Does your organization have IT resilience?

Now is the time to take a close look at your disaster recovery and business continuity plans.

White Paper by

OVHcloud®

If you haven't put a disaster recovery (DR) plan in place, or haven't reassessed your DR solution recently, here are a few stats to get you motivated:

+$300,000 per hr cost

Estimated cost of downtime at $5,600 per minute or $300,000 per hour on average, but can be significantly higher.[1]

1 in 2 SMBs

have experienced an extended break in continuity, which can cost $10,000/hour at minimum.[2]

54% of businesses

said they had experienced a downtime incident in the past five years that lasted at least eight hours.[3]

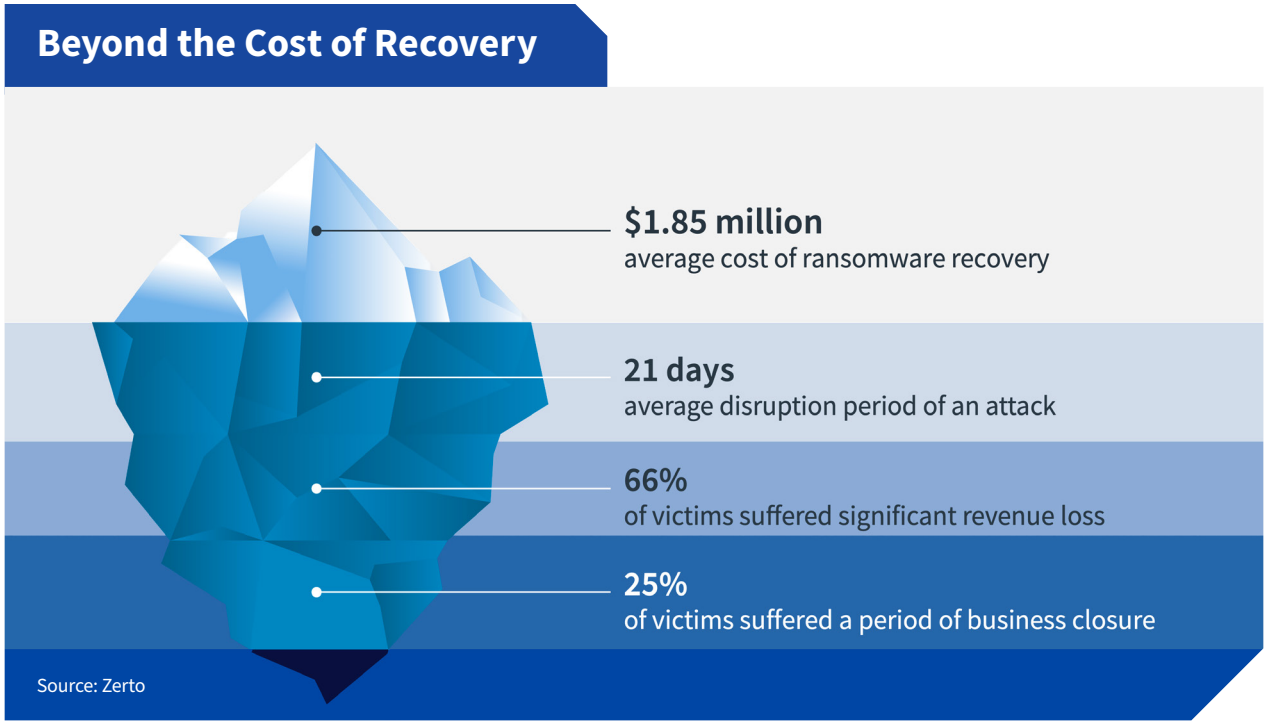
Disasters can cause financial and productivity losses, sales and operation disruptions, legal and investigative costs, credit monitoring and reimbursement costs, extortion payments and settlement costs, regulatory fines and damage to your brand and reputation.

What's the difference between BC and DR Plans?

