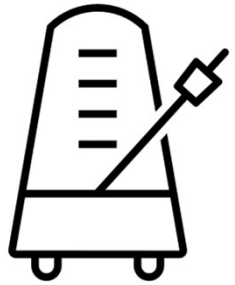
Zerto

Ransomwareschutz zu Ende gedacht

Elias Noll, Account Executive

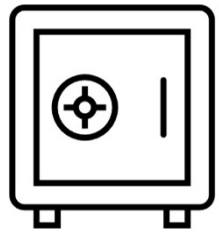
Bei Cryptolockern geht es um Zeit und Wiederherstellbarkeit

- Zeit den Befall zu erkennen
- Zeit die Ausbreitung zu stoppen
- Zeit den bestmöglichen Recoverypunkt herauszufinden
- Verlorene Zeit seit der letzten nutzbaren Kopie (RPO)
- Zeit ein sauberes Umfeld sicherzustellen
- Zeit für den Restore (RTO)
- Zeit die wichtigsten Anwendungen wieder in Betrieb zu nehmen (WRT)
- Zeit zur Recovery der „restlichen“ Anwendungen
- Zeit / Möglichkeit DR im großen Stil zu testen (nicht nur Hochverfügbarkeit)



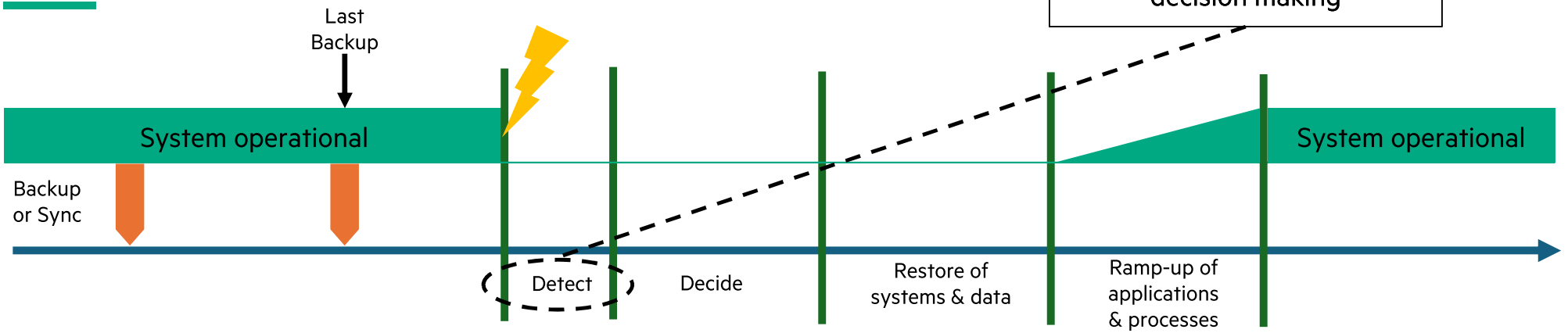
HPE Zerto hilft bei fast allen Punkten!

- Air-Gap
- Immutable copy
- Zero Trust
- Clean room




23
Quelle: https://www.coveware.com

Recovery Timelines



Zerto helps detecting anomalies within the live data-stream and does support quick decision making

aka dataloss
typical: **several hours**
Zerto: **seconds**

RPO

RTO

WRT

MTD

aka downtime
typical: **hours to days**
Zerto: **minutes**

The use of Zerto will reduce dataloss and downtime dramatically and thus reduce impact on productivity, reputation etc.

