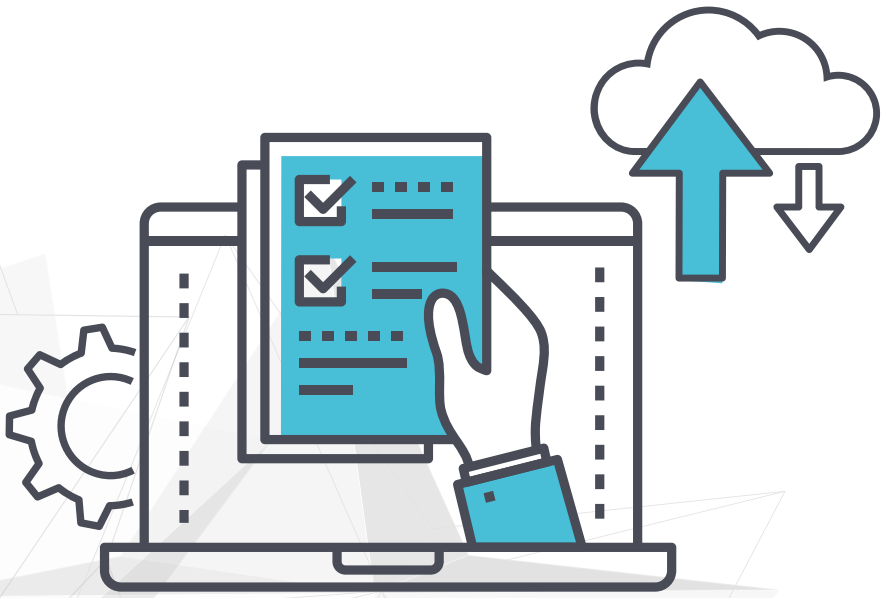
UNITRENDS

IT BUYER'S GUIDE: MICROSOFT AZURE BACKUP

SOLUTIONS TO OVERCOME DATA LOSS AND DOWNTIME



Introduction

Businesses of all shapes and sizes are increasingly leveraging the cloud to transform their business operations and gain an advantage over their competition. The Big Three cloud providers, namely Amazon Web Services (AWS), Microsoft Azure and Google Cloud, account for almost two-thirds of the worldwide cloud market share.

According to estimates from the **Synergy Research Group**, AWS remains the primary shareholder of the cloud market, with 32% of the total share as of the first quarter of 2023. However, its chief competitor, Microsoft Azure, is swiftly gaining market share. While AWS's figures have remained fairly consistent over the last five years (floating between 32% and 34%), Azure's market share has increased from 19% to 23% in just the previous two years, rapidly narrowing the gap with AWS.

With over 200 products and cloud services, Azure is an eminent cloud platform that can serve you well in your digital transformation journey. Companies of all sizes and maturities, including 95% of Fortune 500 companies, leverage Azure for their digital transformation. However, like every other technology platform, you must keep certain things in check while leveraging Azure if you don't want to risk treading deep water.

While migrating your data and workloads to Azure presents a whole range of opportunities, it also comes with risks. For instance, as you migrate your workloads to the cloud, security concerns such as data loss and privacy become more crucial than ever. According to a threat outlook survey by **Statista**, organizations worldwide expect the highest increase in cyberattacks to take place on their cloud services.

The shared responsibility model (SRM) of cloud security places the onus on the respective organizations to protect their data and workloads in their cloud tenant(s). According to the SRM, the provider is responsible for protecting the cloud infrastructure and networks. However, identity and access management (IAM), encryption and protection of cloud-based data fall into the customers' hands. In fact, most cloud providers' service level agreements (SLAs) warn that they may not be able to retrieve your data every time, and the SLAs even recommend third-party services for backing up your data. For example, Microsoft's SLA states: "We recommend that you regularly back up your content and data that you store on the services or store using third-party apps and services."

Microsoft offers native solutions — Azure Backup and Azure Site Recovery — to facilitate the backup and recovery of data stored in Azure. However, even the combination of both these services leaves gaps in protection. For instance, Azure Backup cannot egress (move) your data to a separate cloud environment, leaving your organization vulnerable to single-cloud risk and downtime. Native Azure services also come with variable per-incident charges, making it extremely difficult to calculate and forecast the total cost of ownership (TCO). Another big disadvantage of using Azure Backup is its disjointed nature. Azure Backup is a collection of multiple backup components that require piecing together for full functionality. Moreover, IT teams need extensive expertise in these native solutions to manage hybrid cloud environments. However, in today's macroeconomic situation, hiring in-demand Azure-certified technical professionals can be challenging and expensive.