A business continuity (BC) plan focuses on policies, procedures and the big picture of how to get the organization back up and running as quickly as possible. A disaster recovery (DR) plan is a subset, focusing on ensuring the infrastructure, data and applications are as protected as possible, how leadership and employees access the system, and how they can consume all the data that's being backed up. A DR plan with no solution on how to make the data available and consumable in a secure way can be very costly. If you feel challenged by it all, you're not alone. A survey of the CIOs and CISOs of 1,200 organizations revealed that while cyberattacks to steal IP or data were top concerns, over a third said they would describe their data protection policies as ad hoc or nonexistent, and 59% lament that budget constraints limit the ability to battle against cyber threats.[4]

An unexamined plan can be disastrous.

Compounding the problem is the fact that the perimeter and surface exposure has become much greater. There are employees, customers and partners, cloud and on-prem, IoT and apps, systems and data, mobile devices and remote access. It's estimated that more than seven billion people and businesses and at least 30 billion devices are connected to the internet, and data is expected to hit 175 zettabytes by 2025.[5] Workloads are more diverse and disparate, across different platforms and geographic regions, from the edge, the core and the cloud. And all applications that impact user experiences must be protected and available 24/7/365 to meet today's digital expectations and need for speed.



It's not a matter of if, it's a matter of when.

Today in the US, a company is targeted by ransomware every 14 seconds. In a recent IDC survey, 50% of the companies surveyed had suffered an unrecoverable data event in the last three years.[6] While hardware and software failures are the main reasons for full failover, the next cause is cyberattacks – ransomware, malware and hacking — followed by power failures and network failures.[7]

Cyberattacks can and do create total disasters, and your DR plan should address them as the threat they are to your recovery and continuity. Consider the worst possible scenario and what data will need to be recovered and how fast. No one-size-fits-all solution exists. DR is as unique as each organization and every data point that needs to be detected and recovered.

So, if you haven't done so yet, now is the time to take a very close look at your BC and DR plans because protecting your infrastructure and data from malware and ransomware attacks is about planning for when not if. A comprehensive BC plan can mitigate the risk to your operations, and a well-architected DR plan can significantly minimize and even eliminate downtime.

Building on the three core pillars of IT resilience.

Delivering IT resilience is based on three critical pillars that ensure you can withstand any disruption, leverage new technology seamlessly and move forward with confidence.

1. Continuous DR — To protect against any disruption and deliver an always-on customer experience, your backup must be continuous and not a periodic or snapshot-based backup. Continuous replication is a great way to ensure constant availability with no downtime or data loss.
2. Workload Mobility — With migrations and consolidations to new infrastructures, you have to have the confidence to move your business applications and data workloads with ease, without risk and with 100% protection along the way.
3. Multicloud and Hybrid Cloud — It's essential to leverage cloud to accelerate your business, take advantage of the benefits cloud offers and ensure you have the freedom to choose your cloud and are able to move to, from or between clouds.

> "93% of companies without Disaster Recovery who suffer a major data disaster are out of business within one year."
>
> — sysgroup.com

The journey to IT resilience.

The first step to IT resilience is to remove systemic risk, which means converging and automating your DR processes, making sure your business is protected against any disruption so you can deliver a 24/7/365 experience, and ensure business SLAs are met. By automating your DR processes, you can reduce staff workload, reduce costs and provide better protection for unplanned disruptions.

> "96% of companies with a trusted backup and disaster recovery plan were able to survive ransomware attacks."
>
> — sysgroup.com

Once done, you can shift resources to focus on executing a multicloud and hybrid cloud strategy to provide the agility your business needs. Intelligent data workload placement anywhere, whether on-prem or cloud, allows infrastructure modernization to move beyond legacy applications and evolve your operations and business. With your resources aligned to support the growth of the business and continued transformation, you can then achieve operational efficiency, and your IT can deliver at the speed of business.

Backup and replication — what's the best approach?

Backup involves making a copy or copies of data. It's a relatively inexpensive way to avoid complete data loss. It relies on snapshots of the data taken at pre-determined points in time. It requires a tape library in a secure place. Backup typically is used to duplicate everything in the enterprise and for long-term archival of business records. While valuable for historical purposes and compliance, it doesn't ensure the smooth continuity of operations.

