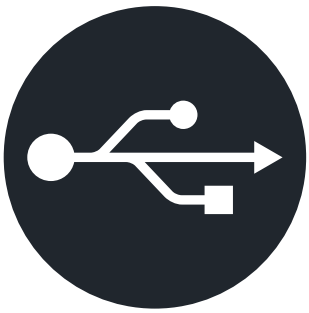
Comment autoriser l'accès d'une clé USB

sans compromettre la sécurité des terminaux

#KingstonIsWithYou #KingstonIronkey

Introduction

Le lancement en janvier 1996 de la spécification officielle USB 1.0 annonçait une nouvelle ère d'uniformité, de commodité et de polyvalence pour les fabricants d'appareils et les utilisateurs finaux. Vingt-sept années plus tard, chaque nouvelle révision maintient la rétrocompatibilité et le protocole USB conserve son rôle de pierre angulaire de l'interface matérielle informatique, depuis les serveurs jusqu'aux smartphones.



La simplicité du Plug N Play et les débits toujours plus élevés ont contribué au succès du stockage portable via USB. Cela étant, cette convivialité implique certaines concessions en matière de sécurité des données. Dans le monde actuel, sans l'utilisation d'outils appropriés tels que la protection des ordinateurs hôtes et les pratiques de sécurité des données, les utilisateurs qui font preuve de négligence dans l'utilisation du stockage USB portable s'exposent, ainsi que les autres, à d'éventuelles violations des données qui pourraient être coûteuses pour l'utilisateur final et même compromettre une organisation ou un gouvernement tout entier.

Outre la protection déployée sur l'ordinateur hôte, il convient également de sécuriser la clé USB à l'aide d'un mot de passe et d'un chiffrement matériel sur l'appareil. Ce niveau de protection est bien plus robuste contre les intrusions. Vous allez découvrir ci-après quelques-unes des meilleures pratiques pour renforcer la sécurité de l'utilisation des clés USB. Nous en profiterons pour fournir également des informations plus poussées sur les clés USB en général.

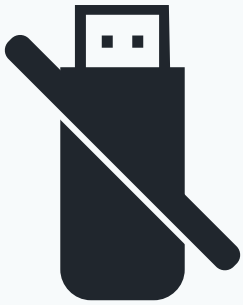
S'il est vrai que la démarche combinée est idéale, il ne faut pas oublier que la fiabilité du chiffrement et la solidité des composants matériels de la clé USB en elle-même sont d'une importance cruciale. Les secteurs d'activité les plus divers, depuis la finance jusqu'aux soins de santé en passant par la fabrication et le secteur militaire, en profitent. Ces deux éléments interviennent également dans le travail à distance, lorsque l'accès au réseau n'est pas disponible, n'est pas protégé ou n'est pas pratique.

Les clés USB à chiffrement matériel sont disponibles avec différents niveaux de certification tout en offrant une gamme de fonctions de sécurité. En examinant leurs attributs et les possibilités de personnalisation, leur aptitude à être des solutions autonomes est également illustrée en assurant leur place dans toutes sortes d'environnements sensibles.

Gestion des ports : stockage USB et logiciel de prévention des pertes de données pour la gestion des terminaux

Depuis des décennies, les applications antivirus et anti logiciels malveillants offrent une protection au niveau le plus fondamental - en analysant automatiquement les téléchargements et les appareils connectés et en signalant les contenus suspects ou en agissant en conséquence. La protection offerte par les logiciels NGAV (antivirus nouvelle génération) franchit un pas supplémentaire. Ces logiciels ne comptent plus exclusivement sur la mise à jour permanente de bases de données des signatures de virus. En effet, ils ajoutent également le machine learning et la détection des comportements afin d'identifier les menaces inconnues et d'adopter les mesures d'atténuation requises.

L'arsenal de protection ne se limite pas à ces options. Si vous souhaitez blinder la protection des appareils des utilisateurs, envisagez l'utilisation d'un logiciel de prévention des pertes de données (DLP) pour gestion de terminaux afin de refuser les accès de tout type aux ports USB et autres points d'accès.



La démarche du « Bloquer tous les ports » en matière de sécurité élimine sans aucun doute le risque et dans certaines situations, cette technique est souhaitable. Toutefois, son manque de finesse peut avoir des conséquences indésirables.

