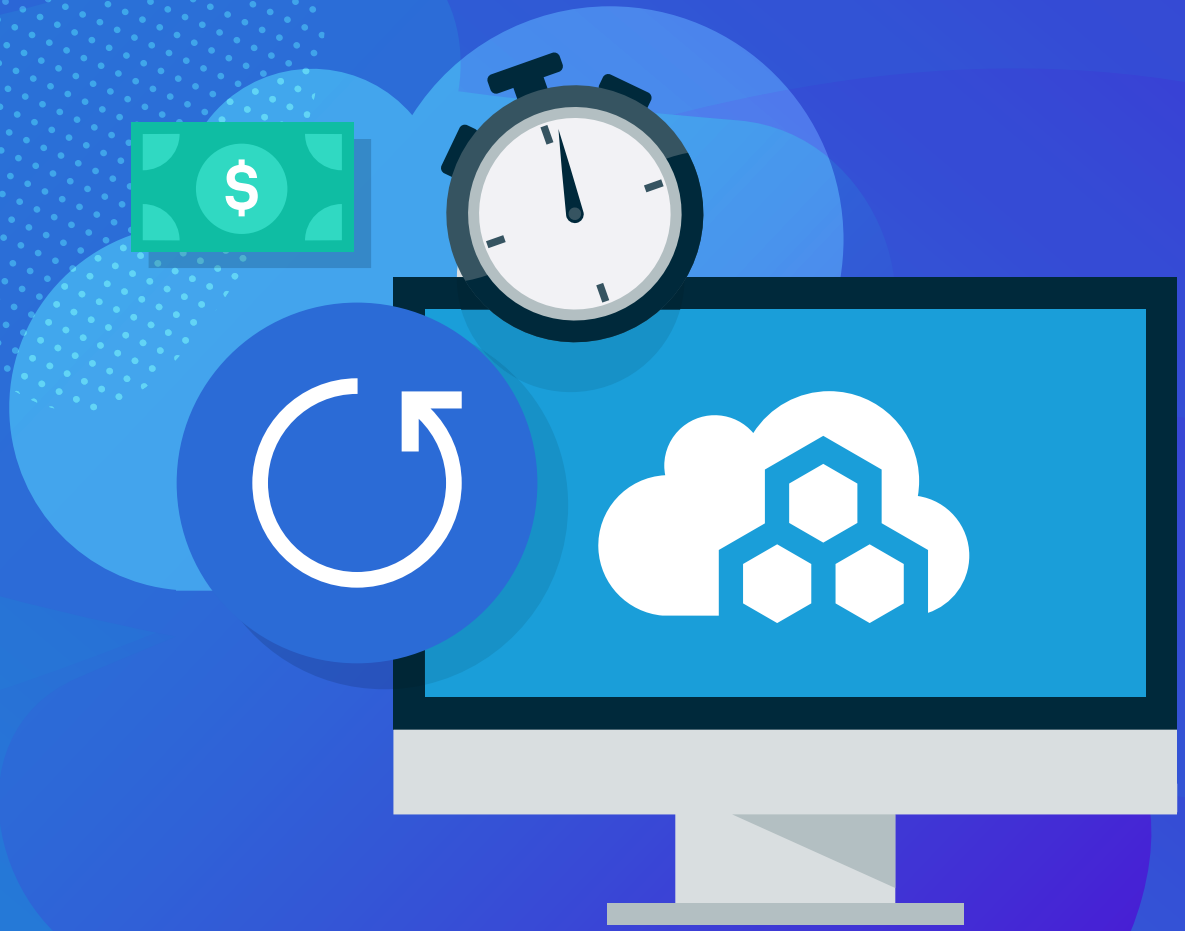
eBook

E-TECH



The SMB's Guide to

Business Continuity and Disaster Recovery (BCDR) on Azure

Introduction

As cloud adoption continues to grow among small and medium businesses (SMBs), Microsoft Azure has emerged as a popular option.

