Hewlett Packard Enterprise

2023 HPE **Data Services Innovation** Day

HPE Data Protection Strategy

P2V 에서 On Premise/Cloud DR까지

자동화된 DR 훈련에서 랜섬웨어 감지까지

김흥준 매니저 | HPE

DR + Backup 솔루션

HPE Zerto 젤토

Hewlett Packard Enterprise

재해복구

[포커스온] 데이터의 시대, 백업과 재해 복구는 선택이 아닌 필수

석주원 기자 | 승인 2023.06.02 13:54 | 댓글 0

기업의 자산뿐 아니라 개인들의 소중한 추억까지 지켜 주는 데이터 보호 솔루션

현대 산업의 가장 중요한 자원은 데이터라는 말이 있다. 물론 여전히 석유가 없이는 현대 사회를 유지할 수 없겠지만, 데이터라는 무형의 자원의 가치가 그 정도로 커졌다는 의미를 빗대어 표현한 말이다. 실제로도 데이터를 잘 다루는 기업들의 가치는 이미 에너지 기업의 가치를 뛰어 넘고 있다. 그래서 기업들은 이제 데이터 자산을 어떻게 관리하고 활용해야 할지 고민하고 있다. 그리고 동시에 이 소중한 데이터를 어떻게 보관하고 지켜야 할지에 대한 고심도 깊어지고 있다.

- 제8항의 규정에 따른 금융회사 등은 자체적으로 업무의 중요도를 분석하여 핵심업무를 선정하고, 핵심업무가 주센터를 통한 서비스가 곤란한 경우에도 재해복구센터를 이용하여 복구목표시간내에 서비스가 가능하도록 업무지속성이 확보되어야함. 이 경우 복구목표시간은 3시간 이내이며, 보험회사는 24시간 이내임(제9항)

- 제8항의 규정에 의거 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시(제10항)

* 금융감독원 : 전자금융 감독규정 제23조

https://zdnet.co.kr › view

엔씨소프트, 전사 재해 복구 모의훈련 진행 - 지디넷코리아

2022. 12. 16. — 올해 모의 훈련은 재난 상황 발생 시 목표 시간 내 서비스를 복구하는 'IT 서비스 연속성' 유지를 목표로 진행됐다. 지진, 화재, 건물 붕괴 등 발생 ...

https://www.data.go.kr › bbs › ntc › selectNotice

[한국수력원자력] 재해복구 모의훈련에 따른 서비스 중단 안내

2022. 12. 13. — 한국수력원자력의 OPEN API 데이터를 이용해주셔서 감사드립니다. 우리 회사는 주요 정보시스템의 **재해**,재난에 대비해 실제 재난 상황을 가정한

대전교육정보원, 2022년 재해복구시스템서비스 전환 모의훈련 실시

홍대인 기자 htcpone@naver.com

시공·안전 > 전기공사

전기공사공제조합, 재해복구 모의훈련 실시

나지운 기자 | 입력 2022.10.26 09:43 수정 2022.10.26 17:31 댓글 0

랜섬웨어

"랜섬웨어 피해 80%가 中企 점검·복구 종합대응 마련해야"

지난 7월 콜택시 시스템 운영업체가 랜섬웨어 공격을 받으며 교통대란이 벌어졌다. 경기도, 경상북도 등 전국에서 콜택시 호출이 먹통이 됐다. 부산에서는 장애인 특별교통수단인 두리발 서비스가 차질을 빚었다. 한국 맞춤형 '귀신(GWISIN)' 랜섬웨어까지 기승을 부리고 있다. 보안 기업인 SK쉴더스 관계자는 "제조·금융·헬스케어 분야 등 전방위로 랜섬웨어로 인한 기업 피해가 확산하고 있다"고 24일 지적했다.

랜섬웨어 공격에 개인과 기업 할 것 없이 비상이 걸렸다. 랜섬웨어는 인질의 몸값을 뜻하는 '랜섬'과 소프트웨어를 합친 말로 악성 프로그램을 심은 뒤 시스템을 복구해주는 대가로 금전을 요구하는 사이버 범죄다. 지난해 한국랜섬웨어침해대응센터가 추정한 국내 총피해액은 2조원에 이른다.

과학기술정보통신부에 따르면 올해 국내 랜섬웨어 피해 신고 건수는 225건(8월 기준)으로 2년 만에 77% 급증했다. 피해 기업 중 80%가 보안에 취약한 중소기업이었다. 한국인터넷산업협회(KISA) 관계자는 "과거엔 무작위로 파일을 암호화하는 방식을 썼지만, 최근엔 기업 내부 중요 파일을 선별적으로 암호화한 뒤 경쟁사에 전송하는 등 협박 형태가 진화하고 있다"고 우려했다.

기업 내부 시스템이 랜섬웨어에 감염되면 업무 중단에 따른 매출 감소, 법적 소송까지 이어질 수 있다는 지적이다. 사전 점검, 위협 탐지, 복구 등 종합적인 대응이 중요한 이유다. SK쉴더스는 자체 랜섬웨어 대응센터를 통해 기업들과 초기 대응 방법을 공유하는 식으로 협업하고 있다. SK쉴더스 화이트해커 그룹 이큐스트(EQST)가 원격으로 기업의 피해 상황과 정보기술(IT) 환경에 대한 정확한 분석을 진행한다. 자체 제작한 랜섬웨어 위협 진단 툴을 제공해 PC나 서버가 랜섬웨어에 노출됐는지 쉽고 빠르게 점검할 수 있도록 돕는다. 개인 사용자는 주요 랜섬웨어 20종을 비롯해 취약점 14개에 대한 테스트를 무료로 제공한다.

임직원 대상 랜섬웨어 이메일 모의훈련을 해보고 대응 시스템이 적절한지 평가하는 서비스도 있다. 이메일을 통한 랜섬웨어 공격에 대응 가능한 '이메일 보안 관제 서비스'도 중소기업의 보안 역량 고도화에 힘을 보태고 있다는 평가다.

SK쉴더스 관계자는 "맞춤형 모의 해킹, 랜섬웨어 전용 상품 '사이버가드', 사고 대응 및 복구 서비스 등 랜섬웨어에 특화된 다양한 보안 서비스를 제공하고 있다"고 말했다. SK쉴더스는 랜섬웨어 피해로 인한 고객의 손해배상, 복구 비용 지원 등 종합적인 피해 보상을 돕는 보험 상품도 선보일 예정이다. 다양한 보안 솔루션과 연계해 랜섬웨어 통합 대응 시스템 구축에 속도를 낸다는 각오다.

김병근 기자

금증하는 랜섬웨어 피해 신고
(단위: 건)

※2022년은 8월 누적
자료: 한국인터넷진흥원

작년 국내 총피해액만 2조
韓 맞춤 랜섬웨어까지 기승
SK쉴더스, 모의훈련 등 지원

"지난달 랜섬웨어 피해 급증…대책 수립해야"

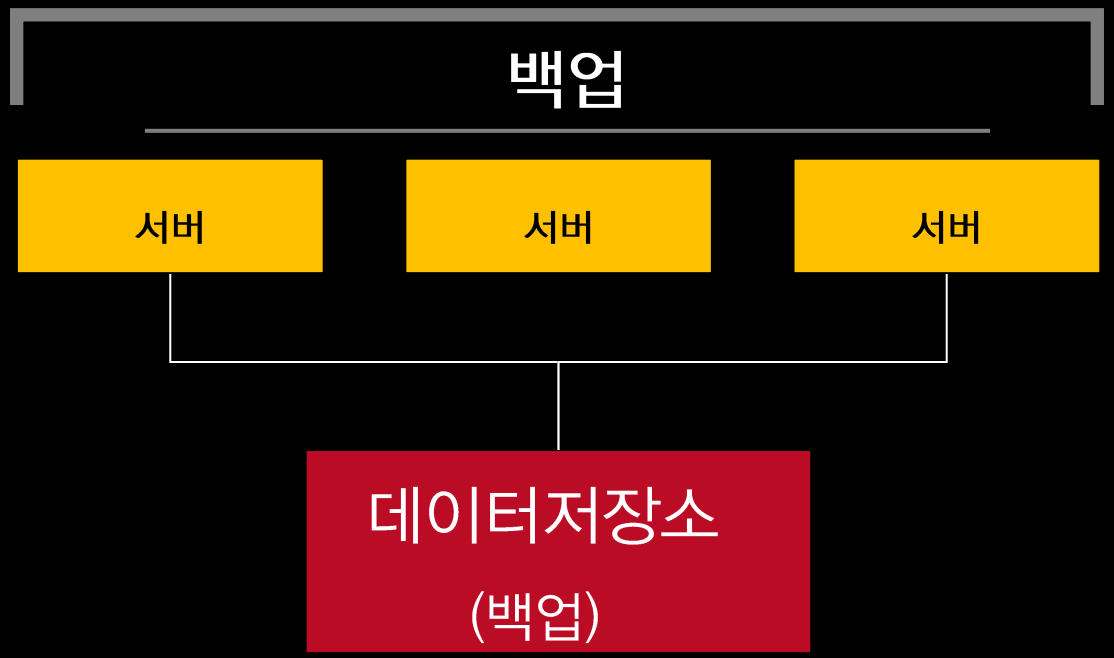
이도경 기자 | wudstok@seoulfn.com | 승인 2023.04.21 14:35 | 댓글 0

