KINGSTON IRONKEY™

소프트웨어 암호화 대 하드웨어 암호화

호스팅

컴퓨터의 리소스를 공유하여 컴퓨터의 다른 프로그램과 데이터를 암호화하며, 내 컴퓨터 정도로만 안전합니다.

암호화된 드라이브에 물리적으로 위치한 **전용 프로세서**를 사용합니다.

비밀번호

데이터를 스크램블하는 암호화 키로 **사용자의 비밀번호**를 사용합니다.

프로세서에는 **임의 숫자 생성기**가 포함되어 있어 사용자의 비밀번호로 잠금을 해제하는 암호화 키를 생성합니다.

업데이트

소프트웨어 업데이트가 **필요할 수 있습니다.**

호스트 시스템에서 **암호화를 오프로드함으로써** 성능을 향상시킵니다.

복호화

소프트웨어 암호화는 쉽게 구할 수 있는 온라인 도구를 이용한 **무차별 암호 대입 공격에 대한 보호 기능이 약하기 때문에** 해킹에 취약합니다.

암호화 하드웨어 내에서 키와 중요한 보안 매개변수를 보호하십시오.

인증

인증은 **호스트 시스템 리소스**를 사용합니다.

인증은 **하드웨어 암호화된 드라이브에서 이루어집니다.**

보호

공격에 취약하며 호스트 시스템 정도로만 안전합니다.

콜드 부트 공격, 악성 코드, 무차별 암호 대입 공격 등 가장 일반적인 공격으로부터 보호합니다.

설치

운영 체제 **호환성은 다를 수 있습니다.**

호스트 PC에 어떤 종류의 소프트웨어도 **설치할 필요가 없습니다.**

유연성

모든 유형의 미디어에 구현할 수 있습니다.

암호화가 **특정 장치에 연결**되어 있으므로 항상 암호화가 켜져 있습니다.

비용

소규모 애플리케이션 환경에서 비용 효율적입니다.

중간 규모 이상의 애플리케이션 환경에서 비용 효율적이며 쉽게 확장할 수 있습니다.

전문가에게 묻기

올바른 솔루션을 계획하려면 프로젝트의 보안 목표를 이해해야 합니다.
Kingston의 전문가가 민감한 데이터를 보호하는 최선의 방법을 안내해 드립니다.

www.kingston.com

#KingstonIsWithYou #KingstonIronKey

©2024 Kingston Technology Far East Corp. (Asia Headquarters) No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.
모든 권리는 본사가 소유합니다. 모든 상표 및 등록 상표는 해당 소유주의 자산입니다