Data protection

Peter Kúšik – Slovak Telekom

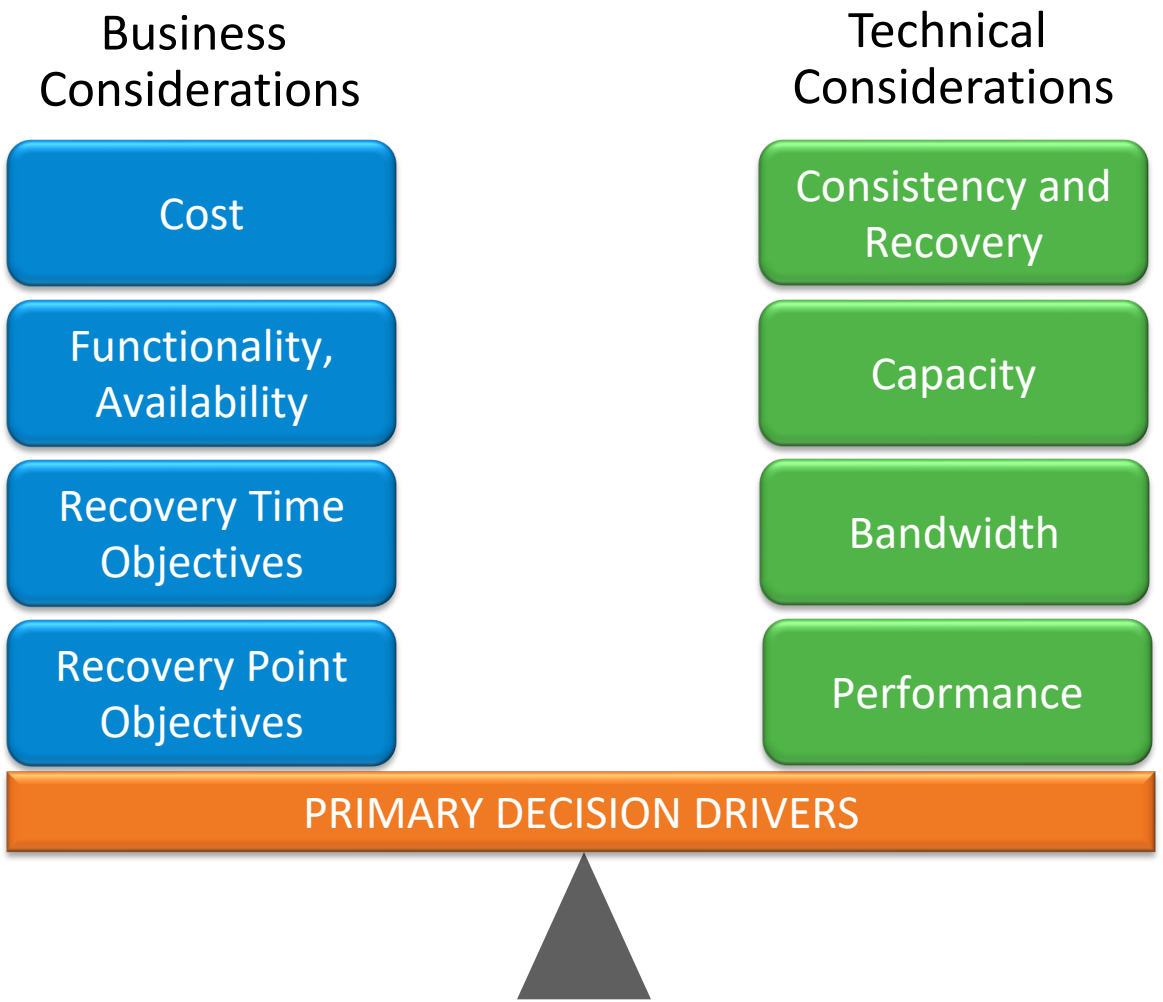
LIFE IS FOR SHARING.

Agenda

- Business continuity
- Primary data vs Backup data
- Backup data protection – Recovery Vault (WORM)
- Backup data protection – Anomalies detection
- Typical restore from local Backup and Cloud

LIFE IS FOR SHARING.

