UNITRENDS
A Kaseya COMPANY

4 Steps You Need to Take to Fully Protect all your Clouds

Are you ready to deal with the unique challenges of protecting multiple clouds?

INTRODUCTION

Gone are the days of a single data center containing the entire computing infrastructure of an organization. Yesterday you could protect everything with a single backup and recovery solution because everything was located in one virtual location. Today most organizations have servers, storage and apps running locally, remotely, and using several different computing, storage, and SaaS cloud vendors at the same time. We have evolved to a multicloud environment. So how do you protect everything with no gaps and without spending dozens of hours of effort per week?

WHAT IS A MULTICLOUD ENVIRONMENT?

Wikipedia defines multicloud as this – "Multicloud is the use of multiple cloud computing and storage services in a single heterogeneous architecture. For example, an enterprise may concurrently use separate cloud providers for infrastructure (IaaS) and software (SaaS) services, or use multiple infrastructure (IaaS) providers." What Wikipedia leaves out of their definition is the complexity is even greater than this. They have not included that most organizations still have a sizable on-premises deployment that has to be managed.

THE PROTECTION CHALLENGE

How do you protect a multicloud environment without leaving gaps in your coverage? Legacy backup and recovery solutions were not designed to protect an environment as complex as a multicloud. Having multiple backup and recovery solutions will leave gaps in coverage and result in unprotected apps. You need a single recovery architecture, one with many facets to protect such diverse environments such as SaaS, local, remote and cloud-computing workloads, which acts as a single product..

You should be looking for a fully integrated data protection and recovery architecture.

WHAT TO LOOK FOR IN A RECOVERY ARCHITECTURE

You have a couple options with respect to building your recovery architecture – the first is for you to select each vendor and component and craft a custom solution. The issue is that you don't have enough time in the day to understand the gaps in coverage, the different management functions, impacts to your network, and different User Interfaces.

The other option is to go with a pre-integrated solution with all components designed specifically for the optimization of backup and disaster recovery. You should be looking for an integrated data protection and recovery architecture. How can you tell all the features are completely integrated? Look for these features:

CENTRALIZED MANAGEMENT

You should be able to manage your entire multicloud backup and recovery solution from a single console, on a single device, at a single location.

It is most effective to administer a multicloud recovery architecture centrally. This means using a single device to manage all your data from a one location. Rather than trust remote employees to follow a complex set of rules and regulations, a single team should be able to perform all protective functions no matter where the assets physically reside, within you firewalls or in the public cloud. A comprehensive and easy to use User Interface (UI) can automate a recovery strategy. It should always be possible to operate your backup system without having to refer to a manual so that just about anyone in the organization can stand in when primary admins are unavailable.

SINGLE VENDOR SUPPORT

You should have every element of your data protection solution covered by a single service organization.

When one element of your recovery architecture goes down you don't want to be the one trying to figure out which vendor is responsible and which service organization to call. This only leads to finger pointing. You need to have your entire recovery architecture supported by a single service organization available by phone, chat, and email—24 hours a day, 7 days a week, 365 days a year. Ideally the support engineers should be located in the US and at the same location as central engineering to ensure easy access for advanced questions. Ask your vendor to document their satisfaction rating to see how satisfied existing customers are with their support.

Some service organizations will also manage the DRaaS infrastructure for you. Vendors that offer "White Glove Services" will take on the responsibility of set up, testing, maintenance, and disaster failover and recovery for you so you don't have to become an expert in public cloud software

AUTOMATED RECOVERY TESTING

You should be able to automatically and regularly test all elements of your recovery architecture with one set of tests for no additional charge.

The only way to know if you can recover in an emergency is to test regularly and each time you make a change to your infrastructure. You need to schedule time out of your busy schedule to conduct the tests and then deal with any issues that arise. You also may not be able to use the production servers to host your tests since business performance may suffer. In addition, recovery testing cannot always be done in the local environment. Therefore, you may need to have testing done in remote or managed DR locations.

New, intelligent tools are available that can greatly ease your concerns by automatically testing local and remote assets to ensure all components are in place and capable of recovering or identifying issues if the test fails. Recovery tests should be full application recoveries with standard and / or customized tests that ensure all settings and data elements are in place so business users can get back to work immediately upon recovery. Additionally, you should receive an easy to read, formal report certifying that your disaster recovery solutions have been tested and document the results. The reports should be so good they can be used in compliance audits to prove you have recovery procedures in place, they are regularly tested, and recoveries are delivering the required RPO and RTOs.

You should be able to automatically and regularly test all elements of your recovery architecture with one set of tests for no additional charge.

It is most effective to administer a multicloud recovery strategy centrally. This means using a single device to manage all backups and recoveries from a central location.

CENTRALIZE YOUR DRAAS STRATEGY

You should be able to fail over any workload to a single DRaaS service regardless of size, criticality, or where it originated - from the cloud or on premises. Even public cloud workloads should be included in this strategy.