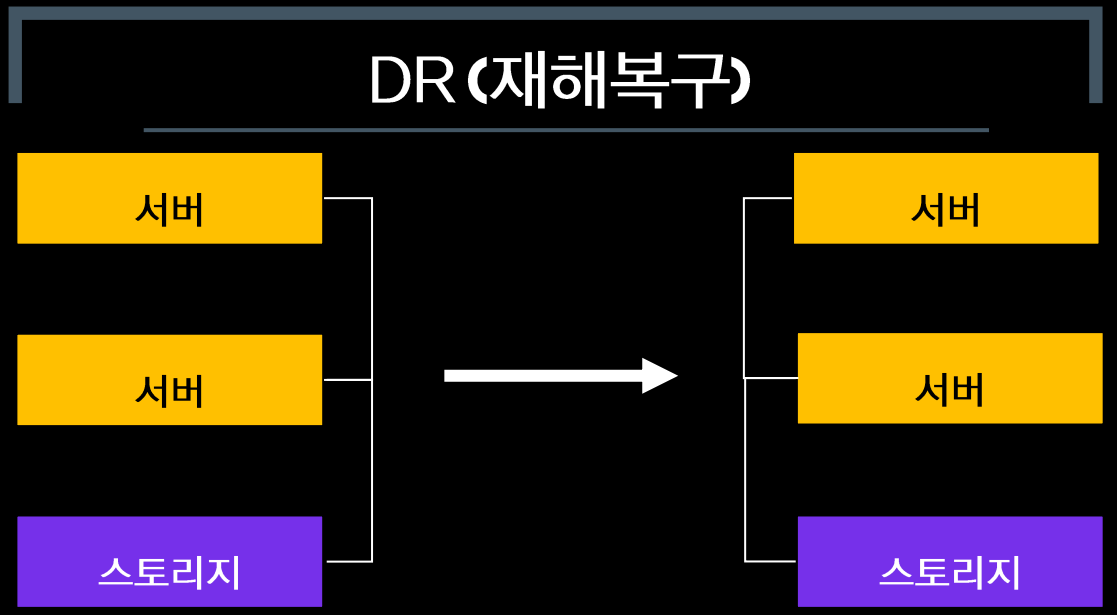
> 1분기 랜섬웨어 공격 933건…3월 한 달간 절반 집중

1분기 가장 많이 발견된 랜섬웨어는 '락빗'(290건)으로 조사됐으며 △클롭(110건) △블랙캣(90건) △로열(72건) △비안리안(51건) 등이 뒤를 따랐다.

업종별는 제조업(180건)과 서비스업(139건)에서 랜섬웨어 피해가 컸으며 △유통·무역·방송(88건) △IT·웹·통신(78건) △의료·제약·복지(73건) 순이었다.

백업 vs DR





가상화, 클라우드 환경의 DR + 백업 솔루션

오케스트레이션 | 오토메이션

Zerto 10

랜섬웨어 복구

DR 재해 복구

멀티 클라우드 복구

Continuous Data Protection

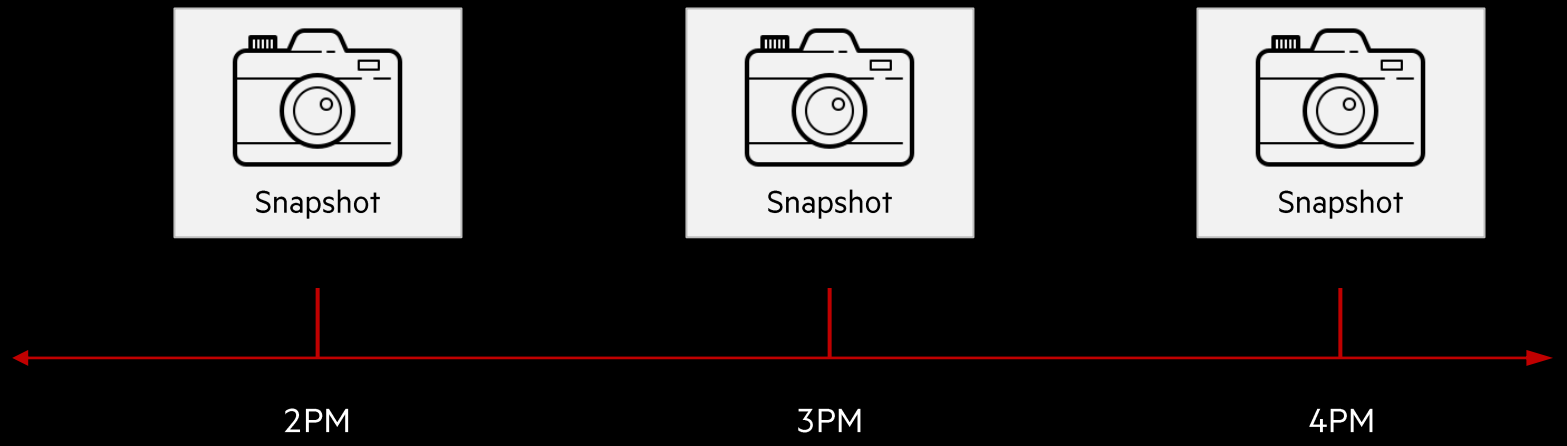
vmware | Microsoft Azure | aws | IBM Cloud | ORACLE CLOUD | Hewlett Packard Enterprise | MSP

Google Kubernetes Engine | IBM Cloud Kubernetes Service | Amazon EKS | RED HAT OPENSHIFT | VMware Tanzu | Google Cloud

