druva

Executive Brief

CHOOSING THE RIGHT MODEL FOR ENTERPRISE BACKUP & RECOVERY

The Executive Guide

Q417-CON-10681

Before You Begin

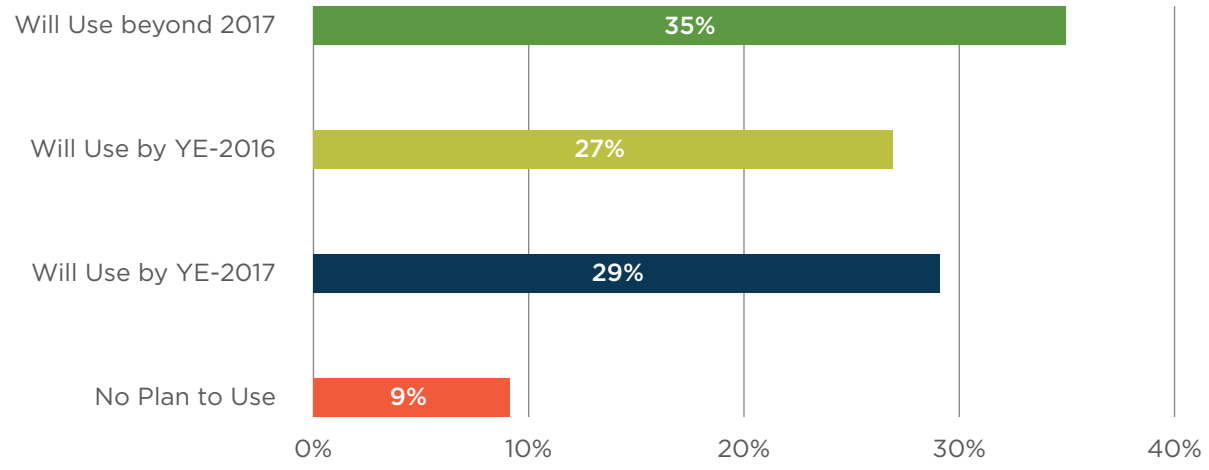
Gartner predicts that 62 percent of organizations will deploy applications and services to the public cloud by the end of 2017. “Cloud adoption continues unabated as cloud use cases shift beyond simple tactical outcomes to strategic benefits,” their study finds. But what advantages do public cloud services providers have over other types of cloud deployments? And for those just beginning their search, what other types of cloud deployments are out there, and which ones should you even consider?

The public cloud can be a cheap and easy way to store a large volume of data, which makes backup and data protection an ideal fit for most organizations. However, cheap disk-based data center storage options can be an inexpensive and convenient solution as well. You’ll need a lot more than just storage though to make an effective data-protection solution run, let alone scale along with the growing needs of your business. To get started, here are some important questions to ask yourself:

- How will I use the cloud?
- Will I consume a public cloud, build a private cloud, or something in between?
- Which software and/or hardware solution or cloud provider is best for my needs?
- What geographic regions do I need coverage in?
- What services do I need for my application to function properly?

The answers to these questions can vary dramatically from business to business. Not having a clear understanding regarding priorities as well as the needs of the business before the task of migration even begins can result in making disastrous and costly errors.

Organizations Deploying to Public Cloud



"The dilemma of where to allocate available IT budgets between on-premises and cloud resources will become more common and more critical."

–Gartner, Cloud Computing to Drive Digital Business

The decision to deploy and maintain your own data protection application, pay someone to manage one for you, or leverage the capabilities of a Software as a Service (SaaS) provider is an important choice. While an on-premises or hybrid solution may seem easier because it leverages owned internal resources, a cloud option may offer superior durability and reliability that are unrivaled by anything hosted in your own data center.

While the value of data protection is clear, the choices available to enterprises may not have as much clarity. In this Executive Brief, we'll examine the four leading contenders and provide you with the pros and cons for each. This will help you to make an informed decision that ensures your chosen solution meets your organization's unique needs.

Your Options for Data Protection Solutions

1. On-Prem (Private Cloud)

With data protection hosted on-prem in a pure private cloud, you operate a secondary data center for the express purpose of backing up your business data. While it may resemble your primary data center in many respects, the hardware requirements will be different as they will need to be optimized for longer-term storage and increased data reliability. Budget permitting, you may also decide to incorporate multiple layers of redundancy to ensure data durability.

