

DatAshur encrypted drives: protect your data but be sure to back it up too

The iStorage DataAshur USB flash drive is a neat way to encrypt your data. Lost USB storage devices are a common cause of data theft anxiety: in most cases the finder won't care about your data but you can never be certain.



The DatAshur is simple to operate but highly secure, presuming it meets the advertised specification. All data written to the drive is automatically encrypted with 256-bit AES CBC (Advanced Encryption Standard with Cipher Block Chaining) and meets the US FIPS 140-2 standard. The encryption is transparent to the operating system, since decryption is built into the device and enabled by entering a PIN of 7 to 15 digits.

Note that a snag with this arrangement is that if your PC is compromised a hacker might be able to read the data while the drive is connected. If you are really anxious you could get round this by working offline, or perhaps using Microsoft's clever Windows to Go (WTG) technology where you boot from a USB device and work in isolation from the host operating system. Unfortunately DatAshur does not support WTG (as far as I know) but there are alternatives which do, or you could boot into WTG and then insert your DatAshur device.

Normally you enter the PIN to unlock the drive before connecting it to a PC or Mac. This does mean that the DatAshur requires a battery, and a rechargeable battery is built in. However if the battery is exhausted you can still get your data back by recharging the device (it charges whenever it is plugged into a USB port).

OK, so what happens if a bad guy gets your device and enters PINs repeatedly until the right one is found? This will not work (unless you chose 1234567 or something like that) since after 10 failed tries the device resets, deleting all your data.

You should avoid, then, the following scenario. You give your DatAshur drive to your friend to show it off. "I've just updated all my expenses on this and there is no way you'll be able to get at the data". Friend fiddles for a bit. "Indeed, and neither can you".

Here then is the security dilemma: the better the security, the more you risk losing access to your own data.

The DatAshur does have an additional feature which mitigates the risk of forgetting the PIN. You can actually set two PINs, a user PIN and an admin PIN. The admin PIN could be retained by a security department at work, or kept in some other safe place. This still will not rescue you though if more than 10 attempts are made.

What this means is that data you cannot afford to lose must be backed up as well as encrypted, with all the complexity that backup involves (must be off-site and secure).

Still, if you understand the implications this is a neat solution, provided you do not need to use those pesky mobile devices that lack USB ports.

The product tested has a capacity from 4GB to 32GB and has a smart, strong metal case. The plastic personal edition runs from 8GB to 32GB and is less robust. An SSD model offers from 30GB to 240GB, and larger desktop units support SSD or hard drive storage from 64GB to 6TB, with USB 3.0 for fast data transfer.

Prices range from around £30 inc VAT for an 8GB Personal USB stick, to £39.50 for the 4GB professional device reviewed here, up to £470 for the monster 6TB drive or £691 for a USB 3.0 external SSD (prices taken from a popular online retailer). The cost strikes me as reasonable for well-made secure storage.

More information on DatAshur is [here](#).