Hewlett Packard Enterprise

24시간 365일,

지속적인 데이터 보호를 책임져 줄 단 하나의 솔루션

HPE Zerto

일 시 2024년 1월 18일(목), 14:00 ~ 15:00

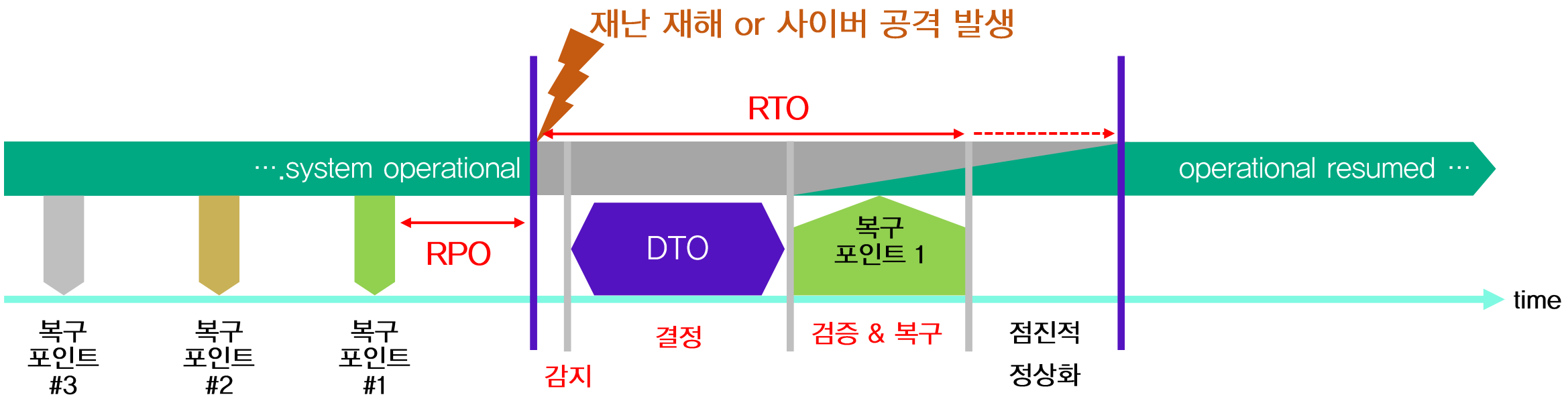
Hewlett Packard Enterprise

24시간 365일,
지속적인 데이터 보호를 책임져 줄 단 하나의 솔루션 HPE Zerto

재해복구 및 사이버 공격 현황

이청영 매니저 I HPE

데이터 보호 핵심 용어



용어	정식 명칭	설명
RPO	Recovery Point Objective	장애로 인해 데이터 Loss 허용 가능한 범위
RTO	Recovery Time Objective	장애로 인해 서비스 Down 허용 가능한 범위
DTO	Decision Time Objective	Failover 또는 복구를 위한 결정에 걸리는 시간

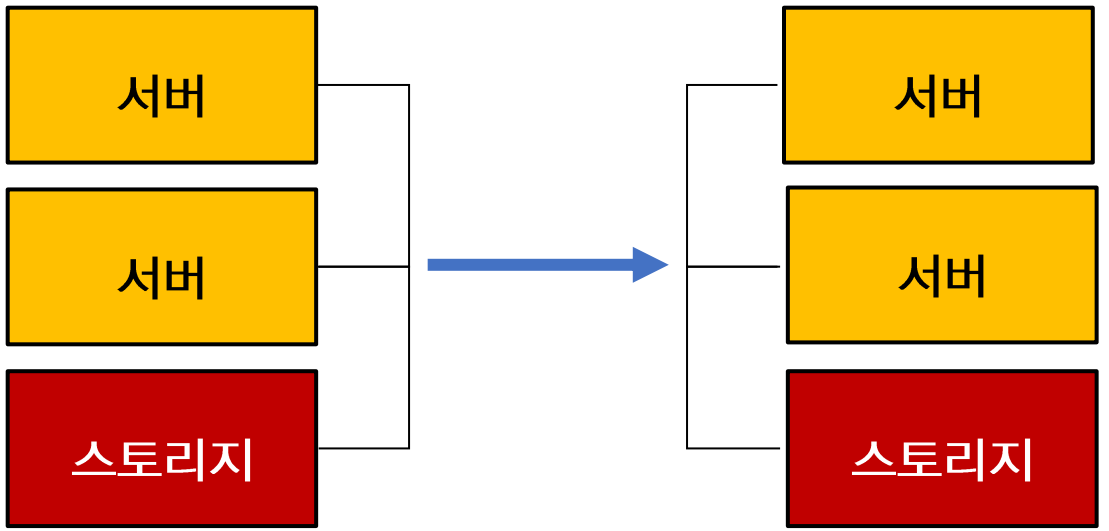
Hewlett Packard
Enterprise

백업 vs 재해복구

백업

- 같은 장소에 데이터를 여러 벌 복사 및 저장 (일/주/월별)
- 적은 비용으로 데이터 복구 가능 (중복제거/압축)
- 재난 또는 데이터 유실 시 **데이터 복구 용도**
- 서비스 불가, 복구에 장시간 소요

DR (재해복구)



- 다른 장소에 데이터 저장 및 최신 1벌만 저장
- 재난 시 **서비스 운영 용도**
- 센터 유지관리 비용 및 초기 투입 비용 많이 필요
- 복구 뿐만 아니라 빠른 서비스 전환이 핵심

Hewlett Packard Enterprise

재해복구 센터 규정

금융감독원 전자금융 감독규정 제23조

- 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)

금융사	보험회사
RTO 〈 3시간	RTO 〈 24시간

[단독]'연간 거래액 2조원' 전자금융업자 재해복구센터 구축 의무화

발행일 : 2023-10-09 13:55 지면 : 2023-10-10 1면

이에 따라 카카오페이, 네이버페이, 토스 등 대형 빅테크와 쿠팡페이, 우아한형제들, 지마켓, SSG닷컴 등 대형 전금업자를 포함 40여곳이 DR센터 의무화 대상에 포함될 전망이다.
금감원에 따르면 지난해 기준 연간 거래금액 2조원을 넘는 35개사 중 DR센터가 없는 곳은 10곳이 넘는다.

이미 DR센터를 구축한 곳들도 의무 대상에 포함됨에 따라 재해복구 전환훈련 등 금융당국 기준에 맞춰 DR센터 운영 및 전자금융사고 대응 프로세스 등 지침을 따라야 한다. 올해 연간 거래액 2조원 돌파를 눈앞에 둔 전금업자들도 있어 의무 대상은 지속 늘어날 전망이다.
페이업, 포트원 등 중견 PG사들이 대표적이다.

출처 : 전자신문

재해복구 모의 훈련 설문 조사

출처 : ConnectWise

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

22% 만 주기적인 모의훈련 성공적 수행

고객의 58% 만 1년에 한번 이상 수행

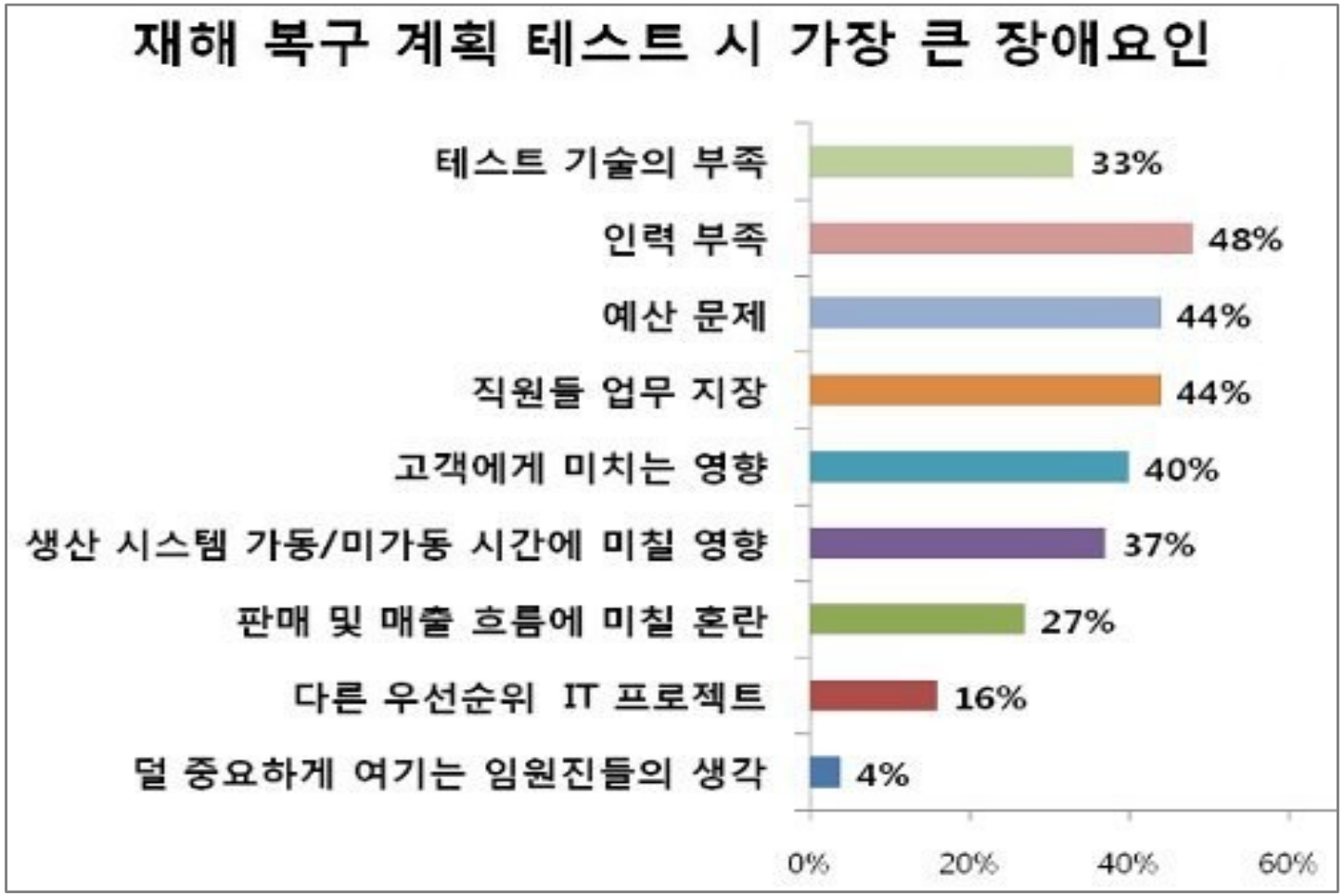
Hewlett Packard Enterprise

재해복구 모의 훈련 필요 사항

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				

Hewlett Packard Enterprise

재해복구 모의 훈련 어려움



출처 : 데이터넷

Hewlett Packard Enterprise

급증하는 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 전 방위로 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