aka cont. downtime
typical: **days to weeks**
Zerto: **minutes**

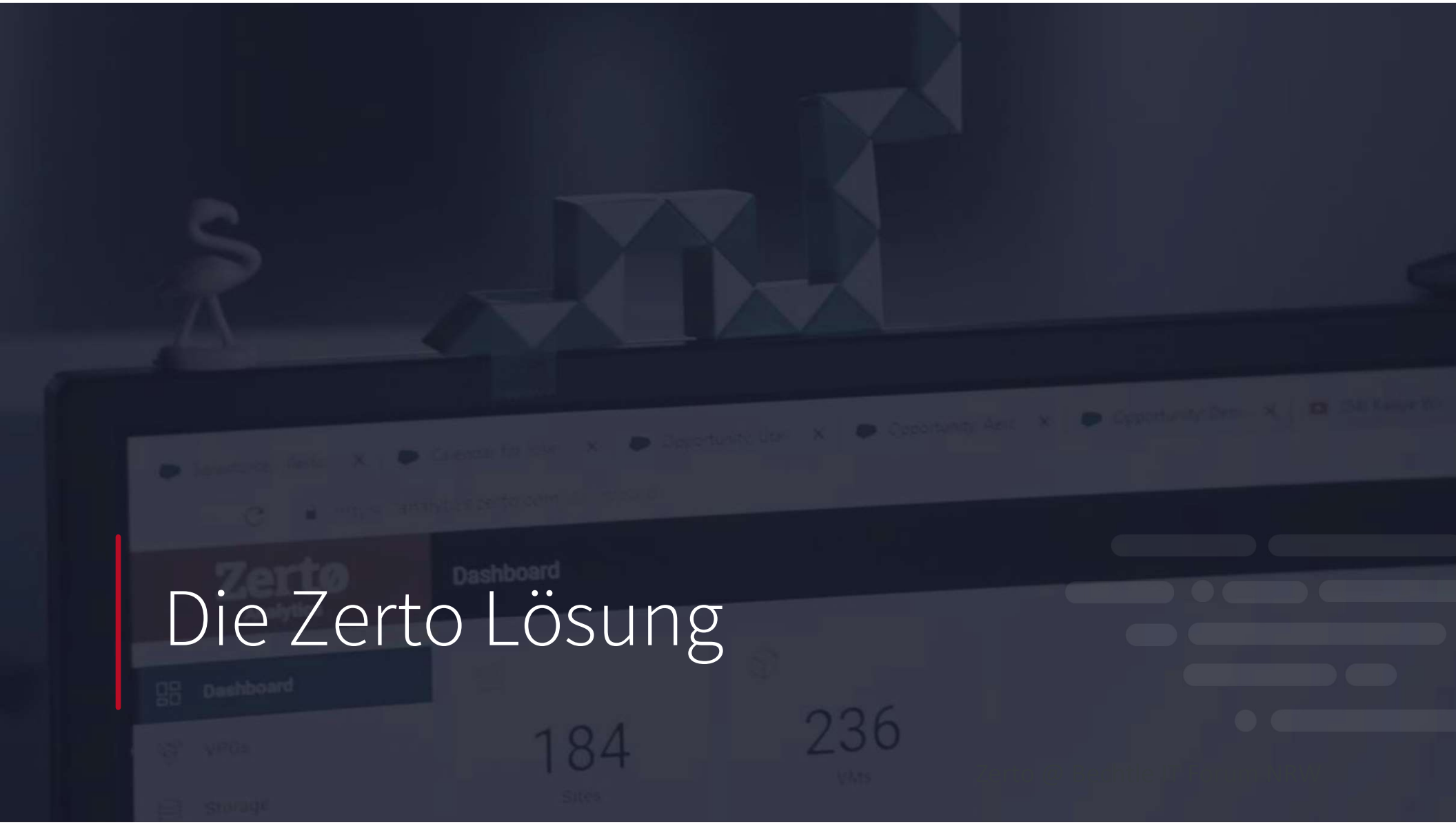
Risk matrix

Case	Mirroring	Backup	Zerto DR	Impact
Physical desaster (power outage, fire, ...)				existence-threatening
Other desaster (Cryptolocker, sabotage, ...)				existence-threatening
Single object loss (Files, tablespace, email, ...)				moderate
Desaster Recovery Test of at least 1/3 of environment				depending on compliancy

Three Layers of Data Protection

	Active-Active	Zerto a Hewlett Packard Enterprise company	Backup
RPO	0	5 – 15 seconds	12 – 24+ hours
RTO	0	Minutes	Hours/Days
Technology	Synchronous	CDP	Snapshot
Solution Type	Hardware	Software	Both
Main Use Cases	Natural disaster; hardware failure	Natural disaster; hardware failure; human error; ransomware	Regulatory & compliance; long-term retention; last resort recovery
Bandwidth	High	Low	High during backup window
Workload Tier	Mission-critical	Mission-critical and business-critical	All tiers

