What's the best way to prepare for the unexpected?

All you need to know about data protection and backup

Take control of your data protection

Protection
is about ensuring the confidentiality, integrity, and availability of data.

Carrying
out backups ensures that data is available and recoverable when needed.

Maturity levels

While this process requires thought, time, and investment, you can go at your own pace with suitable, targeted actions.

0 NON EXISTENT	1 INITIAL	2 REPEATABLE	3 DEFINED	4 MANAGED	5 OPTIMIZED
Everything needs to be done	Unpredictable, inconsistent, and high-risk	Reactive, unstable, and manual	Documented, standardiszed and reviewable	Proactive, monitored, and partly automated	Automated, integrated, and predictable

Downtime & Loss

With data volumes growing exponentially, and a growing number of companies declaring themselves to be "data driven", the risks are higher than ever.

x2 THE AMOUNT OF DATA DOUBLES APPROXIMATELY EVERY TWO YEARS.[1]

60% OF COMPANIES HAVE TAKEN STEPS TO BE "DATA DRIVEN".[2]

94% OF COMPANIES HAVE REPORTED UNPLANNED DOWNTIME.[2]

An increasingly complex issue

Data-driven organizations are faced with increasing complexity when it comes to data protection and disaster recovery.

Not just a hypothetical scenario...

Threats to data tend to multiply and intensify.
And when they do occur, the consequences tend to get worse.

During 2021

93% of businesses experienced a data-related service interruption.[2]

68% of respondents had experienced at least 4 such interruptions.[2]

83% reported that at least one attack had resulted in their data being corrupted.[2]

60% found that their data was irrecoverable.[2]

2.3 INTERRUPTIONS on average per month[4]

5.1 HOURS average time from the start of the interruption to service recovery[4]

Where do these threats come from?

There are multiple sources, both internal and external.

DDoS ATTACKS ransomware CYBER ATTACKS malware viruses
HARDWARE phishing FAILURES OUTAGES OVERHEATING power supply issues
hardware loss and theft deletions internal information leaks HUMAN UNAUTHORIZED ACCESS ERROR misconfigurations inadequate security policies
FLOODS earthquakes NATURAL DISASTERS fires hurricanes WILDLIFE

23% Human error is the number one cause of data breach incidents.[3]

x2,5 Ransomware is 2.5 times more likely to cause an incident than a natural disaster.[2]

62% Increase in ransomware attacks worldwide in 2020 compared to 2019.[5]

2 The number of the main reasons for requiring disaster recovery: 56% software failures and 47% hardware failures.[2]

1st The biggest challenge is the reliability of backup and recovery operations.[2]

3-2-1 backup strategy

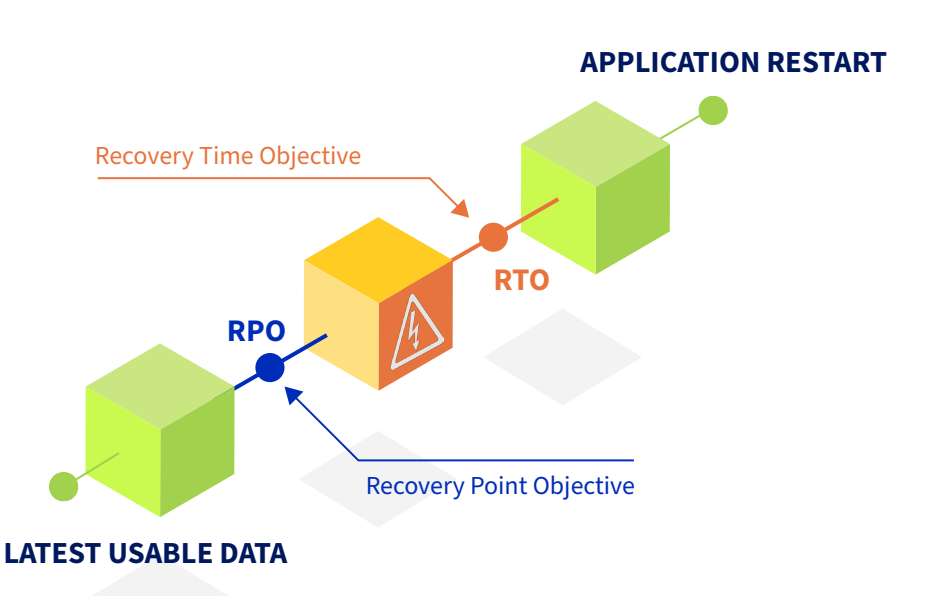
x3 x2 x1

- **Create 3 copies of your data** i.e. the original plus 2 backup copies
- **Store them on 2 different media:** disk and/or tape on a remote site, cloud storage, etc.
- **Keep 1 copy offline** on 1 storage solution disconnected from the rest of the network or on 1 removable storage media

A comprehensive data protection strategy:

1. Evaluate all risks
Identify all the threats your organization could face, as well as your most sensitive/critical data.

