August 2024 | eBook

Building Business Resilience

Leveraging the Public Cloud for Business Continuity and Disaster Recovery

NUTANIX

Introduction

As organizations strive to stay agile in an increasingly fierce marketplace, it's more critical than ever to choose IT solutions and infrastructure that enable them to stay flexible and responsive to their customers and stakeholders. Most modern organizations are choosing to move applications and other workloads to the public cloud – multiple public clouds, in many cases – with that agility and flexibility in mind.

Managing and maintaining infrastructure that includes on-premises, multiple private or public clouds, and edge deployments can get very complicated, very quickly. And if simply managing that infrastructure is challenging, what happens when part of the system goes down or is breached in a malicious attack? How do business continuity and disaster recovery work in a hybrid multicloud world?

In this eBook, we'll take a look at why enterprises are working with more public cloud providers today and the disaster recovery challenges they face when the worst-case scenario becomes reality. We'll also cover what successful enterprises are doing to mitigate the risks and realities of downtime and ensure better business continuity so they can compete more successfully and thrive.

Contents

Business resilience is critical to enterprise success.

Keeping operations up and running – or getting them back online as quickly as possible – is a business imperative today. Customers expect agile, convenient service and support, as well as omnichannel interactions with most businesses. In today's fast-paced digital landscape, if your retail website goes down, chances are your customers will find what they need somewhere else within minutes. If your application doesn't work, many customers will be quick to vent their frustration in social media forums.

It's not just customers that downtime affects, either. Your organization's stakeholders, suppliers, partners, and internal employees also rely on consistent access to data and systems. Business suffers if they can't do their work or communicate efficiently with your company or representatives. Without business continuity, you risk your brand reputation, bottom-line revenue, customer experiences and satisfaction, brand loyalty, and more.

One recent study found that unplanned IT downtime causes a total enterprise loss of $400 billion every year. That monetary loss is not only due to lost transactions or lost customers, it can also be legal fines or penalties. Inability to prevent downtime or recover quickly from it threatens the very existence of enterprises today.

In addition to business continuity, enterprises must have a strong disaster recovery strategy – or a plan for how you will bring systems back up and restore normal operations after an unplanned interruption. A disaster recovery plan helps you maintain business continuity.

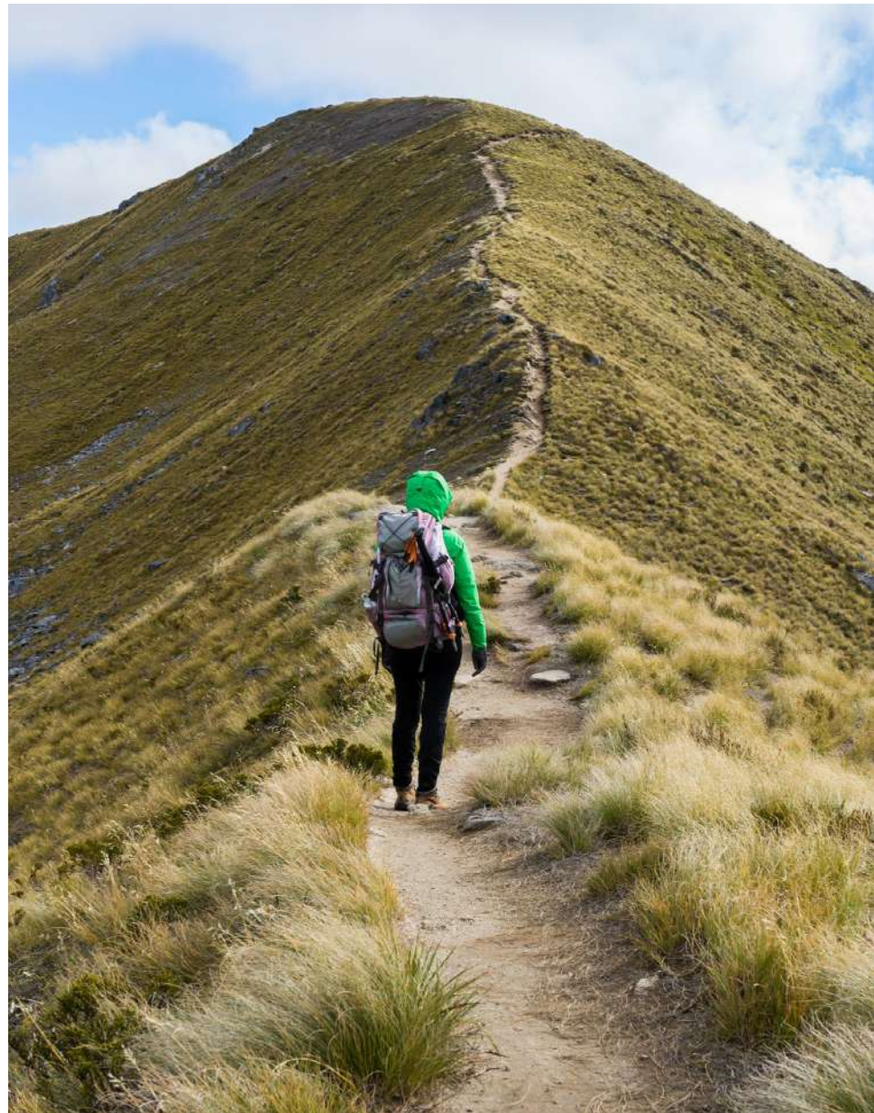
Disaster recovery falls within the umbrella concept of business continuity. Business continuity also includes data protection, which involves backing up data at rest and replicating production data to restore from in the event of a malicious attack or other unplanned event. Data protection and disaster recovery are critical factors in overall business resilience, which is how quickly you can bounce back or adapt to sudden, unexpected changes that pose a threat to your operations, employees, services, assets, or customers.

