OVHcloud

VEEAM

WHITE PAPER

Backup-as-a-Service:
a key tool for business continuity

CONTENTS

INTRODUCTION

Your company's operations and performance may depend entirely on the availability of IT systems. However, **these systems face numerous risks that can impact their functionality**, including outages, malfunctions, accidental mishandling, disasters, and cyberattacks. Such incidents can cause severe disruptions or even a complete halt of activities for an indefinite period.

A backup strategy is essential to protect your business from these risks and help recover healthy data when needed. Restoring data is a critical step for your business to resume operations as quickly as possible.

Backups involve copying data from an information system to another medium so that it can be restored in the event of failure or unavailability.

The use of hybrid architectures, with an increasing emphasis on cloud hosting, suggests a good understanding of the responsibilities between business customers and hosting providers in terms of securing data. Each party's responsibilities may vary depending on the nature of the hosting service they have ordered, but they will be set out in the contract with your hosting provider.

In the vast majority of cases, you are responsible for your cloud-hosted data, just like the data you store on-premises. Therefore, it is your responsibility to put in place appropriate measures to ensure successful backup and recovery.

In this white paper, we review the importance of backups and offer **practical solutions that can be adapted to a range of situations** to help protect your data and operations.

When are backups useful?

- Accidental deletion or improper handling of data
- Version update failure (operating system or application)
- Protecting hybrid deployments and migrations
- Internal threats: Malicious users, such as employees leaving the company
- External threats: Ransomware/malware
- Unexpected system and network downtime
- Legal retention and compliance requirements (archiving)

There are many threats to your data, and some are unpredictable. However, in recent years, cyberattacks (ransomware, malware, etc.) have been the most common type of attacks on businesses. Ransomware is a significant risk.

of companies have experienced at least one cyberattack in the past year*

of companies were able to recover data without paying the ransom**

of companies paid a ransom but never recovered their data*

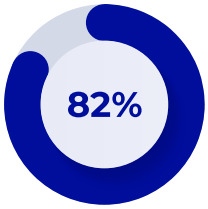
*2023 Veeam Data Protection Report
**2022 Veeam Ransomware Trends Report

1 DATA BACKUP: ADOPT THE RIGHT HABITS!

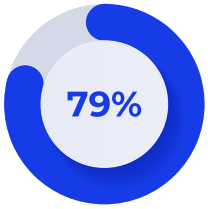
Backing up your data is all about being able to restore it from a reliable, integrated source. It helps you to relaunch in the event of a loss, compromise, or incident affecting one of your data versions. You will need to include the methods for this relaunch in the more general context of your Disaster Recovery Plan (DRP). Whatever your situation, we recommend following a number of best practices to ensure your backups are relevant and secure.

Review your fundamentals

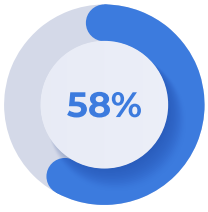
Most organizations feel that they are fully prepared for any loss of data thanks to their backups, but the reality is sometimes surprising. The 2023 Veeam Data Protection Report revealed some figures that challenge prior assumptions:



82% of organizations have an "availability gap" between how quickly they need to recover their systems and how quickly they can be restored.



79% report a "protection gap" between how often their data is backed up and how much they can lose after a failure.



In addition, **58% of the restorations fail**, leaving corporate data unprotected and irrecoverable from a cyberattack.

In the context of pervasive cyber threats and an increased dependence on IT production facilities, it is essential to follow the fundamentals of data backup.

The historical 3-2-1 rule (three separate copies of data, two different media for each set of copies, and one remote site between each set of copies) continues to apply! But with the evolution of IT threats, some additions have been made:

- One set of offline or immutable copies
- Zero errors during restore and data recovery tests

Data protection: the extended 3-2-1 backup rule

Three separate copies of data

Two different media

One offsite copy

One copy (air gap) immutable

Zero errors during backup and

This is why we suggest **evaluating your data recovery strategy** to find any weaknesses or areas for improvement.

Draw up a backup plan, depending on your activity

Here are some key points to address in order to build a relevant backup plan.

