TRAVAIL HYBRIDE

Assurer votre sécurité

Le travail hybride est devenu la norme pour beaucoup d'entre nous. De nombreux employeurs encouragent un mélange sain de travail au bureau et à distance. Certaines personnes s'épanouissent dans un bureau mais éprouvent des difficultés à travailler à domicile, un environnement mixte peut donc offrir le meilleur des deux mondes. Le travail à distance, qu'il soit réalisé depuis votre bureau à domicile ou en déplacement, a prouvé qu'il augmentait la productivité, réduisait les coûts et contribuait au bien-être personnel.

Mais il s'accompagne de certaines préoccupations. Le problème le plus important est sans doute celui de la sécurité des données : les travailleurs à distance sont plus susceptibles de se faire voler ou de perdre des objets.

Une façon de réduire ce risque est d'utiliser un stockage crypté. En sauvegardant vos fichiers sensibles sur des disques durs, des SSD ou des clés USB dotés d'un cryptage matériel AES 256 bits, vous vous assurez qu'en cas de perte ou de vol, les données ne seront pas accessibles. Bien qu'il soit frustrant de perdre le disque, cela donne à chacun la tranquillité d'esprit que les fichiers sont à l'abri des regards indiscrets !

Stockage crypté : Solutions biométriques

Les disques durs et SSD Executive Fingerprint Secure utilisent une combinaison de cryptage matériel AES 256 bits et de technologie biométrique pour une sécurité totale des informations, le tout dans un boîtier élégant en aluminium.

Disques Durs et SSD Executive Fingerprint Secure

- Stockez vos données et sécurisez votre disque dur avec votre empreinte digitale.
- Disque dur portable USB-C™ avec scanner d'empreintes digitales intégré.
- Accès au disque à l'aide de l'empreinte digitale d'un utilisateur autorisé.
- Cryptage matériel AES 256 bits premium.
- Jusqu'à huit utilisateurs autorisés plus un administrateur (via un mot de passe).
- Design élégant en aluminium.
- Prise en charge de l'interface USB Super-speed (5Gbps).
- Logiciel de sauvegarde Nero Backup inclus*.

AES-256 ENCRYPTION

up to 8 users

USB-C™

RÉF.	DESCRIPTION
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

*Le logiciel Nero Backup convient uniquement aux systèmes d'exploitation Windows.

Stockage crypté : Solutions biométriques

Vous faites à nouveau la navette pour travail ? Sauvegarder votre travail en toute sécurité est une chose dont vous devez vous assurer. Les solutions de stockage cryptées à l'aide de vos empreintes digitales de Verbatim vous assureront que vos données sont sauvegardées en toute sécurité, où que vous soyez !

Disque dur Fingerprint Secure

- Accès par reconnaissance des empreintes digitales.
- Connexion USB-C™.
- Cryptage matériel AES 256 bits premium.
- Jusqu'à huit utilisateurs autorisés plus un administrateur (via un mot de passe).
- Stockez et transportez des données confidentielles tout en étant protégé contre la perte ou le piratage.
- Design noir élégant avec une surface 3D assortie à la gamme SSD.
- USB 3.2 GEN 1 avec connexion USB-C™ et adaptateur USB-C™.

