



SECUREDIVES



SDSRDD

SECURE DATA STORAGE - REMOTE DATA DESTRUCTION

Le SDSRDD est un disque dur SSD externe / interne 2.5" auto-chiffrant qui a été spécifiquement développé pour répondre aux besoins sécuritaires des données des gouvernements et des entreprises.

Le SDSRDD protège contre:

- **La menace directe des keyloggers (enregistreurs de frappe) matériels et logiciels** – par l'authentification par jeton et non par mot de passe depuis un PC
- **La perte accidentelle ou le vol** – par la destruction des données à distance depuis un GSM
- **Les techniques de récupération de données** – par la destruction physique des NAND-Flash SIMs
- **L'accès au disque dur par la force** – par un boîtier inviolable activant la destruction physique instantanée
- **La déconnection du PC** – en vérifiant la présence du connecteur SATAII

Un concept global pour la sécurité des données

www.securedrives.co.uk

SecureDrives – Security by design



SECUREDRIVES

Disque dur Interne / Externe

Capacités

- Disque dur SSD de 64Go & 128Go

Dimensions

- 100.5mm x 69.85mm x 9.5mm

Interfaces de Données

- Micro USB 3.0 (Externe)
- SATAII (Interne)

Caractéristiques de Sécurité

- Authentification indépendante du PC
- Authentification à deux facteurs par jeton
- Cryptage matériel complet du disque
- Destruction physique des NAND-Flash SIMs
- Destruction des données à la demande par GSM
- Surveillance du SATAII
- Batterie de secours

Cryptage

- Enchaînement des blocs AES 256-bit
- FIPS 140-2 - niveau 3
- Clé de cryptage avec la fonction effacer / inverser
- Création de clés de cryptage renforcées par instruction de l'utilisateur
- Communication par TPM entre le jeton et le disque dur

Indépendant de toute plate-forme

- Aucun logiciel requis
- Indépendant de l'O/S
- Aucune mise à jour ou correctif

Station de Sauvegarde Sans Intervention (Accessoire)

- Sauvegarde automatique de disque dur à disque dur sous forme cryptée
- Assure l'intégrité de la sécurité des données
- Aucun logiciel ou ordinateur requis

Setting a new bench mark for security of Data-at-Rest

- Authentification à base de jetons – protection contre les keyloggers (enregistreurs de frappe). Permet un mouvement sécurisé des données entre différents lieux avec un jeton à chaque emplacement
- Authentification à deux facteurs par jeton & par code PIN – code PIN jusqu'à 22 caractères
- Essais du code PIN – Le disque dur lance l'autodestruction physique si le nombre d'essais du code PIN prévu à l'origine est dépassé. Cela protège contre les essais innombrables du code PIN pour tenter d'obtenir un accès non autorisé à des données
- Chiffrement complet du disque au niveau matériel par moteur cryptographique FIPS 140-2 de niveau 3, assure des taux de transfert de données à haute vitesse
- Création de chiffrement de clé par un générateur TPM de nombres aléatoires qui, de plus, est renforcé par une instruction de l'utilisateur depuis une interface par jeton. La gamme de lecteurs SDS n'utilise pas la création automatique de clés de cryptage utilisées dans les moteurs cryptographiques en raison de la prévisibilité des clés
- Interfaces de données doubles – options d'installation flexibles permettant un usage interne et externe
- Aucun logiciel Windows ne gère le disque dur en raison de la faiblesse de la sécurité. Aucun correctif du logiciel ou du firmware
- Destruction physique instantanée de stockage NAND-Flash SIMs. Elle empêche l'utilisation des techniques de récupération de données sur le disque dur
- Commande GSM de destruction à distance des données par SMS. L'option 'seuil de signal du réseau GSM' empêche la perte délibérée du signal GSM pour contourner la sécurité
- Vérification de la présence de l'interface SATAII – Elle protège contre la déconnection du disque dur du PC afin de transmettre les données du disque. Le disque s'autodétruit à la perte de l'interface
- Batterie de secours – protection contre les tentatives de contournement de la sécurité par coupure du secteur d'alimentation. L'option de surveillance du niveau de la batterie protège contre toute tentative de contournement de la sécurité suite à un affaiblissement de la batterie
- Boîtier inviolable – lancement de la destruction physique des données à l'ouverture du boîtier par la force