

Business Continuity and Disaster Recovery (BCDR) for Microsoft Azure

G-Cloud 15

IT Auxilium Ltd
E: hello@gpitservices.co.uk
T: 01223 827 410

Backup for Microsoft Azure

Business continuity and disaster recovery solution for Microsoft Azure workloads – at 30-50% lower cost than native solution.



Backup for Microsoft Azure is a unique business continuity and disaster recovery (BCDR) solution, delivering a customized and profitable BCDR practice protecting customers' critical business infrastructure residing in Microsoft Azure.

1,400+ daily cyberattacks on Microsoft Azure

With its growing popularity, Microsoft Azure became one of the primary targets for cybercriminals, and businesses must realize that no infrastructure is immune to cyberattacks, including public clouds.

While preparing robust business continuity and disaster recovery plans for Azure, MSPs face several challenges:

Whopping 98% of ransomware targets backups first

If you choose native Azure data protection tools or third-party solutions enclosed in Azure, you are increasing the risks of backups being inaccessible, as they are stored under the same organization account, or compromised by sleeper ransomware variants – exactly like if you were to keep backups of your on-premises servers on the same premises.

High costs of native solutions

Hyperscale clouds are notorious for an attractive "cheap" price, but ending up being expensive due to the complex web of costs for workloads, storage, egress, support, etc. While the price may look attractive on the surface, the total cost often are higher than all-in-one solutions.

Management complexity weighs on technicians

Microsoft Azure is an extremely powerful hyperscale cloud with a lot of capabilities, which comes with complexity. Adding dozens of configuration parameters and settings – and the lack of built-in integrations with your technology stack – can reduce the efficiency and profitability of your BCDR practice.

Backup for Microsoft Azure

Backup for Microsoft Azure is purpose-built: It offers single-pane-of-glass management, easy deployment, and streamlined day-to-day operation, all delivered at a simple pricing, 30%-50% lower than native solution.

It offers hourly replication to the "invisible", secure Cloud that eliminates single-cloud risk to provide rapid recovery during downtime, cyberattacks and outages.

Enterprise-grade protection

- **Trusted, comprehensive BCDR** built on proven SIRIS technology, delivering consistent management and protection from endpoint to server to cloud.
- **Outstanding resilience** with secondary offsite replication to the secure, reliable Cloud, which ensures better RTO and eliminates single-cloud risk.
- **Secure architecture** protects each client with a single-tenant model and encrypted disks.

Rapid and reliable recovery

- **Multi-cloud continuity** with hourly backups to the secure offsite Cloud, enabling maximum redundancy and optimal RTO/RPO.
- **Rapid recovery** by instantly virtualizing a VM (virtual machine) in the Cloud or restoring it to the original Azure environment.
- **Streamlined restore** via a simple recovery process managed through a single, intuitive interface, allowing recovery of multiple files, folders or the entire disks as required.

Built to scale

- **Profitability and predictability** with unique licensing and pricing, lower by 30-50% than the native solution, and no surprise fees – £0 egress for multi-cloud replication, £0 DR and £0 DR testing.
- **Single pane of glass** to manage on-premises and Azure backups, organised in a client-centric view for consistent data protection.
- **DR planning & support** helps with planning, tests, actual recoveries/restores and live disaster support.
- **Easy deployment and day-to-day management** from a turnkey solution that is ready to use in a few clicks, increasing efficiency with smart features like screenshot verification, automated testing and email alerts.

How it works

Backup for Microsoft Azure backs up your clients' virtual machines (VMs) to the our owned Azure tenant. Every hour, the backups are replicated to the Cloud for an extra layer of protection.

Our Cloud

The Cloud is purpose-built for cloud backup and disaster recovery. Its immutable architecture sets the standard for a secure cloud infrastructure with features like Cloud Deletion Defense.

- **Multi-regional presence** to help you support geographically redundant backups.
- **Consistent stack** for you to protect client PCs, SaaS apps and servers.
- **Cloud Deletion Defense** for protection against ransomware, enabling access to deleted cloud snapshots when an agent is either mistakenly or maliciously deleted.
- **Virtualization to Cloud** within minutes when you need to recover workloads outside of Azure.



Considerations for building your cloud practice

There are many things to consider when building your BCDR offering for Azure workloads. In this eBook, we'll walk through three key areas you need to understand in order to be well-equipped to offer BCDR in the cloud:

- Protections
- Cost
- Management

But before covering these areas, we recommend first walking through the fundamentals of BCDR on Azure.





Microsoft Azure grew by 29% in the third quarter of 2023, outpacing Google Cloud (22%) and Amazon Web Services (12%).¹

Why build your cloud practice on Azure?

Flexible hybrid capabilities

Azure meets customers where they are in their cloud journey by providing strong options for enabling hybrid cloud implementations. For example, Azure solutions can extend modern cloud capabilities, like elastic scale, automation and unified management, to on-premises infrastructure.

Comprehensive compliance portfolio

Azure boasts one of the most comprehensive portfolios of compliance offerings among cloud providers, covering global, industry and government-specific regulations, including GDPR, HIPAA, NIST, FedRAMP and more — making it easier for customers to meet their regulatory requirements.

Innovative technology and open-source integration

Multiple Azure cloud services offer integration with open-source software and development platforms such as Linux, Kubernetes, .NET and more. This provides a future-proof platform that enables you to run and develop workloads more flexibly and innovate more freely in cloud-first, on-premises and hybrid setups.

¹ <https://www.cnbc.com/2023/10/27/microsoft-azure-outpaced-aws-and-google-cloud-in-latest-quarter.html>



When you run workloads in Azure, the responsibilities for security and data protection are shared between Microsoft and you, the customer.

