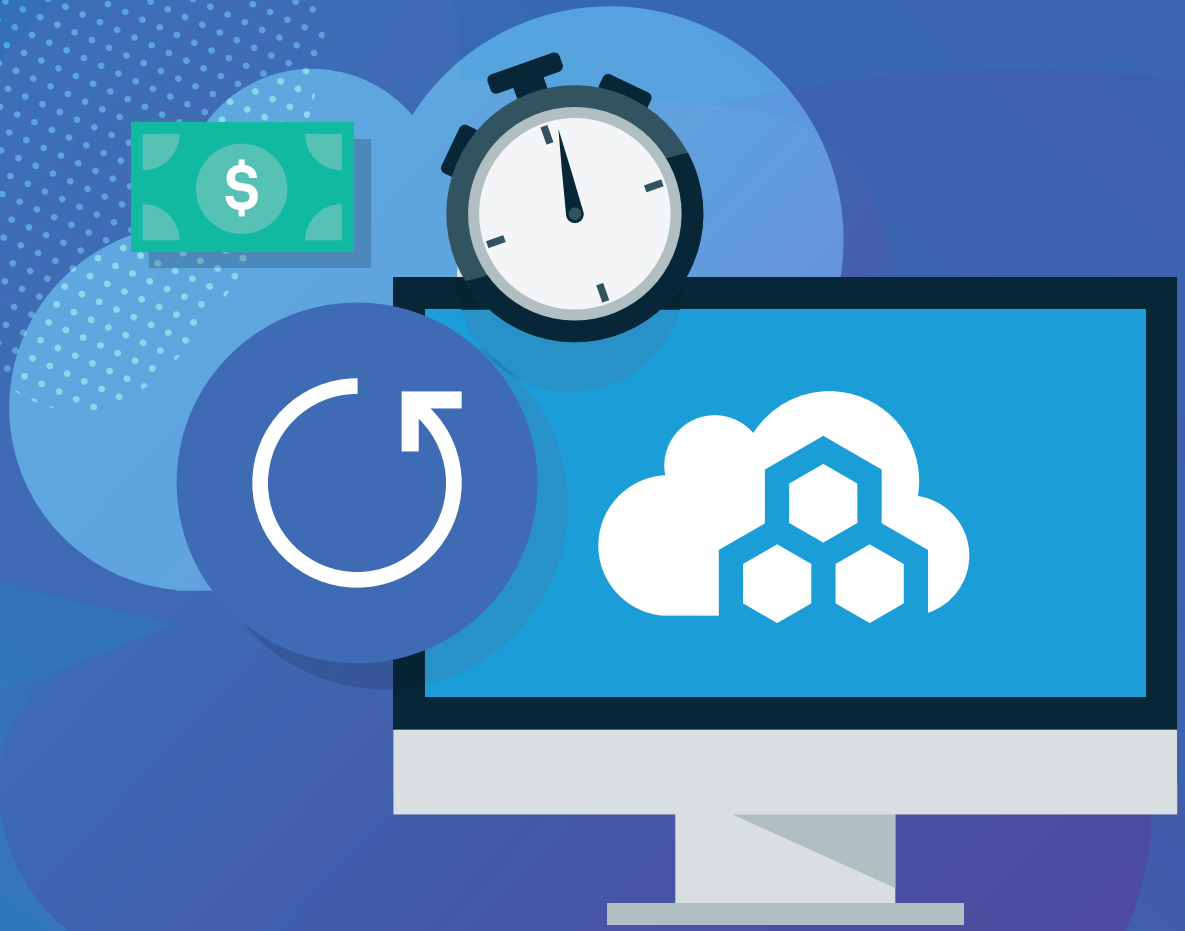
eBook



KubeNet®
Your Trusted Technology Partner.

Achieving Business Resilience with BCDR and MSP Support

Introduction

Small and medium businesses (SMBs) are looking to Microsoft Azure to drive business growth and enhance IT operations. To ensure a successful and secure Azure adoption, your organisation can work with KubeNet, a trusted managed services provider (MSP) to build a business continuity and disaster recovery (BCDR) plan that keeps your operations stable and your data safe in the cloud.

