inetum realdolmen
Positive digital flow

Ransomware: wat als alleen back-up u nog kan redden?

Conny Van den Steen, Inetum-Realdolmen

inetum
realdolmen
Positive digital flow

Ransomware

What if only backup can save you?

‘A common ransomware "feature" enhancement is deleting or encrypting backup data prior to launching the main attack. … Cyber attackers are intelligent — and dedicated — deleting and encrypting backups is a critical way to improve their odds of receiving the ransom.’

“Data Of Last Resort: Building Cyber Recovery”

Agenda

Backup best practices

Choosing the right backup technology

Cloud data protection

Enterprise backup vs Point backup solutions

Zero trust concepts in backup

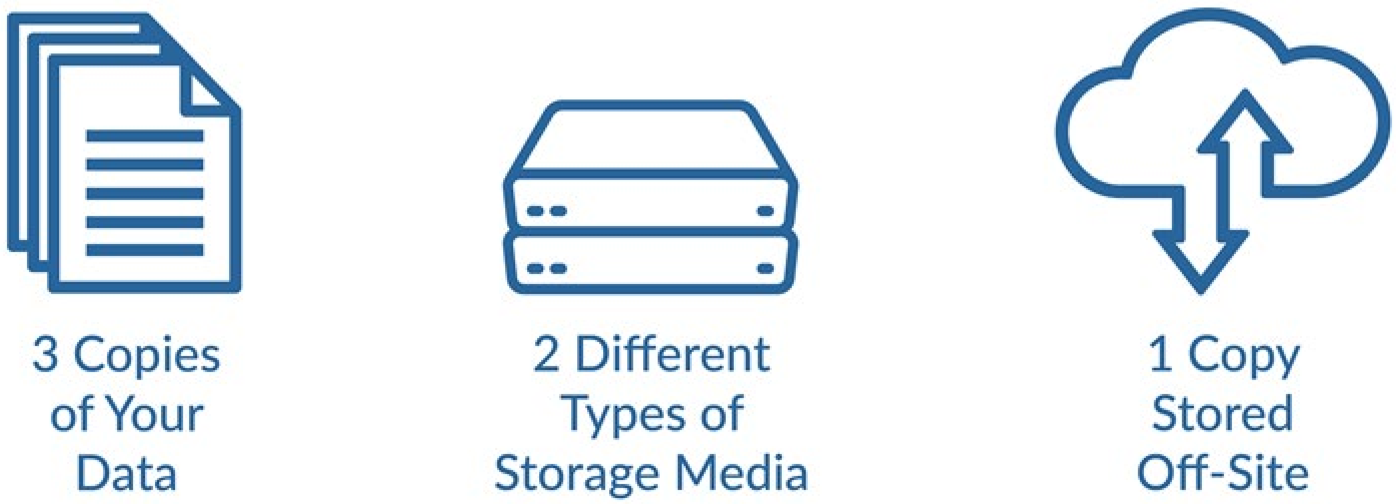
Backup data restore as response to ransomware

Where to start with implementing a backup strategy?

data
backup
L
M
Shif

Backup basic best practices

- Take regular & automated backups
- Encrypt data that is kept offsite
- Perform regular restore tests
- Follow the **3-2-1 backup rule**:

