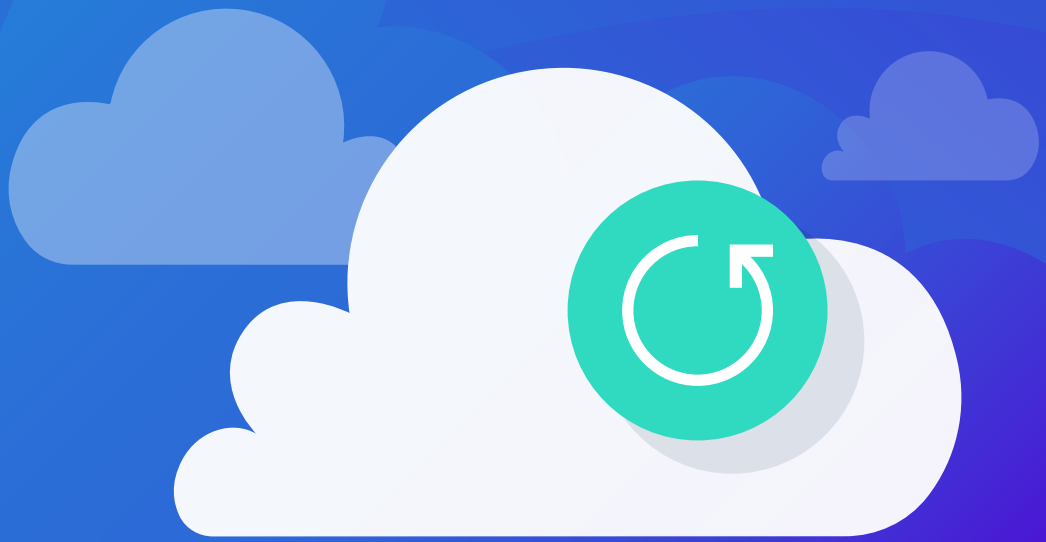
A Buyer's Guide to Business Continuity



Introduction

Ensuring that the systems your business relies on can recover from anything — a natural disaster, a ransomware attack, or the corruption of a customer database — is an essential part of business leadership and risk management.

You need a business continuity and disaster recovery (BCDR) solution that goes beyond basic backup and allows your business to recover swiftly in even the worst circumstances.

The best BCDR solutions today take advantage of the cloud, but you should understand that not all cloud BCDR solutions are alike. This guide will help you pick a BCDR solution that meets your expectations and the needs of your business.

You should understand where offsite backup and recovery resources will live — not just "the cloud" but cloud BCDR you can trust.

Evaluating BCDR and DRaaS Solutions

Once you understand that BCDR is not something you should go without, you have some decisions to make.

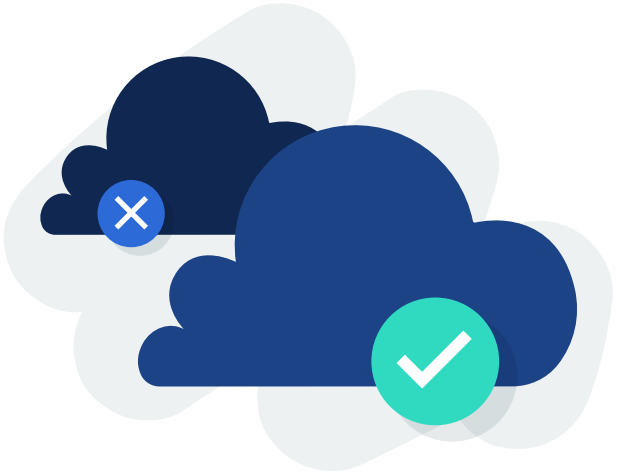
One of the biggest is whether to handle BCDR with internal resources — employees, hardware, software, cloud accounts — or seek help. And if you seek help, what kind of help? Will you choose a managed service provider (MSP) who has, in turn, cobbled together a solution? Or a service provider who can provide access to an all-in-one, cloud-based solution?

While you may want your service provider to obsess over the details — so you don't have to — you should understand where offsite computer and storage resources will live and whether you can trust them. The cloud component can be a public cloud, an MSP-hosted cloud, or a DRaaS cloud specifically designed for BCDR. You should understand the tradeoffs.

Regardless of the approach, you need a complete BCDR toolkit, including software, cloud, and hardware. Also, the system as a whole must meet your security and compliance requirements.

BCDR Software Options

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 the state of a server or workstation to a specific point in time (before it failed or data was corrupted). They can also be mounted or "virtualized" to recover



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

server operations on a secondary device or in the cloud. This process is known as failover.

