessibile ai dispositivi.

Security Resistente al Phishing: Protezione basata su hardware contro il phishing e il furto di credenziali.

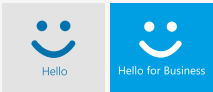
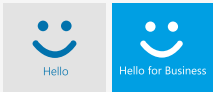
Certificato FIDO2 Livello 2: Rispetta i più alti standard del settore per l'autenticazione senza password e supporta CTAP2.1.

Cross-Platform: Compatibile con Windows, macOS, Android, iOS e i principali servizi e browser.

Non è Necessaria alcuna Configurazione Biometrica: Veloce da implementare—nessuna registrazione delle impronte digitali richiesta.



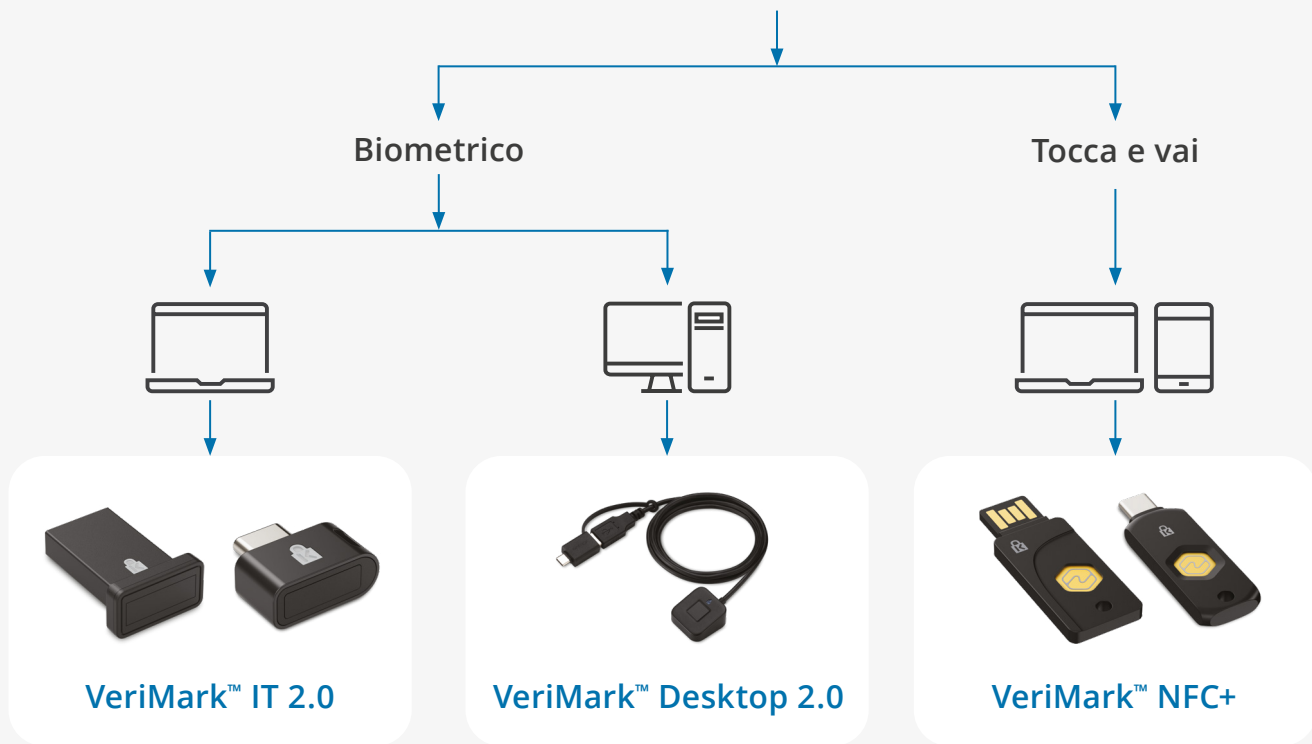


	CHIAVETTA CON LETTORE DI IMPRONTE DIGITALI VERIMARK™ IT 2.0	VERIMARK™ CHIAVETTA CON LETTORE DI IMPRONTE DIGITALI DESKTOP 2.0	VERIMARK™ GUARD 2.1 CHIAVE DI SICUREZZA PER IMPRONTE DIGITALI	TOKEN DI SICUREZZA VERIMARK™ NFC+
Articolo #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Windows Hello			Non supportato	Non supportato nativamente, ma può accedere tramite software (VeriMark™ Access) + App mobile companion
Microsoft Enhanced Sign-in Security (ESS)	Supportato tramite Windows 11	Supportato tramite Windows 11	Non supportato	Non supportato
FIDO2 and FIDO U2F	Non supportato Compatibile con WebAuthn	Non supportato Compatibile con WebAuthn		
CTAP	Non supportato	Non supportato	Supporta CTAP2.1 ed è retrocompatibile con CTAP2.0	Supporta CTAP2.1 ed è retrocompatibile con CTAP2.0
Dispositivo				
Sistema operativo				
Google, Amazon, Apple e Microsoft Services				
Servizi Web				
Gestori password				