Business continuity and data protection challenges



Recovery point objective (RPO):

How recent is the point in time for your recovery?

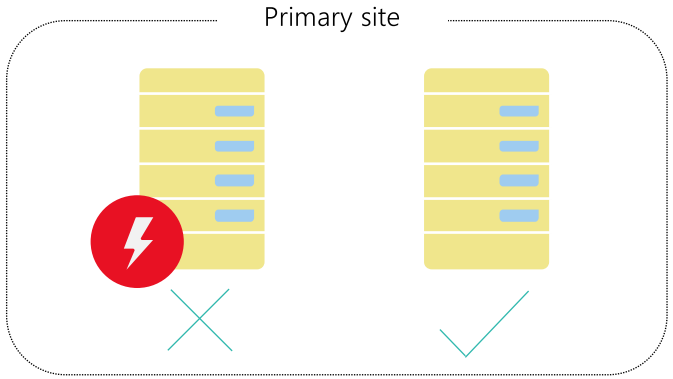
Recovery time objective (RTO):

How fast can you restart a failed application?

(RPO+RTO = Acceptable Risk)

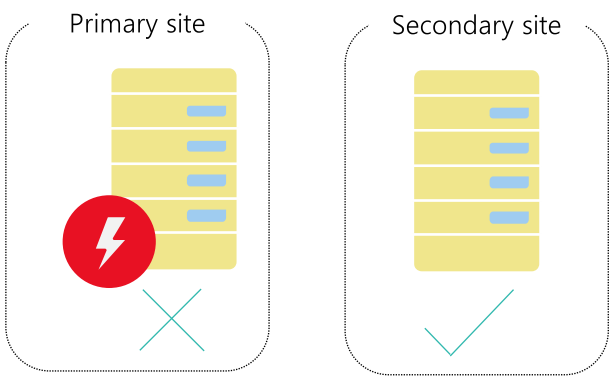
Business continuity strategy

WE need all three



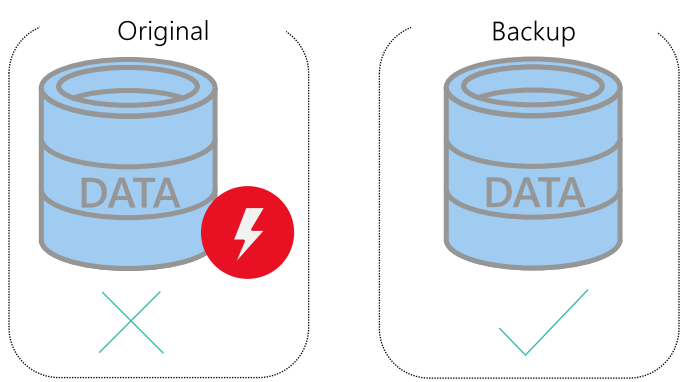
High availability

When our applications have a critical failure, run a second instance



Disaster recovery

When our site has a catastrophic failure, run them in public cloud or a secondary datacenter



Backup and restore

When our data is corrupted, deleted or lost we can restore it

Primary data vs Backup data protection

Primary data protection - 3DC

Data protection against DC disaster natural disasters and manmade disasters.

High Availability (Hitachi GAD or TrueCopy)

(local synchronous copy between two storages)

Asynchronous replication to another DC

(far copy of data over 400km)