- What are your critical/sensitive data and databases?
- Which systems are essential to business continuity?
- Are there any interdependencies between systems?
- What is the maximum acceptable interruption time (Recovery Time Objective)?
- How much data could you accept losing (Recovery Point Objective)?
- What backup frequencies and retention periods are necessary to achieve these objectives?
- What alternative remote sites are available?

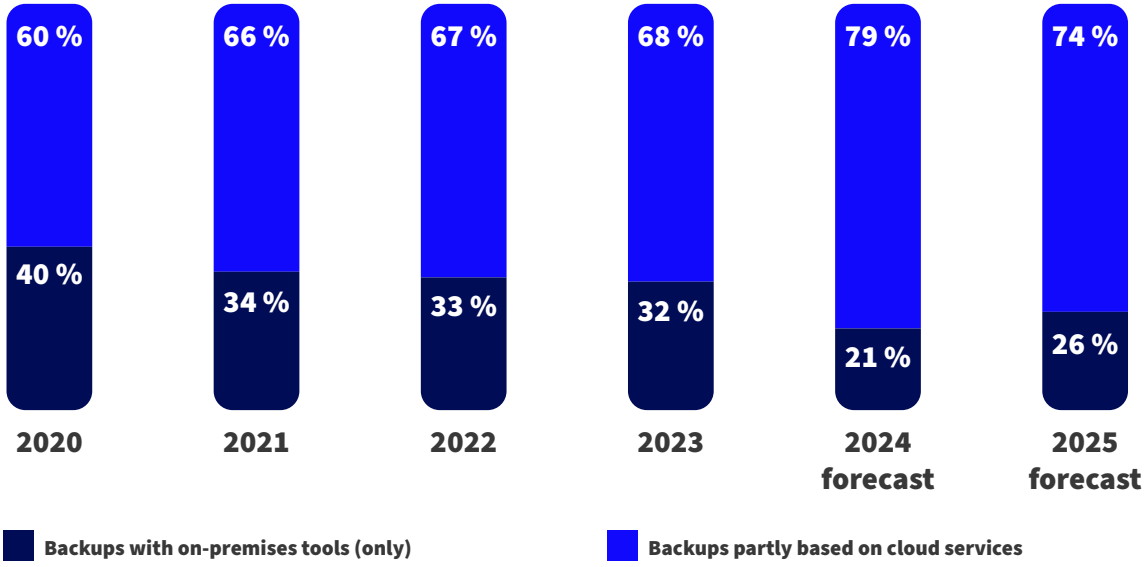
This assessment will help you implement an effective data backup and recovery strategy to secure your business.

Consider Backup-as-a-Service

In an era of increasingly sophisticated cyber threats, companies often lack the resources to enhance their data protection. Luckily, **Backup-as-a-Service** (BaaS) solutions are expanding. In 2023, the trend towards **outsourcing backups** to a cloud hosting provider was clear to see.

According to the 2023 Veeam Data Protection Report, 74% of companies plan to start using a cloud-based backup solution by 2025.

Delegating backups to a cloud service provider is a worthwhile solution for simplifying or automating backup management. You get specialized services and concrete commitments (SLAs, penalties, etc.).



2 COULD YOUR BACKUP STRATEGY BE IMPROVED?

Whatever your current hosting method (on-premises or cloud), **it's your responsibility to protect your data**. When faced with a multifaceted threat, some commonly used security devices are inadequate. Here is an illustration using two specific examples.

If you're hosting data in the cloud... a snapshot is not a backup!

You have an IaaS cloud solution hosted by a service provider (such as the Hosted Private Cloud powered by VMware on OVHcloud). Your contract may include protective devices for your virtual machines (VMs) or instances. You can also take these snapshots yourself.

What this covers

Snapshots are an image of your VMs taken at a given time. You can use them to restore the previous state of your VM.

This covers certain situations, such as handling errors, version upgrade issues, or a failure of the systems hosting the VMs.

What this does not cover

- Snapshots do not recover individual files or a data/system partition (they are limited to an entire machine recovery).
- Snapshots reside on the same media as production data, so they remain exposed to incidents that may affect this medium.
- According to best practices, snapshots aim for short retention periods (daily or weekly). They do not allow you to go back to an old version of the VM and data.
- If the production data is encrypted by ransomware, the snapshot will copy it as is. It will not allow the recovery of sound data.

