Hewlett Packard Enterprise

2024 HPE DID

Data services Innovation Day

일시 2024년 6월 11일(화), 10:00 ~ 17:30

장소 포시즌스 호텔, 그랜드볼룸 (3F)

STORE

MANAGE

PROTECT

Hewlett Packard Enterprise

2024 HPE **Data services Innovation Day**

PROTECT

어떠한 상황에도 24시간 365일 지속적인 서비스 (ZERTO)

HPE 조성택, 차지훈 매니저

Jun 11, 2024

지능적으로 진화하는 랜섬웨어

2024년 2월 / 한 달간 산업별 랜섬웨어 피해 사례 및 종류

● Manufacturing (제조)

- **LockBit**
- 8Base
- Tie Between
- BlackBasta, Medusa, and Play

● Healthcare (헬스케어)

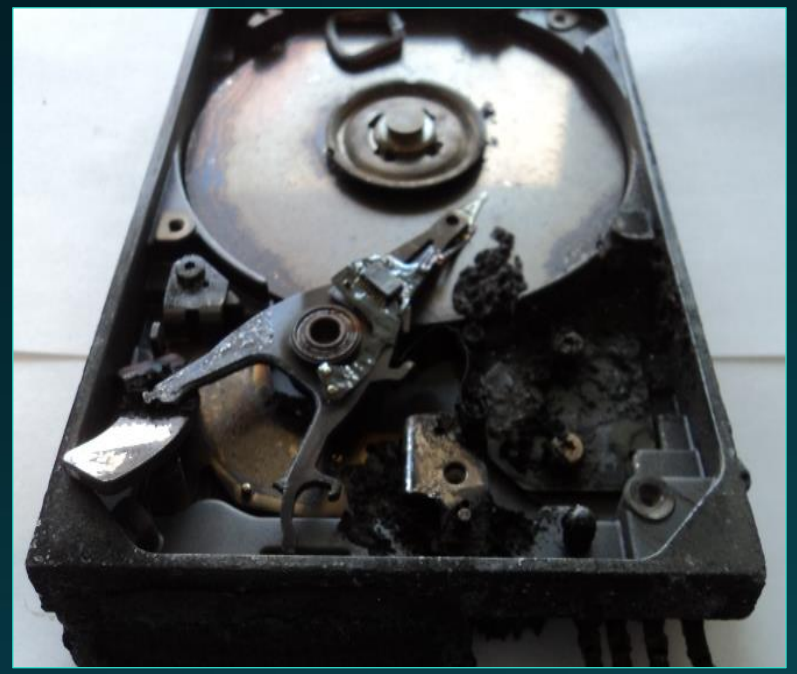
- **Alphv**
- LockBit
- BianLian

● Retail & Wholesale (유통)

- LockBit
- 8Base
- **BlackBasta**

- **타깃형 랜섬웨어** – 특정 공격 대상 지정
- **다양한 변종 랜섬웨어** - 추가 공격 위험
- **안전모드로 자동부팅** - 암호화 실행
- **악성코드 서비스 등록** - 폐쇄망 위협

백업만으로 충분할까요?



데이터 복구 불가

백업 소프트웨어 또는 데이터
세트가 공격 받는 경우

느린 복구 속도

낮은 미디어로부터의 복구 및
원본 데이터 복제 등으로 인한 지연

서비스 중단

전체 인프라 복구 불능 상태이거나
검증된 복원 지점 없음

서비스 연속성을 위해 더욱 강력한 전략 필요

최적의 복구 목표 시점 및 시간 - **RPO** (Recovery Point Objective) / **RTO** (Recovery Time Objective)

재해시 서비스 연속성 보장을 위한 자동화 및 관리 체계

데이터 변경 불가 **(Immutable)** / 외부 환경과 격리된 안전한 데이터 **(Isolated)**

어떠한 외부 공격에도 서비스 지속성이 보장된 (외부와 격리된) 인프라

데이터 보호 복구 솔루션까지 공격 받을 경우 대비 체계

“Cyber Resilience Vault”

랜섬웨어 피해 고객 사례 - 제조 A사

감염

협박

복구시도

1 FAILURE	2 REVERT	3 RESTORE	4 OUTSOURCE	5 RECOVER	6 RECONSTRUCT	7 RESTORE	8 TEST
Catalog failure with Symantec back-up exec	Reverted to previous D2Ds – they also would not catalog	Unable to restore ANY data from disk	Shipped tape files to a company who specialized in restoring data	Company was able to recover with a program they had, however the recovery points were all different times with significant gaps (1 wk, 2 wk)	Reconstructed the file server	Restored the files	Tested the files and the servers

데이터 손실
12시간

데이터 복구
14일

Zerto 도입 이후

1 SELECT POINT	2 RECOVER	3 TEST	4 RECONNECT
Select recovery checkpoint a few minutes prior to ransomware attack	Recovered the VM with a few clicks	Tested the VM	Connected to the network

"Zerto 도입 이후, 같은 사이버 공격을 받았지만 간소화된 절차와 빠른 복구로 피해를 최소화 할 수 있었다"

데이터 손실
10초

데이터 복구
10분

랜섬웨어 피해 고객 사례 - 의료 B사

ALPHV 공격 → 모든 파일 암호화 → 의료 데이터 유출 → 댓가 지불 후 일부 복구

데이터 손실 추정불가

데이터 복구 3주

Zerto CRV 도입 이후

어떠한 외부 공격에도
볼트를 활용한 서비스 연속성

백업 데이터 복원 절차 없이
볼트에서 직접 서비스 가능

"IDV (불변 데이터 저장소)를 갖춘 격리된 복구 환경(IRE)은 내부 위협, 랜섬웨어 및 기타 형태의 해킹에 대해 최고 수준의 보안 및 복구를 제공합니다"

