



PCN contact info:

<http://www.pcni.us>

support@pcni.us

907-244-1101 Ryan Croghan

907-244-7434 Peter Barclay

5 Essential Benefits of Hybrid Cloud Backup for SMBs

The Value of Business Continuity

A hybrid cloud solution combines private (internal/on-premise) and public (external) cloud deployment models. With a typical *private* cloud solution, one would build, develop and manage their own cloud infrastructure. The most common deployments of private cloud solutions are in enterprise-level environments. Businesses that have the capital to fund a private cloud operation will usually purchase the necessary equipment, hire their own dedicated IT support teams, and build or lease their own data centers. This allows the company to have complete control over their cloud environment. The primary downside of a private cloud is that it is very expensive to implement and maintain. It also requires highly skilled engineers to manage the network.

In a *public cloud* scenario, one utilizes web-based applications and services. Hardware or software is not owned or maintained by the client, and resources are completely acquired from third party vendors. Google Apps, Salesforce, and Amazon Web services are all common examples of public clouds. With these deployments, end-users will work strictly through the Internet via web-based portals. Generally, application data is not stored locally. All relevant information is stored through the cloud provider.



While these solutions are cost-effective, the lack of control of data center resources, monthly fees, and increased support costs can hinder the viability that a public cloud will align with every business. The fact that business critical data is stored only offsite can also be disconcerting for businesses. One must also consider the possibility that the cloud provider could go out of business, experience a service outage, be acquired by another company, or suffer a security breach. Any of these scenarios could spell disaster for a business' data.

With a hybrid cloud model, aspects of both platforms are merged to form a single, unified platform. A business owns some form of local hardware, which is integrated with resources owned by a third party. Depending on what attributes of the business are being pushed to the cloud, there are many options for how a hybrid cloud platform can be constructed.

What is Hybrid Cloud Backup?

In the context of data backup, a combination of private and public backup solutions can be used to form an efficient and robust platform. Hybrid cloud vendors use their expertise to engineer enterprise-grade backup solutions that can be affordable for businesses of any size.

On the private cloud side, an end-user would have a local device that acts as a NAS (Network-Attached Storage) unit backing up data locally, while concurrently pushing data off-site to a secure, third party cloud. What sets these units apart from a typical NAS unit is that they also apply complex data deduplication, compression, file conversion, and other processes which are unique to each vendor. These processes help reduce storage space on local devices and off-site servers, keep local bandwidth reduction at a minimum, and optimize the backup process to make data recovery as efficient and quick as possible, both locally and in the cloud.

The public cloud side is comprised of the data center infrastructure developed by the cloud provider. Mirrored backup images from local backup devices are stored and archived in proprietary data centers, so they can be accessed in the event that backup records are not available locally (i.e. a disaster scenario ¹).

Having the cloud infrastructure developed by a third party is valuable to consumers because through economies of scale, backup cloud vendors can provide space in the cloud at lower costs per GB than the average MSP could provide if they built their own cloud. This enables IT service providers and their clients to leverage cloud storage, without having to pay high monthly fees. Also, by utilizing third party technology, end-users and MSPs need not worry about maintenance of the cloud; that liability lies entirely with the vendor.

¹Disaster scenario: For the purposes of this report a "disaster scenario" is classified as any event that occurs at the local site and affects the functionality of the local production machine and backup device. This could range from a power outage, to a server room fire, to a tornado that destroys an entire office. In any disaster scenario access to original files and local backups will not be possible.



1. Business Continuity

A desired benefit of most hybrid cloud backup solutions is the ability to achieve *business continuity*. Business continuity is a proactive way of looking at disaster preparedness. By having the proper tools and procedures in place, businesses can be assured that they will remain functional during a disaster scenario, large or small.

Business continuity, in the context of data backup, means that in the event of a disaster, cyber-attack, human error, etc., a business will never lose access to their critical data and applications. In the data backup industry, the lack of access to business critical data is referred to as *downtime*. Business continuity is critical to any business, because downtime can potentially bring operations to a halt while IT issues are being repaired. This can be extremely costly for any SMB to endure.

While proper business continuity planning is necessary throughout an organization, one technology that enables continuous up-time is virtualization of servers and workstations. A virtualized server or workstation is commonly referred to as a virtual machine or VM. This is essentially a copy of a workstation or server that runs on the hardware of a cloud server, as opposed to the hardware of the original production machine². The VM is booted off of a production machine's backup file that is housed in cloud servers. Once the VM is booted, every aspect of the virtual machine (i.e. operating system, applications, and files) will run exactly like the original machine did.

