DATALOCKER

UNIDAD CIFRADA DL4 FE

FIPS 140-2 Nivel 3 (Cert. #4008) Unidad portátil cifrada con potente gestión remota

SEGURO HASTA EL NÚCLEO

El DL4 FE es un dispositivo certificado FIPS 140-2 Nivel 3 (Cert. #3972) construido alrededor de una poderosa arquitectura de hardware criptográfico AES de 256 bits que luego agrega capa tras capa de seguridad con políticas automatizadas que cambian de manera inteligente su postura de seguridad en función de su ubicación, cómo se usa y el tipo de datos que se almacenan en él. El DL4 FE es un dispositivo compatible con TAA que cumple con los requisitos de seguridad más estrictos al tiempo que ofrece una gran capacidad (hasta 15,3 TB) y una pantalla táctil fácil de usar para su configuración y uso. Una poderosa adición a la línea DataLocker de soluciones administradas de forma segura, el DL4 FE continúa nuestra orgullosa tradición de proporcionar soluciones Simply Secure™ , además está respaldado por una garantía limitada de 3 años.

Potente cifrado desde el primer momento

Todo lo que necesita para cifrar datos está integrado en el FIPS 140-2 Nivel 3 y con certificación Common Criteria* K350. Sin controladores. Sin configuración. Solo cifrado AES de 256 bits basado en hardware y blindado en una interfaz fácil de usar, que está protegida por un grupo de políticas de seguridad automatizadas.

Nunca se arriesgue a perder sus datos

Las políticas de gestión remota con SafeConsole® permiten a los administradores bloquear, borrar o inutilizar los dispositivos de forma remota con la detonación remota del dispositivo, destruyendo todos los datos en caso de intento de robo. SilentKill™ ofrece además a los usuarios un código especial para destruir los datos cifrados del dispositivo en caso de emergencia.

Garantice la adopción del usuario con un teclado fácil de usar

Una pantalla táctil a color brinda a los usuarios finales acceso rápido a datos seguros y les permite personalizar su dispositivo. Las instrucciones en pantalla hacen que la configuración sea rápida y sencilla. El diseño aleatorio del teclado con letras, números y caracteres especiales evita el análisis superficial de las huellas dactilares o evita que los atacantes adivinen un patrón de entrada repetido.

Administre y audite de forma remota toda su flota

Todas las unidades DL4 FE se pueden administrar de forma remota con SafeConsole, lo que brinda a los administradores la capacidad de bloquear o borrar unidades de forma remota, restablecer contraseñas, ver las últimas ubicaciones utilizadas y ver qué datos se agregaron, eliminaron o cambiaron en la unidad. Establezca políticas específicas de dispositivo o grupo para todas las unidades de su flota.

*El K350 está en proceso de obtener la certificación Common Criteria cPP. La inclusión oficial como Producto en evaluación por parte de NIAP se espera para 2021.

Get a Custom Demo

datalocker.com | latam@datalocker.com

DISTRIBUIDO POR DATALOCKER INC. ©2023 DATALOCKER, INC. TODOS LOS DERECHOS RESERVADOS. DATALOCKER ES UNA MARCA COMERCIAL REGISTRADA DE DATALOCKER INC. TODAS LAS DEMÁS MARCAS COMERCIALES SON PROPIEDAD DE SUS RESPECTIVOS DUEÑOS.

EL DL4 FE

CERTIFICACIÓN FIPS 140-2 NIVEL 3

Certificación FIPS 140-2 nivel 3 y certificación Common Criteria EAL5+ pendiente. Proporciona cifrado basado en hardware siempre activo. El motor criptográfico dedicado AES de 256 bits en modo XTS cumple con rigurosos estándares criptográficos y es más seguro que las alternativas basadas en software. Interiores endurecidos y recinto para mayor seguridad física.

SILENTKILL™

Permita que los usuarios, bajo coacción, destruyan el dispositivo o los datos almacenados sin dejar rastros ingresando un código especial (configurable por el administrador).

DISPOSITIVO COMPLETAMENTE MANEJABLE

Utilice DataLocker SafeConsole para gestionar dispositivos individuales y grupos mediante políticas automatizadas.

POLÍTICAS DE ADMINISTRACIÓN Y RECUPERACIÓN DE DATOS DE USUARIO

Los administradores pueden establecer políticas de contraseña rigurosas (caracteres especiales no secuenciales, que no se repiten, caracteres mínimos). Si los usuarios olvidan una contraseña, los administradores pueden desbloquear el K350 con la contraseña de administrador. Los administradores también pueden recuperar los datos del usuario iniciando sesión con la contraseña de administrador. El usuario se verá obligado a restablecer su contraseña en su próximo uso.