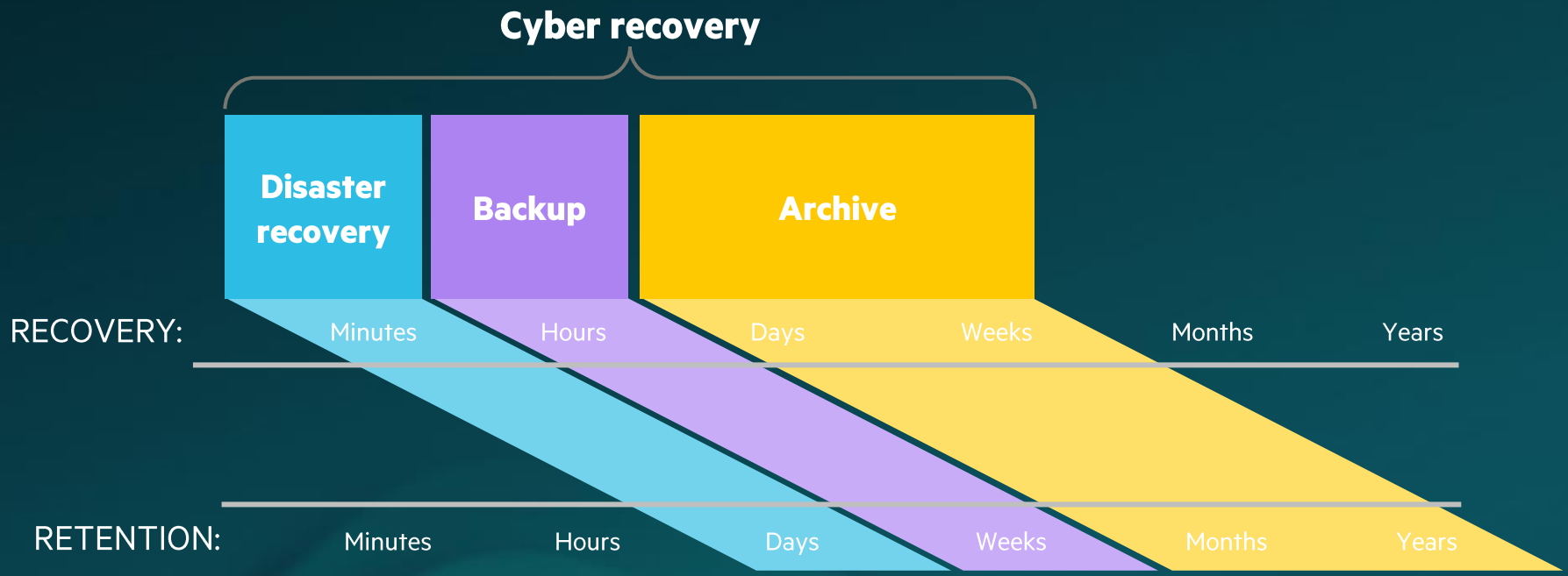
Gartner

데이터 손실
10초

데이터 복구
20분

사이버 공격에 대한 데이터 보호 전략

백업과 DR을 함께 구현하여 데이터 보호 전략 강화!



사이버 공격에 대한 차별화된 데이터 보호 전략

HPE Zerto

기존과 다른 차별화된 사이버 재해 전략을 수립

1 실시간 감지

- 실시간 암호화 이상 징후 감지
- 실시간 사용자 알림

2 빠른 복구시점 파악

- 최적 복구 시점 제공 기능
- 모의 훈련 기능을 통해 데이터 무결성 체크

3 5초전으로 수분내 복구

- 데이터 유실 최소화 **(RPO=5sec)**
- Journal 방식을 통한 수분내 데이터 복구
- 손쉽게 몇번의 클릭으로 복구

4 DC 수준의 데이터 보호금고 (Cyber Resilience Vault)

- Air-Gap / Immutable 기능을 통한 외부와 차단
- 3시간내 대 고객 서비스 재개

랜섬웨어의 공격구조 – 데이터 암호화

MITRE ATT&CK 프레임워크

얼마나 빨리 암호화를 감지하고
복구할 것인가?

