Kanguru's Secure Firmware USB Devices Help Protect Organizations From Malware Threats

Millis, MA, USA – November 13, 2018 – Many organizations are turning to secure firmware USB devices by Kanguru that focus on helping protect from malicious third-party firmware-based attacks. With RSA-2048, digitally-signed secure firmware, the non-encrypted **Kanguru FlashTrust**™ USB flash drive offers consumers and organizations the same level of trusted secure firmware protection typically reserved for encrypted, high-end flash drives to non-encrypted USB device users.

In addition, the **Kanguru UltraLock™** Hard Drive, Solid State Drive, **Kanguru Slim DVD Burner**, and **Slim Blu-ray Burner** offer similar protected firmware to protect an organization's infrastructure from malware.

The purpose of secure firmware USB devices is to help security-conscious organizations defend against potential, malicious firmware-based attacks (also known as "**badUSB**") with on-board, RSA-2048, digitally-signed secure firmware. If a Kanguru secure firmware USB device is tampered with by a third-party hacker in any way, the firmware on the USB device is designed to shut down the drive, protecting networks from a nasty threat of malware.

Protecting Organizations From Potential Threats With Trusted USB Devices

Over the last several years, organizations have become aware through research, of a potential malware threat regarding third-party hackers who might tamper with USB devices like webcams, keyboards, thumb drives, or a computer mouse to compromise an organization's infrastructure. This threat, called "badUSB," could pose a serious hazard if networks are not protected or prepared. Industries such as defense, energy, utilities, healthcare, financial and government could be particularly vulnerable to such type of attack.

However, short of blockading the use of USB altogether, as some organizations have done to their own detriment, USB remains the most convenient, reliable, offline way for organizations to quickly transfer information back and forth in a business environment. A far better solution for organizations is to enforce stronger USB security policies that would better control the offensive with a secure line of defense, restricting company-wide use solely to trusted USB devices on a network, and blocking out any USB devices that should not be allowed. By permitting use exclusively to trusted USB devices, the network is protected.

A network is vulnerable if any employee, staff member, customer or client is allowed to plug in just about any type of USB device off the street. One hypothetical situation is that hackers could simply leave an unsuspecting, cheap thumb drive on the ground near the entrance to a facility they wish to infiltrate. A curious employee could pick it up and inadvertently plug it into their computer attached to an unprotected network to see what is on it. If a savvy hacker has compromised the firmware of the drive with malicious malware, the entire infrastructure could be maligned.

Restricting use to Kanguru trusted secure firmware drives ensures that such a scenario would be a non-event, as the USB device would simply shut down in the event of a firmware-based, malware attack.

Ideal USB Data Solutions With Endpoint Security

Organizations using Endpoint Security can enforce strong security policies by restricting the network exclusively to trusted USB drives. Many have turned to Kanguru's well-trusted, secure firmware USB devices which are ideal for use with Endpoint Security applications:

- **Kanguru FlashTrust™ Secure Firmware USB Flash Drive**
- **Kanguru UltraLock™ Hard Drive (HDD)**
- **Kanguru UltraLock™ Solid State Drive (SSD)**
- **Kanguru QS Slim DVDRW DVD Burner**
- **Kanguru QS Slim BDRW Blu-ray Burner**

A Perfect USB Solution For Non-Encrypted Environments

Where encrypted USB devices are an ideal solution for high-security organizations, some organizations may not have the need for such high-end data encryption for general data use. However, secure firmware offers a different kind of protection when it comes to protecting a network and infrastructure. Kanguru's RSA-2048, digitally-signed secure firmware USB and protected firmware USB products help organizations secure their infrastructure with the same trusted secure firmware protection used in encrypted USB flash drives, which has been tested by the FIPS accredited laboratory.

If you would like to learn more about Kanguru secure firmware USB drives and protected firmware drives, 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. 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