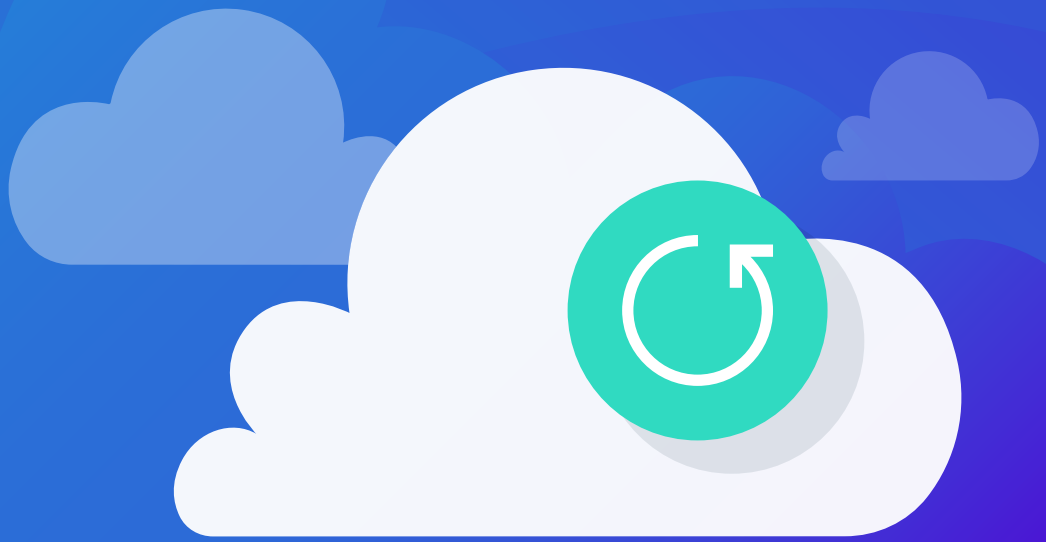
eBook

datto
A Kaseya COMPANY

# BCDR Buyer's Guide For MSPs



## Introduction

When a client's server goes down or is compromised in a cyberattack, managed service providers (MSPs) need an effective business continuity and disaster recovery (BCDR) solution to restore data and operations quickly, without sacrificing margin. That means industry-leading recovery technology from a vendor that is there to support you 24x7x365, no matter what. Simply put, you need a solution you can rely on. One that delivers peace of mind—for you and your clients.

In this eBook, we dispel common myths and misconceptions about BCDR solutions and offer tips on what to look for when selecting a BCDR solution. You'll also learn how Datto Continuity makes BCDR efficient and profitable for MSPs.

You may also be interested in:


## Common BCDR myths and misconceptions

Whether you are new to BCDR services or replacing your current product, it's important to get beyond common myths and see the bigger picture. Understanding these misconceptions can help you select the right product for your managed services practice.

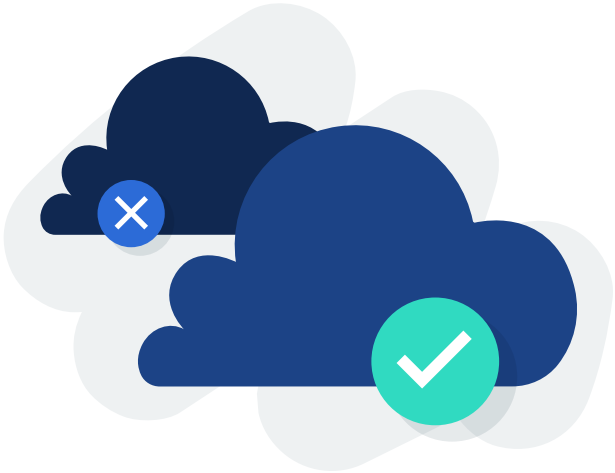
### Myth #1: **Backup is good enough**

Backup is obviously a critical part of business continuity and disaster recovery. However, on its own, backup leaves businesses susceptible to costly downtime. Why? Because recovering large data sets (such as the contents of an entire server) can be time consuming. Not to mention the time it takes to procure new hardware if primary systems become inoperable. Meanwhile, productivity grinds to a halt and revenue stops flowing.

