Kanguru Offers A Unique Hybrid Approach To Data Security With KRMC™

Millis, MA, USA – October 23, 2018 – Ask any security-conscious organization what their biggest challenge is, and most will likely admit securing data in today's digital world. Ensuring that private data is safe should be a top priority for every organization given present online threats, but with many options to choose from, how do organizations know what the best choice is for keeping data secure? Data is the most important asset for any organization as it drives business and is a key part of its infrastructure. Hackers know this, and may stop at nothing to break in and steal valuable data. As a result, government is cracking down with tougher regulations on organizations to protect the private data of its customers and citizens, with some steep fines for violating compliance. On top of that, citizens are being empowered with many rights to file lawsuits if one feels their private records have been compromised in any way. Organizations need to consider not only what's convenient for their business, but what is the best security option to protect both the data of their customers, and to protect themselves.

Cloud Storage VS Local Storage

Over the last decade or so, organizations have been making tremendous shifts to store their data in the cloud. There are advantages; convenience being the most prominent, with other benefits like backing up data to an offsite location in case of disaster. Popular cloud storage services, however, have seen some major data breaches over the last few years, prompting many organizations to wonder just how safe they really are. The convenience of having access to your data from any internet connection anywhere in the world could also unfortunately be its security downfall, as others might find ways to gain unauthorized access to it as well.

Local storage like encrypted USB flash drives, hard drives and solid state drives on the other hand, cannot be compromised when closely guarded in the hands of the owner under password protection. In contrast to cloud storage, its usage is solely limited to the person holding the device under password protection- disconnected from the internet and the rest of the world. The very nature of its restrictive intent makes it the securest way to protect data, but it can be challenging if an organization needs to use that closely-guarded information in a variety of locations around the globe. The danger is reversed if an untrustworthy individual with a USB device suddenly chooses to unlawfully use a device to remove private information from an organization. Without being able to monitor such data loss, the damage control could be enormous unless there was a way to remotely wipe and destroy the stolen drive. The logic behind **Kanguru Defender's encrypted USB drives with fully-integrated Remote Management** is precisely for administrators to have the ability to remotely manage their encrypted drives.

A Hybrid Approach to Secure Data Storage

Kanguru offers a unique hybrid solution which combines the outstanding security of local secure USB storage, with the convenience of management through the cloud, **KRMC-Cloud™, (Kanguru Remote Management Console).** Enterprise and security-conscious organizations around the world have been using KRMC for many years to successfully protect their data. By storing sensitive information on local USB encryption, and using the

cloud to manage their drives around the globe, IT Administrators can monitor their data assets without compromise.

This fully-integrated, hybrid approach offers a robust, secure, two-fold process of checks and balances for organizations, putting tremendous safeguards in place for Administrators and sensitive data that is unparalleled by cloud storage. Since data is stored solely on the local secure USB drive under strong AES 256-Bit hardware encryption and not in a cloud interface, it cannot be compromised through internet connections. Simply put, Administrators manage the security perimeters of the drives while the users manage the sensitive data separately. The authorized user holds the information confidential and is able to use the drive under the permissions provided by the organization. The Administrator or Sub-Administrators use the convenience of the cloud to remotely manage the security, monitor and grant permissions, ensure the integrity of the secure USB drive's security and report on any concerning activity.

The IT Administrator can configure and deploy a fleet of **Kanguru Defender® hardware encrypted USB drives** beforehand with specific permissions or restrictions accordingly, manage password guidelines, set a master password, and more, based on the security policies of the organization. Then with KRMC Cloud, remotely manage the location, permissions, rules and security of the drives anywhere in the world.

Encrypted USB drives can be closely monitored, with specific permissions or restrictions. If a user forgets a password, Administrators can reset it remotely. If a user loses a drive, or it is stolen, the admin can remotely disable, delete or even wipe the drive. Administrators can provide reports, schedule actions, and even send a message to drives, making quick policy changes.

This safeguard system can even be ideal for use in different departments, with sub-administrators managing silos of information to end-users of specific sectors, and one super-administrator managing the big picture.

KRMC and Kanguru Defender hardware encrypted USB drives is a robust, hybrid system that helps organizations maintain full security of their data with the freedom to use it wherever it is needed around the world, while keeping an administrative check on the location of the data at all times.

If you would like to learn more about Kanguru Remote Management Console (KRMC), Kanguru Defender Secure USB Drives, and how Kanguru's fully-integrated system could work for your organization, please call Kanguru at **(1) 800-KANGURU**, or visit **www.kanguru.com**.

*Kanguru is a global leader in manufacturing highly-certified data storage products, providing the very best in FIPS 140-2 and Common Criteria Certified, hardware encrypted, secure USB drives fully-integrated remote management security applications and Endpoint Security. Kanguru also manufactures duplication equipment for cloning hard drives, SSDs, blu-ray, DVD discs and more. For more information on Kanguru, please visit **kanguru.com**.*

FOR MORE INFORMATION, PLEASE CONTACT:
Don Wright, Marketing Manager
Kanguru Solutions
marketing@kanguru.com
(1) 508.376.4245