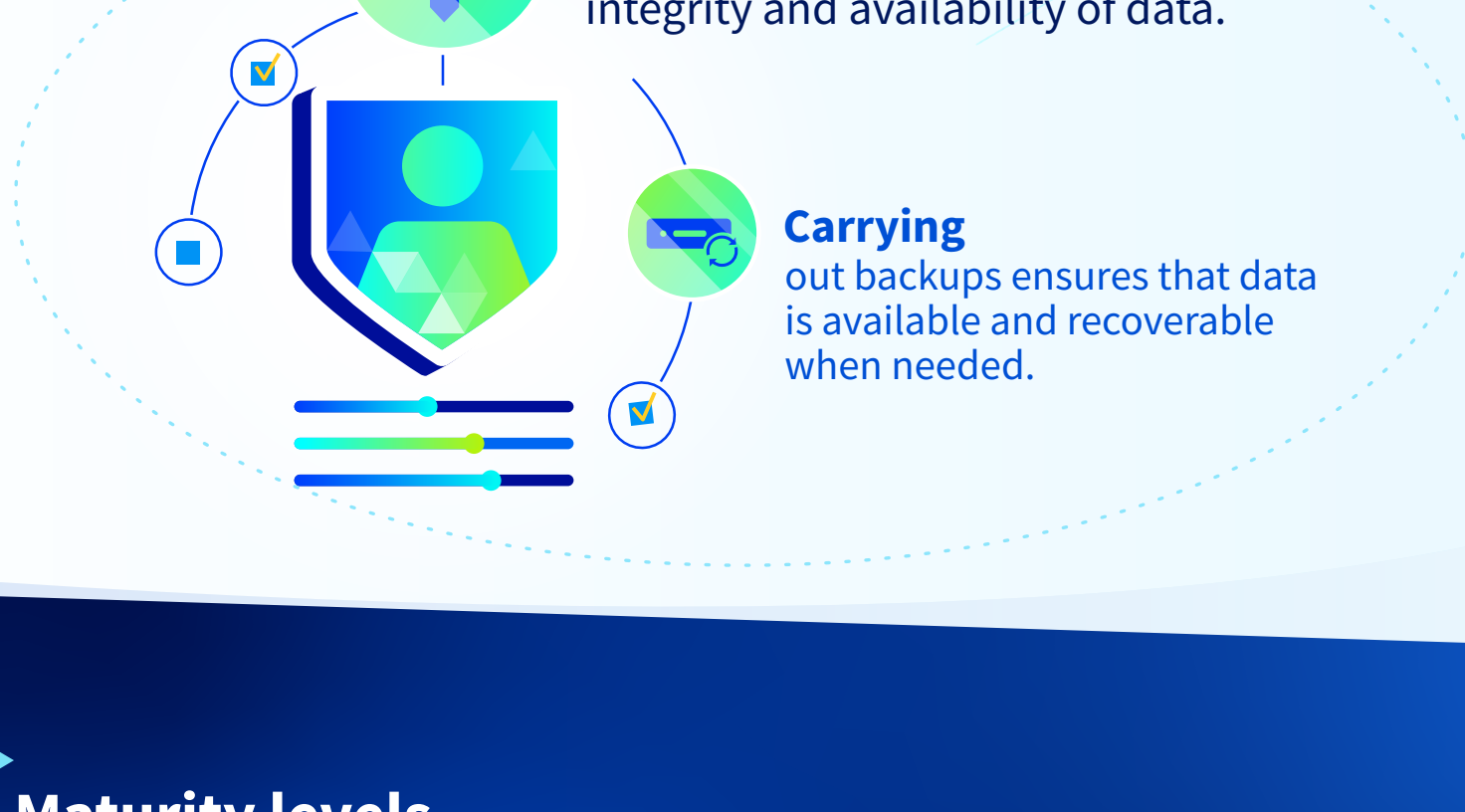




What's the best way to prepare for the unexpected?