CDP Continuous Data Protection 기반

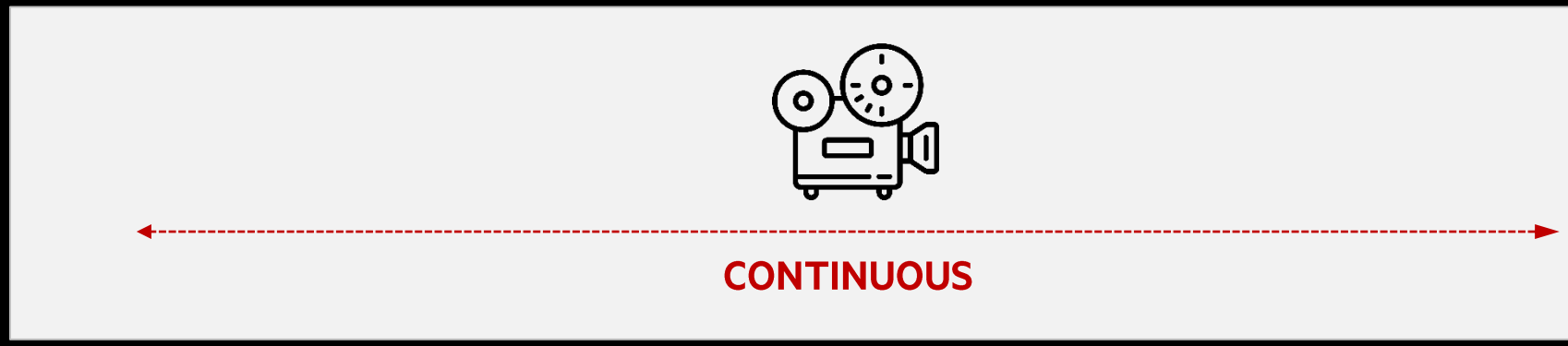
Traditional

일반적인 형태의
snapshot/backup



Zerto
a Hewlett Packard Enterprise company

Journal 기반의
CDP, Data
Protection



Hewlett Packard
Enterprise

제품 사상

Zero to Ø

데이터와 서비스의 **Zero Down Time** 목표

2009년도 설립

80개국 9500개 고객사, 450 개 MSP

국내 **100여개 고객사**

Hewlett Packard Enterprise

14년 축적 된 경험과 노하우, 검증 된 솔루션

CDP 기반의 복제기술

Public Cloud
AWS/Azure

빅데이터 분석용
파일 검색 엔진

모의훈련
무인 자동

Migration
CDP 백업

K8S
컨테이너

2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

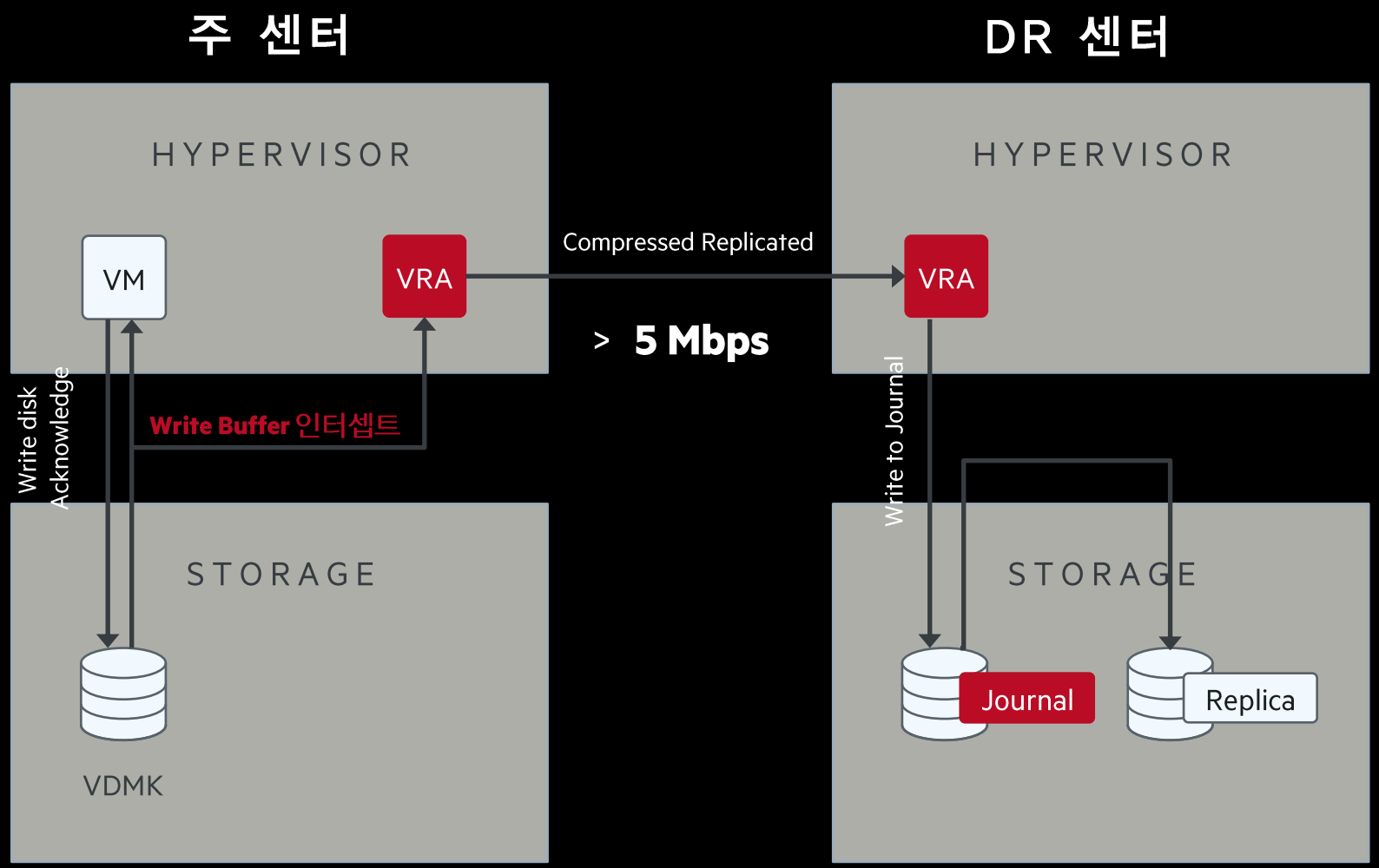
TOP EU MANUFACTURER
1,200 VMs
5 Sec RPO
SCHWARZ
5,000 VMs
7 sec RPO

FORTUNE 10 ORGANIZATION
1,200 VMs
9 sec RPO
American Airlines
7,200 VMs
7 Sec RPO