Zerto
a Hewlett Packard Enterprise company



Die Zerto Lösung

CONTINUOUS PROTECTION FOR ANY APP, ANY CLOUD, ANY THREAT

Orchestration | Automation | Analytics

Ransomware Resilience

Resume in minutes to seconds before an attack

Disaster Recovery

Foolproof recovery with fastest RTOs and RPOs

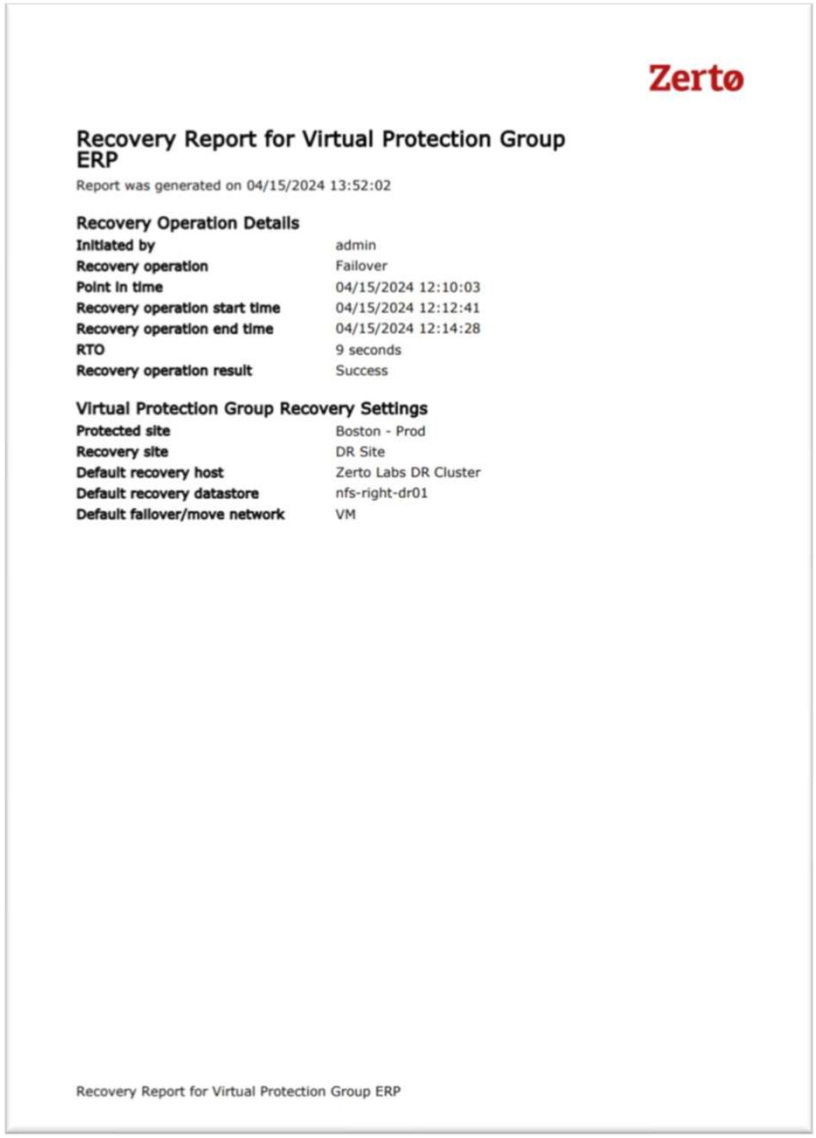
Multi-Cloud Mobility

Freedom to innovate across clouds

Continuous Data Protection

Microsoft Hyper-V · vmware · Microsoft Azure · aws · IBM Cloud · ORACLE CLOUD · Hewlett Packard Enterprise · MSP · Google Cloud

