LAVORO IBRIDO

Come conservare i dati al sicuro

Il lavoro ibrido è ormai la normalità per tanti, con molti datori di lavoro che incoraggiano un sano mix di lavoro in ufficio e da remoto. Alcune persone preferiscono stare in un ambiente d'ufficio mentre trovano difficile lavorare da casa, quindi un ambiente misto può fornire il meglio di entrambe le soluzioni. È stato dimostrato che il lavoro a distanza, svolto dall'ufficio di casa o in viaggio, aumenta la produttività, riduce i costi e contribuisce al benessere personale.

Ma con esso vengono alcune preoccupazioni. Forse il problema più importante è la sicurezza dei dati. Infatti, i lavoratori da remoto hanno una maggiore probabilità di subire furti o di smarrire un proprio oggetto durante i trasferimenti.

Un modo per ridurre questo rischio consiste nell'utilizzare un dispositivo di archiviazione con crittografia. Eseguendo il backup dei tuoi file sensibili su dischi rigidi, SSD o unità flash USB con crittografia hardware AES a 256 bit, puoi essere sicuro che in caso di smarrimento o furto, non sia possibile accedere ai dati. Benchè rimanga frustrante perdere una memoria con i propri dati, per lo meno c'è la tranquillità che i file sono al sicuro da occhi indiscreti!

Archiviazione crittografata: soluzioni biometriche

I dischi rigidi e gli SSD Executive Fingerprint Secure utilizzano una combinazione di crittografia hardware AES a 256 bit e tecnologia biometrica per la totale sicurezza delle informazioni, il tutto in un elegante involucro di alluminio.

HDD e SSD Executive Fingerprint Secure

- Conserva i dati e proteggili con la tua impronta digitale
- Disco rigido portatile USB-CTM con scanner delle impronte digitali integrato
- Accesso mediante impronta digitale di un utente autorizzato
- Crittografia di sicurezza hardware AES a 256-bit Premium
- Fino a otto utenti autorizzati più un amministratore (tramite password)
- Design elegante in alluminio
- Cavo da USB-C™ a USB-A e adattatore USB-C™
- Software Nero Backup incluso*

AES-256 ENCRYPTION

fino a 8 utenti

USB-C™

PN	DESCRIZIONE
HDD	
53652	Executive Fingerprint Secure Portable HDD 1 TB
53653	Executive Fingerprint Secure Portable HDD 2 TB
SSD	
53656	Executive Fingerprint Secure USB-C SSD 512 GB
53657	Executive Fingerprint Secure USB-C SSD 1 TB

*Il software Nero Backup è compatibile solo per i sistemi operativi Windows.

Archiviazione crittografata: soluzioni biometriche

Stai andando di nuovo al lavoro? Salvare in sicurezza il tuo lavoro è qualcosa di cui devi assicurarti. Le soluzioni di archiviazione crittografata di Verbatim che utilizzano le tue impronte digitali garantiranno il backup dei tuoi dati in modo sicuro, ovunque tu sia!

Disco Rigido Fingerprint Secure

- Disco rigido portatile USB-C™ con scanner integrato di impronte digitali per prevenire che utenti non autorizzati accedano ai vostri dati
- Crittografia di sicurezza hardware AES a 256 bit premium
- Fino a otto utenti autorizzati più un amministratore (tramite password)
- Conservazione e trasporto di dati riservati protetti da eventuali smarrimenti o hacking
- Elegante design nero con superficie 3D che si abbinarsi alla gamma SSD
- USB 3.2 GEN 1 con connettore USB-C™ e adattatore

