

# KANGURU Defender V2™ Product Data Sheet



## 256-bit AES Hardware Encryption

The backbone of the Defender V2™ 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.

## On-board Anti-Virus & Malware

Every Kanguru Defender V2™ comes with a free one year subscription to BitDefender™ Anti-Virus. Built right into the drive, this feature prevents the Kanguru Defender V2™ 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 V2™ requires no drivers or additional software to work on Windows, .
- No administrative privileges are required to use a Defender V2™ drive.
- All data stored on the Defender V2™ 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 V2™ is a cost effective, highly secure hardware encrypted, remotely manageable device for those organisations that do not require FIPS 140-2 validation.**

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 V2™ will prevent you having to deal with hefty fines from regulatory bodies, and the inevitable loss of confidence and goodwill from negative publicity.

The Kanguru Defender V2™ hardware encrypted flash drive offers industry leading security features at an attractive price. Designed for commercial use, it offers top notch security features such as 256-bit hardware encryption, on-board anti-virus and malware protection, with remote central administration management capabilities.

# KANGURU Defender V2™ Product Data Sheet



## Secure Remote Management

Using Kanguru Remote Management Console (KRMC), this optional feature gives you the ability to control your Kanguru Defender V2™ flash drive(s) 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 V2™ secure flash drives can be special ordered with customized 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 197 certified devices can be remotely managed with our 'SaaS' cloud based console, or via local server based central administration software.
- The Kanguru Defender V2™ will work seamlessly with your security mandates, regardless of the type of organisation.

### Compatibility :

- Windows 2000 / Windows XP / 2003 / Vista / 7
- 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: 20-33MB/s  
Write: 10-13MB/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 G
- 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 197 Certified, 256-bit AES hardware encryption, no public partition
- Virtual keyboard for password input
- No administrator rights required
- Physical write protection
- Integrated virus and malware scanner

### 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)