This is invaluable in disaster scenarios, because if the original production machine is taken out of commission, a business can transition to the virtual machine immediately, while the original production machine is repaired or replaced. This is known as *failing over*. By allowing servers to *failover* to the cloud, a business is able to combat downtime and continue to manage their data and applications until the local IT infrastructure is fully operational.

The flexibility of the hybrid cloud platform is truly what enables IT Service Providers to deliver business continuity to their clients. Since backup files are stored both on the local device and in the cloud, *it is possible to virtualize both on-site and off-site*.

For example, if a failover virtualization is necessary because of a server malfunction, it can be done quickly and easily on the local device. The business will function off of a VM of their malfunctioning machine. Once technical issues are resolved, and the server is back up and running, the business can transition back to their original infrastructure with a bare metal restore (BMR)³. The BMR will return all backed up data and applications to a new or repaired server so operations can continue as usual without losing any changes in data that occurred during the outage.

In the event that an actual disaster occurs on-site, where a production machine and the local backup device are taken out of commission (e.g. fire, power outage, tornado, earthquake, etc.), the business data is not lost. Virtualizations are still possible via the off-site cloud. Businesses will run off of VMs just as they would if it was stored on the local device, while a new local device will be seeded with data to replace the destroyed device.

² Production machine: A production machine is the "live" workstation or server that is in place at an end-user's business. These are the machines that are being backed up.



After the device is replaced on-site, the VM can be transitioned to the replacement device. The business will continue to run off of the local VM until a BMR can be performed. Once the BMR is completed, the business will have returned to full operations without incurring downtime, even if their office was completely destroyed.

The flexibility to virtualize both on-site and off-site mitigates the threat of downtime. Businesses can continue to function regardless of external or internal challenges their IT infrastructure may encounter.

2. Data Insurance

The hybrid cloud backup process generates a backup locally, and then a backup of the backup is replicated off-site (in some cases, data is replicated to two off-site locations). This provides a great deal of data security. With local hardware, all data is in-house, protected by preexisting firewalls, security protocols, and the encryption inherent to the backup device. Furthermore, by sending encrypted data to dedicated data centers, users are ensured that there are redundant copies of the data secured off-site. This is invaluable in the event of a disaster.

The combination of local and off-site backups affords far greater peace of mind than simply pushing data over the web to a backup service provider or strictly housing data locally on a NAS or in a data center.

This figure is a representation of how data is secured in the hybrid cloud (page 5). As the diagram shows, at any given moment, copies of a client's data will be located in three unique locations. The original on the client's server or workstation, a backup on the local device, and a mirrored backup in a data center off-site. Also, since both clouds not only store data, but are also capable of virtualizing and restoring the production machine, MSPs and VARs have multiple comprehensive resources to assist their clients in data protection and restoration.

³Bare Metal Restore (BMR): A bare metal restore is the complete restoration of a machine, from operating system to applications to individual files, onto new or original hardware.

Assessing Your Backup Solution

When assessing whether a particular solution is capable of providing business continuity, two key metrics need to be assessed. The first is RPO, or Recovery Point Objective. This figure represents how frequently backups can be taken, or how much data one is willing to lose if a production machine were to fail.

For example, if a business is utilizing a backup solution with an RPO of 1 hour, then a backup can be taken once an hour. If a business were to utilize that solution to backup an important server, then it is stating that it is comfortable with sacrificing up to an hour of data change on that server in the event of an outage. Both business continuity and traditional backup solutions can provide good RPOs, with some business continuity solutions achieving RPOs of up to 5 minutes.

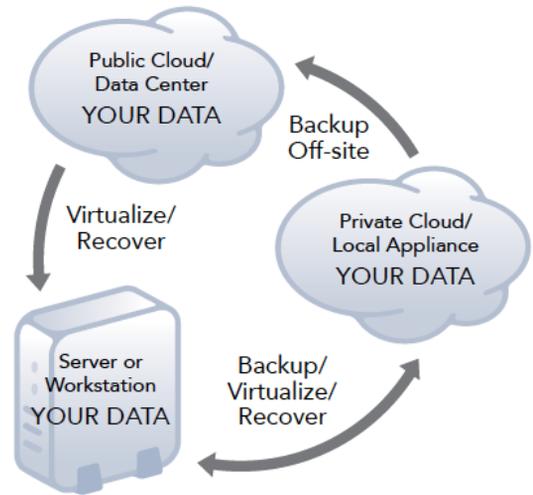
Where business continuity truly differentiates itself is with the Recovery Time Objective, or RTO. RTO represents how long it will take to get data back after a disaster. This is an essential figure to know because even though data is backed up and secured from loss, a business cannot function properly until the data is recovered.