That's why businesses need a solution that enables fast restores in addition to backup. For many organizations today, that means BCDR. BCDR solutions, focusing on the disaster recovery, offer on-premises and cloud DR, automated failover and failbacks, advanced networking capabilities, and other advanced features to ensure success of DR.

### Myth #2: **Software-only BCDR vendors are less expensive**

It's understandable why this myth exists, because software-only products, on the surface, do have a cheap price tag when compared with all-in-one solutions. However, that price tag is only for the software, and does not include hardware, operating systems, networking, cloud charges (storage, compute, egress, etc.), and more. If you look at the total cost of ownership (TCO), software-only products can actually be more expensive than all-in-one solutions in the long run.



Yes, all cloud providers deliver highly available server and storage infrastructure. But, that does not mean they are created equally for BCDR.

With all-in-one solutions, ease of use is prioritized. You get a single vendor (and monthly fee) for hardware, software, and cloud. Technical support is straightforward, no matter where the issue lies. Also, hardware is right-sized for client deployments, reducing manual labor, configuration errors, and the associated costs of each. All-in-one solutions may even include hardware replacement and capacity upgrades, easing scalability over time. Finally, there are no unexpected cloud costs, which you'll see below.

## Myth #3: **All clouds are the same**

Yes, all cloud providers deliver highly available server and storage infrastructure. But, that does not mean they are created equally for BCDR. Public cloud costs are unpredictable at best. Yes, you only pay for what you use, but that means costs spike at the worst possible time—when you mount and run a recovery virtual machine (VM). Additionally, cloud providers charge egress fees for moving data out of the cloud. So, downloading a large data set from the cloud (e.g., to restore a server) can be costly as well. Finally, some clouds have different tiers for compute, storage and security, which can add complexity.

Some all-in-one BCDR solutions include cloud costs in a single monthly fee. This can be a benefit for MSPs, because it keeps OPEX costs predictable. It makes billing clients for BCDR services simple and ensures margins on services remain consistent. Some all-in-one solution providers offer additional security measures like two-factor authentication at every step and hardened cloud appliances. Others might offer data immutability and automated retention capabilities that help organizations meet security objectives and compliance regulations.

### Myth #4: **All BCDR solutions carry the same risk**

This simply isn't true. The amount of risk you assume when delivering BCDR services can vary widely depending on the solution and vendor you choose. Again, let's compare all-in-one solutions with software-only products.

With software-only products, you're relying on multiple vendors for hardware, software, and cloud. This can result in multiple points of failure and potential finger pointing among vendors, so it takes longer to resolve issues. What's worse, if one vendor makes a change, it can impact the entire solution. For example, a software update might result in anything from a minor decrease in performance to a costly hardware upgrade.

With all-in-one solutions, MSPs get single-vendor backing and support across software, hardware, and cloud. This means less risk for MSPs.

## Evaluating BCDR and DRaaS Solutions

As you have likely gathered, one of the biggest decisions is whether you'll choose a single-vendor, all-in-one BCDR solution that includes cloud DRaaS, or build your own using products from multiple vendors. You'll also need to consider where offsite compute and storage resources will live. That might be a self-hosted cloud, public cloud, or a BCDR vendor's cloud. Regardless of the approach, MSPs need a complete toolkit to deliver BCDR to clients. This includes:

### Software

BCDR software is used to automate and manage backup and recovery processes. After an initial full server backup, BCDR software takes incremental snapshots to create "recovery points," or point-in-time server images. Recovery points are used

to restore primary server data to a specific point in time (i.e., before it failed). They can also be mounted or "virtualized" to recover server operations on a secondary device or in the cloud. This process is known as failover.

