Hewlett Packard
Enterprise

HPE Zerto – DR and Cyber Vault

Yves Venneman

November 2024

And what could have been avoided?

Humans will always be a point of failures

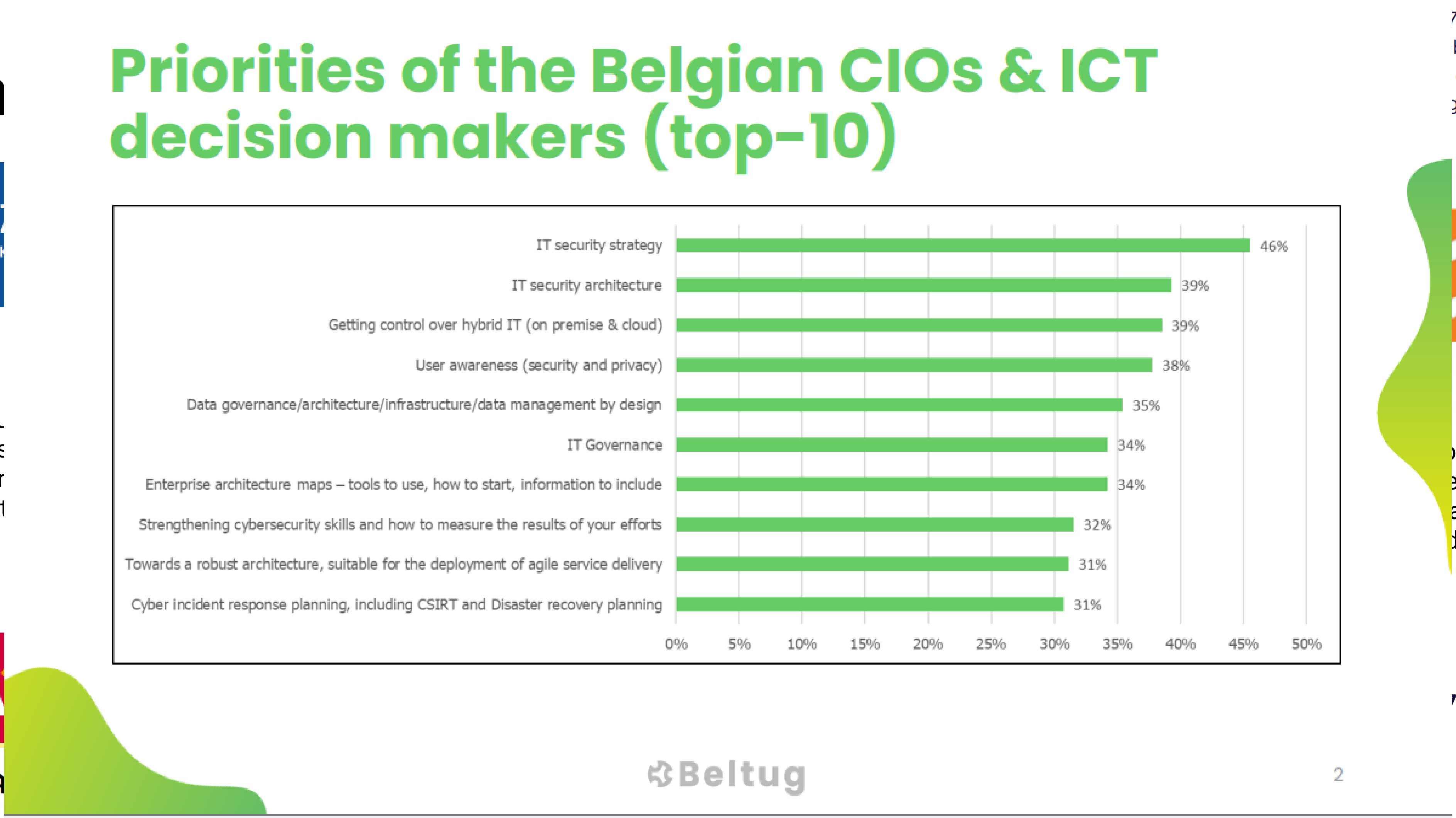
Using a ZTA architecture could have help to prevent or minimize the damage.

So , is security important ?

Belgian websites under attack from pro-Russian hackers for the 5th day in a row

7 has carried out
bsite of the
on the Telegram
gs to Belgium".

a



Priorities of the Belgian CIOs & ICT decision makers (top-10)

Beltug

2

in May 2022 in Lu
Wallonia: as a res
attack, Belgian pr
Vivalia switched t
management.

of Le Soir
ewspaper
after
due to a

' companies

Welkom in A

Several Belgian municipalities recently fell victim to ransomware | Centre for Cyber security Belgium

NIS2 REGULATION - WHAT FOR WHO ?

- Successor of **NIS1** – guideline, introduced in 2016.
- Proposed by **European Commission** in December 2020.
- Every EU member state has to implement the EU NIS2 guidelines in its national law by **17 October 2024.**

Why NIS2 instead of NIS1?

- *“NIS2 is NIS1 on steroids”*
- More **collaboration between national governments**
- More extensive **national cybersecurity** strategies
- **Cybersecurity crisis management framework**
- Extension in **European collaboration** around crisis & policy.
- Extension to **more sectors**

Space

Government, Public Admin

Transport

Banking

Energy

Digital Infrastructure

Financial Markets

Healthcare

Post & Courier

Chemical Production

Manufacture, Production

Research

Waste Management

Life Sciences

Digital Providers

Delivery

***Difference between highly critical & other critical entities** lies with the **severity of the sanctions** that can follow in case of non-compliancy.

Source

Achieve NIS2 + DORA Readiness

Continuous Data Protection

"Implement policies, procedures, protocols and tools that aim to ensure resilience, continuity, and availability of ICT systems"

Real-Time Encryption Detection

"Have in place mechanisms to promptly detect anomalous activities"

Testing and Reporting

"Shall put in place, maintain, and periodically test appropriate ICT business continuity plans"

One-to-Many Replication

"Maintain at least one secondary processing site endowed with adequate resources, capabilities, and functions"

The Digital Operational Resilience Act (DORA) is a European Union regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the financial sector

NIS 2 -

WHAT ELSE IS NEW IN THE NIS2 REGULATION?

