



SECUREDIVES



SDSRDD

SECURE DATA STORAGE - REMOTE DATA DESTRUCTION

Das SDSRDD ist eine externe / interne 2.5" selbstverschlüsselte Solid-State Festplatte, welche speziell für die Sicherheitsbedürfnisse von Regierungen und kommerziellen Organisationen entwickelt wurde.

Die SDSRDD bietet Sicherheit gegen:

- **Den direkten Angriff von Keylogger Hardware & Software** – mittels Token Authentifizierung and nicht PC basierter Passwort Authentifizierung
- **Unbeabsichtigter Verlust oder Diebstahl** – mittels GSM basierter ferngesteuerter Datenvernichtung (SDSR)
- **Datenwiederherstellung** – mittels physischer Zerstörung der NAND-Flash SIMs
- **Gewaltvoller Zugang zur Festplatte** – mittels Eingriffssicherung für das Gehäuse - Aktivierung sofortiger physischer Zerstörung
- **Entfernung vom PC** – mittels Überwachung der Präsenz einer SATAII Verbindung

Ein ganzheitlicher Ansatz zur Datensicherung

www.securedrives.co.uk

SecureDrives – Security by design



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
- Datenvernichtung auf Wunsch mittels GSM
- 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

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.
- GSM gesteuerte Eingabe zur Datenvernichtung via SMS. GSM Serviceausfall-Option verhindert bewussten GSM-Ausfall zur Umgehung der Sicherheitsvorkehrung. (nur beim SDSR-Modell).
- 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.