jack henry & ASSOCIATES INC.
2,000 VMs
5 sec RPO
Anthem
8,000 VMs
6 sec RPO

UNITED AIRLINES
4,000 VMs
8 sec RPO
Solera
20,000 VMs
10 sec RPO

Zerto 아키텍처 In-Memory 기반 CDP 기술



Zerto 아키텍처

Daily Backups

Data GAP = 24 hours

일 단위

0 6 12 24

Snapshot-Based Backup

Data GAP = hours

시간 단위

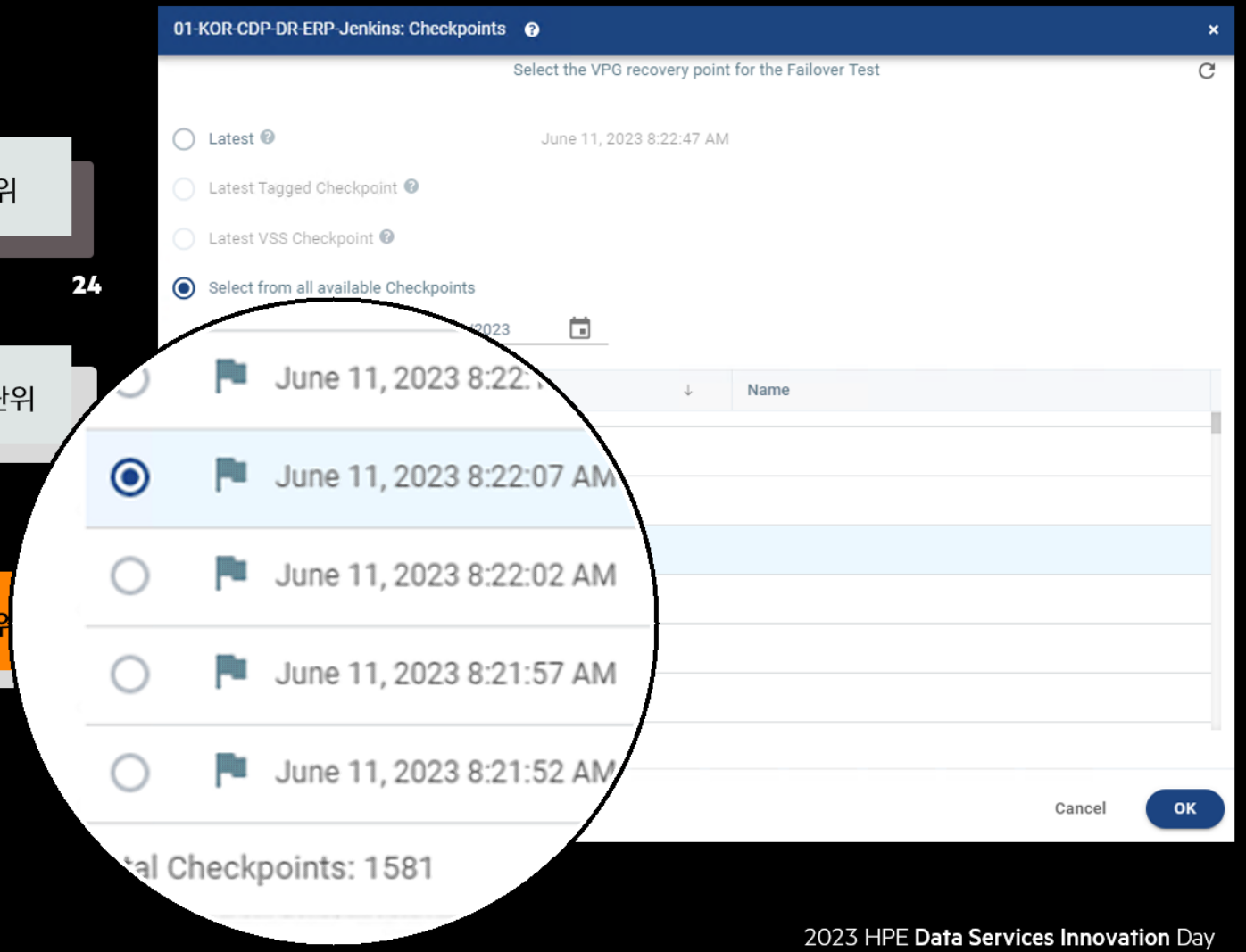
0 6 12

HPE Zerto

Data GAP = Seconds

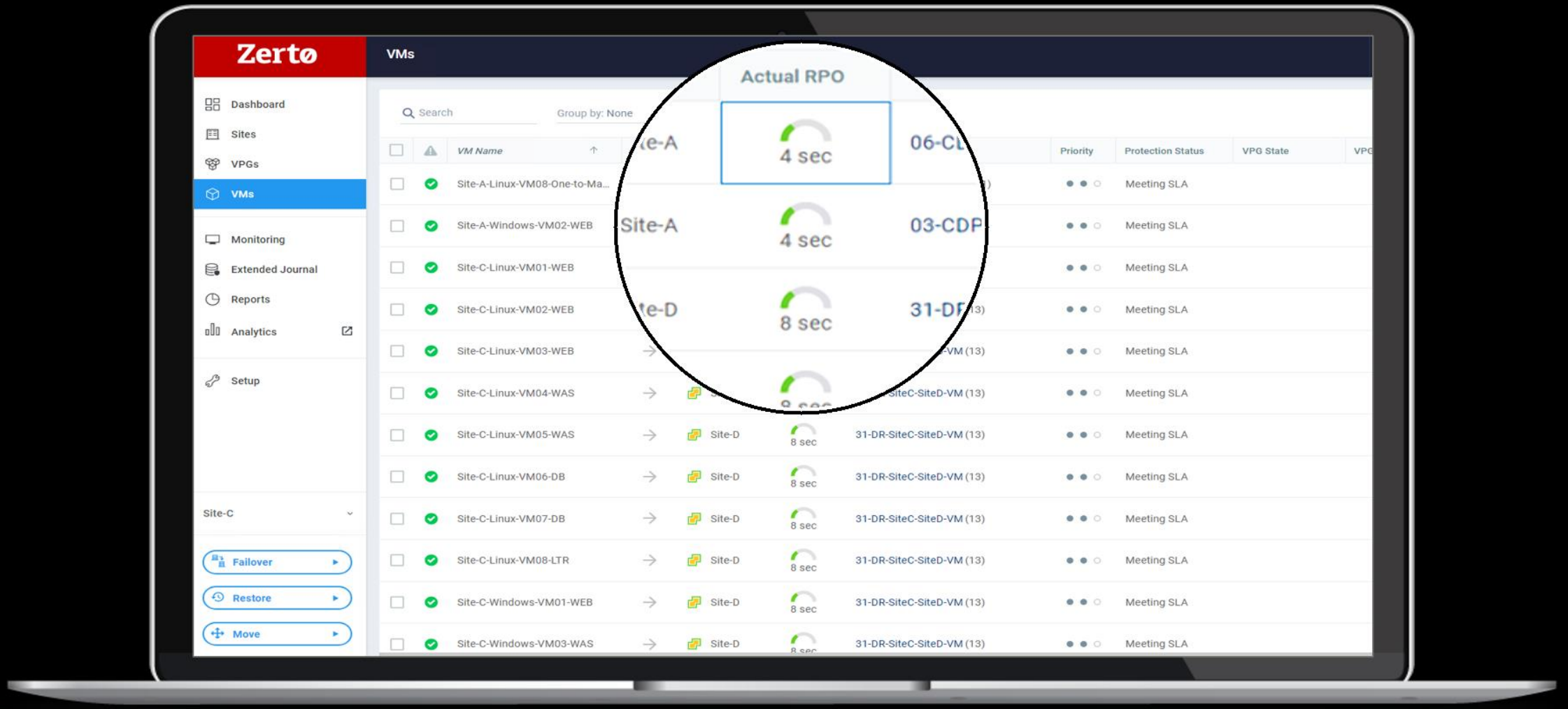
초 단위

0 6 12

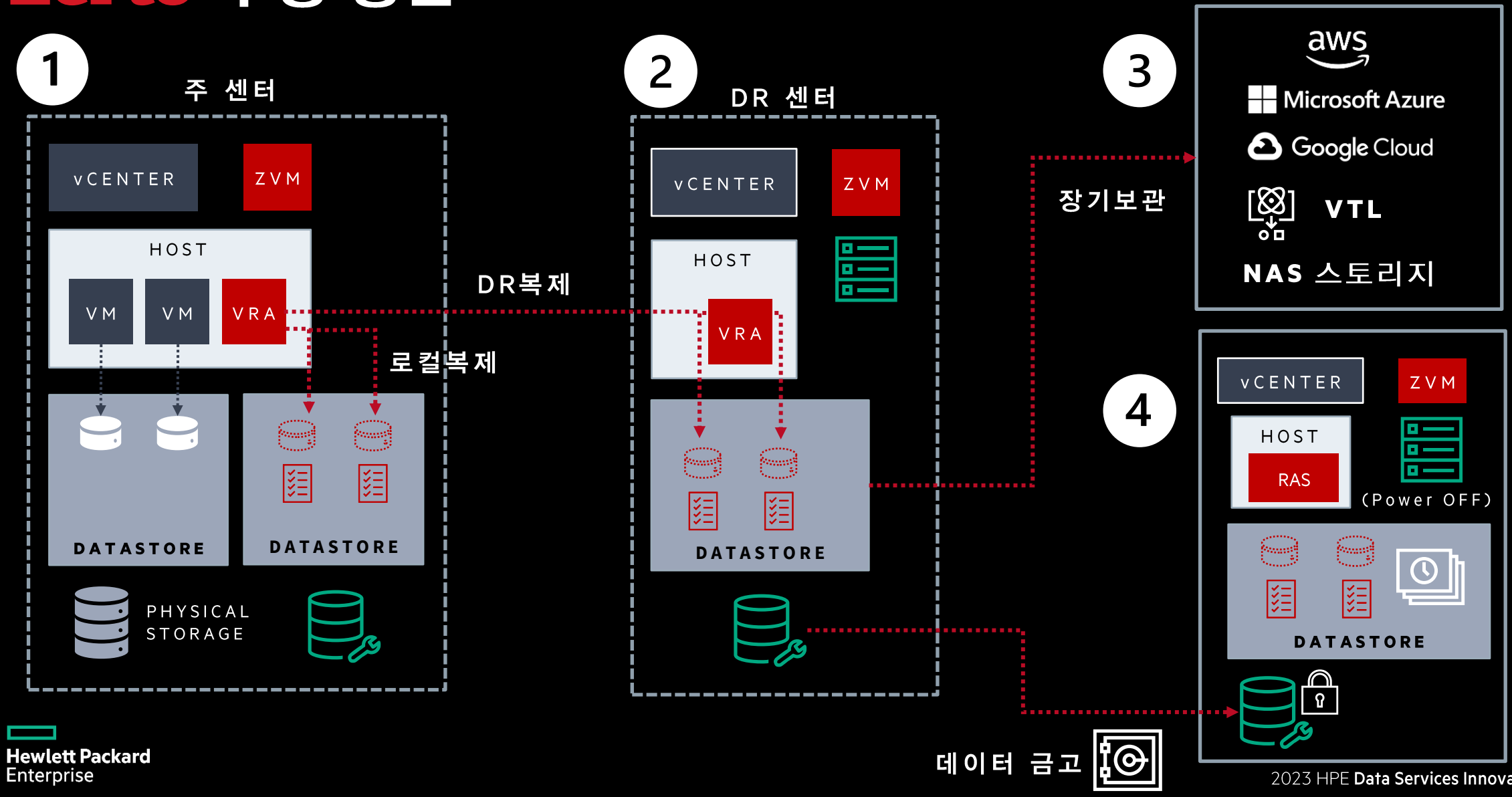


Hewlett Packard Enterprise

Zerto 아키텍처


Zerto
VMs
Dashboard
Sites
VPGs
VMs
Monitoring
Extended Journal
Reports
Analytics
Setup
Site-C
Failover
Restore
Move
Search
Group by: None
Actual RPO
4 sec
4 sec
8 sec
VM Name
Priority
Protection Status
VPG State
Site-A-Linux-VM08-One-to-Ma...
Site-A-Windows-VM02-WEB
Site-C-Linux-VM01-WEB
Site-C-Linux-VM02-WEB
Site-C-Linux-VM03-WEB
Site-C-Linux-VM04-WAS
Site-C-Linux-VM05-WAS
Site-C-Linux-VM06-DB
Site-C-Linux-VM07-DB
Site-C-Linux-VM08-LTR
Site-C-Windows-VM01-WEB
Site-C-Windows-VM03-WAS
Site-D
31-DR-SiteC-SiteD-VM (13)
Meeting SLA

Zerto 구성 방안



Hewlett Packard Enterprise

HPE Zerto 특장점

모의훈련 완전 자동화

Hewlett Packard Enterprise

모의훈련 복잡도

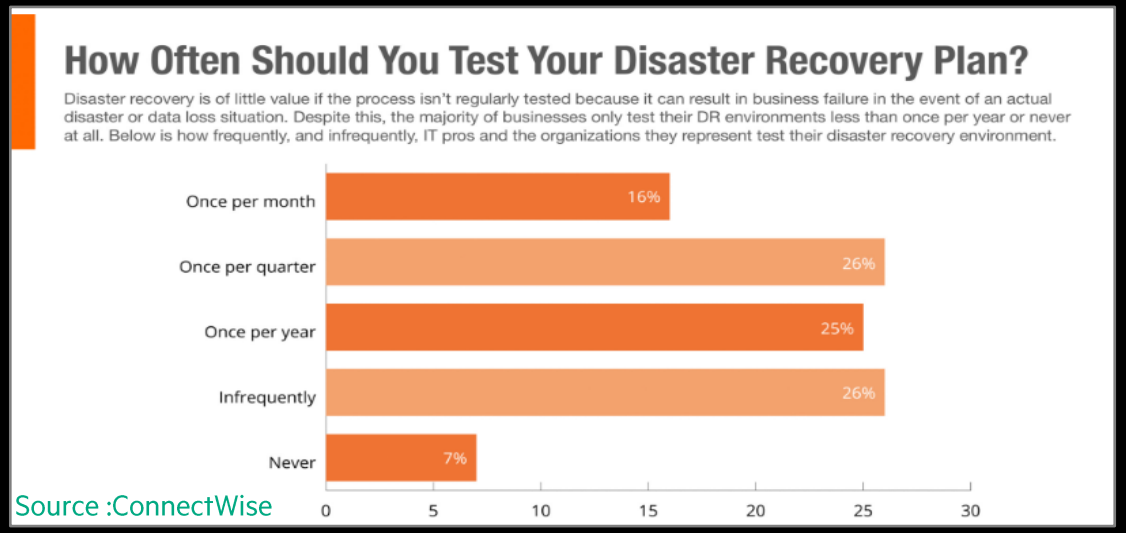
필요한 IT 자원	위험요소		투입 인력	
서버	주 센터 영향도	역 복제 Risk	가상화 엔지니어	관리자
스토리지	운영 망 Risk	IP 충돌	스토리지 엔지니어	운영자
네트워크	MAC 충돌	수동 스크립트	네트워크 엔지니어	네트워크 담당
DR 회선	자동화 구현방안	모의훈련	보안 엔지니어	보안 담당
WAN 가속기	결과 보고서		DR SW 엔지니어	업무 별 담당자
DR 전용 SW			RPO 기대치 1~2 시간	RTO 기대치 5~8 시간

그래서 현실은...

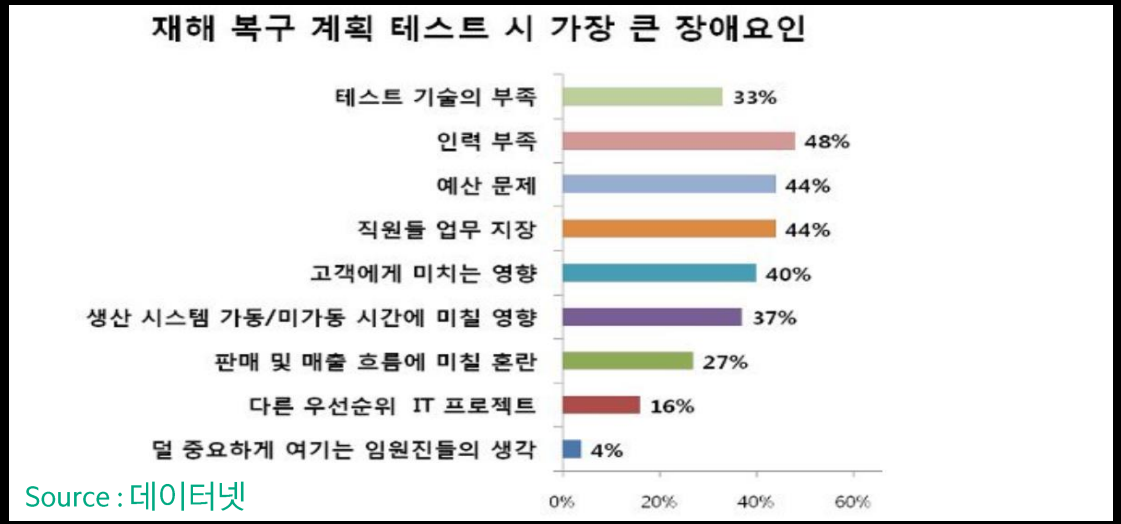
Have you ever tested your disaster recovery plan, and if so, what happened?