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

출처 : 한국경제

"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

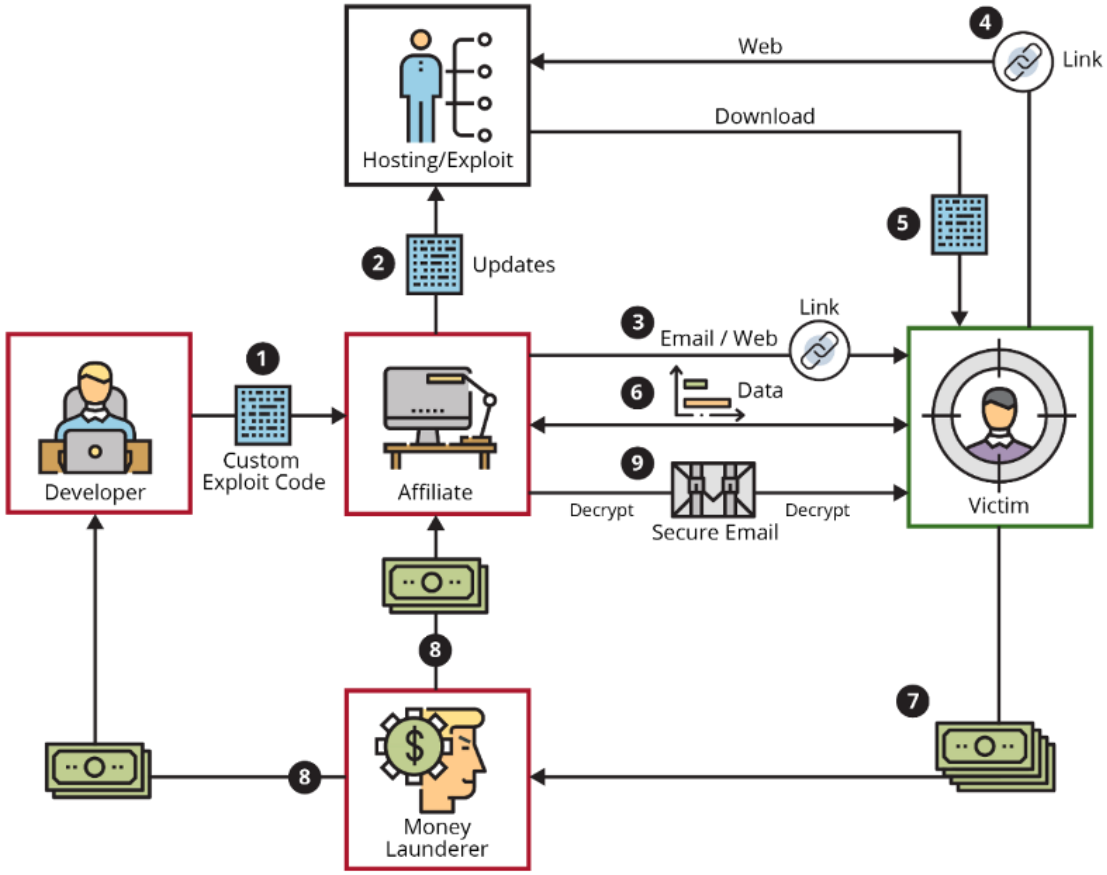
1분기 가장 많이 발견된 랜섬웨어는 '락빗'(290건)으로 조사됐으며 △클롭(110건) △블랙캣(90건) △로열(72건) △비안리안(51건) 등이 뒤를 따랐다.

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

출처 : 서울파이낸스

Hewlett Packard Enterprise

랜섬웨어 급증 원인 Ransomware as a Service & 암호화폐



출처 : 카네기 멜론 대학교 소프트웨어 공학 연구소

Hewlett Packard
Enterprise

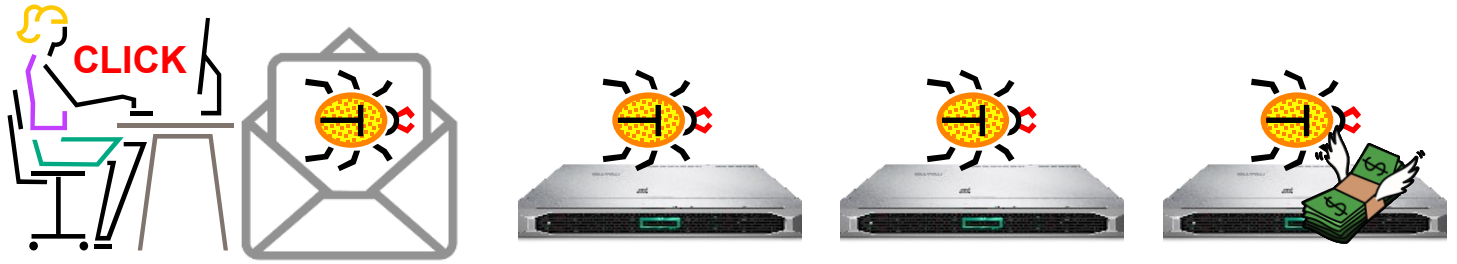
랜섬웨어 피해 양상

전세계 2023년 랜섬웨어 피해액 한화 40조원

73% 의 기업/조직이 랜섬웨어 공격으로 인해 피해

38% 기업/조직이 재 공격 당함 - 예방접종 효과 無

40% 기업/조직이 공격으로 인해 직원을 해고



Hewlett Packard Enterprise

사이버 보험의 출현

지원 내용	• 법적 비용, 시스템 중단으로 인한 피해 보상, 몸값지불, 복구 전문가 및 비용 • 해커 전문 협상가 비용, 과징금, 기업 이미지 회복 비용
미 지원 내용	• 내부자 공격, 내부 오류 (네트워크 오류 등) • 알려진 취약점/결함이 있는 상태에서의 공격
역효과	• 오히려 사이버 보험에 가입한 고객을 집중 타겟으로 공격 • 보험 보장 최대 금액을 요구
현황	• 급증하는 랜섬웨어로 보험료 상승 • 기준이나 표준이 없어 보험사들도 제대로 대처하지 못함 • 까다로운 가입 기준 (인증, 암호화, Zero-trust 미구축 기업 거절)


최후의 보루
Cyber Vault
최신 데이터 보호 기법
격리 Isolated 환경에 변경 불가 Immutable 복제본을 유지
최악의 상황에서도 데이터 복구

정보 보호는 이제 3D 업종

Gartner :

"By 2025 nearly half of cybersecurity leaders will change jobs,
25% for different roles entirely due to multiple work-related stressors."

- Gartner: *Top Cybersecurity predictions 2023-2024* (released Sep 8th, 2023): Link

~25년 사이버보안 부서장 절반이 이직 또는 25% 전직

Hewlett Packard Enterprise

Hewlett Packard Enterprise

24시간 365일,
지속적인 데이터 보호를 책임져 줄 단 하나의 솔루션 HPE Zerto

재해복구 및 랜섬웨어 복구 최적 솔루션
HPE Zerto 젤토

김흥준 매니저 | HPE

젤토-제품 철학

RPO DTO RTO

Zerto = Zero to Ø

데이터 용량에 상관없이 5초 전으로 1분 내에 복구

2009년도 설립

80개국 9500개 고객사, 450 개 MSP

국내 150여개 고객사

Hewlett Packard Enterprise

1개 라이선스로 3가지 솔루션

Zerto

DR

BACKUP

MIGRATION

Hewlett Packard
Enterprise

혁신적인 차세대 데이터 보호 플랫폼

DR	5 초전으로 1 분내 복구	용량에 상관없이
BACKUP	5 초전으로 1 분내 복구	용량에 상관없이
MIGRATION	가상화 클라우드	크로스 플랫폼