BCDR
stands for business continuity and disaster recovery and is used as an umbrella term for all aspects of data protection and disaster recovery.

Business continuity
is an organization's ability to prevent and recover from potential threats and vulnerabilities and return to business as usual within a reasonable time and with minimal damage.

Disaster recovery
is the ability to restore mission-critical IT functionality by implementing tools, policies, and procedures, and reestablishing vital business operations.

Data protection
deals with migrating back data that was lost or damaged during an unplanned interruption.



Today’s hybrid multicloud can present challenges for BCDR.

The modern de facto standard for IT infrastructure is hybrid multicloud. A recent study by Nutanix found that more than 80% of organizations surveyed believe hybrid IT environments are most beneficial to their ability to manage applications and data. And almost half of respondents said that hybrid IT had become a top priority for their CIO.

Hybrid multicloud infrastructure gives enterprises a range of options for deployment of data and applications, as well as a variety of computing cost and billing models. That’s why organizations like it. They can find optimal placements for each workload or application in the environment in which it operates best.

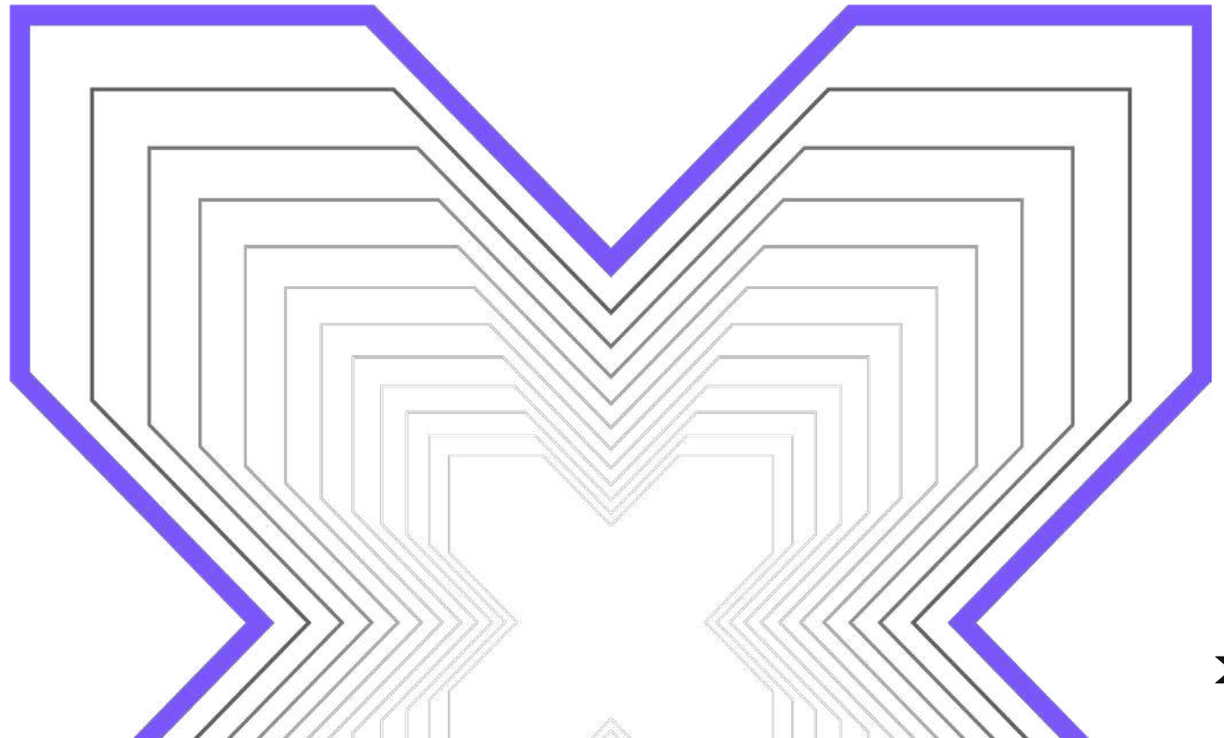
There’s a bit of a downside to all of these options, however. With more environments come more complexities. With hybrid multicloud, many organizations have solutions from multiple providers, and each solution or environment has its own required toolsets, skills and security procedures. It can be a real challenge for IT to manage and monitor hybrid multicloud infrastructure and make each environment interoperable and connected.