AES-256 ENCRYPTION

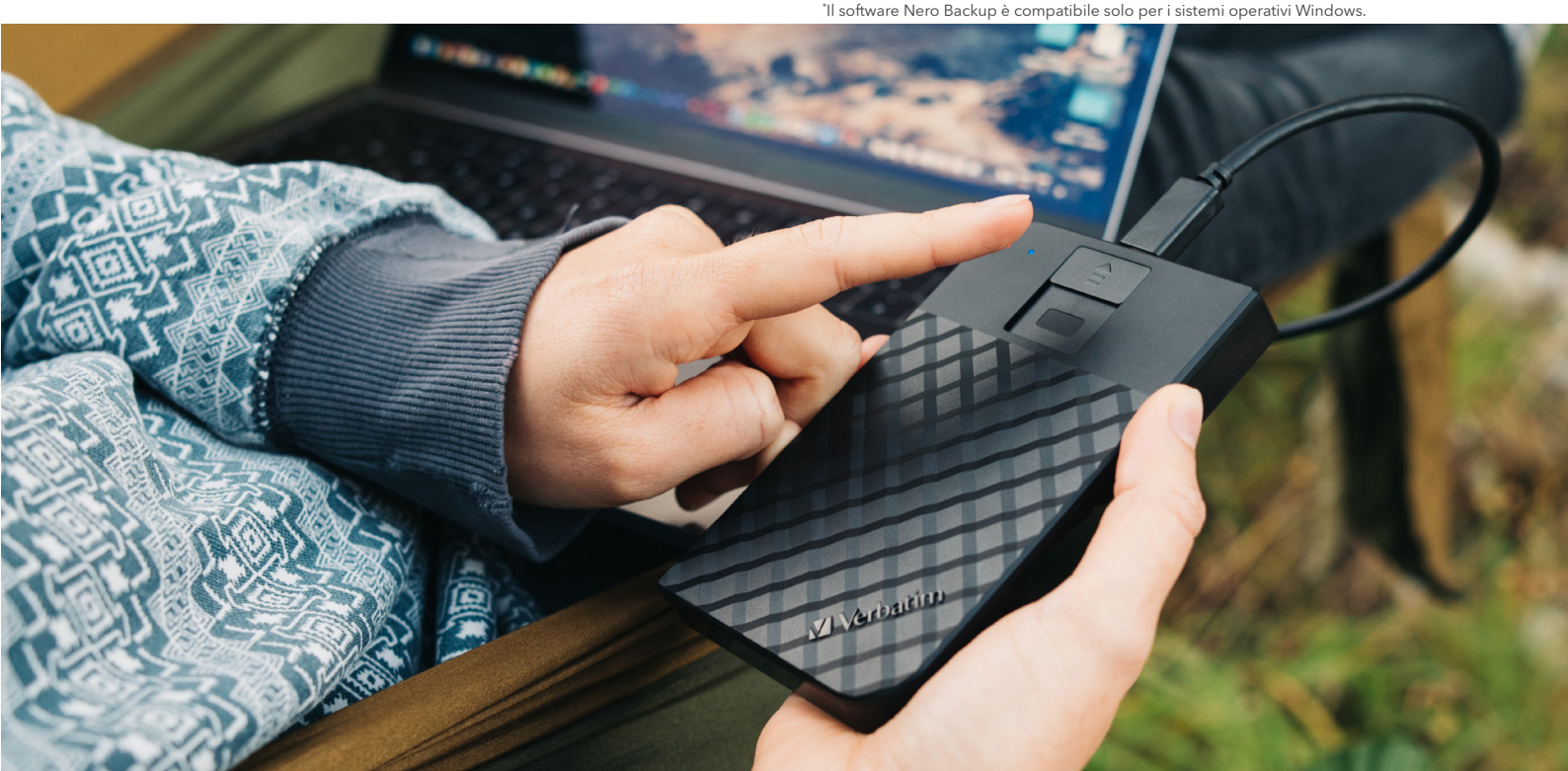
fino a 8 utenti

USB-C™

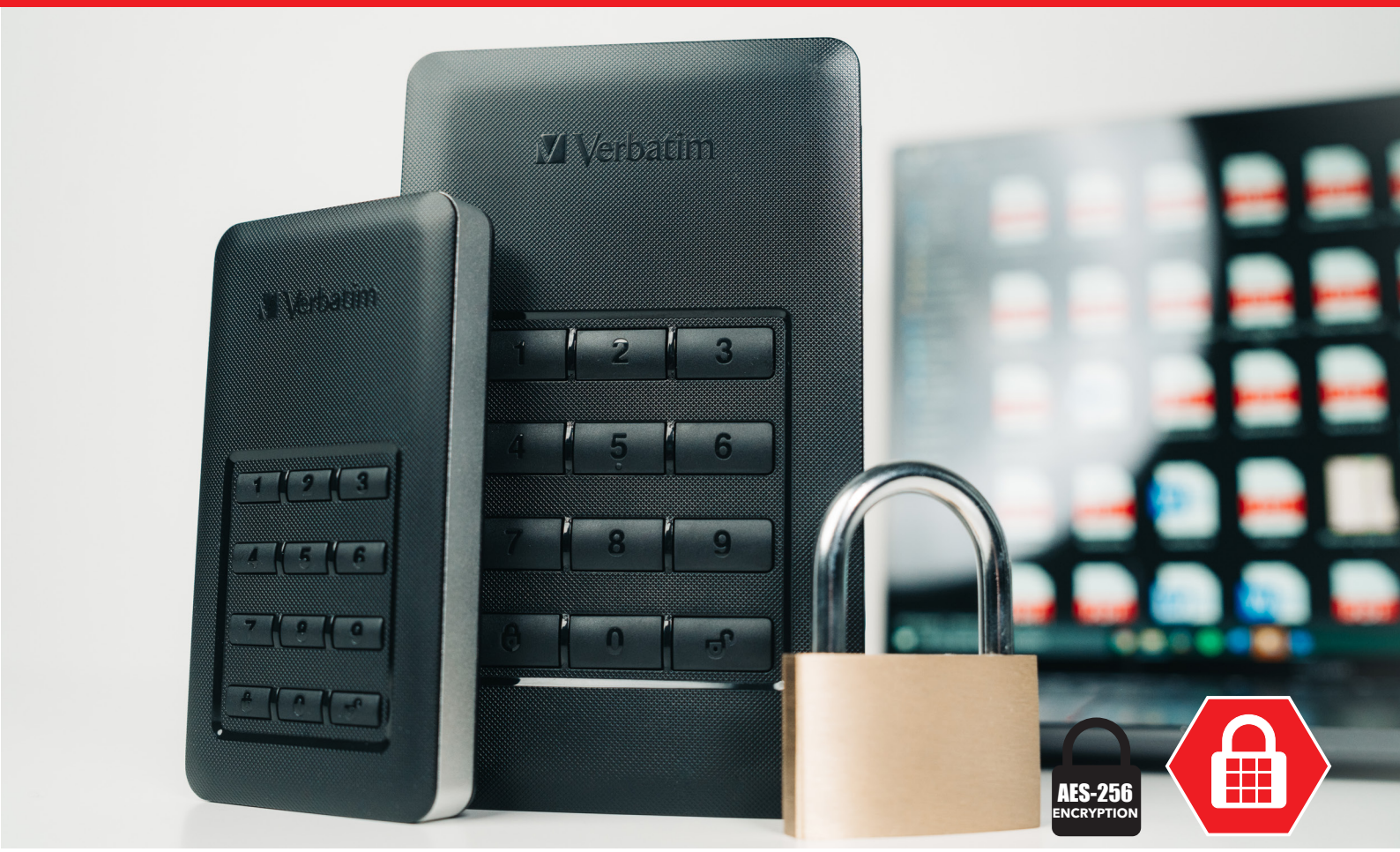
- Indicatori LED per alimentazione / stato di crittografia
- Software Nero Backup in dotazione*

PN	DESCRIZIONE
53650	Fingerprint Secure Portable HDD 1 TB
53651	Fingerprint Secure Portable HDD 2 TB

*Il software Nero Backup è compatibile solo per i sistemi operativi Windows.



Archiviazione crittografata: accesso con codice



La crittografia hardware AES a 256 bit crittografa tutti i dati in tempo reale sull'unità. Per potervi accedere è necessario digitare il codice tramite la tastiera integrata. Una soluzione di archiviazione semplice e sicura.

