



Azure VM Backup:

Why third-party
recovery is second
to none



About us

We're Redstor, your go-to for cloud-first data recovery. Our solutions make backing up, recovering, and protecting data effortless for businesses of all sizes. We streamline data recovery, so IT service providers and businesses can focus on growth and innovation.

Contents

Azure VM Backup: Why third-party recovery is second to none

- 04** Native tools are not enough

- 05** Growing risks demand resilient solutions

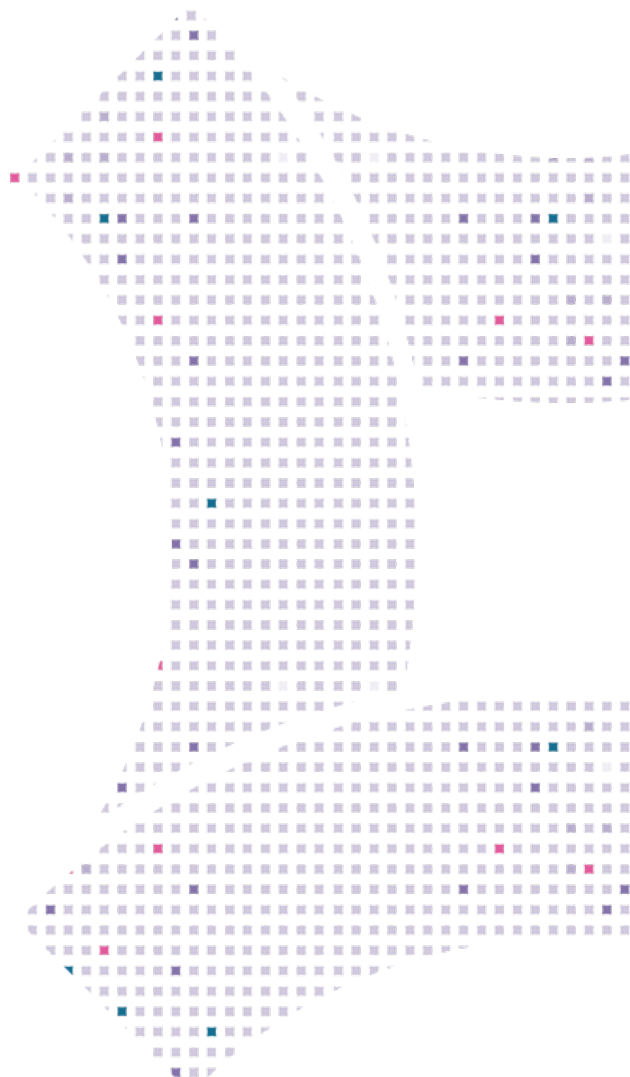
- 06** The importance of cyber resilience

- 07** Where Microsoft's backup falls short

- 08** How Redstor delivers more

- 09** Unlocking added value

- 10** Clear the roadblocks to digital transformation



Native tools are not enough

When budgets are tight, relying on a single cloud provider for both your live data and backup needs can seem like the right solution. But even Microsoft warns that this approach risks leaving your customers' data at risk.

In Microsoft's own words:

“We strive to keep the Services up and running; however, they are not offered with a guaranteed level of quality of service and all online services suffer occasional disruptions and outages. In the event of an outage or disruption to the Service, you may temporarily not be able to retrieve Your Content.

We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.”

This isn't just a service agreement – it's a warning. Microsoft admits that relying on its native tools alone isn't enough. Without a dedicated backup solution, the threat of cyberattacks, accidental deletions, misconfigurations, and outages looms large. You're only one mistake away from disaster.

Third-party recovery solutions not only strengthen security but also reduce costs, simplify pricing, and deliver long-term value. In this eBook, we'll explore the hidden risks of depending solely on native backup tools and show how advanced recovery solutions can unlock the full potential of your Microsoft environment. We'll also highlight how superior recovery options can increase profitability and open up new opportunities.