Toujours est-il que certains administrateurs IT préfèrent rejeter les demandes d'ouverture de ports USB sur les machines des utilisateurs, car une telle ouverture offrirait un accès direct au travers du pare-feu de l'entreprise. Cette attitude prudente est compréhensible, mais s'agissant de l'activation de l'accès pour le stockage USB, l'octroi d'un tel privilège ne devrait pas créer un problème de sécurité massif, à condition de respecter certaines conditions.

Il est essentiel de disposer d'une suite d'applications de gestion des terminaux qui permette de détecter les menaces grâce à des solutions antivirus/anti-logiciels malveillants et de centraliser la surveillance et la gestion des terminaux des utilisateurs.

En général, cette démarche directe est celle que proposent des solutions unifiées de vendeurs reconnus. Prenez par exemple McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection et WinMagic SecureDoc pour n'en citer que quelques-unes.

Listes d'autorisation affinées

La méthode que vous allez choisir pour sécuriser les appareils de stockage USB va dépendre du niveau de protection souhaité. Une démarche simple et efficace consiste à créer une liste d'appareils de stockage USB autorisés sur la base de leurs identifiant de fabricant (VID) et de produit (PID). Il faut savoir que chaque appareil USB qui sort des chaînes de production possède un VID unique, tandis que le PID change à chaque nouveau produit commercialisé.

Dans le cadre de la création d'une liste d'autorisations (ou « liste blanche ») , le recours à la seule valeur VID serait trop vague pour garantir la sécurité, car l'ensemble des appareils jamais produits par ce fabricant seraient autorisés. L'ajout du PID offre une plus grande précision dans l'administration et permet seulement à un modèle spécifique d'accéder au système hôte.

C'est une amélioration appréciable, mais ça n'est pas la solution idéale. Les appareils de stockage USB sont extrêmement populaires car ils permettent aux utilisateurs d'acquérir leurs propres appareils correspondant aux modèles autorisés. Dans ce contexte, Kingston Technology a décidé d'offrir une solution sur mesure pour renforcer la sécurité liée aux appareils de stockage USB.

Kingston Technology a mis en place un programme de personnalisation qui lui permet de créer des profils PID sur mesure propres à une organisation et de les appliquer à une gamme de clés USB chiffrées Kingston. Les sociétés qui décident de déployer des appareils dotés d'un identificateur de produit personnalisé profitent d'une application simplifiée des listes d'autorisation et d'une sécurité renforcée. L'employé aura beau acheter des appareils identiques aux modèles d'appareils autorisés, il n'obtiendra pas l'accès, car il n'y aura pas d'équivalence au niveau du PID personnalisé.

Alors que le recours aux valeurs PID personnalisées permet aux administrateurs informatiques d'intégrer rapidement et facilement de nouveaux appareils de stockage USB, il existe une démarche plus adaptée encore qui repose sur les

numéros de série individuels inscrits sur la majorité des clés USB chiffrées de Kingston. Cet arrangement exige que le numéro de série unique de chaque appareil soit enregistré dans la suite de gestion des terminaux. L'opération requiert la participation du personnel informatique et Kingston peut accompagner chaque commande de la liste des numéros de série (alphanumériques et non séquentiels). Le choix de cette méthode permet des politiques beaucoup plus souples basées sur la propriété de l'appareil personnel, avec en prime une recherche précise de la provenance des dispositifs, ce qui peut être très utile dans un contexte judiciaire. Certaines clés de Kingston possèdent un numéro de série et un code-barre sur le boîtier pour le scannage. D'autres clés sont proposées avec une option de personnalisation impliquant l'ajout d'un code-barre et d'un numéro de série sur le boîtier pour les entreprises. Ces éléments peuvent intervenir dans le suivi des appareils.

Par défaut, les systèmes de gestion de terminaux proposent l'accès au VID/PID pour le blocage des ports et la création de listes d'autorisation. Kingston offre une plus grande polyvalence dans l'exploitation de ces fonctionnalités afin de permettre l'adoption de stratégies plus souples et plus imaginatives pour faciliter l'utilisation des appareils de stockage USB. Dès le moment où vous avez défini une méthode d'identification adéquate, la stratégie globale du « Bloquer tous les ports » devient non seulement trop simpliste, mais également inutile.

Des solutions conformes et sécurisées pour les utilisateurs à distance

En matière de sécurité, la technique des listes d'autorisations ne traite que d'une moitié du problème ou que d'une moitié de la solution.

