OVHcloud

WHITE PAPER

Stand firm against cyberthreats and plan for the unexpected

Now is the time to take a close look at your Disaster Recovery Plan.

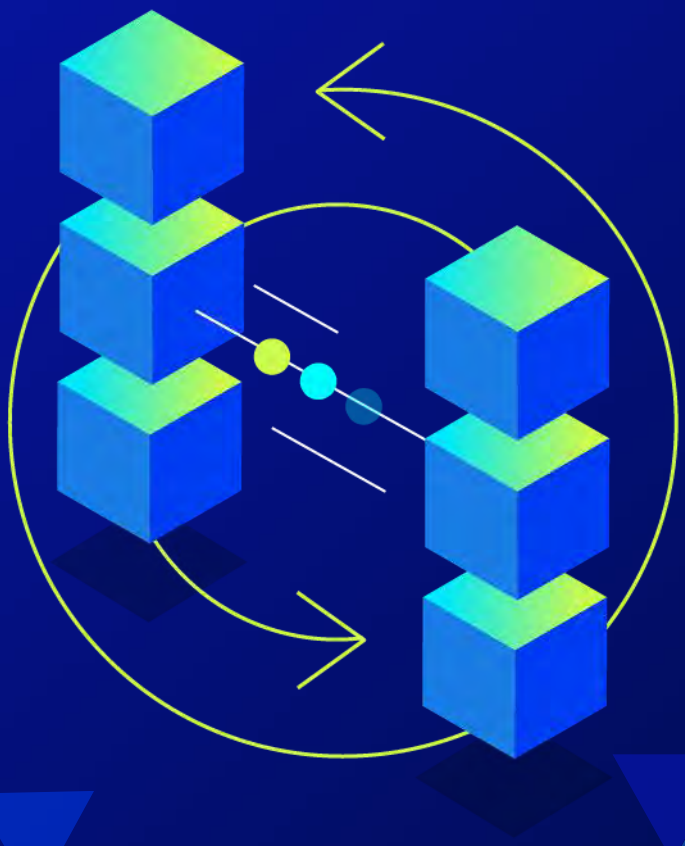


Table Of Contents

A Disaster Recovery Plan is critical component of Your Business Continuity Plan.

Remember when disaster recovery was mostly about protecting against natural disasters, human error, equipment failure, and physical attacks? Today, a new threat has emerged – cyberattacks – and the risk is higher than ever before. The 2022 Veeam Data Protection Trends Report found that **76% of companies taking part in the study have suffered from a ransomware attack** and for the past two reporting years **cybersecurity events** have been **the most impactful outages** they had experienced.[1] Cyberattacks have therefore become the most likely source of data loss worldwide.

Damage related to cybercrime is expected to hit $10.5 trillion annually by 2025.[2]

1 2022 Data Protection Trends Report, Veeam
2 2022 Official Cybercrime Report, Cybersecurity Ventures

Business Continuity and Disaster Recovery Plans — what's the difference?

The **Business Continuity** (BC) plan focuses on the p**olicies and procedures required to keep the company running during an incident**, such as a fire, natural disaster, cyberattack, supply chain failure, pandemic or political issue. The **Disaster Recovery** (DR) plan is a subset, **focusing on the IT infrastructure, data and applications. It addresses whether everything is suitably protected, how leadership and employees access the system, and how to get critical systems restored** as fast as possible to limit the impact on the business.

Building a DR plan that secures your data, whilst also making it available for your employees, is the best way to ensure business continuity. However, if you feel challenged by this, you're not alone.

An unexamined plan can be disastrous.

Compounding the problem is the fact that the perimeter and surface exposure is much greater than they used to be — employees are working in hybrid mode, and interconnected systems and applications are producing and consuming data at exponential speed. It's estimated that over seven billion people and businesses and at least 30 billion devices are connected to the Internet. And data is growing too — it's expected to hit 175 zettabytes by 2025.[1]

Workloads are more diverse, mobile and disparate, across different platforms and geographic regions, whether from the edge, the core or the cloud. All of it needs to be connected to deliver a consistent digital experience. For applications that impact customer and employee experiences there's a growing demand to keep them protected — and available 24/7/365 to meet today's digital expectations and need for speed.

[1] The Digitization of the World, IDC, November 2018

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

If you haven’t done so already, now is the time to take a very close look at your Business Continuity (BC) and Disaster Recovery (DR) plans, because protecting your 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 minimise and even eliminate downtime.

During the Covid-19 lockdown, we turned to the internet for a sense of normality: working, shopping and learning online. This opened a new world of possibilities to cyber criminals who took advantage of society at its most vulnerable. Since then, social engineering and phishing are commonly used to enable other types of cyberattacks, and criminals implement innovative technologies to increase the volume and effectiveness of attacks. In terms of the Information System (IS) exposed to the internet, most companies have more surface exposed now compared to 5 years ago. And more surface equals more risks and requires more surveillance.