2. Define your objectives
What do you need to implement to ensure your business continuity?
In the event of downtime, what will be the recovery time objectives (RTOs) and recovery point objectives (RPO) for your systems and applications, distinguishing between those that are non-critical, essential, and critical?



3. Developing a tailored strategy
Choose an appropriate disaster recovery strategy (cold, warm, or hot scenario), or opt for a cloud disaster recovery plan (DRP) to take advantage of continuous data protection, immutability, one-click failover, automation, scalability, and more.

4. Test and repeat
Check regularly that your strategy is always tailored to your needs and make sure it works.

5. Document the procedures
Provide clear and accurate information on every aspect of your DRP, including response procedures, communication, and system recovery.

6. Train and inform employees
Don't forget to educate your colleagues on best practices in IT security.

7. Monitor, maintain, and update
Be ready to detect suspicious activity so that you can react quickly and effectively. Regularly review and update your DRP to ensure it is relevant and can handle attacks and emerging issues.

#MoveToCloud

55% OF COMPANIES WILL HAVE ADOPTED A CLOUD DATA PROTECTION STRATEGY BY 2025.[2]

Before migrating

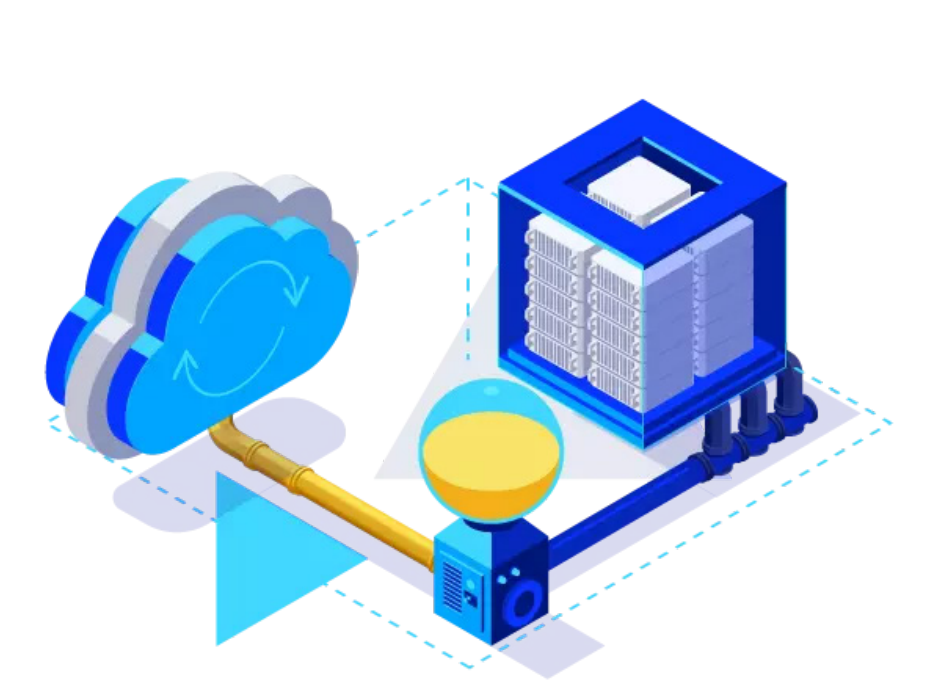
- **Check** the backup services included in the solutions you are using.
- **Move** towards standard secure storage solutions adapted to your current and future needs (compliance, performance, price, etc.).
- **You should also consider** replicating your data (copying and storing it in multiple locations) to improve availability and accessibility.

Choosing a provider

Before you make your choice, we advise you to note down all the guarantees offered in terms of compliance, sovereignty, SLA, reversibility, and so on.

OVHcloud®

Over 20 years of expertise



- **Highly resilient, certified, and secure infrastructures** that host integrated and interoperable services.
- **Predictable invoices** with no hidden fees, so you can accurately manage your investments.
- **An ecosystem of specialists** comprised the market leaders in data protection (NetApp, Nutanix, Veeam, VMware, and Zerto) as well as a network of more than 1,000 partners.

Sources :

[1] According to Moore's Law, an empirical observation made by Intel's co-founder, corroborated by numerous research reports and studies published by the analyst firm IDC and EMC Corporation

[2] Based on an estimate from IDC's *The State of Ransomware and Disaster Preparedness* white paper published in May 2022

[3] Based on an estimate from IBM's 2020 *Cost of a Data Breach Report*.

[4] According to the annual report *The Cost of a Data Breach* published by Ponemon Institute in 2021

[5] According to the *SonicWall Cyber Threat's 2021 Annual Report*

Infographic created in June 2023