UNITRENDS

CHECKLIST
4 STEPS YOU NEED TO TAKE TO FULLY PROTECT ALL YOUR CLOUDS

Introduction

Long gone are the days of a singular data center housing the entire computing infrastructure of an organization. Organizations have evolved to multicloud environments as data is increasingly dispersed across on-premises, remote endpoints, clouds and SaaS applications.

TechTarget defines *multicloud* as the "use of two or more cloud computing services… any implementation of multiple SaaS or PaaS cloud offerings… generally referring to a mix of public Infrastructure-as-a-Service (IaaS) environments such as AWS and Microsoft Azure."

Legacy business continuity and disaster recovery (BCDR) solutions were not designed to protect the heterogenous environments brought about by the shift towards multicloud. How do you protect a multicloud environment without suffering from overwhelming complexity or leaving gaps in coverage? You need a single recovery architecture, one that is complete and agile enough to protect all workloads across diverse environments, yet simple and elegant enough to seamlessly manage all backup deployments from a single interface.

What to look for in a recovery architecture

You have options with respect to building your recovery architecture – you could select each vendor based on their ability to protect certain workloads and craft a custom solution by stitching together various disparate components. The challenge with this approach is that many IT teams don't have the time and resources to keep up with and manage such a solution daily. This leads to potential gaps in coverage, underutilization of various management functions and procedures, time wasted hopping between siloed user interfaces (UIs) and negative impacts to the network.

Alternatively, you could opt to deploy a holistic, pre-integrated solution with all components designed specifically to optimize backup and disaster recovery functions without unnecessary complexity. You should look for an integrated data protection and recovery architecture. But how will you know whether all the features you need are completely integrated?

The following checklist outlines various aspects of a solution and breaks down their functions and importance to the solution.

FEATURE	DESCRIPTION	
Global Management Console	You should be able to manage protection across your multicloud environment from a single, unified console. This provides a single team with the ability to perform all protective functions regardless of whether the protected assets are on-prem, remote or in the cloud. Modularization of the interface and the ability to leverage SSO to reverse proxy into more granular controls cuts down on technician time spent switching between dashboards and portals.	☐
Single Vendor Support	When one element of your recovery architecture fails, you need a quick and timely resolution. Finger pointing between disparate vendors is all too common. You should look for a unified solution where every element of the data protection platform is supported under a single service organization 24/7/365.	☐
Automated Recovery Testing	The only way to know you can recover in an emergency is to test regularly, especially when changes are made to your infrastructure. Unfortunately, organizations don't always have the resources or budget to perform regular testing. New, intelligent tools are available by automating testing for local and remote assets to ensure all components are in place and capable of restoration. Look for a solution that integrates an automated recovery testing engine with the need for additional proxies or licensing.	☐
Centralized Disaster Recovery Strategy	Public cloud infrastructure, while robust, is not immune to **outages** that impact service delivery. Redundancy is critical in these situations to maintain continuity of local and/or cloud-hosted workloads. You should be able to failover any workload to singular Disaster Recovery-as-a-Service (DRaaS) regardless of workload size, criticality or where it originated from. DRaaS enables organizations to spin up applications in an independent cloud specifically tuned to failover and recovery use-cases.	☐
Bring Your Own Cloud Storage	Protecting cloud workloads can be expensive. A virtual appliance protecting cloud infrastructure is often run in the same cloud environment (for example, EC2) as the production workload. Utilizing production resources for backup and recovery increases public cloud costs. For protecting that data, you should have the choice to leverage a number of different approaches, whether by replicating to an alternate cloud service or utilizing Direct-to-Cloud technologies that mitigate the need for a local appliance.	☐
WAN-Optimized Replication	Moving data over the WAN, whether to or from the cloud, can be a cumbersome task, especially for larger data sets. In order to meet today's tight RTO and RPO SLAs, you need a solution that optimizes replication to efficiently move data from the source to the recovery target as quickly as possible in order to be ready for a recovery event. Look for a solution that utilizes a combination of WAN optimization and acceleration technologies, including, but not limited to, global, source-level deduplication, in-flight compression, encryption, source point querying, simple rate limits and bandwidth throttling.	☐
AES 256-bit Encryption	Encryption secures data privacy both at-rest and in-flight. Backups should be encrypted to secure data and meet regulatory and corporate requirements to protect that data from unauthorized access and theft. All data should remain encrypted until a request is made to restore the data.	☐
OAuth 2.0 Access Protocols	An estimated **80%** of security breaches involve a privileged account. Software and SaaS solutions that use service accounts to access applications put data at risk. To reduce the chance of comprise to a privileged account, look for a solution that utilizes the industry-standard OAuth 2.0 protocol to provide application-level authorization. OAuth 2.0 enables your backup solution to enable OAuth data transfers to take place in the Secure Sockets Layer (SSL) to ensure the most trusted cryptography industry protocols are being used to keep your credentials secure.	☐

4 Steps To Protect All Clouds With Unitrends Unified BCDR

At Unitrends, we've architected our Unified BCDR to provide users with the most complete, agile and secure solution in the marketplace today. We do so by offering support for more than 250 operating systems, hypervisors, applications and cloud formats, along with injecting automation and artificial intelligence to simplify complex systems, and help IT accomplish more with less.