Don't know if we have a disaster recovery plan	6%	8
We definitely don't have a disaster recovery plan	12%	16
Never tested it, no idea if it works	17%	22
Tested it, we crashed and burned	1%	1
Tested it, we'd forgotten a few things	17%	23
Tested it, couldn't meet down-time SLA (RTO)	2%	2
Tested it, couldn't meet data-loss SLA (RPO)	0%	0
Tested it, couldn't meet either SLA	0%	0
Tested it once, everything went to plan	14%	19
Test it regularly, everything goes to plan	22%	29
Other? Enter here...	9%	12

Source :sqlskills.com — Total: 132 responses



Source :ConnectWise

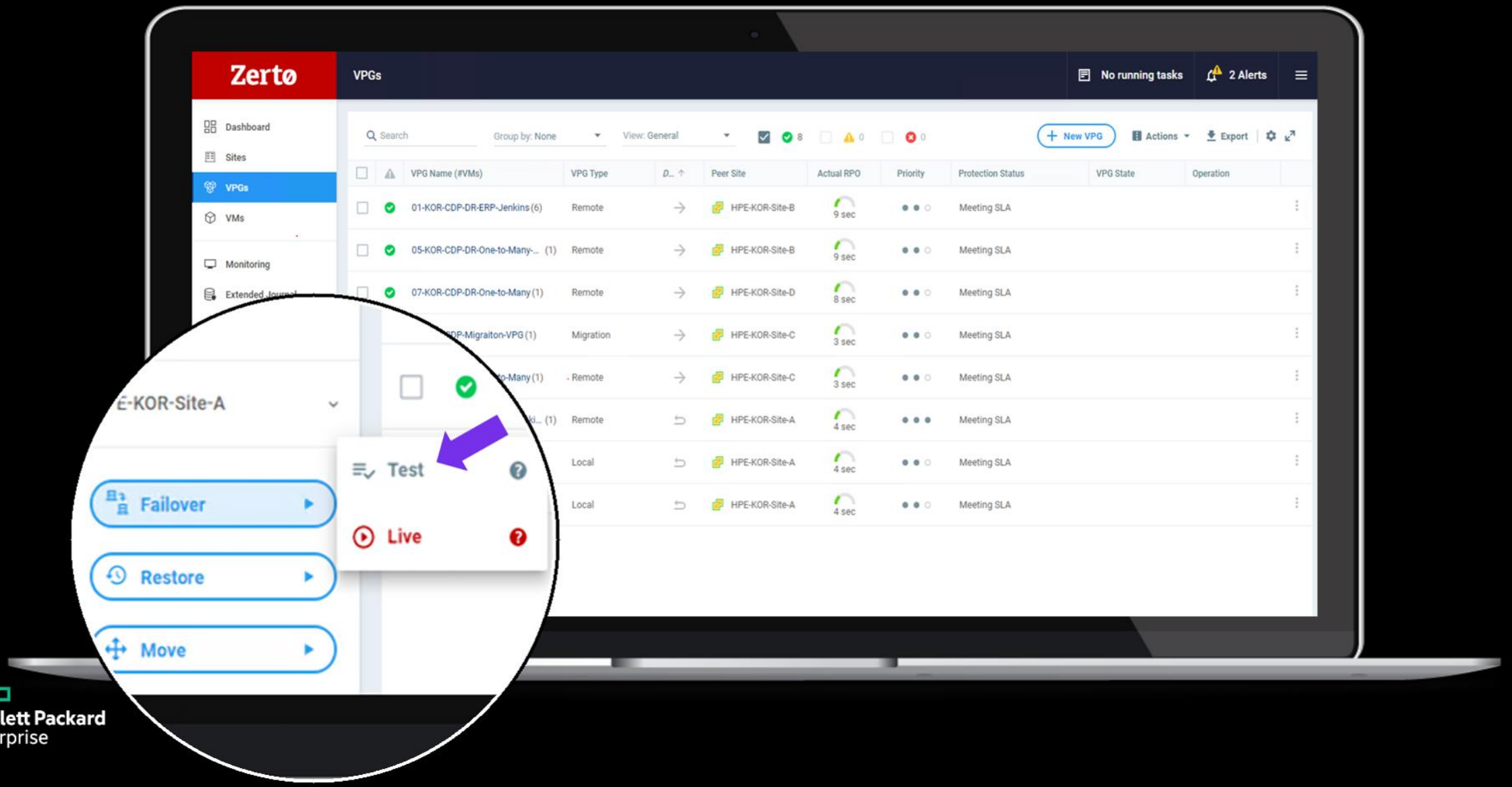


Source : 데이터넷

- **58%** 만 **1**년에 한번 이하 수행
- 그 중의 **22%** 만 주기적인 모의훈련 성공적 수행

Hewlett Packard Enterprise

Zerto 모의 훈련



Hewlett Packard Enterprise

Zerto 모의 훈련 보고서

Zerto

Recovery Report for Virtual Protection Group Site-A-Multiple-VM-VPG

Report was generated on 04/04/2023 12:13:57

Recovery Operation Details

Initiated by	Administrator
Recovery operation	Failover Test
Point in time	04/04/2023 12:11:53
Recovery operation start time	04/04/2023 12:12:02
Recovery operation end time	04/04/2023 12:13:35
RTO	21 seconds
Recovery operation result	Passed by user
User notes	Stop Test for VPG Site-A-Multiple-VM-VPG

Virtual Protection Group Recovery Settings

Protected site	Site-A
Recovery site	Site-B
Default recovery host	7esxi216-02.hpe.local
Default recovery datastore	ESXi02-ZERTO-DS02-BASE
Default test recovery network	ZERTO-TEST-BUBBLE

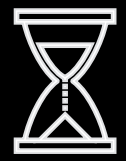
Detailed Recovery Steps

#	Step Description	Result	Start Time	End Time	Execution Time
1.	Fail-over test VM 'Wordpress-2'	Success	10:07:37	10:07:38	00:00:01
1.1.	Create recovery VM 'Wordpress-2 - testing recovery'	Success	10:07:37	10:07:38	00:00:01
2.	Fail-over test VM 'Wordpress-1'	Success	10:07:37	10:07:38	00:00:01
2.1.	Create recovery VM 'Wordpress-1 - testing recovery'	Success	10:07:37	10:07:38	00:00:01
3.	disable DRS	Success	10:07:38	10:07:38	00:00:00
3.1.	disable DRS	Success	10:07:38	10:07:38	00:00:00
3.2.	disable DRS	Success	10:07:38	10:07:38	00:00:00
4.	Fail-over test VMs' 'Wordpress-2' volumes	Success	10:07:38	10:07:56	00:00:18
4.1.	Create scratch volume for VM 'Wordpress-2 - testing recovery'	Success	10:07:38	10:07:45	00:00:06
4.2.	Detach volume 'Wordpress-2-0:0:' from 'Z-VRAH-esxi-left-prod01.zerto.lab-889184'	Success	10:07:45	10:07:51	00:00:06
4.3.	Attach volume 'Wordpress-2-0:0:' to VM 'Wordpress-2 - testing recovery'	Success	10:07:51	10:07:56	00:00:05
5.	Fail-over test VMs' 'Wordpress-1' volumes	Success	10:07:38	10:07:56	00:00:18
5.1.	Create scratch volume for VM 'Wordpress-1 - testing recovery'	Success	10:07:38	10:07:45	00:00:06
5.2.	Detach volume 'Wordpress-1-0:0:' from 'Z-VRAH-esxi-left-prod01.zerto.lab-889184'	Success	10:07:45	10:07:51	00:00:06
5.3.	Attach volume 'Wordpress-1-0:0:' to VM 'Wordpress-1 - testing recovery'	Success	10:07:51	10:07:56	00:00:05
6.	get ip for VM 'vm-7019'	Success	10:07:56	10:07:56	00:00:00
7.	get ip for VM 'vm-7010'	Success	10:07:56	10:07:56	00:00:00
8.	Start VMs	Success	10:07:56	10:07:58	00:00:01
8.1.	Start VM 'Wordpress-2 - testing recovery'	Success	10:07:56	10:07:58	00:00:01
8.2.	Start VM 'Wordpress-1 - testing recovery'	Success	10:07:56	10:07:58	00:00:01