Therefore, Snapshots are not complete backup systems and cannot serve as a standalone data protection strategy. Additionally, they are not suitable for regulatory archiving and are not covered by any SLAs from the hosting provider.

Snapshots capture and save the state, data, and configuration of a virtual machine, enabling a quick and easy recovery to that previous state.

If you carry out your backups internally... ... a copy on a second site is essential!

You host your production data on-premises and/or with a hosting provider. **You carry out your backups yourself without outsourcing and without making a second copy on a site separate from where the production data is located**. You perform regular restore tests. At first glance, this is working seamlessly.

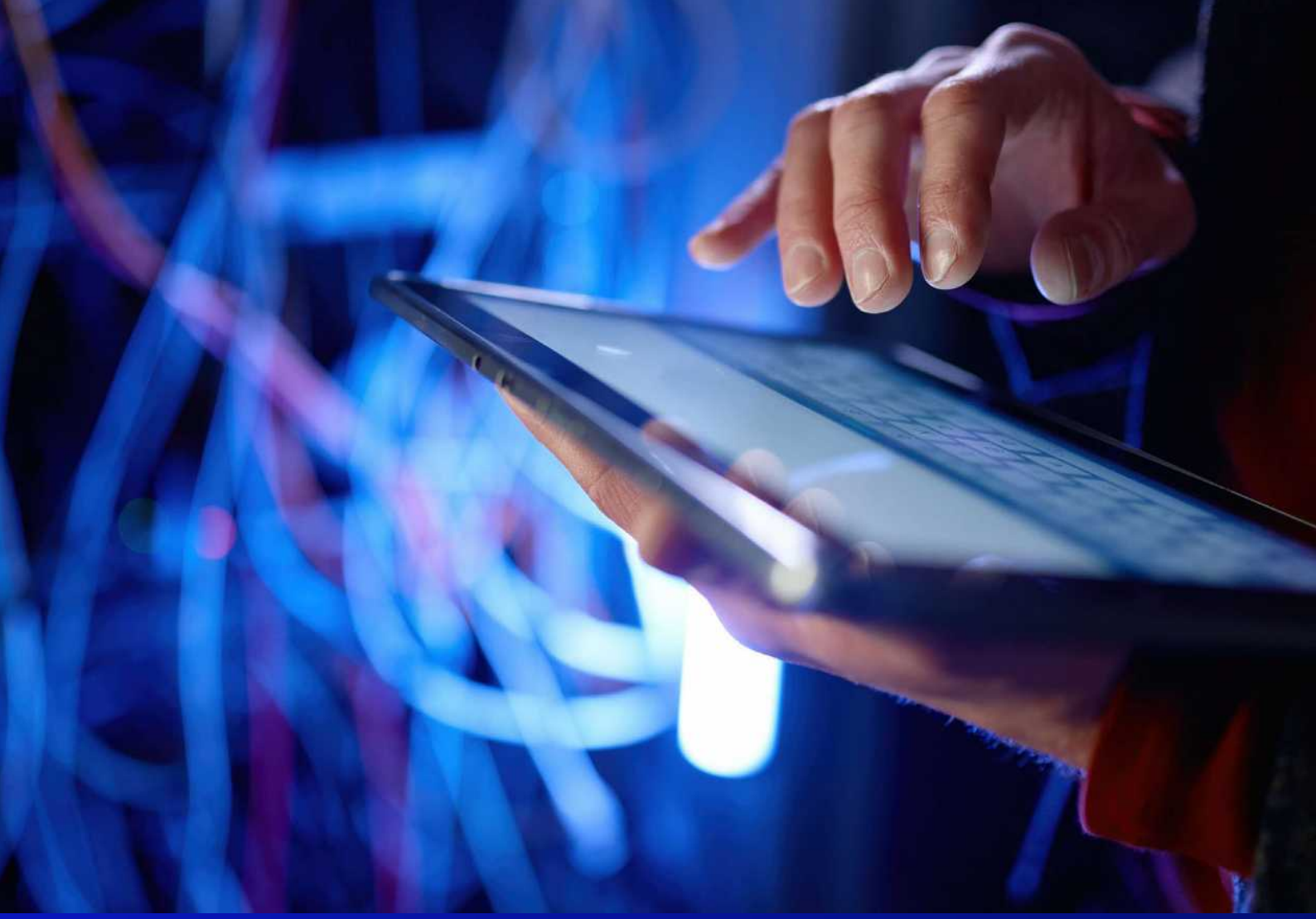
What this covers

- You get a first level of consistent security for your data in a hybrid environment.
- You are protected against handling errors or version upgrade faults.
- You can restore your data with different levels of granularity: file, complete system, logical, physical, etc., with the ability to choose your retention periods (for archiving and audits).
- You can deal with hardware failures on your own systems or those of your hosting provider.

