

The popularity of portable computing and removable storage devices have put strain on enterprise data security. Julian Ashbourn looks at encryption products that raise safety

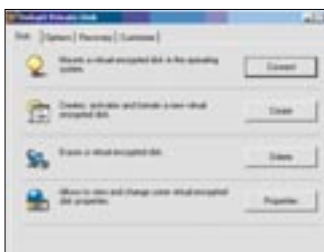
When conventional access controls are defeated, data on portable storage devices becomes open to inspection. It is similarly worrying with respect to data stored within databases and networks, and the possibility of such data being stolen or otherwise misused.

In order to respond to these chal-

lenges, various data encryption methodologies have been developed, from simple, file-based symmetrical encryption to comprehensive PKIs and a host of ideas and techniques in between. In parallel, encryption algorithms have also developed to offer greater "strength" as regards to the possibility of them being defeated.

When contemplating deploying such a system, whether on a stand-alone computing device or across a network, among the more important parameters to consider will be ease of use, enterprise key management and recovery, should the authorised user find themselves locked out of their own data.

## Dekart Private Disk



**Supplier** Dekart

**Price** £24.40

**Contact** [www.dekart.com](http://www.dekart.com)

Dekart's approach to encryption is innovative, albeit using accepted standards where appropriate. The company offers a range of useful security-related products and utilities, within which Private Disk plays an important part.

It is a small footprint program to provide data encryption in a seamless manner, as many other products claim, but offers further useful functionality.

The concept of a disk firewall is particularly interesting, providing application-level access control, whereby a whitelist of trusted applications is maintained within

the encrypted disk area. If an application not on this list tries to access any protected file, it will simply be blocked.

This not only guards against malware but, with judicious use, may also prevent file copying or other manipulation of data – a simple and effective idea. Also interesting is the ability to run Private Disk directly from portable media, allowing access by authorised users even when using a different PC – again, a simple and effective approach that many users will find useful.

As for the encryption itself, AES 256-bit algorithms are used, and SHA 512 hash algorithms are used for key generation. Thus, the core functionality is based upon established standards.

Private Disk is flexible in its application and can work with a broad range of portable media, including USB sticks, flash memory cards and indeed, almost anything that can store data. This flexibility allows the user to conceive and configure the type of protection best suited to their own working situation in a straightforward and intuitive manner.

This is an important factor. If

configuration and operation are too complex, users are likely to become frustrated and fail to make full use of the benefits offered. Private Disk is logical, intuitive and easy to use by anyone.

For those inclined towards paranoia, Dekart also claims that, due to its origins, Private Disk contains no "back doors" or government-induced escrow keys to allow decryption of your data by the authorities.

For developers, a Private Disk SDK is available. All in all, this is an interesting, effective product that offers very good value for those looking for encryption in an easily managed manner.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★☆
Value for money	★★★★★
<b>OVERALL RATING</b>	<b>★★★★★</b>
<b>For</b>	Ease of use, innovative features, robust encryption.
<b>Against</b>	A comprehensive manual would be nice.
<b>Verdict</b>	An interesting and capable product at an attractive price.

Contact details:



**Dekart**  
Alba Iulia 75  
Chisinau  
2071  
Moldova  
Tel: +373 22 245580  
Fax: +373 22 225742



An interesting and capable product at an attractive price.

Julian Ashbourn