Management

Reporting

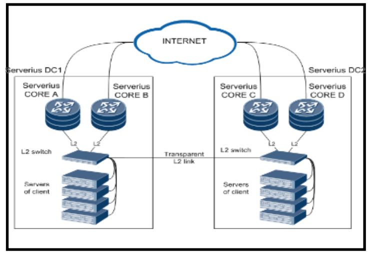
Risk Management

Business Continuity

6 Levels of data protection

LEVEL OF DATA SECURITY

1 High Availability



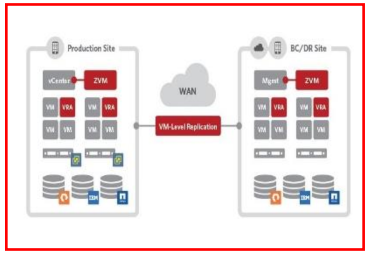
Transparent and automated failover AKA Metrocluster

Easy to operate

RPO = 0 / RTO=0

no protection against malware/cyberattack

2 Disaster Recovery



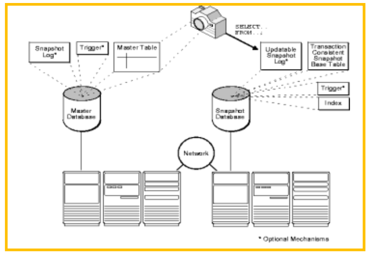
RPO = short (seconds)

Multi datacenter or cloud

Orchestrated recovery

User initiated failover
Minium protection against Cyberattack
Cost

3 Cyber resilient copy on the array



protection against malware/cyberattack

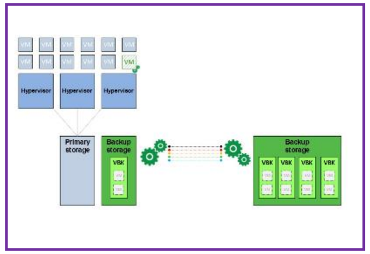
Native and efficient integration

Quick restore

No application integration

RPO = medium (hours)

4 On-Premises Back-up



protection against malware/cyberattack

Application integration

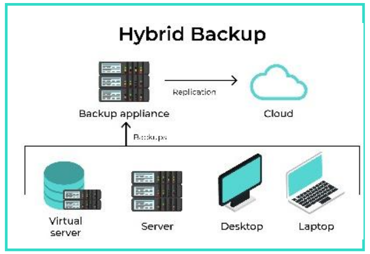
3-2-1 rule

Complexity

end to end Performance

RPO = long (day)

5 Back-up to the Cloud



protection against malware/cyberattack

Application integration

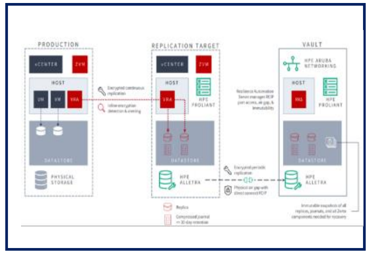
Lower cost

Cost of restore

Long RTO

Networking / security

6 Cyber Resilience Vaulting



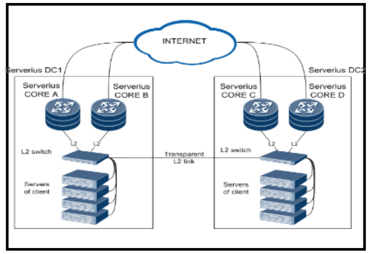
Ultimate cyber resilience solution

$ $$$$

6 Levels of data protection by HPE

Data security

1 High Availability

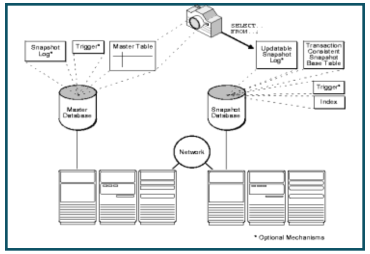


Stretched Clustering

Metrocluster

Peer Persistence

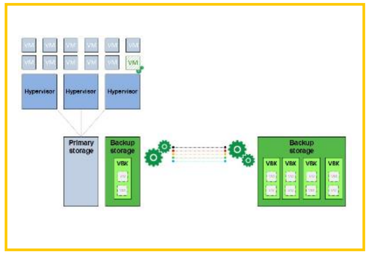
2 Cyber resilient copy on the array



Snapshotting

Simplivity backup

3 On-Premises Back-up

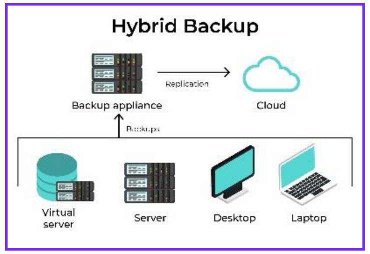


StoreOnce/Tape/ Object

HPE Partnerships:

- **Veeam**
- **CommVault**
- **Cohesity**

4 Back-up to the Cloud

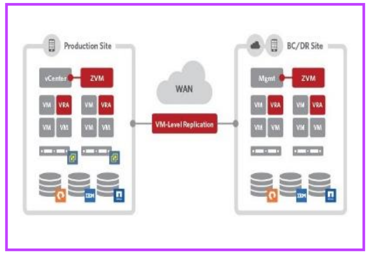


StoreOnce CloudBank

HPE Partnerships:

- **Veeam**
- **CommVault**
- **Cohesity**

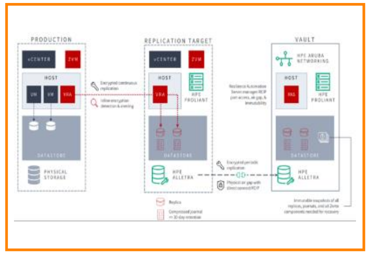
5 Disaster Recovery



HPE GreenLake for Disaster Recovery*

Zerto

6 Cyber Resilience Vaulting



Zerto Vault Bundles

*VMware only

Let’s talk about
–
Ultimate cyber resilience solution

Top challenges about secure the security

Evolving threats

Last year, 61% of disaster responses were triggered by **ransomware**[1]

Ransomware's dilemma

Lose data or pay ransom—and **only 4%** of those who paid got all their data back[2]

Slow speed of recovery

Average time to recover from ransomware is **one month**[2]