Enterprise-class business continuity solutions should be able to provide RTOs of under 10 seconds. This is far superior to the weeks it can take to download large backup records from online services, or the hours that it takes to covert server images for virtualization on a traditional BDR unit.

This level of security provides a great value proposition to end-users when framed in the context of insurance. Businesses insure every aspect of their infrastructure (buildings, equipment, employees) yet most of them don't insure the most important pieces of their entire business; their data. By having redundant copies of data located in multiple locations, hybrid cloud owners can rest assured that in the event of a disaster their data is protected and can be made available at any time.

3. Local Storage Flexibility

A benefit of hybrid cloud solutions is that the entire backup is not solely housed on-site. By leveraging the "infinite" storage space of the cloud, a business can decide how long they want their local retention to be, and scale it according to their needs. Files can be restored with ease whether they are on-site or off-site, so businesses do not need to worry about losing on-demand access to their data.



This offers a great benefit to smaller businesses, because it provides some flexibility if the local backup device has limited storage. In the event that a business starts to run out of space on their device, they can either consolidate incremental backups and/or prune off local copies of older backups that have already been replicated and secured off-site. This reduces the necessity to purchase more local storage as a result of data growth. This is a huge pain-point for users, as many businesses do not have the resources to purchase, house, and maintain a backup infrastructure that is scalable to their data growth requirements.

If a business outgrows the storage capacity of their local device, such that excessive maintenance is required to keep space free for new incrementals⁴, then an upgrade may be necessary. Fortunately for end-users, some vendors are aware of this inevitability and have made upgrade processes very simple, seamless and cost effective.

By utilizing the hybrid cloud platform, a business can have the peace of mind that their data is safe regardless of the size and growth of their data. They will only be required to provide the amount of space required to backup their files locally.

⁴Incrementals: during the backup process, multiple backups are taken on an incremental basis to keep up with data change. Smaller segments combine to form the full backup of the system. The combination of these incremental backups form what is known as the backup chain.



4. Cost Benefits of Hybrid Clouds

Private clouds are expensive:

- Hardware acquisition, ownership, development, and implementation costs lead to large financial investments.
- Expenses and manpower costs required to maintain the solution can add up fast.

Hybrid clouds keep costs down:

- Initial investments are low.
 - End-users/MSP don't need to own all of the essential pieces of the puzzle.
 - e.g. Datto only requires the local unit to be purchased, while the rest of the infrastructure lies in the proprietary Datto cloud.
- No costly maintenance is required by the MSP.
 - Decreased power, cooling and physical maintenance costs.
- Low monthly service fees/licensing costs.
 - Cover the cost of leveraging the cloud, software agents, and services outlined in SLAs.

Business models in this industry are not universal. With some solutions, hardware is not directly purchased, but leased or provided with no upfront cost (HaaS model). While no initial investment is required, monthly service fees are generally higher and require long-term contracts.

5. Standards Compliance

For some industries, it is necessary to keep specific data backed up in order to comply with government regulated standards (i.e. HIPAA, PCI, SOX). Backup vendors are aware of these stringent regulations and have built their clouds to meet the needs of these verticals. The hybrid cloud platform lends itself perfectly, because if a local backup device is decommissioned all files are already located off-site and can be accessed easily when necessary. This fulfills many verticals' requirements for contingency plans in emergency scenarios.

Archiving capabilities are mandatory to these industries as well. For example, medical entities governed by HIPAA regulations require a six year retention policy for certain personal and medical records. By having redundant copies of backup records, companies protect themselves in the event of an audit.

For example, Datto archives backup images for one year after they have been deleted from the local device. So if a five year old backup was removed from a local unit, it would still be housed off-site a year later. If necessary, a business can increase their off-site retention to extend compliance off-site.

All in all, the hybrid cloud backup platform encapsulates the best of the private and public models to form a feature rich, highly efficient, and affordable system