암호화 공격 발생 시점에 실시간 감지

Oracle.VM.encrypted
SQL.VM. encrypted
DC.VM. encrypted

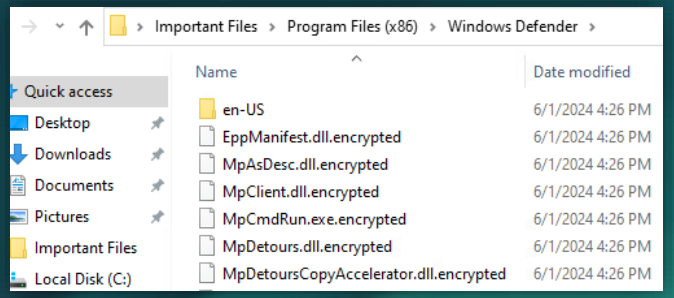
VM/File Encrypted

Ransomware

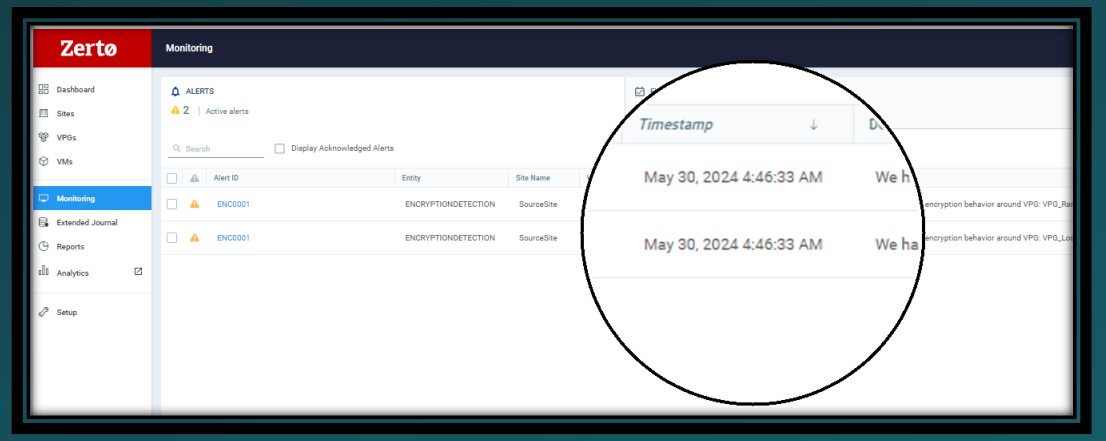
VM VM VM VM

OS/Hypervisor

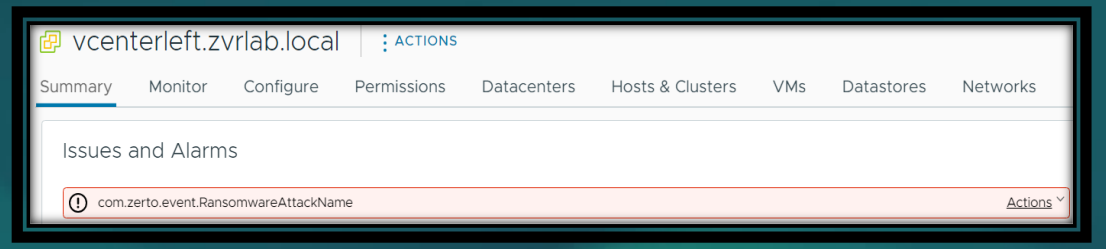
고객 서비스 인프라



HPE Zerto 콘솔 및 사용자 email 알림

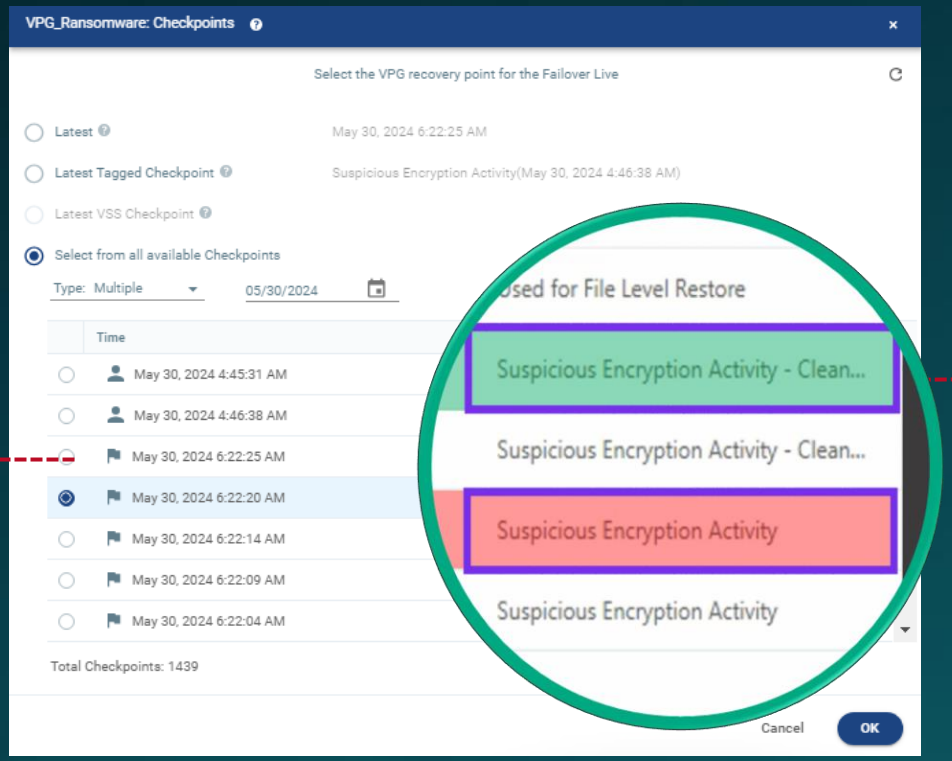


vCenter 내 알림



신속한 대응 ! HPE Zerto 가 도와 드립니다.

모든 변경 사항을 복제하고
5초 마다 복구 가능 시점
생성



암호화 이상 징후 감지 전
데이터가 오염되지 않은
시점 제안 기능

"실시간 암호화 이상 감지로 랜섬웨어로 인한 위험에
선제적으로 대응할 수 있다는 확신을 갖게 되었습니다."

– 제조 회사의 네트워크 팀 고객-

빠른 서비스 재개로 서비스 연속성 확보!

용량에 상관 없이 수분내 원하는 시점으로 데이터 복구

용량에 상관없이 수분내 복구

- **5초** 간격의 원하는 시점으로
- 용량에 상관 없이!
- 수분내 데이터 복구

DR 센터로 즉시 서비스 재개

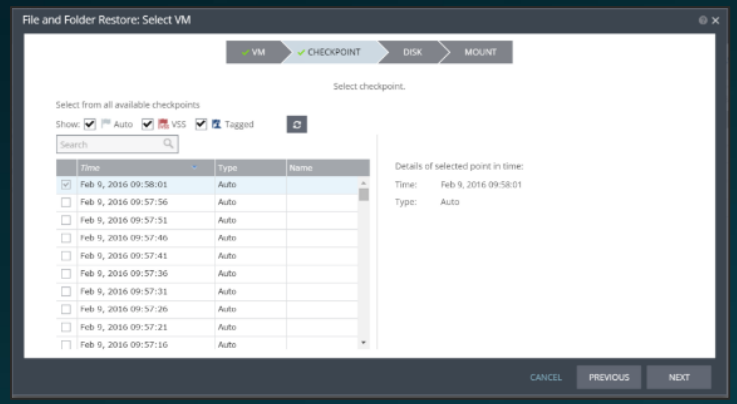
- 수십분내 인프라 구현
- 자동 역 복제를 통해 빠르게 주 센터 운영 복귀