The imminent risks of downtime and data loss force organizations today to look beyond native services for backup and recovery of their Azure data. On that front, third-party solutions can effectively tackle the security challenges while filling the gaps where Azure's native services fall short. This guide is designed to aid you in understanding the various options available in the marketplace today for backup and disaster recovery of Azure workloads. It will give you pivotal insights into the features you must look for while choosing the ideal solution for your Azure data. Let's see what attributes add up to make a perfect backup and recovery solution for Microsoft Azure.

How to Use This Guide

Once you acknowledge the significance of backing up your Azure data, choosing the right tool for the job is equally important. At first, you must be mindful of the requirements you expect from the solution. As you evaluate the hundreds of vendors and innovations available in the space, keep these key goals in mind:

Your solution must:

1. Eliminate single-cloud vulnerabilities
2. Streamline management
3. Reduce TCO of cloud infrastructure
4. Guarantee recoverability

Let's explore each one of these attributes in detail. At the end of each section, we have also created a concise checklist so you can quickly check whether your backup and recovery solution addresses each aspect.

Eliminate single-cloud vulnerabilities

Imagine backing up your data in a single place only to discover it's unavailable when you most need it. That's why it's essential to back up your data in multiple locations.

Whether you choose Azure native services or third-party solutions, production workloads may face the risk of public cloud outages. However, in the case of native Azure solutions, your data backups remain within the same Azure region. It's only very recently that **a networking outage took down the entire Azure platform** along with its services, such as Teams and Outlook. That's why storing your backup data in a redundant location away from your production Azure stack is critical.

Moreover, when leveraging native Azure data protection, your backup is stored behind the same login credentials as your production, which exposes your data backup to a wide range of threats like cyberattacks and malicious insiders.

While using third-party solutions, however, you must ensure that your solution supports replication to redundant cloud infrastructure, isolates your backup credentials and facilitates dynamic data mobility.

Feature to look for	What it achieves	
Replication to redundant cloud infrastructure	Secondary off-site replication does away with downtime and enhances your cyber resilience. The ability to spin up recovery infrastructure in the redundant cloud ensures you can meet aggressive recovery time objectives (RTOs).	
Backup credentials isolation	It ensures that your backup credentials are out of the reach of bad actors, even if your production credentials are compromised. This improves the resilience of your backup copies.	
Data mobility/failover	Ensures you can migrate data from on-premises to the cloud, cloud-to-cloud or from cloud to on-premises. This enables you to recover workloads outside the Azure cloud.	

Streamline management

Managing the backup and recovery of Azure data using native services can be an administrative nightmare, even for Azure-certified IT pros. Azure Backup is a collection of different backup components, including the Microsoft Azure Recovery Services (MARS) agent, Azure Backup Server, Azure IaaS VM Backup and System Center Data Protection Manager (DPM). None of these backup components can meet every backup requirement on its own thus requiring you to piece them all together for full functionality. Managing the multiple configuration settings of these components and depending solely on their capabilities can drastically affect the efficiency of your business continuity and disaster recovery (BCDR) process.

However, managing Azure data doesn't have to be complicated. With the right solution, you can streamline the entire BCDR process and eliminate the complexities involved. The key is to find a single platform that can replace the different cloud and legacy backup solutions.

Feature to look for	What it achieves	
A singular, all-in-one backup solution	Developing a BCDR strategy around a single backup solution eliminates any data silos and gaps in coverage. Since you do not have to piece together multiple vendors and contracts, you will have only one set of configuration concerns and one toolset to learn from. The centralized platform will act as the one common entry point for all your BCDR functions and services. A singular solution also means centralized management, a standard process and a unified support experience.	
Flexible recovery options	Look for a solution that offers flexible recovery options to address a variety of scenarios. These may include granular file and folder recovery, the ability to spin up new virtualizations in Azure, export VM images and the ability to spin up workloads in a redundant cloud environment should Azure services be unavailable.	
Streamlined recovery	The capability to streamline the entire recovery process via a single, intuitive interface that doesn't require manual scripting or mounting disks is paramount. This enables complete and rapid recovery of multiple files, folders or the entire disk within the specified RTO and RPO.	
Automation	Automation is a critical facet of the backup and recovery process. It ensures the regular backing up of Azure data while reducing the possibility of human errors. Automating key tasks, such as screenshot verification and DR testing, assures recoverability without manual configurations of instances and manual verifications that considerably drive up your TCO.	