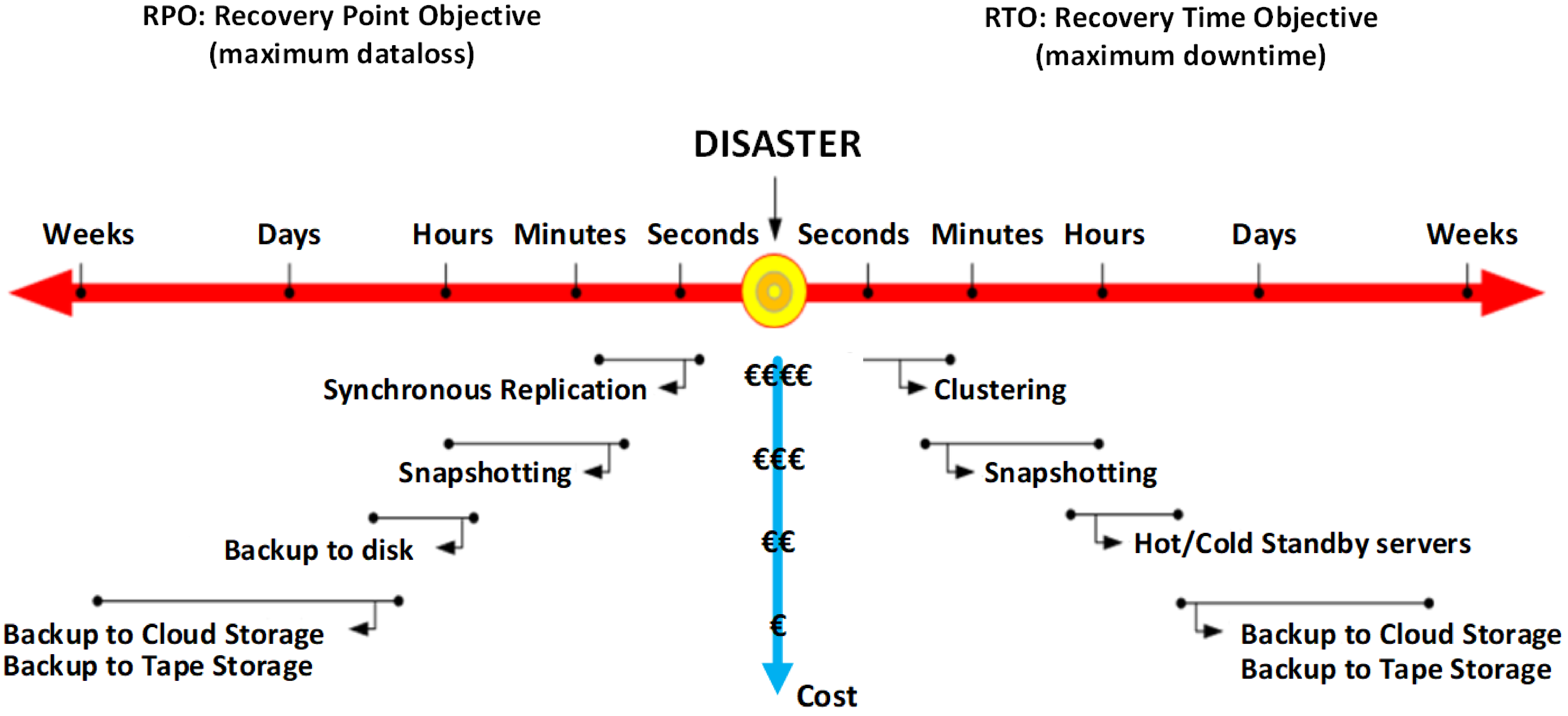


3 Copies of Your Data

2 Different Types of Storage Media

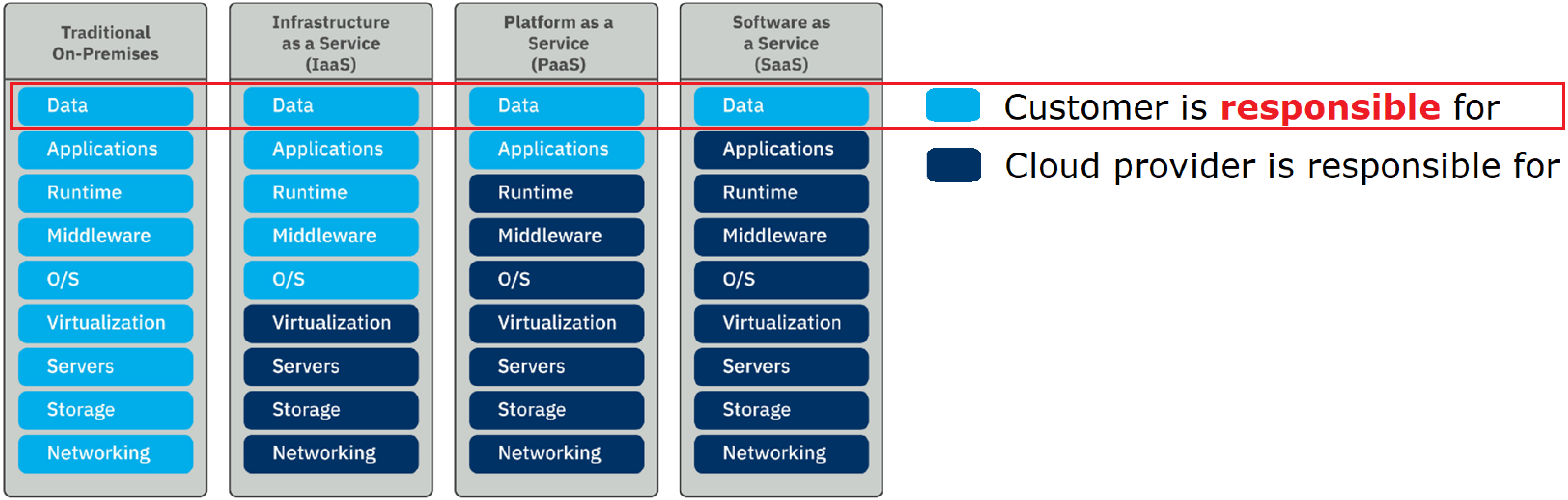
1 Copy Stored Off-Site

How to choose the correct technology?



And what about my data in the cloud?

Shared responsibility model



Traditional On-Premises	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Data	🟦 Data	🟦 Data	🟦 Data
🟦 Applications	🟦 Applications	🟦 Applications	⬛ Applications
🟦 Runtime	🟦 Runtime	⬛ Runtime	⬛ Runtime
🟦 Middleware	🟦 Middleware	⬛ Middleware	⬛ Middleware
🟦 O/S	🟦 O/S	⬛ O/S	⬛ O/S
🟦 Virtualization	⬛ Virtualization	⬛ Virtualization	⬛ Virtualization
🟦 Servers	⬛ Servers	⬛ Servers	⬛ Servers
🟦 Storage	⬛ Storage	⬛ Storage	⬛ Storage
🟦 Networking	⬛ Networking	⬛ Networking	⬛ Networking

🟦 Customer is **responsible** for

⬛ Cloud provider is responsible for

Data in the cloud definitely needs backup!

Enterprise vs point backup solutions

Enterprise backup solutions

- Broad support for many different platforms (incl. Cloud), applications & databases
- Many features (hardware snapshotting, REST API , deduplication, encryption …)
- Highly configurable.
- Can get complex.