What this does not cover

- Your approach does not address specific risks.
- You are not protected **against a major disaster** affecting your infrastructure or that of your hosting provider (natural or accidental disasters, fires, floods, power failure, etc.). Therefore, you don't fulfill the conditions for drawing up a DRP.
- Your strategy does not protect you **from ransomware** attacks. These will contaminate your backups before encrypting the primary data.

To avoid a disaster, it is highly recommended that you backup to a remote site. The server will not be subject to the same attack rules and, therefore, will not have the same vulnerabilities. In addition, to ensure that you have healthy backup data in the event of a ransomware attack, these backups will need to be "offline" (air-gapped) or made immutable.



Backup immutability: A major challenge

A backup is deemed immutable when the backed-up data can no longer be modified at all. The goal of an immutable backup is that data will **be able to be restored on production servers with complete confidence** and with the certainty of having healthy, uncorrupted data.

Traditional backups may not be enough to restore encrypted data during an attack, as the backup itself may have been contaminated. **Your backup data must be isolated and unchangeable**; this is the only way to ensure recovery if the systems in production have been infected.

Best practices for setting up immutability recommend a minimum retention period of 14 days.

WHAT SOLUTIONS ARE THERE TO BOOST YOUR BACKUP SECURITY?

Here are two types of solutions developed to combat current threats and strengthen backup security.

The managed backup service

A Backup-as-a-Service (BaaS) solution from your cloud service provider offers a comprehensive backup plan for your hosted systems. Backups are stored in secure data centers and are based on technologies and architectures that can better guarantee their immutability. This enhances the integrity of the backed-up data and protects it against any subsequent modifications or attacks.

Managed backup services are turn-key solutions that boost the level of protection for your cloud-based systems and data. In terms of usage, they provide you with:

- **Advanced logical recovery capabilities** at a file level
- **Total reversibility**, with the ability to retrieve all of your backed-up data if you wish
- Flexibility in your **choice of retention periods**
- **Time-saving** and access to state-of-the-art expertise
- The use of **up-to-date backup tools**

The commitments provided by a BaaS service are formalized by service level agreements (SLAs) in accordance with the rules for transferring responsibilities between the customer and hosting provider. Disaster recovery or restoration procedures remain the responsibility of the customer in accordance with the terms of their DRP. These procedures must also be regularly tested.

Backup to a remote cloud

If your data is hosted in your own data center (on-premises) or you have a hybrid infrastructure, you can opt for a remote backup with a second cloud service provider. With this approach, the backup environment is separate from your production environment. **This helps protect your systems in several ways:**

- Your backups are conducted and stored in a remote data center, protected **from any incidents or disasters at your production site(s).**
- You benefit **from the different technologies in your production and backup** sites, as the backup storage formats are different from those of the production site. This is part of the response to ransomware-type attacks, acting as a barrier to prevent their spread.

Object storage: The key to immutability

In the field of digital data storage, WORM (Write Once Read Many) technology allows data to be written to media only once and prevents its erasure or subsequent modification. The data is considered immutable; authorized users can read it as often as necessary, but they cannot edit or delete it. This immutable aspect plays a vital role in meeting security and data compliance requirements and protecting against ransomware and other threats.

Based on a set of certified hardware and tools, OVHcloud Object Storage provides object immutability by using the WORM model via the Object Lock feature. Object Lock prevents objects from being deleted or overwritten for a set time period and/or indefinitely.