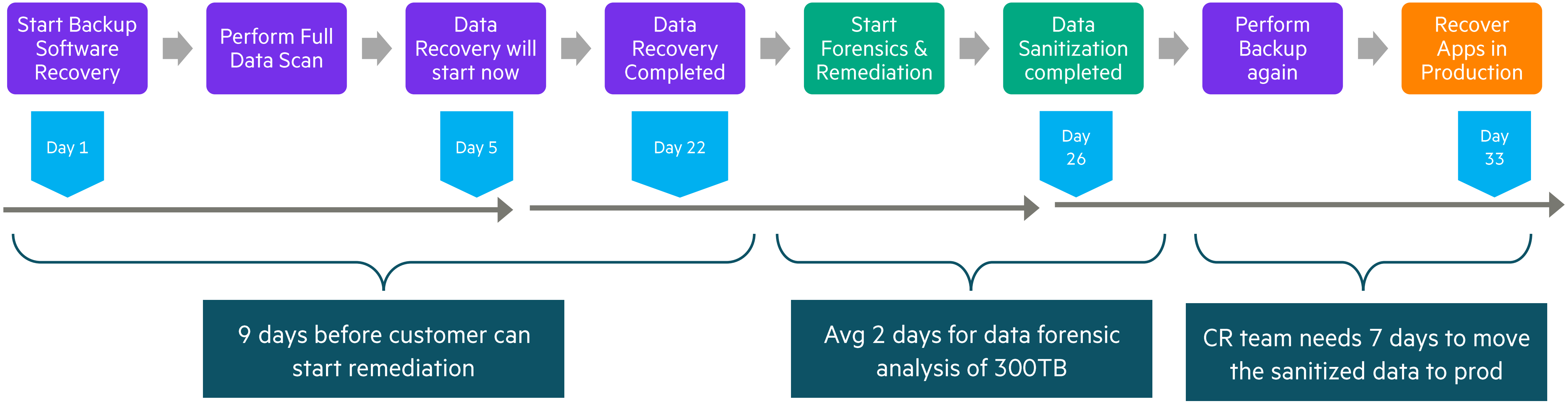
Staying in compliance

Myriad standards & regulations, e.g. GDPR, SOX,NIS2, HIPAA, DORA, FISMA

[1] The State of Ransomware and Disaster Preparedness: IDC
[2] Sophos: The State of Ransomware

Backup Cyber Recovery Timeline

RTO = Minimum 30 days to recover



Start Backup Software Recovery → Perform Full Data Scan → Data Recovery will start now → Data Recovery Completed → Start Forensics & Remediation → Data Sanitization completed → Perform Backup again → Recover Apps in Production

Day 1

Day 5

Day 22

Day 26

Day 33

9 days before customer can start remediation

Avg 2 days for data forensic analysis of 300TB

CR team needs 7 days to move the sanitized data to prod

* Example using 300 TBs of front-end data

HPE - Zerto

Continuous availability from edge to cloud

Orchestration | Automation | Analytics

Disaster Recovery

Radically reduce data loss and downtime with lowest RTOs and RPOs

Ransomware Resilience

Real-time detection, protection and cyber recovery

Multi-Cloud Mobility

Freedom to move and protect across clouds

Continuous Data Protection

vmware by Broadcom

aws

Microsoft Azure

HPE GreenLake

ORACLE CLOUD

IBM Cloud

Google Cloud

MSP

Microsoft Hyper-V

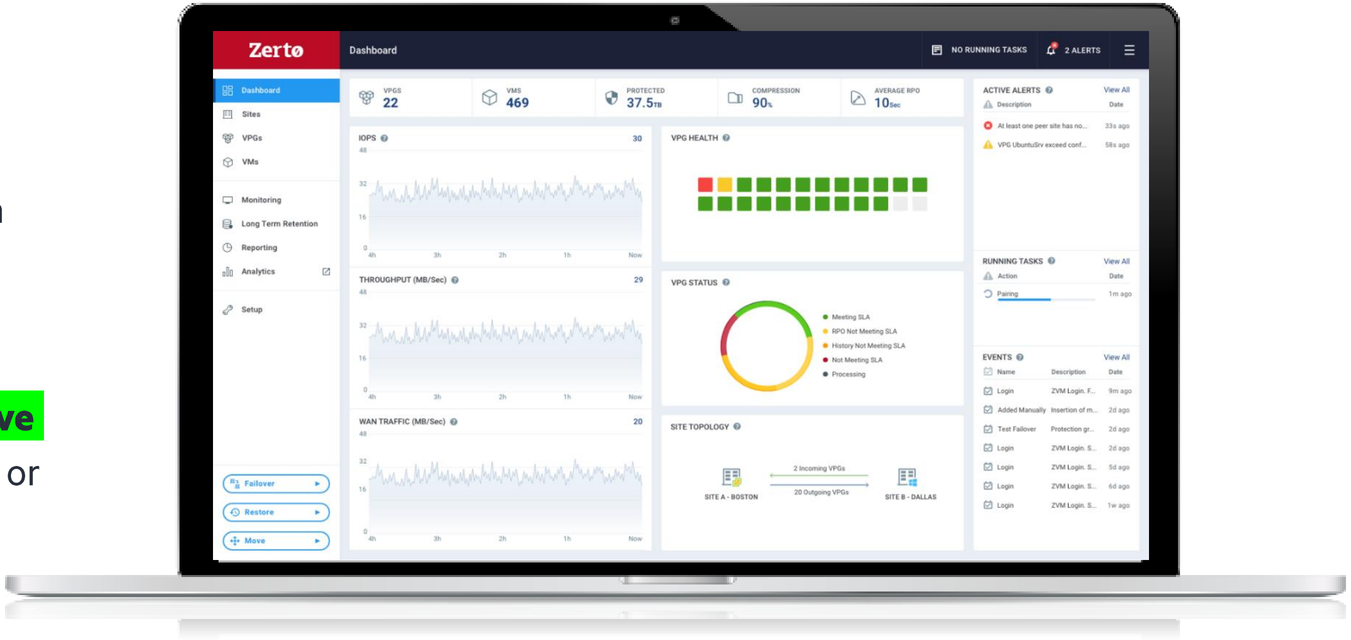
Leader in data recovery since 2011

Eliminate data loss and downtime with continuous data protection

Software-only, hypervisor-based replication for flexible, always-on protection without storage lock-in

RPOs of seconds and RTOs of minutes to quickly restore operations by rewinding and resuming from any point in time from the past