Here are four steps you can take with Unitrends to protect your entire infrastructure:

01 **Protect On-Premises Data, Whether Local Or Remote**

02 **Protect Your SaaS Applications**

03 **Protect Public Cloud Workloads**

04 **Protect Everything With Disaster-Recovery-as-a-Service (DRaaS)**

1] Protect On-Premises Data, Whether Local Or Remote

Your environment may be complicated but protecting it doesn't have to be. You need to be able to protect everything in your data center as well as new data being created on endpoints and laptops by your remote workforce. Unitrends Recovery Series enables organizations with a turnkey, purpose-built backup and recovery appliance to protect physical and virtual systems, including emerging hyperconverged technology such as Nutanix AHV and VMware VSAN. A singular appliance is easier to install, upgrade and maintain. For an organization with multiple sites, look for a solution that allows you to manage all appliance deployments from a singular interface. Today's leading appliances natively protect all computing platforms, enable local recoveries to be run on the appliance itself, and converge supplemental capabilities, such as deduplication, compression, encryption, recovery testing, enterprise reporting and WAN-accelerated replication, without the need for add-ons and proxies. A local appliance may replicate to a secondary recovery target, such as another appliance or dedicated cloud service, to protect data and maintain continuity in the face of site-level disasters such as extreme weather, electrical failures or a cyberattack.

2] Protect Your SaaS Applications

SaaS providers, such as Microsoft 365 and Google Workspace, operate under a model of shared responsibility. It's up to you to protect corporate data in the cloud the same way you protect your local infrastructure. While cloud providers protect against data loss caused by system issues, customers are responsible for data loss caused by accidental or malicious deletions, third-party software errors, cyberattacks 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 Workspace 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 data protection solution must be part of a recovery solution architecture in order to 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 an active account. You can even roll back to a specific version of a file, folder or document library.

3] Protect Public Cloud Workloads

As is the case with SaaS applications, it's the subscriber's responsibility to protect data being generated in public cloud instances. The best technology for protecting public-cloud-based applications is the same that's 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 another cloud provider of your choosing.

For recovery of cloud workloads, it's optimal to use another cloud environment rather than spinning up applications in your local datacenter. That would require extensive and expensive spare computing and storage capacity. Many organizations have opted to transition to the cloud in order to relive themselves of that burden. Your solution should offer you the ability to choose where you back up and recover cloud-based workloads — either within another region of the primary cloud provider or to a different cloud provider.

4] Protect Everything With Disaster-Recovery-as-a-Service (DRaaS)

DRaaS has become an attractive option for organizations of all sizes. By partnering with a cloud provider who offers expertise in cloud recovery and has optimized their cloud infrastructure to support failover use-cases, you will have the highest levels of confidence in your ability to recover. Unitrends **DRaaS** supports recovery of local workloads as well as workloads operating in public clouds such as AWS or Azure. As a "white glove" service, Unitrends DRaaS frees an organization's IT from having to learn, manage and deploy cloud recoveries. The DRaaS provider works as an extension of your team to complete DR planning, configuration of the cloud recovery environment and recovery testing for full proof and confidence that pre-defined SLAs will be met. Recovery is initiated by a simple phone call with the service provider, who will then begin the failover sequence and aid local IT in rerouting network traffic to the DR site. Unitrends DRaaS offers 1-hour and 24-hour written SLAs for application recovery. This high-touch DRaaS can be managed and deployed from any location to protect headquarters as well as any remote sites located around the world.

Conclusion

Your data is at risk like never before. As the volumes of data requiring protection grow, the chances of a fast recovery diminish unless you are prepared, equipped and well-versed in recovery procedures. Unitrends enables organizations with a complete recovery architecture by combining local appliances, cloud-based SaaS protection, public-cloud virtual appliances and Direct-to-Cloud support for remote endpoints. Unitrends Cloud and DRaaS are fully integrated to offer you the ultimate protection for your multicloud environment with no gaps in coverage or delays in recovery.

See for yourself how easy Unitrends platform is to use and get complete confidence that your data is protected and your applications are fully recoverable.

Get started today!

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY

PART #WP-2091-ENG-B