The 2023 Thales Global Data Threat Report found that the share of **cyberattacks targeting European Union countries has risen** spectacularly from 9.8% **to 46.5%** in the past six months[1]. The respondents have seen an increase in the volume of malware attacks (59%) and 22% of them experienced a ransomware attack. Fighting cybercrime has therefore become an important part of EU policy.[2]

While the main IT issues that require full site-failover are still hardware and software failures, the most common cause of outages is cybersecurity events, including ransomware, malware and hacking, followed by accidental data deletion or corruption and network failures.[3]

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

The share of cyberattacks targeting European Union countries has risen spectacularly from 9.8% to 46.5%.

1 2023 Thales Global Data Threat Report
2 https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact
3 2022 Data Protection Trends Report, Veeam

The three core pillars of IT resilience

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

- **Continuous Disaster Recovery** – 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. Replication is recommended to aim at continuous availability with no downtime or data loss.
- **Workload mobility** – From migrations, consolidations and moving to new infrastructure, you need the confidence to move your business applications and data workloads easily, without risk, and with 100% protection along the way.
- **Multi-cloud and hybrid cloud** – It's essential to leverage the cloud to accelerate your business. Ensure you experience the benefits of the cloud, have the freedom to choose your cloud, and can move to, from or between clouds.

The journey to IT resilience

The first step on the journey to IT resilience is to reduce systemic risk, which means converging and automating your Disaster Recovery processes, making sure that 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 reduce staff workload, reduce costs and risks, and provide better protection for unplanned disruptions.

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

Backup and replication — what's the best approach?

Backup involves making a copy or copies of data. It's a relatively affordable way to reduce data loss. Backup is typically used to duplicate everything in the enterprise and for long-term archival of business records. It often involves taking snapshots of the data at predetermined points in time. A **backup and restore approach** uses **external backup to bring back an application** in the same datacentre as the original workload, if it's available, or in another one in the case of a major incident.

Replication, however, can deliver a higher level of resilience as it involves making copies or taking snapshots of application data every time a change occurs, and then moving them between a company's data sites. Replication can be **asynchronous or synchronous**.

Asynchronous replication uses snapshots to **capture a point in time and then sends data to a secondary location** later. This means that copies in different sites may not be completely up-to-date and there's still the risk of losing data before all replicas are updated and consistent.

Synchronous replication takes data protection and availability to another level. Data is written to primary and secondary storage locations and acknowledged by the system. All the **replicas always contain the same data and there's no risk of data loss** in case of outage. This method, however, requires low latency and should be performed only on a storage layer. For companies with large volumes of data or high write loads it may be impractical or the overhead cost of writing data to multiple locations can be too high.

Replication technology requires investment in a second site (in an active or inactive mode), therefore it's more expensive, but it truly is disaster recovery because it aims at 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.

Disaster Recovery 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 Disaster Recovery plan.

RPO describes the interval of time since the data was last saved. RTO is the duration of time and a service level within which a business process is restored. Simply put, it's all about how much data you can afford to lose and how much delay in restoring your application you can tolerate. Defining the right balance for your business between RPO and RTO is essential.

RPO — the amount of data to recovered

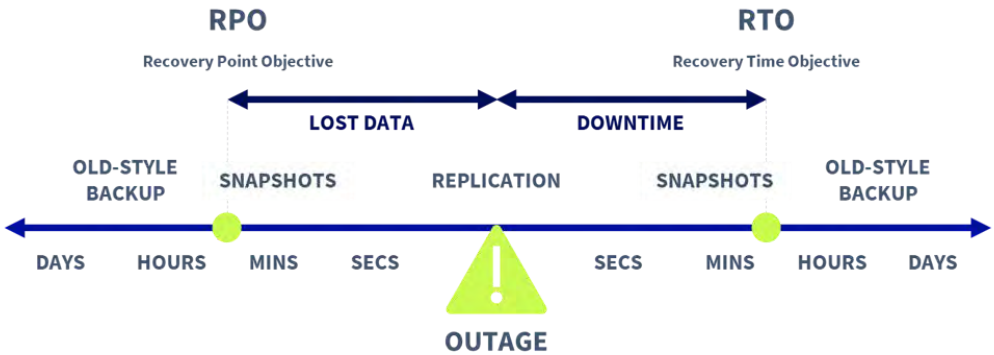
RPO refers to how much data is at risk using a particular method. Here's an example. Let's say a company runs a full backup of their data every day, and their data gets changed regularly throughout those 24 hours. If they run their backup at noon on the button and suddenly their systems fail at 13:00, they've only lost an hour of live data. But if everything is running smoothly until a failure next day at 11:59, they've lost almost 24 hours of data changes since the last backup.