AES-256 ENCRYPTION

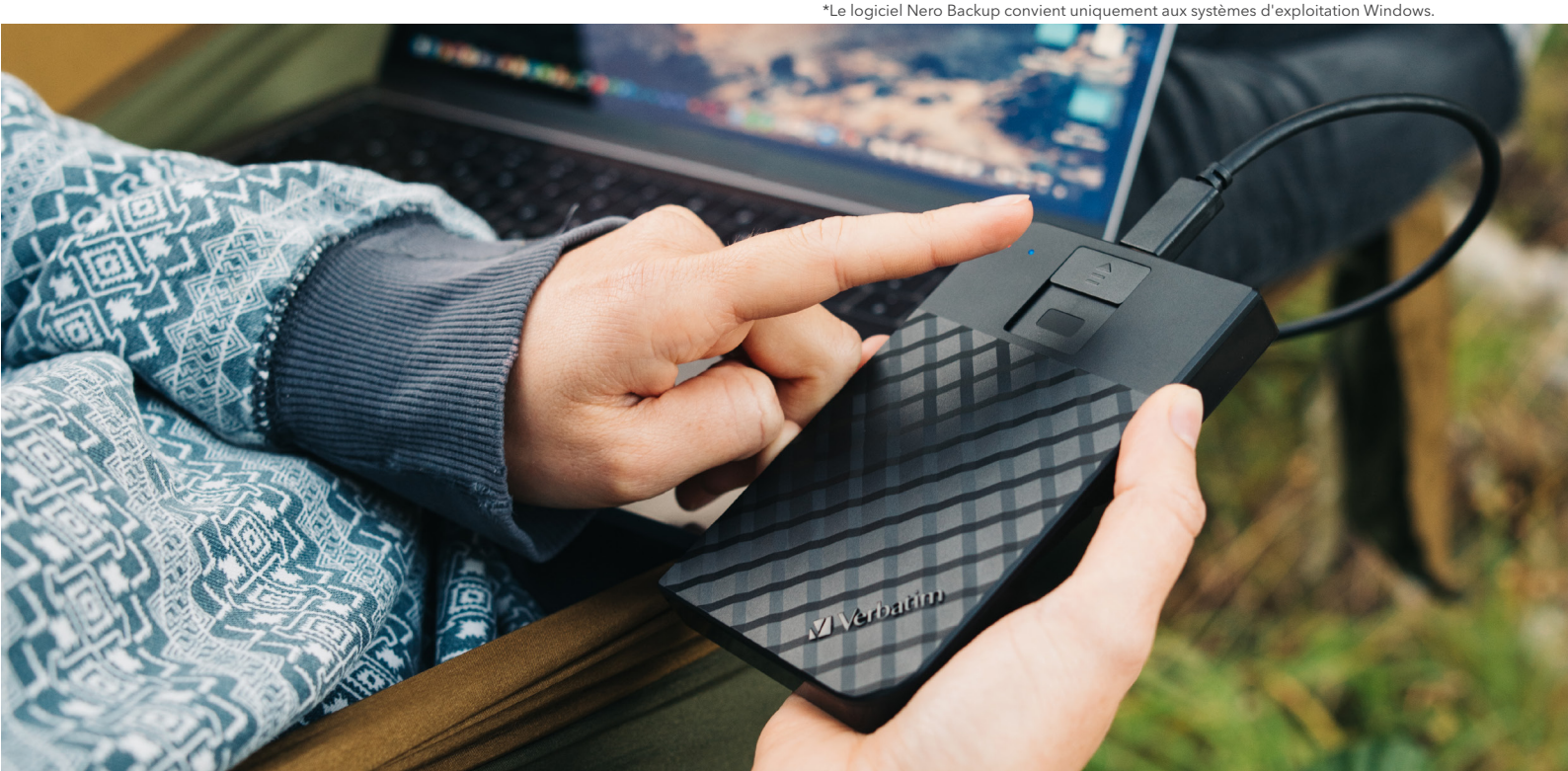
up to 8 users

USB-C™

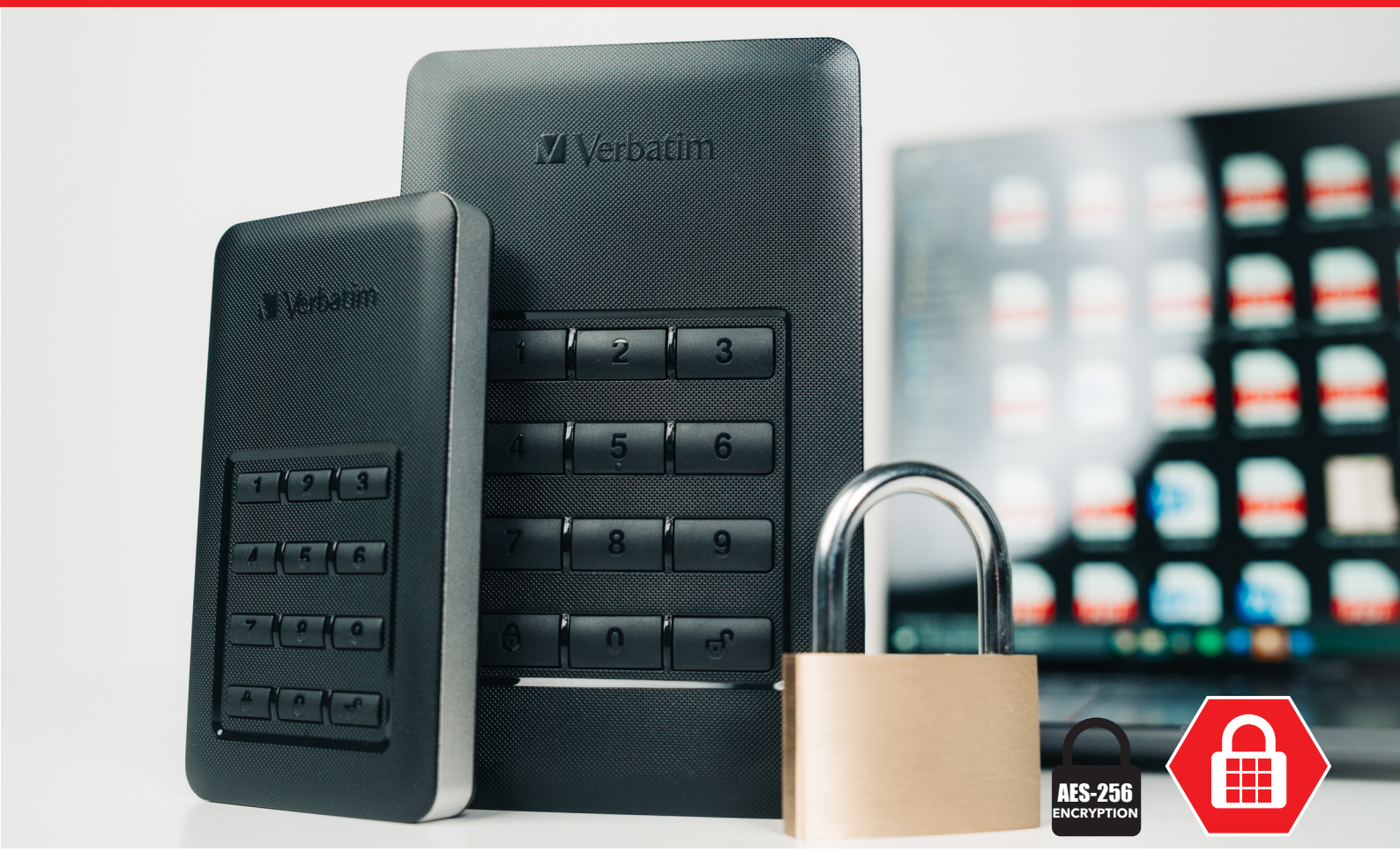
- Indicateurs LED d'état d'alimentation/de cryptage.
- Logiciel Nero Backup inclus*.

RÉF.	DESCRIPTION
53650	Fingerprint Secure Portable HDD 1 TB
53651	Fingerprint Secure Portable HDD 2 TB

*Le logiciel Nero Backup convient uniquement aux systèmes d'exploitation Windows.



Stockage crypté : Solutions avec accès par clavier



Le cryptage matériel AES 256 bits chiffre en temps réel et de manière transparente toutes les données présentes sur le disque. Il faut un mot de passe pour y accéder via le clavier intégré. Une solution de stockage simple et sécurisée.

Disque dur portable sécurisé avec accès par clavier

- Cryptage matériel AES 256 bits premium.
- Clavier intégré pour la saisie du code d'accès (5 à 12 chiffres).
- Peut être utilisé avec des téléviseurs (fonctionnalité incompatible avec les disques durs cryptés ordinaires).
- USB 3.2 GEN 1 avec connexion USB-C™ et adaptateur USB-C™.
- Indicateurs LED d'alimentation/d'état de cryptage.
- Logiciel Nero Backup inclus*.