Growing risks demand resilient solutions

Cloud integration is skyrocketing, with 94% of enterprises now using cloud services.¹ The global cloud computing market is projected to reach **\$1.6 trillion by 2030**, up from \$446 billion in 2022.²

But as cloud adoption accelerates, so do the threats that come with it. The modern digital landscape is fraught with risks that can jeopardise your customers' operations.



1. Data breaches and leaks

Misconfigured services, unprotected endpoints, and sophisticated attacks have made data breaches alarmingly common. A single breach can cost businesses millions, and Azure isn't immune to vulnerabilities.

2. Ransomware and malware attacks

Ransomware attacks have become a billion-pound industry. Cybercriminals often target cloud systems to lock businesses out of their data or steal it outright. Malware can also lie dormant in backups, waiting to be unleashed during recovery.

3. Phishing and impersonation scams

Microsoft's popularity makes it a prime target for phishing attacks, with the company accounting for **32% of all brand impersonation attempts**.³ These attacks can trick employees into granting access to critical systems, putting your customers' data and operations at risk.

4. Hardware failures

Even global cloud providers like Microsoft experience outages that disrupt business continuity. Hardware failures can cause significant downtime and data loss, especially if backups are stored in the same environment as live data.

5. Insider threats

Employees or contractors with access to sensitive data can pose significant risks either intentionally, by leaking information, or accidentally, through misconfiguration or phishing.

¹ [Cybersecurity Stats: Facts And Figures You Should Know](#)

² [Cloud Computing Market Size to Reach USD 2297.37 Bn by 2032](#)

³ [Exploring Q4 2024 Brand Phishing Trends: Microsoft Remains the Top Target as LinkedIn Makes a Comeback](#)

The importance of cyber resilience

With such a wide range of threats, failure is inevitable. It may not happen today or tomorrow, but without the right protection in place, that's not a chance you want to take – and nor do your customers.

Whatever the cause of data loss, the most important thing is how you recover. That's why having a bulletproof recovery plan is essential.

As cyber risks escalate, organisations are turning to **cyber resilience** both to prevent failures and to respond decisively when they occur. The National Institute of Standards and Technology (NIST) defines cyber resilience as:

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources”.

At its core, cyber resilience depends on the speed and reliability of data recovery. Whether it's a ransomware attack, hardware failure, or accidental deletion, the ability to recover quickly and protect business continuity will define the outcome for you and your customers.

An unreliable recovery plan jeopardises your customers' operations when they need you most. Speed and reliability aren't just technical goals – they're critical to safeguarding your reputation, minimising financial losses, and securing long-term trust from your clients. Incomplete backups and hidden vulnerabilities simply don't cut it.

Where Microsoft's backup falls short

Microsoft's basic safety net for Azure VM users is just that – basic. Relying solely on native tools can leave organisations exposed to unexpected costs, recovery delays, and data loss.

Let's examine three critical gaps.

1. Single point of failure

Relying solely on Microsoft for both your operational data and your backups puts all your eggs in Microsoft's basket. With one outage, disruption, or attack, you risk losing access to both datasets.

Microsoft is known to experience outages. Without third-party data backup, organisations risk being unable to recover when it matters most. Diversifying your recovery strategy ensures your backups remain accessible, even if your primary cloud provider is offline. Separating operational data from backups allows users to add a critical layer of redundancy.

2. Weak malware protection

Never assume that just because you have a backup saved, you're protected. Malicious payloads often lie dormant in backups until it's time to recover, trapping businesses in an endless cycle of reinfection.

While Microsoft provides some capabilities to quarantine files and data, these measures are far from comprehensive. Third-party recovery tools leverage advanced threat detection tools to screen backups before restoration, automatically quarantining malicious files. This proactive approach neutralises both known and emerging malware threats, ensuring every recovery is clean and safe.