Reports



Zerto

Recovery Report for Virtual Protection Group ERP

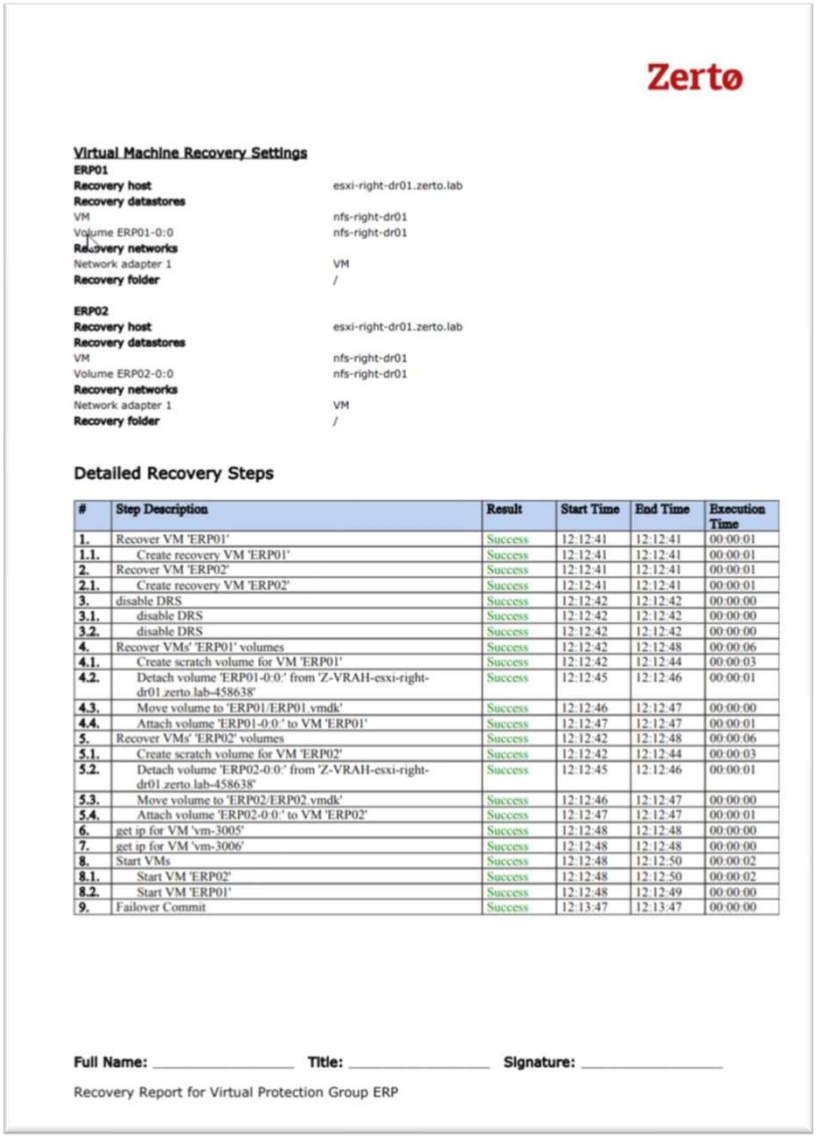
Report was generated on 04/15/2024 13:52:02

Recovery Operation Details

Initiated by	admin
Recovery operation	Failover
Point in time	04/15/2024 12:10:03
Recovery operation start time	04/15/2024 12:12:41
Recovery operation end time	04/15/2024 12:14:28
RTO	9 seconds
Recovery operation result	Success

Virtual Protection Group Recovery Settings

Protected site	Boston - Prod
Recovery site	DR Site
Default recovery host	Zerto Labs DR Cluster
Default recovery datastore	nfs-right-dr01
Default failover/move network	VM



Zerto

Virtual Machine Recovery Settings

ERP01

Recovery host	esxi-right-dr01.zerto.lab
Recovery datastores	
VM	nfs-right-dr01
Volume ERP01-0:0	nfs-right-dr01
Recovery networks	
Network adapter 1	VM
Recovery folder	/

ERP02

Recovery host	esxi-right-dr01.zerto.lab
Recovery datastores	
VM	nfs-right-dr01
Volume ERP02-0:0	nfs-right-dr01
Recovery networks	
Network adapter 1	VM
Recovery folder	/

