

Kanguru Introduces New FIPS 140-2, USB 3.0 Secure Flash Drive with Physical Write Protect Switch



Millis, MA. - September 21, 2015 – Kanguru has released its newest FIPS 140-2 Certified secure flash drive with SuperSpeed USB 3.0 technology, making it one of the fastest high-performance, hardware encrypted USB flash drives available on the market today. The new [Kanguru Defender Elite300™](#) combines superior FIPS 140-2 Certification with convenient high-speed USB 3.0 data transfer rates and a unique physical write protect switch for high-security environments including government, health care and financial segments, and will exceed even the most demanding security regulations.

This new FIPS secure flash drive with physical write protect switch provides blazing read speeds of up to 260MB per second, and write speeds of up to 120MB per second, delivering exceptional data transfer rates for today's mobile organizations.

Advanced Features for the Kanguru Defender Elite300:

- SuperSpeed USB3.0
- FIPS 140-2 Certified
- AES 256-Bit Hardware Encryption (XTS Mode)
- Physical Write protect Switch
- On-Board Anti-Virus
- Remotely Manageable
- RSA-2048 Digitally-Signed Secure Firmware Resistant to "badUSB"
- Rugged Alloy Housing
- Customization Available
- TAA Compliant

Along with FIPS 140-2 Certified AES 256-Bit hardware encryption and on-board anti-virus, the physical write protect switch provides additional security protection, with the ability to quickly and easily toggle between read/write, or read-only protection if so desired. This can be useful in certain conditions where the secure USB flash drive may be used on a computer system that could contain viruses, since read-only mode makes it virtually impossible for a virus to infect the flash drive.

Remote Management for Kanguru Defender® Secure USB Drives

Remote Management for secure USB drives is a powerful optional feature sold separately, and is a great way for security teams to manage a fleet of secure USB thumb drives and secure external hard drives for their organization. Administrators can configure Kanguru Defender secure USB pen drives and distribute to staff for confidential organizational use. Then using the [Kanguru Remote Management Console](#) (KRMC), restrictions can be made for where the pen drives can or cannot be used with online or offline permissions, password changes can be scheduled and strengthened, users can be notified, and custom security policies can be automatically implemented and enforced. Additionally, if a secure thumb drive was ever lost or stolen, it could even be deleted or disabled remotely anywhere in the world.

Kanguru is a global leader in providing exceptional-quality FIPS 140-2 and Common Criteria Certified, TAA Compliant hardware encrypted secure USB flash drives, external hard drives, solid state drives, thumb drives, jump drives, pen drives, portable USB storage devices and more. In addition, Kanguru offers remote management applications, duplication equipment, accessories and more. Kanguru is committed to offering the highest level secure products and services to enterprise, government, healthcare, organizations and consumers worldwide with easy-to-use, certified IT products and data storage. For more information on Kanguru, please visit kanguru.com.

FOR MORE INFORMATION, PLEASE CONTACT:

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