3. Slow and costly recovery

In today's agile business landscape, cyber resilience demands rapid access to your data to maintain operations. Prolonged downtime impacts not only your bottom line but also your long-term reputation.

Microsoft's Azure snapshots are not true backups. They can be deleted, lack long-term retention, and become expensive over time by being billed as disk storage. Third-party recovery solutions solve these problems by offering flexible, cloud-based options that deliver faster access and predictable pricing.

How Redstor delivers more

Redstor's Azure VM Backup is built to empower partners by accelerating data recovery, simplifying operations, and driving revenue. Thousands of customers worldwide trust us to protect and manage their data with confidence. Here's why:

Faster recovery, guaranteed resilience

Redstor delivers instant access to files. This enables businesses to resume operations in seconds, even before the full recovery process is complete. Minimising downtime is vital for maintaining customer trust.



InstantData™ technology: Recover entire VMs or individual files instantly, without waiting for full downloads.



Granular restores: Retrieve only what you need, eliminating slow and unnecessary full restores.



Complete VM state capture: Restore entire configurations, including storage and network settings.

Security without compromise

Redstor ensures that data remains secure, accessible, and compliant. With ransomware threats rising and complex compliance rules across different jurisdictions, it's never been more important to stay on top of requirements.



Immutable, off-site backups: Tamper-proof storage prevents ransomware attacks and unauthorised deletions.



Data sovereignty assured: Multiple storage regions support compliance with local and global regulations.



End-to-end encryption: Military-grade AES-256 encryption secures data from backup to recovery.



Lower costs, higher efficiency

The biggest cost driver for native Microsoft users is data volume. Predicting factors like retention length and backup duration can feel like guesswork, with costs quickly spiralling. Service providers who switch to Redstor often see their **costs drop by 2x to 4x**, delivering immediate savings and long-term value:



Predictable pricing: With a flat monthly fee, Redstor eliminates unpredictable charges for storage, data transfer, or egress to avoid surprises.



Cross-sell ready: Azure VM Backup integrates seamlessly with Microsoft 365, Azure Blob, and Entra ID, allowing partners to bundle and increase customer lifetime value.



No hardware: Redstor is fully cloud-native with zero infrastructure costs, reducing overhead and complexity.

Unlocking added value

As a former MSP, Redstor understands the unique challenge of managing separate recovery solutions. We know the complexity of multiple cloud providers and on-premise systems, as well as how they can quickly drive up costs and compromise efficiency.

We built our backup and data recovery solution to address these issues. Here's how:



Multi-tenancy: Manage multiple clients effortlessly with one tool. Our customisable dashboards and straightforward provisioning save time and streamline administration.



Comprehensive coverage: Protect everything through a single platform, from your entire Microsoft suite to cloud platforms like Google Workspace and on-prem systems.



Enhanced customer communication: Offer your clients a co-branded app with built-in recovery capabilities to boost customer satisfaction and reduce overheads.