All you need to know about data protection and backup

Take control of your data protection



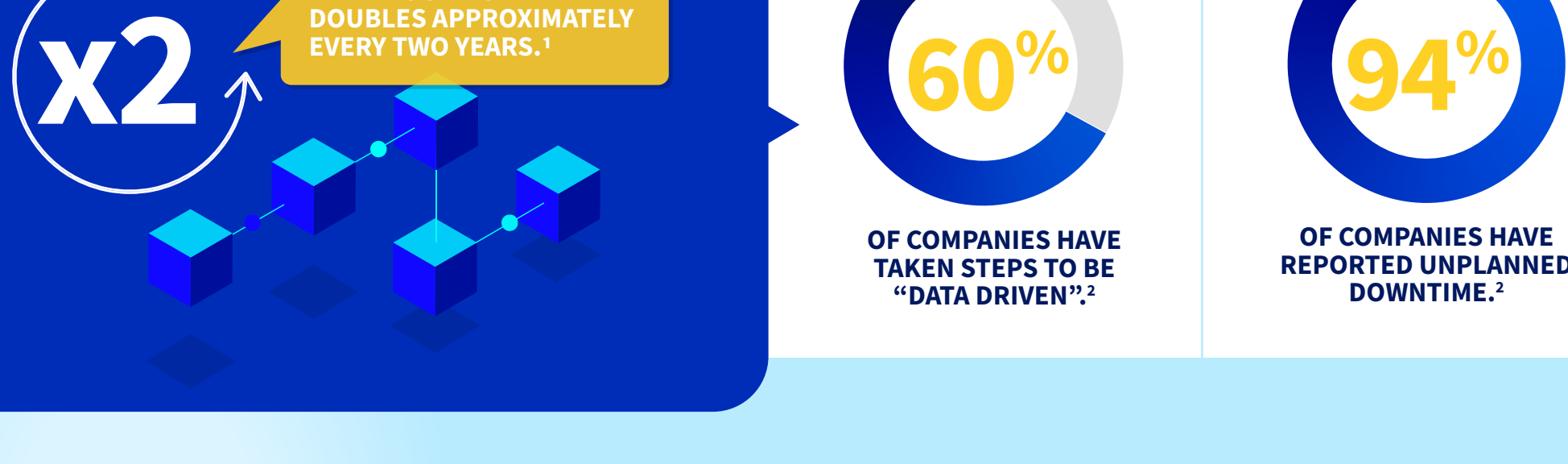
Maturity levels

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



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.



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...

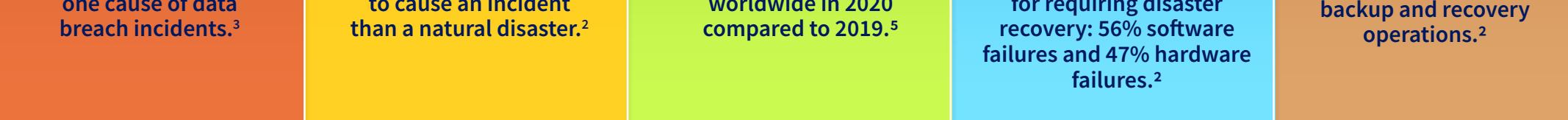
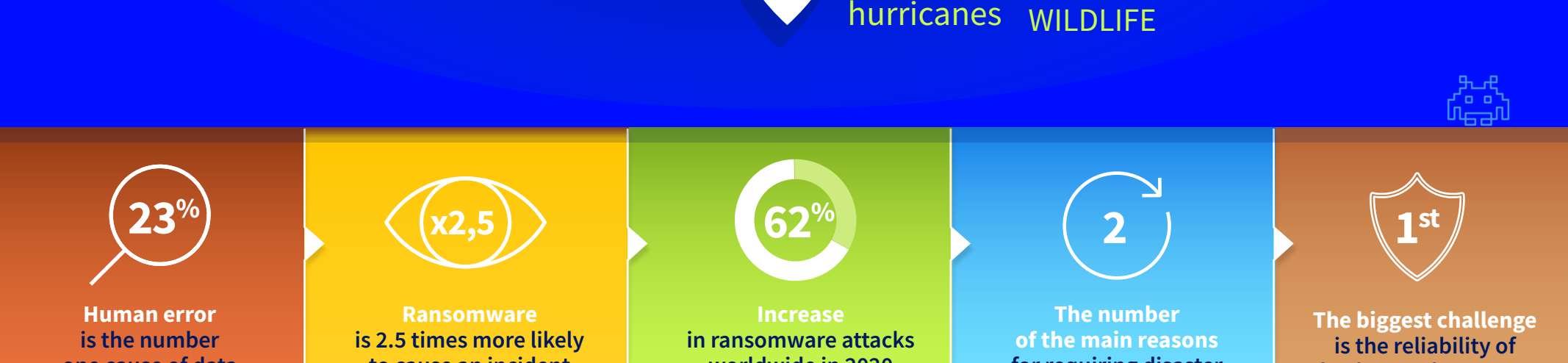
Threats to data tend to multiply and intensify. And when they do occur, the consequences tend to get worse.