**Proper BCDR software enables:**

- Local and cloud backup
- Local and cloud failover, as well as failback
- Restore capabilities that meet a variety of recovery scenarios*

**Recovery scenarios can range from restoring a few lost files to a complete server failure. So, look for solutions that address specific restore needs. In addition to VM failover, a BCDR solution should offer capabilities like file and folder restore, ransomware detection and rollback, server image export, and bare metal recovery.*

### RPO/RTO

Recovery point objective (RPO) and recovery time objective (RTO) are key considerations. These metrics refer to the point in time you can restore to and how fast you can perform a restore, respectively. When it comes to BCDR, RPO and RTO are dictated by the frequency of backups, the amount of data under protection, software capabilities, hardware and/or cloud performance, and the cloud provider you choose.

## Cloud

As noted above, today's BCDR solutions also include a cloud backup and recovery component. In the event that both primary and BCDR hardware become inoperable, you must be able to spin up the system in the cloud.

**Depending on the approach you take, the cloud might be:**

- Public cloud (build-your-own)
- Self-hosted cloud (build-your-own)
- BCDR provider's cloud (all-in-one)

The cloud serves two purposes for BCDR. First, it is the offsite storage repository for tertiary backup server images used for restores. And second, a system can be started in the cloud to take over primary server operations during failover.


In the event that both primary and BCDR hardware become inoperable, a server image can be mounted as a VM in the cloud.

## Cloud costs and hidden fees

Choosing an all-in-one solution or building your own using a public cloud has an impact on costs, so let's take a look at each:

| All-in-one vendor cloud | Public cloud |
|---|---|
| Single, predictable monthly fee for cloud storage and compute | Cloud compute costs spike during disaster recovery |
| Predictable cloud compute performance during disaster recovery operations | Cloud provider may not provide performance guarantees/minimums (or costs may increase to meet performance needs) |
| No additional cost for restores back to primary server | Cloud provider charges egress fees for moving data out of the cloud |
| Physical restore device shipped overnight (important for restoring large data sets) | Restore to primary server occurs at Internet speed |
| Dedicated tech support during during disaster recovery operations including failover and failback | MSP must conduct DR operations, including potentially complex failback, without assistance |
| Rich security features including administration access and invariable backup snapshots that cannot be infected with ransomware | A "shared model" where the onus of data security lies with the data owner, not the cloud provider. An example is the AWS Shared Responsibility Model |

By contrast, all-in-one solutions make billing straightforward, with a single flat fee that includes cloud storage, compute, and restore costs.

As you can see, cloud costs vary considerably depending on the approach you take. As an MSP, this is an important consideration from a billing perspective. For example, if you opt to use a public cloud will you build (estimated) restore costs into your monthly fees for clients? Or, will you bill them separately for restore costs? The former provides a better customer experience, but incurs risk: What happens if you underestimate costs? The latter mitigates MSP risk, but may lead to unhappy clients when costs spike.

By contrast, all-in-one solutions make billing straightforward, with a single flat fee that includes cloud storage, compute, and restore costs. This provides a straightforward customer experience and ensures predictable margins on services delivered.

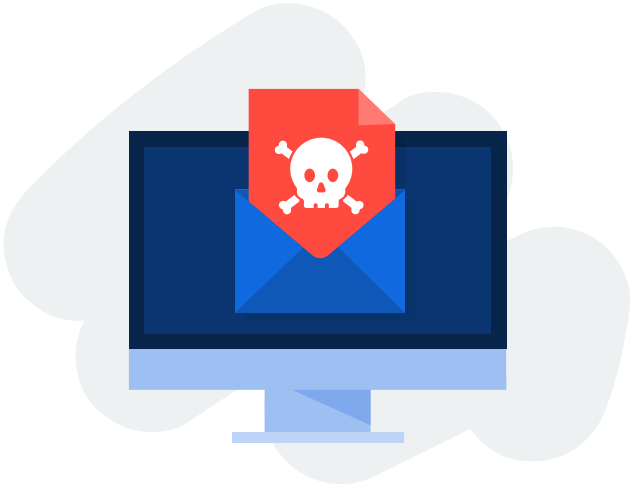
## Hardware

BCDR hardware serves a number of purposes. First, it powers BCDR software operations. Second, it provides the storage repository for backup server images used for restores. Third, it transmits server images to the cloud for disaster recovery purposes. And finally, it takes over for the primary server during local failover, allowing business operations to continue while the failed primary server is restored.

