KINGSTON IRONKEY™

Chiffrement matériel ou logiciel

Comprendre les principales différences et déterminer quelle est la meilleure option pour vos besoins.

Dans la lutte permanente pour la sécurité des données, la différence entre le chiffrement matériel et le chiffrement logiciel réside dans l'emplacement où réside la sécurité et dans son degré d'exposition dans la pratique. Dans le cas des clés USB et des SSD, l'emplacement du système de chiffrement détermine le niveau de sécurité des données et leur degré de dépendance vis-à-vis du système environnant.

MATÉRIEL	ET	LOGICIEL
Gestion des clés de chiffrement Les clés de chiffrement sont générées en interne par le matériel et stockées en toute sécurité au sein du lecteur.		**Gestion des clés de chiffrement** Le mot de passe utilisateur est utilisé directement comme clé de chiffrement, et les clés peuvent se trouver dans la mémoire système.
Protection contre les attaques par force brute Conçue pour protéger contre les attaques par force brute en limitant le nombre de tentatives avant que le lecteur ne s'efface automatiquement, empêchant ainsi toute personne d'accéder aux données sensibles en cas de perte ou de vol du lecteur.		**Protection contre les attaques par force brute** Vulnérable aux attaques par force brute, l'ordinateur tente de limiter le nombre de tentatives de déchiffrement, mais les pirates peuvent accéder à sa mémoire et réinitialiser le compteur de tentatives.
Exigences en matière de logiciels ou de pilotes Aucun pilote ni logiciel ne doit être installé sur le système hôte.		**Exigences en matière de logiciels ou de pilotes** L'installation d'un logiciel est requise ; la compatibilité des pilotes et du système d'exploitation peut varier.
Ressources du chiffrement Utilise un processeur cryptographique dédié intégré au lecteur lui-même.		**Ressources du chiffrement** Utilise le processeur et les ressources système de l'ordinateur hôte pour chiffrer et déchiffrer les données.
Dépendance vis-à-vis du système hôte / exposition La sécurité est isolée à l'intérieur de l'appareil et reste efficace même lorsqu'il est connecté à des ordinateurs non fiables ou infectés.		**Dépendance vis-à-vis du système hôte / exposition** Comme la sécurité dépend du système d'exploitation hôte, elle est davantage compromise si l'ordinateur est infecté par un logiciel malveillant.
État du chiffrement Le chiffrement est activé par défaut, et ne peut être ni désactivé ni contourné.		**État du chiffrement** Le chiffrement peut être activé, désactivé ou mal configuré.
Incidence sur les performances Incidence minime sur les performances, car le chiffrement est pris en charge par le processeur matériel.		**Incidence sur les performances** Peut nuire aux performances, car le chiffrement mobilise des ressources du processeur.
Flexibilité Le chiffrement est lié à la clé USB ou au SSD concerné(e).		**Flexibilité** Peut être mis en oeuvre sur pratiquement n'importe quel support de stockage.

Le chiffrement logiciel offre une grande flexibilité, tandis que le chiffrement matériel garantit une sécurité isolée et moins exposée aux risques au niveau du système. En comprenant comment chacune de ces solutions protège les données et contrôle les accès, vous serez en mesure de choisir le niveau de sécurité adapté à vos processus et à votre profil de risque.

www.kingston.com/ironkey