



The fine folks at Origin Storage shipped us a review copy of their Data Locker security hard drive solution. This was one of the most talked about devices shown in this field at this year's Infosecurity Europe event held in London, so we decided to test it and feature it in this post-summer, "back to work" issue of (IN)SECURE Magazine.

Data Locker is a hard drive solution with a unique security twist - it features an LCD display used for PIN based authentication and, besides the hard drive, the enclosure contains a hardware based encryption chip.

This device is available in a couple of sizes and sports different types of encryption. The Pro version works with 128 bit AES encryption, while the Enterprise one uses the tougher-to-break 256 bit AES cipher. Depending on your storage needs, each of the flavors is available in 160GB, 320GB and 500GB versions. For the purpose of this article, I have been playing with the 160 GB Enterprise version.

Look and feel

I was pleasantly surprised when I saw that the Data Locker box doesn't contain a big, puffed

up enclosure- its size is approximately 0.5 inches wider, longer and thicker than my iPhone. It's weight is about the double of an iPhone. As you can see from the accompanying product photos we shot, besides the rather impressive size and weight characteristics, the device is an aesthetically pleasing addition for your work environment.

It comes with a USB cable (mini to standard), with an additional Y cable that could be of use for some computers and USB hubs for extra energy. From my tests on different Mac and PC computers, one USB connection was just enough. For those that don't have luck with one or even two USB cables, there is a DC input slot that supports power adaptors. The last feature on the back side is something that is often disregarded with this type of smaller hard drives – the on/off switch. Including this switch is a good move - I dislike pulling USB



cables out of the computer or devices just to shut them down and plugging them back in to switch them on.

Now we are coming to the most interesting part - the LCD touch screen display. When the disc is powered on, the display starts-up and provides a simple menu. The touch screen works well and the keys are quite large so there shouldn't be any usage problems.

Just a little heads-up to users of iPhone and similar devices - you will need to press this LCD display a little bit harder than you are used to.

Setting up Data Locker

Data Locker's main task is providing a secure storage space for your personal files. It demands a secret PIN code and until you successfully authenticate, the disk can't mount

and therefore doesn't "exist". The device comes preloaded with a default password of 000000. Accessing the menu is easy - just authenticate by punching in the default PIN and quickly tap the setup button. After you do that, you will get access to a couple of options:

Change PIN: When you're thinking of PINs, you are probably thinking of a sequence of 4 numeric characters. In Data Locker's case, the PIN must be at least 6 characters long and can take up to 18 numbers.

Change encrypt key: The drive contains data encrypted with your PIN code and the current encryption key. Changing the encryption key should be done when changing the owner of the disk, if you think formatting and changing the PIN is not enough. Modifying the encryption key instantly renders the current data on drive absolutely unusable.



Further customization

There is an additional menu option located on the bottom of the the setup screen. Hitting "other" will give you three possibilities you can toggle on and off:

Key tone: Every successful tap on the display generates a rather generic computer audio sound that confirms that something was done. It is turned on by default and if the sound becomes annoying, you can turn it off.



Self-destruct: If turned on, this option will destroy the data on the disk after nine unsuccessful login attempts. The anti brute force mechanism cannot be fooled into restarting after a couple of failed tries. The device remembers the attempts and after the ninth the decryption key is deleted and you can say bye-bye to your data. If this happens, you will need to reconnect the device to your computer and login with the password you previously used.

Random key-pad: Although it is hard to see what is happening on the LCD display if you don't have it right in front of you, this option is another security mechanism that works against those who would want to snoop on you. Every time you open the PIN code input form, the number position will be scrambled, so it will almost impossible to approximately position your PIN code. Also, this type of character scrambling would work pretty good against someone analyzing fingerprint marks to try to "hack" your device.

Data Locker usage

The entire process after the login can be described in just a couple of words - it acts just like a normal hard drive. After authorizing to the device, the drive mounts and you can use it for whatever purposes you had in mind.

When you want to remove the disk, or just lock it so no one can use it, you need to hit the appropriate button on the LCD display and voila! The only consideration you should have is to always use "safely remove device" or "unmount" functions before locking the device. This is a healthy way of taking care of your data.

Data Locker is a multi-platform device - as it doesn't use any type of application for the cryptographic processes and it can be connected to any operating system. There is just one thing I need to mention and it is related to Mac OS X users. The Data Locker drive is NTFS formatted, so you won't be able to use it out of the box on your Mac computers. This is, of course, nothing specific to Data Locker, so you will have one of the usual two solutions: re-format the disk with FAT32 (or HFS+ if you will just share data on Macs) or install the NTFS-3G driver that provides NTFS read/write capabilities on non-Windows systems.



This being a hard drive review, you are probably expecting some benchmarking data. I recently read an article in an upscale IT magazine, in which it was said that the file transfer speeds for this disk are slower when compared to other robust hard drives. I guess they forgot that this is a security solution with a crypto operation, so it is expected to be slower than the regular drive.

FYI - transferring 1 GB file from my 2.4 GHZ Intel Core Duo iMac to Data Locker (NTFS) took 88 seconds, while the same procedure to another disk (XFS+) took 37 seconds. The difference is substantial, but like I said, from my point of view this is not a big issue.

By the way - what to do if your device gets into some kind of a rumble? When the LCD display ends up being smashed and if the hard drive is intact you should get yourself a new Data Locker enclosure and access to your data will be spot-on.

Final thoughts

Over the past couple of years I have evaluated a number of secure data storage devices, but this was the first time I crossed paths with a hard drive empowered by a PIN authorization mechanism. Built on an exceptional idea, the unit works very well and it is a tough and robust solution for keeping your data and backups highly secure.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.