E-TECH

Azure Data Protection:

Why Even Cloud Servers Need Backup

A common misconception is that moving to the cloud means no longer having to backup data. This idea encourages businesses to take unnecessary risks with Software as a Service (SaaS) applications like Microsoft 365 and Infrastructure as a Service (IaaS) clouds like Microsoft Azure.

There are many reasons for growing businesses to take advantage of the flexibility, scalability, and other strengths of Azure. However, cloud servers are not foolproof. They can fail just like on-premises servers because of hardware failure, ransomware, data corruption, and user error.

Microsoft does not take sole responsibility for protecting information hosted on its cloud servers. Instead, users operate under what is known as a "shared responsibility model."

In this model, Microsoft protects against:

- Service interruptions due to hardware or software failure
- Loss of service due to natural disaster or power outage
- Users must protect data against:
- Accidental deletion and other user errors
- Hackers, ransomware attacks, other malware
- Malicious insiders
- Data corruption

How To Protect Azure Workloads

You can protect workloads in Azure in many ways. Some vendors use existing backup software, while others specifically target Azure. A more important consideration is whether you'll simply back up data or use a solution that enables fast recovery of normal business operations — a business continuity and disaster recovery (BCDR) solution.

We recommend choosing a BCDR solution that gives you a variety of options — including granular file restore, VM-based server recovery, and bare metal recovery to an on-premises server — to meet varied recovery scenarios.

These are the same choices you need to make regarding the protection of on-premises server workloads. That's the point, though. Nearly everything about on-prem data protection applies in Azure. True, you don't need to procure and maintain server hardware. The cloud provider handles that.

As a managed service provider, we shield our clients from the complexities of using cloud services. However, you still need to decide the level of protection your business requires. One key decision: where will backups live?

There are two broad options: Public cloud (Azure or a secondary provider) or a backup vendor's cloud.

Public Cloud Tradeoffs

Public cloud often is sold on the promise of affordability, and in many situations it delivers. However, consider the costs and risks before you put your trust in a single cloud provider.

Both the strength and weakness of public cloud computing is that it is metered, according to measures of compute power, storage, and data transfer. Use two or three times as much of any of these in a given billing period, and you can expect costs to multiply. Unfortunately, demand for those resources explodes in a crisis. For example, if you need to download system images to another cloud or to an on-premises server, you can expect to pay "data egress" charges.

Even if we, as your MSP, commit to absorbing some or all of those costs, we must charge more to ensure those uncertainties are priced in. We don't want to be in the position of passing the costs on to you in your hour of need.

Tradeoffs to Microsoft's Own Azure Backup

Many organizations rely on native Azure services as part of their business continuity and disaster recovery (BCDR) offerings. However, it's important to verify that these services meet your needs for cost and redundancy. For example, let's look at Microsoft Azure Backup.

Again, pricing is an important consideration. Microsoft charges a flat backup fee, based on the size of the protected instance, plus a charge for the backup storage that is used. Users pay for the number of instances that are protected with Azure Backup, including SQL servers, VMs, and applications servers. You also can choose between Locally Redundant Storage (LRS) or Geo-Redundant Storage (GRS), paying more to get your data backed up to multiple, geographically dispersed data centers.

Safeguarding data with Azure Backup can invite significant cost fluctuations. You pay only for the data you use with the platform, which is cost-effective until a recovery operation is necessary. Depending on the Backup Storage tier you are employing, Microsoft may charge a one-time data retrieval fee. This pricing structure can be confusing, so refer to Microsoft's Azure Backup pricing page for full details.

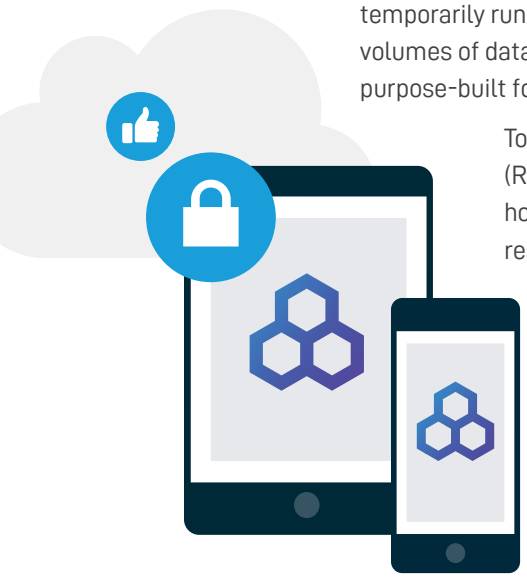
Finally, Azure Backup can't protect data in the case of a larger Azure outage that also impacts the backup service. This is a possibility we must consider for our clients' BCDR needs.

The Third Party Backup Alternative

Third-party backup can eliminate these concerns. With a third-party backup solution featuring a multi-cloud design, we can provide an extra layer of protection in case of a worldwide Azure outage. In both routine and extreme scenarios, we can quickly recover data, applications, or VMs.

By replicating to a cloud that is purpose-built for BCDR and provides predictable pricing, we provide you with superior but affordable data protection.

Our recommended solution, in partnership with Datto, provides backup to geographically distributed data centers without extra fees. With "instant recovery," we can restore a virtual machine within minutes, temporarily running it in the BCDR cloud. This eliminates the delays that accumulate when large volumes of data must be transferred and server configurations must be recreated. The Datto Cloud is purpose-built for BCDR and provides predictable pricing.



To ensure your satisfaction, we can tailor the solution to your recovery point objectives (RPO) and recovery time objective (RTO) requirements. In other words, we take into account how much or how little data you can afford to lose and how quickly you must be able to restore operations.

Ready to learn more? Contact us today. Or download our eBook, The SMB's Guide to Business Continuity for Microsoft Azure to learn more.