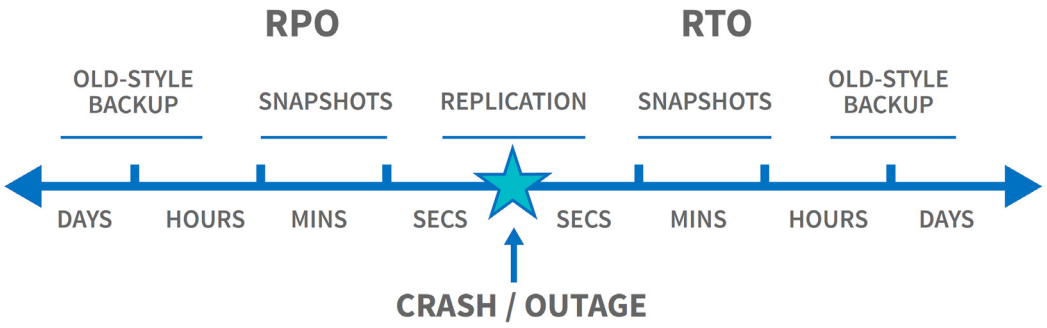
Replication, however, can ensure that data and processes are always available, even after an outage. It is the act of copying and then moving data between a company's data sites. It requires investment in a second infrastructure, so it's more expensive, but it truly is disaster recovery because it enables quick and easy resumption of operations. There's a VM that's continuously replicating and just waiting to be switched over if needed.

Let RPO and RTO be your DR guides.

Replication is typically measured in Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These are the key parameters for guiding you on the optimal data backup and replication options for your DR plan. RPO describes the interval of time that might pass during a disruption before the quantity of data lost exceeds the maximum allowable threshold. RTO is the duration of time and a service level within which a business process is restored. Finding the right balance for your business between RPO and RTO is critical.

RPO is the amount of data to be recovered.

RPO refers to how much data is at risk using a particular method. Here's an example. A company runs a full backup of their data once per hour, and data gets changed regularly throughout every hour. If the backup is run at 12:00 noon and systems fail at 12:01, they've only lost a minute of live data. But if the failure occurs at 12:59, they've lost 59 minutes of data changes. An organization may be fine with a 24-hour RPO if changes lost in the last 24 hours won't have a major impact. For businesses with financial transactions or medical data, even just minutes of data loss can be too damaging, so the RPO has to be much shorter because the risk is much greater.



RTO is the amount of time to recover the data.

RTO is all about how long it will take to get lost data back into a consumable format so you can be up and running again. RTO helps you determine the method and technologies used. If you go with backups, how many backups is it going to take and how long? A backup takes all of the data, de-duplicates it and compresses it into one file, which goes on to another storage device. To recover the backup, you have to access and read all the data, rehydrate it and recover it to a physical or virtual replacement server to make it usable again. Compared to backup, replication is lightning fast in terms of RTO. With replication, the changes made to a live virtual server are copied to a secondary location. In the event of a failure, the secondary site can be brought up (failed over) and the server can continue its functions far more quickly.

So, as you look at your BC and DR plans, RTO is critical to consider – what data, systems and applications need to be available within minutes, hours or days? If you need all your data instantly because it's mission critical, you'll want 100% replication since it's real-time or as close to real-time as possible. You flip the switch, turn on the VM, and you're back in business. However, if you have different levels of data and application needs, you can opt for a plan that includes both replication and backup.

Think of your enterprise and DR in three tiers.

> "75% of small businesses have no disaster recovery plan objective in place."
>
> — sysgroup.com

With an understanding of the processes and parameters, you can look at your enterprise from a perspective of three different tiers – what's mission critical and needs to come back up immediately, what's business critical but can wait a few hours, and what's noncritical and can wait a few days. You can use different methods of protection for different tiers. For instance, multiple terabytes of data from over the past decade may be important to keep for historical or compliance reasons, but it's not going to hurt if it takes several days to recover. Business critical data that is important to your organization's daily functioning may be okay if it takes a few hours to stand back up. But if it is data that absolutely can't be lost and could be devastating if it's not backed up immediately, it's mission critical.