Orchestrated failover, failback, and non-disruptive testing with reporting to easily recover files, VMs, or multi-VM app stacks



ACTIVE ALERTS

Description	Date
At least one peer site has no...	33s ago
VPG UbuntuSrv exceed conf...	58s ago

RUNNING TASKS

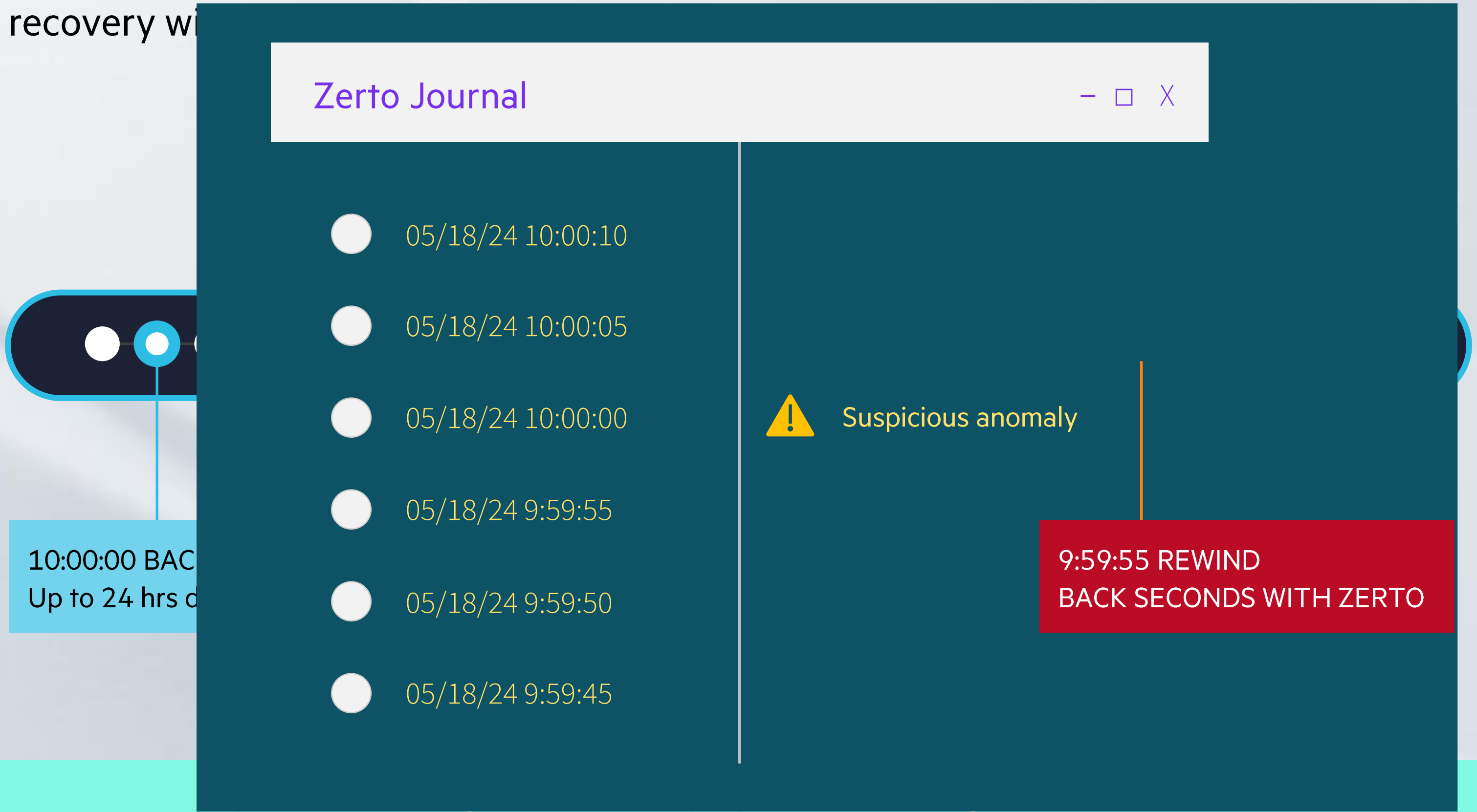
Action	Date
Pairing	1m ago

EVENTS

Name	Description	Date
Login	ZVM Login. F...	9m ago
Added Manually	Insertion of m...	2d ago
Test Failover	Protection gr...	2d ago
Login	ZVM Login. S...	2d ago
Login	ZVM Login. S...	5d ago
Login	ZVM Login. S...	6d ago
Login	ZVM Login. S...	1w ago

Replicate and detect

- Granular, point-in-time recovery wi



Zerto Journal

- ○ 05/18/24 10:00:10
- ○ 05/18/24 10:00:05
- ○ 05/18/24 10:00:00
- ○ 05/18/24 9:59:55
- ○ 05/18/24 9:59:50
- ○ 05/18/24 9:59:45