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

Hewlett Packard Enterprise

Zerto 모의 훈련 특장점

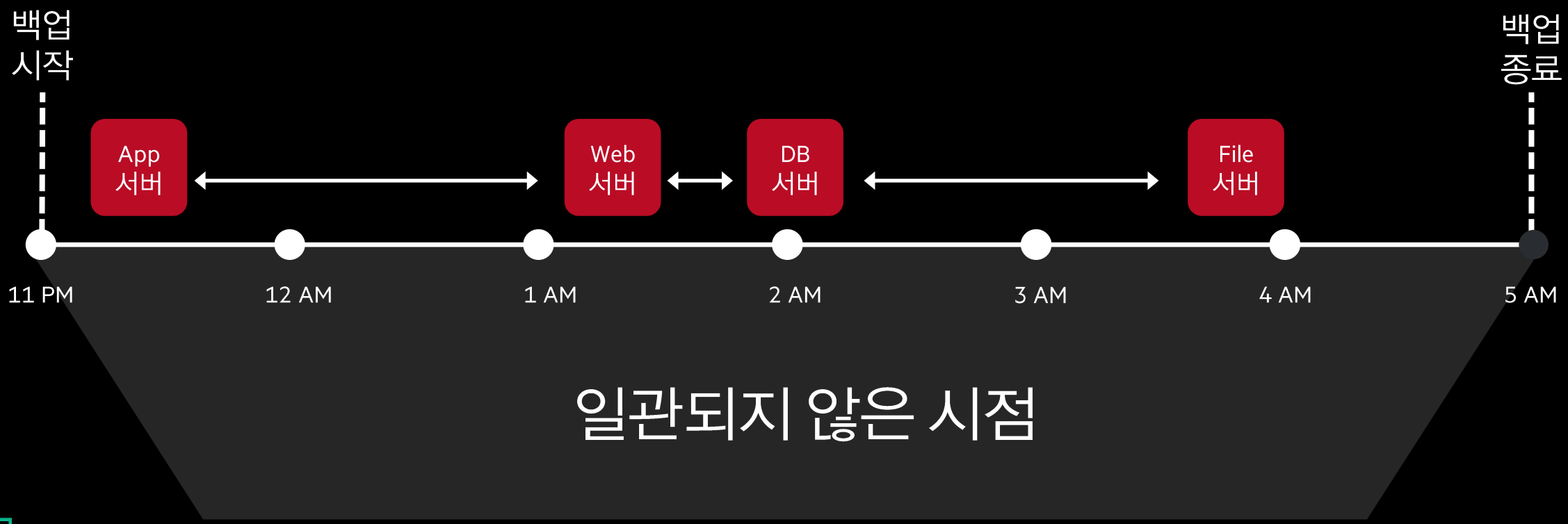
주 센터 영향 無	완벽한 DR 검증	정확한 시간 예측	결과 보고서 생성
			

HPE Zerto 특장점

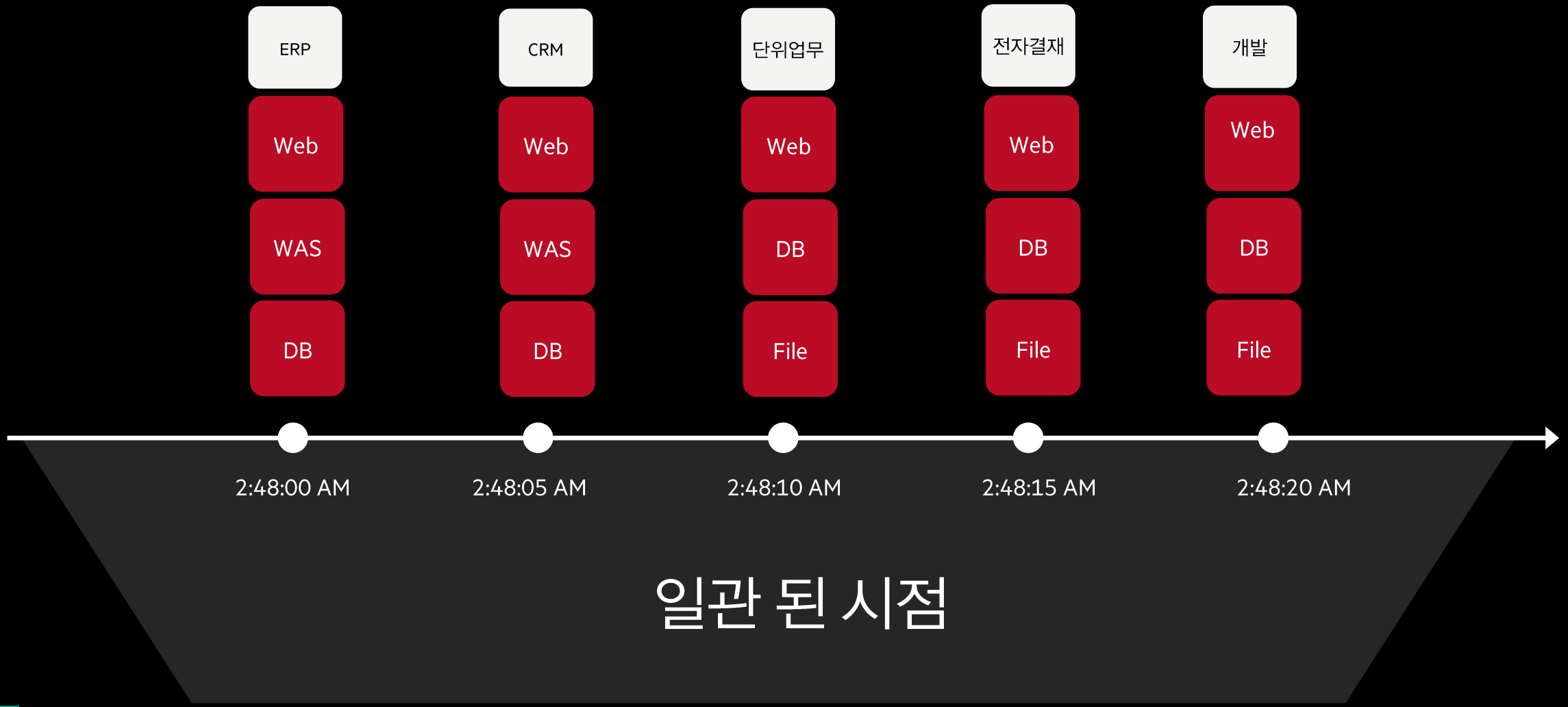
데이터 정합성 보장

Hewlett Packard Enterprise

기존 백업


백업
시작
백업
종료
App
서버
Web
서버
DB
서버
File
서버
11 PM
12 AM
1 AM
2 AM
3 AM
4 AM
5 AM
일관되지 않은 시점

Zerto 정합성 그룹


ERP
Web
WAS
DB
CRM
Web
WAS
DB
단위업무
Web
DB
File
전자결재
Web
DB
File
개발
Web
DB
File
2:48:00 AM
2:48:05 AM
2:48:10 AM
2:48:15 AM
2:48:20 AM
일관 된 시점