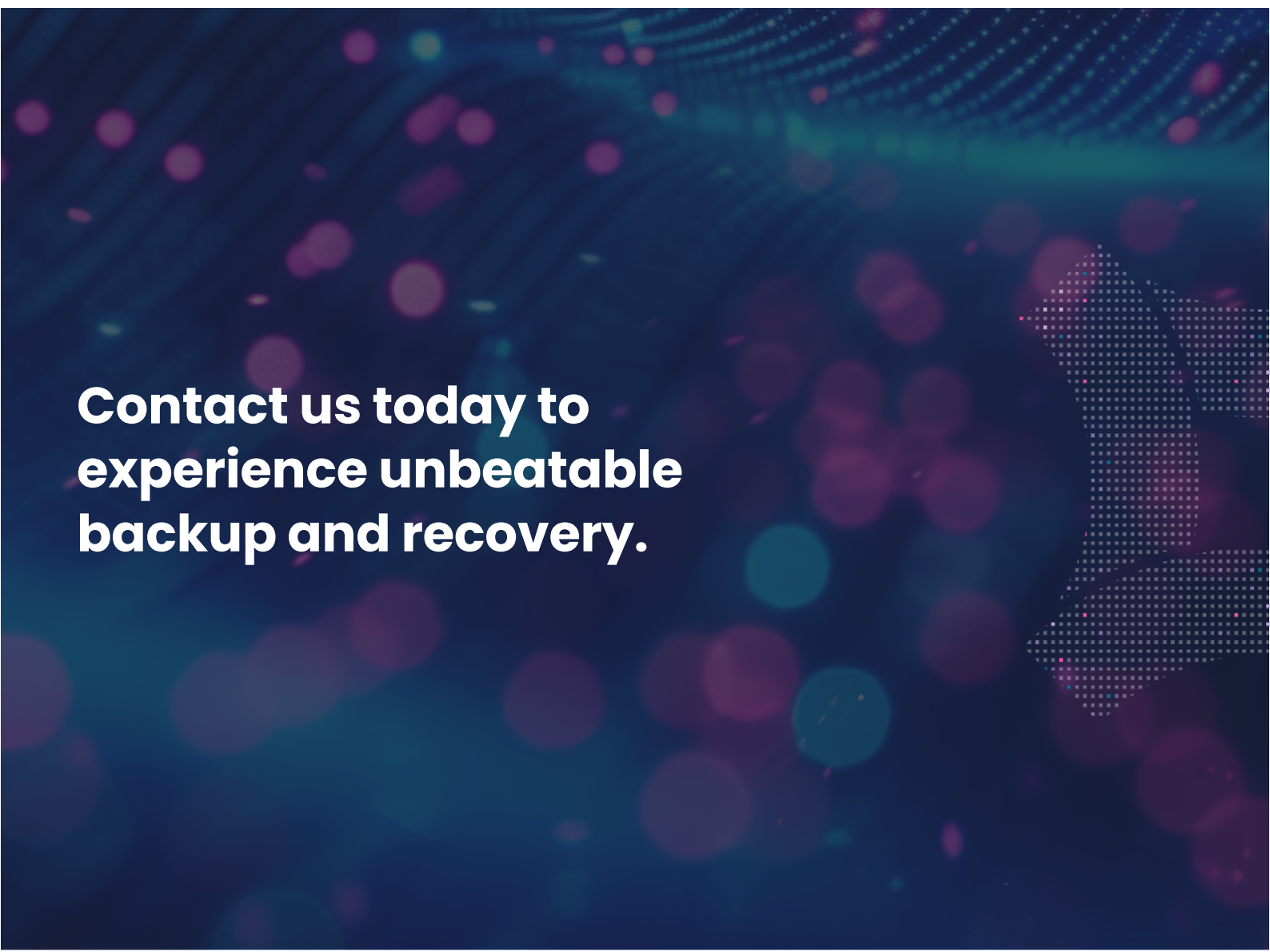
Cloud-first simplicity: Fully cloud-native and agentless, our solution eliminates the need for costly staging hardware or error-prone scripts. Scale protection effortlessly, reduce administrative burdens, and start securing data with just a few clicks.

Redstor doesn't just cut costs for data backup and recovery – we simplify your operations across services. By improving efficiency and lowering the total cost of ownership (TCO), we make it easier for you to deliver unbeatable value to your customers.

Clear the roadblocks to digital transformation

The cost, security, and operational complexities of cloud migration can leave end users in despair. Redstor's ability to scale data recovery across environments through predictable pricing clears a major obstacle to their digital transformation journey. This lets you focus on delivering exceptional services to your customers while highlighting the simplicity and power of your offerings.

Native tools are not the answer. Nor is complex hardware with hidden costs. By diversifying risk management with Redstor, you can help your customers avoid the vulnerabilities of relying entirely on Microsoft and put your worries to rest.



**Contact us today to
experience unbeatable
backup and recovery.**