VM / File 단위 데이터 즉시 복구

- Local 복제 및 복구 가능
- 다양한 복구 시나리오 제공

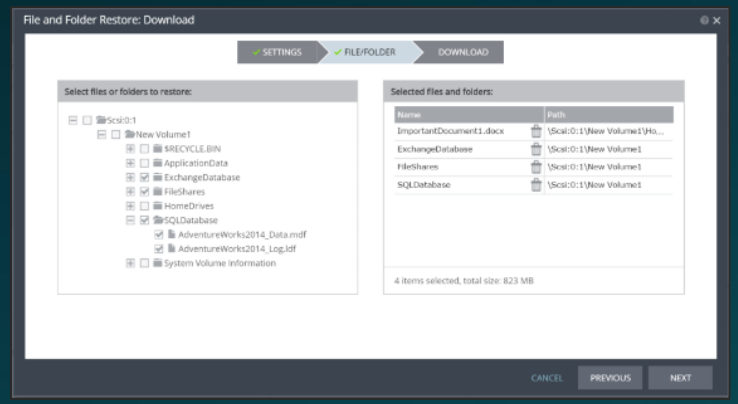
랜섬웨어 피해 수준에 맞는 복구 옵션

데이터 복구 기능



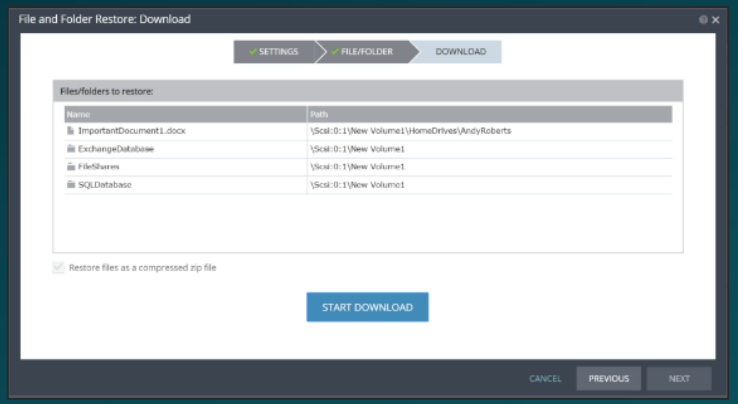
- 가상 머신 수준의 복구
- 5초 단위 어느 시점이나!

파일 또는 폴더 수준 복구



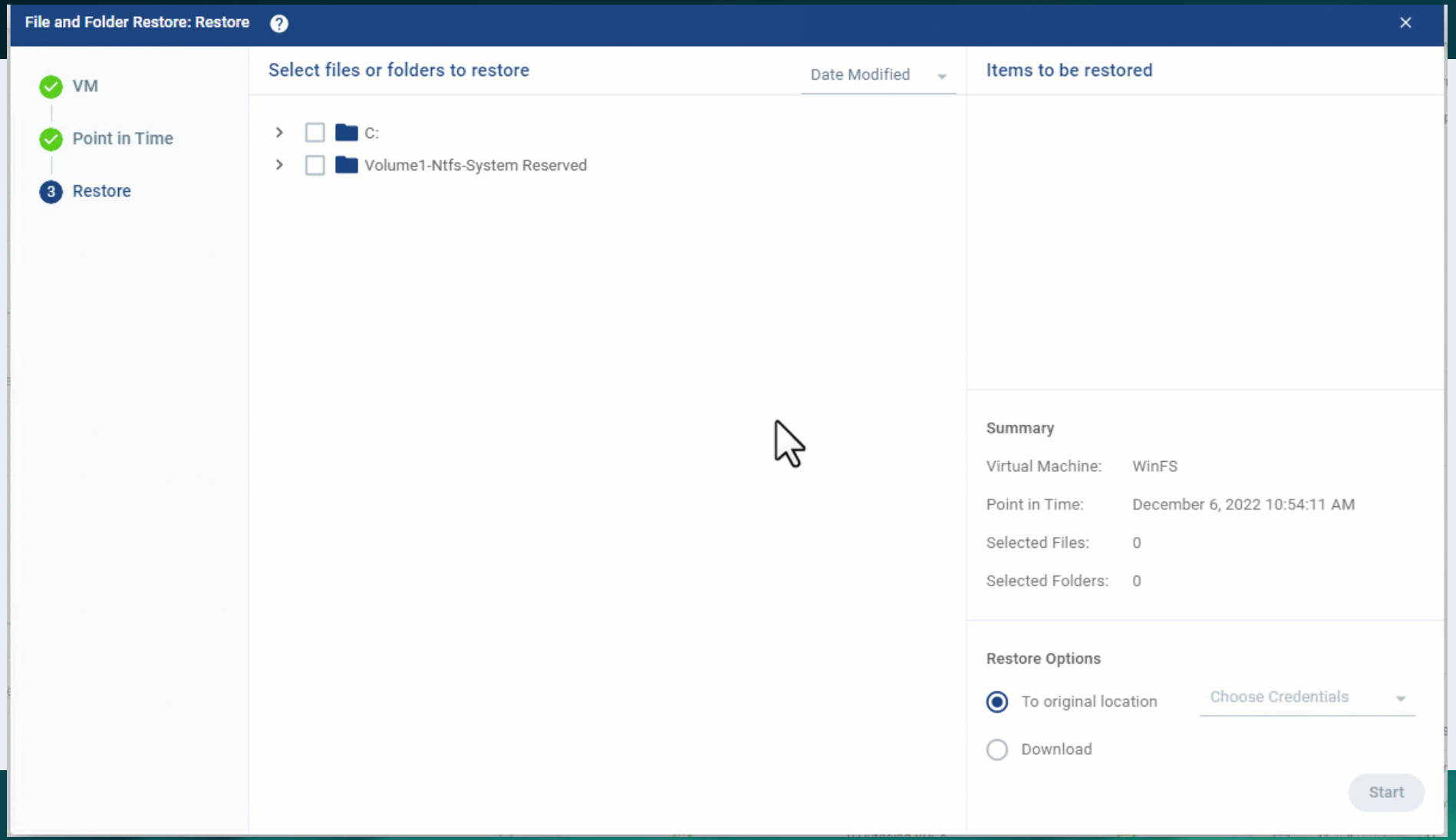
- 파일 서버 데이터
- 어플리케이션 데이터
- SQL, Oracle, Exchange 데이터베이스 파일