⚠ Suspicious anomaly

9:59:55 REWIND
BACK SECONDS WITH ZERTO

10:00:00 BAC
Up to 24 hrs c

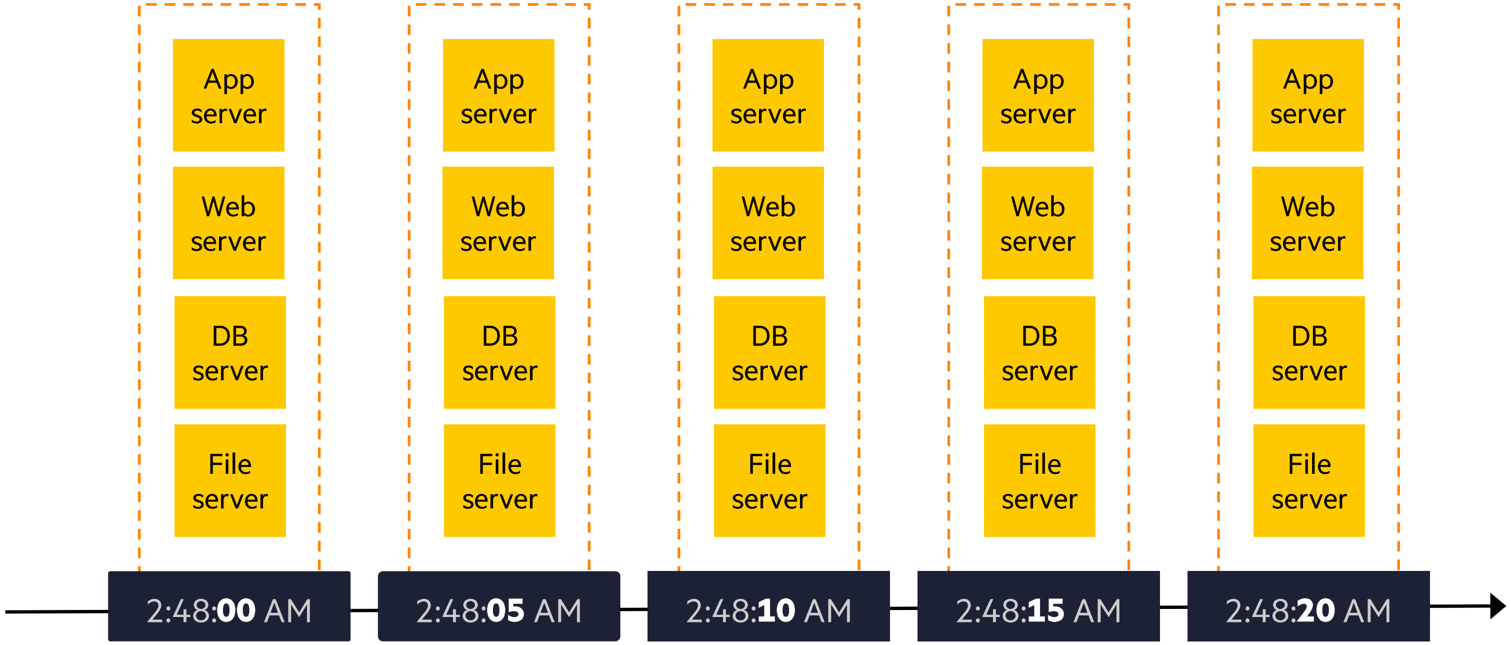
DETECT
anomalous encryption in real-time to alert to possible ransomware

RESPOND
quickly to minimize data loss & downtime with low RPOs and fast RTOs

RECOVER
in minutes to a clean state seconds before an attack or disruption

Application-centric protection

Replicate and recover multi-VM app stacks as one consistent whole



✓ Write-order fidelity and validation across all VMs or containers in an app

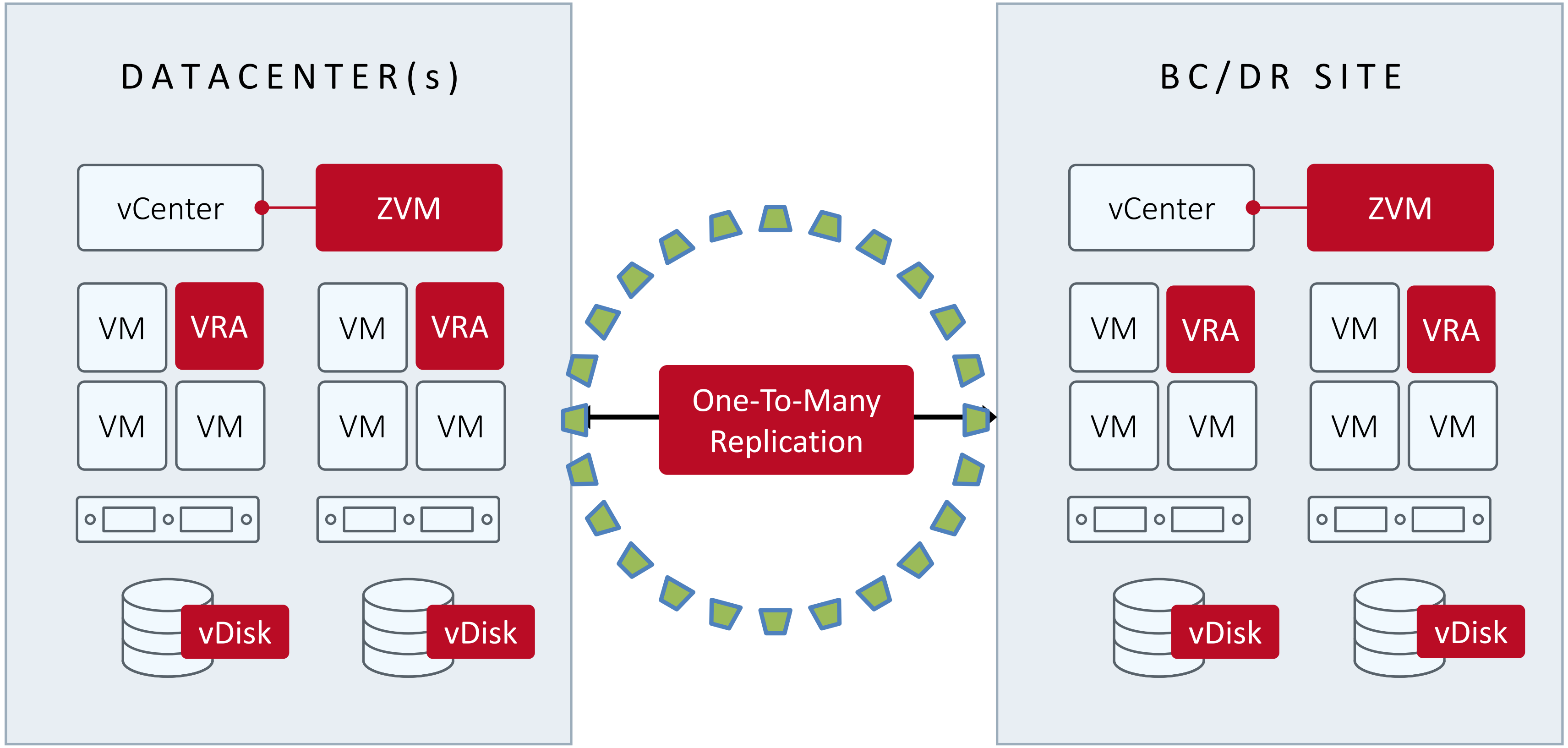
✓ Consistent restore points even for VMs on different datastores or hosts

