SECUREDRIVES

SDSDSP
SECURE DATA STORAGE DATA SECURITY PROTOCOL DRIVE

Das SDS / SDSR ist eine externe / interne 2.5” selbstverschlüsselte Solid-State Festplatte, welche speziell zum Gebrauch des Data Security Protocol Switch (DSPS) für die Sicherheitsbedürfnisse von Regierungen und kommerziellen Organisationen entwickelt wurde.

Die SDSDSP bietet Sicherheit gegen:

- **Den direkten Angriff von Keylogger Hardware & Software** – via Token Authentifizierung and nicht PC basierter Passwort Authentifizierung
- **Datenwiederherstellung** - mittels physischer Zerstörung der NAND-Flash SIMs
- **Gewaltvoller Zugang zur Festplatte** – mittles Eingriffssicherung für das Gehäuse - Aktivierung sofortiger physischer Zerstörung
- **Entfernung vom PC** – mittels Überwachung der Präsenz einer SATAII Verbindung
- **Diebstahl oder Entfernung von einem bestimmten Ort** - mittels Überwachung der Präsenz des DSPS.

Ein ganzheitlicher Ansatz zur Datensicherung

SECUREDRIVES

Interne / Externe Festplatte

Kapazitäten
- 64GB, 128GB, 256GB & 512GB Solid-State Festplatte

Abmessung
- 100.5mm x 69.85mm x 9.5mm

Anschlüsse
- Micro USB 3.0 (Extern)
- SATAII (Intern)

Sicherheitsfunktionen
- PC-unabhängige Authentifizierung
- 2 Formfaktor Token Authentifizierung
- Vollständige Hardware Verschlüsselung
- Physische Zerstörung der NAND-Flash SIMs
- SATAII Überwachung
- Batterie Backup

Verschlüsselung
- 256-bit AES Cipher-Block Verkettung
- FIPS 140-2 - Level 3
- Verschlüsselung Schlüssellöschung / Flip-Funktion
- Verschlüsselung Schlüsselgenerierung mittels Nutzereingabe
- TPM Token-To-Drive Kommunikation
- TPM Drive-to-DSPS Kommunikation

Plattformunabhängig
- Keine Software benötigt unabhängig vom Betriebssystem
- Keine Upgrades oder Patches

Zero Touch Backup Pod (Zugang)
- Automatisches Drive-to-Drive Backup in verschlüsselter Form
- Sichert unversehrte Datensicherheit
- Keine Software oder Computer benötigt

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

- Token-basierte Authentifizierung – Sicherheit gegen Keylogger.
- 2 Formfaktor Token & PIN-Code Authentifizierung – PIN-Code mit bis zu 22 Stellen.
- PIN-Code Fehleingaben – Limitierte Anzahl von PIN-Code Fehleingaben bevor die Festplatte einen verschlüsselten Keyflip initiiert. Diese Sicherheitsvorkehrung schützt vor der mehrmaligen Eingabe falscher PIN-Codes beim Versuch eines unauthorisierten Datenzugangs.
- Hardware vollständige Festplattenverschlüsselung via FIPS 140-2 Level 3 Kryptographie-Modul – sorgt für Hochgeschwindigkeits-Datenverkehr.
- Verschlüsselungsgenerierung durch TPM mittels Zufallsnummern. Eingeleitet durch Nutzereingabe in der Token-Bedienoberfläche. Die SDS Festplatten generieren keine automatischen Verschlüsselungen aufgrund zu hoher Vorhersagbarkeit.
- Duales Daten-Interface - Flexible Anschlussoptionen erlauben internen oder externen Gebrauch.
- Keine Windows-basierte Software zur Festplattenverwaltung benötigt - aufgrund von Sicherheitsschwächen. Keine Patches benötigt.
- Sofortige, physische Zerstörung des Speicher des NAND-Flash SIMs –verhindert die Anwendung einer Datenwiederherstellung.
- Das Näherungssignal (SP) sichert gegen Signalausfall ab. Sollte eine SDSDSP Festplatte vom DSPS für eine bestimmte Zeit (vom Nutzer festgelegt) kein Signal erhalten, nimmt die Festplatte an, dass es sich um einen unautorisierten Zugriff handelt und zerstört sich selbst.
- SATAII-Interface Überwachung - Sicherheit gegen Festplattenentfernung aus dem PC. Festplatte initiiert verschlüsselten Key-Flip bei der Entfernung des Interface.
- Batterie Backup - Sicherheit vor Stromausfall und Abschaltung der Sicherheitsfunktionen. Überwachungsoption zur ständigen Kontrolle des Batteriefüllstands.
- Eingriffssicheres Gehäuse - initiiert verschlüsselten Key-Flip beim Versuch des gewaltvollen Eindringen in das Gehäuse.