Azure is Microsoft's Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud offering, a global network of data centers that makes computing and storage capacity conveniently available to purchase on a subscription basis. In addition to offering tremendous economies of scale, Azure provides access to advanced technologies like machine learning and artificial intelligence tools. Many businesses also take advantage of Software as a Service (SaaS) options like the Microsoft 365 office suite, and Azure lets you leverage the economics and flexibility of the cloud for any commercial or custom software. It's not limited to Microsoft or Windows software.

When you run workloads on Azure, you agree to a shared responsibility model. In this model, the cloud provider (Microsoft) assumes responsibility for the security and protection of the physical data centers, hosts, and network, while the user is responsible for everything else—including information and data, applications, and more.

Managed service providers (MSPs) can assist with ensuring the security and protection of cloud infrastructure. However, as discussed later in this eBook, in the shared responsibility model, Microsoft makes it clear where its responsibility ends. This presents two key challenges.

First, businesses face the ever-present risk of business disruption events caused by human error, hardware failure, or natural disasters. Second, ransomware attacks and an increasingly complex cybersecurity landscape make it essential to plan for business continuity and disaster recovery (BCDR).

As of the end of 2020, Azure achieved a 20% market share, up from 10% percent market share in Q1 2017.[1]

There are many things to consider when building BCDR into your plans for Azure. 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

Before covering these areas, let's review why Azure is attractive in the first place and examine the shared responsibility model in more detail.

Why we recommend 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 to meet your 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

[1] Synergy Research Group, 2021.

Azure scored the highest satisfaction in terms of product capabilities, profitability, and maturity of the consumption/ subscription-based pricing[2].

a future-proof platform that enables you and your technology partners to develop and run workloads more flexibly and innovate more freely in cloud-first, on-premises, and hybrid setups.

Microsoft Azure shared responsibility model for IaaS

When you run workloads in Azure, the responsibilities for security and data protection are shared between you and Microsoft. As your MSP, we can assist with your portion. The chart below gives you a breakdown of exactly how these responsibilities are split.

Microsoft Azure Responsibility		MSP + SMB 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	

[2]CRN: https://www.crn.com/news/cloud/aws-vs-microsoft-vs-google-how-partners-rank-the-big-3-cloud-companies

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

Azure data protection options

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

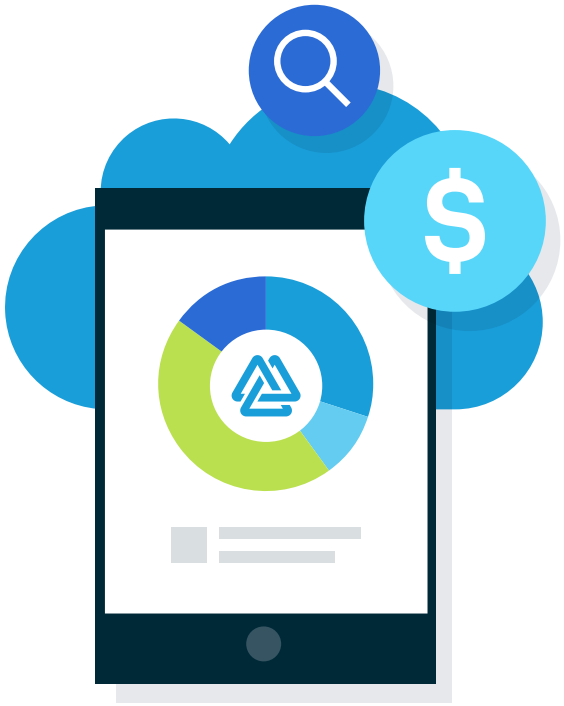
- **Azure's native single-cloud backup and recovery services:** Services offered by Microsoft to enable local- or geo-redundant backups and recovery within the Azure network.
- **Third-party BCDR tools in Azure:** Independent software vendor (ISV) offerings that protect data natively in Azure.

While these solutions are suitable for many organizations, they may not fully address challenges related to protection, cost, and management. That's why Datto worked with Microsoft to develop Datto Continuity for Microsoft Azure (DCMA) -- a BCDR solution designed for SMBs and supported by MSPs like us.