Hewlett Packard
Enterprise

100% Software Only 종속성 없는 자유로움

Any Server

Any Storage

Any Cloud

Hewlett Packard
Enterprise

차세대 데이터보호 플랫폼

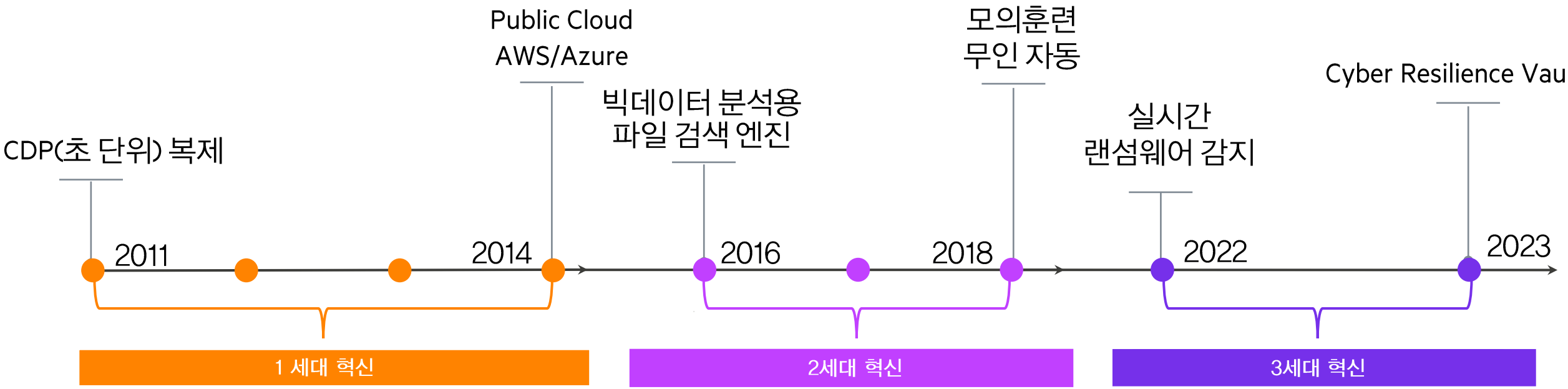
DR

BACKUP

MIGRATION

Hewlett Packard
Enterprise

15년간 축적 된 경험과 노하우, 검증 된 솔루션



유럽 최대 제조기업

1,200 VMs
5 Sec RPO

포춘 10대 기업

1,200 VMs
9 sec RPO

UNITED AIRLINES

4,000 VMs
8 sec RPO

American Airlines

7,200 VMs
7 Sec RPO

Solera

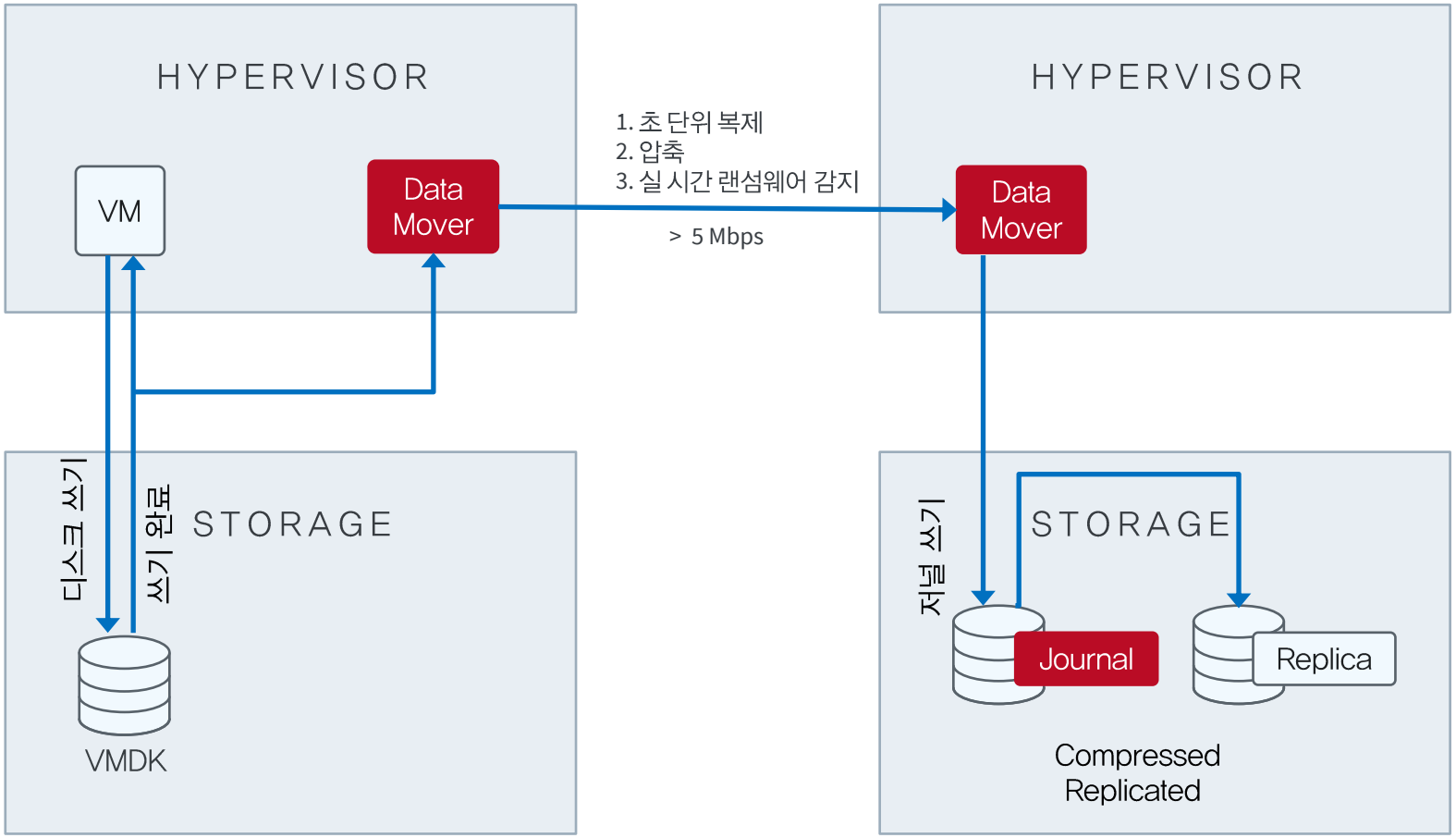
20,000 VMs
10 sec RPO

Hewlett Packard Enterprise

차세대 혁신 기술 - In memory 복제엔진 탑재

In-Memory CDP

1. RPO 5초, RTO 1 분내
2. 운영 시스템 영향 없음
3. 회선 비용절감



Hewlett Packard Enterprise

초 단위 복구시점 제공

Daily Backups

Data GAP = 24 hours

일 단위

0 6 12 24

Snapshot-Based DR

Data GAP = hours

시간 단위

0 6 12

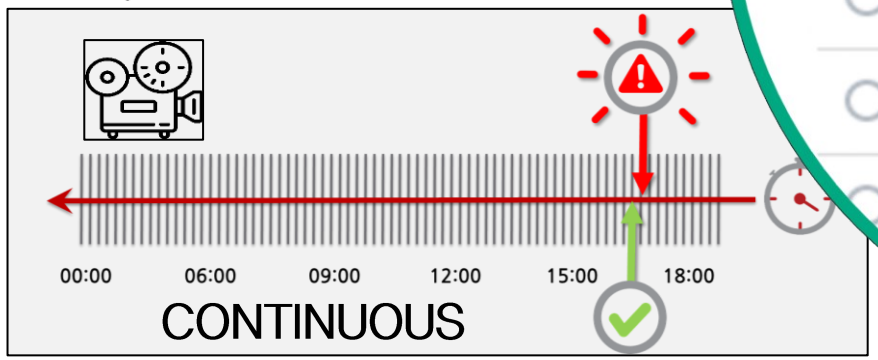
HPE Zerto

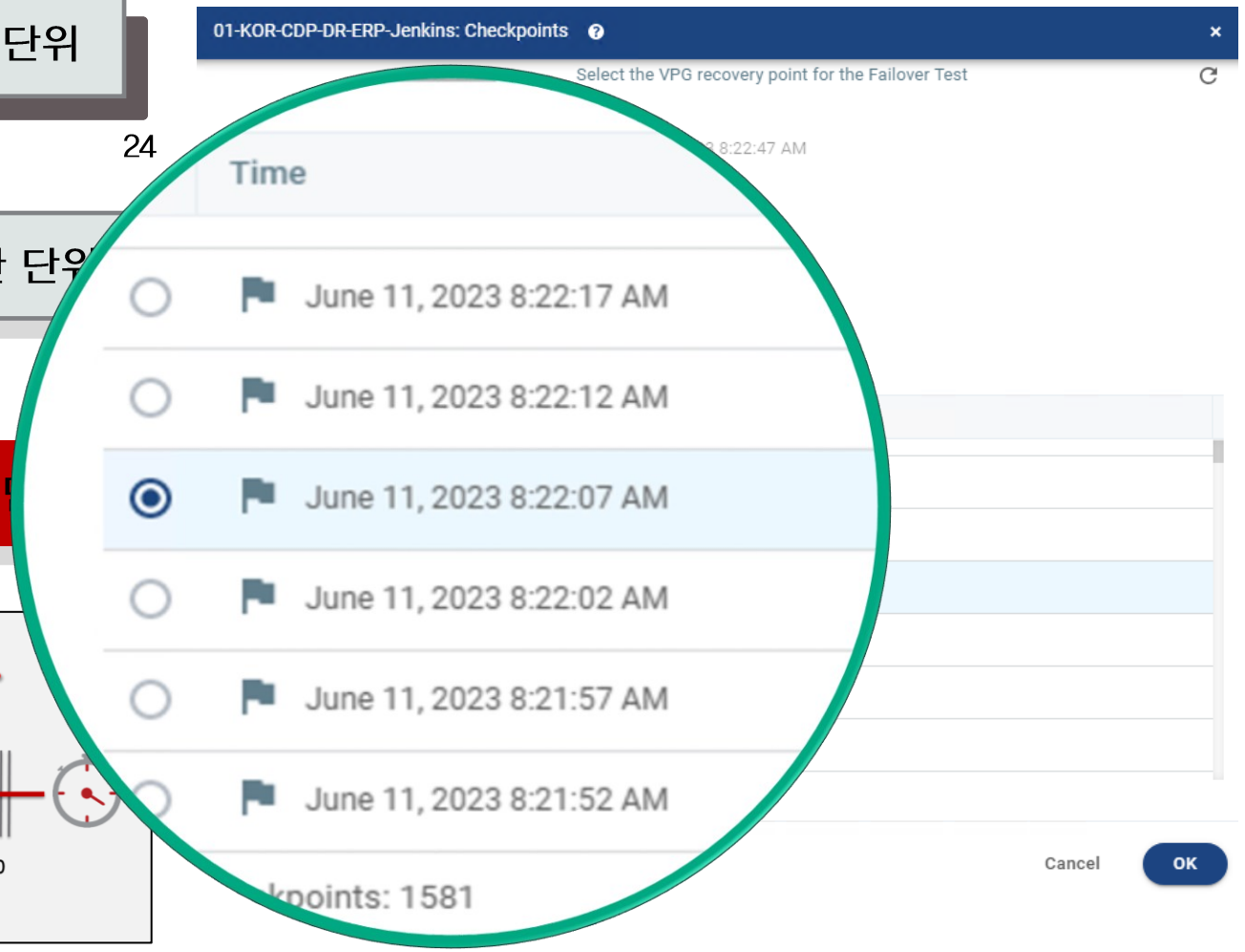
Data GAP = Seconds

초 단위

0 6 12

*CDP 복제





* CDP : Continuous Data Protection

Hewlett Packard Enterprise

업무에 영향 없는 무 중단 실전 모의훈련

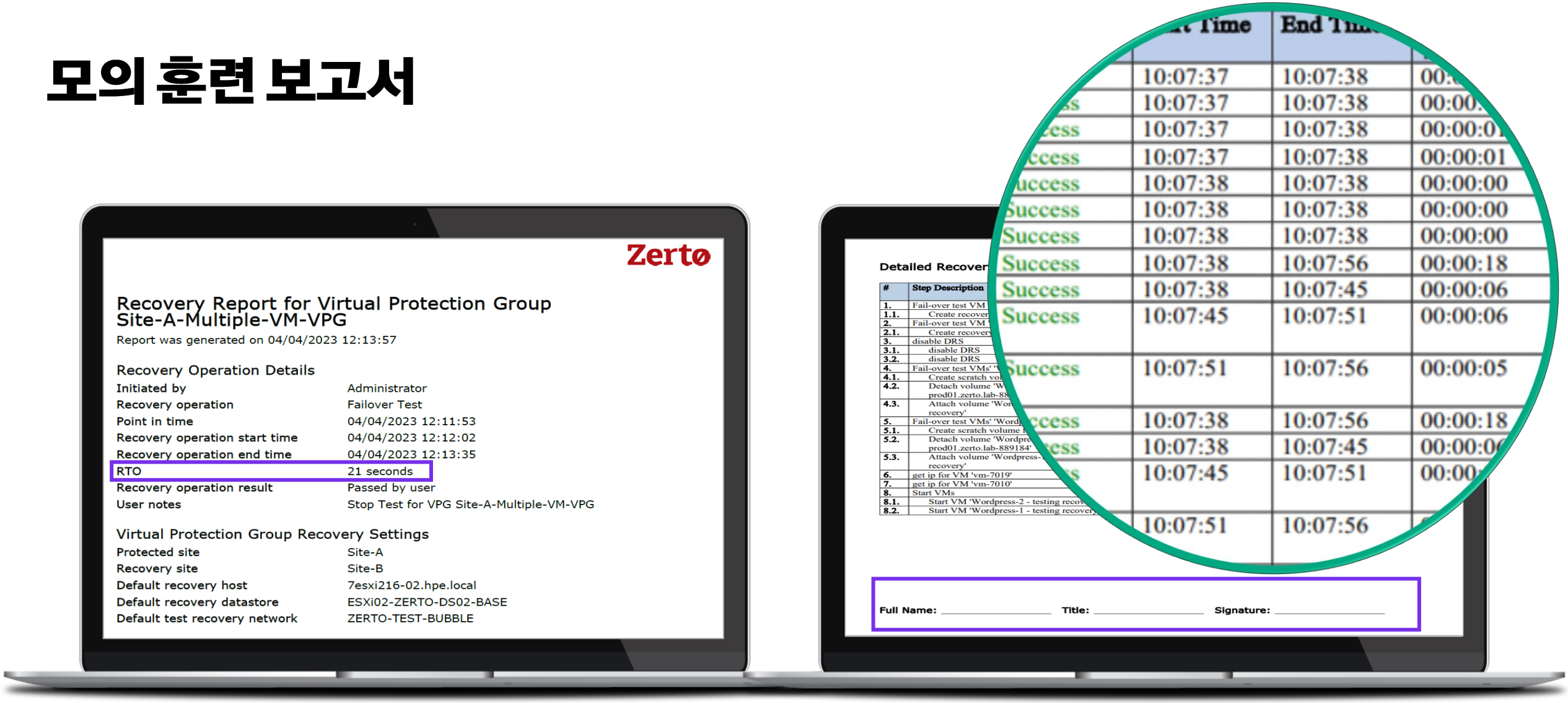
주 센터 영향 無	완벽한 DR 검증	정확한 시간 예측	결과 보고서 생성
			

Hewlett Packard
Enterprise

‘One Click’ 모의훈련 수행

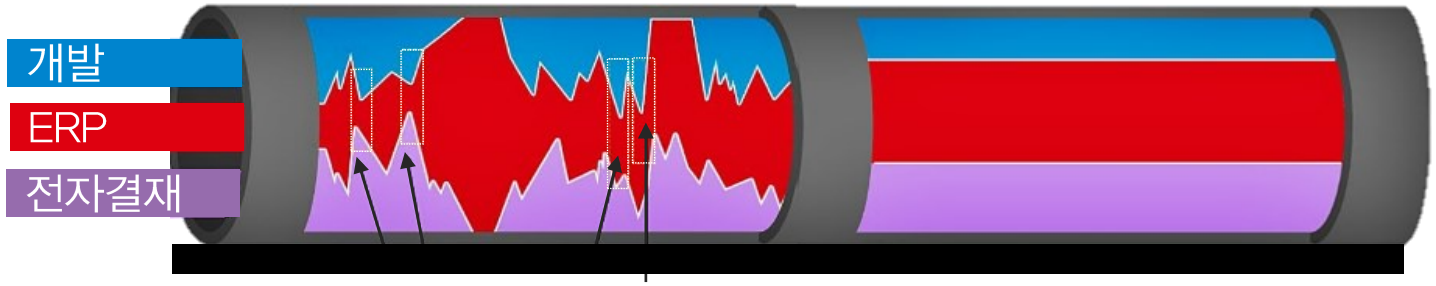
Hewlett Packard Enterprise

모의 훈련 보고서



Hewlett Packard Enterprise

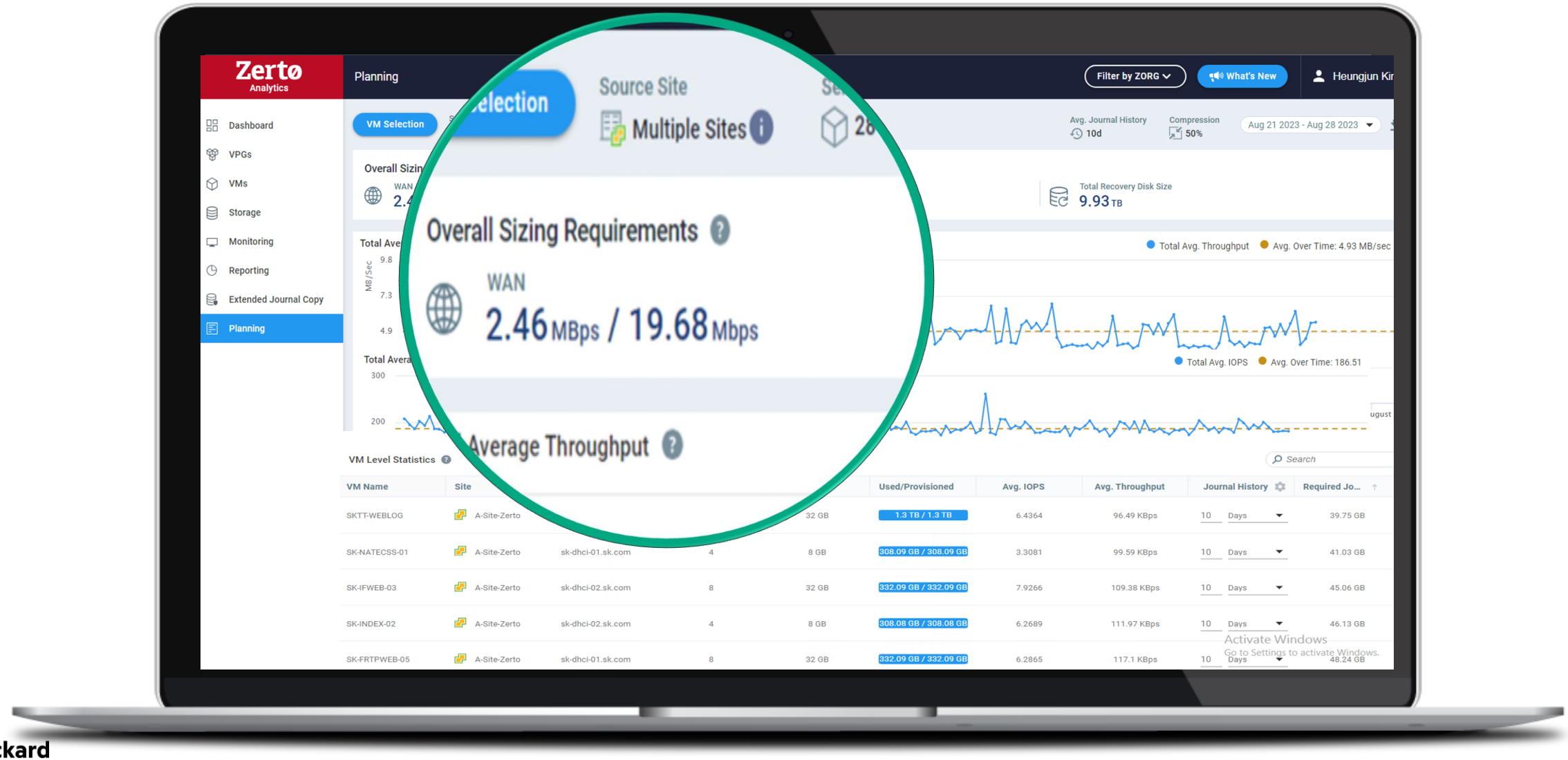
비용 효율성과 최적화를 위한 데이터 전송 기술



