## Kanguru Remote Management for Kanguru Defender Secure USB Drives

### Manage & Customize all Your Secure USB Drives From One Convenient Console

Kanguru Remote Management Console<sup>™</sup> (KRMC)<sup>™</sup> is a powerful security application designed for remotely managing Kanguru Defender USB storage devices. This robust software tool simplifies the administration of an organization's fleet of flash drives and Kanguru Defender HDD/SSD devices. A security officer or administrator can customize, enforce, verify, and audit security policies from a central enterprise server or web interface anywhere in the world. The Console stores no data, which is maintained on the encrypted devices.

A Kanguru drive configured with KRMC will automatically connect to a remote server when plugged in. The drive checks for pending actions, messages and software updates even before the user logs in. KRMC also allows an administrator to quickly locate a particular drive anywhere and make policy updates, delete lost or stolen drives, and more. This powerful tool helps organizations comply with data security regulations, significantly reducing the risk of a sensitive data breach.

#### • Customize Security Settings for All Secure USB Drives Configured With Your Organization:

- Specify Password Complexity & Attempts
- Manage Enable/Disable Settings
- Restrict Online/Offline Access
- Schedule Actions
- Set Master Policies
- Communications Secured by the FIPS 140-2 Validated OpenSSL FIPS Object Module
- Simple and Easy to Use
- Remotely Delete / Wipe Lost or Stolen Drives
- Limit Invalid Login Attempts
- Generate Reports
- and much more...



FOR MORE INFORMATION, PLEASE CONTACT:

Self-Service Password Management for Kanguru

Defender<sup>®</sup> secure flash drives, is a new service of

• KRMC Cloud<sup>™</sup> Edition (Part #: KRMC-CLOUD-xx)

KRMC Enterprise<sup>™</sup> Edition (Part #: KRMC-ENTxx)

KLA<sup>™</sup> Configuration Software (Part #: KDA-BSC-xx)

Kanguru Remote Management Console. Learn More...

KRMC Cloud Pro<sup>™</sup> Edition (Part #: KRMC-CLOUD-PRO-xx)

REMOTE MAN

GEMENT

Kanguru Solutions sales@kanguru.com 1-888-KANGURU www.kanguru.com

Flexible Options

© 2020 All Rights Reserved, Kanguru Solutions™ Kanguru Remote Management Info Sheet August 2020

Page 1 of 2

# Kanguru Remote Management for Kanguru Defender Secure USB Drives



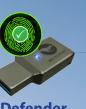
Defender 3000







**Defender Elite**30







Defender HDD300



Defender SSD300



#### KRMC Cloud Edition<sup>™</sup> (Part #: KRMC-CLOUD-xx)

The Kanguru Remote Management Console™ (KRMC™) Cloud Edition is a cloud-based, management service hosted on a secure, enterprise-level, international web hosting platform. Available in a convenient one-year subscription.

#### KRMC Cloud Pro Edition<sup>™</sup> (Part #: KRMC-CLOUD-PRO-xx)

This Cloud-based service is an upgrade to an existing KRMC Cloud subscription and enables an organization to assign multiple administrators under one super-administrator. Assign sub-administrators specific tasks, restrict permissions and privileges depending on the type of access needed.

#### KRMC Enterprise Edition<sup>™</sup> (Part #: KRMC-ENTxx)

Kanguru Remote Management Console™ (KRMC™) Enterprise is a secure, self-hosted system. An add-on module for USB Endpoint Security is also available.

#### KLA<sup>™</sup> Configuration Software (Part #: KDA-BSC-xx)

With Kanguru Local Administrator (KLA), Administrators can configure and customize a wide variety of security and functionality features before and after distributing devices to employees and staff, which will greatly simplify end-user setup and assure all devices are in line with company policy.



## **Key Features:**

#### Customize Security Settings for All Secure USB Drives

- Specify Password Complexity & Attempts
- Manage Enable/Disable Settings
- Restrict Online/Offline Access (IP & Domain Control)
- Schedule Actions (Present or Future Times)
- Set Master Password and Policies
- Quick and Easy Configuration and Deployment
- **Remote Delete** (Deletes all data on the target drive)
- Remote Disable (Keep data but disable the drive)
- Advanced event and Hostname Auditing
- Locate via IP Address
- Manage Device Groups
- Remote Messaging
- Remote Policy Modifications And Actions:
  - Password Strength and Length (i.e. 10 characters: 2 upper, 2 numbers, etc)
  - Password Retries (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
  - Disable device
  - Remote update
  - Remote message
- SAML Integration for Federated Logins with Microsoft<sup>®</sup> ADFS, PingFederate, and Okta (Available in KRMC-Cloud PRO Accounts Only)

FOR MORE INFORMATION, PLEASE CONTACT: Kanguru Solutions sales@kanguru.com 1-888-KANGURU www.kanguru.com