다양한 복구 방법 지원

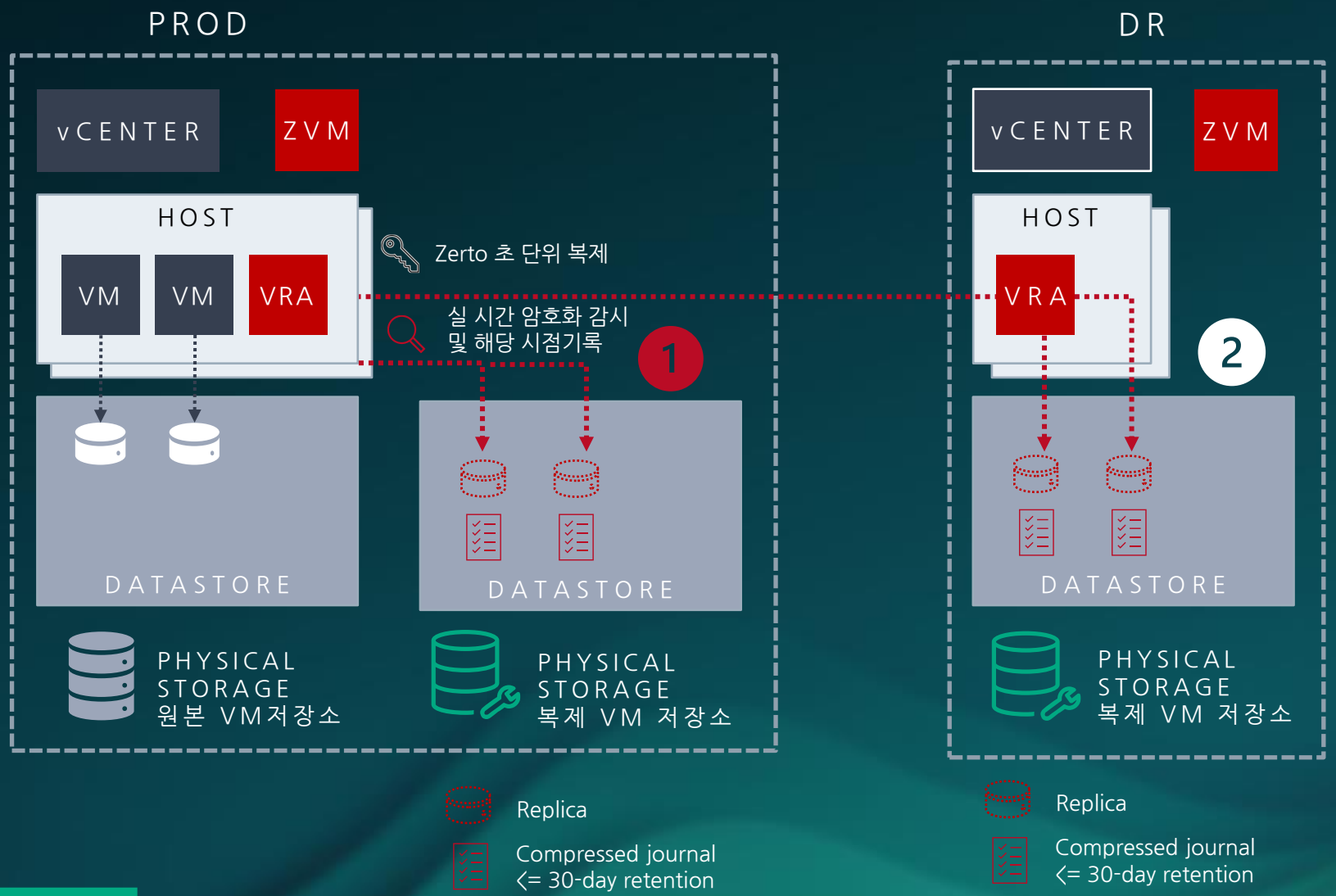


- 브라우저 다운로드
- 운영환경 내 복구 가능

파일 복구 데모


File and Folder Restore: Restore
VM
Point in Time
3
Restore
Select files or folders to restore
Date Modified
C:
Volume1-Ntfs-System Reserved
Items to be restored
Summary
Virtual Machine:
WinFS
Point in Time:
December 6, 2022 10:54:11 AM
Selected Files:
0
Selected Folders:
0
Restore Options
To original location
Choose Credentials
Download
Start

랜섬웨어 공격 대비 아키텍처 제안



1차 보호 - 랜섬웨어 보호 차원의 In-House 구성

- 랜섬웨어 감염 시 즉시 로컬에서 신속 히 복구 or 복구 전까지 서비스 제공
- 저렴한 서버 or 재활용 서버로 구성 가능
- 로컬 데이터 센터에서 발생 한 개별 VM 장애 발생 시, 로컬에서 즉시 복구

