

Kanguru Defender

The Kanguru Defender devices are hardware encrypted, tamper proof USB flash drives. If you want to have absolute peace of mind over your personal and company portable data storage, the Kanguru Defender fits the bill perfectly. These devices have been designed to meet and exceed regulations but in place by the US government. If its good enough for countries governments secure data, it has to be good enough for yours.

Defender Elite

are highly secure, hardware encrypted flash drives meeting government, healthcare and financial industry standards.

- 256-bit AES Hardware Encrypted
- Central/Remote Management Ready
- On Chip Password Matching
- FIPS 140-2 Certified
- HIPAA, SOX and GLB Compliant



Defender v2

are hardware encrypted flash drives offering industry leading security features at an attractive price. Secure, hardware encrypted flash drives designed for commercial use, complete with remote management.

- 256-bit AES Hardware Encrypted
- Central/Remote Management Ready
- On Chip Password Matching
- Real-time Antivirus Scanning



Defender Basic

are hardware encrypted flash drives offering industry leading security features at an attractive price. Designed for consumer use, it offers top notch security features such as 256-bit hardware encryption and onboard anti-virus.

- 256-bit AES Hardware Encryption (100% Encrypted)
- 1 Free Year of On-board Anti-Virus (BitDefender)



Kanguru Remote Management Console

is a web based application that allows administrators to remotely manage selected Kanguru USB flash drives from anywhere in the world. If a device is lost or stolen, an administrator can automatically delete its data as soon as the device is connected to a computer. With the Enterprise Edition, KRMC is fully managed on the customer's server and is ideal for enterprise businesses and government agencies because it is entirely self-managed giving the IT administrator full control.

Data Sheet

Kanguru Remote Management Console (KRMC™) is a web based application that allows administrators to remotely manage selected Kanguru USB flash drives from anywhere in the world. If a device is lost or stolen, an administrator can automatically delete its data as soon as the device is connected to a computer. With the Enterprise Edition, KRMC is fully managed on the customer's server and is ideal for enterprise businesses and government agencies because it is entirely self-managed giving the IT administrator full control.



KRMC is designed to work specifically with the Kanguru Flash Drives. (Currently KanguruDefender, KanguruDefender Pro, Defender Elite and Kanguru Bio AES encrypted models). When an approved Kanguru Flash Drive is connected to a computer with a network or internet connection, an administrator will be able to view detailed information and activity reports about the device. KRMC allows the administrator to monitor where the device is connected and the hostname of the computer. If the administrator has chosen to delete a device's data, the audit function will verify when the remote deletion occurs. An administrator can export audit logs, allowing compatibility with applications such as Excel and databases. User and administrator activities can be logged for various regulatory compliances.

Additional security is available when KRMC is combined with Kanguru USB Device Control, adding endpoint security to control which devices are allowed to access your workstations or network. When used together, they create a turn-key solution with unmatched security at a fraction of the cost of a la carte solutions.

Key Features

- Remote Delete (Deletes all data on the target drive)
- Scheduling of actions (present or future times)
- Auditing at administrator and super administrator level
- Locate via IP address (IP Address / network location)
- Locate via hostname
- Remote policy modifications:
- Password Strength and Length (i.e. 10 characters: 2 upper, 2 numbers, etc)
- Limit Invalid Login Attempts (i.e. 3 retries before drive is wiped)
- Rate at which password should be changed (i.e. every 30, 60, or 90 days)
- Change user password
- Change master password
- User groups (Admin & Super Admin)
- Device import - Support for single or batch import of device(s)
- License import - Support for single or batch import of license(s)
- Advanced Users & Groups management
- IP & Domain Control
- Active Directory Support
- Support for TLS & SSL communication
- Export audit log data to XLS
- Advanced filtering
- Real time graphical reports

Kanguru is a trademark of Kanguru Solutions. Purple Rage logo is a trademark of Purple Rage Limited.