✓ No staggered backup windows and no scheduled replication jobs

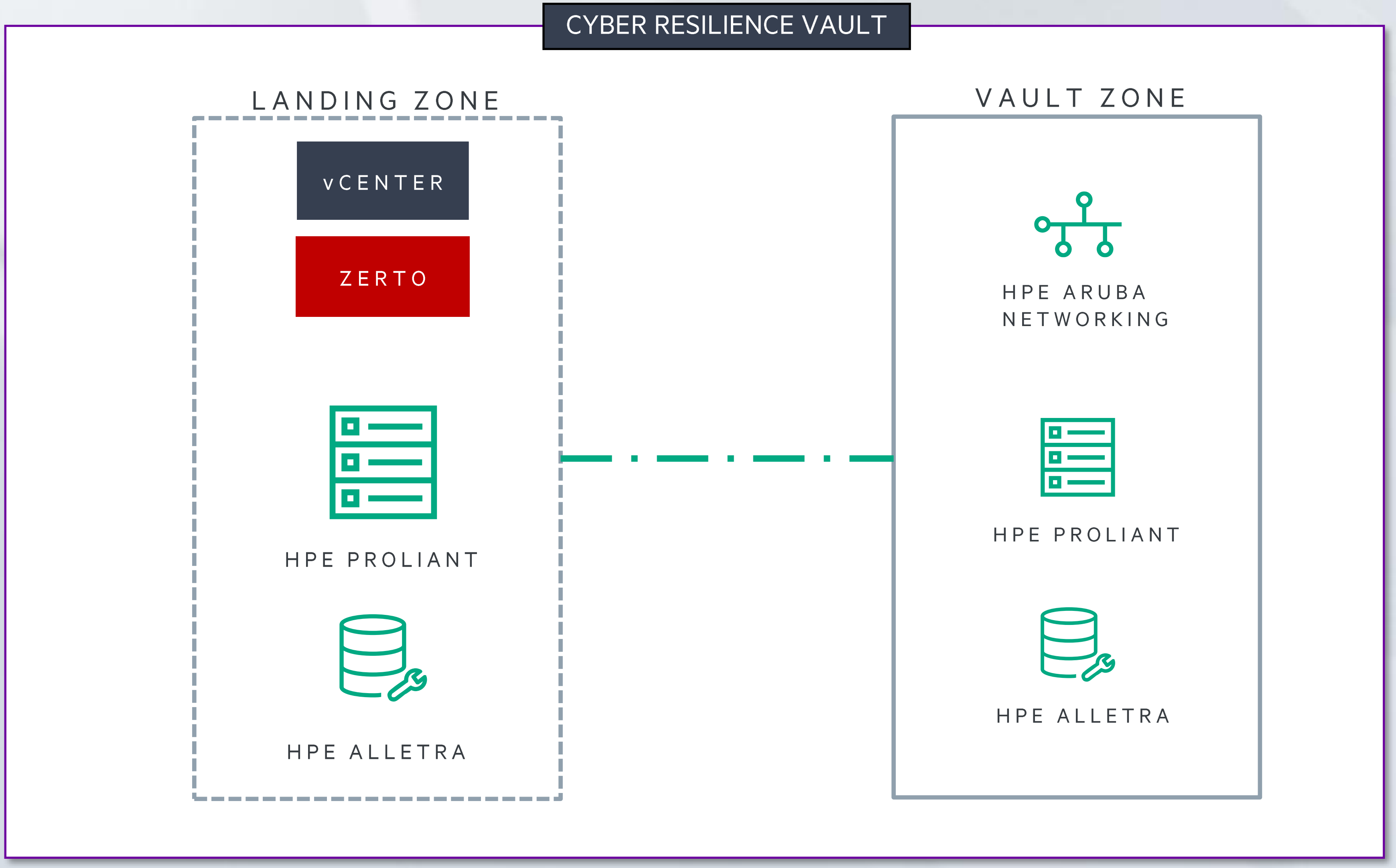
How it works

- Continuous data protection
  - Replication
  - Journal
  - **App-centric recovery**
  - Real-Time Detection

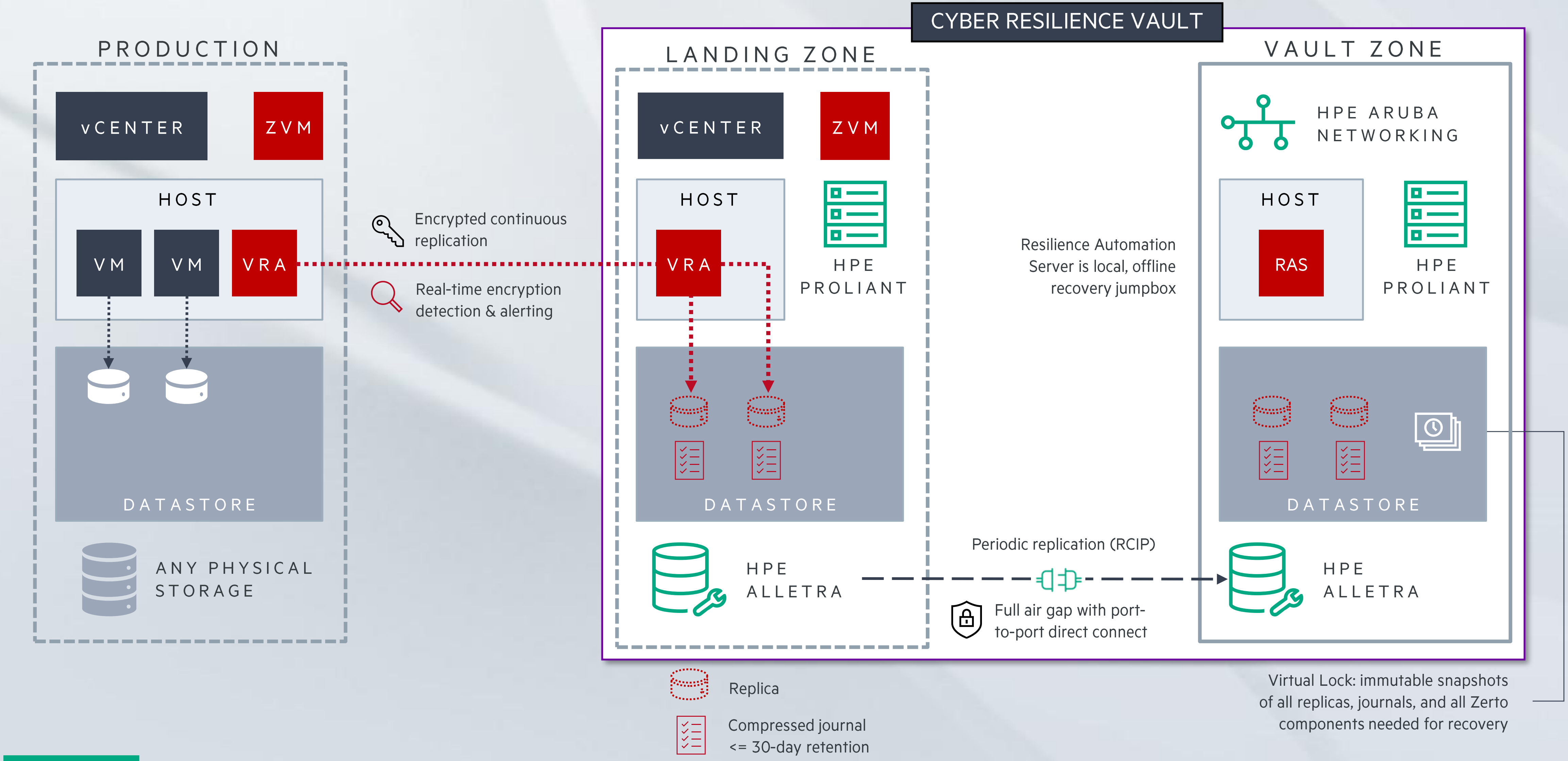
Continuous Data Replication for your mission critical applications