La convivialité et la simplicité d'utilisation des appareils de stockage USB les rendent indispensables dans de nombreuses entreprises et institutions où la portabilité est un concept essentiel afin d'éviter les difficultés en matière de transfert de données. Dans la majorité des environnements, il convient de fournir aux membres du personnel des clés USB chiffrées pour des raisons de conformité et de bonnes pratiques informatiques. La combinaison de la protection par mot de passe et du chiffrement de l'appareil donnent au stockage portable les protections requises pour éviter l'accès aux données sensibles en cas de perte ou de vol d'un appareil ou lorsque ce dernier se retrouve dans une situation de potentielle vulnérabilité.

Il ne s'agit pas d'une solution uniforme, car les techniques de chiffrement varient et les différences les plus notables apparaissent au moment de comparer les solutions de chiffrement logiciel et matériel. Lequel des deux est le meilleur ? La réponse dépend de vos besoins. La question qui mérite d'être posée serait plutôt « Lequel des deux est le plus sûr ? »

Le chiffrement logiciel est essentiellement un choix budgétaire qui satisfera certains secteurs ayant des activités plus modestes. Le chiffrement logiciel peut également être l'option adoptée par les entreprises où les transferts de données ne sont pas sensibles et où la priorité est avant tout la conformité à une politique.

Cela étant dit, le principe de fonctionnement du chiffrement logiciel constitue également son talon d'Achille, car l'exécution des tâches de chiffrement requiert des applications clients installées sur un ordinateur. Par conséquent, la sécurité d'un appareil de stockage à chiffrement logiciel est directement proportionnelle à la sécurité de l'ordinateur hôte.

L'exposition aux exploits est également accrue car les pirates ayant accès à la mémoire de l'ordinateur peuvent « renifler » les clés de chiffrement/déchiffrement. Les données stockées sur la clé peuvent également être victimes d'attaques par force brute vu que la protection par mot de passe n'est pas requise s'il est possible d'accéder aux fichiers chiffrés et de les copier.

Il ne faut pas oublier non plus qu'il faudra probablement appliquer de temps à autres des mises à jour logicielles pour le chiffrement logiciel. Ces mises à jour peuvent compliquer la mise en œuvre en augmentant la charge de travail du personnel informatique. Pire encore, le chiffrement logiciel peut être totalement supprimé par des employés frustrés qui ont des problèmes avec la portabilité du disque sur différentes plateformes. En effet, l'utilisateur de la clé chiffrée peut copier les données sur un ordinateur, reformater la clé en clé non chiffrée, puis copier à nouveau les données sur celle-ci. Dès ce moment, les données ne seraient plus protégées et le risque de divulgation serait total. Pour des raisons de conformité aux lois et réglementations sur la confidentialité des données, la désactivation de la sécurité d'une clé USB est proscrite.

Le chiffrement sur puce : la solution robuste et rapide

Une clé USB à chiffrement matériel, quant à elle, ne dépend d'aucun ordinateur, car elle intègre un processeur dédié chargé de gérer le chiffrement sur la clé. Le chiffrement est activé en permanence et il est doté d'une protection contre les attaques de mot de passe par force brute. Les données chiffrées sont inaccessibles et ne peuvent être copiées.

Les clés USB à chiffrement matériel de niveau industriel ou militaire de Kingston adoptent le chiffrement AES 256 bits en mode XTS. Approuvé à travers le monde, le chiffrement AES 256 bits offre une protection des données rigoureuse. En utilisant deux clés distinctes à différents stades du processus de chiffrement/déchiffrement, le mode XTS a un effet similaire à celui d'un double chiffrement des données.

Dans la pratique, la clé de chiffrement est dérivée du générateur de numéro aléatoire du contrôleur de la clé USB que l'utilisateur déverrouille à l'aide du mot de passe. Vu que l'authentification se déroule au sein du matériel de chiffrement de la clé, les clés de chiffrement et les autres fonctions de sécurité critiques ne sont pas exposées aux codes d'exploitation communs tels que BadUSB, aux attaques de démarrage à froid, au code malveillant ou aux attaques par force brute.

Parmi les avantages immédiats du chiffrement matériel, il faut citer la performance de la clé qui est sensiblement supérieure à celle d'une clé à chiffrement logiciel, car les tâches de chiffrement ne sont pas transférées à l'ordinateur hôte. Tout se déroule au sein même de la clé.

