Kanguru Expands Its Remote Management Solutions for Kanguru Defender® AES Hardware Encrypted Data Devices

Millis, MA, USA – October 13, 2016 – Organizations are looking for ways to maintain high level security for sensitive data to stop hackers, prevent cyber theft and the potential for a data breach. But how do organizations secure information in an increasingly mobile workforce, and manage data while conducting global business? When it comes to protecting information, there's simply no safer way than locally-stored data on AES hardware encrypted data storage. **Kanguru Defender® AES Hardware Encrypted USB drives** are the way to go, providing the robust hardware encryption organizations need, and **Kanguru Remote Management Console, (KRMC™)** ensures that all configured encrypted USB drives remain under the organization's security policies.

Kanguru offers two types of convenient remote management solutions:

- **KRMC-Cloud**, Cloud-based; perfect for organizations large or small
- **KRMC-Enterprise**, Self-hosted; for IT staff who wish to manage internally

Both versions enable Administrators to customize and manage their Kanguru Defender secure, hardware encrypted devices from one convenient console anywhere in the world:

- Disable/wipe lost or stolen drives
- Roll out new security policy updates
- Manage passwords
- Audit, report and much more

Kanguru is proud to announce impressive enhancements to both remote management options, with the release of **KRMC Enterprise 7**, and **KRMC-Cloud-2**. Both provide even greater intelligence features like:

- **Self-Service Password Management**
- **Automatic Global Provisioning**
- **Streamlined License Management**

Self-Service Password Management (SSPM) is a great new feature enabling users to reset their own password through a secure reset if they forget the login to their secure device. Administrators can allow/disallow the option for certain drives.

With **Automatic Global Provisioning**, Managers can create consistent, global security policies up-front, provisioning parameters for which all secure drives will follow automatically. By doing so, managers ensure consistent deployment of drives company-wide, securing all present and future drives to that company policy.

With more **streamlined license management**, administrators can easily control, add or remove licenses and on-board anti-virus subscriptions quickly and easily.

Consider how **Kanguru's fully-integrated remote management** could work for your organization; call Kanguru at **(1) 888-KANGURU**.

*Kanguru is the global leader in providing the very best in FIPS 140-2 Certified, TAA compliant, hardware encrypted secure USB drives, as well as fully-integrated remote management security applications. For more information, visit **kanguru.com**.*

FOR MORE INFORMATION, PLEASE CONTACT:

Don Wright, Marketing Manager
Kanguru Solutions
marketing@kanguru.com
(1) 508.376.4245