Reduce TCO of cloud infrastructure

The cost of protecting your data and workloads in hyperscale clouds like Azure can be very unpredictable and complex to calculate. The variable fees cloud providers charge for data egress and the ad hoc usage of instances for things like DR testing and other services make accurate budgeting and forecasting nearly impossible and can balloon the TCO of your cloud infrastructure.

For instance, cloud providers charge high data egress fees when moving data from the cloud storage where it was uploaded. Unlike subscriptions, data egress costs are not fixed and are usually not negotiated in advance. They rack up as your business relocates its data, which could be due to various reasons like a change in your IT strategy, a new subsidiary acquisition or a venture into a new sector. Data egress costs can increase your organization's cloud budget by at least 20–30%. When it comes to BCDR-related functions, variable costs like data egress and the cost to spin up new VMs for verification and testing purposes must be kept in check to ensure your costs don't go through the roof.

Feature to look for	What it achieves	
Eliminate variable costs	Eliminating egress charges and other variable costs (associated with screenshot verification and DR testing) ensures there's no individual component-based billing. Look for a solution that offers all of the above services with a flat-fee pricing model for a predictable TCO.	
Third-party hosting	The ability to replicate your backups in a redundant, secure cloud data center that does not charge egress fees can be a huge advantage. This helps to overcome the risk of your single-cloud vulnerability while eliminating variable charges for replication and recovery.	
Licensing structure	A licensing structure based on the number of appliances or backup capacity will considerably increase over time as your environment grows. Look for a solution with a licensing structure that accounts for the managed disk capacity of your protected assets and includes backup retention. This will ensure that you have a cost-predictable model for the whole lifecycle of your Azure backups.	
Predictable retention plans	Accumulating backup retention can snowball your costs as data grows in the public cloud. The ideal solution should be able to offer specific retention periods for your data at a predictable price.	

Guarantee recoverability

Recovery testing with native Azure data protection solutions is highly time- and cost-intensive since it necessitates extensive manual configurations and involves high computing, storage, networking and DR costs. Another drawback is its inability to offer proper ransomware detection.

Consider the following features in your solution to eliminate uncertainty and gain 100% confidence in your recovery capability.

Feature to look for	What it achieves	
Immutable storage	Ensures your backups are stored in a secure and immutable format so they cannot be modified, changed or deleted until the specified retention period ends. Features like role-based access control can also come in handy while ensuring the integrity of your data backup.	
Backup frequency	Most solutions offer once-daily backups in addition to on-demand backups. However, they are inadequate to meet today's aggressive RPO and RTO requirements. Look for more frequent backups by default — like hourly — so you can rest easy knowing that your most recent data is secure and readily available in case you need it.	
Screenshot verification	Screenshot verification ensures that VMs boot correctly from backups and are recoverable. Look for a solution that offers automated verification to save you the time and cost it takes to perform manual spin-up.	
Ransomware detection	Advanced ransomware threats increasingly target backup and recovery infrastructures, especially those within the cloud. The solution must be able to detect ransomware threats at an initial stage to enable rapid response.	
DR testing	DR testing is the only way to know that you'll be able to meet your RTO and RPO goals during an outage. Look for a solution that includes automated DR testing for your workloads, alleviating the burden and cost of configuring manual testing in the cloud.	
Alerts	Automated, system-generated alerts will help you monitor hardware and software failures and immediately notify you of out-of-normal range events.	
Reporting	Smart reporting is another facet that you should look for in your solution. It will help you get detailed reports on different functions, including backup jobs, recovery operations, backup copies and storage usage, for distribution or analysis.	

Unitrends Backup for Microsoft Azure

Now that you know what features to look for in an ideal Microsoft Azure backup and recovery solution, take a look at Unitrends Backup for Microsoft Azure. The solution takes hourly backups of your Azure VMs and replicates them to the Unitrends Cloud for redundancy, where they can be spun up for disaster recovery. Regular screenshot verification and DR testing validate recoverability of backups.

GET A DEMO

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

© 2023 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

PART # WP-2063-ENG-E