iStorage cloudAshur Review - Cloud Nine

With cloud security data breaches on the rise - and many of them caused by human error - it's natural to be worried about how exactly the data you store on cloud services is being protected. While most cloud security protocols are pretty strong, there's still a good chance that hackers, accidents, or good old-fashioned human error could put paid to the idea that your files are secure and not open to being exploited when you store them on Google Drive, Dropbox, or similar services.

That's where iStorage comes in. The London-based tech firm has made a name for itself with encrypted storage devices like the DataShur USB drive and the DiskAshur encrypted hard drive (there's also a solid state version available). iStorage's newest product, the cloudAshur, bills itself as an "encrypted cloud module" that adds a layer of security to files you've got stored in the cloud. Will this be the solution you need for peace of mind?

The first thing to note about the cloudAshur is that it's a very sturdy bit of kit indeed. Taking it out of the box, you'd be forgiven for thinking it's simply a USB storage drive, were it not for the cool spy-like keypad on the front (that's for entering your PIN when you want to access or encrypt your files). The construction on this thing is hard-wearing; it's not easy to break or accidentally damage, which is ideal given its function.

So, what exactly does the cloudAshur do? In essence, it's a data encryption tool. Using the free companion program (available for Windows and Mac, naturally), the cloudAshur will encrypt files you have on the cloud and make it so that you need to go through a process of authentication every time you want to access them. There are five factors of authentication available, one of which is the device itself and four of which are information only you can know.

That's one of the main things you need to know about the cloudAshur: it's definitely for security-heads. Although we'd still recommend picking one up if you're someone who only dabbles in cloud storage, you likely won't get the kind of usage out of it that

a serious user would. In other words, you're only likely to get the most out of the cloudAshur if you've got a lot of very sensitive or important data tied up in cloud services like OneDrive or Dropbox.

That said, if you are that person, you'd be hard-pressed to find a better and more secure device than this. The cloudAshur comes complete with full military-grade hardware encryption and supports USB 3.0 for lightning-fast data transfer. The microprocessor inside this device is probably about as much security as anybody needs against hackers; a lot of sensitive data breaches could have been avoided if major businesses picked up cloudAshurs for moving and sharing important data.

It's also important to note that the cloudAshur isn't for the forgetful. If you manage to enter your user PIN incorrectly 10 consecutive times (unlikely, but possible), it'll be deleted and your drive can only be accessed using the admin PIN. Enter that 10 times incorrectly and it's gone forever, meaning you'll need to completely reset the drive. This is a good feature for deterring hackers, but it does mean you could accidentally lock yourself out. Maybe nobody's fault but yours, but still something to keep in mind.

The cloudAshur module also comes with a suite of software. KeyWriter allows you to share data with authorised users by copying encryption keys; it only works if you let it, and it only shares data with users you deem appropriate. You'll never see the encryption key anywhere but where you've sent it, and the software itself can't actually see the key or the decrypted data. It's a very smart system, and one that iStorage should be thoroughly proud of.

There's also the Remote Management program. The user interfaces on these pieces of software are impressively clean and uncluttered despite the amount of detail they present; you won't find this difficult to use even if you're not a tech-head. Remote Management gives you full control over all the data you're sharing, allows you to restrict file types, and lets you remotely shut down recipient users if you suspect there's something wrong.

The best thing about cloudAshur is that it's a tool with as much or as little customisation over your security as you want. If you want to delve deeply into security protocols and technical details, you can. If you're someone who just wants to protect their data on the cloud and doesn't feel it's necessary to understand the full ins and outs, then the intuitive software and plug-and-play nature of the cloudAshur makes that side of things easy, too.

It's not difficult to recommend cloudAshur to anyone who has files tied up in the cloud. If you don't use Google Drive (or other cloud services) much, or if you're not worried about your file security, then this probably isn't the product for you. However, for the niche it's trying to serve, it's hard to think of a better alternative for cloud security than cloudAshur. Hopefully, we'll see this tool picked up and used as industry-standard, because we don't know what we'd do without it now we've got it.+