2차 보호

로컬 데이터 센터 전체 장애 시, DR 센터에서 서비스 기동

랜섬웨어의 공격 구조 – 데이터 센터 장애

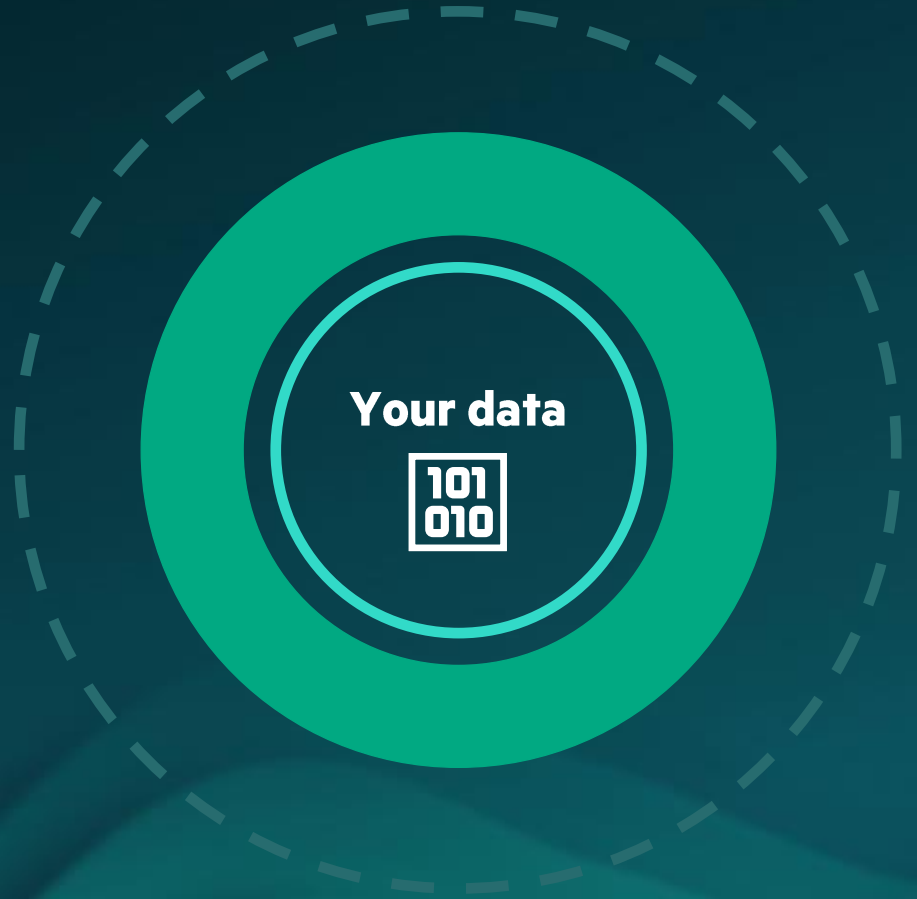
MITRE ATT&CK 프레임워크

사이버 공격으로 인프라 전체가 무력화된
최악의 시나리오에서는 어떻게 인프라를
정상화 할 것인가?

Zerto Cyber Resilience Vault

사이버 공격으로 인한 최악의 시나리오에 대비

- ✓ 격리된
- ✓ 에어 갭
- ✓ 변경불가한
- ✓ 제로 트러스트

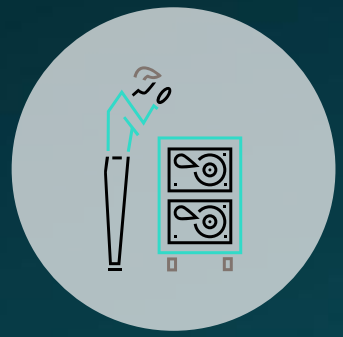


제로 트러스트 아키텍처를 사용하여 **변경 불가능한** 데이터 복사본으로 격리, **오프라인, 에어 갭** 제공

사이버 복구를 위해 **특별히 설계된** 최악의 시나리오에서 최후의 수단으로 사용 가능

Zerto Cyber Resilience Vault

신속하고 안전한
안전한 고성능 올플래시 하드웨어기반에 에어 갭 및 변경 불가능한 데이터 복사본을 저장.