COMMVAULT

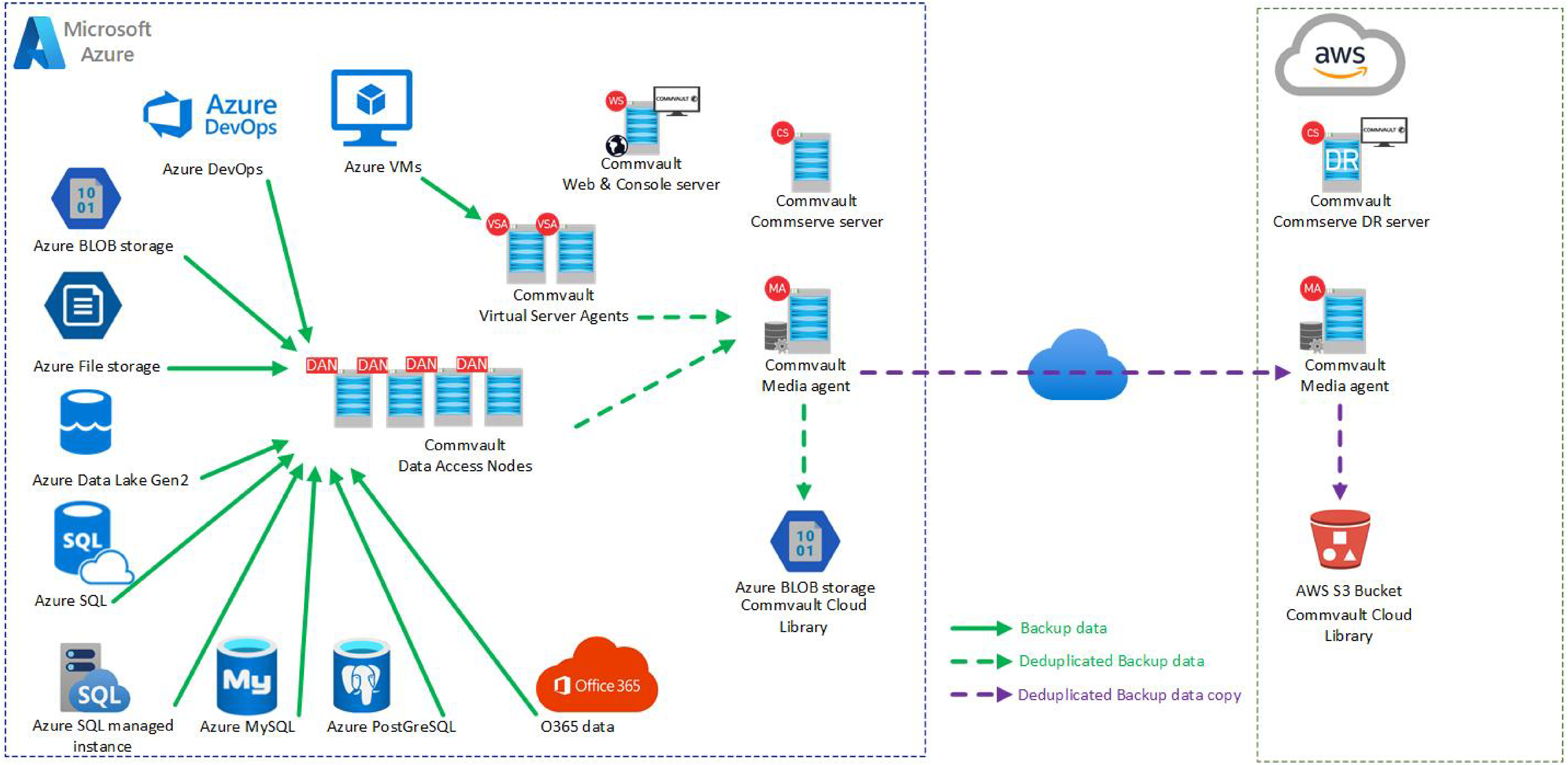
Point backup solutions

- Specialize in protecting 1 or a few platforms (for ex. M365).
- Can be on-prem or SaaS (or both).
- Aim for ease-of-use.

AvePoint

Example of an EBS in the cloud

Based on COMMVAULT


Microsoft Azure
Azure DevOps
Azure VMs
WS
Commvault Web & Console server
CS
Commvault Commserve server
Azure BLOB storage
VSA
Commvault Virtual Server Agents
Azure File storage
DAN
Commvault Data Access Nodes
MA
Commvault Media agent
Azure Data Lake Gen2
Azure SQL
Azure BLOB storage Commvault Cloud Library
Azure SQL managed instance
Azure MySQL
Azure PostGreSQL
Office 365
O365 data
Backup data
Deduplicated Backup data
Deduplicated Backup data copy
aws
CS
DR
Commvault Commserve DR server
MA
Commvault Media agent
AWS S3 Bucket Commvault Cloud Library