데이터 압축	우선 순위 설정	회선 대역폭 QoS	Self Healing

Hewlett Packard Enterprise

자동으로 회선 용량 산정



Hewlett Packard Enterprise

데이터 정합성 - VPG 업무 별 일관된 복구시점 제공

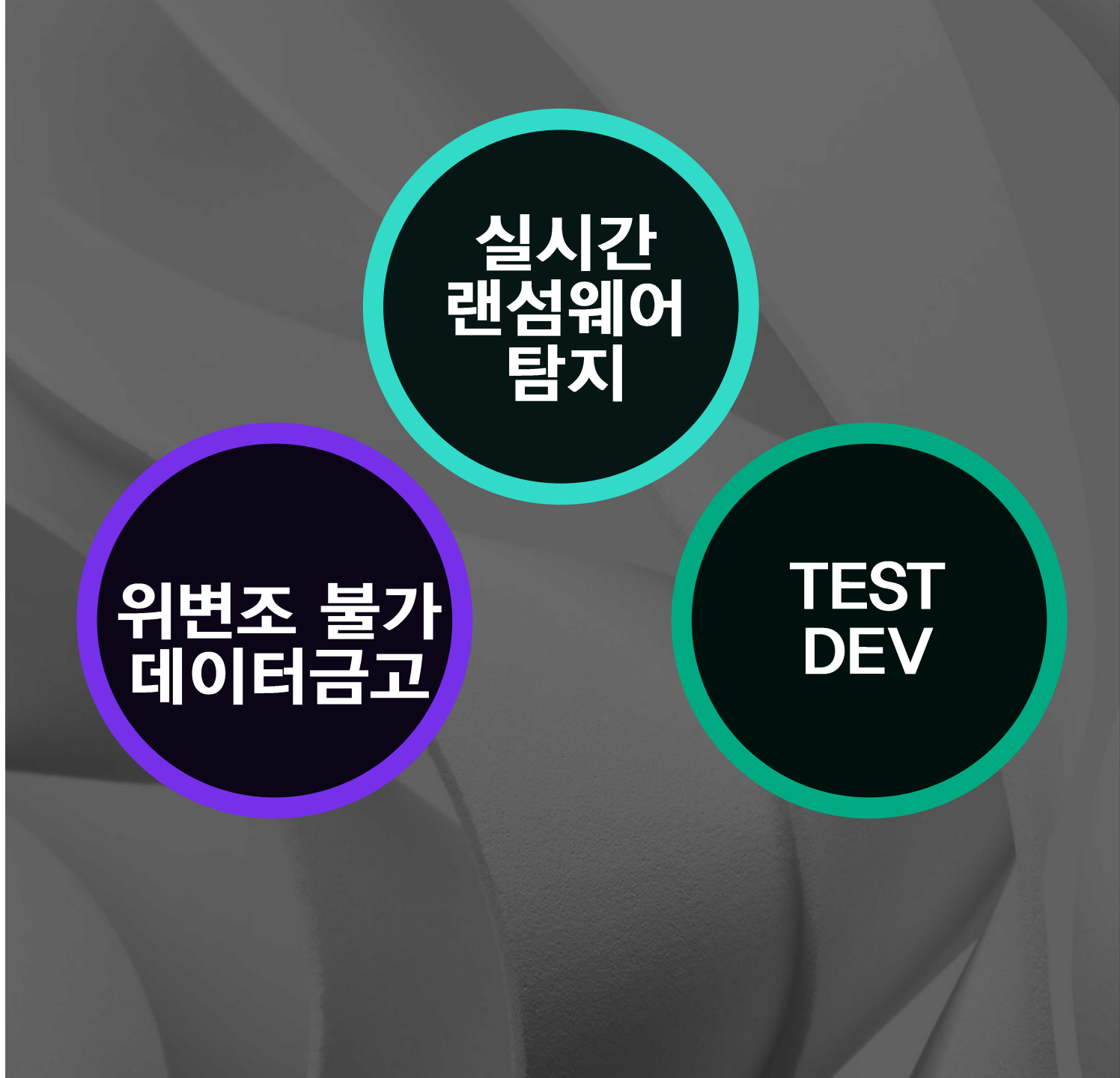
Hewlett Packard Enterprise

차세대 데이터보호 플랫폼

DR

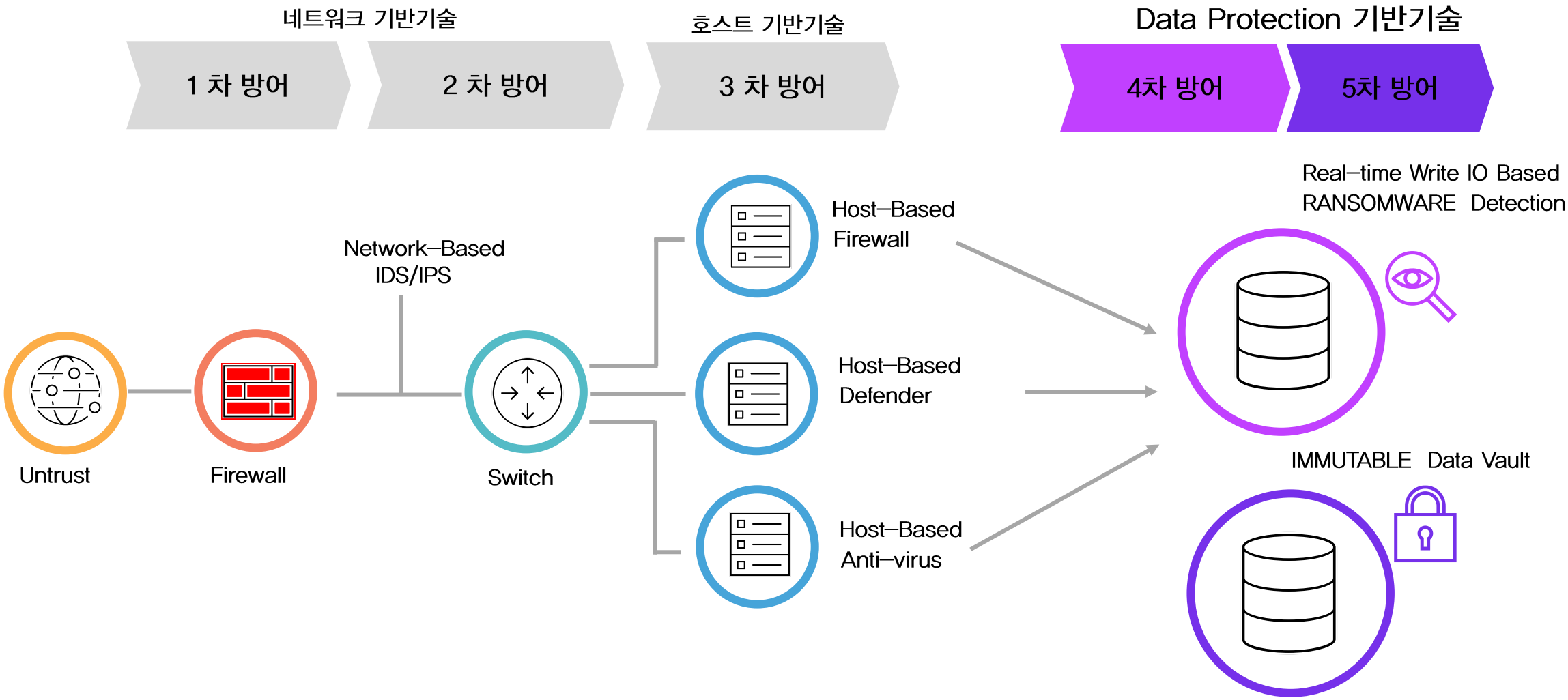
BACKUP

MIGRATION



Hewlett Packard
Enterprise

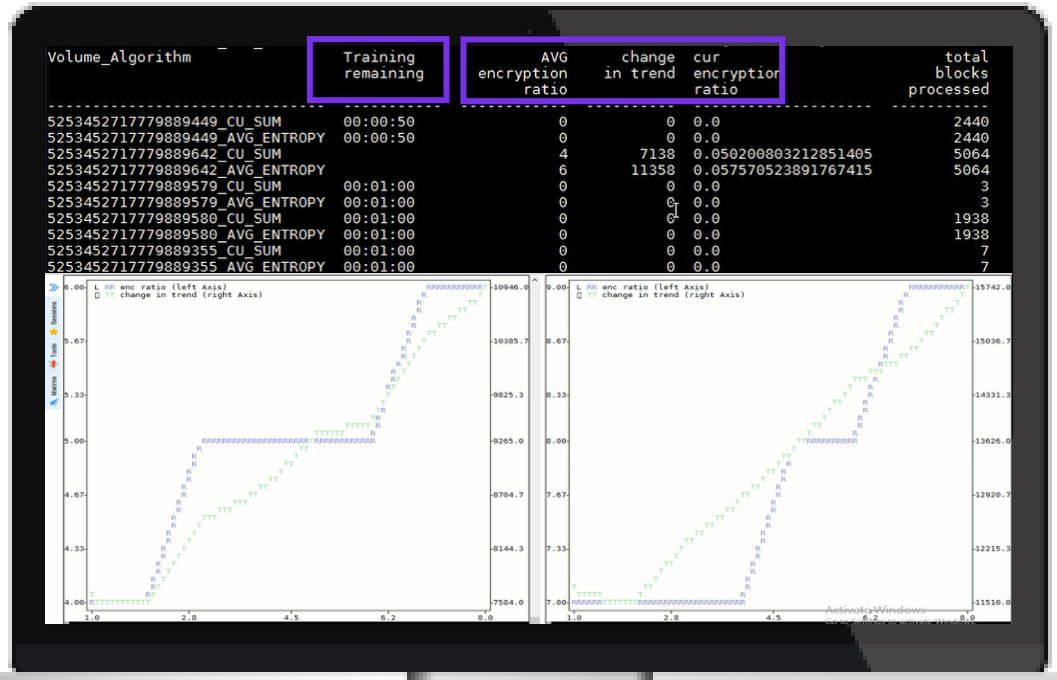
Data Protection 기반의 랜섬웨어 대응



Hewlett Packard
Enterprise

Machine Learning 기반 랜섬웨어 실시간 탐지

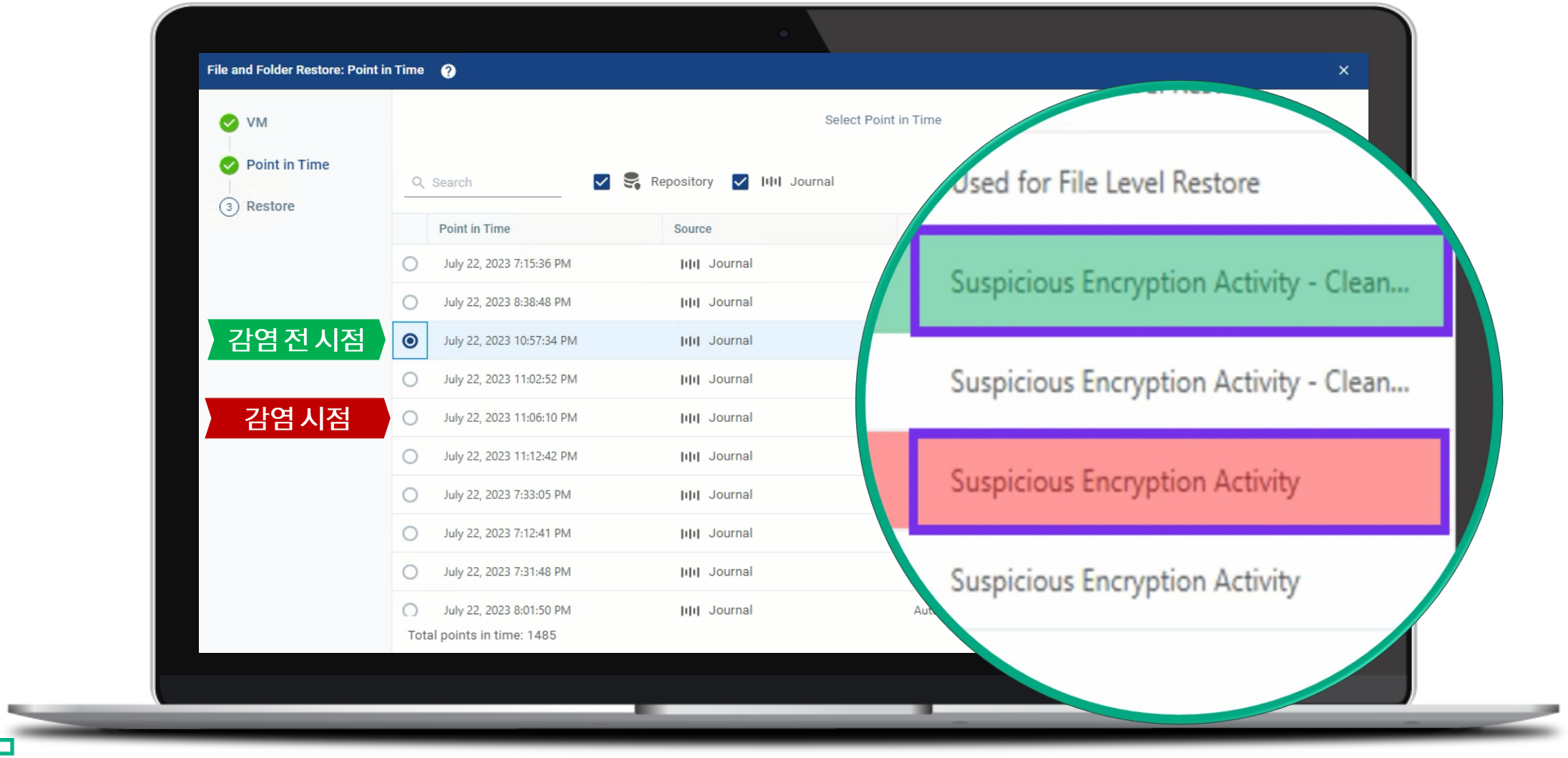
Fine Tune, Machine Learning 탑재



다양한 모니터링 Tool 연계

Hewlett Packard Enterprise

감염 전 깨끗한 시점으로 즉시 복구



Hewlett Packard Enterprise

랜섬웨어 감지- 특장점/ 기술 비교

1 세대 기술

리소스 변화량만 측정 – 매우 낮은 탐지율
- 백업/스냅샷 변경량
- 데이터 압축률 변경
- CPU 사용량

2 세대 기술

고정형 엔트로피 Detection
- 최신 지능화 된 랜섬웨어 탐지 불가
- Standard Shannon entropy detection
- 고정 된(256) 랜덤 임계값 대비 엔트로피 증가를 측정하는 방식
- 일부 데이터만 샘플링 하여 탐지

3 세대 신 기술

Data–Adaptive Detection (Zerto 특허출원)
가변형 엔트로피 Detection
트리거 임계값을 동적으로 실시간 처리
Machine Learning 기반의 IO 패턴 분석

Dynamic calculation of thresholds.

This is one of the key and unique aspects of the HPE approach. You see, the *typical* way for detecting encryption is entropy calculations and comparing to a fixed threshold of randomness.

There are several challenges that massively complicate having a fixed detection threshold:

- Different data types
- Whether the data is compressed already or not
- Insidious tricks like encoding data using base64 make encrypted data seem like it has *less* entropy (converts binary to text), which breaks fixed threshold detection systems.

The entropy equation is this (there's no test later, relax, we will focus on just one thing here):

$$H(X) = -\sum_{i=1}^{n} P(x_i) * \log_2 P(x_i)$$

The big thing we do is that we dynamically calculate the "n" above, **which is not done by other vendors (they assume a fixed, high value, for instance 256 for a byte, since that's the total number of all possible values using 8 bits).** The "n" just means the cardinality of the data "alphabet", which would naturally be different if the data was plain text, compressed text, normal binaries, etc.

This is a huge deal, since it enables us to dynamically adjust detection thresholds based on different types of data. For instance, if the cardinality turns out to be that of normal text, we will accordingly lower

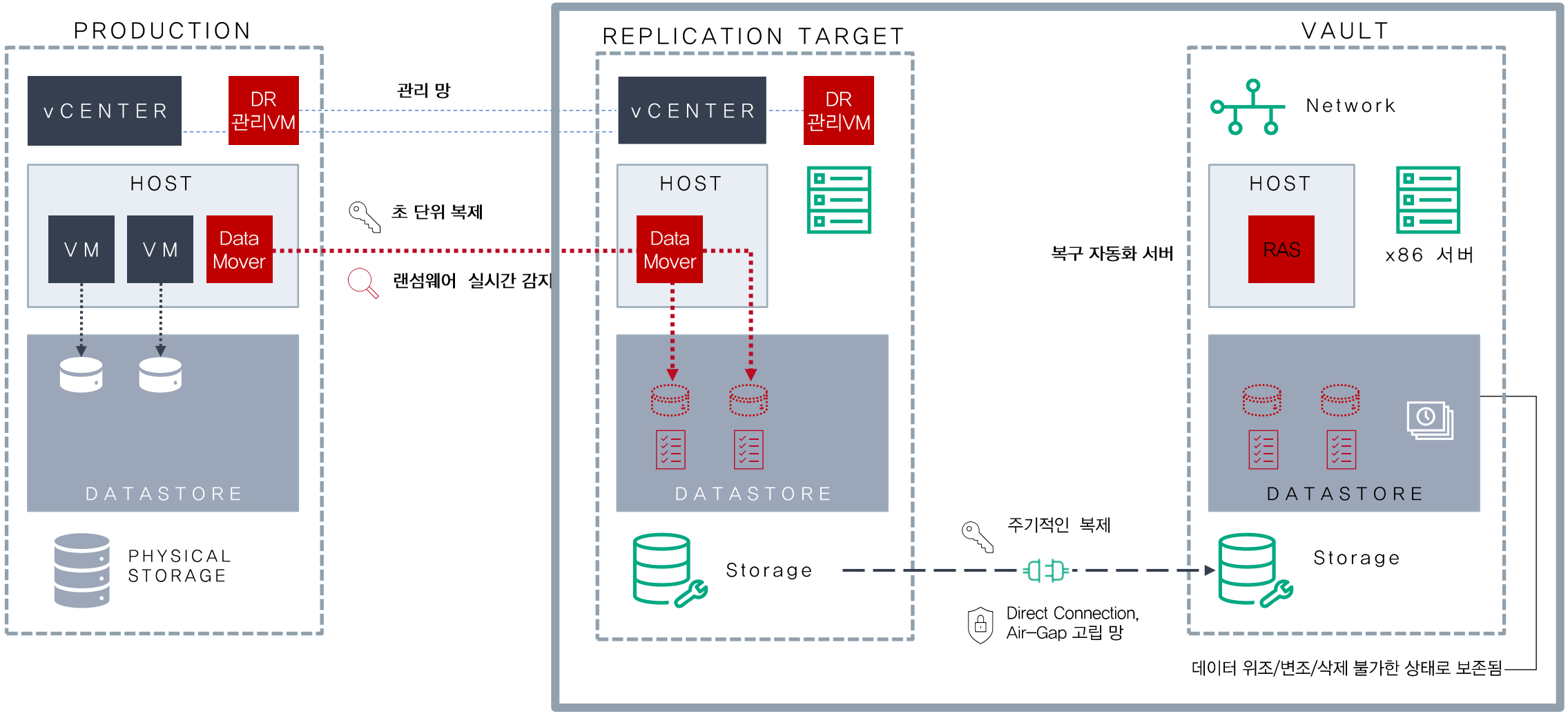
3세대 기술 기대 효과

- 파일의 일부분만 암호화 할 경우도 탐지
- Base64 encoding 교묘한 공격에도 효과적
- 정상적인 암호화와 랜섬웨어 암호화 비교
- 다양한 유형의 데이터 암호화 감지
- 정확도와 신뢰성 확보
- No Agent, No Internet , No more Cost
- 샘플 당 1~2 µs 고성능 처리

