SECRETS TO

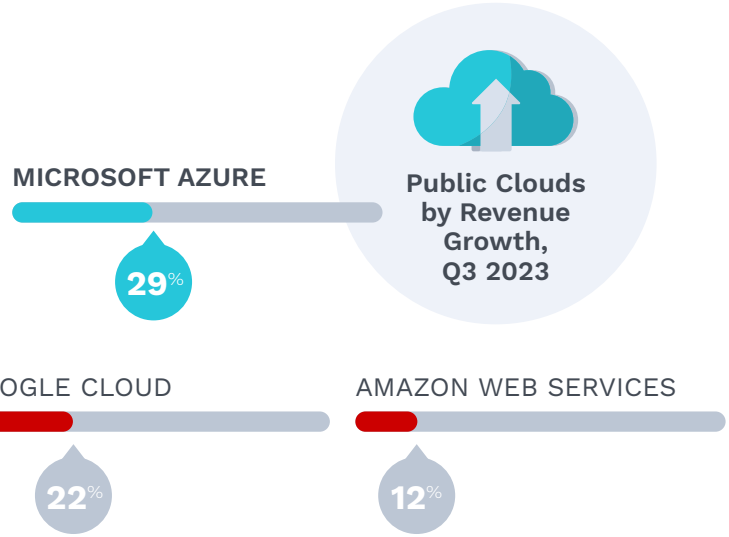
BUSINESS CONTINUITY AND DISASTER RECOVERY FOR MICROSOFT AZURE

UNITRENDS
A Kaseya COMPANY

INTRODUCTION

In this digital era, where data fuels business operations, the need for robust data protection has become even more critical, especially within cloud environments like Microsoft Azure. Azure is becoming the top cloud pick for small and midsize businesses (SMBs) and midmarket enterprises (MMEs). As per Microsoft's Q1 Earnings Report 2024, **Microsoft Azure's revenue increased 29% in the third quarter of 2023**, surpassing the growth of both Google Cloud (22%) and Amazon Web Services (12%).

When compared with other public cloud options, Microsoft Azure is often more affordable and provides better performance for important tasks like SQL — and the Microsoft ecosystem is a familiar one. Plus, it lets you extend cloud capabilities to on-premises infrastructure to optimize hybrid environments.

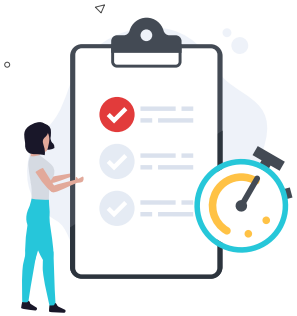


Microsoft Azure serves as a cornerstone for countless organizations, offering scalable and flexible computing and storage solutions. However, this convenience comes with the responsibility of safeguarding your sensitive information. Data protection in Microsoft Azure is essential for preserving the integrity, confidentiality and availability of your critical data.

In this eBook, we've outlined major data protection challenges in Microsoft Azure and provided key insights and strategies to overcome these challenges confidently. Read on to learn the secrets to business continuity and disaster recovery (BCDR) for Microsoft Azure.

WHY PROTECTING YOUR CRITICAL WORKLOADS IN MICROSOFT AZURE IS NON-NEGOTIABLE

Migrating workloads to the cloud offers numerous possibilities but comes with its own set of risks. It is also essential to remember that moving to the cloud doesn't free you from data protection responsibilities. Microsoft Azure and other hyperscale providers do not provide backup by default. Similar to on-premises systems, it's essential to back up cloud workloads. Having a plan in place for business continuity and disaster recovery of your critical Azure workloads is essential to overcoming any obstacles that come your way, including:



BUSINESS DISRUPTION EVENTS

Business downtime due to disruptive events, like power outages, hardware failures and natural disasters, is inescapable. As per a recent study by Hitachi Vantara, over 55% of IT infrastructure decision-makers surveyed said **technology downtime had a significant impact on their organization's revenue**.

Azure offers a 95% uptime **service-level agreement** (SLA) for virtual machine (VM) instances running Standard HDD Managed Disk. **This equates to up to 37 HOURS of DOWNTIME PER MONTH within SLA.** Additionally, there's no limit on the number of outages. You receive service credit when Azure fails to comply with SLA, but the repercussions on the business go far beyond the Azure VM bill.

INCREASED CYBERTHREAT LANDSCAPE

With cyberattacks becoming even more frequent and threatening, data security remains a top concern for businesses. According to Gartner's recent survey, an astounding 80% of CIOs surveyed said their **organizations will increase their cyber/information security investments in 2024**.