Backups can be stored locally — on an appliance or backup server in your data center — or remotely, in the cloud. For BCDR, it's best to keep copies of your backups in both places. In other words, if it's not possible to restore a system locally, you can failover to the cloud.

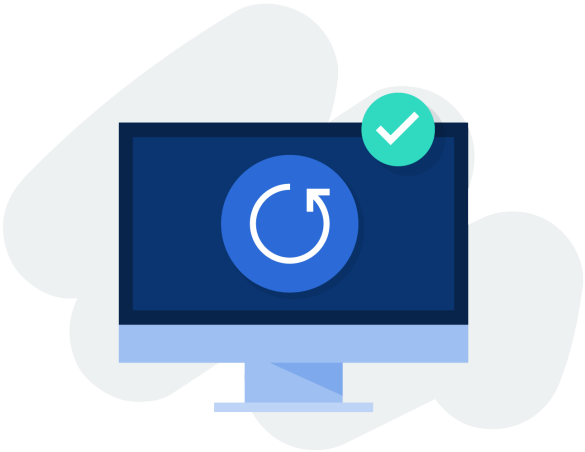
Similarly, your solution should address a variety of data restoration scenarios, ranging from restoring a few lost files to recovering from a complete server failure or the destruction of multiple servers and PCs. Restoring from local backup is faster, while the option of failing over to the cloud gives you ultimate protection against worst-case scenarios.

Evaluating BCDR and DRaaS Solutions

BCDR hardware serves several purposes:

- Hosts for BCDR software
- Stores local copies of backup server images used for routine restores
- Transmits server images to the cloud for disaster recovery
- 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 for normal server operations and enough storage capacity



Even as many business computing workloads move to the cloud, most businesses continue to operate important local servers, as well as desktops that ought to be protected.

to maintain recovery points for a specific period (for example, 90 days).

BCDR hardware might be an X86 server, a dedicated BCDR appliance, or a virtual appliance. Unfortunately, trying to save money by deploying BCDR software on commodity hardware could be a decision you will regret if it fails when it is needed most. Instead, BCDR should be hosted on either a hardened, pre-configured appliance or as a virtual machine on hardware configured to exacting specifications for performance and reliability.

Even as many business computing workloads move to the cloud, most businesses continue to operate important local servers, as well as desktops that ought to be protected.

Make sure you can trust whatever BCDR hardware is installed on-site and to any data center operated by you or your service providers.

BCDR Cloud Options

Today's leading BCDR solutions include a cloud backup and recovery component. The cloud serves two purposes for BCDR. First, it is the offsite storage repository for server and workstation images used for restores. Second, a virtual machine can be mounted in the cloud to take over critical operations during failover.

Backups "in the cloud" are off your equipment and your premises, but the extent to which they can be off your mind and worry-free varies between different types of clouds. The categories most relevant here are:

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.

- Public cloud — shared information resources like storage, processing, and servers available by remote access from a service like Amazon AWS, Microsoft Azure, or Google Cloud
- MSP-hosted cloud — your service provider's data center configured as a cloud
- DRaaS cloud — a cloud service specifically for BCDR

To understand why we have chosen to work with a DRaaS cloud specifically designed for BCDR, you must understand the tradeoffs between these options.

Tradeoffs with the Public Cloud

The public cloud providers offer reliable cloud infrastructure on a massive scale, but their services are relatively generic because they are used for many different purposes.

Rather than creating their cloud services, some MSPs resell access to storage capacity in the public cloud. Or they might arrange for you to contract directly with the public cloud provider, while they handle the hardware and software setup and configuration.

Using the public cloud as a data repository might be less expensive in the ordinary course of business, but BCDR is about making sure you're protected in a crisis. That's just when the cost of a cloud solution tends to spike — particularly if you're paying the public cloud bill directly, or your service provider passes the cost on to you. Most public cloud services charge "egress fees," and getting data out of the

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

cloud may also be throttled by bandwidth.

In other words, the public cloud data storage services that are most attractive in terms of price are not designed to support the rapid restoration of data you want during disaster recovery. For both financial and functional reasons, you should be wary of reliance on the public cloud.

Tradeoffs with MSP Built and Operated Clouds

Any organization with sufficient resources can build its own "cloud," if by that we just mean a data center for remote access to virtualized computing resources. Some multinational corporations operate their own "private clouds" offering services to different divisions and subsidiaries.

However, many of the virtues popularly associated with "the cloud" assume multiple, geographically dispersed data centers and levels of redundancy that most IT service providers can't deliver on their own. Even very large MSPs (who typically cater to very large businesses) may not offer a cloud specifically configured for BCDR.