USB-C™

RÉF.	DESCRIPTION
53401	Store 'n' Go Keypad Secure Portable HDD 1 TB
53403	Store 'n' Go Keypad Secure Portable HDD 2 TB

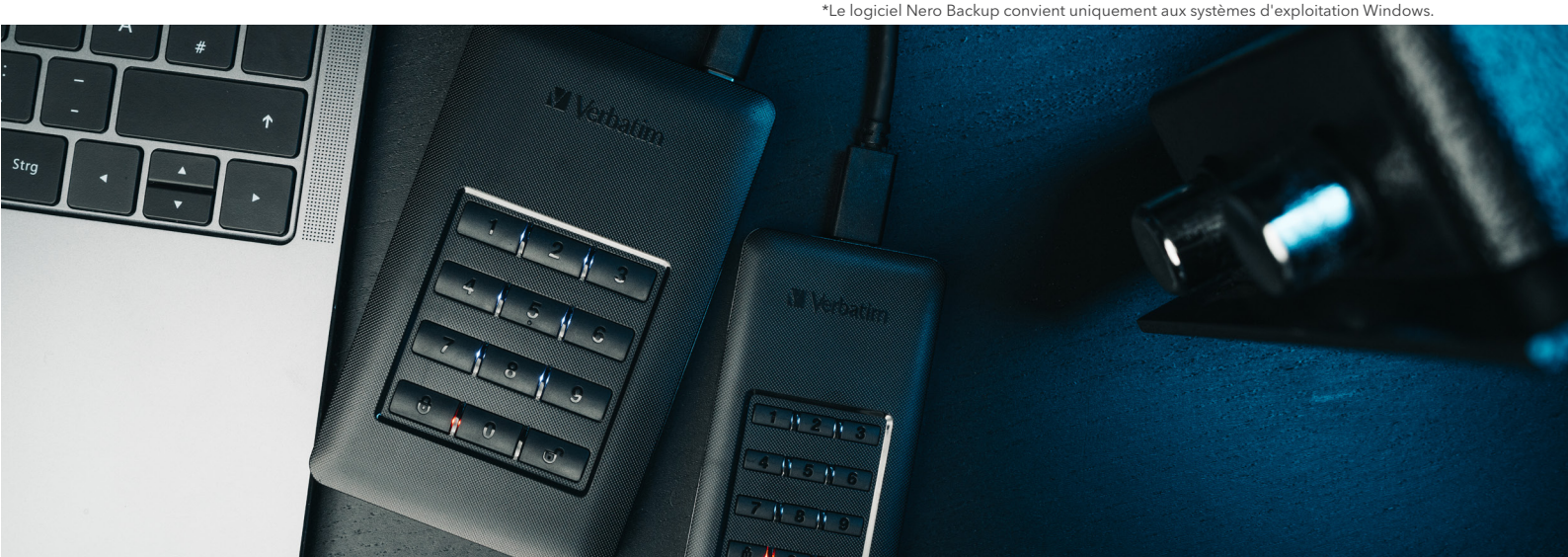
SSD Store 'n' Go sécurisé avec accès par clavier

- Cryptage matériel AES 256 bits premium.
- Clavier intégré avec saisie du code d'accès (5 à 12 chiffres).
- Les SSD utilisent un espace de stockage en mémoire flash pour des vitesses plus rapides, des performances plus élevées et une plus grande fiabilité.
- USB 3.2 GEN 1 avec connexion USB-C™.
- Indicateurs LED d'état d'alimentation/de cryptage.
- Plus sûr que le cryptage logiciel.
- Logiciel Nero Backup fourni*.