Les clés USB à chiffrement matériel comme la Kingston IronKey D500S sont des appareils protégés par mot de passe qui sont chiffrés dès leur sortie de l'emballage. Dans la pratique, seul le volume de lancement protégé en écriture est visible au départ. Il contient l'application qui permet d'authentifier le mot de passe et de déverrouiller le volume de stockage chiffré principal. Grâce à cette procédure, il n'est pas nécessaire d'installer un pilote ou un logiciel sur l'ordinateur hôte.

De plus, les clés USB à chiffrement matériel de Kingston sont dotées de firmware à signature numérique, ce qui empêche toute manipulation du firmware au sein de la clé. Cette couche de sécurité supplémentaire protège contre les attaques telles que BadUSB qui exploite une vulnérabilité inhérente au firmware des appareils USB. Cette attaque peut déboucher sur l'exécution de commandes ou de code malveillant sur l'ordinateur hôte à l'insu de l'utilisateur.

Certes, le concept du « Bloquer tous les ports » limiterait le risque d'attaques BadUSB, mais vaut-il la peine de sacrifier la productivité pour une pratique si dépassée ? Comme nous l'avons vu ci-dessus, il est possible de maintenir un environnement sécurisé avec l'utilisation d'appareils de stockage portables si les procédures d'achat et de déploiement adéquates permettent d'introduire des clés USB à chiffrement matériel.

Travail à distance conforme et sécurisé

S'agissant des collaborateurs qui travaillent à distance, hors de l'environnement de travail sécurisé d'une entreprise, il est nécessaire de revoir la stratégie et de réexaminer les priorités.

Alors que vous envisagez un plan de sécurité appliqué au travail à distance, vaut-il vraiment la peine de bloquer les ports USB du PC portable du collaborateur si celui-ci va se connecter à Internet en vue d'accéder à un serveur pour charger ou récupérer des documents ? Il peut arriver que le collaborateur en déplacement n'ait d'autre choix que de se connecter à Internet via un point d'accès Wi-Fi non sécurisé ou douteux, ce qui l'expose à une grande variété de dangers qui augmentent le risque d'une divulgation des données. L'interception de données et la surveillance via la substitution, les attaques de l'homme du milieu

(Man-in-the-Middle, MitM) et l'écoute de réseau ne sont que quelques exemples des méthodes toujours plus sophistiquées que les cybercriminels utilisent. Il y a même eu des cas où un VPN a été compromis.

La connexion du réseau d'une entreprise à Internet n'est rien d'autre qu'un terminal et son exposition inhérente en fait un point d'entrée particulièrement vulnérable et ciblé. Si vous y octroyez l'accès à distance, vous vous exposez à d'autres risques, surtout au niveau des données sensibles.

En mettant des clés USB protégées par mot de passe et à chiffrement matériel à la disposition de vos collaborateurs, vous éliminez le risque de vulnérabilités réseau. Mais avant de pouvoir mettre un tel plan en marche, il convient d'analyser attentivement les types de clés USB disponibles et de voir comment elles répondent aux exigences de chaque environnement de travail à distance. La décision ne porte pas simplement sur la capacité de stockage de la clé USB ou sur la nécessité ou non d'enregistrer son numéro de série. Il faut s'intéresser également à la construction physique de l'appareil en lui-même.

Garanties de sécurité : les options concrètes

Ici, le problème principal est de savoir si une clé USB à chiffrement matériel est vraiment inviolable. Le niveau de protection contre de telles interventions figure dans des normes telles que FIPS 140-3 qui permet de définir plusieurs niveaux de résilience de la construction physique d'une clé sans utiliser des méthodes de chiffrement.

La certification connexe FIPS-197 porte uniquement sur les attributs de chiffrement matériel et sur des clés telles que la IronKey Vault Privacy 50 et des SDD externes tels que le Vault Privacy 80 qui sont destinés aux entreprises dont les exigences en matière de sécurité des données n'atteignent pas le niveau militaire. Ces appareils coûtent moins cher, mais ne jouissent pas de la protection contre les manipulations physiques.

Avec la certification FIPS 140-3 de niveau 3 (en cours), les méthodes déployées pour démontrer la résistance aux manipulations des appareils sont de qualité militaire. Kingston fournit ces appareils FIPS140-3 de niveau 3 à des entreprises, des gouvernements et des organismes militaires à travers le monde entier.