Disco rigido protetto con tastierino di accesso

- Crittografia Hardware a 256 bit AES
- Tastierino integrato per inserimento del codice (da 5 a 12 cifre)
- Utilizzabile con i televisori (funzionalità non possibile con i normali memorie crittografate)
- USB 3.2 Gen 1 con connessione USB-C™
- Indicatori LED per alimentazione / stato di crittografia
- Più sicuro della crittografia software
- Software Nero Backup in dotazione*

USB-C™

PN	DESCRIZIONE
53401	Store 'n' Go Keypad Secure Portable HDD 1 TB
53403	Store 'n' Go Keypad Secure Portable HDD 2 TB

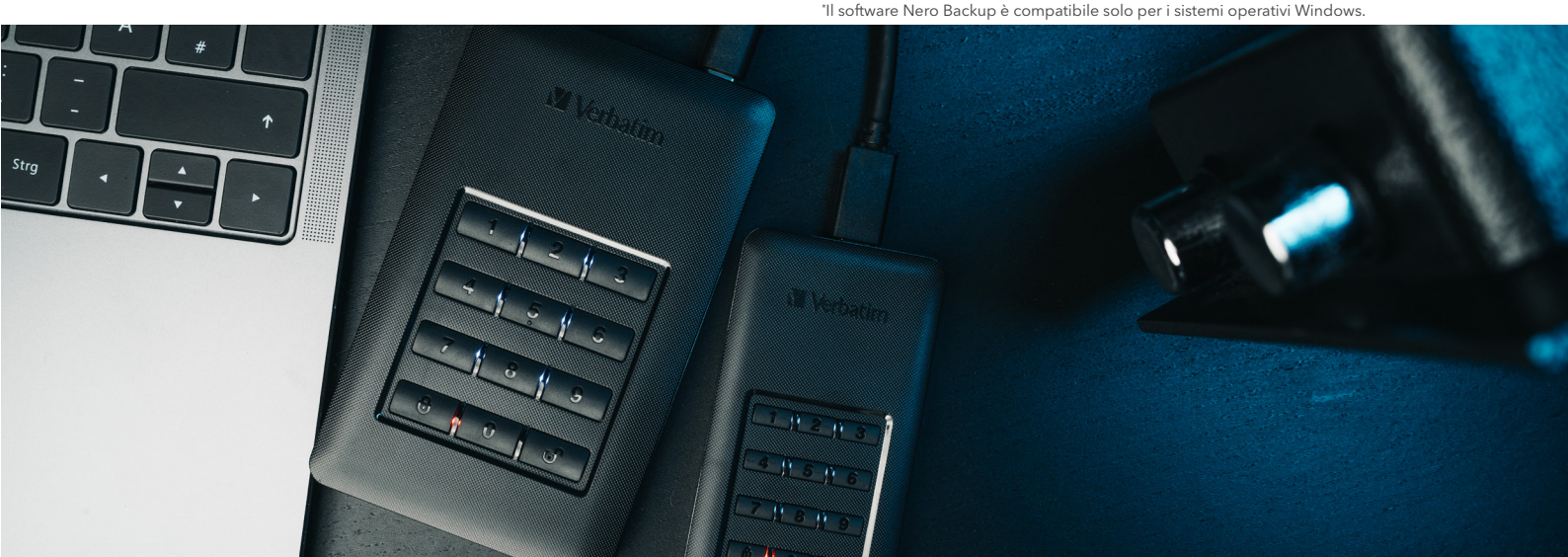
SSD Store 'n' Go protetto con tastierino di accesso

- Crittografia Hardware a 256 bit AES
- Tastierino integrato per inserimento del codice (da 5 a 12 cifre)
- Le memorie SSD utilizzano spazio di archiviazione con memoria flash per la massima rapidità, performance migliori e maggior affidabilità
- USB 3.2 Gen 1 con connessione USB-C™
- Indicatori LED per alimentazione / stato di crittografia
- Più sicuro della crittografia software
- Software Nero Backup in dotazione*

