DATALOCKER
DISQUE DUR EXTERNE CHIFFRÉ DL4 FE

Périphériques chiffrés certifiés FIPS 140-2 niveau 3 * avec gestion à distance puissante

UNE SECURITÉ ABSOLUE

Le DL4 FE est un périphérique externe de stockage certifié FIPS 140-2 niveau 3 construit autour d'une puissante architecture matérielle de chiffrement AES 256 bits, qui ajoute plusieurs couches de sécurité avec des politiques automatisées qui changent intelligemment ses fonctions selon son utilisation, sa position géographique ou encore la nature des données stockées. Le DL4 FE est un périphérique compatible TAA qui répond aux exigences de sécurité les plus strictes tout en offrant une grande capacité de stockage (jusqu'à 15,3 To) et un écran tactile facile à utiliser pour la configuration et l'utilisation. Un puissant atout dans la gamme DataLocker en matière de solutions gérées en toute sécurité. Le DL4 FE perpétue une tradition dont nous sommes fiers : fournir des solutions sûres tout simplement. Garantie de 3 ans.

Puissant chiffrement dès son branchement

Tout ce dont vous avez besoin pour chiffrer les données est intégré au DL4 FE validé FIPS 140-2 niveau 3 (en attente *). Pas de pilotes. Aucune configuration. Mais juste un chiffrement matériel AES 256 bits puissant et une interface facile à utiliser, qui est en outre protégée par des politiques de sécurité automatisées.

Ne risquez jamais de perdre vos données

Les politiques de gestion à distance avec SafeConsole® permettent aux administrateurs de verrouiller, d'effacer ou de rendre les périphériques inutilisables à distance, détruisant ainsi toutes les données en cas de tentative de vol. SilentKill ™ donne en outre aux utilisateurs un code spécial pour détruire les données chiffrées du périphérique.

Assurer l'adoption par l'utilisateur grâce à l'écran tactile facile à utiliser

Un écran tactile couleur donne aux utilisateurs un accès rapide aux données sécurisées et leur permet de personnaliser leur périphérique. Les instructions à l'écran rendent l'installation rapide et facile. La disposition aléatoire du clavier avec des lettres, des chiffres et des caractères spéciaux empêche l'analyse de surface des empreintes digitales ainsi que la possibilité de deviner l'emplacement des caractères utilisés.

Gérez et auditez à distance l'ensemble de votre flotte

Tous les périphériques DL4 FE sont gérables à distance avec SafeConsole, ce qui permet aux administrateurs de verrouiller ou d'effacer à distance les périphériques, de réinitialiser les mots de passe, d'afficher les derniers emplacements utilisés et de voir quelles données ont été ajoutées, supprimées ou modifiées sur le périphériquee. Définissez des politiques spécifiques au périphérique ou au groupe pour tous les lecteurs de votre parc.

* Le DL4 FE a été conçu avec une norme FIPS 140-2 niveau 3 et est testé par un laboratoire accrédité NIST. Le produit est en cours de certification et est officiellement répertorié par le NIST. La certification Critères Communs cPP du DL4 FE est également en cours. La liste officielle du NIAP concernant les produits en cours d'évaluation est attendue en mars 2021.

LE DL4 FE

CERTIFICATION FIPS 140-2 NIVEAU 3
Certification True Device niveau 3 avec un contrôleur intégré certifié Critères Communs EAL5+. Fournit un chiffrement matériel permanent. Le moteur de chiffrement en mode XTS AES 256 bits répond à des normes cryptographiques rigoureuses et est plus sûr que les solutions logicielles. Composants internes et boîtier renforcés pour une sécurité physique accrue.

SILENTKILL ™
Permet aux utilisateurs sous la contrainte de détruire le périphérique ou les données stockées sans laisser de traces en entrant un code spécial (configurable par l'administrateur).

PÉRIPHÉRIQUE ENTIÈREMENT GÉRABLE
Utilisez DataLocker SafeConsole pour gérer des périphériques individuels et des groupes de périphériques à l'aide de politiques automatisées.

POLITIQUES ADMINISTRATIVES ET RÉCUPÉRATION DES DONNÉES UTILISATEUR
Les administrateurs peuvent définir des politiques de mot de passe rigoureuses (caractères spéciaux non séquentiels, non répétitifs, caractères minimum). Si les utilisateurs oublient leur mot de passe, les administrateurs peuvent déverrouiller le DL4 FE à l'aide du mot de passe administrateur. Les administrateurs peuvent également récupérer les données de l'utilisateur en se connectant avec le mot de passe administrateur. L'utilisateur sera obligé de réinitialiser son mot de passe lors de sa prochaine utilisation.