HPE - Zerto / Cyber Resilience Vault Architecture terms



Isolate and Lock: HPE Zerto Cyber Resilience Vault



Encrypted continuous replication

Real-time encryption detection & alerting

Resilience Automation Server is local, offline recovery jumpbox

Periodic replication (RCIP)

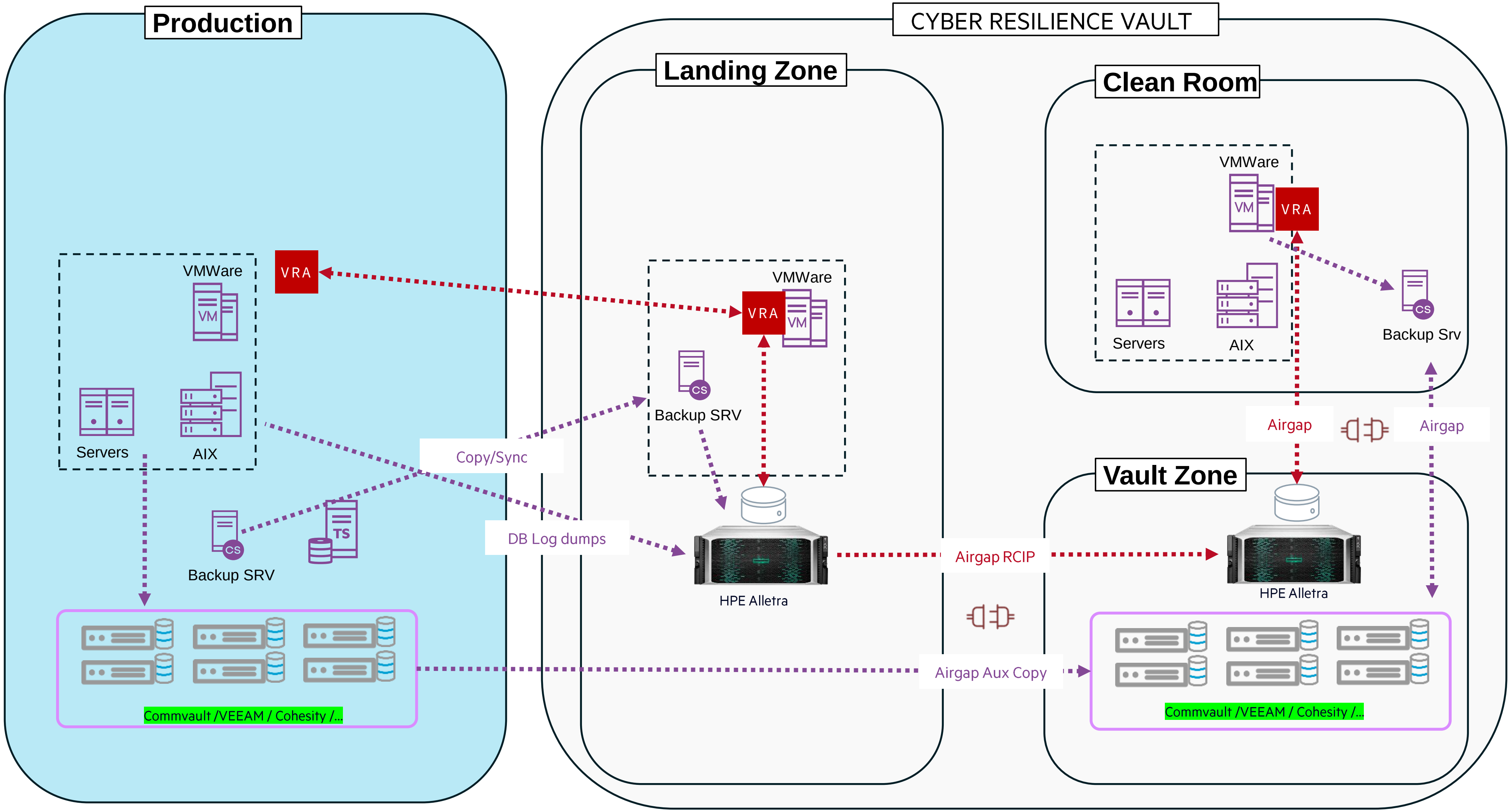
Full air gap with port-to-port direct connect

Replica

Compressed journal <= 30-day retention

Virtual Lock: immutable snapshots of all replicas, journals, and all Zerto components needed for recovery