1. Noncritical Data

For noncritical data, backups are still a very cost-effective solution for retaining copies of data and virtual machines. These backups can be stored on-site, off-site at another geographical location, or a combination of both for increased data protection and long-term retention needs.

> "According to the latest business continuity statistics, 84% of businesses currently store data and backups in the cloud."
>
> — comparitech.com

2. Business Critical Data

For business critical data, there are DR solutions that use VM snapshot technology combined with changed block tracking (CBT) to create a replica of a virtual machine. While the snapshot is being taken, a redo file is created, and all changes made during the replication process are written into this file. Once the replication job is finished, the redo file is merged with the snapshot into a live disk file. The next time the replication job is started, only changes made since the last job will be copied to the replica virtual machine. The big advantage is being able to more efficiently capture and store data for long-term retention needs. The RPO is also a five-minute minimum.

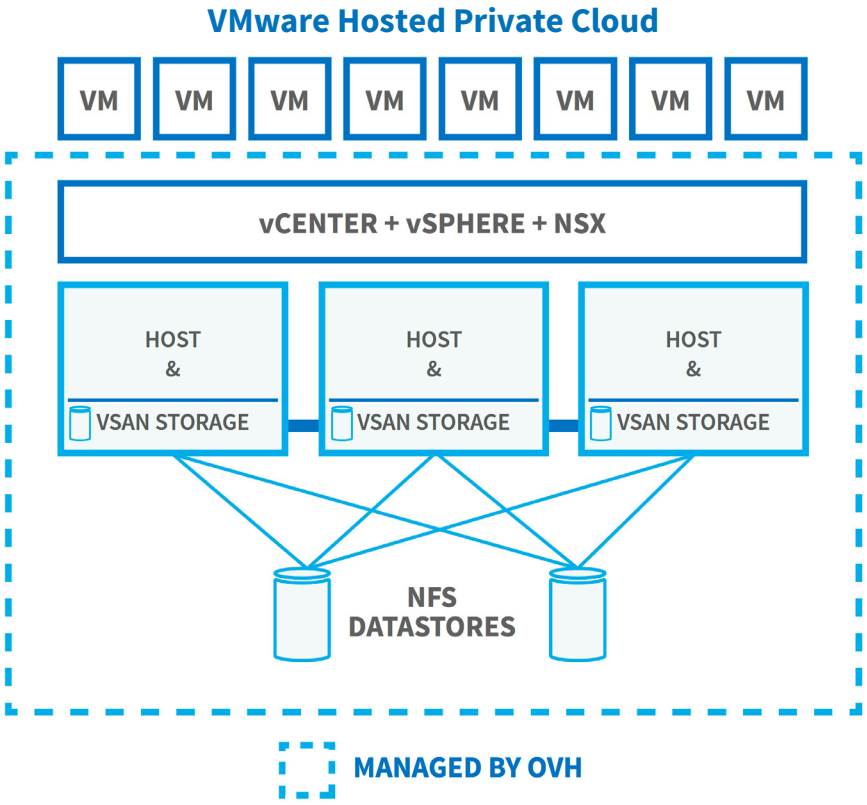
3. Mission Critical Data

For mission critical data, the most robust solution is replication technology that deploys small virtual machines on physical hosts. These VMs capture the data as it's written to the host and then send a copy of that data to a replication site. This process results in near-synchronous replication since the data is sent to the DR site at the same time it is written to the production disk array. This replication process is continuous, so the delay between writing data to the host machine and sending it offsite is minimal. The RPO can be measured literally in seconds, so you won't even lose five minutes' worth of data.

> "Small businesses have a higher adoption rate. 93% of small businesses store data or backups in the cloud. "
>
> — comparitech.com

This almost instantaneous replication method is a 100% dedicated disaster recovery solution for virtual architectures with real-time replication orchestration, allowing for granular failover and DR testing. It has the capability to replicate down to a single VM or at the application level. So, if you're having trouble with a specific database, application or website, you can orchestrate the failover just for that particular issue, giving you the flexibility to maintain availability and take corrective action with little downtime.