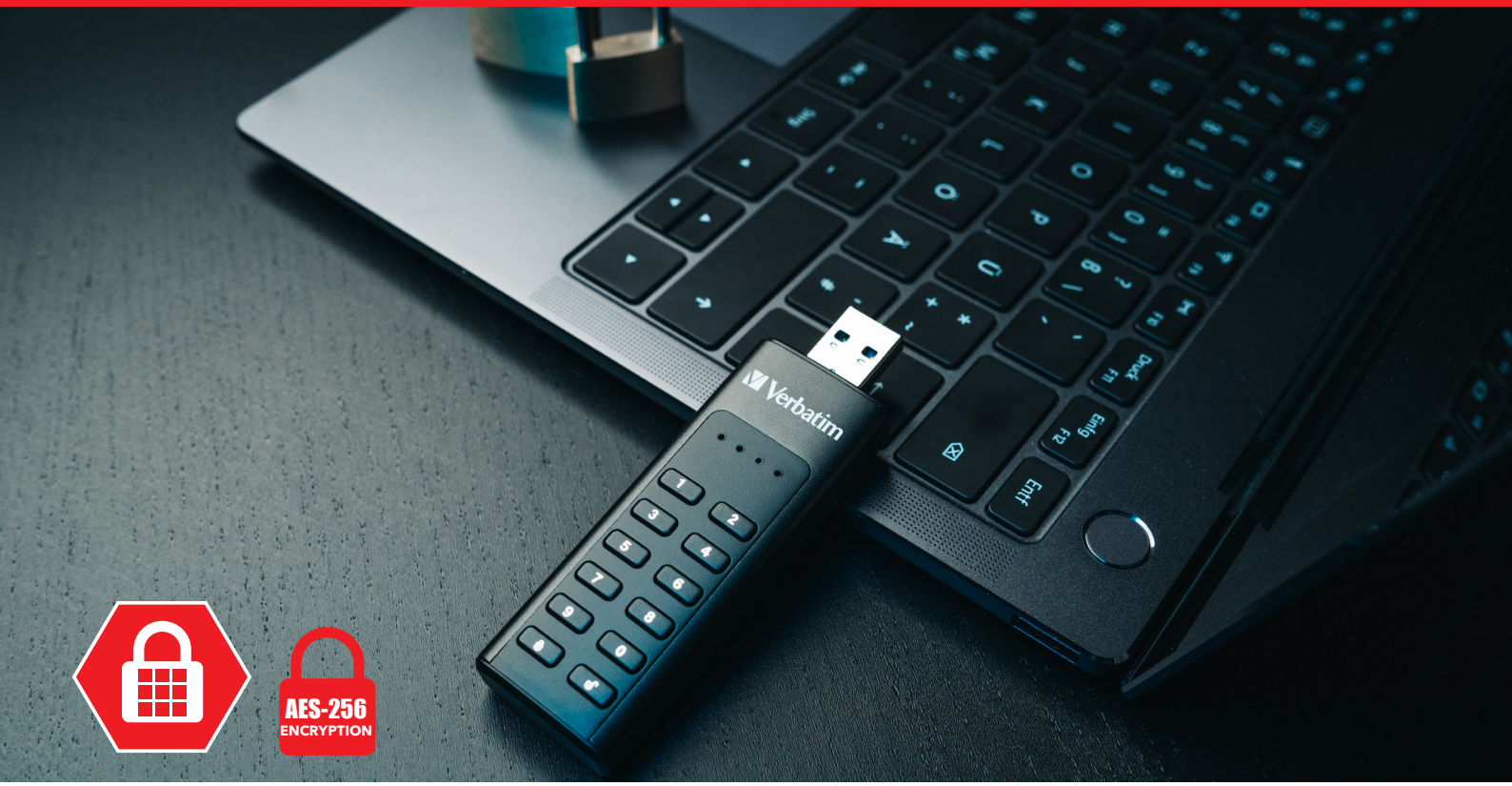
USB-C™

PN	DESCRIZIONE
53402	Store 'n' Go Keypad Secure Portable SSD 256 GB

*Il software Nero Backup è compatibile solo per i sistemi operativi Windows.



Archiviazione crittografata: Soluzioni USB



La chiavetta USB Keypad Secure offre una crittografia hardware AES a 256 bit e protegge i dati tramite un codice d'acceso da digitare con il tastierino integrato. Se stai cercando qualcosa di sicuro e conveniente allo stesso tempo la memoria USB Secure Data Pro è la soluzione che fa per te.