An organisation with data that changes slowly may be fine with a 24-hour RPO if changes lost in the last 24 hours won't have a major impact or if it can be easily recreated. You can insert invoices from one system to another, but can you ask your customers to come back to an online shop after it was unavailable? For businesses with financial transactions or medical data, even 10 minutes' worth of data may be impactful, so the RPO should be much shorter.

RTO - the amount of time required to recover

RTO is all about how long it's going to 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.

A backup service usually takes all the data for the first copy (**full backup**) and then adds only the data that has been changed (**incremental backup**). Optionally, the data is de-duplicated and compressed together into a file, and that file goes on to another storage device. To recover the backup, you need to access and read the data, rehydrate it, and recover it to the replacement server (physical or virtual) 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 much 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 is mission-critical, you'll want 100% replication because it's as close to real-time as possible. However, if you have different levels of data and application needs, you can opt for a plan that includes both replication and backup, while taking into consideration application dependencies and priorities.

Think of your enterprise and Disaster Recovery in three tiers.

Now that you understand 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 **essential** and can wait a few hours, and what's **non-critical** and can wait a few days. You can use different methods of data protection for different tiers. For instance, multiple terabytes of data from the past decade may be important for historical or compliance reasons, but it's not going to hurt if it takes a few days to recover. Business-critical data that is important to your organisation's daily functioning may be okay if it takes a few hours to restore. But if it is data that absolutely can't be lost – it's different.

Non-critical workloads

For non-critical applications, 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. The choice of solution depends on the **volume of data, retention time, and restoration process** you'd like to put in place. For large archives you need to store for years, cold storage (also known as archiving) will have the best price per TB ratio, but the long restoration time makes it an insufficient solution for weekly backup copies.

Essential workloads

For business-critical applications, there are disaster recovery and backup solutions that allow you to restore your workloads quickly and automatically in the primary or secondary location.

The **golden rule of backup** suggests you should have at least **3 copies of your data, stored on 2 different media,** and at least **one of the copies** should be in an **offsite** location. For further protection, one of your copies can be fully offline - this way your organisation can navigate the risks of ransomware. However, any backup is only good as it is being verified. Make sure you monitor your backup tasks daily and regularly test the restoration process.

Mission-critical workloads

For mission-critical applications, the most robust solution is **replication technology** that **continuously creates a copy of data** in a distant location. For a near-synchronous replication, the delay between writing data to the production host and sending it offsite is minimal. The RPO can be measured literally in seconds, so you're reducing the risk of losing minutes' worth of data.

This almost instantaneous replication method is a disaster recovery solution for virtual architectures with real-time replication orchestration allowing users to do granular failover and DR testing. It can 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 workload, giving you the flexibility to maintain availability and take corrective action with little downtime.

The DR solutions that meet your needs and budget.

The Professional Services experts and Solution Architects at OVHcloud can help you determine the best Disaster Recovery solution based on your unique IT enterprise, business operations, and budget.

Protecting data from loss, wherever they are hosted

Whether you host your applications on-premises or in the cloud, you need a durable backup solution that will protect you from data loss. For non-critical applications that tolerate the RPO >24h and RTO > 48h, it's important to have a simple solution that's compatible with your environment. **OVHcloud Object Storage**, certified as **Veeam Ready**, is a high-performance, cost-effective, and S3-compatible storage solution that you can easily add to your existing IT landscape, whether it's a **Public Cloud, Hosted Private Cloud**, or even pure **Bare Metal** environment.

Learn more about Veeam Backup & Restore solutions from OVHcloud and Veeam's experts

Download the white paper

Managed backup solutions for cloud-native applications

At OVHcloud you'll find all the essential building blocks for your cloud-native applications - compute instances in various flavours, **Object Storage** and **Block Storage**, and a vast range of managed database services. To accelerate and simplify your deployments, OVHcloud also provides ready-to-use backup solutions for each component of your application. You can use **Volume Backup** for your **Block Storage** data, Instance Backup to protect data hosted on an instance's disk, and **Automated Backups** for Managed Databases. All these options are integrated with your Public Cloud project and managed via API and CLI.

Learn more about backup and storage options

For VMware on OVHcloud workloads, you can easily set up a backup strategy with our **Veeam Managed Backup** service. Your backups are created from selected VMs, and transferred to your complimentary, dedicated storage. These tasks are fully managed by OVHcloud teams, and you will receive a status report of all your backup tasks daily.

Discover Veeam Managed Backup

Disaster Recovery Planning for essential workloads

Once you have established your backup approach for non-critical applications, it's time to implement a Disaster Recovery solution for your essential workloads. For business-critical applications which should be up-and-running in a few hours, you can set up a secondary site in standby mode and replicate your data there. The secondary datacentre will be running with minimal resources and scaled to the required capacity after the incident.