Some points of attention

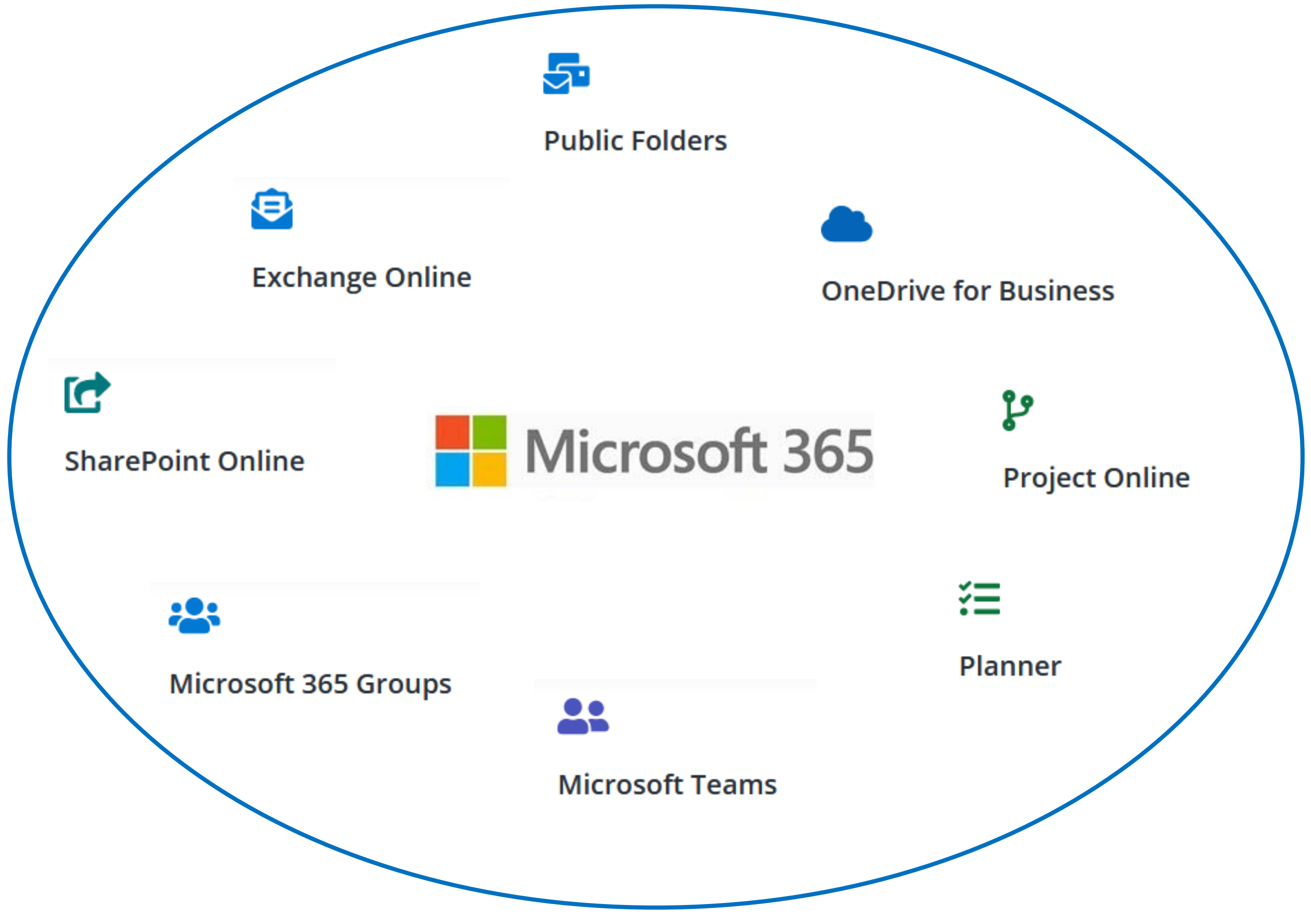
- Data egress costs need to be considered (cloud-to-cloud copies, restores).
- Data seeding can take a long time.
- Early access and early deletion costs need to be considered (choice of storage).
- Bandwidth, compute, storage … all need to be calculated to avoid bottlenecks.

But …

- You have **full control** over what you backup and where you store it, how you store it and how long you retain it.
- All backup activity is centralised
- Your backup environment is managed with a “**single pane of glass**”.
- limited integration in native SaaS applications

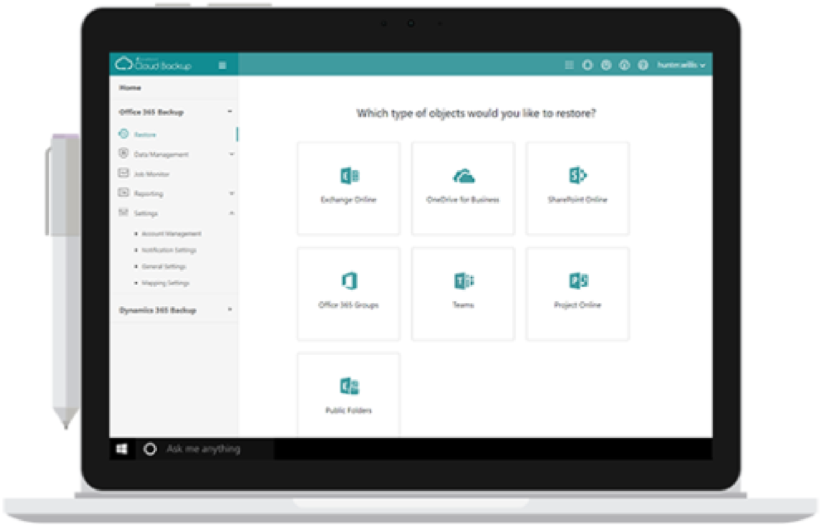
Example of a point solution in the Cloud

Based on AvePoint



Backup data

AvePoint Cloud Backup For Office 365



Which type of objects would you like to restore?

