

SecureWave  
**Sanctuary**<sup>®</sup>  
Certified Device



## Kingston Technology DataTraveler Secure – Privacy Edition – SecureWave Certification Number: CERT-SDC-06-11-0019

Secure, waterproof and fast, DataTraveler<sup>®</sup> Secure – Privacy Edition (DTSP) offers unique protection to safeguard critical data even if the drive is lost or stolen. It's an enterprise-grade USB Flash drive with 256-bit AES (Advanced Encryption Standard) hardware-based, on-the-fly encryption – 100 percent of the stored data is secure, with no public area to expose files. Its strong password rules and lock-down control protect against brute force attacks.

These advanced security features make DTSP ideal for corporations and service organizations that require employees to transport large digital files consisting of confidential documents. DTSP helps companies avoid the financial and legal consequences of lost or stolen data.



Major features include:

- > Full privacy – 100% of stored data is protected by 256-bit AES hardware-based encryption (no public area on the device compared with DataTraveler Secure device)
- > Secure – drive locks down after 10 intrusion attempts
- > Strong password protection – password is user-set with minimum characteristics
- > Waterproof – protected against water damage

For more information, please visit: [www.kingston.com/flash/privacyUSB.asp](http://www.kingston.com/flash/privacyUSB.asp)

## Sanctuary Device Control

Sanctuary<sup>®</sup> Device Control extends the enforcement of enterprise policies to I/O devices. Users can access only explicitly authorized devices, such as Kingston's DataTraveler Secure Privacy Edition USB drive. 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<sup>®</sup> 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, (Sanctuary Device Control encryption features are not to be used with DataTravelerSecure devices)
- > 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<sup>™</sup> technology.

For more information, please visit: [www.securewave.com/sdc](http://www.securewave.com/sdc)

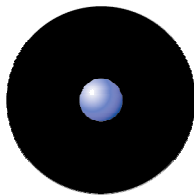
Request a free 30 days fully enabled evaluation at [www.securewave.com/evaluation](http://www.securewave.com/evaluation)

**When used together, DataTravelerSecure – Privacy Edition and Sanctuary Device Control enable organizations to strongly enforce device usage policies while ensuring high data confidentiality with removable media AES 256 hardware based encryption. Gone is the risk of losing sensitive information on an unsecured or unauthorized device.**

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/](http://www.securewave.com/alliances/)  
Locate a SecureWave Sanctuary Official Channel Partner: [www.securewave.com/channel/](http://www.securewave.com/channel/)



## SecureWave

Safeguarding Tomorrow

### North America

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

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

### 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

[www.securewave.com](http://www.securewave.com)  
[info@securewave.com](mailto:info@securewave.com)