eBook

datto
A Kaseya COMPANY

Know the 3 pillars for business continuity in Microsoft Azure

The cloud isn't optional anymore. It's where modern businesses run now. Small and midsize businesses (SMBs) are embracing cloud platforms like Microsoft Azure for their scalability, flexibility and lower infrastructure costs. However, what often gets overlooked with this shift to the cloud is the risk associated with data protection. Many IT teams underestimate the gaps in cloud data protection. The biggest one among that? The shared responsibility model of cloud security that Azure operates on.

In this model, Microsoft secures the physical infrastructure, network and hosts. Everything else — your data, applications, configurations and user access — is your responsibility. If a disgruntled employee deletes data or ransomware locks you out, Microsoft won't restore anything. These scenarios aren't covered under their service level agreement (SLA). For instance, 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."

Meanwhile, cyber insurance is making things even tougher for businesses. Policies now demand air-gapped backup copies, geographically distributed storage, unique credentials for backup environments and a tested failover plan that can spin up a hot site if your primary systems go down. If you don't meet any of these requirements, your application for coverage or any future claim could be denied.

As threats targeting cloud data grow and cyber insurance demands tighten, are you confident you can stay in control and keep the business running no matter what comes your way? This eBook reveals three critical foundations every internal IT team must have to protect their Azure workloads and keep business operations running without disruption.

How to achieve resilient continuity in Microsoft Azure

To secure Azure workloads and ensure true business continuity, IT teams need proactive planning. Here are three key pillars to consider, which will not only strengthen your Azure environment but also help you get more value from every dollar of your IT investment:

Pillar 1: Resilient backups

Because recovery is only possible if your backups survive the attack

The challenge: Does backing up still back you up?

Modern ransomware attacks don't just go after your production environment — they go straight for your backups. Once backups are deleted, altered or encrypted, recovery becomes impossible. That's why backups must be built with resilience from the start. Redundant, encrypted, immutable and always ready to restore. If even one layer fails, continuity is out of reach.

Same cloud, same risk

However, strong backups aren't enough if they're sitting in the same environment as everything else. If your data, apps and backups all live within the same tenant or cloud region, a single compromise or outage can take down your entire operation. The old saying holds true in data protection: Don't put all your eggs in one basket. It's especially relevant when your entire business relies on access to data.

On July 30, 2024, Microsoft Azure experienced a 10-hour global outage.[1]

Businesses relying solely on Azure services had no access, no recovery path and no control during the downtime.

Insurance demands separation

Cyber insurance providers and third-party auditors are catching on. Many now require separation between production and backup environments, often mandating that organizations use different vendors for each. The goal? Reduce vendor lock-in and eliminate single points of failure — because no platform, not even Azure, is immune to disruption.

The solution: Datto ensures your business stays online, no matter the disruption:

Datto's multicloud backup and disaster recovery solution gives IT teams the control, flexibility and protection they need. Even if a disaster strikes, your business keeps running.

1-Click Disaster Recovery (DR) in Datto Cloud

In the event of an outage, you can instantly spin up critical workloads in the purpose-built Datto Cloud with Datto's patented 1-Click Disaster Recovery feature. You can clone virtual machines (VM) and network configurations from previously successful DR tests, eliminating the need to manually reconfigure settings during an actual disaster. Your operations don't stop, even if Azure does.

Built-in ransomware and anomaly detection

You get automated scans for signs of ransomware, unauthorized encryption or unusual file behavior. When threats are detected, you're alerted immediately so you can act fast before damage spreads.

Isolation by design

Datto stores your backups completely outside of Azure, making them invisible to attackers who've breached your primary tenant.

- **Immutable: Backup data can't be altered or deleted — even by admins.**
- **Encrypted: Data is protected in transit and at rest.**
- **Separate credentials: Access is managed through an independent interface with enforced multifactor authentication (MFA).**

This layered isolation ensures attackers can't touch your recovery infrastructure even if they gain access to your Azure environment.

Global reach, local compliance

Datto maintains a global network of geographically distributed data centers. This gives your backups true off-site protection while keeping data within the country of origin to meet regulatory requirements. Whether you operate across borders or within a single region, you get redundancy without violating compliance.

Pillar 2: Reliable recovery

Because a backup is useless if you can't recover it — fast

The challenge: Can you really recover what you've backed up?

Meeting SLAs isn't about just having backups — it's about having full control over recovery. With Microsoft Azure's native recovery capabilities, that control is limited and fragmented, forcing IT teams to piece together a recovery strategy across multiple services. Confidence in recovery drops when every step adds friction.

Once a day isn't always enough

Azure Backup defaults to one backup per day. To increase frequency, you'll need an Enhanced Policy, which raises snapshot usage and nearly doubles your monthly costs. More backups mean more data, more expense and still no built-in verification to ensure those backups can be restored when needed.

Two tools, one problem

To get full business continuity and disaster recovery (BCDR) coverage in Azure, IT teams must juggle both Azure Backup and Azure Site Recovery. These tools operate in silos with distinct functionalities, policies and configurations. The result? Extra admin time, more complexity and reduced overall efficiency.