Detailed Recovery Steps

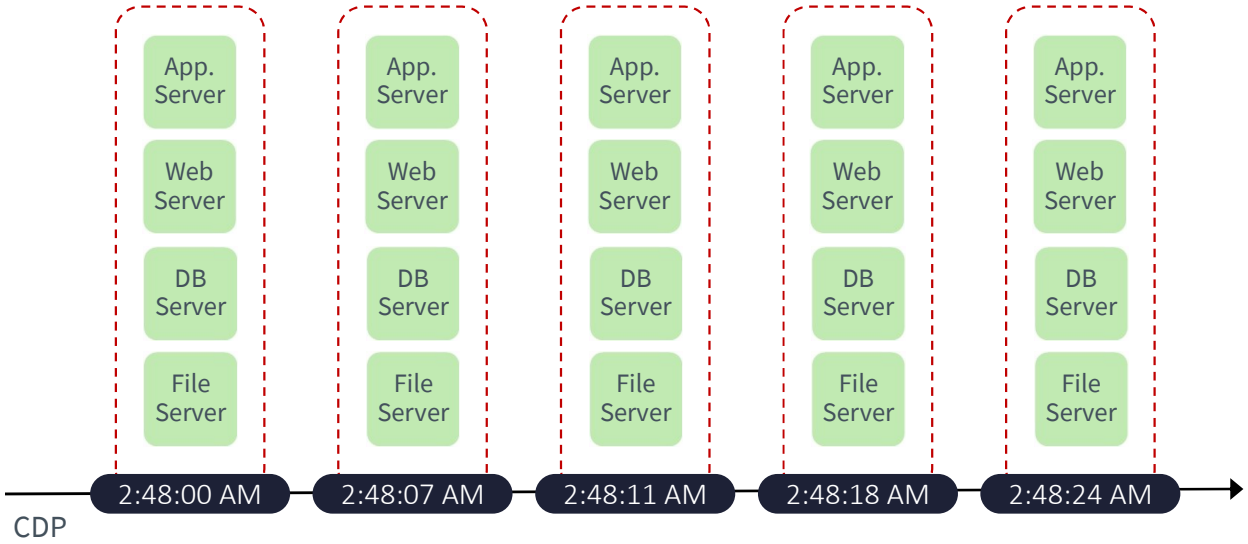
#	Step Description	Result	Start Time	End Time	Execution Time
1.	Recover VM 'ERP01'	Success	12:12:41	12:12:41	00:00:01
1.1.	Create recovery VM 'ERP01'	Success	12:12:41	12:12:41	00:00:01
2.	Recover VM 'ERP02'	Success	12:12:41	12:12:41	00:00:01
2.1.	Create recovery VM 'ERP02'	Success	12:12:41	12:12:41	00:00:01
3.	disable DRS	Success	12:12:42	12:12:42	00:00:00
3.1.	disable DRS	Success	12:12:42	12:12:42	00:00:00
3.2.	disable DRS	Success	12:12:42	12:12:42	00:00:00
4.	Recover VMs' 'ERP01' volumes	Success	12:12:42	12:12:48	00:00:06
4.1.	Create scratch volume for VM 'ERP01'	Success	12:12:42	12:12:44	00:00:03
4.2.	Detach volume 'ERP01-0:0:' from 'Z-VRAH-esxi-right-dr01.zerto.lab-458638'	Success	12:12:45	12:12:46	00:00:01
4.3.	Move volume to 'ERP01/ERP01.vmdk'	Success	12:12:46	12:12:47	00:00:00
4.4.	Attach volume 'ERP01-0:0:' to VM 'ERP01'	Success	12:12:47	12:12:47	00:00:01
5.	Recover VMs' 'ERP02' volumes	Success	12:12:42	12:12:48	00:00:06
5.1.	Create scratch volume for VM 'ERP02'	Success	12:12:42	12:12:44	00:00:03
5.2.	Detach volume 'ERP02-0:0:' from 'Z-VRAH-esxi-right-dr01.zerto.lab-458638'	Success	12:12:45	12:12:46	00:00:01
5.3.	Move volume to 'ERP02/ERP02.vmdk'	Success	12:12:46	12:12:47	00:00:00
5.4.	Attach volume 'ERP02-0:0:' to VM 'ERP02'	Success	12:12:47	12:12:47	00:00:01
6.	get ip for VM 'vm-3005'	Success	12:12:48	12:12:48	00:00:00
7.	get ip for VM 'vm-3006'	Success	12:12:48	12:12:48	00:00:00
8.	Start VMs	Success	12:12:48	12:12:50	00:00:02
8.1.	Start VM 'ERP02'	Success	12:12:48	12:12:50	00:00:02
8.2.	Start VM 'ERP01'	Success	12:12:48	12:12:49	00:00:00
9.	Failover Commit	Success	12:13:47	12:13:47	00:00:00