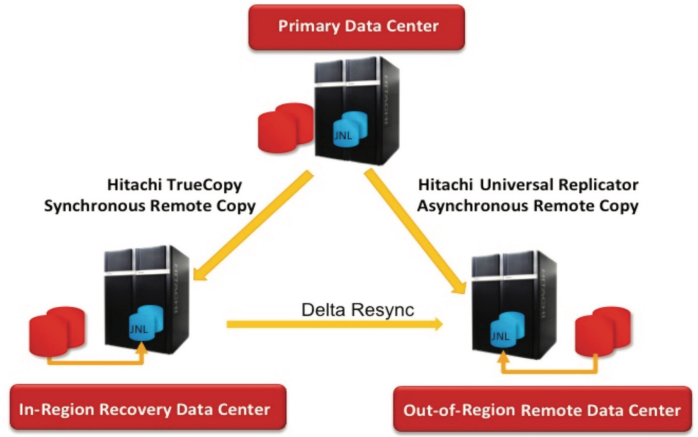
Backup data protection

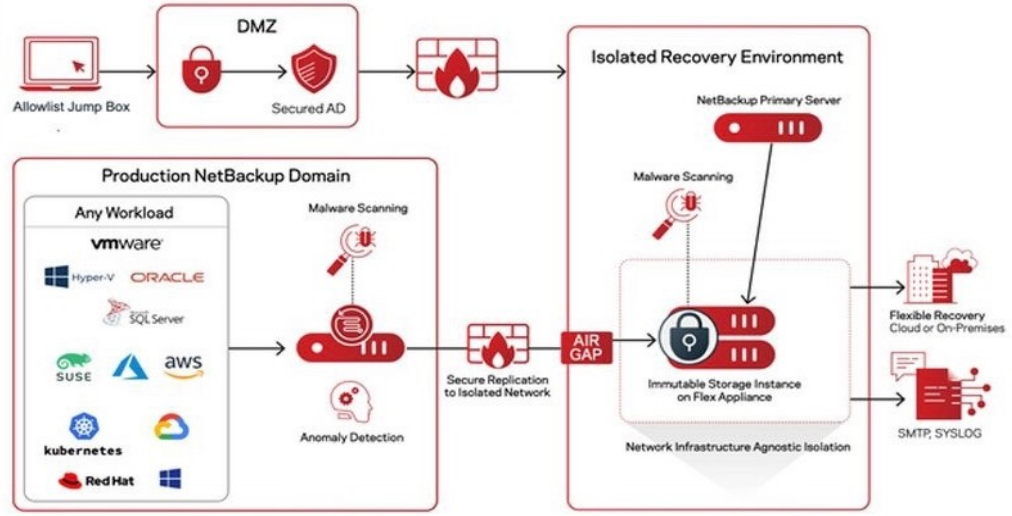
Protection against human/operator error, and ransomware