Keypad Secure USB con tastierino d'accesso

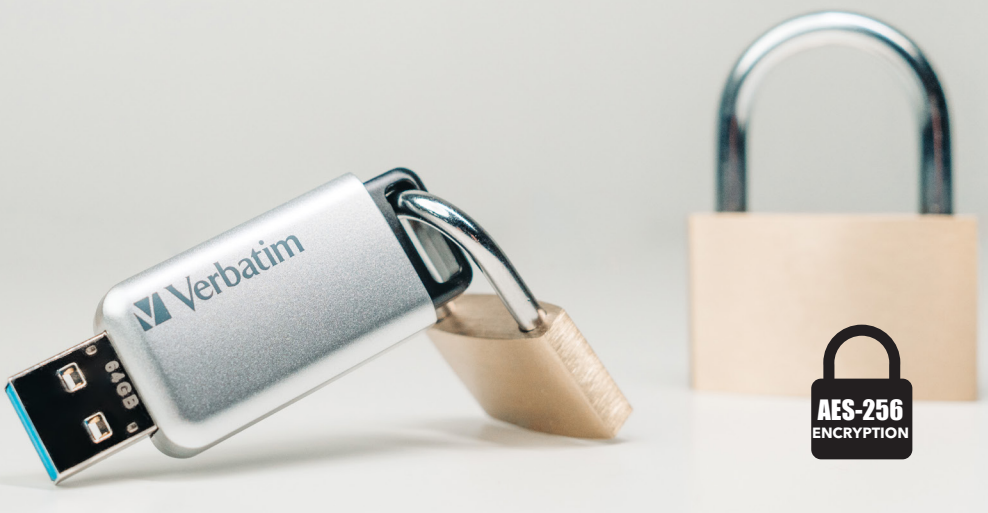
- Crittografia Hardware a 256 bit AES, cripta tutti i dati sull'unità in tempo reale
- Tastierino integrato per inserimento della password (fino a 12 cifre)
- Utilizzabile con i televisori (funzionalità non possibile con i normali dispositivi crittografati)
- Indicatori LED per alimentazione / stato di crittografia
- Non conserva la password nel computer o nella memoria volatile del sistema, garantendo quindi una maggiore protezione rispetto alla crittografia software
- Compatibile con PC e Mac

PN	DESCRIZIONE
Keypad Secure USB 3.2 Gen 1	
49427	Keypad Secure USB 3.2 Gen 1 Drive 32GB
49428	Keypad Secure USB 3.2 Gen 1 Drive 64GB
49429	Keypad Secure USB 3.2 Gen 1 Drive 128GB