PROTECTION CONTRE LES ATTAQUES BRUTE FORCE
Lorsqu'il est utilisé, les administrateurs peuvent configurer le nombre de tentatives de mot de passe échouées nécessaires avant que le dispositif détruise le contenu du disque.

RIEN À INSTALLER
Tout le chiffrement, l'administration et l'authentification sont effectués sur l'unité DL4 FE. Cela signifie que les périphériques en mode autonome ne nécessitent pas de logiciel et sont prêts à fonctionner dès qu'on les branche.

FONCTIONNALITÉS GÉRÉES PAR LE DL4 FE

DÉTONATION DU PÉRIPHÉRIQUE À DISTANCE
Permet aux administrateurs de détruire fonctionnellement le périphérique et ses données à distance pour se protéger contre le vol de données ou de clé de chiffrement (configurable par l'administrateur. Nécessite SafeConsole).

ANTI-MALWARE EMBARQUÉ
Analyse automatiquement les fichiers et met en quarantaine / détruit les applications / fichiers défectueux en fonction des paramètres de sécurité (mise à jour en option. Nécessite SafeConsole).

GÉOLOCALISATION DES DONNÉES
SafeConsole utilise la géolocalisation, les réseaux de confiance et ZoneBuilder pour garantir qu'un périphérique modifie sa position de sécurité en fonction de son emplacement (configurable par l'administrateur. Nécessite SafeConsole).

CAPACITÉS D'AUDIT COMPLETS
Obtenir un enregistrement complet de l'activité des fichiers (y compris les changements de noms sur le périphérique), des tentatives de connexion, des emplacements du periphérique et des stations de travail, de son état et des politiques en vigueur (configurable par l'administrateur. Nécessite SafeConsole).

SPÉCIFICITÉS TECHNIQUES

CAPACITÉS
SSD: 1 To, 2 To, 4 To, 7,6 To, 15,3 To

HDD: 500 Go, 1 To, 2 To

DIMENSIONS
L: 12,3 cm l: 7,7 cm
H: 2,1 cm

L: 4.8" l: 3" H: .82"

POIDS
0,65 lb / 294 grammes et plus

SÉCURITÉ PHYSIQUE
Kensington Security Slot ™

Composants et boîtier renforcés

PROCESSUS CRYPTOGRAPHIQUE
FIPS 140-2 niveau 3 et certification cPP Critères Communs en cours.

Cryptage matériel AES 256 bits XTS intégré.

Intègre un microprocesseur sécurisé certifié Critères Communs EAL 5+.

INTERFACE
USB-C sur le périphérique, compatible avec USB 3.2, USB 2.0 (périphériques 8 To et moins)

(Câbles USB-C vers USB-A et USB-C vers USB-C inclus)

VITESSES DE TRANSFERT
USB-C 3.2: 150 Mo / s en lecture, 100 Mo / s en écriture

USB 2.0: 40 Mo/s en lecture, 20 Mo/s en écriture

NORMES ET CERTIFICATION
Conformité TAA
Certifié IP64
Conforme RoHS
FCC
CE

COMPATIBILITÉ
Microsoft Windows

SYSTÈMES D'EXPLOITATIONS COMPATIBLES
Microsoft Windows, macOS®, Linux® ou toute machine prenant en charge un périphérique de stockage de masse USB.

MODÈLES
DL4-500GB-FE
DL4-1TB-FE
DL4-2TB-FE
DL4-SSD-1TB-FE
DL4-SSD-2TB-FE
DL4-SSD-4TB-FE
DL4-SSD-7.6TB-FE
DL4-SSD-15.3TB-FE

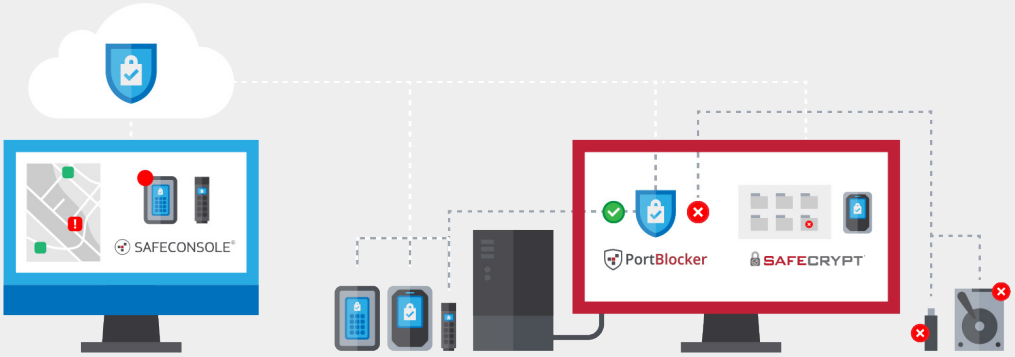
LANGUES DISPONIBLES
Anglais, français, allemand, espagnol

GARANTIE
Garantie limitée de 3 ans

APPROUVÉ PAR

LA SOLUTION COMPLÈTE DATALOCKER

La solution complète DataLocker permet aux employés de disposer d'un stockage USB mobile sécurisé tout en donnant aux administrateurs la possibilité de surveiller, auditer et gérer les périphériques à distance. Du transport de données sensibles à la mise à jour des machines distantes, en passant par la sécurisation des dossiers médicaux, etc., les solutions DataLocker sont un moyen puissant de protéger vos données les plus sensibles.