The DR solution that meets your needs and budget.



The experts at OVHcloud can help you determine the best DR solution based on your unique IT enterprise and business operations. OVHcloud's Hosted Private Cloud gives you great performance and security at the right price.

Powerful, Private, Dedicated

Gain the power of virtualization on an OVHcloud infrastructure, managed by OVHcloud, composed of resources that are entirely dedicated to you.

High-Level Certifications

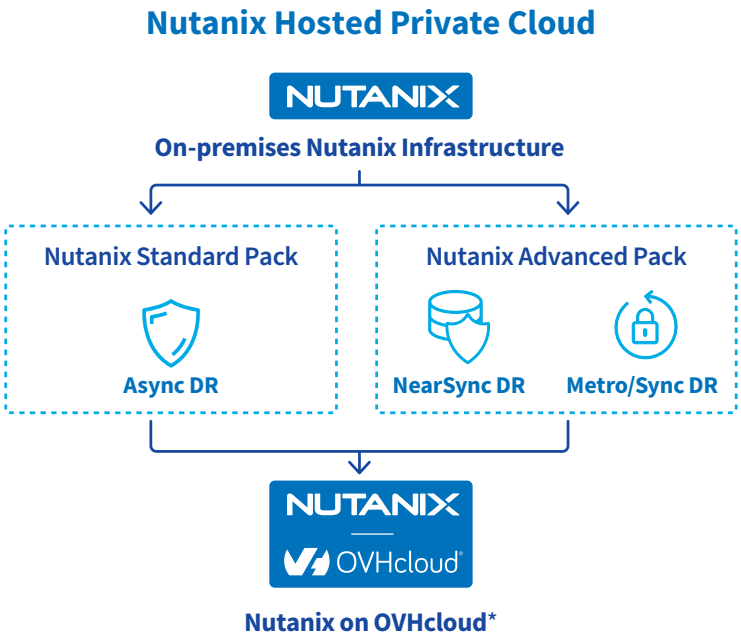
Benefit from HIPAA and PCI-DSS certifications to host your sensitive data, such as personal health, financial and consumer business data.

On-Demand Scaling

Peak load forecast? Provision resources by the hour or month. Depending on your uses, you can revise your dimensions upwards or downwards. You control your infrastructure.

Hybridization and Reversibility

Already using Nutanix? Easily and seamlessly employ the same Nutanix technology that you use internally to orchestrate your infrastructure in a hybrid cloud environment.



*Customers are responsible for obtaining licenses from Nutanix.

Straightforward, Flat-Rate Monthly Billing

Know exactly how much you're going to spend on storage and per VM. There are no commitments or hidden charges for network usage and no ingress, egress or API call fees. There are no zone, region or bandwidth charges. You get a solid product with a predictable price, predictable service and predictable experience. Our pricing is based on a per-VM basis, enabling clients to precisely select the most critical workloads for disaster recovery in a completely transparent model. You can take advantage of OVHcloud Hosted Private Cloud and low RPO and RTO solutions and know all of your costs upfront.

---

[1] Cybercrime Magazine

[2] IASIS

[3] Gartner blog

[4] EY, GISS Report, 2017

[5] Seagate

[6] Zerto

[7] Verizon, Data Breach Investigations Report, 2019

OVHcloud US is a subsidiary of OVHcloud, a global player and Europe's leading cloud provider operating more than 400,000 servers within 37 data centers across four continents. For over 20 years, the company has relied on an integrated model that provides complete control of its value chain from the design of its servers to the construction and management of its data centers, including the orchestration of its fiber-optic network. This unique approach allows it to independently cover all the uses of its 1.6 million customers in more than 140 countries. OVHcloud now offers latest generation solutions combining performance, price predictability, and total sovereignty over their data to support their growth in complete freedom.


us.sales@us.ovhcloud.com


x.com/OVHcloud_US


us.ovhcloud.com