L'utilisation d'époxy en interne pour recouvrir tous les circuits de l'appareil est un gage de sécurité, et le fait de coller les composants internes au boîtier crée un autre mur de défense. Toute tentative d'ouverture du boîtier métallique serait extrêmement difficile et entraînerait la rupture des puces et des autres composants internes, ce qui rendrait la clé inutilisable. La présence de cette couche d'époxy dure et opaque rend pratiquement impossible toute manipulation des composants vitaux. Les clés USB telles que les Kingston IronKey D500S et S1000 disposent de cette mesure de sécurité complémentaire.

La protection des clés ne se limite pas aux mesures physiques. Ainsi la Kingston IronKey S1000 porte le concept d'inviolabilité à un tout autre niveau. La puce interne de l'IronKey S1000 est capable de détecter toute manipulation physique et de rendre la clé inutilisable dès que celle-ci est alimentée. L'adoption d'appareils de stockage USB à chiffrement matériel pour accéder aux fichiers sensibles et les transférer est un choix pragmatique qui facilite les opérations à distance et qui garantit de manière efficace la sécurité sur le terrain.

Ne manquez pas d'évaluer le matériel et les fonctionnalités de sécurité des clés USB que vous envisagez d'acheter afin de confirmer qu'elles sont à la hauteur de vos besoins particuliers et de votre contexte d'utilisation. Il convient d'examiner chaque clé USB au cas par cas et de tenir compte des accréditations de confiance au moment de faire votre choix. Quelles que soient vos priorités, Kingston propose un éventail de clés USB à chiffrement matériel et d'options de personnalisation à différents tarifs qui trouveront leur place dans les environnements les plus divers, depuis la conformité générale jusqu'aux spécifications militaires les plus strictes.

Priorité à la sécurité : pas de réseau, pas de problèmes

Aujourd'hui, le bureau n'a plus de frontières et l'essor du télétravail a mis en lumière les problèmes de vulnérabilité de l'accès à distance pour de nombreuses entreprises. C'est la première fois qu'elles doivent relever de tels défis, et elles recherchent des moyens plus sûrs de s'engager dans cette tendance croissante.

Pour répondre à ces besoins dans un large éventail de secteurs, les entreprises ont déjà adopté les appareils de stockage USB à chiffrement matériel en tant que solution sécurisée pour le transfert de données lorsque le transfert via des réseaux n'est pas pratique ou souhaitable pour différentes raisons.

Dans le secteur financier, les organismes de réglementation sollicitent souvent des données pour vérifier la conduite et la conformité de l'entreprise. Le risque d'exposition est bien trop élevé pour envisager de transférer via un réseau des documents sensibles contenant les détails d'investissement, d'échanges boursiers ou d'autres transactions bancaires confidentielles. La solution simple et efficace consiste à remettre ces informations sur une clé USB à chiffrement matériel.

Dans le secteur de la santé, les intervenants utilisent chaque jour des clés USB sécurisées pour transférer des fichiers. Cela simplifie également la vie des médecins ou des spécialistes qui souhaitent analyser des dossiers, les transmettre à des chercheurs ou présenter des cas cliniques à leurs étudiants. Il existe également des besoins plus concrets pour les systèmes exclusifs comme les dispositifs d'imagerie médicale pour lesquels l'accès au réseau est tout simplement indisponible ou peu sûr. L'utilisation de clés USB à chiffrement matériel conformes permet de transférer facilement des fichiers vers un autre bureau.

Bonnes pratiques

✓ **Utiliser des clés USB conformes et sécurisées** et étudier les spécifications afin de commander les clés qui répondent aux besoins de chaque déploiement.

✗ **Ne pas adopter de politiques permettant aux collaborateurs d'apporter leurs propres terminaux (BYOD)** car la perte d'une clé USB non chiffrée est un prix trop élevé à payer en termes de dommages financiers et de réputation entachée.

✓ **Déployer une suite de gestion des terminaux** et utiliser des clés USB à chiffrement matériel offrant des fonctions de listes d'autorisations (ou « listes blanches ») distinctes.

✗ **Ne rien laisser au hasard.** Évaluer comme il se doit les exigences de l'environnement de travail sur site et à distance.

✓ **Former le personnel** aux questions de sécurité. La protection de l'entreprise contre les divulgations de données va dans leur intérêt.

✗ **Ne pas compliquer la sécurité** au point où les collaborateurs commenceraient à chercher des raccourcis, car cela pourrait déboucher sur l'utilisation de solutions informatiques non approuvées. L'application depuis toujours d'une politique générale ne signifie pas que celle-ci soit adaptée à tous les scénarios. Le lieu de travail évolue et le choix de bonnes solutions permettra de développer et de mettre en œuvre de nouvelles stratégies.