Your recovery architecture should be supported by optional cloud-based Disaster Recovery-as-a-Service (DRaaS). DRaaS allows organizations to spin up their applications in an independent cloud regardless if the original applications are located in a datacenter or cloud. This is the ultimate level of protection as business critical applications can be run on remote infrastructure allowing business users to continue doing their jobs even if the cloud or data center is completely destroyed. You should look for written performance guarantees against publicly committed recovery times.

TAKE THESE 4 STEPS TO PROTECT EVERYTHING IN YOUR INFRASTRUCTURE

1 - PROTECT ON-PREMISES ASSETS - LOCAL AND REMOTE

Your environment may be complicated, but protecting it doesn't have to be. You need to protect everything in your data center, whether it is physical or virtual, on emerging hyperconverged infrastructures such as Nutanix and VMware VSAN, deployed on premises in your central data center or at a remote location.

Best-in-class organizations deploy a single, all-in-one appliance, specifically designed for data and application protection. An appliance is easy to install, upgrade, and manage. Today's leading appliances natively protect all computing platforms, including virtual systems, physical Windows and Linux systems, legacy systems, hyperconverged platforms, and remote devices. Local recoveries can be run on the appliance itself. Appliances in different locations can act as backups for each other so that site level disasters such as electrical failures or floods do not bring down the entire enterprise.

2 - PROTECT YOUR SAAS APPS

You are as responsible to protect corporate data in the cloud as you are to protect it on premises. SaaS vendors such as Microsoft and Google protect you from data loss caused by system issues, but customers are responsible for data loss from accidental or malicious deletions, third party software, ransomware, and other user issues.

For example, SaaS apps have a Recycle Bin for basic recovery services. Deleted items are purged from the Exchange Recycle Bin, for example, and are unrecoverable after 14-30 days, depending on your settings. Similar limits exist for Google G Suite and Salesforce. It is impossible to recover a file once it has been deleted from the Recycle Bin unless you have optional backup capabilities.

SaaS data protection is more about backup than continuity. It is highly unlikely that the entire Microsoft Azure O365 cloud goes down, but very likely the end user will delete a folder they believe is no longer important. A SaaS protection service must be part of a recovery solution architecture that replicate files, folders, contacts lists and even entire shared drives to a different public cloud to protect them from catastrophic disasters and user errors. Recovery can be performed in seconds even if a user has permanently deleted data from his active account. You can even rollback to a specific version of a file, folder or document library.

3 - PROTECT PUBLIC CLOUD WORKLOADS

The best technology for protecting public cloud-based applications is the same as that which is used for your datacenter. Install a software appliance in the public cloud that automatically backs up data, applications and system settings and replicates them to another area of the cloud, to your data center or even a different public cloud provider. Lost data files can be restored from the backups and the backups can be used to quickly restore the entire computing infrastructure if needed.

For recovery of cloud workloads it is better to use another cloud than to bring the apps to your on-premises data center. This would require extensive and expensive spare server and storage capacity which is probably one of the reasons you went to the cloud in the first place. You can choose to backup and recover to a different cloud location within

World-class DRaaS providers now offer “White Glove” services that free enterprise IT from having to learn, manage and deploy recoveries.

one vendor or to an entirely different cloud provider.

4 - PROTECT EVERYTHING WITH DRAAS SERVICES

This will give you the highest level of confidence in your ability to recover. Protect everything with Disaster Recovery-as-a-Service (DRaaS), even workloads operating in public clouds such as AWS or Azure. DRaaS has greatly evolved from its first iterations. World-class DRaaS providers now offer “White Glove” services that free enterprise IT from having to learn, manage and deploy recoveries. DRaaS White Glove providers will do complete DR planning, including setting up the server reboot order so business-critical applications are the first to recover. Recovery is initiated by a simple phone call with the service provider doing all the work. And the best part is that DRaaS White Glove providers offer both 1-hour and 24-hour written Service Level Agreements (SLAs) for application recovery with financial recourse for any delays. This high-touch version of DRaaS can be managed and deployed from any location and protect remote sites around the world.

CONCLUSION

Your business is at a greater risk of an outage than ever before. As the volumes of data requiring protection increase and the complexity of data centers grow, the chances of a fast recovery diminish unless you are prepared, equipped, and trained in recovery. Unitrends offers all the components of a complete recovery architecture. Unitrends Recovery Series hardware appliances, Unitrends Backup software virtual appliances, Spanning Backup for SaaS applications, Unitrends Forever Cloud, and Unitrends DRaaS Services are fully integrated to protect an entire multicloud environment with no gaps in coverage or delay in recovery.

See for yourself how easy Unitrends products are to use to provide the highest levels of confidence that your data is protected and your applications will recover. Request a demo.

**READY TO PROTECT YOUR CLOUD?
WATCH A UNITRENDS DEMO NOW.**