**Today, BCDR hardware typically refers to a secondary, on-premises server with:**

- Ample processing power to run normal server operations, and
- Enough storage capacity to maintain recovery points for a specific period of time (e.g., 90 days).

BCDR hardware might be a commodity X86 server or it could be a dedicated BCDR



Threat actors are increasingly targeting backups in ransomware attacks to eliminate the ability to easily recover without paying ransom. So, MSPs need a BCDR solution that addresses these concerns.

appliance. With software-only solutions, obviously you'll deploy the BCDR vendor's software on an x86 server. On the other hand, all-in-one solutions may ship with BCDR software pre-installed on an appliance or as software alone.

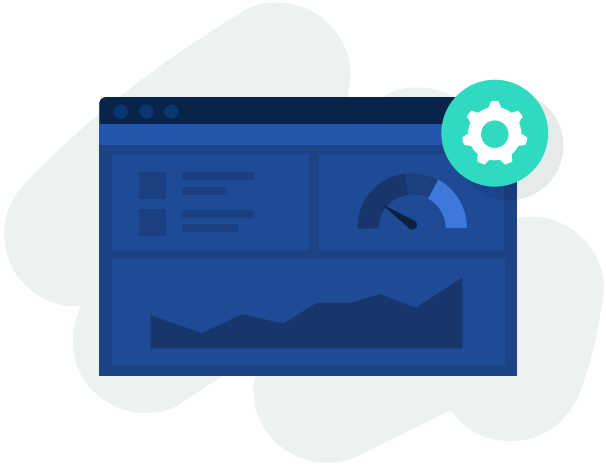
Deploying a dedicated BCDR appliance can be a benefit for MSPs. Software and hardware can be optimized to work together and the vendor might configure and right size the device to meet specific clients needs. However, if you want the all-in-one vendor experience but would prefer to choose your own hardware, that's an option as well—look for BCDR vendors that enable flexible deployment.

As businesses move some or all primary server workloads into the cloud, local BCDR hardware needs may change or become unnecessary. However, while our annual State of the MSP survey indicates that cloud adoption is on the rise, for now, local hardware is the norm.

## Security and Compliance

Many MSPs serve clients in verticals with significant security and compliance requirements. Additionally, threat actors are increasingly targeting backups in ransomware attacks to eliminate the ability to easily recover without paying ransom. So, MSPs need a BCDR solution that addresses these concerns. Ransomware detection and point-in-time rollback capabilities are a must. Data immutability is another important consideration.

Data immutability means that data is stored in a manner that it cannot be modified by external operations. It ensures that backups cannot be corrupted by ransomware or deleted in some other form of attack. It also may help some organizations meet specific compliance standards that require data archiving. Look for BCDR solutions that offer data immutability, store data in compliance



Look for products that integrate with critical tools you rely on, such as remote monitoring and management (RMM) and professional services automation (PSA) software.

with Service Organization Control (SOC 1 / SSAE 16 and SOC 2 Type II) reporting standards, and feature mandatory two-factor authentication throughout.

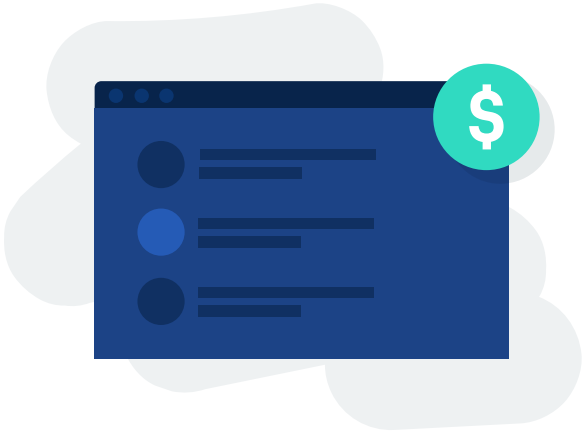
Solutions that enable automated, policy-based retention management to meet compliance standards can reduce the need for manual intervention—streamlining management and ensuring client data is stored in the cloud for the proper length of time.

