CHECKLIST

Protecting Your Microsoft Azure Workloads

Your cloud workloads are at risk. Even as workloads move from on-premises to the cloud, human mistakes, like accidental deletion and scripting errors, malicious attacks, or real-world threats, such as natural disasters, can wreak havoc on your business continuity.

When you run workloads on Microsoft Azure, you agree to the **shared responsibility model (SRM)**. This means you, the customer, are responsible for protecting the data and other assets stored in Azure, whereas Microsoft holds the responsibility for the security of the cloud platform and its infrastructure — hardware, networks and services.

Although Microsoft Azure offers native solutions — Azure Backup and Azure Site Recovery — to facilitate backup and recovery, you must piece together the two offerings for full disaster recovery functionality. These offerings require manual configuration and carry high costs for computing, storage, networking and carry variable costs for backup verification, DR testing and data egress making forecasting total spend difficult. What's more, these solutions do not offer replication to a separate cloud environment, leaving you at risk of single-cloud outages and uncertain recoverability.

Using **third-party Azure backup solutions** is a smart alternative since they can ease the burden arising from the SRM and fill in gaps where native Azure backup services fall short.

Here's an in-depth look into the challenges in protecting your Azure workloads and the best practices to overcome them efficiently. Consider these criteria when evaluating a third-party backup solution for your Microsoft Azure workloads.

Single-cloud vulnerability

Whether you choose native Azure data protection tools or third-party solutions, there are risks of public cloud outages. In the case of the former, data backups remain within the same Azure region and are stored behind the same set of login credentials as production, leaving them potentially exposed to nefarious actors such as hackers and malicious insiders.

To improve your organization's preparedness in tackling such vulnerabilities, consider the following features:

Checklist: Eliminate Single-Cloud Vulnerability

Feature/Attribute	Description	
Replication to redundant cloud data center	Combats Azure downtime and ensures strong resilience against cyberattacks by storing backup data in a redundant location away from your production Azure stack. Secondary off-site replication guarantees better recovery time objectives (RTOs).	☐
Isolating your backup data	Isolating backup credentials ensures they're out of reach should production credentials be compromised. According to the UK's National Cyber Security Centre, the ideal process is to connect the backup to live systems only when necessary and not connect all the backups simultaneously.	☐
Data mobility/failover	Make sure your backup solution enables you to recover workloads outside the Azure cloud. Your backup strategy must support data migration from on-premises to the cloud, cloud-to-cloud or from cloud to on-premises.	☐

Management complexity

The complex nature of Microsoft Azure can overload your Azure-certified techs. Multiple configuration settings of native Azure business continuity and disaster recovery (BCDR) solutions or depending solely on Azure capabilities can bring down the backup efficiency, enhancing the total cost of your BCDR solution.

Take a look at the following best practices to avoid complexity in management:

Checklist: Best Practices to Avoid Management Complexity

Feature/Attribute	Description	
Singular backup solution	Creating a BCDR strategy around a single backup solution can be instrumental in eliminating data silos and any existing gaps in coverage. A singular solution means one set of tools, common processes and a unified support experience.	☐
Hourly backups	Once-daily backups are at odds with today's aggressive recovery point objectives (RPOs), while on-demand backups don't account for unplanned issues, result in non-routine retention and are difficult to manage holistically. Look for more frequent backups by default, for example, hourly, to ensure the availability of your backup data when needed, improve RTOs and simplify data protection management at-scale.	☐
Streamlined recovery	Instant virtualization of a virtual machine (VM) in a third-party cloud or restoring data in the Azure environment allows for rapid recovery in the event of an Azure disruption. Consider streamlining recovery via a single, intuitive interface that doesn't require manual scripting or mounting disks while enabling complete recovery of multiple files, folders or the entire disk.	☐
Automation	Automation ensures regular backing up of your Azure data, reducing the chances of human error. Automating key tasks, such as screenshot verification and DR testing, assures recoverability without manual configurations of instances and performing verifications manually that drive up your TCO.	☐
Ease of deployment	Signifies your solution is ready to use in just a few clicks. Smart features like screenshot verification, email alerts and automated testing make daily management hassle-free, increasing overall efficiency.	☐

Rising infrastructure costs

The costs for storing workloads in the case of hyperscale clouds like Azure are extremely unpredictable and complex to calculate. The variable fees for data egress, DR testing and failover make accurate forecasting and budgeting of infrastructure costs difficult.

Some of the best practices to bring down the ballooning infrastructure costs are mentioned below:

Checklist: Regulating the Rising Infrastructure Costs

Feature/Attribute	Description	
Eliminating variable costs	Eliminating egress charges for multicloud replication and variable costs (screenshot verification and DR testing) ensures there's no individual component-based billing. Instead, look for a solution that offers all of the above with a flat-fee pricing model for a predictable TCO.	☐
Priced by managed disk capacity	Solutions based on backup appliances capacity increase the cost over time as the backup set grows and retention builds. However, solutions that license against the managed disk capacity and include retention ensure a cost-predictable model during the lifecycle of your Azure backups.	☐
Predictable retention	When managing your own storage in the public cloud, building out backup retention can result in snowballing costs. The ideal solution should be able to offer specific retention periods for your data at a predictable cost.	☐

Uncertainty of recovery

The only way to check your recovery capability is to carry out regular testing. However, recovery testing with native Azure data protection solutions can be time-consuming since it requires intensive manual configurations and involves high computing, storage, networking and DR costs. Also, it fails to provide proper ransomware detection.

Consider the following features to eliminate the uncertainty of recovery:

Checklist: Eliminating the Recovery Uncertainty

Feature/Attribute	Description	
Hourly backups	Regular backups, especially hourly, can support more aggressive RPOs, thereby running additional backups on demand at any time. In comparison, Azure backup users can only run backups for around four hours.	☐
Screenshot verification	Screenshot verification ensures 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	Modern ransomware is increasingly targeting backup and recovery infrastructures, especially in the cloud. Detecting ransomware threats at an initial stage is, therefore, necessary to enable rapid response.	☐
Disaster recovery testing	DR testing is the only way to know you'll be able to deliver on RTO and RPO goals. Look for a solution that includes automated DR testing for your workloads, alleviating the burden and cost of configuring testing manually in the cloud.	☐

When it comes to holistic BCDR, Azure-native solutions fall short, requiring more than one backup solution to provide BCDR capabilities. Azure-native solutions fail to eliminate single-cloud risks and add complexity with manual tuning, monitoring and configuration.

Unitrends Backup for Microsoft Azure — a purpose-built solution for backup and disaster recovery of Azure VMs — changes the game. It offers single pane of glass management and easy deployment while streamlining daily operations — all at a predictable cost.

With Unitrends Backup for Microsoft Azure, you get hourly replication to the Unitrends Cloud, minimizing the single-cloud risk and ensuring rapid recovery in the event of downtime, cyberattack or other cloud outages.

WANT TO GET SUPERIOR DATA PROTECTION FOR AZURE VMS AT A PREDICTABLE TCO?

LEARN MORE AT

WWW.UNITRENDS.COM/AZURE

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over 30 years of focussing 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 #IN-9019-ENG- A