

SecureWave
Sanctuary[®]
Certified Device



Kanguru – KanguruMicro Drive AES

SecureWave Certification Number: CERT-SDC-06-06-00013

The KanguruMicro Drive AES is the only USB Flash Drive that meets federal requirements for insuring the confidentiality of sensitive data and information accessed by portable flash drives! This high speed, high quality USB2.0 Flash Drive is FIPS 140-2 certified for Government use! The KanguruMicro Drive is ultra secure, utilizing 256 bit AES Encryption to protect data stored on the drive. Plug the KanguruMicro Drive AES into any available USB or USB 2.0 port and begin using it! Store and transport your work files in a safe, secure fashion. The KanguruMicro Drive AES comes bundled with an encryption program called Kanguru Lock, which creates a virtual disk protected with 256 Bit AES encryption on your KanguruMicro Drive. The encrypted disk is password protected and will automatically mount when the correct password is entered. All data stored in the encrypted disk is encrypted and decrypted on the fly, with minimal performance loss. When the KanguruMicro Drive is removed from the system the encrypted disk is automatically locked, and cannot be read until the correct password is supplied.

Major features include:

- > 256-bit AES Encryption – FIPS 140-2 Certified
- > Meets federal requirements for computer storage security!
- > High speed USB 2.0 – Backwards compatible with USB1.1
- > Can be uniquely serialized
- > Capabilities up to 8 GB
- > Uses Top Grade Flash Memory



For more information, please visit:

<http://www.kanguru.com/aesmicrodrive.html>

Sanctuary Device Control

Sanctuary[®] Device Control extends the enforcement of enterprise policies to I/O devices. Users can access only explicitly authorized devices, such as KanguruMicro Drive AES USB device. Sanctuary Device Control manages this by applying an Access Control List (ACL) to each device type. To grant access, the administrator need only associate user or group objects to the authorized device.

Sanctuary[®] Device Control supports several directory platforms, including Microsoft Active Directory and Novell eDirectory. Sanctuary has also been ported to Windows Embedded platforms in addition to the Windows Server and Desktop versions. Sanctuary Device Control:

- > Ensures USB Security through management of any removable media,
- > Provides complete control and management over all I/O devices through any port including USB, Firewire, WIFI, Bluetooth, etc.,
- > Prevents data theft and data leakage via removable media,
- > Prevents malware introduction via removable media,
- > Audits I/O Device usage,
- > Detects and blocks Keyloggers,
- > Encrypts removable media that may not provide their own hardware based encryption,
- > Enables Regulatory Compliance with enforceable policies that include extensive logging and auditing,
- > Provides centralized logging and retention of an exact copy of all data written to authorized devices using SecureWave's proprietary Shadowing[™] technology.

For more information, please visit: www.securewave.com/sdc

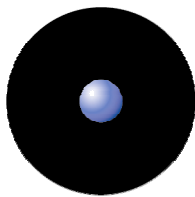
Request a free 30 days fully enabled evaluation at www.securewave.com/evaluation

Manage the use of KanguruMicro Drive AES with Sanctuary Device Control and enforce your secure removable media policies solution with FIPS 140-2 certification while protecting against data loss, unauthorized removable media usage and hardware keyloggers!

SECUREWAVE SANCTUARY CERTIFIED DEVICE

SecureWave Sanctuary® provides policy-based control over endpoint applications and devices. Using an automated whitelist approach, Sanctuary enables the development, enforcement, and auditing for application and device use in order to maintain IT security, reduce the effort and cost associated with supporting endpoint technologies, and ensure compliance with regulations. Sanctuary links application and device policies to Microsoft® Active Directory™ or Novell® eDirectory® user and user group information, dramatically simplifying the management of endpoint application and device resources. More than 1,300 enterprises worldwide in the financial, government, military, manufacturing and healthcare sectors utilize Sanctuary. SecureWave, named a Red Herring Top 100 Innovator, is headquartered in Luxembourg and services its global customer base via offices in the U.K., Washington D.C. and Research Triangle Park, N.C., as well as a network of reseller and service provider partners worldwide.

More information about SecureWave Technology Partners: www.securewave.com/alliances/
Locate a SecureWave Sanctuary Official Channel Partner: www.securewave.com/channel/



SecureWave

Safeguarding Tomorrow

North America

Sales

13755 Sunrise Valley Drive
Suite 203
Herndon, VA 20171
United States of America

+1 (703) 713-3960 Phone
+1 (703) 793-7007 Fax

Marketing and Corporate Development

Research Triangle Park
2530 Meridian Parkway
Suite 200
Durham, NC 27713
United States of America

+1 (919) 806-4410 Phone
+1 (919) 806-4770 Fax

www.securewave.com
info@securewave.com

United Kingdom

Midsummer Court
314 Midsummer Boulevard
Milton Keynes MK9 2UB
United Kingdom

+44 (0) 1908 357897 Phone
+44 (0) 1908 357600 Fax

Continental Europe

Atrium Business Park
23- ZA Bourmicht
L- 8070 Bertrange
Grand Duchy of Luxembourg

+352 265364-11 Phone
+352 265364-12 Fax

SECUREWAVE SANCTUARY CERTIFIED DEVICE