Recovery testing takes a toll

Backup testing in Azure is a manual process. That means more work for IT, more room for error and more costs creeping in over time. Regular testing is essential for real recovery confidence — but with native tools, it's rarely fast or simple.

The solution: Recovery that's proven, not assumed

Backups don't matter unless you can trust them to recover what you need when you need them. Real confidence comes from knowing that your backups have been tested and verified and are always recovery-ready.

Hourly backups with built-in verification

With Datto's automated screenshot verification, backups are verified daily to ensure VMs can boot and recover correctly. This eliminates the need for manual spin-ups and cuts the risk of recovery failure — saving both time and admin effort.

DR testing without the overhead

Regular testing is the only way to be sure you'll meet your recovery time objective (RTO) and recovery point objective (RPO) targets. No-cost DR testing in the Datto Cloud enables you to predefine and test against your DR runbook — should disaster strike, you'll be ready to restore with minimal manual overhead.

1-Click Disaster Recovery

When every second counts, recovery should be instant and seamless. With pre-defined runbooks built from tested backups, you can spin up orchestrated recovery with a single click via the 1-Click DR feature. No manual steps. No chaos. Just controlled, predictable recovery when you need it most.

Pillar 3: Cost control

Because resilience shouldn't come with runaway costs

The challenge: When the meter never stops, budgets break

In Azure, the meter is always running, and for IT teams working with tight budgets, that's a serious problem. Every service, every test, every byte moved has a price tag — and it adds up fast.

Unpredictable costs, everywhere you look

Cloud infrastructure costs are rarely straightforward. Between storage, production workloads, snapshots, DR testing, replication and support, Azure expenses are spread across multiple services and tiers — and most aren't fixed.

- **Service and resource usage fees are variable and complex.**
- **DR testing and failover incur additional virtualization charges.**
- **Data moved between regions or clouds triggers egress fees that spike unpredictably.**

These hidden costs often go unnoticed until the bill arrives.

The hidden drain: Data egress fees

Data egress fees — charged when data moves out of Azure's cloud — are rarely negotiated up front, yet they can drastically inflate your cloud budget. Whether you're recovering data across regions, replicating it to a new cloud or shifting infrastructure due to business changes, these fees follow.

Data egress costs can increase total cloud spend by 20–30% — often without warning.

Impossible to predict, harder to justify

In hyperscale environments like Azure, pricing your full continuity plan is anything but simple. The more features you need, such as DR testing or cross-region recovery, the more variable your costs become. Forecasting becomes guesswork. And the total cost of ownership climbs without clear justification.

The solution: Full continuity without the surprise costs

Controlling cloud costs shouldn't feel like chasing a moving target. Datto offers a simple, predictable flat-rate subscription that covers your entire BCDR plan — no hidden fees, no unexpected bills and no compromises.

One flat fee, everything included

Your flat-rate subscription includes everything: backup, automated screenshot verification, replication to the Datto Cloud, disaster recovery testing and full failover capabilities. There are no variable charges for data egress, storage, testing or recovery — so you can plan confidently without watching the meter.

Now, forecast, manage and justify your BCDR costs to stakeholders. Get the resilience you need with the budget control you demand.

Secure your Azure environment with Datto Backup for Microsoft Azure

When it comes to protecting your Azure workloads, there's no room for compromise. Datto Backup for Microsoft Azure gives you the all-in-one business continuity and disaster recovery solution your team needs — without the hidden costs, complexity or operational burden of native Azure tools.

Why stitch together multiple Microsoft services, pay more and still fall short on critical features like automated daily screenshot verification? With Datto, you get tested, isolated, recovery-ready backups, built-in DR testing and one-click failover — all under one simple subscription.

1. https://www.forbes.com/sites/kateoflahertyuk/2024/07/31/microsoft-confirms-new-outage-was-triggered-by-cyberattack/

No silos. No surprises. No stress.

TAKE THE PRODUCT TOUR

And see how Datto can keep your business running — confidently, continuously and without compromise.

About Datto

As a leading global provider of security and cloud-based software solutions purpose-built for managed service providers (MSPs), Datto, a Kaseya Company, believes there is no limit to what small and medium-sized businesses (SMBs) can achieve with the right technology. Datto's proven Unified Continuity, Networking, Endpoint Management and Business Management solutions drive cyber resilience, efficiency and growth for MSPs. Delivered via an integrated platform, Datto's solutions help its global ecosystem of MSP partners serve over one million businesses around the world. From proactive dynamic detection and prevention to fast, flexible recovery from cyber incidents, Datto's solutions defend against costly downtime and data loss in servers, virtual machines, cloud applications or anywhere data resides. Since its founding in 2007, Datto has won numerous awards for its product excellence, superior technical support and rapid growth, and for fostering an outstanding workplace. With headquarters in Miami, Florida, Datto has global offices in Norwalk, Connecticut as well as Australia, Canada, Denmark, Germany, the Netherlands and the United Kingdom.

datto
A Kaseya COMPANY