Exchange Online
OneDrive for Business
SharePoint Online
Office 365 Groups
Teams
Project Online
Public Folders

Some points of attention

- Backup data resides with the same Cloud provider as the source data.
- You are limited to the offered choices.
- 3-2-1 rule might not be applied.
- Your other data also needs backup, i.e. multiple management consoles.

But …

- The ease of setup and **ease of use** of a SaaS solution is a big advantage.
- **No upfront investments** are a big selling point.
- Often integrated in SaaS application with self service capabilities

Zero trust & backup

Backup is your last line of defense …

… it needs to be protected accordingly!

Secure the backup infrastructure

- Implement **hardening** of all the components in the backup infrastructure: OS, databases used by the backup platform, using CIS (Center for Internet Security) benchmarks.
- **Avoid** integration of the backup environment in MS **Active Directory**.
- Use **Linux** components if and when possible.
- Relocate the **management console** to a dedicated server, limit access to the backup server.
- Enable **secure communications** (encrypted and authenticated communications).
- Implement **auditing** on the backup environment.
- Use network segmentation techniques to isolate and **air gap** storage targets.
- Use **Multi-Factor Authentication** (MFA) to login to the backup environment
- Use **Role Based Access** (RBAC) to ensure ‘least privilege access’.

Secure the backup data

- Incorporate **immutable storage** in the backup strategy …
- Or keep a backup **copy offline** …
- **Encrypt** you backup data.

- Make sure the **management console** of the array where the backup data resides is **secured**.
- Make sure only the **media agent** can **access** the backup data.
- **Validate data** at rest and during copies.

Ransomware

Backup is a copy of your primary data …

… whatever is hiding in your primary data can also be hiding in your backup data!

Detection of viruses, malware, ransomware is primordial to a good recovery.

Recovery is the last step in the ransomware incident’s lifecycle

Step 1 - Preparation

Step 2 - Develop and rehearse an incident response plan

Step 3 - Detection

Step 4 - Analysis

Step 5 - Containment

Step 6 - Eradication

Step 7 - Recovery

Also don’t forget:

- It’s advised to notify the police.
- Also notify CERT.be The Federal Cyber Emergency Team

WHERE
DO I
START
?

Determine your backup strategy

Identify essential **data** & take **inventory** of your multicloud environment

Identify the correct **RTO** and **RPO** for this data

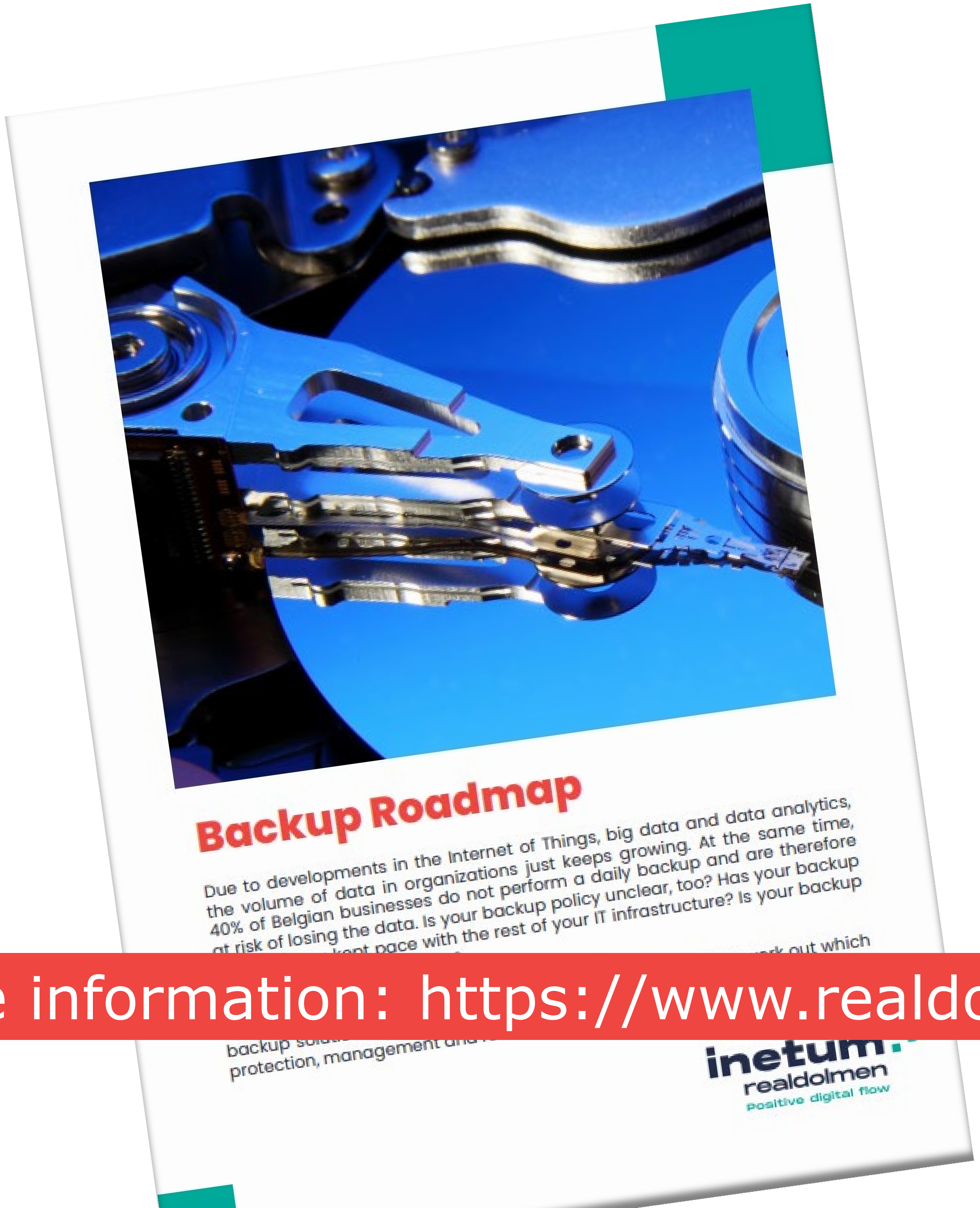
Identify (internal/external) **compliance** rules for the data