Hewlett Packard Enterprise

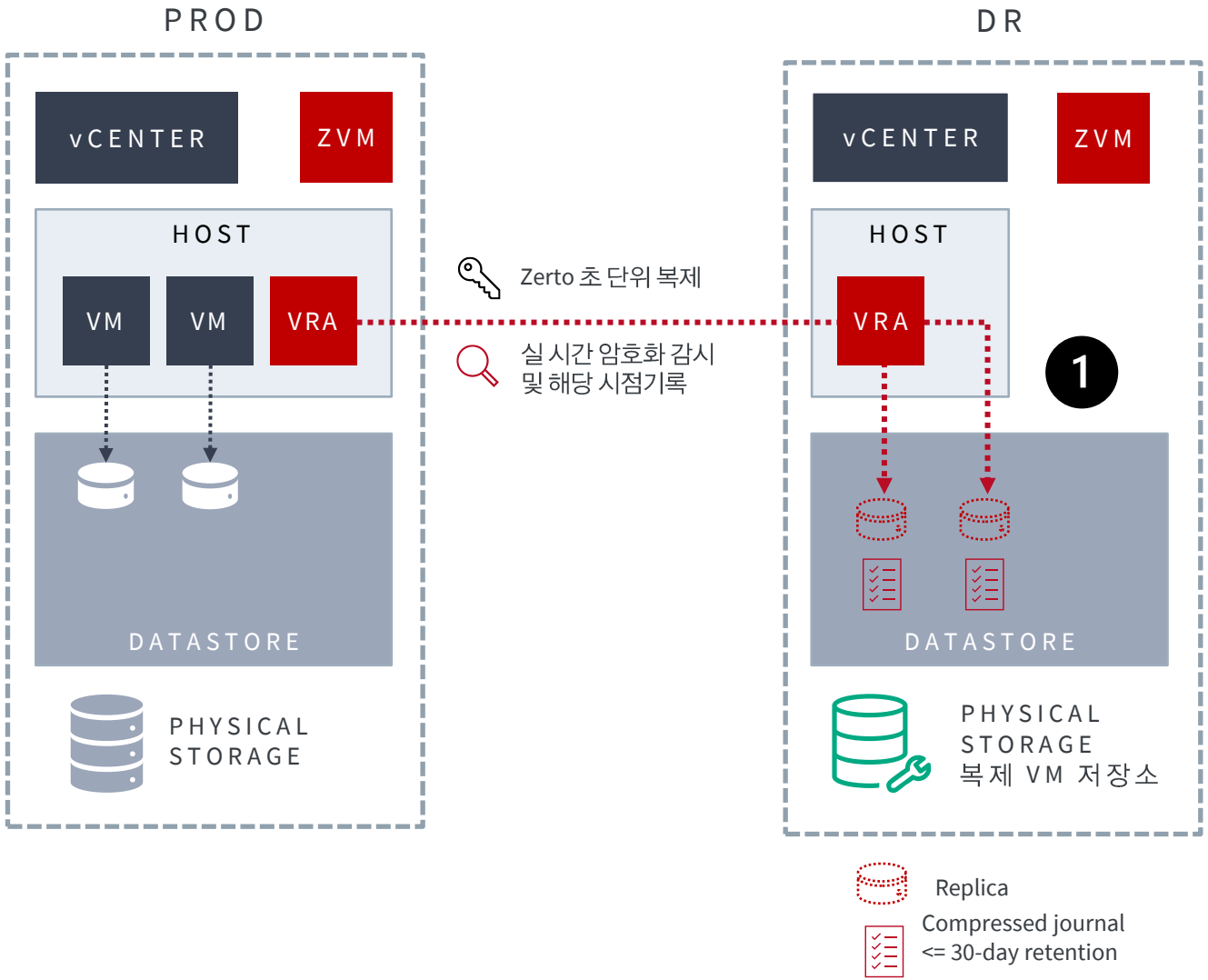

최후의 보루
Cyber Vault
최신 데이터 보호 기법
격리 Isolated 환경에 변경 불가 Immutable 복제본을 유지
최악의 상황에서도 데이터 복구

랜섬웨어 완벽차단 - 데이터금고 (Cyber Resilience Vault)



Hewlett Packard Enterprise

다양한 Data Protection 구성안 #1



DR 초 단위 복제

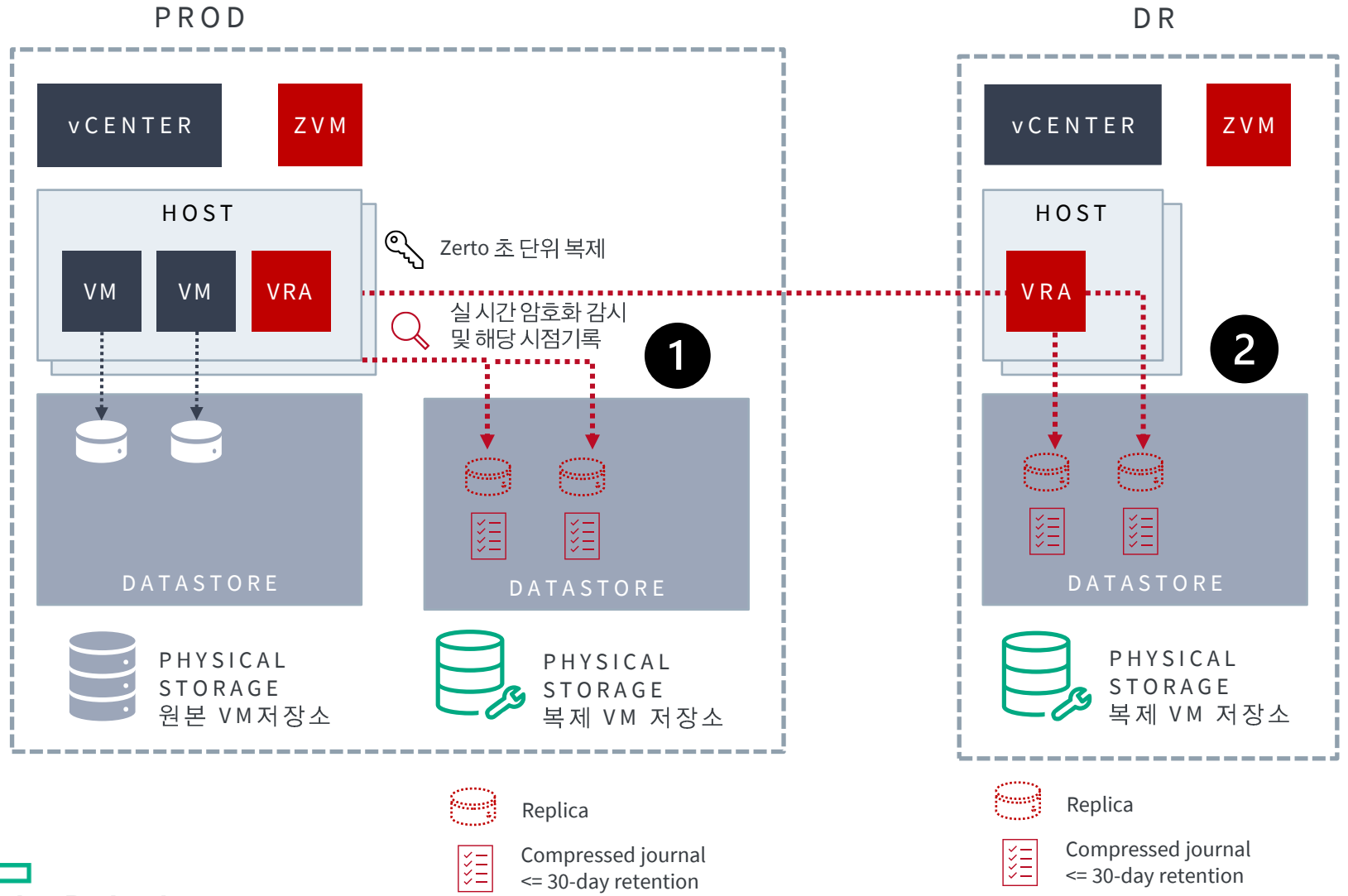
1. 로컬 데이터 센터 전체 장애 시, DR 센터에서 서비스 기동

2. 개별 VM 장애 시, DR 에서 복구 후 다시 Failback 구성.

3. 개별 VM 파일 장애 시, DR 에서 로컬로 파일 복구

Hewlett Packard Enterprise

다양한 Data Protection 구성안 #2



1차 보호- 로컬 초 단위 백업

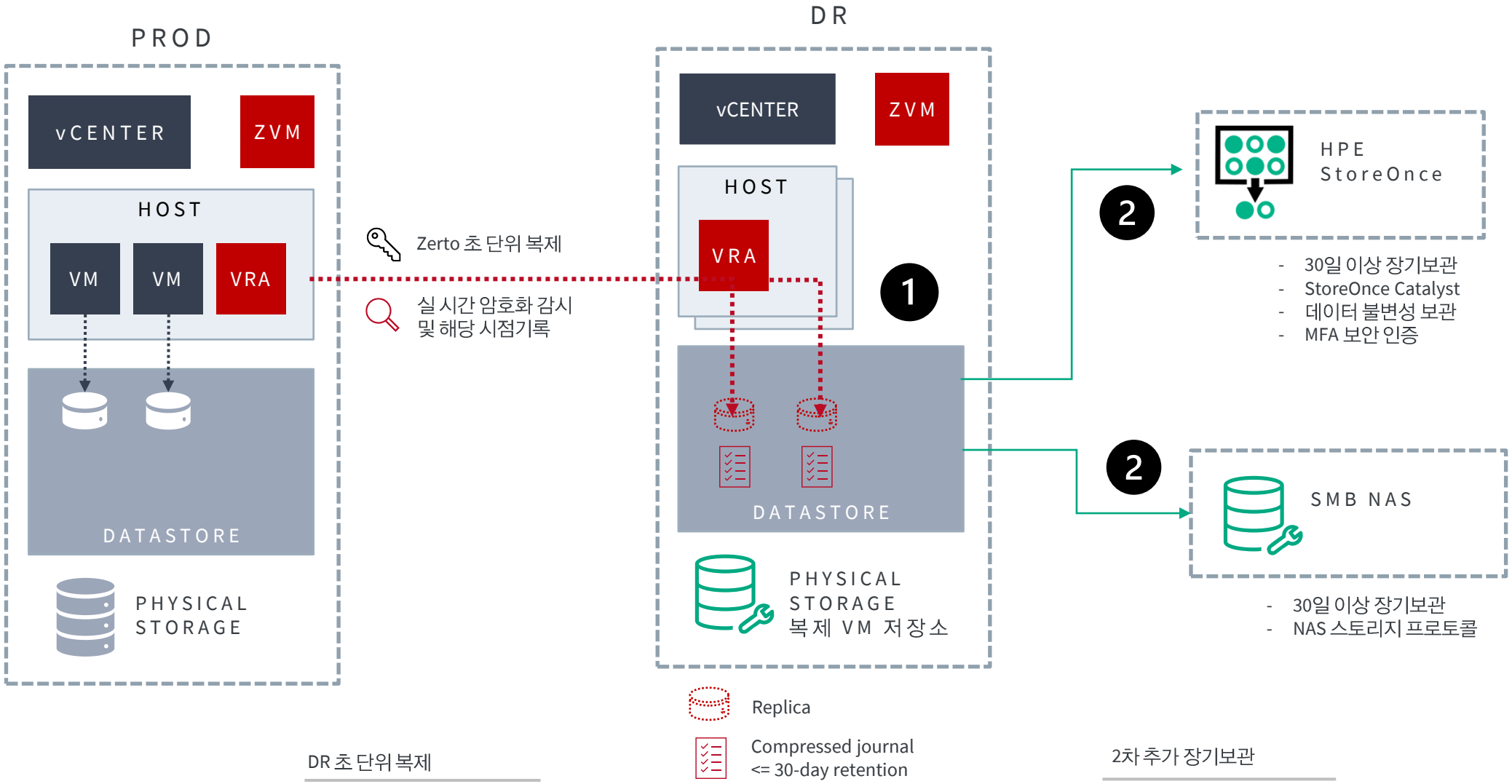
로컬 데이터 센터에서 발생 한 개별 VM 장애 발생 시, 로컬에서 즉시 복구

2차 보호- DR 초 단위 복제

로컬 데이터 센터 전체 장애 시, DR 센터에서 서비스 기동

Hewlett Packard Enterprise

다양한 Data Protection 구성안 #3



DR 초 단위 복제

로컬 데이터 센터 전체 장애 시
DR 센터에서서비스 기동

2차 추가 장기보관

장기보관 데이터 필요 시 구성

도입 효과 - RPO 향상

Before Zerto

10 HOURS

After Zerto

< 10 SECONDS

Hewlett Packard
Enterprise

도입 효과 - RTO 향상

Before Zerto

2 WEEKS

After Zerto

< 10 MINUTES

Hewlett Packard Enterprise

도입 효과 - 모의훈련

Before Zerto		After Zerto
NO TEST		< 20 MINUTES
6 명 운영자		1 명 운영자
23 명 운영자		6 명 운영자