Dans ce scénario, la Kingston IronKey Keypad 200 (KP200) occupe une place à part. En tant que clé indépendante du système d'exploitation, elle ne possède pas de volume de lancement pour saisir le mot de passe. Elle est au contraire dotée d'un clavier alphanumérique qui permet de débloquer l'accès à la clé en vue d'une utilisation sur n'importe quelle plateforme. Elle est un peu le couteau suisse des clés USB à chiffrement matériel. Elle est utilisée dans le secteur de la fabrication où elle permet de transférer en toute sécurité des applications créées dans le monde de la recherche et du développement informatique vers des machines contrôlées par des plateformes de technologie opérationnelle (OT). Pour les plateformes mixtes qui utilisent également Linux, la KP200 est une des solutions sécurisées les plus directes disponible.

Les appareils de stockage USB à chiffrement matériel sont amenés à jouer un rôle important pour les autorités judiciaires également. Ils permettent de protéger et de transférer en sécurité les dossiers, les images et autres preuves aux agents sur le terrain, aux enquêteurs et aux équipes de la police scientifique. Kingston offre un avantage complémentaire sous la forme de clés dont le numéro de série interne est imprimé sur le boîtier à côté du code-barre. La distribution et le classement sont ainsi simplifiés et le suivi est amélioré. Il suffit de saisir manuellement un numéro de série ou de lire le code-barre : l'audit et la gestion d'inventaire n'ont jamais été aussi simples. Cette fonctionnalité est proposée en standard sur les clés USB Kingston IronKey D500S, D500SM et S1000B/E. Il est également possible de l'ajouter à d'autres modèles à chiffrement matériel grâce au programme de personnalisation de Kingston.

Sécurité et mobilité du stockage : état des lieux

La protection par mot de passe, le chiffrement matériel, l'inviolabilité, les listes d'autorisations personnalisées, la certification militaire FIPS 140-3 de niveau 3 (en cours) et l'enregistrement par lecture sont des fonctionnalités standard des clés USB de Kingston, ce qui signifie que vous pouvez les déployer sans délai.

Ces défenses robustes garantissent la sécurité de la clé USB et des données qu'elle contient dans son environnement hôte. Les spécifications peuvent être impressionnantes sur papier. Cela étant, la sélection d'un modèle au hasard sans aucune recherche préalable ne sera pas forcément la solution idéale pour une organisation dont les exigences sont plus strictes.

En tant que fabricant indépendant, Kingston propose un large éventail d'options pour répondre aux besoins de ses clients. Grâce à notre programme de personnalisation, vous pouvez accéder à des solutions de pointe conçues pour offrir une expérience transparente aux utilisateurs.

La personnalisation sécurisée va au-delà de la fourniture à une organisation de son propre PID USB pour l'inscription sur liste blanche. Il est également possible de configurer le profil de sécurité de l'application de lancement à l'aide de quinze préférences différentes depuis les coordonnées et les détails de l'entreprise jusqu'aux indices de mot de passe et la définition d'un nombre maximum de tentatives. Au niveau du boîtier, les entreprises peuvent opter pour des solutions de logotypage et différentes couleurs pour certaines clés USB. La commande minimale est de 50 clés USB. L'ensemble de ces fonctionnalités garantissent une intégration sans aucune difficulté pour leur déploiement.

Si vous ne disposez pas encore d'une suite de gestion de terminaux adaptées aux appareils de stockage USB sécurisés, il existe une solutions de gestion conçue pour les organisations qui souhaitent gérer leur parc de clés USB Kingston, avec notamment l'option de réinitialiser les mots de passe à distance.

La technologie USB est partout et son côté pratique lui a permis de survivre à toute une série de technologies prometteuse. Dans de nombreuses applications, la vitesse du stockage USB contribue à sa longévité. Disponibles et toujours sécurisées, les clés USB protégées représentent une solution simple que tout le monde peut apprécier.

Pourquoi se soucier de divulgation de données via le réseau dans les environnements distants ? Les appareils de stockage USB à chiffrement matériel Kingston IronKey placent la solution au creux de votre main.

Pour en savoir plus sur la manière dont Kingston peut vous venir en aide, rendez-vous sur kingston.com/ironkey Si vous avez des questions plus spécifiques, n'hésitez pas à contacter un de nos experts en clés USB chiffrées.

#KingstonIsWithYou #KingstonIronkey