Nowhere is this challenge more serious than when the worst-case scenario occurs and data is lost or corrupted in a deliberate attack or natural disaster. Disaster recovery and maintaining business continuity across a hybrid multicloud ecosystem can get especially complicated. And without the ability to bring systems back up and restore data, an enterprise can suffer severe repercussions.

Hybrid
IT models are made up of workloads and applications that are located across a variety of environments – including on-premises, hosted, private clouds, public and service provider clouds, and edge locations.

Multicloud
signifies that an organization has data and applications in more than one public cloud.

> With more environments come more complexity. It can be a real challenge for IT to manage and monitor hybrid multicloud infrastructure and make each environment interoperable and connected. Hybrid multicloud also complicates BCDR.



Evolving threat landscape makes BCDR a must.

The increased complexity of hybrid multicloud infrastructure doesn't just apply to managing and maintaining it. It also extends to BCDR. Because hybrid multicloud spans across on-premises, edge and the public cloud environments, how you protect and restore data in each one can differ.

Protecting your data and applications, and being able to quickly restore them when you must, is a business imperative and critical to success. Mostly because today's ever-evolving threat landscape likely means that you will experience unexpected downtime in the form of ransomware, external infiltrators, power outages, and so on. It's a matter of when, not if.

The causes for that downtime can range anywhere from simple equipment malfunction to internal employee mistakes or malfeasance to power or network loss due to natural events such as fires, floods or earthquakes.

One of the most imminent threats to enterprises today is ransomware and other cyberattacks. According to the latest Nutanix Enterprise Cloud Index report, responding enterprises ranked ransomware protection and data security as their organization's biggest data management challenges. And 71% of respondents who had experienced a ransomware attack reported taking days or even weeks to restore full operations. Depending on your business, even mere moments of downtime could be disastrous.

Ransomware isn't going away anytime soon. In fact, the frequency of attacks is growing. A study by Symantec in January 2024 found that "ransomware attacks spiked in October 2023 and the number of organizations affected by ransomware in October 2023 was 66% more than a year earlier."

In the face of growing ransomware attacks and other causes of unexpected downtime, it's more important than ever that enterprises have a strong BCDR plan to increase resilience.

> 71% of organizations who experienced a ransomware attack reported taking days or even weeks to restore full operations. (6th Annual Nutanix Enterprise Cloud Index)

Ensure business resilience – wherever your data resides.

A good BCDR plan will be a lifeline when downtime occurs. Restoring data and maintaining business continuity doesn't always have to be a major operation, either. Think of BCDR as a range of processes that encompass everything from a simple backup to comprehensive disaster recovery. It might occasionally be as simple as rolling a system back to the most recent snapshot or just keeping your data in as current a state as possible.

Today's bad actors and ransomware are targeting not only primary data but also on-premises backups. This leaves organizations vulnerable to more risk because if they can't access their backups, they're more likely to pay the ransom. For this reason, it's important to create and store offsite copies of your data and compute environment, such as operating systems and applications.

For a long time, the IT industry has relied on the 3-2-1 backup rule, and it's still valid today. It dictates that an organization should have at least **three** copies of its data in at least **two** locations – with **one** of those locations being offsite.

One advantage of a hybrid multicloud infrastructure is that you already have data and applications in a range of environments. Each environment can also serve as a backup for data and applications located elsewhere in the system.

Achieving a solid BCDR strategy isn't easy. It involves a careful mix of best practices, regular IT resource backup and frequent disaster recovery plan testing.

Business continuity and disaster recovery require that data be protected from corruption, loss or compromise. The two subcategories of data protection are:

Backup

The process of creating a copy of data. Most backup solutions take occasional complete backups complemented with regular, often nightly, incremental backups that copy only data that has changed since the previous backup. Organizations set backup frequencies and retention policies to ensure sufficient recovery points and comply with regulations.

Replication

The act of copying and then moving data between a company's sites. It is typically measured in Recovery Time Objective (RTO) and Recovery Point Objective (RPO). It delivers uninterrupted operation of mission-critical and customer-facing applications after a disaster. Replication should be complemented with failover and failback capabilities to ensure minimal downtime and data loss during a disaster.