If, like many others[1], you decided to host your enterprise cloud on VMware solutions, you can benefit from the **Zerto DRP solution**. No matter if you host your infrastructure on-premises and need a secondary site, have your primary and secondary sites in two separate distant OVHcloud locations, or would like to implement DRP from OVHcloud to a third-party cloud provider, the Zerto platform aims at enhancing the resilience of your data in a datacentre of your choice.

Discover Zerto for VMware DRP

TIPCO, an Austrian FinTech company, combines IT skills with many years of treasury expertise to deliver the Treasury Information Platform (TIP) for treasury departments. To address their DAX-indexed customers' needs, from account management to workflow and reporting automation, TIPCO needed secure, dedicated and immediately available IT infrastructure.

HHandling financial data for listed companies requires strict security policies and compliance with European regulations. This need for data sovereignty was a major factor in TIPCO's decision to move their business-critical workloads to OVHcloud.

TIPCO implemented managed **Hosted Private Cloud** in two distant locations, in Roubaix and in Limburg. The company also deployed a multi-level backup and disaster recovery plan. To protect workloads in case of host failure, there's always one "empty" host in the virtual datacentre. VMware vSphere built-in fault tolerance can use it to restart priority virtual machines (VMs) immediately when one of the hosts loses connectivity. As a main backup solution, TIPCO uses **Veeam Managed Backup** to perform automated copies of VMs. The backup copies are stored in a dedicated, complementary infrastructure. The third level of data protection is delivered by **Zerto DRP**. TIPCO configured their DRP via Zerto Virtual Manager (ZVM) for the concerned VMs. Data is securely replicated to the secondary site in France via the private fibre optic network. This way both sites can be either recovery or primary sites.

1 VMware Continues to Lead the HCI Market in Q2 of 2022 for Market Share, according to IDC https://blogs.vmware.com/virtualblocks/2022/10/06/vmware-continues-to-lead-hci-market-q2-2022/

Tailored solutions for mission-critical workloads

To properly adapt the DRP approach to your mission-critical applications, it's not enough to use an out-of-the-box solution. Most enterprise IT landscapes are complex and based on multi-cloud, which calls for a personalised approach and **custom-built DRP** solutions that consider multi-level dependencies and data pipeline meanders. Unless you have a team of experts in-house, the designing and deployment of a robust disaster recovery plan can be a daunting task.

With more than 10 years of expertise, **OVHcloud Professional Services** can provide you with technical advice at every step of your DRP - from defining target infrastructure to training your teams. OVHcloud teams can perform workload and infrastructure audits to understand the criticality level of each of your IT assets and help you to estimate RPO and RTO. They will design and deploy a Disaster Recovery scenario, and finally, test it with your teams to ensure all the necessary processes are in place. For more demanding projects, we can reach out to our partners who will deliver the best experience for your cloud and on-premises environments.

Discover Professional Services

Browse our Partner repository

Why choose OVHcloud?

Resilient & Interoperable Infrastructure

- Standard and proven technologies (including VMware, Nutanix, and OpenStack)
- Highly scalable services
- Mix & match solutions to address your unique IT needs

Cost Control & Predictable pricing

- Transparent pricing
- Unmetered traffic with no egress or ingress fee
- API calls included

Security & Compliance

- Data sovereignty
- Rich certification portfolio
- Security by design
- Enterprise-grade network with Anti-DDoS protection

Contact us

OVHcloud is a global player and the leading European cloud provider operating over 400,000 servers within 33 data centres across 4 continents. For more than 20 years, the Group 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 centres, including the orchestration of its fibre-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 its customers the latest-generation solutions combining performance, price predictability and total sovereignty over their data to support their growth in complete freedom.

OVHcloud

Legal notice

A Disaster Recovery Plan aims at strengthening your protection against data loss. On their own, the solutions presented in this documentation do not guarantee against the loss of your data. It is your responsibility to design and implement a comprehensive Disaster Recovery Plan to help you get back up and running quickly in the event of service interruption, data loss or compromise.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND OVHCLOUD DISCLAIMS ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL OVHCLOUD BE LIABLE FOR ANY DAMAGES WHATSOEVER (SUCH AS WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE FURNISHING, PERFORMANCE OR USE OF THIS DOCUMENTATION AND OVHCLOUD SERVICES, EVEN IF OVHCLOUD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF OVHCLOUD SERVICES AND THIS DOCUMENTATION REMAINS WITH YOU.

OVHcloud reserves the right to make modifications and/or to discontinue any service at any time. OVHcloud, the OVHcloud logo and all other OVH marks contained herein are registered trademarks of OVH SAS. All other marks contained herein are the property of their respective owners.