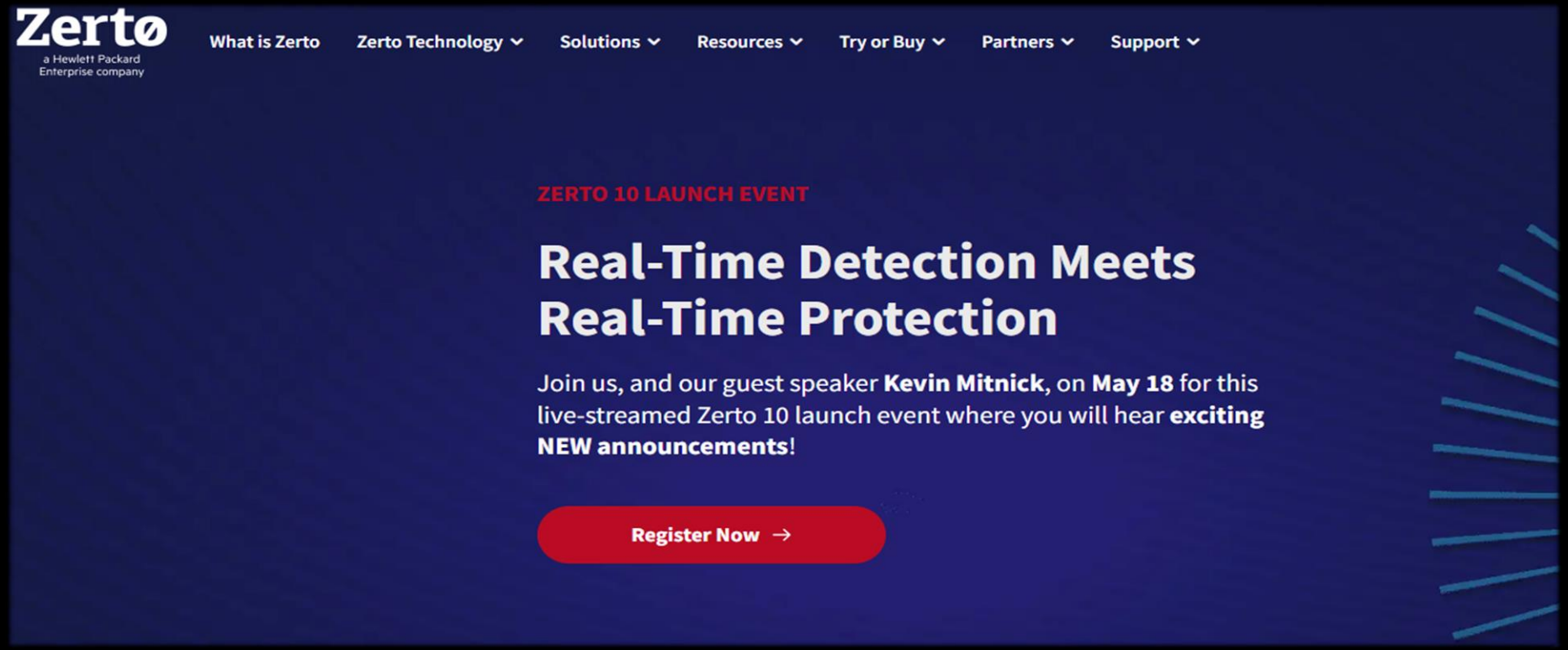
HPE Zerto 특장점

랜섬웨어 특화기능

Hewlett Packard Enterprise

HPE Only

Zerto 실시간 랜섬웨어 탐지



2023.5.18

Zerto 10 발표

Hewlett Packard Enterprise

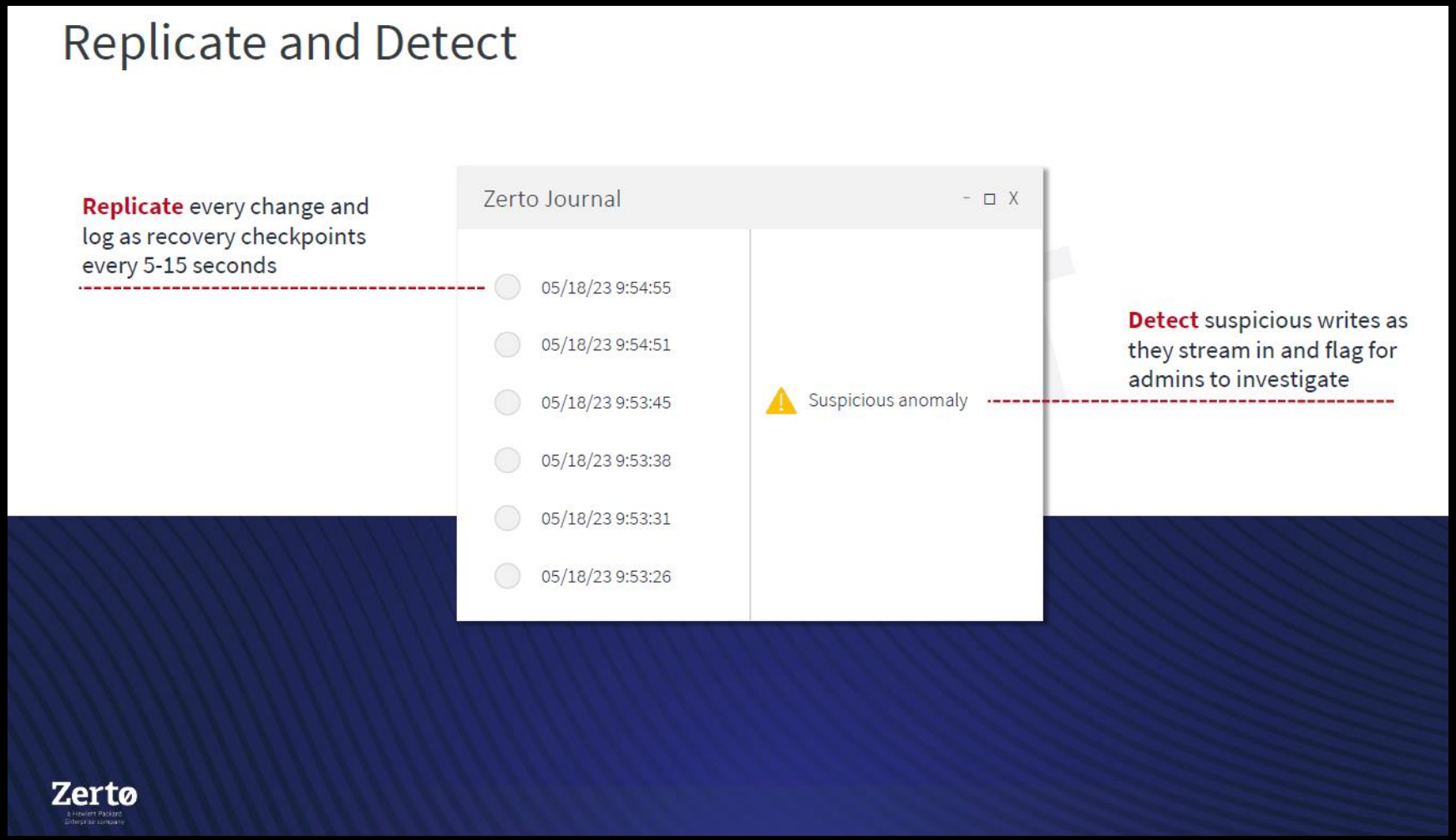
Zerto 암호화 IO 패턴 감지

HPE Only

Hewlett Packard Enterprise

Zerto 이상감지 시점 자동기록

HPE Only

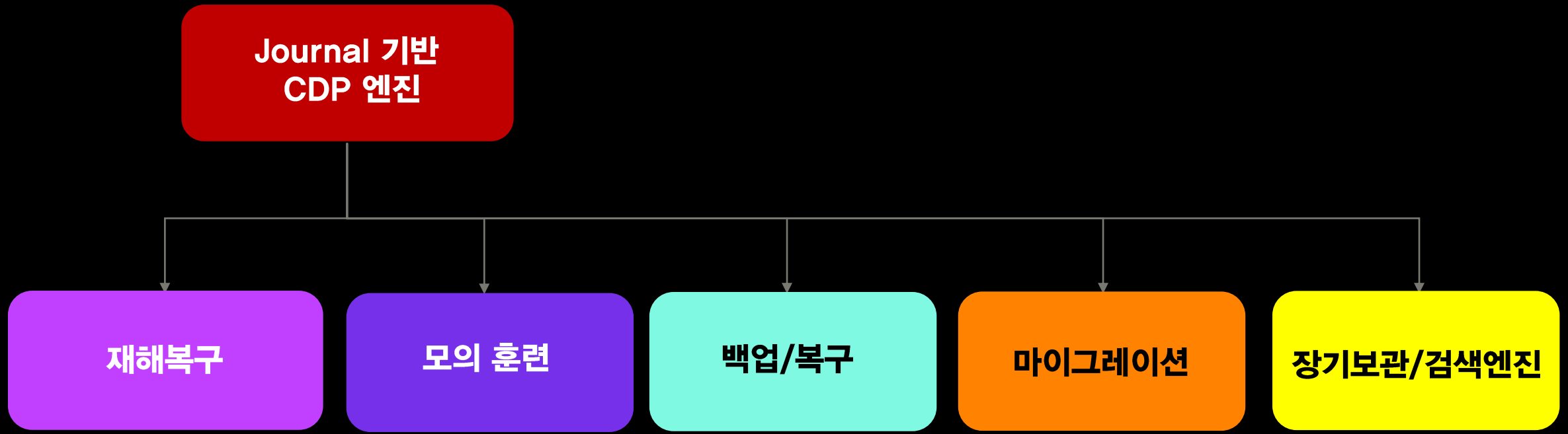


Hewlett Packard Enterprise

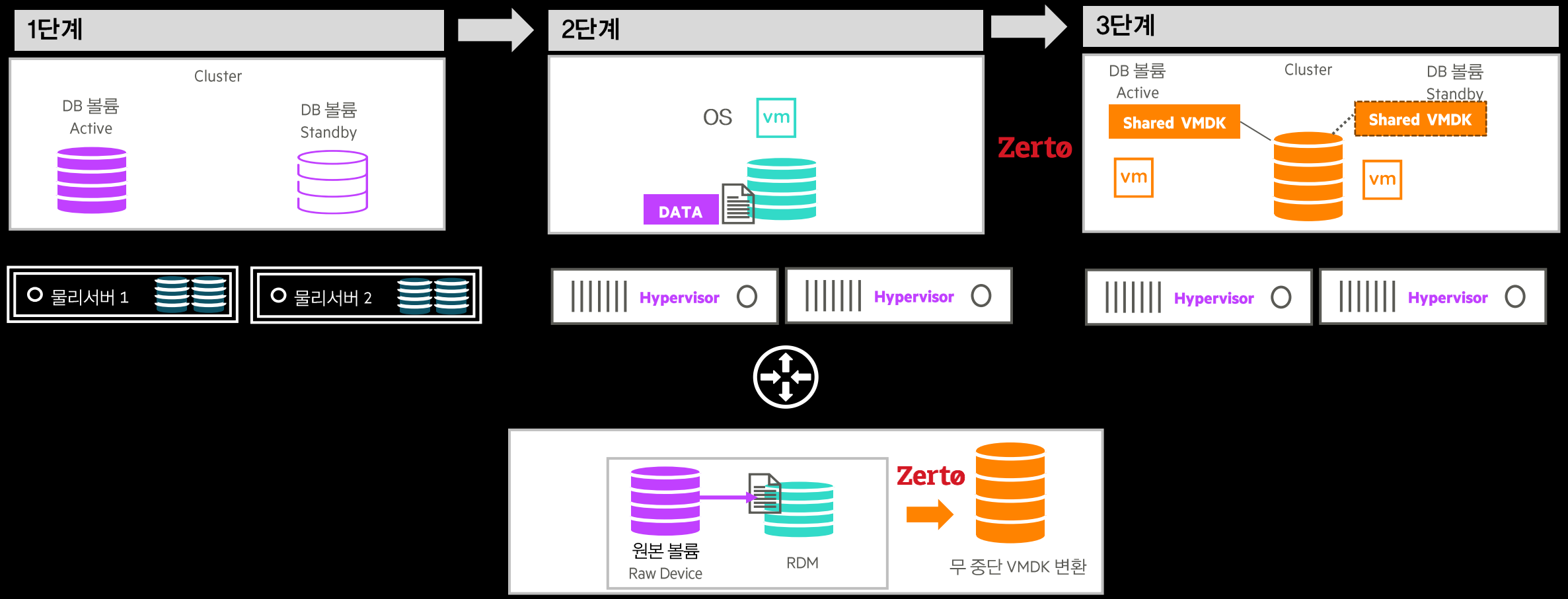
HPE Zerto 특장점

기타

Zerto 주요 핵심 기능

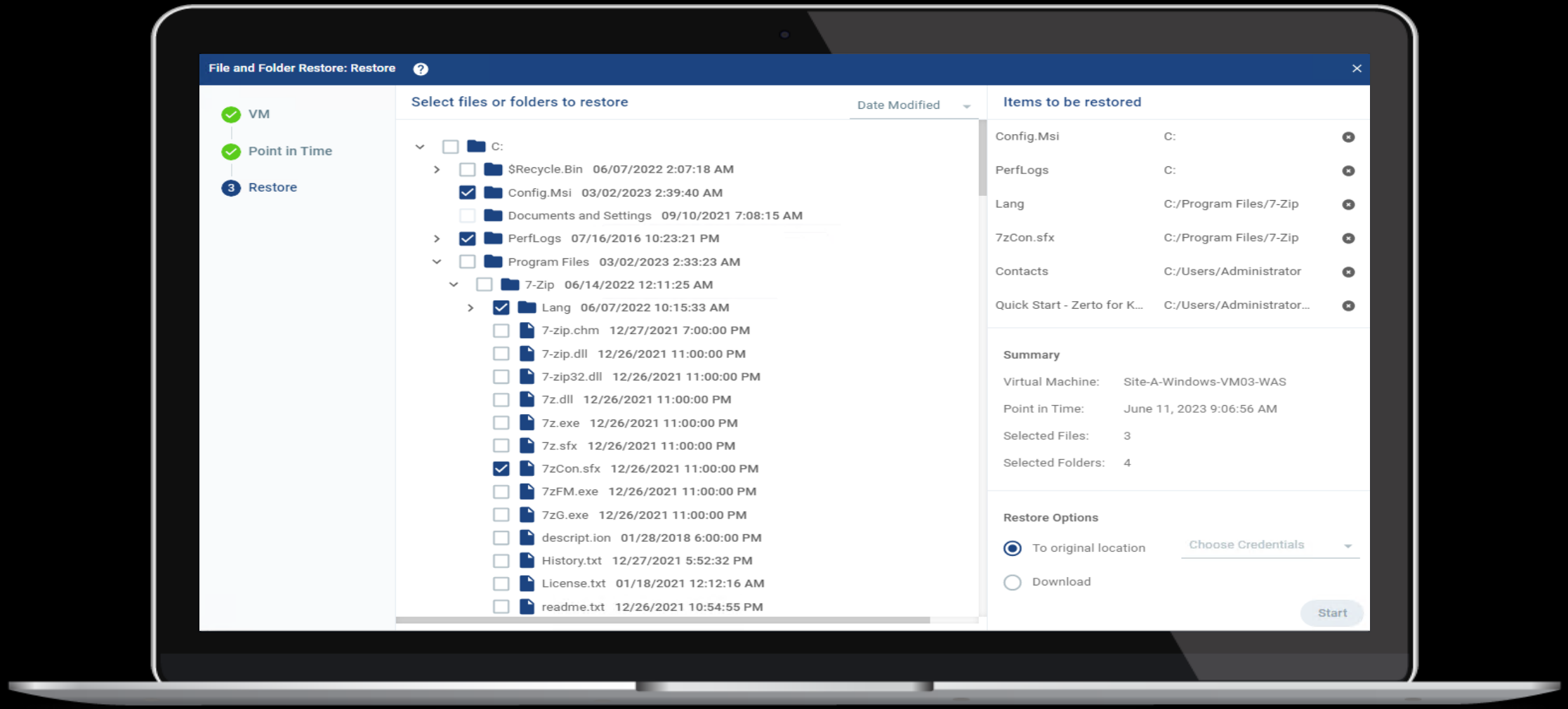


Zerto 혁신적인 P2V 마이그레이션



Zerto

파일 / 폴더 레벨 복구



Hewlett Packard Enterprise

※ Windows 운영체제 및 Linux(EXT) 파일레벨 복구 지원

Zerto 호환성

TARGET

SOURCE	VMware	Hyper-V	Azure	AWS	IBM Cloud	AVS	GVE	OVC
VMware	Z	Z	Z	Z	Z	Z	Z	Z
Hyper-V	Z	Z	Z	Z	Z	Z	Z	Z
