



Kingston IronKey Vault Privacy 50 Series - clé USB - 32 Go - Conformité TAA FIPS

Codes produits :

Référence TE329056

EAN13 : 740617329056

CUP : -

Galerie de produits :



Description brève du produit :

Kingston Technology IronKey 32Go Vault Privacy 50 chiffrée AES-256, FIPS 197, 32 Go, USB Type-A, 3.2 Gen 1 (3.1 Gen 1), 250 Mo/s, Casquette, Noir, Bleu

Description du produit :

Les clés USB de la gamme Kingston IronKey™ Vault Privacy 50 sont des clés USB Type-A et USB Type-C®* haut de gamme qui offrent une sécurité de niveau entreprise grâce au chiffrement matériel AES 256 bits certifié FIPS 197 en mode XTS. Elle offre également une protection contre les BadUSB avec un firmware signé numériquement et contre les attaques par force brute visant les mots de passe. La VP50 a fait l'objet d'un test d'intrusion***** (Pen Tested) pour une sécurité de classe entreprise. Comme il s'agit d'un stockage chiffré sous le contrôle physique de l'utilisateur, la série VP50 offre une sécurité supérieure à Internet et aux services cloud pour la sauvegarde des données.

La Vault Privacy 50 prend en charge l'option multi-mots de passe (admin, utilisateur et récupération à usage unique) avec les modes complexe ou phrase de passe. Cela permet de récupérer l'accès aux données si l'un des mots de passe est oublié. Le mode Complexe classique permet des mots de passe de 6 à 16 caractères en utilisant 3 des 4

jeux de caractères. Le nouveau mode Phrase de passe permet d'utiliser un code PIN numérique, une phrase, une liste de mots ou même des paroles de chanson de 10 à 64 caractères. L'administrateur peut activer un mot de passe utilisateur et un mot de passe de récupération à usage unique, ou réinitialiser le mot de passe utilisateur pour restaurer l'accès aux données. Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, réduisant ainsi les fautes de frappe entraînant des tentatives de connexion infructueuses. La protection contre les attaques par force brute verrouille le mot de passe utilisateur ou le mot de passe de récupération à usage unique si 10 mots de passe incorrects sont saisis de suite, et efface les données sécurisées de la clé USB si le mot de passe administrateur est saisi de manière incorrecte 10 fois de suite.

Pour se protéger contre les logiciels malveillants potentiels sur les systèmes non fiables, l'administrateur et l'utilisateur peuvent définir le mode lecture seule pour protéger la clé USB en écriture. De plus, le clavier virtuel intégré protège les mots de passe contre les enregistreurs de frappe ou d'écran.

Les clés USB de la série VP50 peuvent être personnalisées et configurées avec un identifiant produit (PID) via le programme de personnalisation de Kingston. Et ce, pour les intégrer à un logiciel standard de gestion des terminaux afin de répondre aux exigences des entreprises en matière d'informatique et de cybersécurité.

Les petites et moyennes entreprises peuvent utiliser le rôle Administrateur pour gérer leurs clés USB en local, par exemple pour configurer ou réinitialiser le mot de passe Utilisateur ou le Mot de passe de récupération à usage unique des employés, récupérer l'accès aux données sur des clés USB verrouillées, et se conformer aux lois et règlements lorsque des enquêtes sont nécessaires.

La Vault Privacy 50 offre des performances élevées à double canal sur toutes les capacités. Cette clé USB est étanche avec une classification IPX8****, conforme à la norme TAA, et assemblée aux États-Unis.

Clé USB à chiffrement matériel pour protection des données

Protégez vos données importantes grâce au chiffrement XTS-AES 256 bits certifié FIPS 197. Protections intégrées contre les attaques BadUSB et par force brute, et tests d'intrusion pour assurer une sécurité de classe entreprise.

Option multi-mots de passe pour la récupération de données

Activez les mots de passe Admin, Utilisateur et de récupération à usage unique. L'administrateur peut réinitialiser le mot de passe utilisateur et créer un mot de passe de récupération à usage unique pour rétablir l'accès de l'utilisateur aux données. La protection contre les attaques par force brute verrouille le mot de passe utilisateur ou le mot de passe de récupération à usage unique si 10 mots de passe incorrects sont saisis de suite, et efface les données sécurisées de la clé USB si le mot de passe administrateur est saisi de manière incorrecte 10 fois de suite.

Nouveau mode phrase secrète

Choisissez entre le mode de mot de passe Complexe ou Phrase de passe. Les phrases de passe peuvent être un code PIN numérique, une phrase avec des espaces, une liste de mots ou même des paroles de chansons, et doivent comporter de 10 à 64 caractères.

Paramètres double lecture seule (protection en écriture)

Évitez les attaques de logiciels malveillants avec un mode lecture seule forcé défini par l'administrateur pour l'utilisateur, ou un mode lecture seule basé sur la session défini par l'administrateur ou l'utilisateur.

Gérer les clés USB pour les petites et moyennes entreprises

Utilisez le rôle d'administrateur pour gérer localement les mots de passe utilisateur et de récupération à usage unique des employés, récupérer l'accès aux données sur des clés USB verrouillées et vous conformer aux lois et réglementations lorsque des analyses médico-légales sont nécessaires.

Fonctionnalités supplémentaires liées à la sécurité

Réduisez les tentatives de connexion infructueuses et la frustration en activant le bouton « œil » pour afficher le mot de passe saisi. Utilisez le clavier virtuel pour protéger la saisie de votre mot de passe contre les enregistreurs de frappe et les enregistreurs d'écran.

Kingston Technology IronKey 32Go Vault Privacy 50 chiffrée AES-256, FIPS 197. Capacité: 32 Go, Interface de l'appareil: USB Type-A, Version USB: 3.2 Gen 1 (3.1 Gen 1), Vitesse de lecture: 250 Mo/s, Vitesse d'écriture: 180 Mo/s. Format: Casquette. Protection par mot de passe. Poids: 15 g. Couleur du produit: Noir, Bleu