This eBook focuses on why BCDR is important for those adopting the cloud, and how working with KubeNet can help you migrate successfully to Azure by covering the following points:

1. Understand Azure's Shared Responsibility Model to grasp your security and data protection responsibilities, and what is at stake for protecting your workloads on the cloud.
2. Learn why having a BCDR plan is critical for success on the cloud.
3. Build a BCDR plan that addresses your needs for minimising downtime, defending against cyberattacks, and restoring operations quickly.
4. Discover how you can simplify and optimise your cloud BCDR solution with help from Datto Continuity for Microsoft Azure (DCMA).
5. See how best practices, partnership with an MSP, and Datto's best-in-class BCDR solution come together to help you achieve optimal business continuity.

DCMA is a simple, secure, and reliable business continuity solution for critical business infrastructure in Azure. With simplified pricing, multi-cloud replication, and access to Datto technical experts, KubeNet can ensure comprehensive protection, management, and recovery for their clients' workloads in Azure.

- 78% of MSPs reported SMB ransomware attacks 2018–2020

Datto Continuity for Microsoft Azure (DCMA) is a best-in-class business continuity and disaster recovery (BCDR) solution, built exclusively to meet the needs of MSPs and their customers. It provides the ability to customise protection and streamline recovery for critical business infrastructure residing in Microsoft Azure.

Understanding the Azure Shared Responsibility Model

When organisations adopt the cloud in any capacity, it is important to design their infrastructure with security and resilience in mind. Doing so helps minimise the risk of disruptions and better ensures successful operations in the long term.

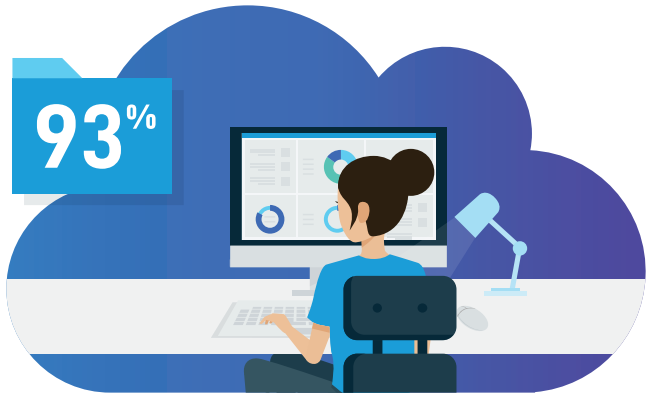
When it comes to protecting customer data as you run workloads on Azure, it is important to understand the division of responsibilities between the customer and Microsoft.

When deploying IT resources on Azure, customers must agree to Microsoft's Shared Responsibility Model, which states that users are responsible for the security of their own workloads and data:

> *"For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type)."*

To help accomplish this, an ideal first step is to explore business continuity and disaster recovery (BCDR) solutions. BCDR can be considered one of the core pillars of data security and addresses the need for information protection and governance. Incorporating BCDR into a cloud security plan helps ensure that sensitive information is safe and protects against manipulation or data loss from cyberattacks in the following ways:

1. Protection against accidental or malicious loss of data (e.g. data corruption, ransomware)
   - It is important for organisations to have a fail-safe they can restore infrastructure back to in case of a cyberattack.
2. Features to protect from data threats (e.g. soft delete, automated backup cleaning)
   - Another data security feature that ensures that important information is not deleted, and that sensitive information is removed compliantly.
3. Ability to remove data from local devices
   - In Microsoft's security vision, the fewer unprotected endpoints, the better. If customers are using an on-premises server for backup, it might not always be up to date with the latest security features—a gap that provides another potential route for attack.



93% of MSPs expect to have at least half of client workloads in the cloud in the next three years

— Source: Datto's Global State of the MSP Report 2021

As an experience MSP, we can help point you in the right direction and offer helpful, consultative services to help roll out the right solution for your business. Learning the basics of BCDR and its value is a great place to start.

99% of MSP clients are using the cloud in some capacity

— Source: Datto's Global State of the MSP Report 2021

Exploring the Value of BCDR

BCDR goes beyond traditional data backup solutions; it is composed of technical and operational processes designed to help organisations recover critical data and workloads in the event of a business disruption, and to quickly resume standard operations.