Azure	○	○	●	○	○	○	○	○
AWS	○	○	○	●	○	○	○	○
IBM Cloud	Z	Z	Z	Z	Z	Z	Z	Z
AVS	Z	Z	Z	Z	Z	Z	Z	Z
GVE	Z	Z	Z	Z	Z	Z	Z	Z
OVC	Z	Z	Z	Z	Z	Z	Z	Z

○ 마이그레이션

● DR & 마이그레이션

Z DR & 마이그레이션 & 변경불가 설정

AVS: Azure VMware Solution
GVE: Google VMware Engine
OVC: Oracle VMware Cloud

Hewlett Packard Enterprise

Zerto 도입 효과

초고속 랜섬웨어 복구

“ 10분내 복구완료

단 몇 초의 데이터만 손실“

미션 크리티컬 업무보호

“시간 당 10억 발권 업무

서비스와 APP 보호”

복잡한 여러 솔루션 대체

“ DR 솔루션을 4개>1개

150억 비용 절감 "

데이터센터 통합

“ 데이터 센터 21개 > 6개 “

국내 100여개 고객사 Zerto 사용 중

Hewlett Packard Enterprise

Zero RPO

Zero RTO

Zero TRUST

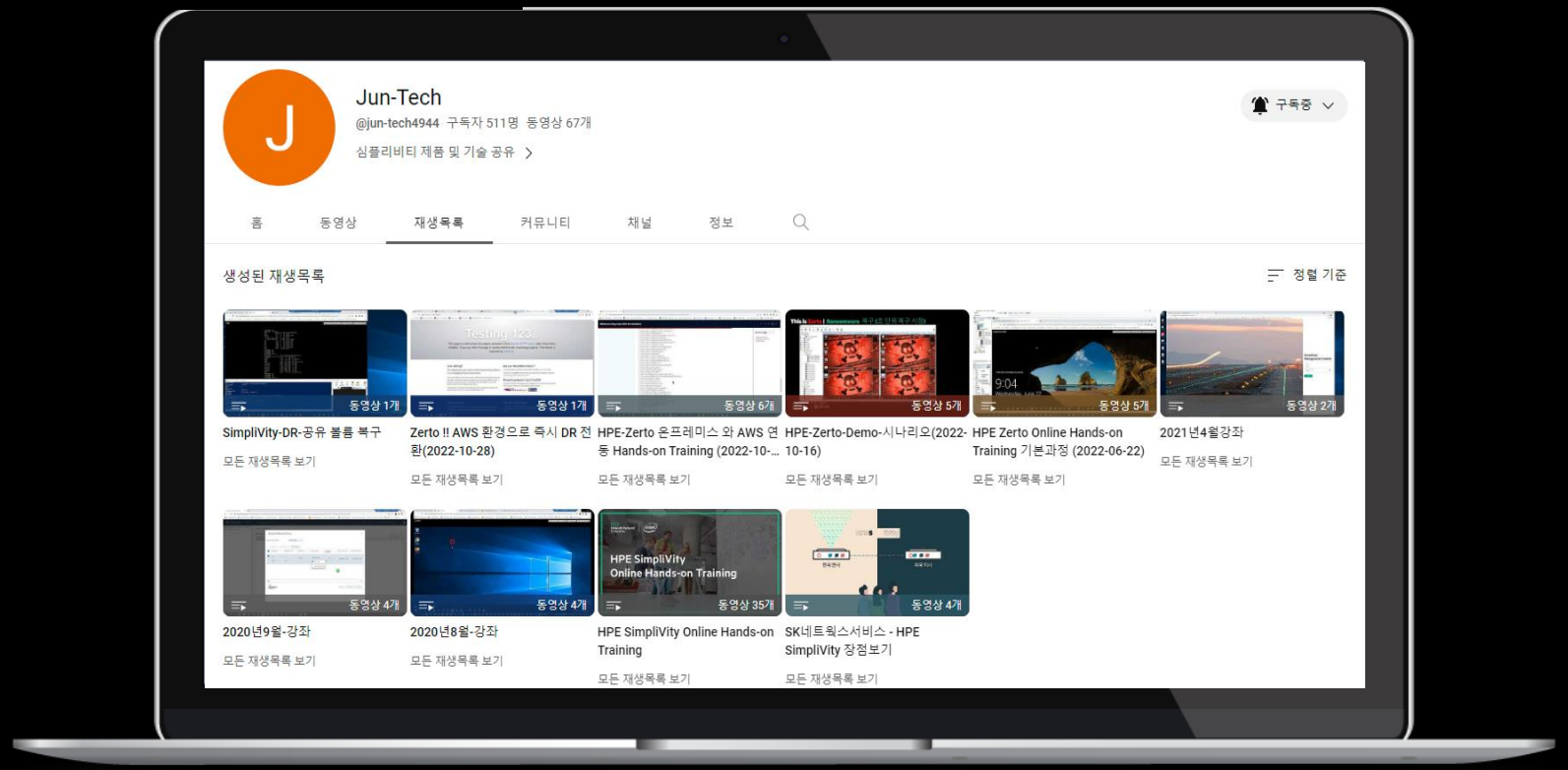
This is the Zerto

Hewlett Packard Enterprise

Zerto Champion

YouTube

Jun-Tech



Hewlett Packard Enterprise

THANK YOU