

Kanguru Defender Elite®

Hardwareverschlüsselter USB-Stick.
Next Generation.

10-fache Sicherheit

Windows / MacOS / Linux

- Hardwareverschlüsselt**
- Passwortgesichert**
- Sicherheitsprüfungen vor
Passworteingabe**
- FIPS-140-2 zertifiziert**
- Optionaler Masterpasswort-Support**
- Physischer Schreibschutz**
- Virtuelles Keyboard**
- Integrierter Virens scanner**
- Tamperproof Epoxy**
- Zentral verwaltbar**



Ungefähr Originalgröße 1 GB bis 16 GB

Datenträger für Geheimniskrämer: Wie viel Sicherheit passt auf einen USB-Stick?

Sicherer als Ali Babas Schatz

Mit Kanguru Defender Elite gehen Ihre Daten nicht verloren, selbst wenn Sie den Stick verlieren: Der Datenträger mit Hardware-Verschlüsselung und automatischer Passwortabfrage gewährleistet den sicheren Transport sehr großer vertraulicher Datenmengen auf kleinstem Raum. Nur wer das Passwort kennt, kann die Daten auf dem USB-Stick sehen.

So sicher war der Transport Ihrer wertvollen Daten noch nie!

Keine Angst vorm ersten Mal ...

Keine Schulung, keine Installation, keine Hürden: Mit Kanguru Defender Elite können Ihre Mitarbeiter sofort loslegen, denn der Datenspeicher funktioniert selbsterklärend. Er verlangt beim ersten Einstecken ein Passwort und gibt sich nicht mit Trivialitäten zufrieden.

Danach die Daten einfach abspeichern, fertig ist der Datentresor!

Für Unternehmen: Kanguru Remote Management Console

Mit der Remote Management Console (KRM) können Sie unternehmensweit alle Kanguru Defender Elite sicher verwalten (auch über das Internet und als Cloud-Lösung).



Next Generation

Weitere Vorteile

- Vertrauliche Daten sind sofort verschlüsselt
- Funktioniert ohne zusätzliche Software an jedem Rechner
- Verschlüsselung kann nicht vergessen oder abgeschaltet werden
- Keine Adminrechte erforderlich
- Keine Adminrechte zum Zurücksetzen erforderlich
- 100% verschlüsselt, keine öffentliche Partition
- Schutz vor Brute-Force-Attacken
- Gemäß den Vorgaben von Telekommunikationsgesetz und Bundesdatenschutzgesetz (BDSG) sowie der Digitalen Steuerprüfung (GDPdU)
- Zu Windows, MAC und Linux kompatibel
- Kurze Zugriffszeit, hohe Lebensdauer
- Speichergrößen 1 GB bis 128 GB verfügbar
- 256-Bit-AES-CBC-Verschlüsselung

Verfügbare Speichergößen

- 1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB, 64 GB und 128 GB

Kompatibilität

- Kompatibel zu Windows Vista, XP, 2000 SP4, Windows 7, Windows Servern, MacOS (OS X 10.5+, Intel based only), Linux (Ubuntu 10+, Red Hat 5+)
- Kompatibel zu portable Apps
- Daten USB-2.0 kompatibel und USB-1.1 abwärtskompatibel
- Einhaltung von Datensicherheitsstandards wie TKG, BDSG, GDPdU

Abmessungen und Gewicht

- Kompakt und robust
- Abmessungen:
bis 16 Gigabyte: 64 x 18,5 x 9 mm, ca. 12 g,
ab 32 Gigabyte: 71 x 27 x 9 mm, ca. 21 g

Sicherheit

- FIPS-140-2 zertifiziert, 100% verschlüsselt, keine öffentliche Partition
- Virtuelles Keyboard zur Passworteingabe vorhanden
- Ausführliche Sicherheitsprüfungen vor Passworteingabe
- Keine Administratorrechte erforderlich
- Physischer Schreibschutz vorhanden
- Integrierter Virens Scanner (nur Windows)
- Tamperproof Epoxy
- Optionaler Masterpasswort-Support

Qualität

- Kurze Zugriffszeit, hohe Lebensdauer
- Transferraten 1 GB - 16 GB:
Lesen 28 - 33 MB/s, Schreiben 11 - 13 MB/s
- Transferraten 32 GB - 128 GB:
Lesen 20 - 33 MB/s, Schreiben 10 - 13 MB/s
- Schreibzyklen: 10.000 Schreibzyklen / Block
- Data Retention: 10 Jahre
- 3 Jahre Garantie
- Shock Resistance: 1000 Gs

Optional

- Managebar über Kanguru Remote Management Console Cloud (KRMC-Cloud)
- Managebar über Kanguru Remote Management Console Lokal (KRMC-Lokal)
- Managebar über Kanguru Local Administrator (KLA)
- Managebar über integrierte Kanguru Endpoint-Protection
- Managebar über Endpoint-Protection

ICT-Security by...

insinova