PROTECCIÓN DE CONTRASEÑA DE FUERZA BRUTA

Los administradores pueden configurar cuántos intentos fallidos de contraseña se necesitan antes de que el dispositivo destruya su carga útil.

NADA QUE INSTALAR

Todo el cifrado, la administración y la autenticación se realizan en la unidad K350. Esto significa que los dispositivos en modo independiente no requieren un agente de software; funcionan nada más sacarlos de la caja.

FUNCIONES GESTIONADAS DEL DL4 FE

DETONACIÓN DE DISPOSITIVO REMOTO

Permite a los administradores destruir funcionalmente el dispositivo y sus datos de forma remota para protegerse contra el robo de datos o claves de cifrado.

ANTIMALWARE A BORDO

Escanea automáticamente archivos y pone en cuarentena/ destruye aplicaciones/ archivos defectuosos según la configuración de la política.

GEOFENCING DE DATOS

SafeConsole utiliza geofencing, redes confiables y ZoneBuilder para garantizar que un dispositivo cambie su postura de seguridad según su ubicación.

CAPACIDADES DE AUDITORÍA INTEGRAL

Tenga un registro completo de la actividad del archivo (incluidos los cambios de nombre en el dispositivo), los intentos de contraseña, las ubicaciones y las máquinas del dispositivo, el estado del dispositivo y las políticas vigentes.

ESPECIFICACIONES TÉCNICAS

CAPACIDADES

SSD: 1 TB, 2 TB, 4 TB, 7,6 TB, 15,3 TB

disco duro: 500 GB, 1 TB, 2 TB

DIMENSIONES

Largo: 12,3 cm Ancho: 7,7 cm Alto: 2,1 cm

Largo: 4.8" Ancho: 3" Alto: .82"

PESO

.65/lbs / 294 gramos y más

SEGURIDAD FÍSICA

Ranura de seguridad Kensington™

Internos endurecidos y recinto

PROCESO CRIPTOGRÁFICO

Dispositivo certificado FIPS 140-2 nivel 3 (Cert. #3972). Certificación Common Criteria cPP pendiente.

Cifrado de hardware AES XTS de 256 bits integrado.

Integra un microprocesador seguro certificado Common Criteria EAL 5+.

INTERFAZ

USB-C en el dispositivo, compatible con USB 3.2, USB 2.0 (unidades de 8 TB y menos)

15,3 TB requiere USB tipo C (15 W+): para usar en hosts con USB A, se requiere un hub USB-A con alimentación y puertos USB-C

(Cables USB-C a USB-A y USB-C a USB-C incluidos)

VELOCIDADES DE TRANSFERENCIA

Tipo	de lectura	de escritura
SSD	USB-C 3.2 -258 MB/s	USB-C 3.2 -244 MB/s
	USB 3.0 -260 MB/s	USB 3.0 -248 MB/s
	USB 2.0 -39 MB/s	USB 2.0 -32 MB/s
HDD	USB-C 3.2 -149 MB/s	USB-C 3.2 -147 MB/s
	USB 3.0 -149 MB/s	USB 3.0 -152 MB/s
	USB 2.0 -39 MB/s	USB 2.0 -31 MB/s

ESTÁNDARES Y CERTIFICACIÓN

FIPS 140-2 NIVEL 3 (Certificado #3972)

Cumplimiento de TAA
Certificado IP64
Conforme RoHS
FCC, CE

COMPATIBILIDAD DE GESTIÓN

Microsoft Windows

COMPATIBILIDAD DEL SISTEMA OPERATIVO

Microsoft Windows,macOS®,Linux® o cualquier máquina que admita un dispositivo de almacenamiento masivo USB.

NÚMEROS DE PIEZA

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

IDIOMAS DEL DISPOSITIVO

inglés, francés, alemán, español

GARANTÍA

garantía limitada de 3 años

CONFIADO POR

DataLocker® Simply Secure

Get a Custom Demo

datalocker.com | latam@datalocker.com

DISTRIBUIDO POR DATALOCKER INC. ©2023 DATALOCKER, INC. TODOS LOS DERECHOS RESERVADOS. DATALOCKER ES UNA MARCA COMERCIAL REGISTRADA DE DATALOCKER INC. TODAS LAS DEMÁS MARCAS COMERCIALES SON PROPIEDAD DE SUS RESPECTIVOS DUEÑOS. 0625