Protection: Single-cloud solutions are susceptible to downtime

Downtime can limit revenue and prevent employees from working. Thus, maximizing uptime is key to business success. Using a single-cloud solution to accomplish this poses some risk for business continuity:

- **Worldwide outages:** If all your business-critical workloads are in Azure, they are susceptible to downtime in the event of a widespread outage. This is one of the issues with using an Azure-based backup solution, rather than an independent one.



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

- **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 login screen and can potentially be held hostage in the event of a ransomware attack.
- **Daily backups:** While common, daily backups mean you risk losing up to a full day's worth of data. Plus, if your solution doesn't offer backup verification, it can be difficult to prove that a previous backup was successful and is bootable.

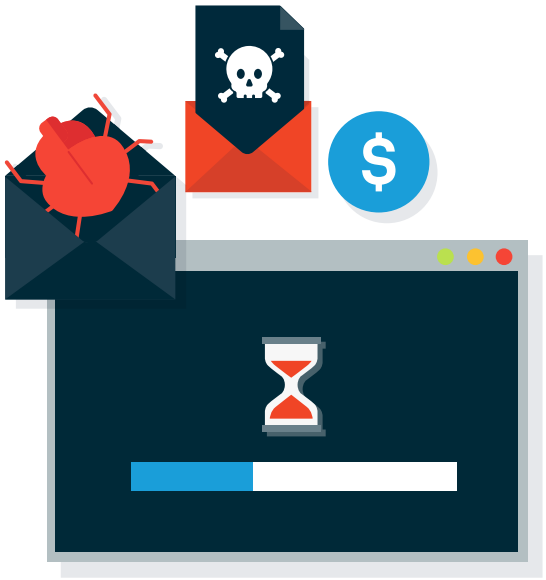
Protection: Multi-cloud backups

To alleviate these concerns, you can use multi-cloud backups through a solution like DCMA to:

- **Stay up and running during Azure outages:** DCMA provides backup and failover to the Datto Cloud with no extra fees for data egress.
- **Gain extra protection against malicious attacks:** Backups are kept secure behind a separate cloud portal located outside of Azure for additional assurance of safety.
- **Verify hourly backups:** 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: Unpredictable spending

As you begin to move your business to 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 you pay only for what you use in the cloud.



Threats like ransomware attacks and the associated downtime and data loss can all lead to huge financial and productivity costs for a business. Downtime costs alone have risen 486% since 2018[3].

While this shift can bring about newfound flexibility to many organizations, it also brings some unpredictability in cloud spending month to month. This is a concern for your business whether you pay Microsoft directly or purchase Azure services through an MSP like us that must build these costs into its own fee structure.

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 or exporting data from the cloud to on premises storage

Also consider 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. Downtime costs alone have risen 486% since 2018.[3]

Cost: Navigate cloud economics with more predictability

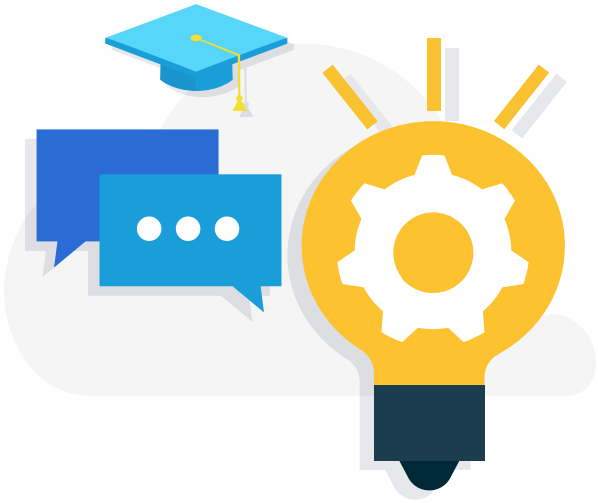
The costs associated with cloud services can be hard to anticipate.

When using DCMA, all of the following is included in the flat-rate fee:

- Data egress
- Virtualization of workloads to Datto Cloud
- Disaster recovery (DR) testing

Features like these allow you to know what you'll be spending each month with greater accuracy.

[3] Datto's 2020 Global State of the Channel Ransomware Report.



