IRONKEY VAULT PRIVACY 50 SERIE

Con crittografia hardware per la sicurezza dei dati

La serie Kingston IronKey Vault Privacy 50 include drive USB Type-A e Type-C®[1] di alta qualità che forniscono sicurezza avanzata con crittografia hardware AES a 256 bit certificata FIPS 197 in modalità XTS e includono la protezione da BadUSB tramite firmware con firma digitale e dagli attacchi Brute Force per decifrare le password. La serie VP50, in quanto storage crittografato sotto il controllo fisico dell'utente, offre una protezione dei dati superiore rispetto a quella offerta dall'utilizzo di Internet e dei servizi Cloud.

Vault Privacy 50 supporta l'opzione multipassword (amministratore, utente e ripristino monouso) con modalità complessa o frase password. Ciò aumenta le possibilità di recuperare l'accesso ai dati in caso una delle password venga dimenticata. La modalità complessa tradizionale supporta password composte da 6 a 16 caratteri tramite l'utilizzo di 3 set di caratteri su 4. La nuova modalità frase password supporta un PIN numerico, una frase, un elenco di parole o persino testi composti da 10 a 64 caratteri. L'amministratore può abilitare una password utente e una di ripristino monouso oppure reimpostare la password utente per ripristinare l'accesso ai dati. Per inserire la password più facilmente, è possibile abilitare il simbolo dell'occhio in modo da visualizzare la password digitata, riducendo gli errori di battitura che portano a tentativi di accesso non riusciti. La protezione dagli attacchi Brute Force blocca le password utente o di ripristino monouso dopo l'immissione di 10 password non valide consecutive ed esegue la cancellazione criptata del drive quando la password dell'amministratore viene inserita in modo errato per 10 volte di seguito.

Per proteggersi da potenziali malware su sistemi non sicuri, sia l'amministratore che l'utente possono impostare la modalità di sola lettura per proteggere il drive da scrittura; inoltre, la tastiera virtuale integrata protegge le password da keylogger o screenlogger.

Grazie alla certificazione FIPS 197 e alla conformità allo standard TAA, le organizzazioni possono personalizzare e configurare i drive della serie VP50 con un codice identificazione prodotto (PID) per l'integrazione con il software di gestione degli endpoint standard al fine di soddisfare i requisiti di cybersecurity e IT aziendali tramite il programma di personalizzazione Kingston.

Le piccole e medie imprese possono utilizzare il ruolo di amministratore per gestire localmente i propri drive, ad esempio per configurare o reimpostare le password utente o di ripristino monouso dei dipendenti, recuperare l'accesso ai dati su drive bloccati e garantire la conformità a leggi e normative nei casi in cui sono richieste indagini forensi.

- **Con certificazione FIPS 197 e crittografia XTS-AES a 256 bit**
- **Protezione da attacchi Brute Force e BadUSB**
- **Opzione multipassword con modalità complessa/ frase password**
- **Nuova modalità frase password**
- **Impostazione doppia di sola lettura (protezione da scrittura)**
- **Gestione locale dei drive per le piccole e medie imprese**

Ulteriori informazioni ››

CARATTERISTICHE/VANTAGGI

Drive USB con crittografia hardware per protezione dei dati — Proteggi i dati importanti con la crittografia XTS-AES a 256 bit certificata FIPS 197. Protezioni integrate dagli attacchi BadUSB e Brute Force.

Opzione multipassword per il recupero dei dati — Abilitare le password di amministratore, utente e di ripristino monouso. L'amministratore può reimpostare una password utente e creare una password di ripristino monouso per ripristinare l'accesso dell'utente ai dati. La protezione dagli attacchi Brute Force blocca le password utente o di ripristino monouso dopo l'immissione di 10 password non valide consecutive ed esegue la cancellazione criptata del drive quando la password dell'amministratore viene inserita in modo errato per 10 volte di seguito.

Nuova modalità frase password — Scegliere la modalità password complessa o frase password. Le frasi password possono essere un PIN numerico, una frase contenente spazi, un elenco di parole o persino testi composti da 10 a 64 caratteri.

Impostazione doppia di sola lettura (protezione da scrittura) — Evitare gli attacchi malware con una modalità di sola lettura forzata impostata dall'amministratore per l'utente oppure una modalità di sola lettura basata sulla sessione impostata dall'amministratore o dall'utente.

Gestione locale dei drive per le piccole e medie imprese — Utilizzare il ruolo di amministratore per gestire localmente le password utente e di ripristino monouso dei dipendenti, recuperare l'accesso ai dati su drive bloccati e garantire la conformità a leggi e normative nei casi in cui sono richieste indagini forensi.

Ulteriori funzionalità di sicurezza — Ridurre frustrazione e tentativi di accesso non riusciti abilitando il pulsante con il simbolo dell'occhio per visualizzare la password digitata. Utilizzare la tastiera virtuale per proteggere l'inserimento della password da keylogger e screenlogger.

SPECIFICHE TECNICHE

Interfaccia
USB 3.2 Gen 1

Capacità[2]
8GB, 16GB, 32GB, 64GB, 128GB, 256GB

Connettore
Type-A, Type-C

Velocità[3]
USB 3.2 Gen 1
8 GB-128 GB: 250 MB/s in lettura, 180 MB/s in scrittura
256 GB: 230 MB/s in lettura, 150 MB/s in scrittura

USB 2.0
8 GB – 256 GB: 30 MB/s in lettura, 20 MB/s in scrittura

Dimensioni
77,9 mm x 21,9 mm x 12,0 mm

Impermeabili[4]
fino a 1,21 m; IEC 60529 IPX8

Temperatura di esercizio
da 0 °C a 60 °C

Temperatura di storage
da -20 °C a 85 °C

Compatibilità
USB 3.0/USB 3.1/USB 3.2 Gen 1

Garanzia/supporto
Garanzia limitata di 5 anni, supporto tecnico gratuito

Compatibile con
Windows® 11, 10, macOS® 10.15.x – 13.x

NUMERI DI PARTE

Type-A	Type-C
IKVP50/8GB	IKVP50C/8GB
IKVP50/16GB	IKVP50C/16GB
IKVP50/32GB	IKVP50C/32GB
IKVP50/64GB	IKVP50C/64GB
IKVP50/128GB	IKVP50C/128GB
IKVP50/256GB	IKVP50C/256GB

1. USB Type-C® e USB-C® sono marchi registrati di USB Implementers Forum.
2. Parte della capacità totale indicata per i dispositivi di storage Flash viene in realtà utilizzata per la formattazione e altre funzioni. Tale spazio non è pertanto disponibile per la memorizzazione dei dati. Di conseguenza, l'effettiva capacità di storage dei dati dell'unità è inferiore a quella riportata sul prodotto. Per ulteriori informazioni, consultare la Guida alla memoria Flash di Kingston.
3. La velocità può variare in base all'hardware, al software e alla tipologia di utilizzo dell'host.
4. Prima dell'uso, il prodotto deve essere pulito e asciutto e dotato di cappuccio.