During 2021



Where do these threats come from?

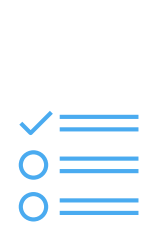
There are multiple sources, both internal and external.



3-2-1 backup strategy



A comprehensive data protection strategy:



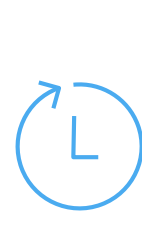
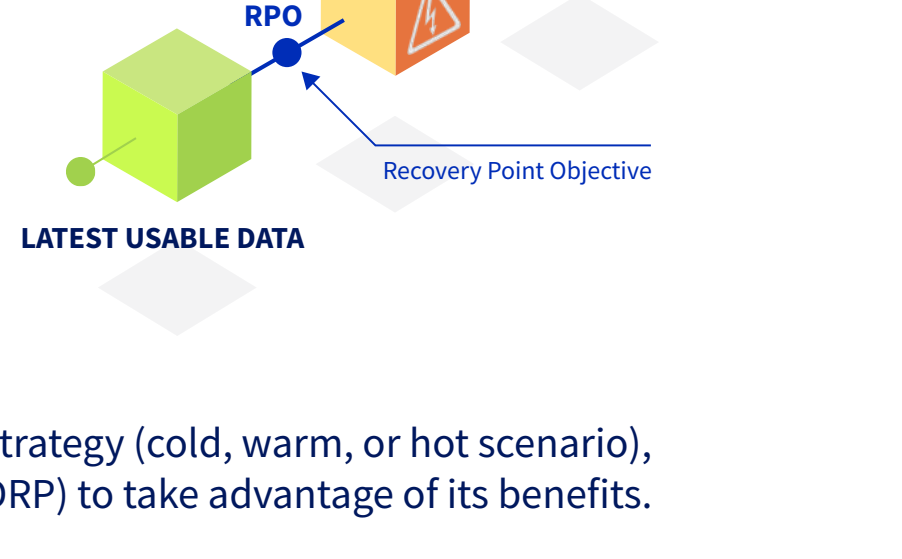
1. Evaluate all risks

Identify all the threats your organisation 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 for your systems and applications, distinguishing between those that are non-critical, essential, and critical?



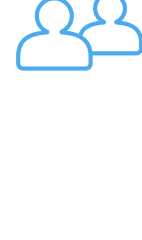
3. Developing a tailored strategy

Choose an appropriate disaster recovery strategy (cold, warm, or hot scenario), or opt for a cloud disaster recovery plan (DRP) to take advantage of its benefits.



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



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** comprising the market leaders in data protection (NetApp, Nutanix, Veeam, VMware, 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