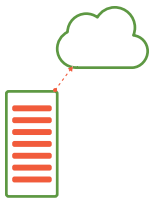
Pros: With your own hardware deployed in your own onsite data center, you always have access to the hardware. You own it, you control it, and you can configure it and upgrade it however you want. You don't have to worry about vendor service level agreements (SLAs), because the hardware is yours. If you are handling extremely sensitive data, this may be a compelling alternative, but make no mistake, any machine that accepts connections from the outside world is vulnerable.

Cons: Unfortunately, there are many cons with using on-prem storage for data protection. First of all, it must be acknowledged that this is not a cloud deployment—your storage space and computing availability are limited by the constraints of your hardware. When requisitioning hardware, you will have to factor in an overhead allowance to account for periods of high demand and for your organization's data growth over time. Thus, you are not leveraging the scalability of the public cloud in any way.

Second, with your data hosted in one central location, any power outage or hardware failure in that location can cripple your business. It may be hours or days before you restore operations, and data that had been backed up and then removed may be lost forever. Compare that with leading cloud vendors such as Amazon Web Services (AWS), which offers uptime and durability guarantees and automatic failover in the event of a disaster.

Finally, compliance and security have become increasingly important in the new regulatory and threat landscapes. Consistently maintaining the security patching and upgrade schedules necessary to address constant vulnerabilities takes dedicated resources in order to even begin to match the capabilities of a public cloud vendor like AWS. And with a host of regulatory certifications like SOC1/2, FIPS, and HIPAA, an organization in a regulated industry can immediately see the benefit of leveraging a public cloud platform.

Some on-prem software vendors will make the argument that deploying their product in your own data center can offer the same benefits as a cloud platform, but it can't. While this may provide the business with the comfort that the solution is in their own domain, none of the cloud benefits are provided under this model. All of the same legacy infrastructure constraints, complexity, maintenance costs, and headaches will still be there



2. Cloud Gateway (Hybrid Cloud)

Often used by legacy backup vendors, a cloud gateway is a hardware- or software-based appliance that links your on-site systems with cloud storage solutions. It provides the basic translation and connectivity required to access incompatible systems, allowing your data to be backed up to the cloud. This attempts to maintain the illusion of having equipment hosted in your own data center, while leveraging the scalability of cloud storage vendors for backup and recovery purposes.

Pros: A cloud gateway relieves the fear that any failure of your on-prem hardware may mean losing data forever, as backup data is stored in a remote location. In addition, you are not responsible for the maintenance and upgrading of remote hardware, only the appliance that lives within your data center.

Cons: While this option enables enterprises to govern the flow of data to the cloud, it also creates problems. All network traffic containing data to be backed up must pass through, and be translated by, the gateway. This device then becomes a bottleneck, both from a networking and a reliability standpoint; if the gateway fails, all access to the cloud fails. Software gateways may also offer limited encryption of data in transit, whereas hardware-based gateways generally do not. In addition, a hardware-based gateway has no facility for providing deduplication of data in the cloud—it actually sends more data than is necessary for secondary storage. As a result, your organization's data can grow exponentially over time, and when you are paying by the gigabyte, these costs can multiply rapidly. Cost is a concern here as well if you have infrastructure housed in multiple locations since the pricing structure requires you to purchase separate hardware for each data center.The same security concerns seen in the on-prem model exist here, as well as deficiencies in compliance capabilities.

3. Hosted Solution (Cloud Colo)

Another common option is the hosted model, in which the cloud service provider essentially duplicates an on-prem architecture and hosts it in a cloud instance. With this model, you buy or license an application and storage, which is then hosted in the vendor's remote location, or in a cloud platform that you control, in an attempt to mimic the appearance of a true cloud solution.

Pros: With a hosted appliance or software solution, you may have the familiarity that comes with understanding your own environment, which can reduce the learning curve for administrators and IT staff. If the solution is hosted on your cloud account, an AWS instance you own, for example, it may also give you the feeling as if you're saving money by utilizing a resource you already have. This model also places increased responsibility on the hosting vendor to ensure that power outages and other disasters do not become a factor.

