

Zabezpečené a kontrolovatelné USB disky

Existuje mnoho způsobů, jak uchovávat a přenášet data, přičemž USB flash disky jsou díky svým vlastnostem jedním z nejpoužívanějších. Zatímco se rozměry těchto zařízení stále zmenšují, jejich kapacita roste, a tak je na nich možné uchovávat velké množství dat, která mohou být pro organizaci velmi citlivá. Z toho plyne značné riziko při ztrátě nebo krádeži dat. Navíc většina USB disků není v rámci společnosti nijak kontrolována či řízena, což zvyšuje riziko neautorizovaného přístupu, úniku důvěrných informací a porušení bezpečnostních politik.

Klíčové charakteristiky:

- ⇒ **Přístup k datům je chráněn dvou faktorovou autentizací** využívající hesla i biometriku. Lze nastavit maximální počet pokusů pro eliminaci útoků silou.
- ⇒ **Data jsou zabezpečena robustními algoritmy** AES-256, což je ověřeno dle FIPS 140-2.
- ⇒ **Shoda s bezpečnostními předpisy** organizace a standardy ISO 27001, HIPAA, SOX, PCI DSS, EUDPD a další.
- ⇒ **Customisation Programme** Kingston nabízí přizpůsobení flash disků pro potřeby organizace, např. vlastní serial number, nastavení kapacity, User a administrator heslo, různé barvy či logo Vaší společnosti.
- ⇒ **Zabudovaná anti-virová kontrola** Anti-virový engine ESET NOD32, pomáhá chránit USB zařízení tím, že data na USB disku jsou automaticky skenována na přítomnost škodlivých virů. Dostupné na DT Vault Privacy 3.0

Chraňte svá informační aktiva a dobrou pověst společnosti

Jedná se o hardwarově šifrovaný USB flash disk, který využívá šifrování AES 256-bit. Tato přenosná zařízení splňují nejprísnejší kritéria pro IT bezpečnost. Každý den opouští zaměstnanci brány organizace s velkým množstvím potenciálně důvěrných informací a vystavují je tak velkému riziku ztráty, krádeže a zneužití. Díky šifrovaným USB zařízením společnosti Kingston mohou být informace organizace na USB nosičích chráněna silnou šifrou a přístupná pouze oprávněným uživatelům.



Centrální správa

Společnost Kingston nabízí dvě možnosti jak centrálně spravovat USB disky. Pro Data Traveler je k dispozici SaveConsole a pro IronKey flash disky Enterprise Management Server/Service. Pomocí centrální správy máme možnost spravovat přenosné USB disky tak, aby splňovaly požadavky na dodržování předpisů, vzdáleně obnovovat hesla, vynucovat podnikové zásady apod. Centrální správa také umožňuje vzdálené smazání dat ztracených či odcizených zařízení.

Chraňte data silnou šifrou

Kingston šifrované USB disky disponují vestavěným HW šifrováním, generováním klíčů a ukládáním certifikátů! Šifrovací klíče nemohou být exportovány nebo zkopírovány, protože nikdy neopustí USB disk. Volitelně mohou být uloženy i další šifrovací

klíče nebo PKI certifikáty. Data na USB jsou šifrována s využitím nejsilnějších, HW - based šifrovacích algoritmů včetně AES-256 šifrování založené na XTS modu a dostupné jsou i certifikace FIPS 140-2 a Common Criteria. Kingston flash disky chrání 100% uložených data a prosazuje komplexní ochranu pomocí hesla aby se zabránilo neoprávněnému přístupu.

Systémové specifikace Kingston Encrypted USB

Typ	Data Traveler 2000	Data Traveler Vault Privacy 3.0	IronKey S1000	IronKey D300
Podporované OS	<ul style="list-style-type: none"> • MS Windows® Vista/7/8/8.1/10 • Mac OS™ 10.8+ • Linux v. 2.6+ • Chrome OS • Android 	<ul style="list-style-type: none"> • MS Windows® Vista/7/8/8.1/10 • Mac OS™ 10.8+ • Linux v. 2.6+ 	<ul style="list-style-type: none"> • MS Windows® Vista/7/8/8.1/10 • Mac OS™ 10.8+ • Linux v. 2.6+ 	<ul style="list-style-type: none"> • MS Windows® Vista/7/8/8.1/10 • Mac OS™ 10.8+ • Linux v. 2.6+
Kapacita	16, 32 a 64 GB	4, 8, 16, 32, 64 GB	4, 8, 16, 32, 64, 128 GB	4, 8, 16, 32, 64, 128 GB
USB typ	USB 2.0, 3.1	USB 2.0, 3.0	USB 2.0, 3.0	USB 2.0, 3.0
256-Bit AES Encryption	ano	ano	ano	ano
Anti-vir	-	Volitelně*	-	-
Management	-	Volitelně	Volitelně	Volitelně

*pouze pro MS Windows