

# KANGURU Defender Elite™ Product Data Sheet



## 256-bit AES Hardware Encryption

The backbone of the Defender Elite's™ security, hardware encryption provides top tier performance unmatched by software encryption solutions. In addition, on chip password matching means that the encryption can't be circumvented; ensuring your data's security.

## FIPS 140-2 Level 2 Certified

FIPS 140-2, a rigorous federal security accreditation program managed by the (NIST) National Institute of Standards and Technology, sets the standard for encryption modules intended for use in protecting sensitive government information.

## On-board Anti-Virus & Malware

Every Kanguru Defender Elite™ comes with a free one year subscription to BitDefender™ Anti-Virus. Built right into the drive, this feature prevents the Kanguru Defender Elite™ from being used as a vehicle for transporting viruses and malware. The anti-virus can also be used to scan the host computer; in effect becoming a portable anti-virus solution for every PC you work on.



- Designed and assembled in a secure manufacturing environment in the United States of America
- Defender Elite™ requires no drivers or additional software to work on Windows, Mac or Linux platforms.
- No administrative privileges are required to use a Defender Elite™ drive.
- All data stored on the Defender Elite™ is always hardware encrypted and secure.
- Ideal platform for secure hardware encrypted portable applications and 'hardened' web browsing.
- A range of flexible management tools are available to easily configure the security profiles of the drives. Ensuring rapid deployment in your organisation.

## The Kanguru Defender Elite™ answers the most important questions about your portable data security.

Ensuring regulatory compliance is common challenge for IT departments and Security professionals. Lost or stolen devices containing sensitive unencrypted data, makes for headline news. The Kanguru Defender Elite™ being one of the world's most secure and remotely manageable drives will prevent you having to deal with hefty fines from regulatory bodies, and the loss of confidence and goodwill from negative publicity.

The Kanguru Defender Elite™ is one of the most comprehensive mobile data security solutions available on the market today. It combines high level, 256-bit AES hardware encryption, FIPS 140-2 Level 2 Certification, and on-board anti-virus and malware protection. In addition to the tamper resistant design, and various local and remote management options, it makes for the deal for solution for carrying sensitive data.

The Kanguru Defender Elite™ is the ideal solution for heterogeneous environments, as it supports Windows, MacOS and Linux natively. So there is no need to provision the drive for a specific platform.

# KANGURU Defender Elite™ Product Data Sheet



## Tamper Resistant Design

The Kanguru Defender Elite's™ casing is filled with an epoxy compound that is water resistant and prevents physical access to the cryptographic chip. Any attempt to remove the epoxy compound destroys the chip, rendering it unusable and inaccessible.

## Remote Management

Using Kanguru Remote Management Console (KRMC), this optional feature gives you the ability to control your Defender Elite™ flash drives from anywhere in the world. Remotely delete drives that have been lost or stolen, manage passwords (strength, updates and remote resets), and ensure drives are in compliance with set security policies and much more.

## Customization

Kanguru Defender Elite™ secure thumb drives can be special ordered with customised options such as engraved Logos, text, unique IDs, and custom colours including green, red, yellow, blue, silver, grey, and tan.



- Kanguru Solutions provides a market leading turn-key solution for your mobile data requirements.

- Our easy to use, highly secure FIPS certified 140-2 Level 2 devices are remotely manageable. They will work seamlessly with your security mandates, regardless of the type of organisation.

### Compatibility :

- Windows XP / 2003 / Vista / 7  
Mac OS X 10.5+ (Intel based only)  
Linux (Ubuntu 10+, Red Hat 5+, openSUSE 11)
- Compatible with virtualised applications suites such as PortableApps, Ceedo, and VMware ThinApp.
- Observance of many worldwide data security standards such as UKDPA 1988, TKG, BDSG, GDPdU, EU Directive 95/46/EC

### Product Information :

- Transfer Rates - 1G-16G Models  
Read: 28-33MB/s  
Write: 11-13MB/s
- Transfer Rates - 32G-128G Models  
Read: 20-33MB/s  
Write: 10-13MB/s
- Writing cycles: 10,000 writing cycles/block
- USB 2.0 (Backwards compatible with USB 1.1)
- Data Retention - 10 Years
- Anti Shock Protection to 1000 Gs
- 3 Year defective warranty

### Dimensions

- **1G-16G Models** - 64mm x 18.5mm x 9mm
- **32G-64G Models** - 71mm x 27mm x 9mm

### Capacities

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

### Security Features :

- FIPS-140-2 certified, 256-bit AES hardware encryption, no public partition
- Virtual keyboard for password input
- No administrator rights required
- Physical write protection
- Integrated virus scanner
- Tamperproof Epoxy

### Additional Features:

- All stored data is 100% hardware encrypted all the time.
- No client software or drives required
- System protection against brute force password attacks
- Automatic updates of anti-virus signatures
- Highly configurable security policies
- Security Checks as drive mounts secure data partition

### Optional Management Software:

- Kanguru Local Administrator (KLA)
- KRMC Enterprise (LAN)
- KRMC Cloud (Hosted)
- USB Endpoint Protection (software)