Even technology giants like Microsoft are not immune to cyberattacks. In 2022, **Microsoft faced over 1,400 attacks daily**. Altogether, the company mitigated over 520,000 unique attacks against their global infrastructure for the said period. As cloud adoption and reliance on cloud services continue to grow, the frequency of cyberattacks is poised to increase further in the foreseeable future. Having a BCDR plan for your critical Azure workloads is critical to navigating the threat-laden digital landscape successfully.

THE SHARED RESPONSIBILITY MODEL

When using cloud services like Microsoft Azure, it's crucial to bear in mind that ensuring data security in the cloud is a collaborative responsibility shared between you and your cloud service provider. **Microsoft Azure's shared responsibility model** clearly states that regardless of the service model, customers are responsible for protecting their data, endpoints, user accounts and access to their workloads.

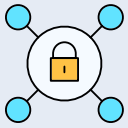
The table below shows the division of responsibilities for the Infrastructure-as-a-Service (IaaS) cloud service model.

FIGURE 1:
DIVISION OF RESPONSIBILITY IN MICROSOFT AZURE

MICROSOFT'S RESPONSIBILITY	RESPONSIBILITY	YOUR RESPONSIBILITY
	Information and data	✓
	Devices (mobile and PCs)	✓
	Accounts and identities	✓
	Identity and directory infrastructure	✓
	Applications	✓
	Network controls	✓
	Operating system	✓
✓	Physical hosts	
✓	Physical network	
✓	Physical data center	

CONSIDERATIONS FOR CLOUD CONTINUITY IN MICROSOFT AZURE

Building a comprehensive BCDR strategy for your Azure workloads requires careful planning. Here are three key factors to consider for maximizing protection for your Azure workloads and deriving more value from your IT investment.



✔ RESILIENCE

✔ CONFIDENCE

✔ AFFORDABLE COST

RESILIENCE

CHALLENGE

Relying on a single cloud leaves you susceptible to data loss and downtime.

REGIONAL OUTAGES

The proverb, "Don't put all your eggs in one basket," stands true for data protection as well. Microsoft's native offering, Azure Backup, cannot transfer your data to another cloud environment, exposing your organization to the risks of relying solely on one cloud and potential downtime. In January 2023, **Microsoft experienced a global outage lasting over five hours** due to network configuration issues, disrupting services globally.

RANSOMWARE AND MALICIOUS INSIDERS

When you choose native Azure data protection tools, your backups are behind the same set of login credentials as production data instances, exposing your data to a wide range of threats like ransomware attacks and malicious insiders.

SOLUTION

Multicloud backup and disaster recovery (DR) ensures your business never stops in the event of a crisis or disaster.

MAINTAIN CONTINUITY DURING AZURE OUTAGES

Unitrends Backup for Microsoft Azure replicates data to the independent Unitrends Cloud for redundancy and availability. Instant recovery in the Unitrends Cloud ensures continuity in a cloud-level downtime event.

RANSOMWARE DETECTION

Unitrends provides ransomware detection with built-in, native monitoring using our proprietary behavioral analysis. In the event of ransomware detection, administrators receive proactive alerts, prompting immediate action.

ISOLATE BACKUP DATA OUTSIDE AZURE

Secondary off-site replication minimizes the risk of downtime while enhancing cyber resilience. The Unitrends Cloud is invisible to would-be Azure attackers and stores your data immutably. Being able to spin up recovery infrastructure in the redundant cloud ensures even aggressive recovery time objectives (RTOs) can be met. Isolating backup credentials also ensures backups remain inaccessible to attackers even if production credentials are compromised.

IMMUTABLE CLOUD STORAGE AND CLOUD DELETION DEFENSE

Backups are stored immutably in a private and secure Unitrends data center. Immutable storage protects against cyberthreats while geographically distributed cloud locations ensure data sovereignty. Unitrends Cloud Deletion Defense acts as a recycle bin in the cloud, allowing you to recover data that's mistakenly or maliciously deleted.

CONFIDENCE

CHALLENGE

Achieving 100% confidence in meeting your SLAs in Azure requires taking full control and managing everything independently.

ONCE-DAILY BACKUPS

In today's increasingly unpredictable business environment, once-daily backups may not be enough to meet aggressive recovery point objectives (RPOs). Additionally, without backup verification, demonstrating the success and recoverability of your previous backup can be challenging. You don't know how long it will take to recover unless you test, and you don't want to wait to find there's an issue with backups when you actually need to restore them.