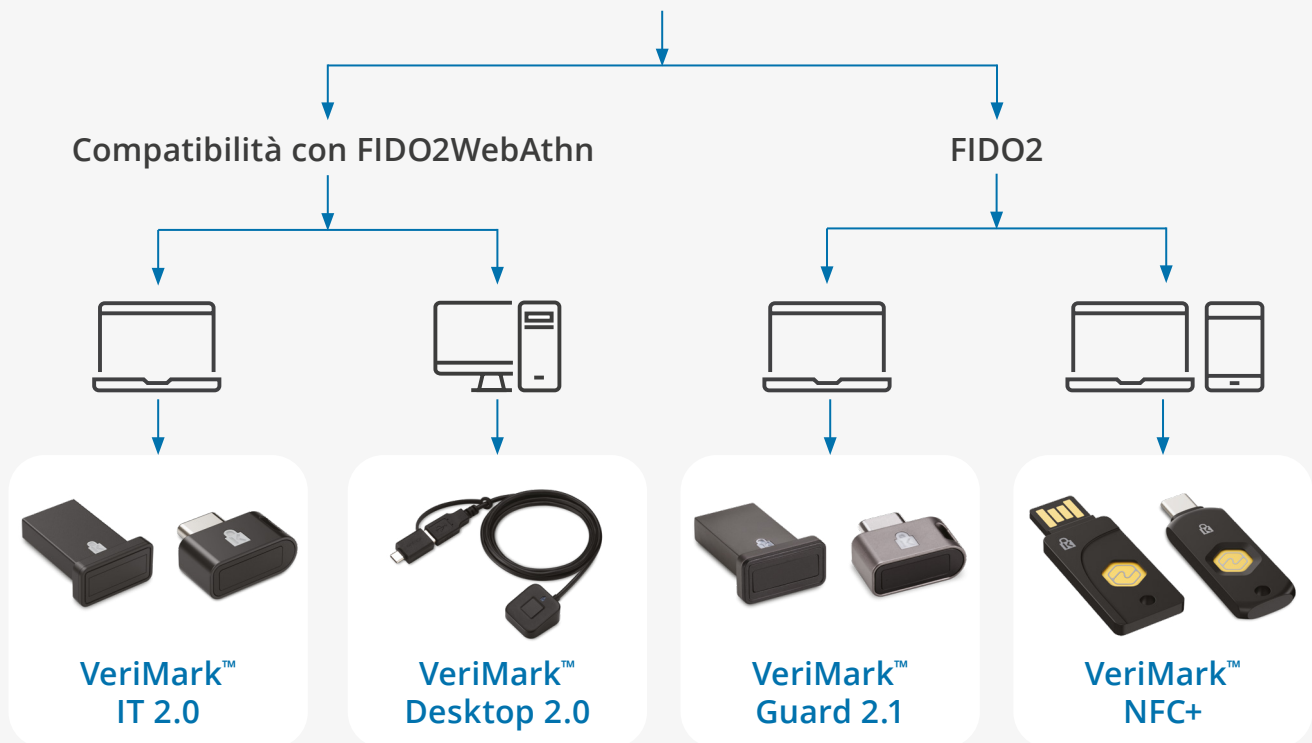


	CHIAVETTA CON LETTORE DI IMPRONTE DIGITALI VERIMARK™ IT 2.0	VERIMARK™ CHIAVETTA CON LETTORE DI IMPRONTE DIGITALI DESKTOP 2.0	VERIMARK™ GUARD 2.1 CHIAVE DI SICUREZZA PER IMPRONTE DIGITALI	TOKEN DI SICUREZZA VERIMARK™ NFC+
Articolo #	USB-A - K64740WW USB-C® - K64705WW	K64741WW	USB-A - K65050WW USB-C® - K65051WW	USB-A - K64738WW USB-C® - K64739WW
Certificazione	 	 	 	 
Tipo di Chiave				
Tipo di Connessione	USB-A o USB-C®	Adattatore USB-A con USB-C®	USB-A o USB-C®	USB-A o USB-C® e NFC
Passkey	Compatibile tramite biometria	Compatibile tramite biometria	Compatibile tramite biometria	Compatibile tramite NFC o Tap-and-Go
Tipo di Autenticazione con Impronta Digitale	Match-in-Sensor™	Match-in-Sensor™	Match-in-Sensor™	-
Punteggio Dati	Dati del modello impronte digitali nella chiavetta	Dati del modello impronte digitali nella chiavetta	Dati del modello impronte digitali nella chiavetta	-
False Rejection Rate (FRR)	2%	2%	2%	-
False Acceptance Rate (FAR)	0,001%	0,001%	0,001%	-
Leggibilità	365 gradi	365 gradi	365 gradi	-

Accesso sicuro per Windows Hello



Accesso sicuro per i Servizi Web





La chiave di sicurezza VeriMark™ NFC+ USB-C® è progettata per rafforzare la sicurezza digitale nei servizi basati sul web. Questa chiave di sicurezza USB-C® abilitata NFC è certificata per FIDO2 Livello 2 e offre autenticazione sicura, conveniente e multiplatforma per utenti sia consumer che aziendali. Eliminando le vulnerabilità delle password con MFA basata su hardware, fornisce protezione di livello aziendale contro phishing e furto d'identità.