4 OVHCLOUD/VEEAM SOLUTIONS

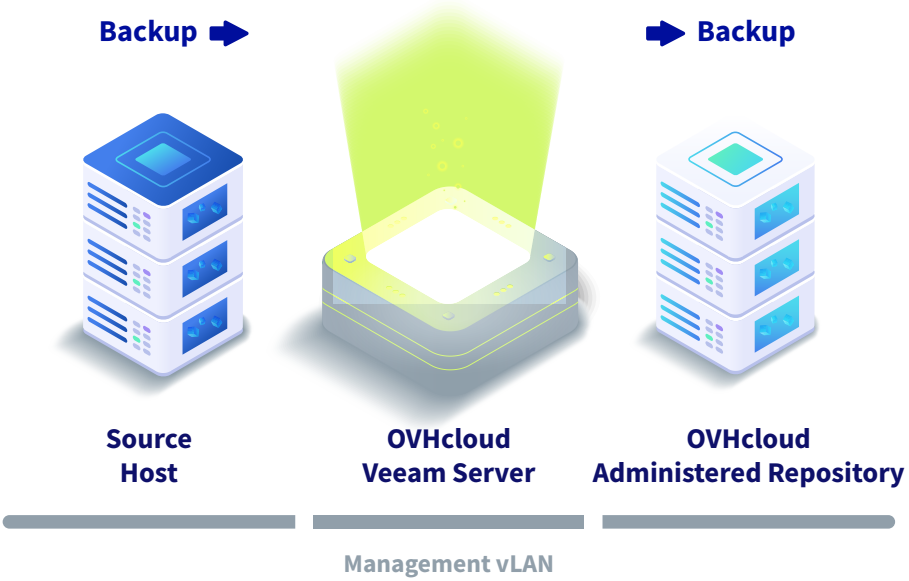
With OVHcloud solutions based on Veeam backup technologies, you can deploy data protection plans adapted to current risks.

VEEAM MANAGED BACKUP

Backup-as-a-Service for backups of your systems hosted on VMware on OVHcloud

OVHcloud's managed backup solution, based on Veeam Backup & Replication technologies, enables you to **delegate automatic backups for your systems**. A clear and precise SLA speaks to the commitment and quality of service.

- **Backup-as-a-Service:** Your system backups are fully automated and monitored by OVHcloud
- **Storage included:** Your data backups are stored in our dedicated US infrastructures. You can access your backups easily via an administration link
- **Daily monitoring:** A customizable report is sent to you every day. This report will include a list of all your backups and their respective statuses
- **Restoration/Reversibility:** You can restore your machines at any time at each file level. You enjoy full reversibility, with the ability to retrieve all of your backed-up data if you wish



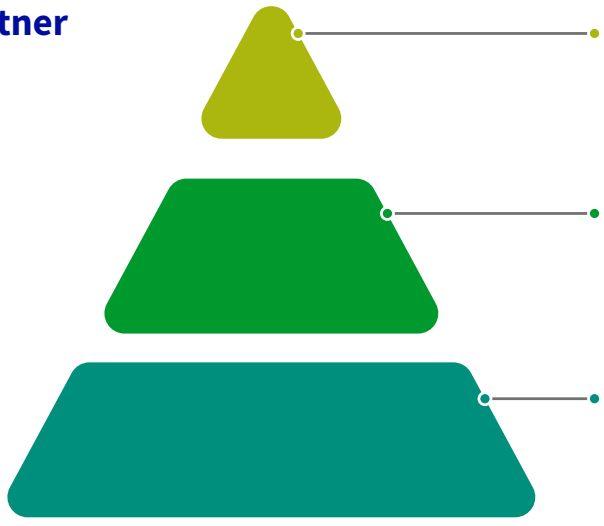
OVHCLOUD OBJECT STORAGE CERTIFIED VEEAM READY

Certified object storage for your backups

As part of your backup framework, Veeam Ready allows you to use certified object storage from OVHcloud and make a second copy of your data on OVHcloud infrastructures. This way, you get an additional, unalterable backup for systems hosted on-premises or with another cloud service provider.

