



DOES YOUR BUSINESS AVOID THE PUBLIC CLOUD DUE TO PRIVACY CONCERNS? NO PROBLEM.

How ioSafe Can Help

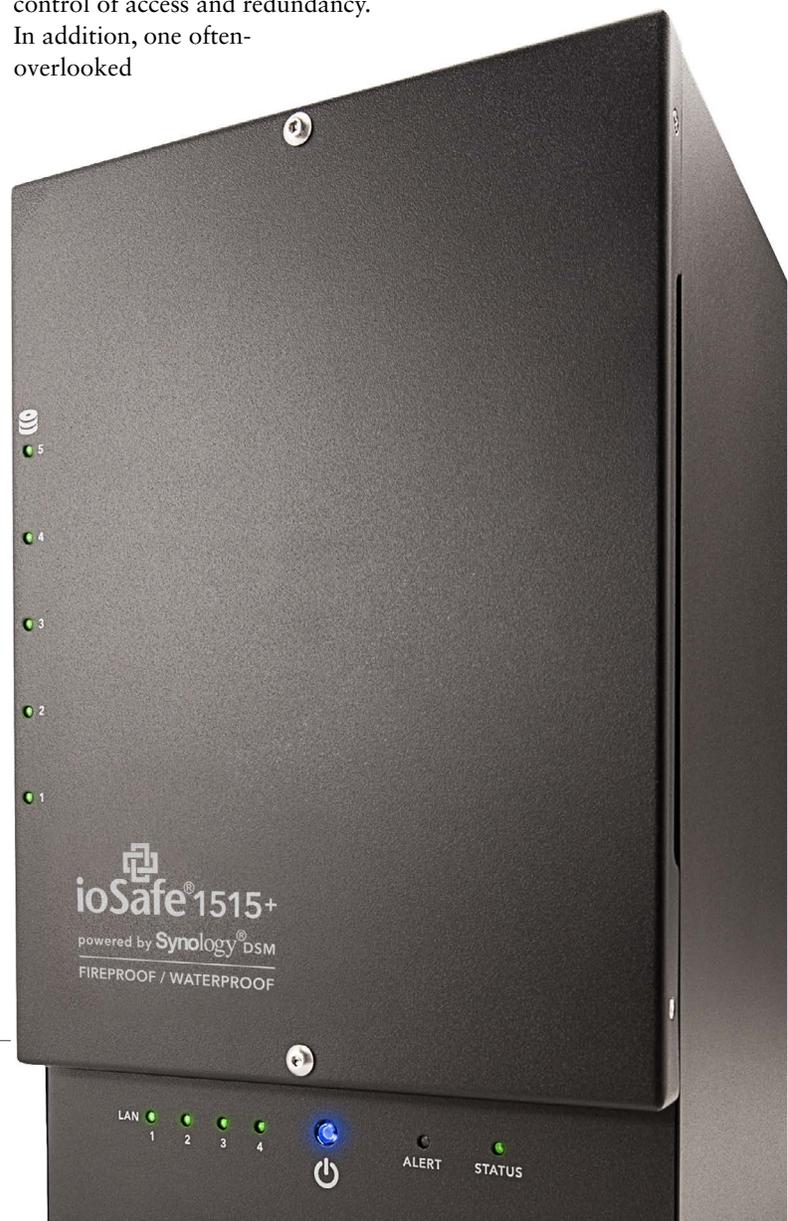
Does your business have a cloud initiative? What is your company's plan for moving to a hosted Storage as a Service, or Software as a Service model? Will switching to the cloud for backup and disaster recovery save you money, or give your CIO peace-of-mind? Even after much of the news about the NSA's electronic surveillance program, your business probably has plans for some type of cloud usage. As recent events have shown, there are however additional issues with the public cloud that many IT administrators need to overcome. This paper will discuss alternatives to the public cloud and how can, instead build a private cloud to take advantage of anywhere access while applying your own security policies to retain complete control of your data.

You Can't Beat the Cloud's Price or Convenience. Or can you?

With major cloud providers such as Box, Google and Dropbox dropping pricing to [less than \\$10 per month](#) for a terabyte, or even [unlimited](#) amounts of storage, it may seem attractive to drop some of your large storage systems which are costing an arm and a leg just for the recurring service contracts, and begin storing employee data in the cloud. This way, your storage is accessible from anywhere, and your service level agreement leaves the burden of backup and disaster recovery on the cloud provider. But despite the numerous benefits, IT personnel are discovering that the cloud creates breaches in security designs presenting risks of unauthorized access and opening holes in corporate compliance. While most services do offer enormous amounts of security protection, there are always risks involved when handing off control to another party.

In fact, after numerous, recent security breaches of corporate networks, the low pricing and convenience of cloud storage suddenly becomes less favorable to on-site, private storage where the owner maintains full control of access and redundancy.

In addition, one often-overlooked



drawback of cloud storage is slow data recovery. While on-line off-site backups provide a business with data resiliency against fire or flooding of a building, it often introduces a lengthy recovery time. Assuming 7TB is about the average amount of data retained by a small to medium business, with the [average US bandwidth of 32Mbps](#), complete data recovery would require approximately 22 days of recovery time from an off-site storage array or Cloud Backup Storage Provider. Recovering a larger data set of say, 15TB would take approximately 46 days, which assumes the restoration operates at peak bandwidth for the entire data recovery. Waiting a number of weeks or even months to resume business operations following a disaster is unrealistic to say the least.