On-premise backup appliances

Cloud Recovery Vault

Backup anomaly detection

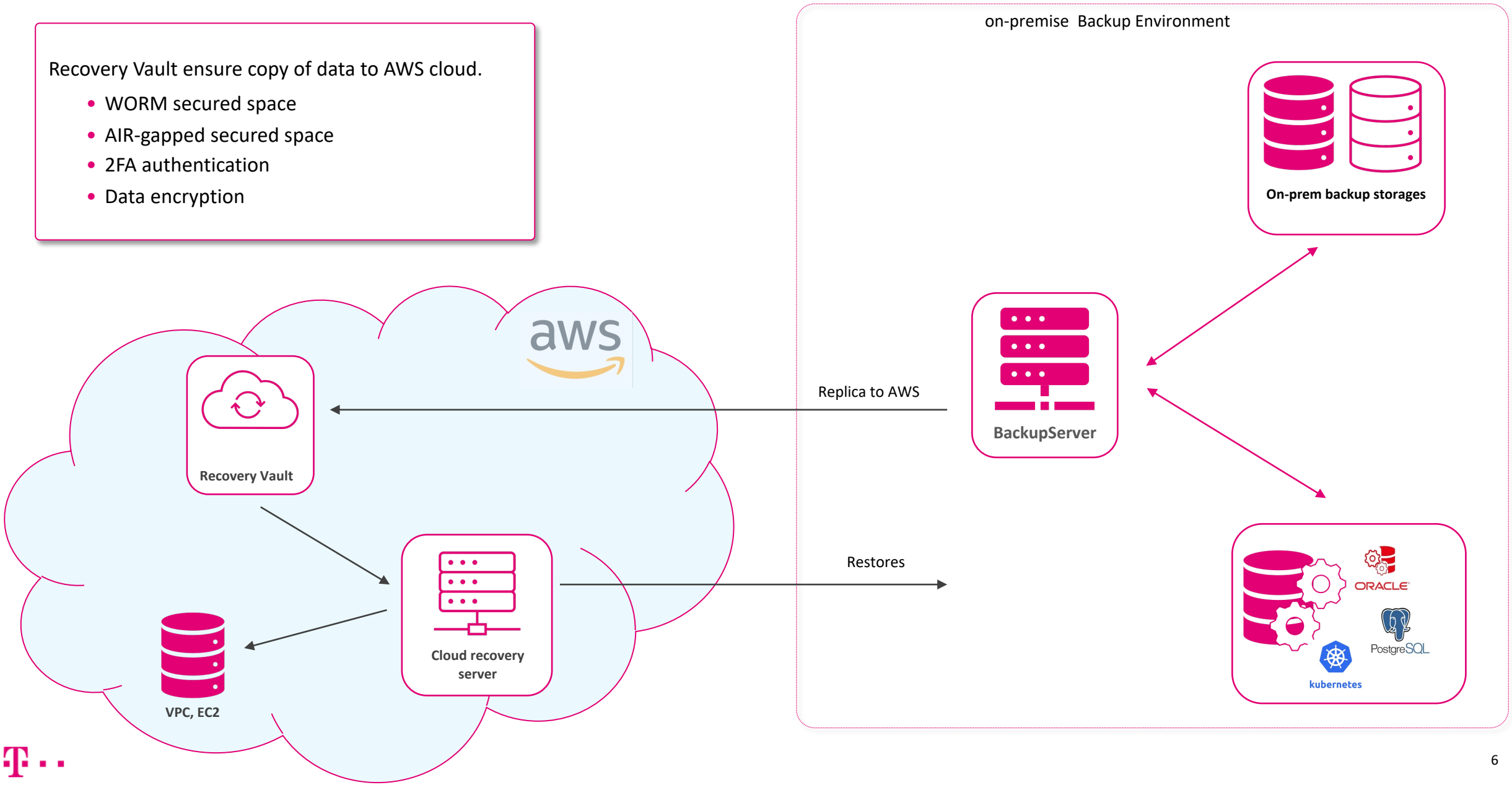




Backup Data protection solution in AWS - Recovery Vault

Recovery Vault ensure copy of data to AWS cloud.

