SECUREDRIVES

SDSDSP
SECURE DATA STORAGE DATA SECURITY PROTOCOL DRIVE

SDSDSP to zewnętrzny/wewnętrzny 2,5-calowy samoszyfrujący dysk SSD, który został opracowany specjalnie do pracy z Przyciskiem DSPS, by sprostać oczekiwaniom zapewnienia bezpieczeństwa danych rządów i organizacji komercyjnych, a nawet je przekroczyć.

Dysk SDSDSP zabezpiecza przed:

- **Bezpośrednim zagrożeniem stwarzanym przez keyloggery sprzętowe i programowe (rejestrujące informacje o klawiszach naciskanych przez użytkownika komputera)** – uwierzytelnianie za pomocą Tokenu a nie hasła wprowadzanego za pośrednictwem komputera
- **Technikami odzyskiwania danych** – poprzez fizyczne zniszczenie układów NAND flash
- **Uzyskaniem dostępu do Dysku przy użyciu siły** – obudowa zabezpieczona przed ingerencją uruchamiająca procedurę natychmiastowego fizycznego zniszczenia
- **Usunięciem z komputera** – monitorowanie obecności wtyczki SATAII
- **Kradzieżą lub usunięciem z określonej lokalizacji** – poprzez monitorowanie obecności przycisku DSPS

Jednolite podejście do bezpieczeństwa danych

Wewnętrzny/ Zewnętrzny Dysk Twardy

SECUREDRIVES

Pojemności
- Dyski SSD 64GB i 128GB

Wymiary
- 100,5mm x 69,85mm x 9,5mm

Interfejsy danych
- Micro USB 3.0 (Zewnętrzny)
- SATAII (Wewnętrzny)

Zabezpieczenia
- Uwierzytelnianie niezależne od komputera
- Uwierzytelnianie dwuskładnikowe z użyciem Tokenu
- Sprzętowe szyfrowanie całego dysku
- Fizyczne zniszczenie układów NAND flash
- Monitorowanie złącza SATAII Wspomaganie bateryjne

Szyfrowanie
- 256-bitowy tryb wiązania bloków zaszyfrowanych AES
- Standard przetwarzania informacji FIPS 140-2 –poziom 3
- Funkcja kasowania/nadpisania klucza szyfrowania
- Generowanie klucza szyfrowania z ciągiem zaburzającym (tzw. solą) wprowadzanym przez użytkownika
- Komunikacja pomiędzy Tokenem a Dyskiem za pomocą modułu TPM
- Komunikacja pomiędzy Dyskiem a przyciskiem DSPS za pomocą modułu TPM

Niezależny od platformy
- Nie wymaga oprogramowania
- Niezależny od systemu operacyjnego
- Nie wymaga aktualizacji ani poprawek

Bezdotykowy zestaw do wykonywania kopii zapasowych (Wyposażenie dodatkowe)
- Automatyczne tworzenie kopii zapasowych z Dysku na Dysk w postaci zaszyfrowanej
- Zapewnia spójność bezpieczeństwa danych
- Nie wymaga oprogramowania ani komputera
- Uwierzytelnianie za pomocą Tokenu – zabezpiecza przed keyloggerami

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

- Uwierzytelnianie dwuskładnikowe z użyciem Tokenui kodu PIN – kod PIN może zawierać do 22 znaków
- Próby wprowadzenia kodu PIN – liczba prób wprowadzenia kodu PIN jest ograniczona zanim dysk zainicjuje procedurę fizycznego samozniszczenia. Funkcja zabezpiecza przed zbyt dużą liczbą prób wprowadzenia kodu PIN w celu uzyskania nieupoważnionego dostępu
- Sprzętowe szyfrowanie całego dysku za pomocą silnika szyfrującego FIPS 140-2 poziom 3 – zapewnia szybki transfer danych
- Generowanie klucza szyfrowania przez generator liczb losowych TPM, do których następnie za pomocą interfejsu Tokenu wprowadzany jest ciąg zaburzający. W linii Dysków SDS nie stosuje się automatycznego generowania kluczy szyfrowania używanego przez silniki kryptograficzne
- Dwa interfejsy danych – elastyczne opcje podłączenia pozwalające na pracę wewnętrzną i zewnętrzną
- Oprogramowanie Windows nie jest stosowane w celu zarządzania Dyskiem z powodu słabości zabezpieczeń. Brak poprawek oprogramowania oraz oprogramowania układowego (firmware)
- Natychmiastowe fizyczne zniszczenie układów NAND flash – zapobiega zastosowaniu technik odzyskania danych z Dysku
- Funkcja Proximity Alert (Alarm oddalenia) – dysk SDSDSP rozpocznie procedurę samozniszczenia w przypadku utraty sygnału wysyłanego przez Przycisk DSPS. Funkcja działa zarówno w przypadku oddalenia dysku od przycisku DSPS, jak w przypadku zakłócenia sygnału (próby blokowania przez źródło zewnętrzne komendy zniszczenia danych)
- Monitorowanie interfejsu SATAII – zabezpiecza przed usunięciem Dysku z komputera umożliwiającym skopiowanie danych z Dysku. W momencie usunięcia interfejsu z Dysku ulega on samozniszczeniu
- Wspomaganie bateryjne – zabezpiecza przed utratą zasilania sieciowego umożliwiającą obejście zabezpieczeń. Opcja monitorowania poziomu naładowania baterii zabezpiecza przed wyczerpaniem baterii umożliwiającym obejście zabezpieczeń
- Obudowa zabezpieczona przed ingerencją – uruchamia procedurę zniszczenia danych przy próbie uzyskania dostępu do obudowy przy użyciu siły