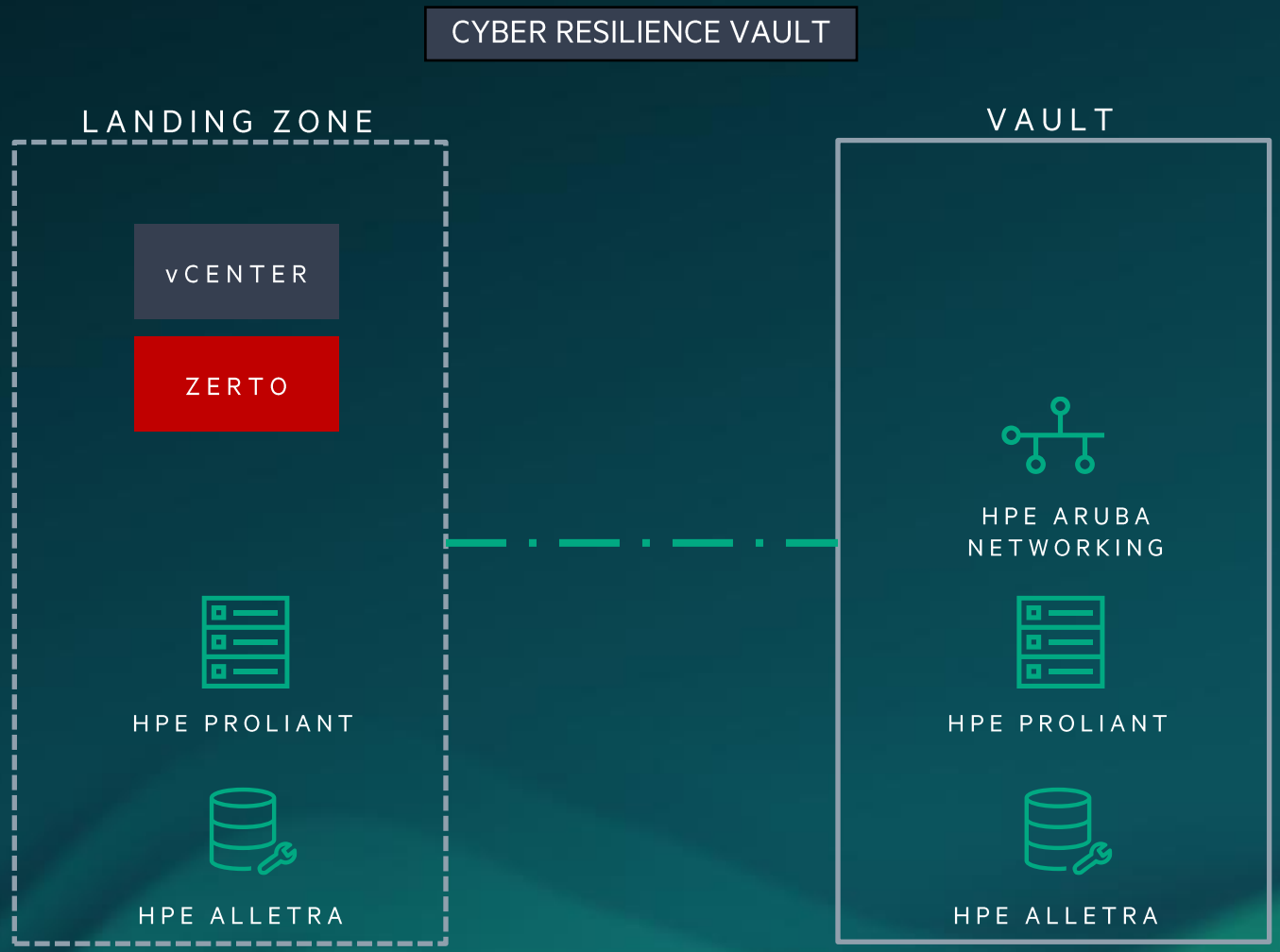


풀스택 솔루션
고유한 제로 트러스트 아키텍처를 사용하여 안전한 데이터 볼트를 갖춘 격리된 복구 환경을 제공합니다.

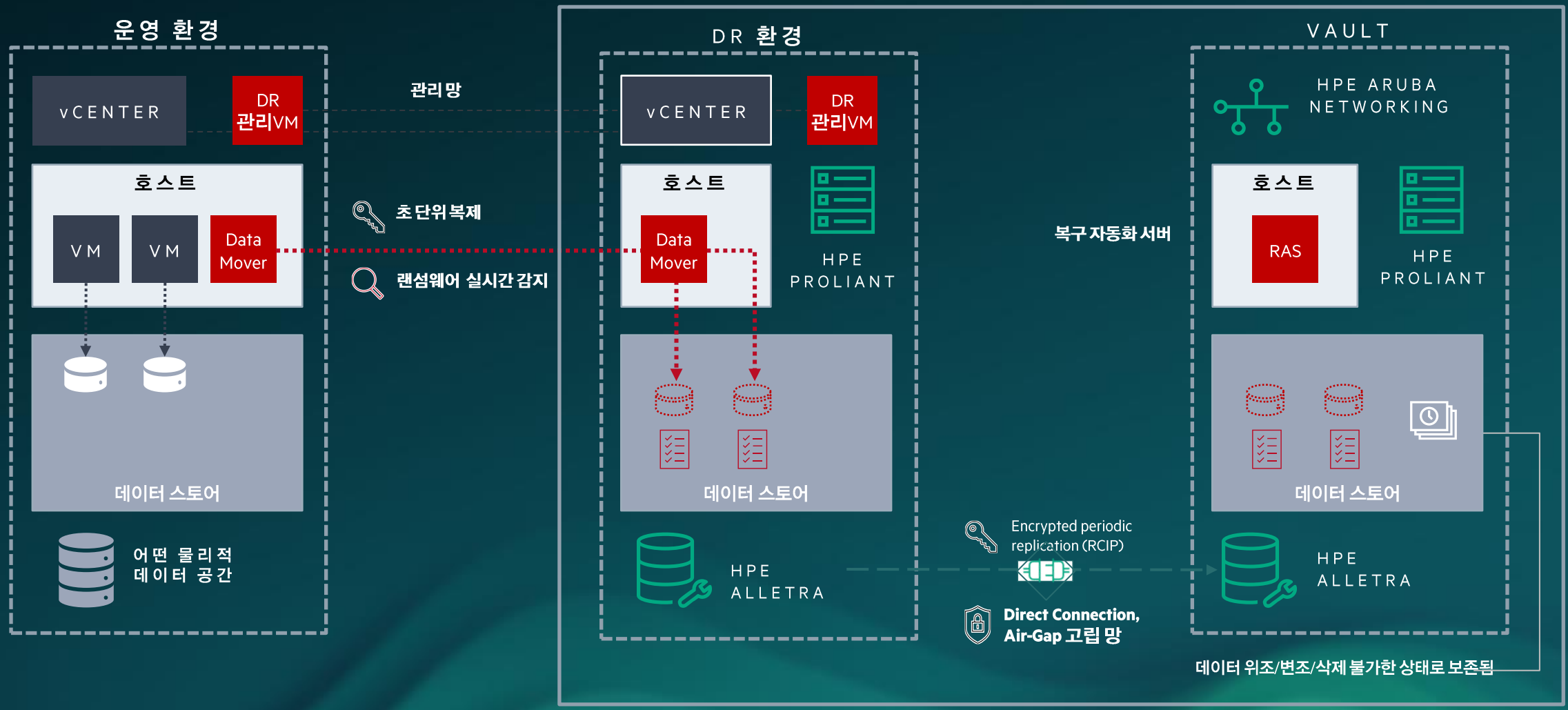
편리함을 넘어선 보안
중앙 집중식 컨트롤 플레인 없음: 외부와 완벽히 차단된 볼트에는 관리 포트가 노출되지 않으며 단일 손상 지점이 없습니다.