Hewlett Packard Enterprise

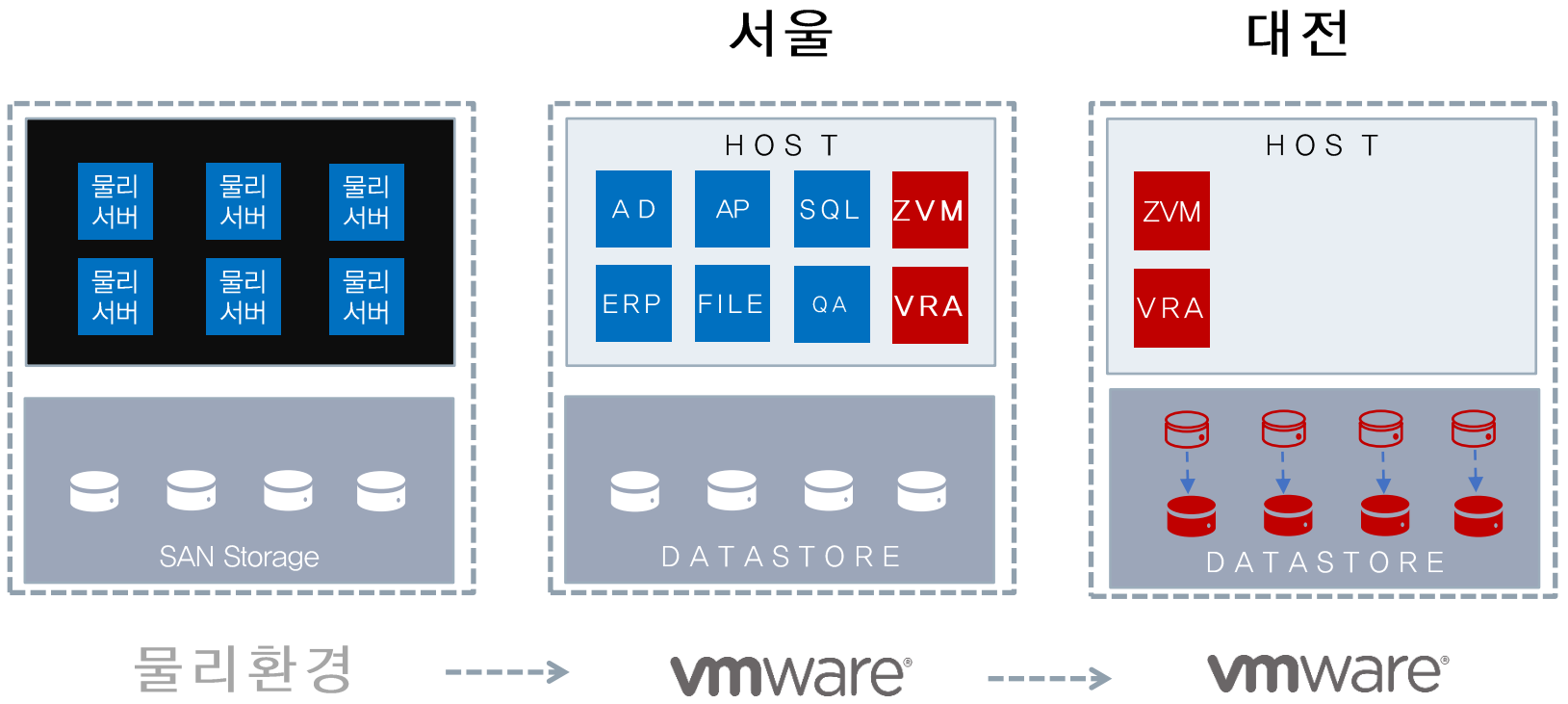
A 국내 대표 사례

ERP 업무

8 Sec

100 Mbps

P2V + DR



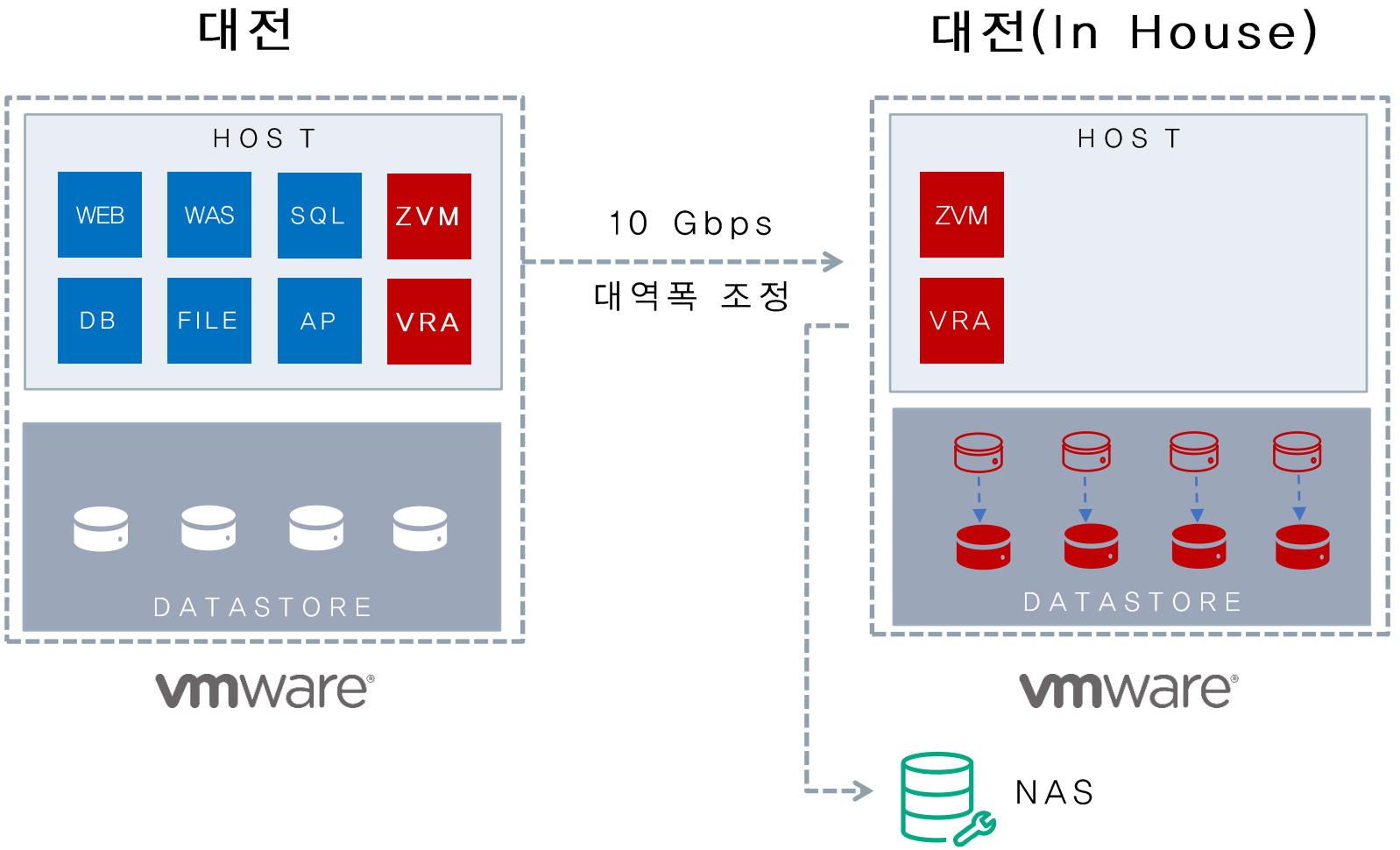
B 국내 대표 사례

내부 포탈 업무

7 Sec

1 Gbps

DR + 장기보관

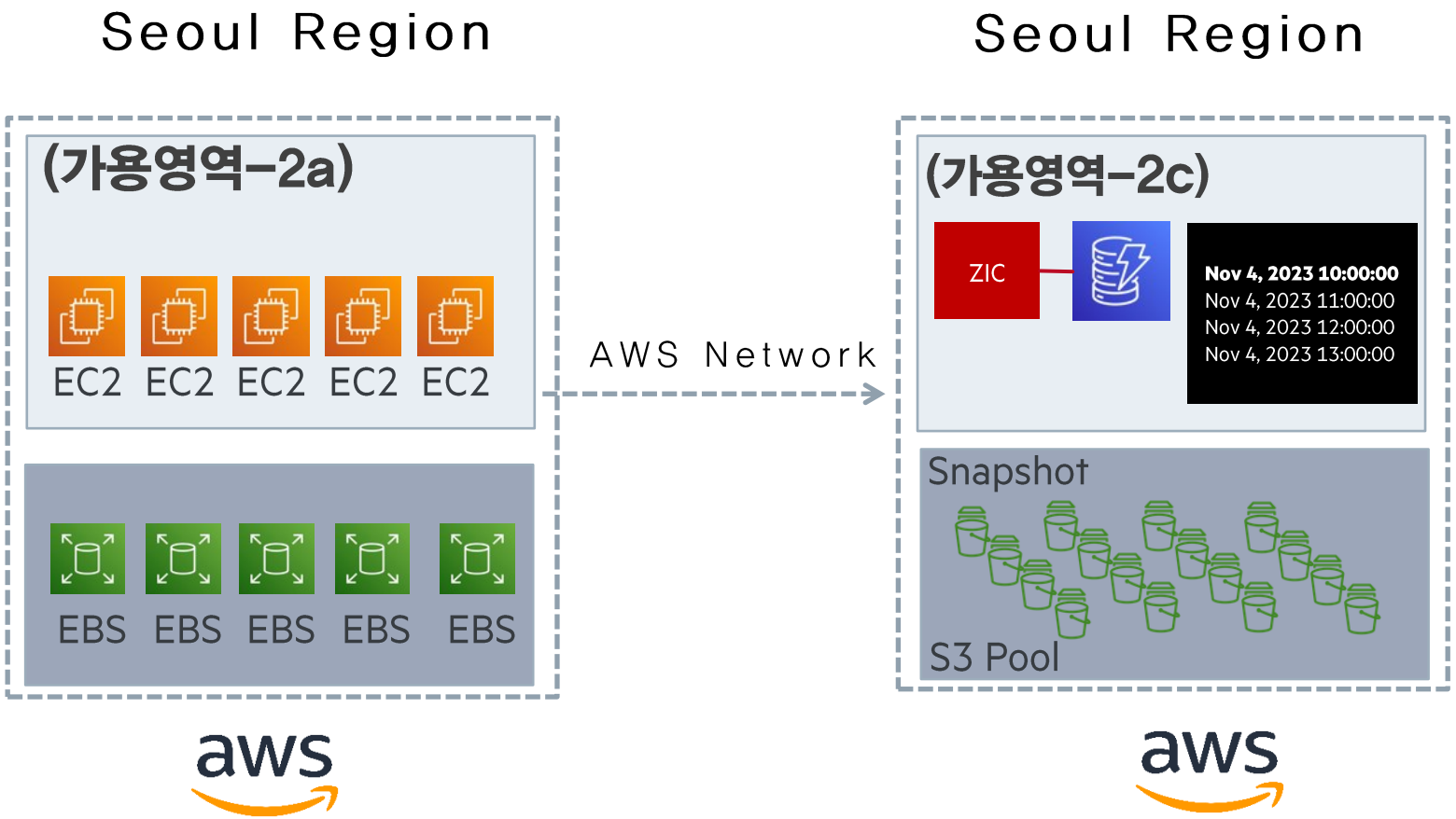


C 국내 대표 사례

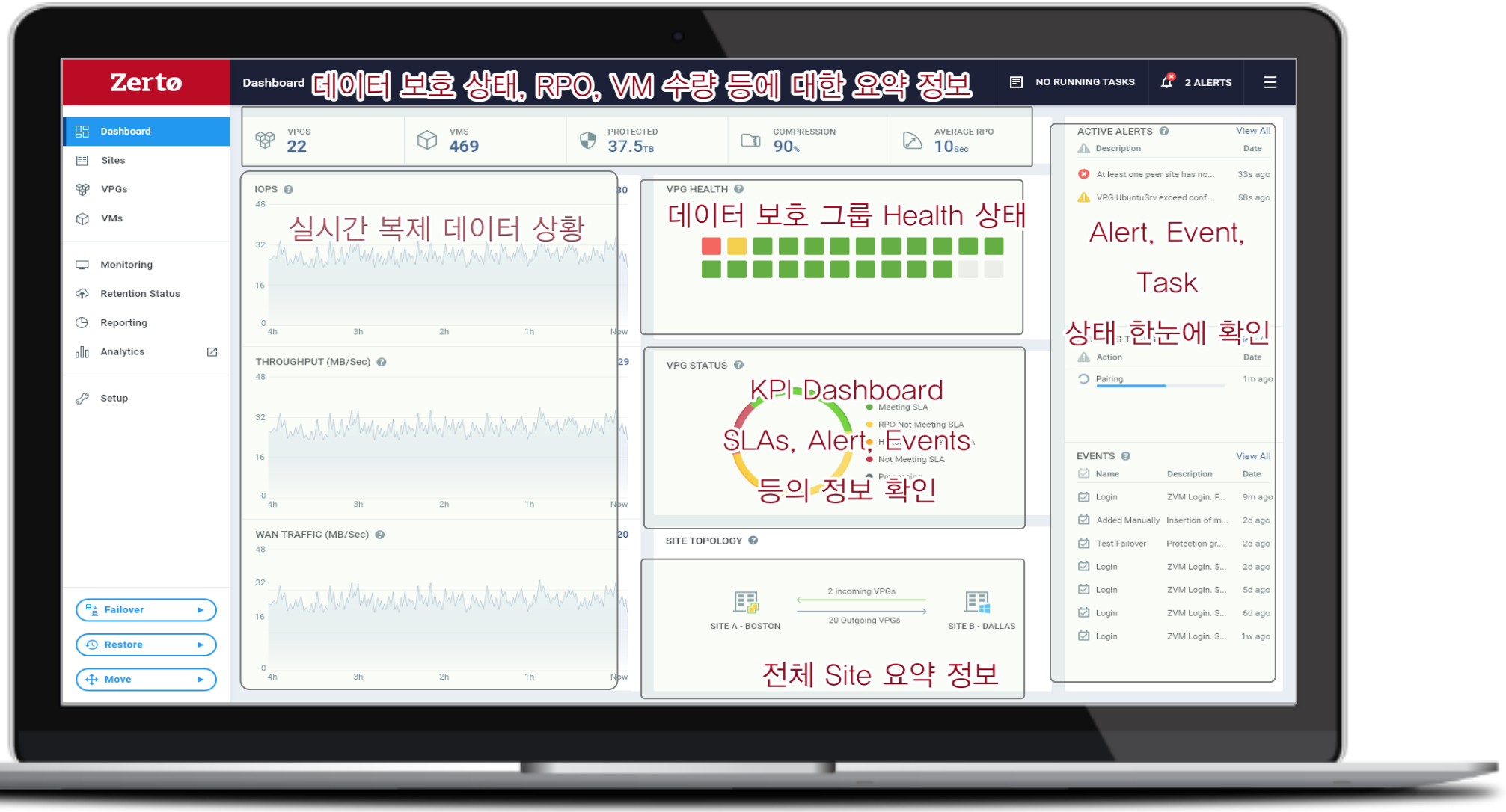
외부 고객서비스

1 Hour

AWS 자체 망



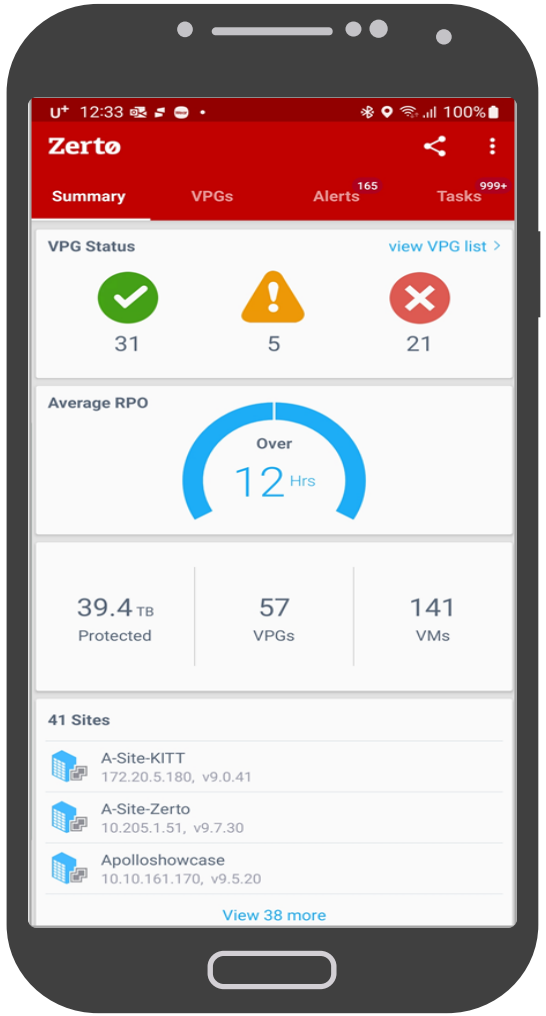
실 시간 DR 관제센터 용으로도 손색이 없음