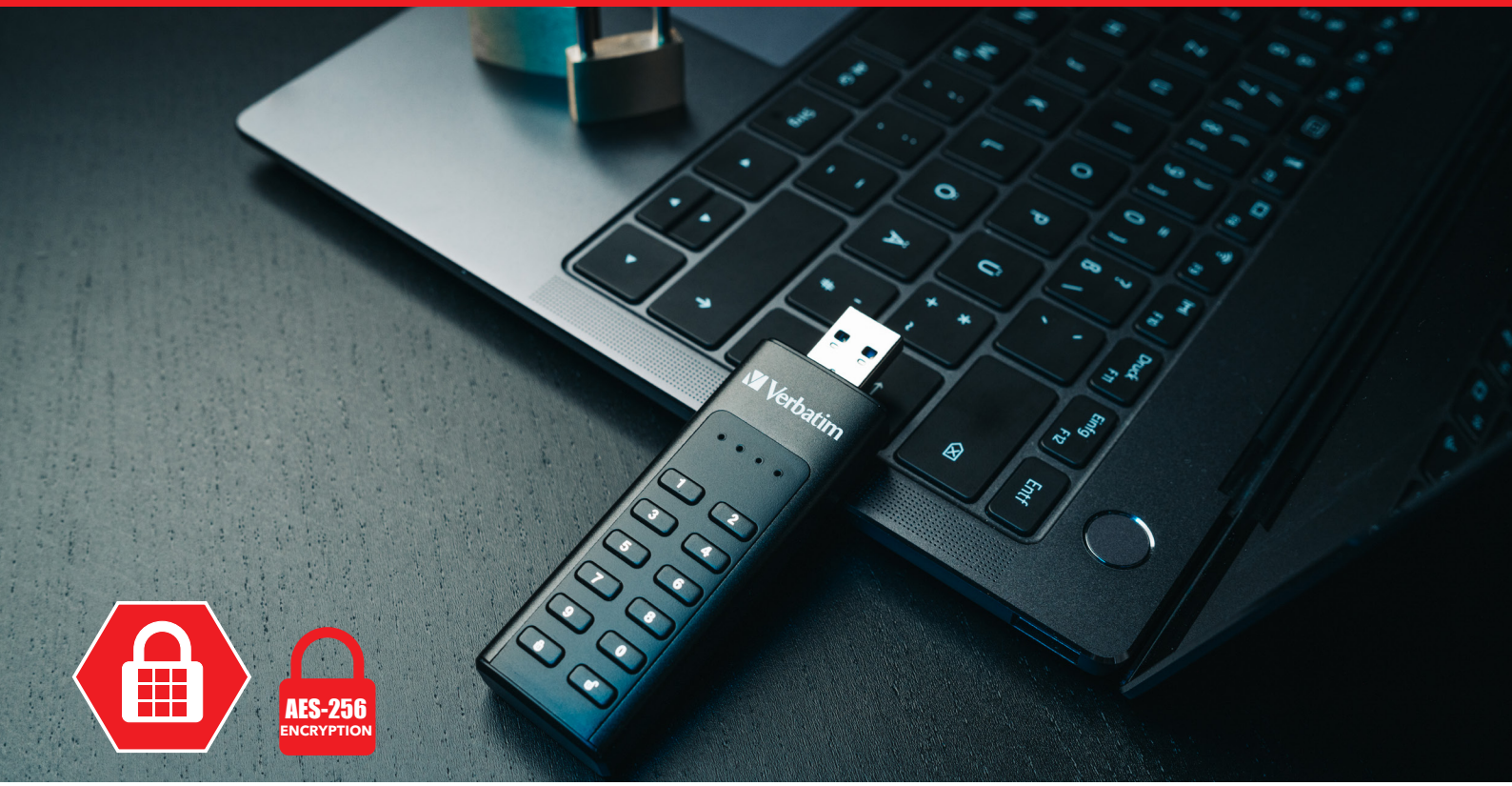
USB-C™

RÉF.	DESCRIPTION
53402	Store 'n' Go Keypad Secure Portable SSD 256 GB

*Le logiciel Nero Backup convient uniquement aux systèmes d'exploitation Windows.