Microsoft Azure shared responsibility model for IaaS

As we mentioned earlier, when you run workloads in Azure, the responsibilities for security and data protection are shared between Microsoft and the customer. This visual below gives you a breakdown of how exactly these responsibilities are split.

Microsoft Azure Responsibility		Customer Responsibility
	Information and data	X
	Devices (mobile and PCs)	X
	Accounts and identities	X
	Identity and directory infrastructure	X
	Applications	X
	Network controls	X
	Operating system	X
X	Physical data center	
X	Physical hosts	
X	Physical network	



Downtime can limit revenue and prevent employees from working. Thus, maximizing uptime is key to business success.

How MSPs approach data protection today

To meet their portion of the shared responsibility model, many MSPs currently use one of the following solutions:

- **Cloud-native backup and recovery services:** A cloud service offered by Microsoft to enable local- or geo-redundant backups and recovery.
- **Third-party BCDR tools in Azure:** Independent software vendor (ISV) offerings that protect data natively in Azure.

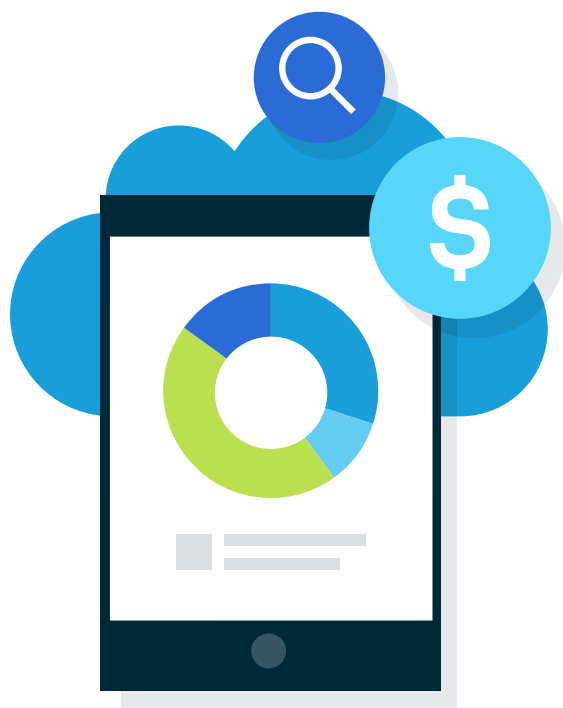
Protection

Challenge: Single-cloud solutions are susceptible to downtime

Downtime can limit revenue and prevent employees from working.

Thus, maximizing uptime is key to business success, but using a traditional, single-cloud solution to accomplish this still bears some risk for business continuity:

- **Worldwide outages:** If all your business-critical workloads are in Azure, they are still susceptible to downtime scenarios in the event of a widespread outage.
- **Ransomware:** It's common for organizations to only back up important data using native tools available in Azure. However, this means those backups are all behind the same Azure account and can potentially be held hostage in the event of a ransomware attack.
- **Backups every 24 hrs:** Common, daily backups won't suffice for some customers. Plus, if your solution doesn't offer backup verification, it can be difficult to prove that a previous backup was successful and is bootable.



As you begin supporting workloads in Azure, it's important to understand the differences in resource costs and payment models compared to on-premises infrastructure.

Solution: Multicloud backups

To differentiate your BCDR offering, we recommend delivering extra protection beyond the standard offerings of traditional business continuity solutions. For example, utilising Backup for Microsoft Azure — our cloud BCDR offering purpose-built — allows you go to beyond basic backup and recovery to offer multicloud protection:

- **Stay up and running during Azure outages:** Backup for Microsoft Azure provides backup and failover to the Cloud with no extra fees for data egress.
- **Gain extra protection against malicious attacks:** Backups are kept secure behind a separate account and separate management portal located outside of Azure for additional reassurance of safety.
- **Verified backups every hour:** More frequent backups and verification means you can better optimize your recovery point objective (RPO) and confirm your backups are both working and bootable.

Cost

Challenge: Unpredictable spending limits BCDR margins

As you begin supporting workloads in Azure, it's important to understand the differences in resource costs and payment models compared to on-premises infrastructure. Migrating to Azure enables organizations to shift from CapEx to OpEx spending models — meaning they pay only for what they use in the cloud.

While this shift can bring about newfound flexibility to many organizations, it also brings some unpredictability in cloud spending month to month. For some this is a challenge because they need to properly understand spending in order to build healthy margins.



Threats like ransomware attacks and the associated downtime and data loss can all lead to huge financial and productivity costs for a business. An hour of downtime now costs businesses at least 50% more compared to 2021-22.¹

Here are some costs you need to prepare for as you move to the cloud:

- Cloud service and resource usage rates
- Virtualization costs for disaster recovery (DR) testing and failovers
- Data egress fees for cross-region/cloud recovery and replication across clouds

Additionally, customers should be thinking about the costs that could be associated with a security breach. Threats like ransomware attacks and the associated downtime and data loss can all lead to huge financial and productivity costs for a business. An hour of downtime now costs businesses at least 50% more compared to 2021-22.¹

Solution: Navigate cloud economics with more predictability

The costs associated with cloud services can be hard to anticipate. You can build a more profitable cloud practice by stabilizing spending for BCDR with a flat-rate solution, like Backup for Microsoft Azure.

When using Backup for Microsoft Azure, all of the following is included in the flat-rate fee:

- Data egress
- Virtualization of workloads to Cloud
- DR testing

Features like these allow you to know what you'll be spending each month with greater accuracy, and thereby be better able to bill your customers accordingly.

¹<https://assets.new.siemens.com/siemens/assets/api/uuid:3d606495-dbe0-43e4-80b1-d04e27ada920/dics-b10153-00-7600truecostofdowntime2022-144.pdf>