Determine the desired approach and design your **architecture**

Identify the possible **backup platforms** that meet your specific requirements

Do all this with a possibility ransomware attack in your mind!!

How Inetum-Realdolmen can help you



Backup Roadmap

Due to developments in the Internet of Things, big data and data analytics, the volume of data in organizations just keeps growing. At the same time, 40% of Belgian businesses do not perform a daily backup and are therefore at risk of losing the data. Is your backup policy unclear, too? Has your backup kept pace with the rest of your IT infrastructure? Is your backup

rk out which

backup solu

protection, management and

inetum.
realdolmen
Positive digital flow

Procedure

The Backup Roadmap comprises the following stages:

Kick-off meeting

During an **exploratory meeting**, your organization and our consultants define the **scope** of the study. What are your backup requirements and which approach do you wish to take for your backup infrastructure? We also cover issues, requirements, constraints that are specific to the environment (e.g. compliance regulations), future projects, etc. Based on this information, a cost estimate is prepared for further work on developing the roadmap. You then receive a quotation with estimates for the study based on the defined scope.

Architectural analysis

An Inetum-Realdolmen consultant will thoroughly review your existing IT environment and backup infrastructure.

Project Roadmap

Based on this analysis we develop a solution for a backup architecture that meets the previously defined objectives, including which service model you want to have/best suits your needs. The solution is unique for each environment and can take many different forms depending on the defined **scope**.

The deliverable you receive is a personalized roadmap.

Scope – a few examples

- A number of backup infrastructure scenarios are developed that can be compared to each other.
- A solution that sends backups off site to the cloud, integrated with the company's DR solution.
- A unified backup solution for on-prem backups and M365 backups.
- A solution for moving away from tape-based backups.
- A solution that removes the burden of backup from the organization altogether.

More information: https://www.realdolmen.com/en/backup_roadmap

Our partners for this event

COMMVAULT®

AvePoint®

Thank you.

inetum.
realdolmen
Positive digital flow

inetum.world

FRANCE | SPAIN | PORTUGAL | BELGIUM | SWITZERLAND | LUXEMBOURG | ENGLAND |
POLAND | ROMANIA | MOROCCO | TUNISIA | SENEGAL | CÔTE D'IVOIRE | ANGOLA |
CAMEROON | USA | BRAZIL | COLOMBIA | MEXICO | RP OF PANAMA | PERU | CHILI |
COSTA RICA | DOMINICAN REPUBLIC | ARGENTINA | SINGAPORE | UAE