Stockage crypté : Solutions USB



La clé USB sécurisée avec accès par clavier Verbatim offre un cryptage matériel AES 256 bits premium et une protection par mot de passe intégrée, ce qui permet de protéger vos données confidentielles. Si vous recherchez quelque chose de sûr et d'abordable à la fois, alors ne cherchez pas plus loin que la clé USB cryptée Secure Data Pro.

Clé USB sécurisée avec accès par clavier

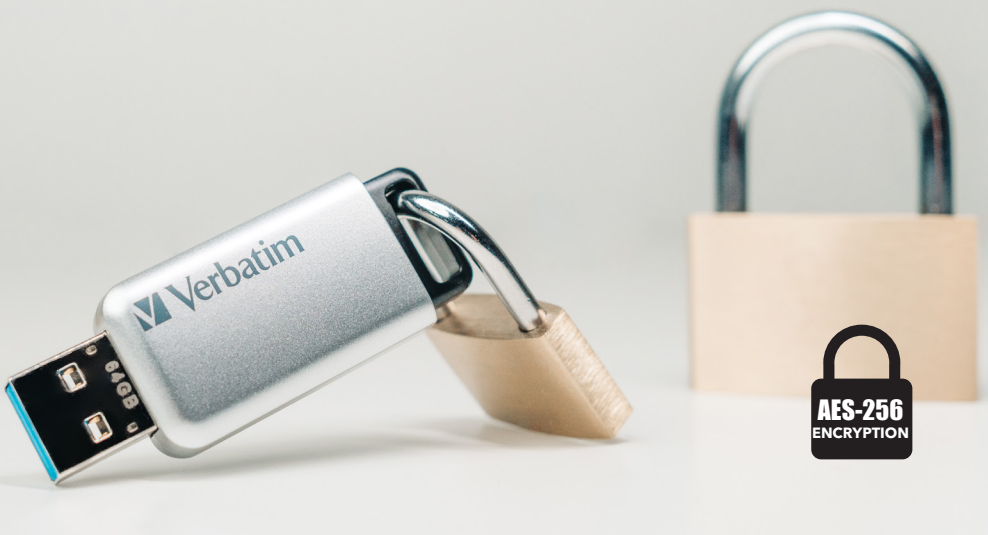
- Cryptage matériel AES 256 bits, qui crypte en toute transparence toutes les données du lecteur en temps réel.
- Clavier intégré pour la saisie du code d'accès (jusqu'à 12 chiffres).
- Peut être utilisé avec des téléviseurs (fonctionnalité incompatible avec les dispositifs cryptés ordinaires).
- Indicateurs LED d'alimentation et d'état de cryptage.
- Ne stocke pas le mot de passe dans l'ordinateur ou dans la mémoire volatile du système, donc beaucoup plus sûr que le cryptage logiciel.
- Compatible PC et Mac.

