Press Release

KANGURU™
Secure. Anytime. Anywhere.

Kanguru Secure Firmware Helps Protect Sensitive Environments From Malware Attacks

For Immediate Release: March 26, 2024

SECURE FIRMWARE
KANGURU FLASHTRUST™
USB3.0 Secure Firmware
KANGURU DEFENDER ELITE300™
USB 3.0 AES Hardware Encryption
KANGURU DEFENDER 3000™
USB 3.0 AES Hardware Encryption
FIPS 140-2 Certified
CE FC RoHS
www.kanguru.com
SECURE FIRMWARE PRODUCTS BY
KANGURU™
Secure. Anytime. Anywhere.

Millis, MA, USA – March 26, 2024 – Certain companies, industries and organizations may be at higher risk of malicious attacks due to the inherent value of the information they are responsible for, which may require special safeguards to help protect their networks, integrity, confidentiality and infrastructure. Aggressors who covet the information may attempt to target these organizations specifically with espionage using malware, phishing, ransomware, or other exploits to gain access to internal and globally connected computer systems, networks and devices. These attacks can then be used to disrupt, damage or profit from the misappropriated information.

In these more sensitive environments, secure firmware becomes a critical component to protect infrastructure and prevent the hijacking of devices by tampering with the firmware that could then be used to deliver malware. The importance of secure firmware has increased with the proliferation of connected devices within an organization and worldwide. Secure Firmware creates a trustworthy foundation for all software running on a device and helps protect against a wide range of threats, including data breaches and sophisticated cyberattacks.

To help prevent such attacks, Kanguru offers digitally signed secure firmware devices that consistently validate the drive's identity with a digital signature, confirming that the drive is what it is expected to be. Organizations using an endpoint environment with strict security policies can rely on secure firmware devices like Kanguru’s to protect their infrastructure from vulnerabilities by integrating security measures directly into the firmware.

How Kanguru Secure Firmware Devices Work

Since secure firmware integrates security measures directly into a device's firmware, the firmware on Kanguru devices is protected. Digitally signed secure firmware self-checks to ensure the identity of the drive and confirms that the firmware has not been altered. This authenticates every time the device boots, proving it only uses software trusted by the Original Equipment Manufacturer (OEM). Kanguru’s digitally signed secure firmware drives instill high trust in organizations, helping them reduce the risk of cyberattacks and maintain the integrity, confidentiality, and availability of their devices and their data.

Organizations that may be at particular risk of malware attacks or firmware tampering are:

- Government and Defense
- Financial Services/Banking/Insurance
- Healthcare/Hospitals/Medical Research
- Energy and Utilities
- Telecommunications
- Automotive
- Consumer Electronics
- Industrial/Manufacturing
- Aerospace
- Retail
- Education / Research

Kanguru: Secure Products You Can Trust

Kanguru has an array of digitally signed secure firmware devices, from AES 256-Bit, hardware-encrypted portable devices and internal self-encrypting drives to regular flash drives, solid-state drives, NVMe SSDs, and BD/DVD burners. Organizations can safely implement these solutions into their infrastructure without worrying about potential firmware attacks.

In addition, Kanguru offers TAA Compliant products as a trusted supply chain partner, where all final assembly is done in a secure, U.S.-based facility. This makes Kanguru products ideal for government procurement contracts, and ensures trustworthy operation of the devices in today's increasingly interconnected and threat-prone environments.

Secure Firmware devices append an additional layer of trust to endpoint security environments and security policies:

- **Defender Hardware Encrypted Secure Drives**
- **Defender Opal Self-Encrypting, Internal Secure Solid-State Drives**
- **Kanguru Ultralock External SSD, HDD, NVMe Drives**
- **Kanguru Standard Flash Drives**
- **Kanguru DVD and Blu-ray Burners**

Learn More: What is Secure Firmware on Kanguru Drives?

If you have questions about any of these products, you may contact the sales team at **1-(508)-376-4245** or email at sales@kanguru.com.

Kanguru is a global leader providing best-in-class, secure storage solutions to help organizations and individuals protect and secure their data. Kanguru has been providing easy-to-use, secure IT products, duplication and data storage for over 30 years. For more information on Kanguru, please visit www.kanguru.com.

Where To Buy

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