HPE Zerto Cyber Resilience Vault and Physical environments



Depending on the needs from small to Large

Reference architecture solution

- T Shirt size sample configurations shown below

Mini

50 Zerto Licenses

(2) Alletra MP Block 2-Node 8 Core

2 x 67 TB Usable

(5) ProLiant DL 360 G10+

(2) ProLiant DL20

(3) Aruba 8100

(1) Aruba 6000

XS

100 Zerto Licenses

(2) Alletra MP Block 2-Node 8 Core

2 x 123TB Usable

(5) ProLiant DL 360 G10+

(2) ProLiant DL20

(4) Aruba 8100

(1) Aruba 6000

(2) SN3600B Fibre Channel

S

300 Zerto Licenses

(2) Alletra MP Block 2-Node 16 Core

2 x 324TB Usable

(7) ProLiant DL 360 G10+

(2) ProLiant DL20

(4) Aruba 8100

(1) Aruba 6000

(2) SN3600B Fibre Channel

M

600 Zerto Licenses

(2) Alletra MP Block 2-Node 16 Core

2 x 613TB Usable

(15) ProLiant DL 360 G10+

(2) ProLiant DL20

(4) Aruba 8100

(1) Aruba 6000

(2) SN3600B Fibre Channel

L

1000 Zerto Licenses

(2) Alletra MP Block 2-Node 16 Core Networked

2 x 1.1PB Usable

(22) ProLiant DL 360 G10+

(2) ProLiant DL20

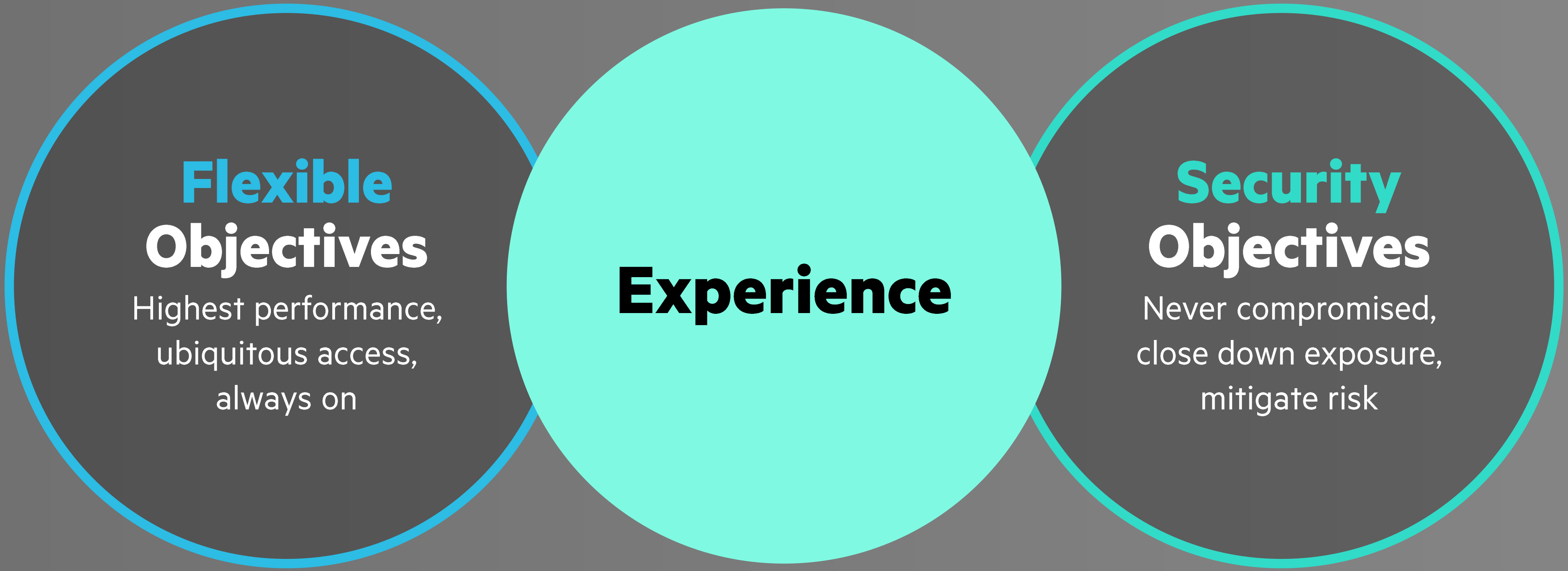
(4) Aruba 8100

(2) Aruba 6000

(2) SN3600B Fibre Channel

The Perpetual Problem

Businesses are Being Forced to Choose



Flexible Objectives

Highest performance, ubiquitous access, always on

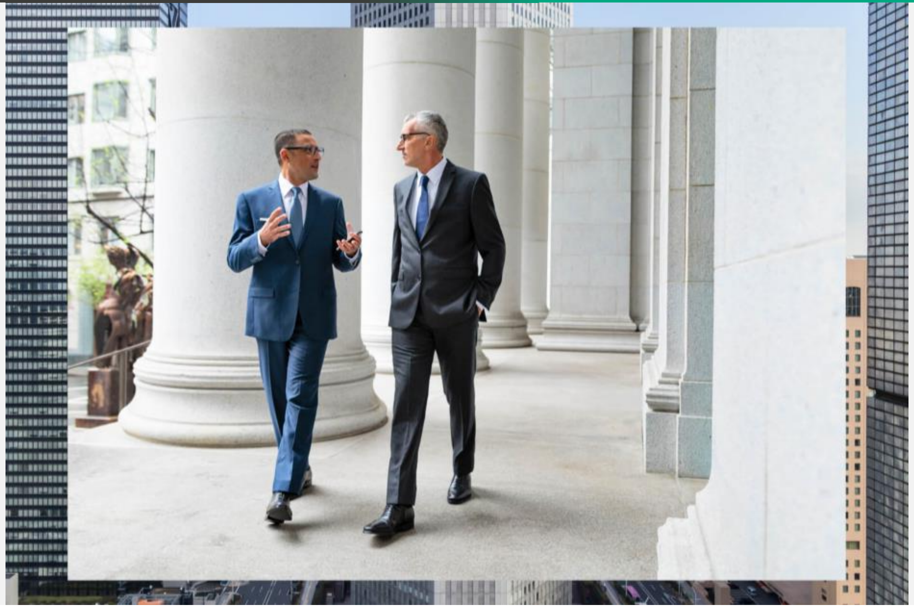
Experience

Security Objectives

Never compromised, close down exposure, mitigate risk

The Perpetual solution – HPE - Zerto

Before State	After State
Protection Strategy: Legacy backup	**Protection Strategy:** Cyber Resilience Vault
Data Loss: est. 12-24 hours’ worth	**Data Loss:** Minimal
Recovery Time: *Weeks*	**Recovery Time:** *Hours*
Compliance: could not pass	**Compliance:** exceed requirements



Hewlett Packard
Enterprise

Thank you