- **Remote backups and location:** For remote backups with Veeam Cloud Connect, you can choose Veeam Ready storage and select the location of your backups
- **Immutability:** The backups made in object storage are not altered or modified
- **Reversibility:** Access your full backup content and restore with OVHcloud or elsewhere as needed
- **Billing:** Based on the volume of storage used. There is no additional charge for repeat API calls
- **Veeam Ready certification:** S3 protocol compatibility provided by Veeam

Our Veeam partner certifications



Veeam Integrated
Partners with complex or deep integrations

Veeam Ready
Veeam Ready Partners with testing-certified Veeam compatibility

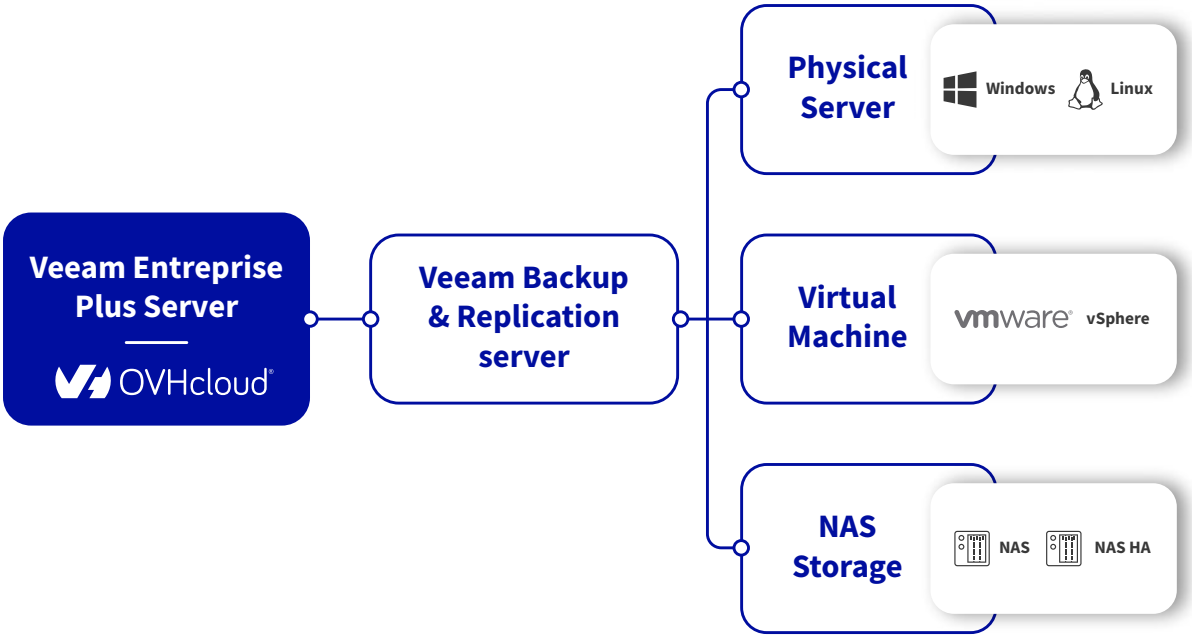
Veeam Infused
Partners using available APIs

VEEAM ENTERPRISE PLUS

Data protection adapted to hybrid infrastructures

Deploy your Veeam Backup & Replication base and use OVHcloud Enterprise Plus licenses to back up your systems yourself.

- **Secure your activity:** Set up backup and replication for your applications, machines, and data to quickly recover from infrastructure downtime.
- **Take control of your backups:** Manage all your backups – at OVHcloud or in your own data center – regardless of the number of machines you have or their location
- **Enable immutability:** You can choose to back up your data to Veeam Ready S3 object storage with OVHcloud
- **Pay-as-you-go:** Your services are billed as closely as possible to your real-time usage of our solution from the following month onwards



A solution such as **S3 Object Storage** hosted at OVHcloud will enable you to store data in an immutability-compatible way.

OVHcloud legal notices

The performance of the services varies depending on usage, configuration, and other factors.

OVHcloud's services are subject to the general and specific terms and conditions in force at the time of ordering. OVHcloud reserves the right to change and terminate its services at any time.

A backup system is a tool that strengthens your protection against data loss. It does not guarantee against the loss of your data on its own. It is your responsibility to design and implement a set of measures in a global disaster recovery plan in order to promote a quick relaunch of your services in the event of service interruption, data loss, or compromise.

Want to strengthen your backup strategy?

Contact us

OVHcloud US is a subsidiary of OVHcloud, a global player and Europe's leading cloud provider operating more than 450,000 servers within 43 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