Product Review

Seagate Personal Cloud Home Media Storage

Your Everything….but, can you trust your everything to The Cloud?

Images: Michelle Massarik / ML1Media 2016

By Bonnie Blatt

The CLOUD has reached critical mass(es). It's everywhere and commonplace. Your mom (or grandmother) even backs up data to *The CLOUD*. No longer the domain of tech-savvy, ordinary users are uploading their valuable information to spectrum of online Cloud services such as Google drive, Apple iCloud, Dropbox, Box, Microsoft OneDrive, and so on. Generally speaking, these services are secure, although there is always a chance that your data could be lost or compromised. While there are many *free* options, users may find the storage limits of free cloud services to be too small to be useful. Google's free storage choice is capped at 15GB. Microsoft and Apple's free option limits out at a paltry 5GB. Of course, much larger storage limits are available...at a price. At Google, for instance, 1TB will cost you $9.99 per month, and 10TB costs a whopping $99.99 per month. This becomes the persuasion point of a Personal Cloud. A Personal Cloud is just that--personal. It mimics cloud storage of the big names, but you buy, own and operate the storage hardware. It's located wherever you choose and allows access (retrieval and storage of files) both locally as a network attached drive(NAS), and remotely via the Internet (like a Cloud Service). There are several excellent choices from familiar names: LaCie, Western Digital, D-Link, and Seagate, all offering multi-terabytes of storage for less than $300.00. We chose to evaluate a Seagate 4 terabyte model, the STCR4000101 single bay/drive model. Ultimately, our choice was not based on storage capacity or price, but features -- most specifically, ***SECURITY***.

Given the choice, we're opting NOT to pay a monthly fee (ransom) for remote, secured storage. The personal cloud hardware offers us our own secured server right in our (secure) office that can be accessed from almost anywhere that internet (or mobile data) access is available. Seagate bills their Cloud storage, the Seagate Personal Cloud Home Media Storage as, "Your Everything". Available sizes are 3, 4, 5, 6 and 8TB in both single bay/drive and (more expensive) double-bay models (allowing for automatic data mirroring/redundancy).

What's in the box: Not much. The Seagate Personal Cloud is a compact rectangle, not much bigger than a Kindle Fire. It comes with a 'wall-wart' type of power adapter, a single Ethernet cable, and a (mostly useless) QuickStart guide. The premise is that it's plug-and-play, but as our tests revealed, plug-and-play does not equal **SECURITY**.

Setup was indeed easy. Connect the power cord, connect the data cable to your local switch (or router) Ethernet port and plug the device into a power outlet (this essentially *is* the QuickStart guide). Once it connects to your network, you simply map a drive letter

Tech Specs

Seagate Personal Cloud Home Media Storage Device

4TB NAS STCR4000101

Manufacturer: Seagate

Retail Price: $179.00 US

System Requirements:

-PC: Windows Vista, 7 or 8; Mac: OS X 10.7 or later; Internet Explorer, Firefox, Chrome or Safari browser

-Router with an available Ethernet port (Wi-Fi router required for wireless file access and backup)

-Internet connection for activation and Internet file sharing

Remote Access App Requirements:

-iOS, Android Smartphone and Tablet (Android 4, iOS 6.0 or later); Desktop PC or Mac OS

Interfaces: Ethernet:1, USB (2.0 & 3.0):2

Number of Physical Drives: 1

Hard Drive Capacity: 4TB

Color: Black

Power source: External block 110v AC

Dimensions & weight: Height:1.89 inches, Width:9.25 inches; Weight: 40.48 ounces; Material: Plastic

Warranty: Parts: 2 years limited; Labor: 2 years limited

(Continued on page 23)

(Continued from page 21)

with your Windows PC or Mac, and upload your files to your personal cloud, much like any Network Attached Storage (NAS). Indeed, the Seagate installation process was one of the deciding factors in selecting a Personal Cloud box. Several of the other vendors in the Personal Cloud marketplace have been noted for very cumbersome, complex, and occasionally impossible setup routines. After unpacking the device, we had the Seagate STCR4000101set up and accessible (locally) in under ten minutes. Seagate's online documentation (a full manual PDF can be downloaded) is complete and thorough and Seagate offers a slew of downloads to compliment management of the personal cloud devices as well as a group of videos that provide in-depth tutorials on configuration, operation and technical troubleshooting of the hardware.

Easy setup and access to local network storage is a plus, but this is a CLOUD device and our interest is not simply Cloud storage/ access, but rather, *SECURE Cloud* storage/ access (see next section). The device is self-configuring, taking approximately 7 minutes after which the status light, inconveniently located on top of the device, will change from flashing red to a steady on white.

Uploading your files to the personal cloud is straightforward. Seagate creates a PUBLIC and PRIVATE folder for data. Anything placed in the public folder can be accessed remotely by yourself or anyone you give permission to access by yourself or anyone *you give permission to access it*. The PRIVATE folder is a secure are kept locally on the device and NOT accessible from any remote devices. Within the PUBLIC folder is an internet shortcut which will launch the Seagate Personal Cloud Setup Wizard. When selected, you are required to agree to the terms and conditions after which the device will check for firmware updates. Our device found several updates and required nearly 20 minutes to complete and restart.

The web interface for the device displays a selection of icons including Device Manager, Download Manager, Backup Manager, App Manager, Sdrive (encryption app) and Seagate Media (app for iOS and Android to view media and stream it to connected devices).

SECURE Cloud? The *average* user (that Seagate expects to own/operate this device), will probably leave the device with its default settings intact. They won't disable any of the extra services Seagate sets up by default (unnecessarily consuming processing power of the box) and most likely wont dig deep enough to rectify the marginal default security settings that are crucial if placing this device on the internet for Cloud access. By default, the device is running an SSH server and uses uPnP for port forwarding.

Many internet-connected devices expose UPnP to the outside world, which potentially allows attackers on the outside to open ports in your local router/network. It is standard security professionals protocol to DISABLE UPnP in your outside connected devices (routers, etc). While uPnP can be an exploited security weakness, it happens to be a requirement for many of the remote access features for this device. Disabling it enhances the devices security, but detracts from it's usability. The second security issue, the SSH server, is a bit more ominous. The SSH server is operating on a non-standard port and there does not appear to be any way to disable the SSH server feature. Seagate technical support was made aware of the concerns and is considering a patch.

Conclusion: While the PC (personal computer) may be 'dead', the *PC* (Personal CLOUD) market is taking off. The Seagate Personal Cloud Server (and many of the other devices in this market segment) is an impressive device. It's a more cost-effective solution than paying for an online cloud-storage service, but the price of ownership/operation should include the indeterminable cost of securing an internet-connected device such as this.

We are (and suggest to others) to take a staged, wait-and-see approach to putting the Personal Cloud into production. We placed on an isolated network, loaded it with some 'interesting' (but harmless) named files and folders an put it on an internet connection.

For the next several weeks, we will be rigorously reviewing the logs on the internet-connected router and the Seagate Personal Cloud device looking for irregularities (port probes, etc) . A follow-up report is already in the works and will appear later this summer.