Full Name: _____ **Title:** _____ **Signature:** _____

Recovery Report for Virtual Protection Group ERP

KONSISTENTE - WIEDERHERSTELLUNG VON ANWENDUNGEN

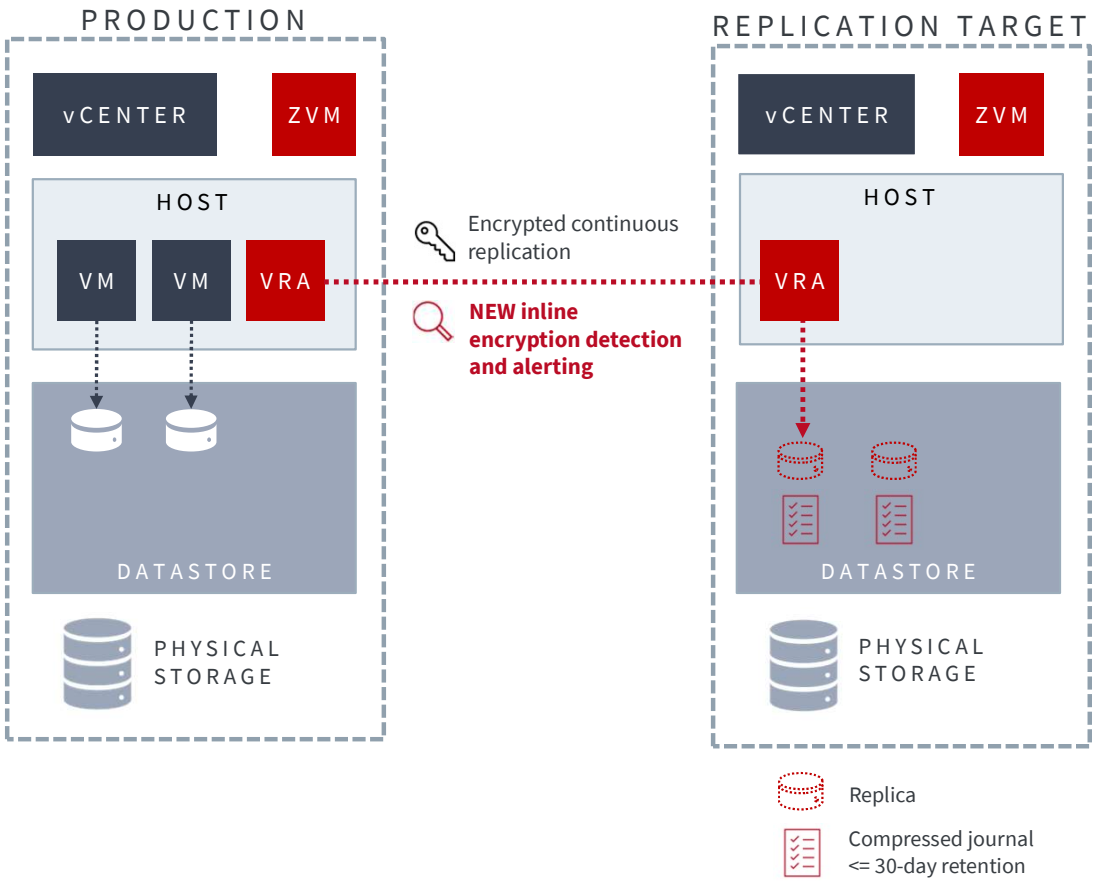
- ▶ CONTINUOUS DATA PROTECTION
- ▶ HYBRID UND MULTI-CLOUDS
- ▶ SKALIERBARE EINFACHHEIT