Cons: The hosted solution is not natively architected to take advantage of the scalability and flexibility of a public cloud environment. This essentially places similar constraints on the hosted application as you would find when hosting a solution in your own data center. Solutions like these can be both expensive to build and expensive to manage, because the provider is no longer managing aggregated storage on its own systems. You're now on the hook for storage costs that could grow exponentially because the application simply isn't optimized for long-term public cloud storage. For that same reason, you could also be exposing yourself to several other cloud providers fees for other compute and networking resources consumed by a piece of on-prem software that is being shoehorned into the cloud. As with the on-prem model, you are responsible for ensuring that you have the computing power to run your applications and the headroom to account for any spikes in demand or future growth.

As with the storage gateway model, your data is stored offsite and requires network connectivity to function correctly. As such, it carries with it the same limitations: if you lose connectivity, you lose access to your data as well as incurring additional costs to accommodate the needs of the application. In addition, security and compliance concerns are not addressed well with this model.

4. Cloud-Native (SaaS)

A true cloud-native SaaS data protection solution is designed from the ground up to take advantage of the revolutionary advantages offered by the public cloud, including global deduplication, uptime guarantees, flexible computing availability, and automated tiered storage models. All of these offer dramatic improvements over legacy solutions.

Pros: This final service option, built natively for existing public cloud service providers (e.g., AWS), provides multiple advantages for enterprises in search of greater efficiency, automation, and on-demand elasticity. It takes advantage of the native capabilities of the public cloud, such as storage, compute, and their efficiencies to create a well-integrated offering from the start. When more or less capacity is needed, the cloud scales up and down seamlessly to meet the changing demands of the business, without complex, cumbersome and costly hardware and software procurement cycles. And, because it does not require a translation layer between older deployments and a cloud-like gateway appliance, it eliminates bottlenecks, boosting both performance and uptime. This cloud-native option also offers more versatility, allowing enterprises to use it as a convergence point for other important activities. It does not use cloud storage as the technological equivalent of a warehouse; rather, the data can be reused for many purposes—for eDiscovery, compliance, disaster recovery, and beyond.

With a pure cloud-native SaaS solution, there is no need for additional resources to maintain the complex adherence to regulatory requirements or to perform the constant maintenance required to combat security threats. All of the burden shifts to the SaaS vendor, who provides all of these services while constantly upgrading and improving the core product that you consume.

Most importantly, the predictable subscription cost structure removes all the volatile and complex expenses of the other models. Instead, it uses a simple model where you only pay for what you need. Other deployment models include maintenance fees, complex licensing costs, and variable resource-consumption expenses that vendors fail to include when they calculate the total cost of ownership (TCO).

Cons: The concerns surrounding a cloud-native offering are minor. With your data backups hosted in the cloud, leveraging the uptime guarantees of providers such as AWS, there is little risk to your data. The biggest concern would be if your office lost Internet connectivity, rendering you temporarily unable to access your applications. But, with so much of today's business conducted online, the impact of this on your overall operation would be minor. Most other concerns, such as the failure of an entire electricity grid (for example), are easily addressed by leveraging multiple availability zones.

The Big Takeaways

While there are a number of competing options for any organization wishing to deploy a data protection solution, there are significant differences between a cloud-native solution and those that call themselves “clouds.”

DIY and Hosted

Any solution that involves leveraging your hardware will come with the same constraints that you find when operating your own data center. In addition, hybrid or hosted solutions fall short of delivering the full benefits that the cloud can provide. Scaling out compute and storage to fulfill the growing needs of the business will still remain a challenge using these models.

Cloud-Native Solutions

Only a data protection solution designed from the ground up with the cloud in mind can deliver the increases in speed, reliability, manageability, and affordability that have helped the cloud become the dominant technology of this decade. As the public cloud matures and becomes an ever brighter fixture in the IT firmament, companies would be wise to consider the significant advantages of a cloud-native SaaS solution.

Questions for Leaders

1. What will be the true costs of ownership when considering each model?
2. What additional value beyond backup does the solution need to offer the business?
3. What type of availability and access is required to meet the needs of the business?
4. What are the long-term goals of a data protection strategy, and which model will be the best fit?

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information - dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva’s award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com