Anyone new to a cloud platform is naturally going to experience a learning curve, but SMBs need their MSPs to be ready to handle any and all cloud situations on day one.

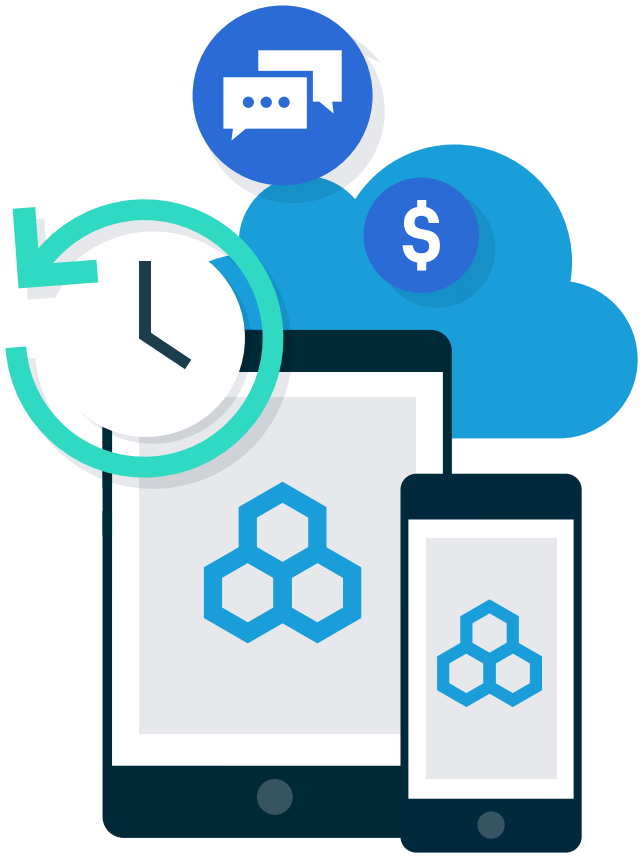
Management: Making it simple

There are many BCDR offerings suitable for businesses running workloads on Azure. However, the majority of these offerings were built for an in-house IT team to manage independently. For an SMB, the point of working with an MSP is to delegate details like ensuring that data is backed up and can be restored quickly. Using a system designed with that partnership in mind is better for us because we manage BCDR for many businesses — and ultimately better for your business because they can serve you more efficiently.

Management: Streamlined efficiency for SMBs and MSPs

Using a solution such as Datto Continuity for Microsoft Azure allows us to serve you effectively with features such as:

- **Single pane of glass:** We can manage your on-premises and cloud Datto backups from one portal for greater ease and efficiency. Not having to switch between multiple platforms and monitoring systems means issues are less likely to go unnoticed or "fall between the cracks."
- **24x7x365 support:** Having one unified solution means we don't need to train and dedicate different staff on multiple platforms. Our entire staff can be proficient in the one solution protecting your business. If we cannot solve a technical issue on our own, we can tap single-vendor technical support, allowing us to save time and eliminate confusion when an issue occurs. Datto is a global organization and Microsoft partner that offers world-class support.



Conclusion

Cloud adoption is growing among businesses of all sizes, and Azure presents compelling opportunities as a leading cloud platform. Working with Datto allows us to help you build on the promise of Azure, while providing a BCDR solution with advanced security and data recovery capabilities.

Datto Continuity for Microsoft Azure (DCMA) is a best-in-class business continuity and disaster recovery (BCDR) solution. It provides the ability to customize protection and streamline recovery for critical business infrastructure residing in Microsoft Azure. It allows SMBs to take advantage of all the virtues of Azure while limiting the risks of cloud adoption.

As an MSP, we are always looking for ways to help our SMB clients take advantage of digital technologies that will boost their business, while avoiding any pitfalls. Offering more comprehensive backup and recovery is one of the ways we are helping our clients capitalize on the best the cloud has to offer.

Ready to learn more? Contact us today to discuss how we can help you migrate to the cloud and get the benefits it brings, while protecting your business.

E-TECH

www.etechcomputing.com

contact@etechcomputing.com

647-361-8191