Using the public cloud as part of a BCDR strategy.

When it comes to the 3-2-1 backup rule, many of today's organizations are using the public cloud as their offsite backup location for on-premises data. In fact, a 2023 survey by IDC found that among enterprises with hybrid and/or multicloud infrastructure, 67% are using a form of cloud-based BCDR.

The same survey reported that the top two considerations in regard to cloud investments are (1) comprehensive security and (2) disaster recovery and backup. It also highlights how backup and disaster recovery are becoming integral to hybrid strategies with the discovery that the most common method today involves backing up data from on-premises private clouds and storing it in the public cloud. The second most common backup method is storing copies of on-premises datacenters in a hosted private cloud.

When it comes to selecting a disaster recovery model, IDC reported that enterprises using hybrid multicloud infrastructure were primarily driven by data protection benefits, speed of data retrieval, and ease of management.

Public clouds can be a significant benefit as part of a disaster recovery strategy.

They make it simple to recover data quickly to help reduce downtime and minimize the effects of an attack or outage. Public clouds also offer a variety of capabilities and benefits that on-premises infrastructure doesn't. These include:

- **No capital costs** or need for additional equipment
- **Automated operations** that ease management
- **Unified management** plane for more efficiency
- **Elimination** of idle resources and outdated backups
- **Lower cost** and reduced IT management burden
- **Fast, simple scalability** whenever it's needed
- **Data immutability** that prevents data deletion or alteration

PENN NATIONAL INSURANCE

Penn National Insurance needed a way to simplify management of its expanding on-premises virtual desktop infrastructure (VDI). At the same time, it was looking for a serious update to its tape-based disaster recovery system.

Nutanix solved both challenges with Nutanix Cloud Clusters (NC2), which runs on-premises and in AWS – allowing the insurance provider to fully embrace a hybrid multicloud model and making it easy to replicate on-premises data to the cloud.

"If we ever have a disaster, we can quickly spin up NC2 on AWS and bring up the replicated data in the cloud," said Craig Wiley, Senior Infrastructure Systems Architect at Penn National Insurance. "By moving our disaster recovery to the AWS cloud, our recovery time has dropped from several days to under two hours.

What to look for in a cloud-based BCDR solution.

Although hybrid multicloud can increase IT complexity for enterprises, you can reduce that risk by selecting a solution with the right features and capabilities.

One of the most important characteristics of a good BCDR solution is that it allows you to manage and monitor all environments across the hybrid multicloud, including on-premises and edge, as one single system. Interoperability is critical. In fact, some experts would even say that a siloed hybrid multicloud, where each environment is separated from the others, isn't true hybrid multicloud. The benefits of the infrastructure are only there if it all works together seamlessly.

Important features and capabilities that can help you meet a range of SLA requirements include:

Snapshots – A quick "picture" of a server at a particular time. It includes files, software and settings. Snapshots preserve a "point-in-time" state and don't require you to copy or move the server's data.

Replication – Copying data to store at a different site, often geographically separated from primary sources.

Disaster recovery tiering – Tiers define how quickly data can be recovered using certain methods. The higher the tier, the faster (and more expensive) the recovery. Tiers range from "no data stored offsite" (Tier 0) to "automated disaster recovery, often with AI" (Tier 7).

AWS elastic disaster recovery integration – Elastic disaster recovery is a fast, simple way to recover data to AWS. Your BCDR solution should integrate with it if you use AWS at all.

Cluster hibernation – Some disaster recovery solutions have the ability to back cluster data to the cloud (such as AWS buckets) when you shut them down or put them in hibernation. Hibernation is beneficial when the cluster isn't in use.

In short, a good recovery solution should allow you to return to business as usual with minimal downtime and data loss.

Synchronous replication
The process of copying data to a repository at the same time it's being written to primary storage.

Asynchronous replication
Information is first written to primary storage, stored in a memory device and then replicated at a later, specified time to another storage location. It uses less bandwidth than synchronous replication and is designed to work better over long distances.

Near-synchronous replication
An always-on process that continuously replicates only the data that's changed. It is unscheduled and doesn't require snapshots.

NC2 simplifies business continuity and disaster recovery.

With NC2, managing your business continuity and disaster recovery plans is simple and efficient. The solution enables organizations to accelerate their hybrid multicloud agenda without adding complexity. It delivers one-click disaster capabilities to
help cut the cost and complications of maintaining many disaster recovery sites. With on-demand elasticity and auto host remediation, it provides a single, consistent management portal for all of your IT environments. If you experience data loss or an attack in the cloud, your data and applications will still be available. That means a lot in today's competitive landscape

NUTANIX

info@nutanix.com | www.nutanix.com | @nutanix