## Ease of use / management

Ease of use is critical for MSPs. Increasing efficiency can expand margins on services delivered, so finding a product that is easy to deploy and manage should be considered essential. Look for BCDR products that are designed specifically for MSPs. That might mean streamlined onboarding, multi-tenant management, a range of deployment options, end-to-end security, and flexible retention policies.

Look for products that integrate with critical tools you rely on, such as remote monitoring and management (RMM) and professional services automation (PSA) software. Integrations can increase your ability to deliver BCDR services efficiently by reducing the number of steps necessary to perform common tasks.

As we've discussed throughout, consider whether you'll opt for an all-in-one solution backed by a single vendor or build your own. Software-only BCDR products are not necessarily harder to manage by nature, but troubleshooting can be more difficult when dealing with multiple vendors.



Solutions that improve efficiency also grow margin and increase revenue, since they require less manual intervention to deploy and manage.

## Profitability

No discussion of product evaluation for MSPs is complete without considering profitability. Look for products that have the features and functionality you need at a price point that allows you to build margins on your services. When evaluating solutions, it is essential to consider the total cost of ownership rather than just software and hardware costs, as we outlined above.

Solutions that improve efficiency also grow margin and increase revenue, since they require less manual intervention to deploy and manage. Look for solutions designed specifically for MSPs that combine efficient, reliable technology, multi-tenant management, and integration with other tools you rely on.

This type of solution can enable you to better support more customers and grow your business. You don't need to waste time struggling with configuration, ongoing management, and troubleshooting. This saves techs' time and reduces OpEx spending—increasing margins and driving revenue.

You may also be interested in:


## Datto Continuity (BCDR)

Datto Continuity is a complete BCDR solution that offers comprehensive backup and recovery for physical and virtual servers. Deployed as a physical appliance, as software installed on a virtual machine, or an image on your own hardware, Datto Continuity provides local and cloud backup, recovery, and failover for a flat monthly fee. There are no hidden charges or unpredictable cloud costs.

MSPs don't need to worry about themselves or their clients being under attack. The solution provides end-to-end security with the immutable Datto Cloud, AES 256 encryption in flight and optionally at rest, Cloud Deletion Defense to protect backups, hardened appliances, and 2FA everywhere.

Patented Inverse Chain technology means backups are resilient to ransomware and all backups are automatically scanned to verify that server images are complete, ransomware-free, and boot-able. Datto Continuity protects against permanent data loss and allows MSPs to easily recover clients' data following a ransomware attack with granular point-in-time backups.

As you know, delivering profitable managed services is all about increasing efficiency and maximizing return on services. Single pane of glass management gives you complete visibility into client backups, further increasing efficiency.

You may also be interested in:


**Datto SIRIS Datasheet**


**Datto Cloud Datasheet**

**REQUEST A DEMO**

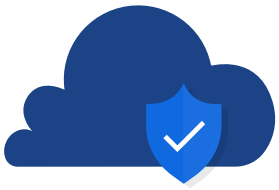
Datto Continuity offers:

- Inverse Chain: patented, ransomware-resilient backups
- Instant recovery
- World-class cloud
- End-to-end security
- Infinite scalability
- Infinite retention
- 24/7/365 US Based Support
- Unlimited Backup Agents
- Unlimited Cloud Storage
- Flat fee pricing
- Flexible deployment
- Secure, multi tenant cloud management

Datto Continuity by the numbers:

Billions of Backups

Tens of Thousands of Recoveries



Exabyte-scale Cloud

**Visit datto.com today to learn more about Datto Continuity.**