SafeConsole - Gérez et auditez à distance les périphériques sécurisés

SafeConsole propose un tableau de bord situé sur le Cloud ou sur site permettant aux administrateurs de gérer et d'auditer les périphériques sécurisés, gérer les lecteurs virtuels et verrouiller les ports USB de n'importe où. Si vous êtes un DSI à la recherche d'un moyen de sécuriser des centaines de périphériques déployés, SafeConsole est une excellente option.

- Gérez les clés USB, les disques durs et les périphériques virtuels chiffrés
- Définissez des règles de politique de sécurité telles que les restrictions de types de fichiers et les limites géographiques
- Configurer des politiques de mot de passe ultra-sécurisées
- Définir à distance les rôles d'administrateur et d'utilisateur
- Auditez les périphériques pour voir quels fichiers ont été ajoutés, supprimés ou modifiés

Disques sécurisés DataLocker - Cryptez les données sur un lecteur mobile, et assurez-vous que personne, sauf ceux autorisés, ne peut y accéder

Qu'il s'agisse d'un petit lecteur flash crypté ultra portable comme le Sentry K300 ou d'un lecteur ultra-sécurisé, rapide et de grande capacité comme le DL4 FE, les lecteurs sécurisés DataLocker offrent un chiffrement AES 256 bits puissant et une utilisation aisée. Tout ce dont un utilisateur a besoin pour chiffrer les données est intégré directement dans le périphérique le rendant ainsi autonome, et avec SafeConsole, il est facile de gérer à distance toute une flotte de périphériques DataLocker.

- Jusqu'à la certification FIPS 140-2 niveau 3 avec chiffrement AES 256 bits
- Autodestruction après l'échec des tentatives de connexion pour empêcher les attaques par force brute
- L'antivirus McAfee intégré analyse les fichiers ajoutés (en option)
- L'effacement cryptographique rapide supprime instantanément toutes les données du périphérique
- Entièrement gérable via SafeConsole (selon modèles)

PortBlocker - Pour s'assurer que les utilisateurs n'utilisent que des périphériques USB approuvés pour prévenir l'intrusion de logiciels malveillants

PortBlocker est une fonctionnalité de SafeConsole qui donne aux administrateurs un contrôle total des ports de tous les terminaux. Cela permet d'éviter la perte ou l'intrusion de données, mais aussi de ne mettre en liste blanche que certains périphériques ou de verrouiller complètement les ports USB, empêchant ainsi les utilisateurs d'introduire des virus via des périphériques USB non sécurisés.

- Liste blanche des périphériques de stockage USB par numéro de fournisseur, de produit ou numéro de série
- Appliquer des politiques de sécurité à des groupes de postes de travail ou à des postes de travail individuels
- Réglez les ports USB en mode lecture seule pour désactiver les capacités d'écriture sur les périphériques de stockage
- Bloquer automatiquement les périphériques lorsqu'un poste de travail est utilisé en dehors d'une politique de géolocalisation
- Afficher toutes les modifications apportées aux politiques ou dans les journaux d'audit SafeConsole

SafeCrypt - Chiffrez toutes les données stockées sur un poste de travail pour verrouiller toutes les données sensibles

SafeCrypt est une fonctionnalité de SafeConsole qui offre une puissante technologie de chiffrement pour les données contenues sur les ordinateurs de bureau, les ordinateurs portables et dans le Cloud. Il permet aux utilisateurs de créer un lecteur virtuel sécurisé sur leur poste de travail. Ce dossier fonctionne comme n'importe quel autre dossier, mais cryptera toutes les données qui y sont ajoutées. Cela permet aux utilisateurs de crypter les fichiers locaux, les lecteurs réseaux, les lecteurs externes et même le stockage Cloud mono-utilisateur.

- Certifié FIPS 140-2
- Chiffrement puissant AES 256 bits
- Crypter les données sur une machine locale, stocker des données n'importe où
- Noms de fichiers chiffrés, mode lecture seule, restrictions par types de fichiers et défense contre les attaques par force brute