Disruptions like service outages, cyberattacks, or natural disasters can have significant negative impacts on your business. Downtime leads to lost revenue, as employees are unable to access work systems, customers are unable to purchase services, and business critical data may be lost permanently.

BCDR helps eliminate downtime and makes it possible to recover any data that might otherwise have been lost as the result of a disruption event. Leveraging the cloud optimises BCDR processes, enabling faster data recovery and offering built-in backup and security tools.

In short, having a strong BCDR plan helps ensure your business will:

- Stay up and running when faced with downtime scenarios
- Keep business-critical data safe from ransomware or other malicious cyberattacks
- Quickly restore business services and recover data if an incident happens

To find the right BCDR solution for your business, it is crucial to understand your needs so you can know what to look for. Working with KubeNet can help you get a comprehensive view of your business drivers, IT infrastructure, and budget, but it can also be helpful to learn the recommended components for a strong BCDR plan.

The Components of a Comprehensive BCDR Plan

A proper business continuity solution should proactively protect systems and data against disasters of all types. Having a strong BCDR plan allows for improved flexibility, redundancy and resilience in keeping your business operational, so it is key to understand what the best practices are for putting BCDR into action.

Each SMB's needs are unique, but implementing a BCDR solution that addresses the following areas is recommended to help maximise its overall effectiveness:

- **Multi-cloud redundancy:** While Azure offers local and geographic redundancy, by backing up and recovering workloads in a separated cloud, SMBs can ensure uptime during downtime scenarios, like public cloud outages.
- **Ransomware protection and prevention:** Advanced cyber threats like ransomware are growing in frequency and complexity. Multi-cloud backups allow you to recover server workloads in an isolated environment to minimise business interruption following a ransomware attack.
- **Rapid restore capabilities:** Resuming business operations as quickly as possible after a disruption event is crucial for avoiding lost revenue and customer satisfaction. Instant virtualisation in Azure and your backup cloud environment enables you to backup, scale and fail-over quickly.
- **Image-based backup:** Ensure all important data is saved and up to date by using a backup solution that takes images of all data and systems rather than simply copying the files into another location.

While these are crucial components to focus on when evaluating BCDR solutions, there may be other concerns your business has when deciding which solution is right for you. Working with KubeNet can help ensure you have all the necessary pieces for a robust BCDR plan, as they can educate your team and provide recommendations for services and products tailored to your needs—for the present and the future.

91% of MSPs said clients with BCDR products in place are less likely to experience significant downtime from ransomware.

— Source: Datto's Global State of the Channel Ransomware Report 2020

Incorporating DCMA into Your BCDR Strategy

To protect your Azure workloads, KubeNet offers Datto Continuity for Microsoft Azure (DCMA), a best-in-class BCDR solution for Azure that is built exclusively for MSPs. Created in partnership with Microsoft, DCMA provides the ability for an MSP to fully customise your protection and streamline recovery for your critical business infrastructure residing in Microsoft Azure.

Benefits of DCMA include the following:

- Stay up and running during downtime scenarios with multi-cloud protection and instant virtualisation in the secure Datto Cloud.
- Ensure your data is safe from targeted attacks with an extra layer of protection against ransomware.
- Quickly restore operations and recover data if an incident does occur.

How Datto and MSPs Can Help You Achieve Optimal BCDR Solution

By understanding the value of BCDR and working with us, SMBs have the knowledge and resources they need to streamline their Azure cloud migration journey.

Datto is committed to helping SMBs and MSPs drive success together by providing the tools needed to deliver valuable BCDR solutions. We help them accomplish this by offering a simple, secure, and reliable business continuity solution for critical business infrastructure in Azure.

With multi-cloud replication and access to Datto technical experts, MSPs can ensure comprehensive protection, management, and recovery for your data in Azure.

Partnering with KubeNet can help you stay online and protect your Azure workloads:

- Maximise availability with a multi-cloud-by-design, BCDR solution
- Prevent ransomware and other malicious attacks
- Get back online in minutes if an incident happens
- Simplify cloud billing with predictable monthly pricing from your MSP

KubeNet®
Your Trusted Technology Partner.

Our team are on hand to discuss your options with you.

E: sales@kubenet.net

W: www.kubenet.net

T: 0344 873 4488 (option 2)

Talk with us to learn more about BCDR for your Azure workloads.