Anwendungen werden als konsistente Einheiten wiederhergestellt

Zerto
a Hewlett Packard Enterprise company

Replicate and Detect

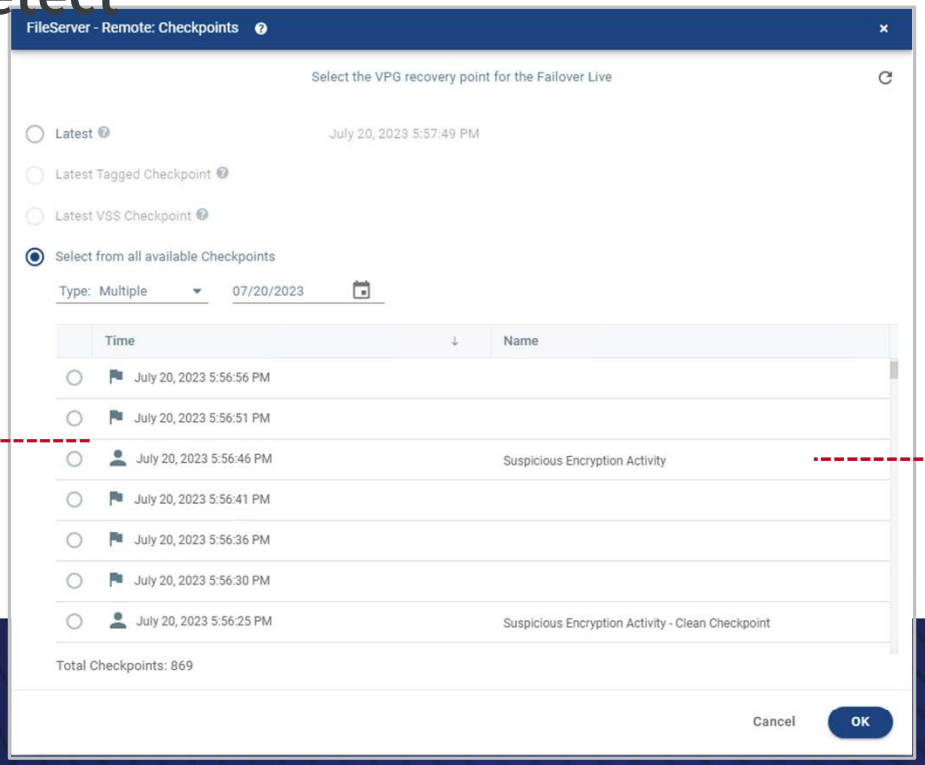


Software only

Copies Data, not VMs

Replicate and Detect

Replicate every change and log as recovery checkpoints every 5-15 seconds

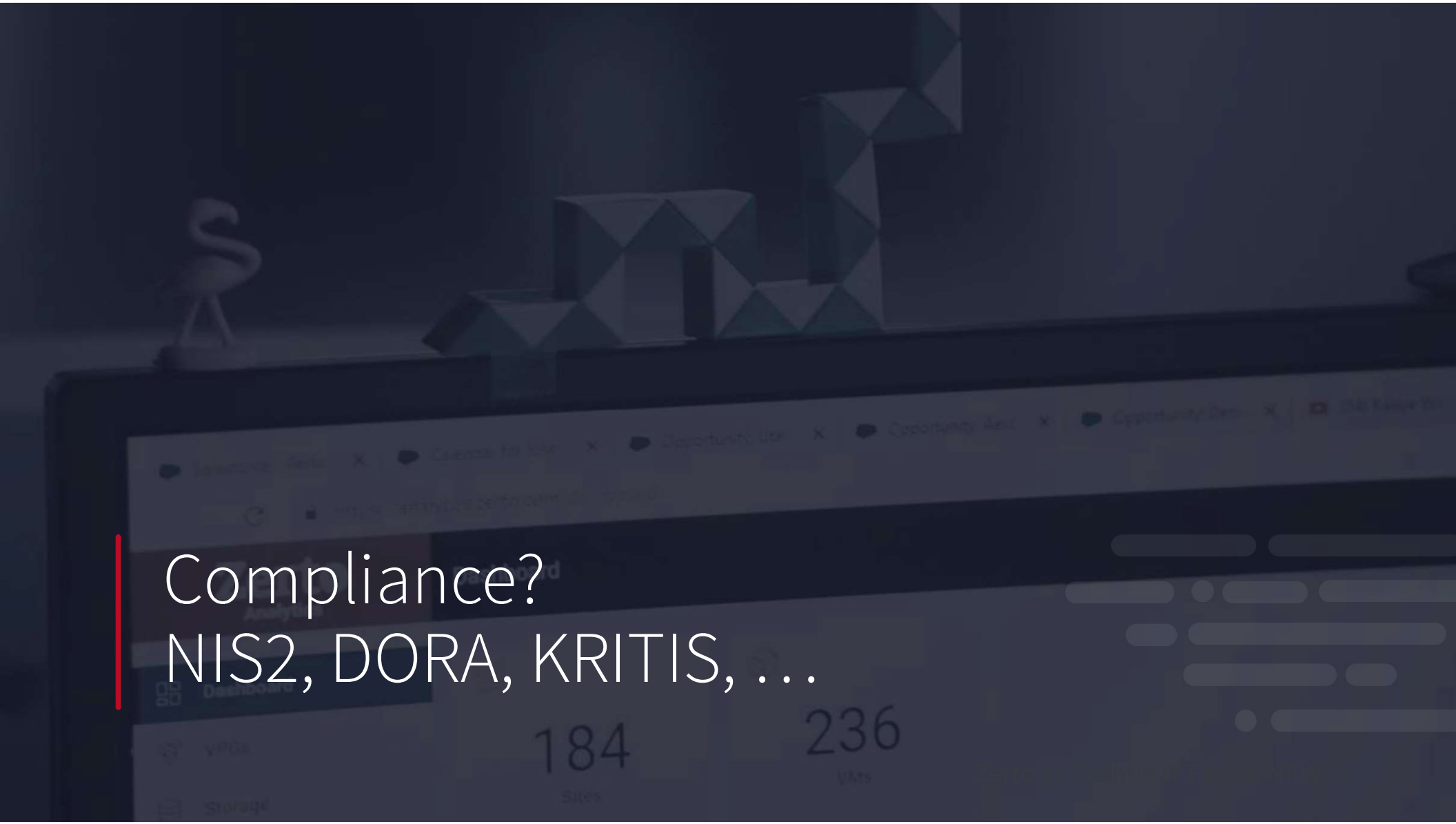


Detect suspicious writes as they stream in and flag for admins to investigate

"[Zerto's] real-time ransomware detection puts us in a much stronger position to both identify and mitigate ransomware attacks. This gives us confidence that we can proactively meet the risks presented by ransomware."