RÉF.	DESCRIPTION
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

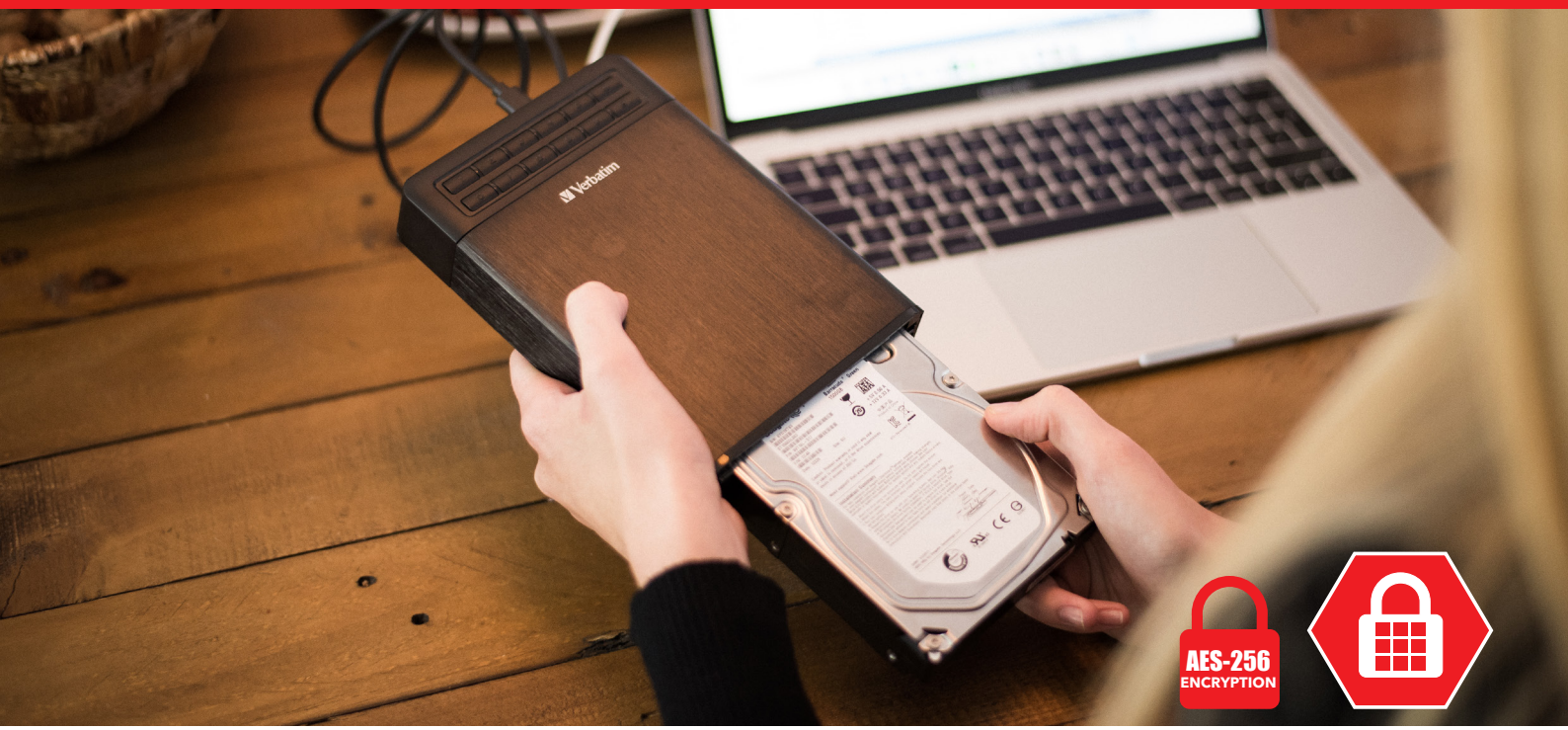
Secure Data Pro
Clé USB 3.2 Gen 1 cryptée

- Cryptage matériel AES 256 bits avec contrôleur de sécurité basé sur un cryptage matériel.
- Application de protection par mot de passe.
- Algorithme de hachage du mot de passe.
- Saisie du mot de passe résistant au piratage.

RÉF.	DESCRIPTION
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



Stockage crypté : Solutions avec accès à clavier pour les boîtiers de disques durs



Transformez votre vieux disque dur interne en un disque dur externe sécurisé grâce à ce kit de boîtier pratique. Il contient tout ce dont vous avez besoin pour convertir un disque dur interne SATA standard de 3,5" en votre propre disque dur externe crypté, y compris un cryptage matériel AES 256 bits et un clavier intégré pour la saisie sécurisée du code d'accès.

Kit de boîtier de disque dur sécurisé avec accès par clavier

- Clavier intégré pour une saisie sécurisée du code d'accès.
- Cryptage matériel AES 256 bits.
- Boîtier pour disque dur de 3,5 pouces.
- Convient à tout disque dur interne SATA standard de 3,5 pouces.
- Installation facile, aucune connaissance technique avancée n'est requise.
- USB 3.1 GEN 1 avec connexion USB-C™ et adaptateur USB-C™.

USB-C™

RÉF.	DESCRIPTION
53405	Secure Desktop Hard Drive Enclosure with Keypad Access