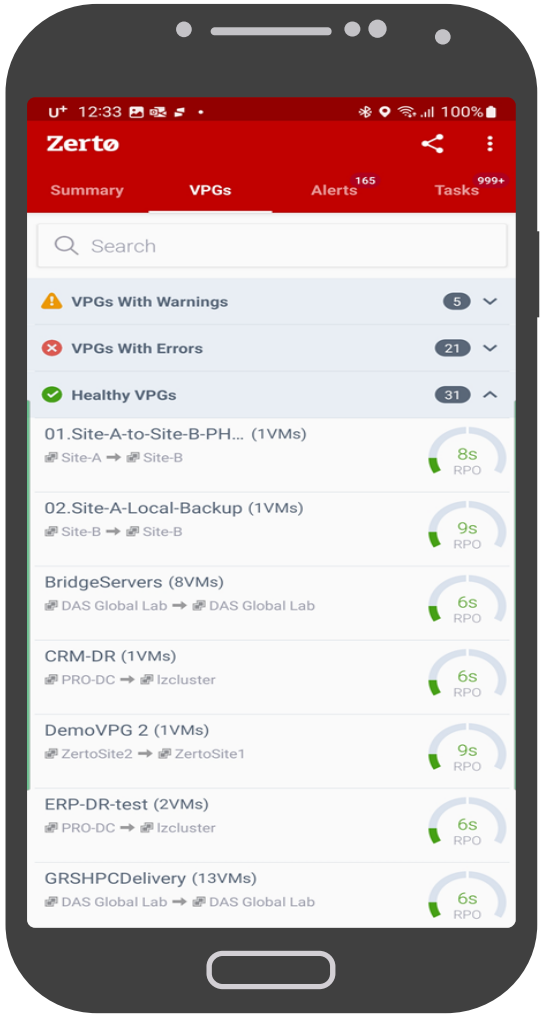


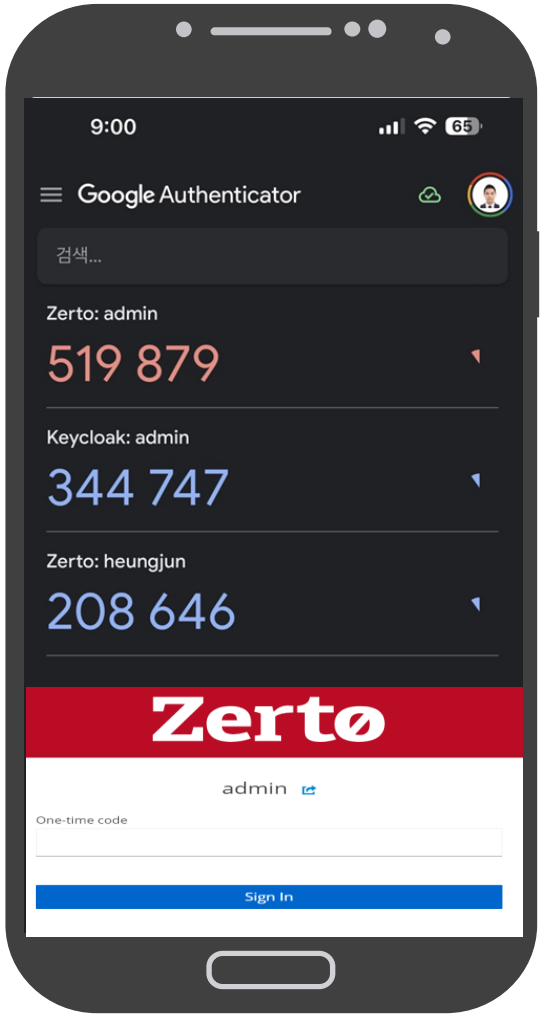
Hewlett Packard Enterprise

앱을 통해 언제 어디서나 확인 가능

MFA | OTP







Hewlett Packard Enterprise

3 가지만 기억하세요

Zerto

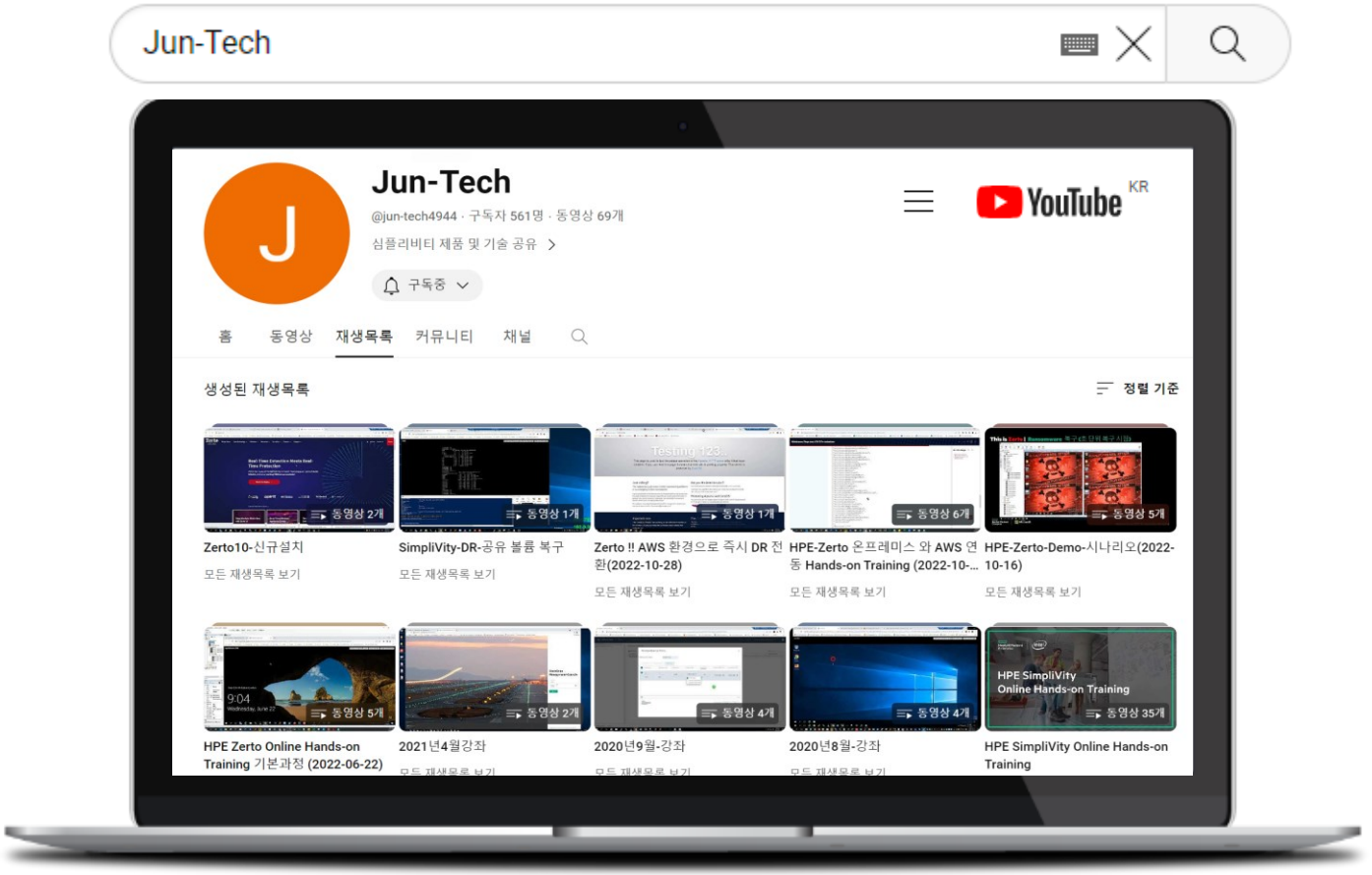
랜섬웨어 실시간 감지

5 초전으로

1 분내 복구

Demo | Hands-on | Installation

Zerto Champion



Hewlett Packard Enterprise

Hewlett Packard Enterprise

24시간 365일,
지속적인 데이터 보호를 책임져 줄 단 하나의 솔루션 HPE Zerto

THANK YOU