– Network admin at manufacturing customer

Zerto
a Hewlett Packard Enterprise company


Compliance?
NIS2, DORA, KRITIS, …
184
236

Isolate & Lock | Cyber Resilience Vault

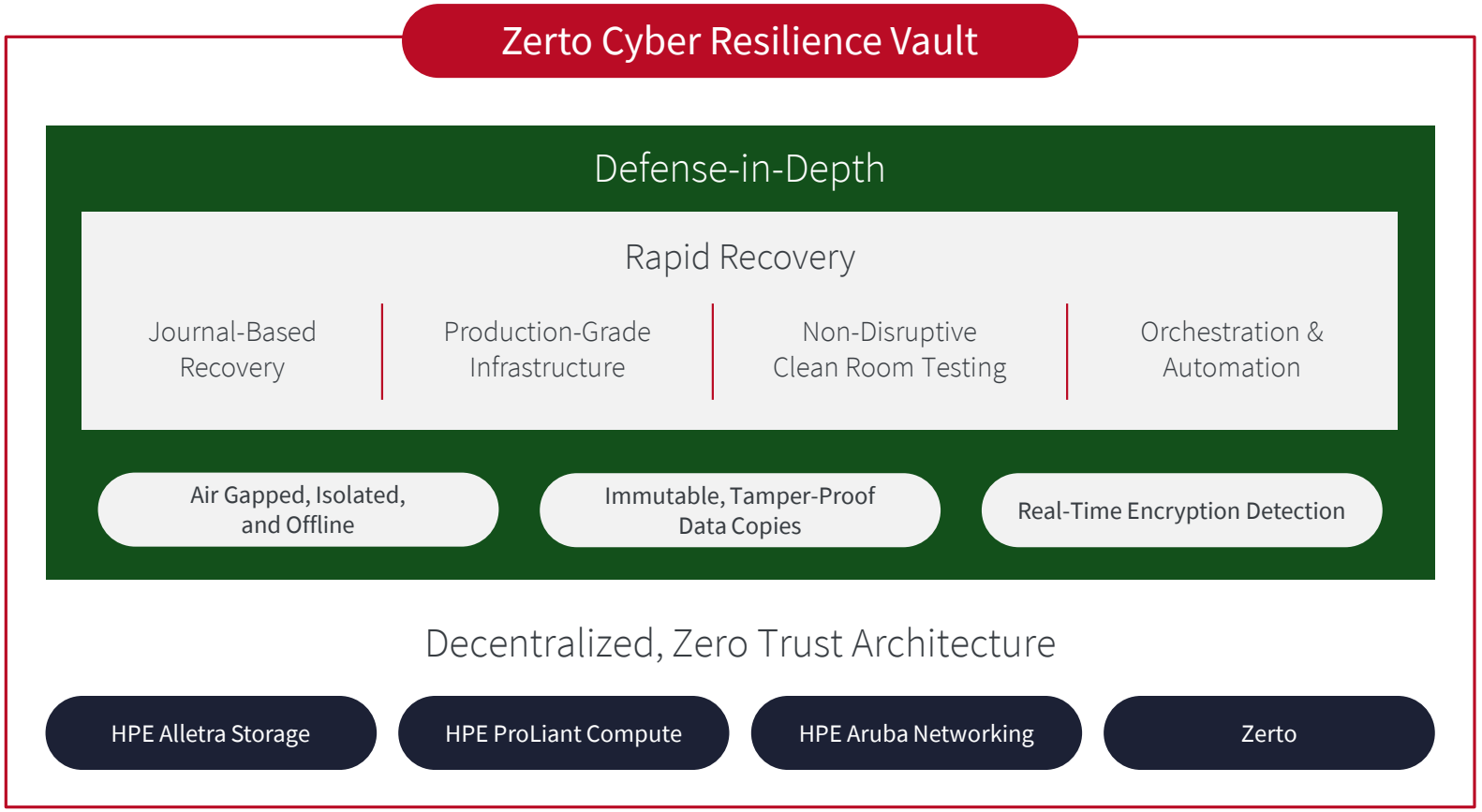
- ✓ **Isolated**
- ✓ **Air gapped**
- ✓ **Immutable**
- ✓ **Zero trust**

Isolated, offline, and air gapped with immutable data copies using zero trust architecture

Purpose-built for cyber recovery—option of last resort in worst-case scenarios

Isolate and Lock

Cyber Resilience Vault combines isolated recovery environment with immutable data vault



Key Take aways

- **Gefährdungslage durch Crypto-Locker erfordert Umdenken**
- **Backup reicht als Schutz nicht aus**
- **Schützen Sie Ihr Unternehmen und testen Sie den Ernstfall**