MANAGEMENT COMPLEXITY

While Microsoft Azure provides a host of capabilities, it also means added complexity for even Azure-certified IT professionals. Managing several configuration parameters and settings or relying solely on Azure capabilities can greatly impact the efficiency of your BCDR process.

MANUAL TESTING

Native Azure data protection solutions require extensive manual configuration for recovery testing, leading to elevated costs in compute, storage, networking and disaster recovery drills.

SOLUTION

Leverage automation to reduce the chances of human error and eliminate risks.

VERIFIED, HOURLY BACKUPS

More frequent and verified backups ensure your most recent data is secure and available for quick recovery if the need arises. Unitrends Backup for Microsoft Azure provides automatic, hourly backups and automated screenshot verification, ensuring backups have run successfully, booted correctly and are easily recoverable.

DR TESTING

Ensure recoverability without manual configurations of instances. Unitrends automates multiple tasks, including testing and screenshot verification, enabling you to achieve stronger RTOs and RPOs with proof and confidence that backups are reliable and bootable. We also offer support-assisted disaster recovery testing to ensure you're prepared to respond to an incident in advance.

PREDICTABLE COST

CHALLENGE

Unpredictable cloud spend and rising infrastructure costs, including costs for workloads, storage, egress, support and more.

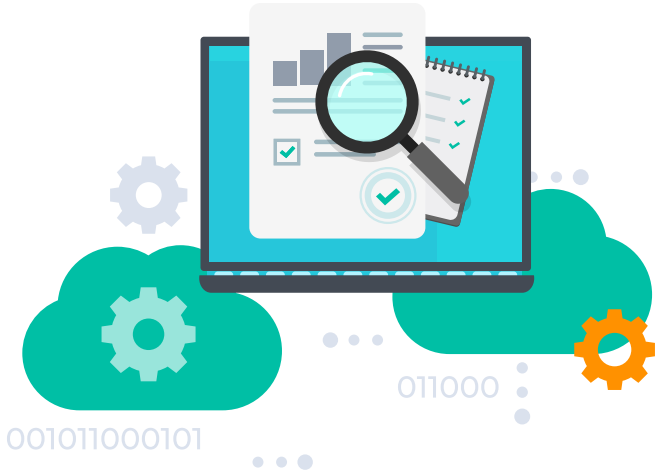
Azure Backup and Azure Site Recovery entail various incremental variable costs, including unexpected charges such as egress, storage, hosting and others. These costs may apply to restores, recoveries and tests, potentially causing a 20 - 30% increase in an organization's cloud expenses. This makes accurate forecasting and budgeting challenging. Additionally, the per-incident nature of many cloud services, like Azure, adds complexity to cost prediction. The native Azure backup solution lacks automation for verifying backups, requiring manual logins and steps, and you will pay for every instance you spin-up for testing.

It's crucial to note that native Azure solutions don't offer in-depth technical support by default. Enhanced support levels, featuring faster response times, high-severity escalations and architecture and operations support, are available as paid add-ons.

SOLUTION

Superior protection at an affordable cost. No more billing surprises.

Unitrends Backup for Microsoft Azure eliminates the uncertainty associated with cloud costs by providing a transparent monthly subscription fee. This fee encompasses all BCDR-related expenses, including egress and failover to the Unitrends cloud. Our solution facilitates multicloud continuity with easy deployment and efficient recovery capabilities, all bundled into a fixed monthly subscription fee for a simple, low cost. There are no variable charges for egress, storage, testing or failover. Our straightforward cost structure — a simple flat fee — includes hourly replication to the Unitrends Cloud, daily screenshot verification, DR and DR testing, without additional costs for stored data, performance or service levels.



SAFEGUARD CRITICAL AZURE WORKLOADS WITH UNITRENDS BACKUP FOR MICROSOFT AZURE

Unitrends Backup for Microsoft Azure tackles the significant challenges encountered by organizations like yours seeking to safeguard cloud-resident workloads. It mitigates risks associated with single-cloud vulnerability, uncertain recoverability, management complexity and gaps in cloud skills. Our solution elevates your organization's resilience, instills confidence in recovery processes and guarantees affordable DR costs.

Ensure the protection of your critical Microsoft Azure workloads through dependable multicloud backup and a simple, swift recovery process with Unitrends. Get a personalized demo with our backup specialists to discover how Unitrends strengthens your organization's BCDR strategy for Microsoft Azure.

BOOK A DEMO 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