Given that today's businesses are working with larger data sets, want the latest revision of data to be backed up, and are looking for quick restoration times, an innovative solution is needed to meet all of these objectives and get a business running in minutes or days.

How Safe Is Your Data In The Cloud?

Before former government contractor [Edward Snowden](#) revealed that the NSA was running a digital surveillance program of enormous scale, corporate cloud policies were based more on employee compliance, than cloud provider security. After the fallout of the NSA scandal, cloud providers now tout high levels of security with features such as two-factor authentication, and IT based policy control of corporate data, but is this enough?

What we now see are cloud providers being completely transparent about how much user data they share and how many requests they receive from the federal government for so called private data. Google now has their [Transparency Report](#), which discloses the number

of unique user data requests that Google receives from the US courts and government. As an example, in Q4 of 2014 Google received 31,698 requests for user data. Rather than hide, Google and other cloud providers comply with laws governing their disclosure of user data and provide data to government entities when required. The question is, are you, as an IT professional with corporate data stored in the cloud, ok with this?

Create Your Own Cloud With Automatic Disaster Recovery and Data Protection

The security of the public cloud is a real concern to those administrators with sufficient experience. In fact [57% of organizations after deploying cloud services](#), have reconsidered and migrated back to an internal infrastructure. And due to compliance issues, not all business data may be stored in the Public Cloud in the first place, including sensitive accounting information, patent information, MRI data, or data created in HIPAA environments. IT administrators stated that the top two considerations for reverting back to private storage were based highly on security concerns, and the lack of guaranteed remote data protection.

As an alternative to the public cloud, administrators have the option of creating an internal private cloud. This creates a secure environment accessible by corporate employees from anywhere. With options for corporate domain security policies, encryption, built-in firewall software, HTTPS and SSL/TLS, administrators can prevent unauthorized access; yet still create an environment where authorized users can access data easily.

The ioSafe Solution

The ioSafe 1515+ and 214 are scalable, fully featured network attached storage servers powered by Synology® Disk Station Manager. ioSafe NAS are the ultimate in storage security because data remains local and is never exposed to the dangers on the traditional



public cloud. All security details are 100% controlled by you – the person that cares the most about the data. Like an aircraft black box for data, there's not another product on the market, which combines the security, protection and features of the ioSafe NAS.

ioSafe NAS with Synology Cloud Station is a smart way to sync files across multiple devices. Whenever a file is changed, the update is synced to your laptop, smartphone, or your office PC. Files can be edited in offline mode and later synced to Cloud Station, which retains up to 32 versions to avoid file overwriting. With unlimited users and unlimited sync folders support, it is the perfect file sync and edit solution for individuals or organizations.

Multi-site businesses can utilize 2-way sync between different ioSafe NAS servers to ensure employees at different locations share the same information in real-time. In more complicated file storage scenarios, synchronization rules can be customized to fulfill administration demands, such as avoiding syncing large files to optimize bandwidth usage. Businesses will find Cloud Station suitable for organization use as it offers domain/LDAP support, flexible administrative tools and encrypted data transfer.

In addition to the private cloud features, ioSafe takes disaster recovery to the next level compared to standard NAS devices, with ioSafe proprietary hardware technology, designed to protect data from fire, flooding and theft. The ioSafe 1515+ and 214 protect from data loss from fire temperatures up to 1550°F/843°C for 30 minutes per ASTM E119. For flood protection, the ioSafe seals the drive bays a waterproof aluminum enclosure, to protect from data loss due to fire hoses or in complete water immersion of up to 10 feet (3.1m) for 3 days. Finally, with their heavy steel construction, ioSafe NAS servers can be secured to a concrete floor to prevent the physical theft of confidential data.

Installing an ioSafe NAS is easy. Simply connect it to an Ethernet network, and power the unit up. After that, install the [Synology Assistant software](#) to find the NAS on the network and open the installation wizard that assist in configuring the access and security policies of the NAS for the environment. Once configured, simply point servers or client backup software to the 1515+ network shares for effortless network backup. The unit also provides instant file sharing, client data protection, disk redundancy with RAID protection, replication and a long list of additional corporate and consumer software services.

ioSafe NAS is the option of choice for businesses deploying a Business Continuity Plan (BCP), when reliance on the Public Cloud to withstand and recover from disasters is no longer an option. With businesses today having larger data sets, maintaining backups in the Public Cloud often incurs a lengthy recovery time, sometimes measuring many days or months. Post disaster, the first step is ensuring the health and safety of those involved, and then moving into implementing your BCP and resuming business operations. With the ioSafe NAS servers on-site, businesses have the ability to create a Disaster Resistant Private Cloud where the RPO and [Recovery Time Objective \(RTO\)](#) is near zero. The ioSafe allows a business to weather a storm, recover data quickly, and resume business operations to full strength in the shortest amount of time.

By choosing the ioSafe, you receive the additional benefits of on-site disaster recovery including free [data recovery services](#) and a no-hassle warranty. By creating a private cloud and essentially becoming a cloud provider you can avoid security leaks and give those in your organization the freedom to share data and access it from anywhere, with the utmost in disaster recovery available today. See how ioSafe can help you protect your data by visiting www.iosafe.com.