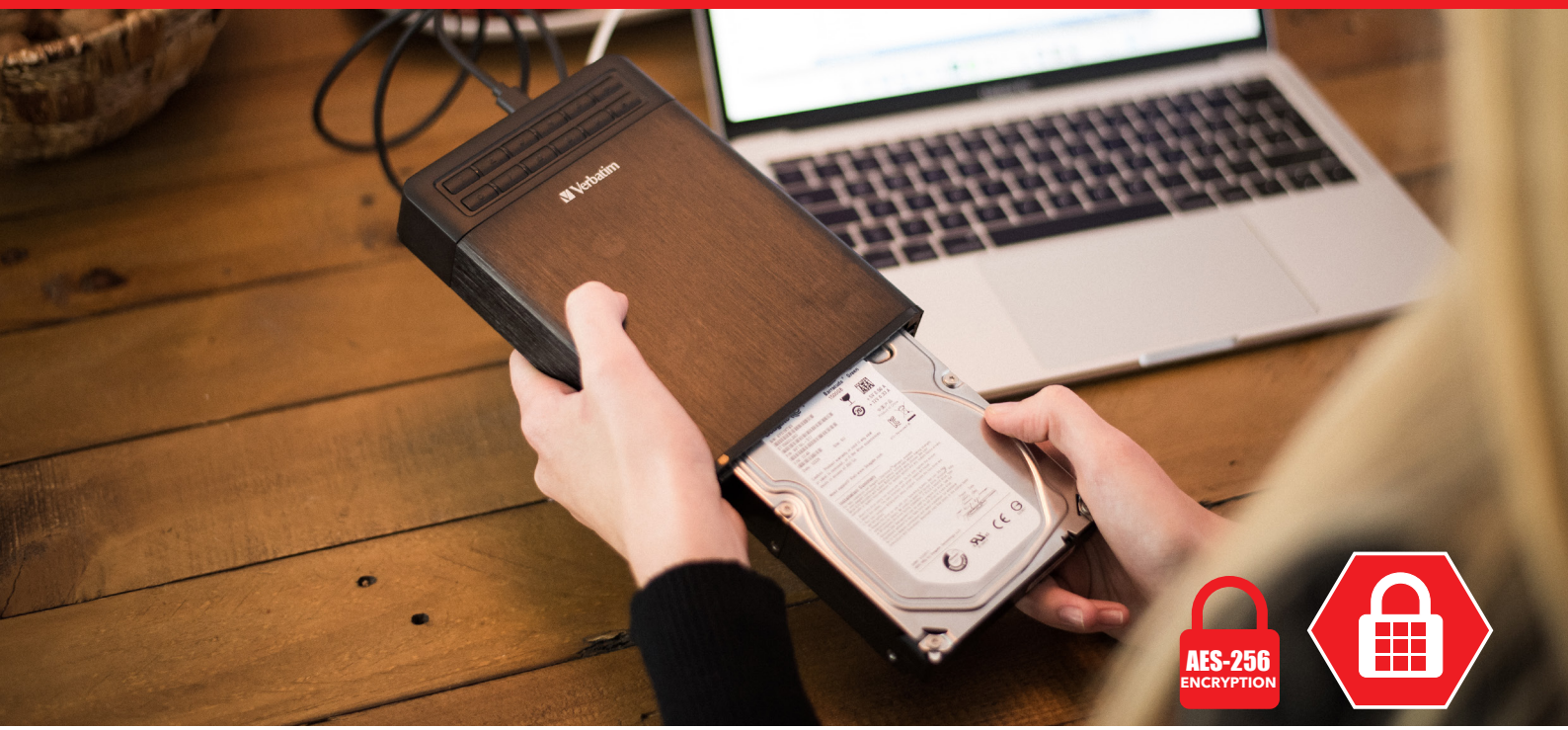
Secure Data Pro
Memoria USB 3.2 Gen 1 crittografata

- Crittografia hardware AES a 256 bit con controller di sicurezza basata sulla crittografia hardware
- Applicazione di protezione tramite password.
- Algoritmo di hashing della password
- Inserimento della password resistente agli hacker.

PN	DESCRIZIONE
98664	Secure Data Pro USB Drive USB 3.2 Gen 1 16GB
98665	Secure Data Pro USB Drive USB 3.2 Gen 1 32GB
98666	Secure Data Pro USB Drive USB 3.2 Gen 1 64GB



Archiviazione crittografata: alloggiamento per HDD con tastierino d'accesso



Trasforma il tuo vecchio disco rigido interno in un sicuro disco rigido esterno grazie a questo pratico kit. Contiene tutto il necessario per convertire un HDD interno SATA standard da 3,5 "in un disco rigido esterno con crittografia hardware AES a 256 bit e un tastierino integrato per l'immissione del codice d'accesso.

Secure Enclosure Kit da tavolo con tastierino numerico

- Tastierino numerico integrato per l'immissione del codice d'accesso di sicurezza
- Crittografia hardware AES a 256 bit
- Alloggiamento per disco rigido interno SATA standard da 3,5"
- Trasforma in pochi secondi il tuo disco interno in uno esterno
- USB 3.1 Gen 1 con connessione USB-C™
- Incluso cavo da USB-C™ a USB-A (con adattatore da USB-A a USB-C™)

USB-C™

PN	DESCRIZIONE
53405	Secure Desktop Hard Drive Enclosure with Keypad Access