



Private Disk version 2.09, from Dekart

Data within the corporate network enjoys the benefits of a wealth of protection measures, but as soon as it goes off-site it loses this security umbrella. Mobile workers - IT support staff, sales people, etc. - all need to have information at their fingertips, but in most cases they will have it stored on a device such as a laptop or notebook, which can all too easily be lost or stolen.

One of the simplest solutions is to encrypt critical data, so that if it does fall into the wrong hands, at least it won't be of any use. Dekart specialises in this field and its Private Disk utility delivers an impressive range of security features. It uses the concept of virtual encrypted disks, which contain all the data you want to secure.

Private Disk implements strong encryption as it employs AES 256-bit algorithms and uses a unique password provided by the user, which is employed to encrypt and decrypt the data.

Private Disk has a small footprint, so it won't have any major impact on general system performance. It offers a simple user interface making it easy to create new virtual disks or mount and unmount existing drives. In reality, the virtual disk is actually just a file, so it can be located on any existing partition.

To create a virtual disk you simply

decide on an image file name and location, choose a size in MB and leave Private Disk to create it. The file can be a local or networked location, and there are plenty of other options as the file can be made read-only, allowing selected data to be protected from modification. The virtual disk can be mounted automatically at start-up and you can have it hidden on creation if required. Removable media support is a smart feature as all required Private Disk components will be copied across to the selected device, allowing the virtual disk to be used on any other system.

Once you've made your choices you need to provide a password - and this will determine how strong the encryption will be. Note that you must not lose this password; if you do it's probable that your encrypted data will be irrevocably lost as well.

Private Disk does provide a brute force password recovery tool, but if you chose a password using a mixture of alphanumeric and non-alphanumeric characters, plus upper and lower case, you could be in for a long wait - years, in fact. Usefully, prior to creating the image, Private Disk will advise you on the strength of your selected password, allowing you the option to change it.

We created a 1GB virtual disk on a dual Xeon test client and with a password score of thirty-seven per cent

the process took a shade over three minutes. Once finished, you can format the drive ready for use, and on mounting it appears in Windows Explorer as a normal local drive, which can also be made available as a shared network resource.

We also created a 50MB virtual drive on a USB flash disk, and after installing Private Disk to the removable media we were able to transport it and mount the disk on another system. The Private Disk firewall is another useful tool, as it blocks applications from accessing the virtual disk unless they have been declared first. Private Disk makes light work of protecting data if you have to leave your desk, as hot-key combinations can be used to disconnect and reconnect specific virtual disks.

Private Disk is an extremely simple solution to a perennial problem. It delivers strong data encryption and application access controls to selected data, is particularly easy to use, and is also very affordable. **NC**

Product: Private Disk v2.09

Supplier: Dekart

Tel: +373 22 245580

Email: sales@dekart.com

Web site: www.dekart.com

Price: Single user licence £24.00 GBP, 2-5 licenses £22.50 per licence excluding VAT