- Sicurezza certificata FIDO2 di livello 2
- Supporto del protocollo FIDO C TAP2. 1
- Interfaccia duale USB-C® + NFC
- Semplicità e software complementari
- Compatibilità multiplatforma
- Compatto e portatile
- Classificato IP68 e resistente alla



Disponibile anche - USB-A

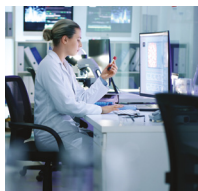


Scopri di più



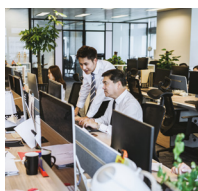
Chiavi per Impronte Digitali – Casi D'Uso e Scopi Ideali

Le chiavi per impronte digitali combinano l'autenticazione biometrica con la sicurezza basata sull'hardware. Sono più adatte per ambienti in cui l'assicurazione dell'identità individuale è critica.



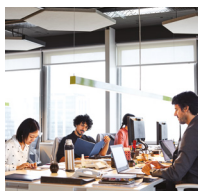
Salute

- Accesso sicuro ai registri dei pazienti (conformità HIPAA).
- Prevenire l'accesso non autorizzato a dispositivi o terminali medici.
- Accesso biometrico per i clinici che utilizzano postazioni di lavoro condivise.



Finanza e Banche

- Accesso sicuro a piattaforme di trading o dashboard finanziari.
- Prevenire il furto di credenziali in ambienti ad alto rischio.
- Rispettare i requisiti normativi (ad es., PCI-DSS, GDPR).



Governo e Settore Pubblico

- Utilizzato in istituzioni federali per MFA biometrico.
- Supporta FIDO2 e Windows Hello for Business.



Istruzione

- Insegnanti e personale utilizzano chiavi biometriche per accesso sicuro.
- Prevenire l'accesso non autorizzato in laboratori informatici condivisi.



IT Aziendale

- Utilizzato per la gestione degli accessi privilegiati.
- Riduce il carico del helpdesk per il ripristino delle password.
- Supporta registri di audit e controllo degli accessi centralizzato.



Chiavi NFC – Casi D'Uso e Scopi Ideali

Le chiavi NFC offrono autenticazione tap-and-go ed sono ideali per ambienti mobile-first, multi-utente o rivolti ai consumatori.



Vendita al Dettaglio e Punto Vendita

- Tocca per autenticare per terminali POS.
- Passaggio rapido tra gli account del personale.
- Prevenire transazioni non autorizzate.



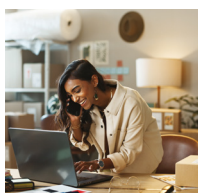
Trasporti e Logistica

- I conducenti utilizzano chiavi NFC per accedere agli strumenti di pianificazione dei percorsi.
- Accesso sicuro ai sistemi di gestione della flotta.
- Ideale per ambienti difficili (certificazione impermeabile IP68).



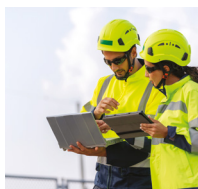
Istruzione

- Gli studenti toccano per accedere ai dispositivi condivisi.
- Gli amministratori IT gestiscono l'accesso senza bisogno di registrazione biometrica.



Consumatori e PMI

- Accesso senza password per dispositivi personali.
- Configurazione semplice per utenti non tecnici.
- Compatibile con Apple ID, Google, Microsoft e altro.



Settore Pubblico - Lavoro sul Campo

- Accesso rapido per lavoratori mobili.
- Nessun bisogno di registrazione delle impronte digitali o memorizzazione del PIN.
- Funziona offline e su più piattaforme.



Tutte le specifiche sono soggette a modifica senza preavviso. I prodotti potrebbero non essere disponibili su tutti i mercati. Kensington, il nome e il disegno ACCO sono marchi registrati di ACCO Brands. Kensington The Professionals' Choice è un marchio commerciale di ACCO Brands. Tutti gli altri marchi registrati e non registrati appartengono ai rispettivi proprietari. Thunderbolt e il logo Thunderbolt sono marchi registrati di Intel Corporation negli Stati Uniti e/o in altri Paesi. © 2026 Kensington Computer Products Group, divisione di ACCO Brands. Tutti i diritti riservati. CBT54577IT

Kensington
The Professionals' Choice™

PER ULTERIORI INFORMAZIONI CONTATTARE: +39 (0)800 029387 • sales.it@kensington.com