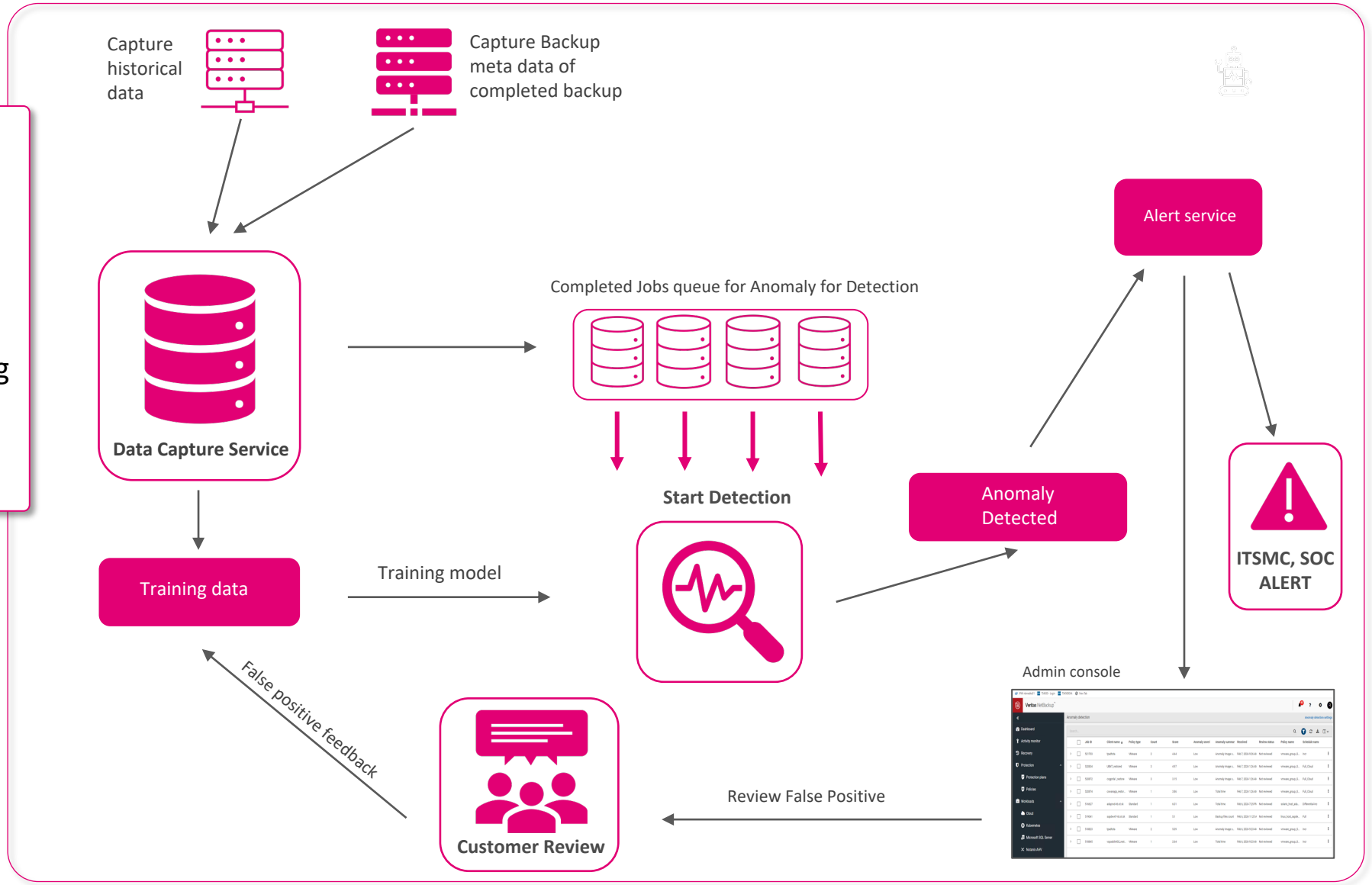
- WORM secured space
- AIR-gapped secured space
- 2FA authentication
- Data encryption



Backup Data protection - Backup anomaly detection

Ransomware protection

This anomaly detection relies on **artificial intelligence (AI)** to identify abnormal behaviour within the pool of collected NetBackup data, with the objective of providing advanced warning of a **ransomware event**.



Typical restore from local Backup and Cloud

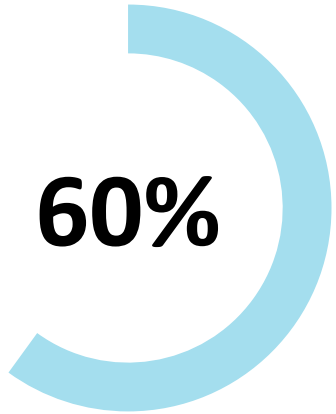
Busines critical mission

First critical servers and application available to customers in **2 days**

Restored Business critical server

Critical mission

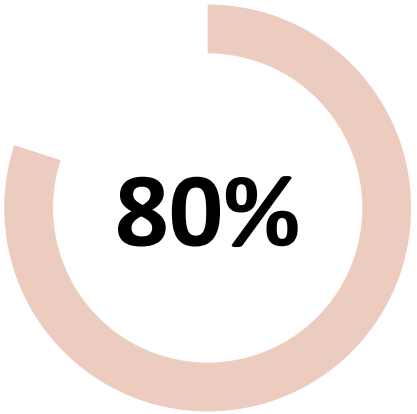
First **4 days** from incident most critical application restored, from backup or local data



Restored critical server

Normal priority

First **week** from incident all production environment restored.



Restored all Prod environment

Test/DEV

Two or Three weeks from incident whole environment restored.

Restored whole environment

The End

Thank you for an attention!

LIFE IS FOR SHARING.