The DRaaS Alternative: a Purpose-Built BCDR Cloud

In contrast, a cloud service specifically designed for BCDR offers predictable pricing and a cloud specifically designed for data protection, restoration, and rapid data recovery.

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

Security and Compliances

Europe's General Data Protection Regulation (GDPR) and similar laws proliferating around the world have imposed significant security, privacy, and data protection requirements on businesses of all sorts. Regulated industries like healthcare and financial services bear many additional compliance burdens. Meanwhile, threat actors are increasingly targeting backups in ransomware attacks to eliminate the ability to easily recover without paying the ransom.

A BCDR solution should address 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 cannot be modified by external operations. It ensures that backups cannot be corrupted by ransomware or deleted in some other form of attack, even by an insider.

BCDR also addresses industry-specific compliance requirements for data archiving. Look for BCDR solutions that offer data immutability, comply 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 your data is stored in the cloud for the proper length of time.

Because we provide predictable pricing (no “data egress” surcharges for retrieving data from the cloud), we protect you against being hit with excessive fees when you can least afford them.

Our Choice: A Complete BCDR Solution

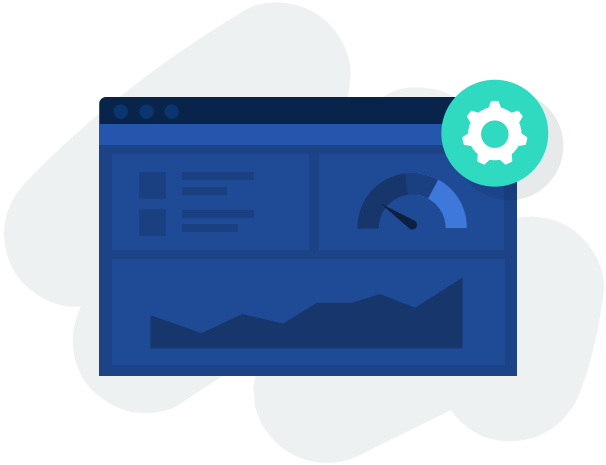
We offer BCDR services in partnership with Datto, a specialist in hybrid cloud and local BCDR for businesses of any size.

Deployed as a physical appliance, as software installed on a virtual machine, or as an image on your preferred hardware, Datto Continuity is a complete solution that provides cloud and local backup, recovery, and failover for physical and virtual servers.

Because we provide predictable pricing (no “data egress” surcharges for retrieving data from the cloud), we protect you against being hit with excessive fees when you can least afford them.

Returning to our discussion of different types of clouds, here are the trade-offs:

	Public cloud	MSP-Built Cloud	Our Solution
Reliable Infrastructure	Yes	Not necessarily	Yes
Scalable	Yes	Not necessarily	Yes
Purpose Built	No	No	Yes
Immutable	No	NO	Yes



Our cloud solution is immutable, meaning that it is always possible to recover protected files and server images, even in the event of a ransomware attack.

Secured Against Ransomware	No	Not necessarily	Yes
Recovery Costs	Unpredictable, potentially high	Variable, ask the provider	Predictable
Fixed Cost	No	Not necessarily	Yes

Our cloud solution is immutable, meaning that it is always possible to recover protected files and server images, even in the event of a ransomware attack. Our cloud solution protects against accidental or malicious deletion, so you can be confident backup data is safe.

Did you know that 59% of buyers are likely to avoid companies that suffered from a cyberattack in the past year? That's why all data backed up by our solution is scanned for malicious software. Inverse Chain and Patented Screenshot Verification technologies ensure all backups are complete and bootable. We provide end-to-end security with the strongest data encryption available (AES 256), the option of hardened backup appliances, and Two-Factor Authentication everywhere to ensure backups are not tampered with.

The administration is performed using the secure, cloud-based administration portal. All backup and recovery operations including individual file restore and an entire system recovery can be performed remotely within the portal. Whether you access the portal directly or rely on us to manage it, we have a single, centralized

means of ensuring all servers, virtual machines, and workstations included in your BCDR plan are backed up and recoverable.

Our continuity by the numbers:

- Over 10,000 cloud recoveries per month
- Exabyte-scale cloud supporting over 1 million organizations

Here is what our continuity offers to protect your business:

- Instant recovery
- World-class cloud
- End-to-end security
- Infinite scalability
- Infinite retention
- 24/7/365 dedicated, in-house support
- Unlimited Cloud Storage
- Flexible deployment
- Secure, multi-tenant cloud management

Talk to us today about how we can help keep your organization healthy and growing. Part of that is making sure your business is resilient against major disasters, minor mishaps, and everything in between.

To learn more, visit tpx.com