낮은 TCO로 엄격한 규정 준수 달성

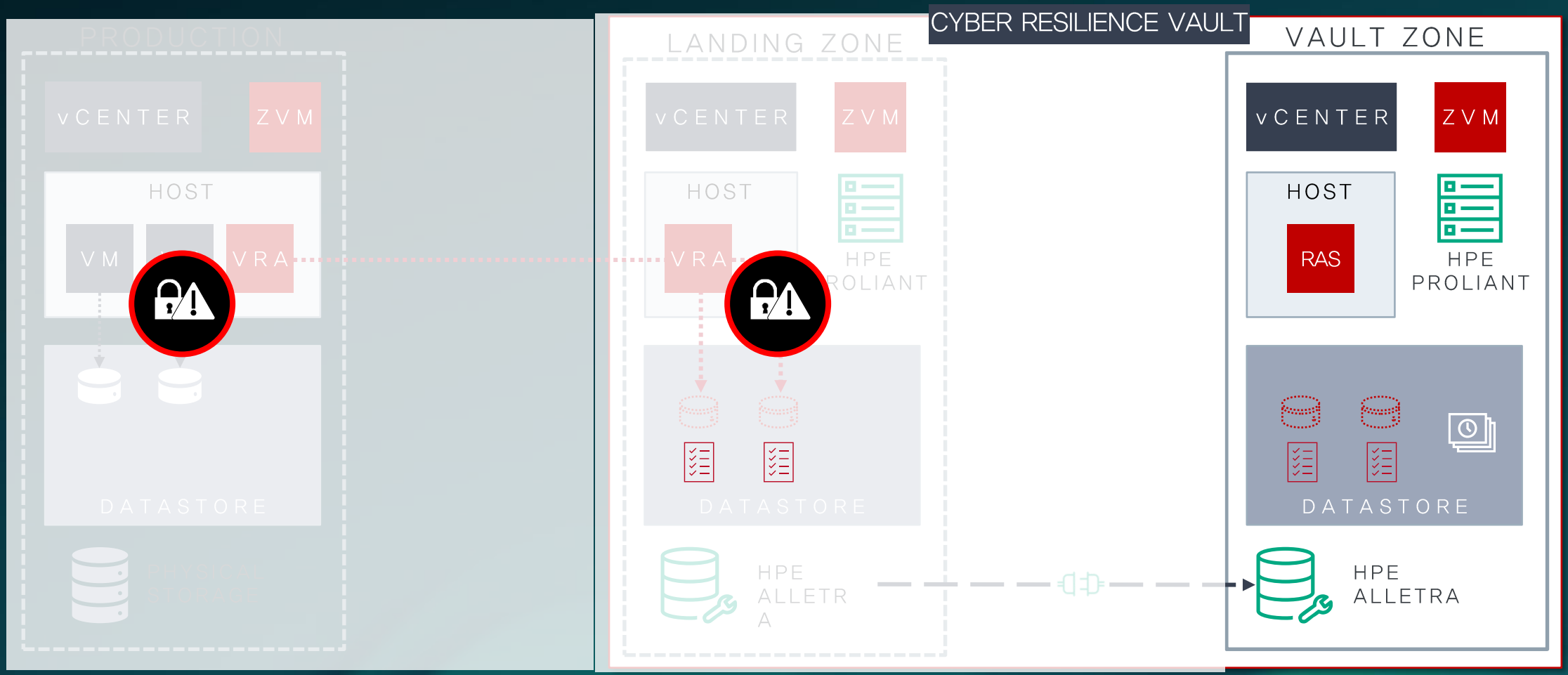
Zerto Cyber Resilience Vault 아키텍처



Zerto Cyber Resilience Vault 구성도



Zerto Cyber Resilience Vault 시나리오



1 복구할 app 또는 VM을 선택

2 볼트 저널로부터 깨끗한 Center, 접근 and Z

3 VMS 파워 온

중단 없이 깨끗한 복원 지점을 테스트하고 검증하기

3 클린 체크포인트를 사용하여 Zerto 저널에서 복구하기

Zerto Cyber Resilience Vault ROI

빠른 복구 = 사이버 공격 피해 최소화

	백업 중심 솔루션- Cyber Vault 기준 *	Zerto a Hewlett Packard Enterprise company	Zerto Benefits
오염되지 않은 최신 데이터 (RPO)	2 days	4 hours or less	**87% 이상 감소**
복구 시간 (RTO)	**22** days	**2** hours	**99% 이상 빠름**
총 랜섬웨어 피해 기간	3 – 5 Weeks	6 hours or less	**99% 피해 감소**
저널 방식 복구 여부	NO	YES	**유일한 저널 방식의 데이터 금고 솔루션**

* 300개의 가상 머신과 300TB를 보호하는 고객을 기반으로 한 실제 사례

WHY “PROTECT” BY HPE?

1. 랜섬웨어에 **완벽히 대응**하고 계십니까?.
2. 기존 백업 운영에 **손쉬운 운영이 가능한 재해복구 솔루션**을 추가해야 합니다.
3. 사이버 공격은 **항상 실시간으로 감지하고 즉시 복구 가능**해야 합니다.
4. **사이버 볼트(Cyber Resilience Vault)는** 선택이 아니고 **필수** 입니다.
5. 백업 기반의 볼트가 아닌 **즉시 서비스를 재개할 수 있는 사이버 볼트(Cyber Resilience Vault)** 입니다.

Askstorage@hpe.com

AskDR@hpe.com