PURESTORAGE®

무중단 서비스를 위한 데이터 보호 현대화 전략

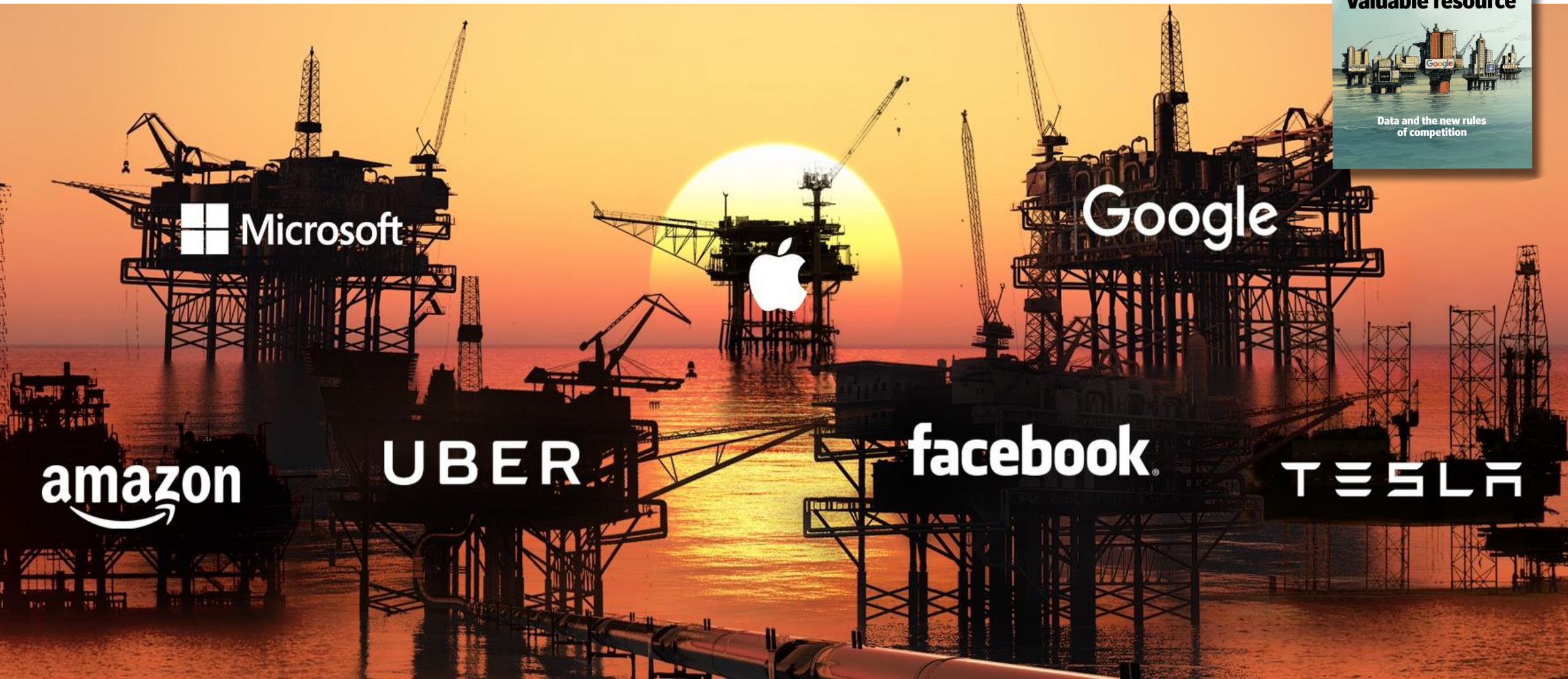
퓨어스토리지 강신우 부장
Sr. Systems Engineer

Sean.kang@purestorage.com

Oct 2022

데이터가 기업의 가장 중요한 지원

데이터 관련 비즈니스의 급격한 수요 증가



Re-Think Business Continuity

데이터 관점에서의 장애 유형

물리적 장애 [Physical Failure]
: 하드웨어 또는 전원, 데이터센터와 같은 물리적인 장비의 문제로 발생되는 장애

- 자연재해 – 지진, 폭우, 지진, 화재
- 하드웨어 노후화로 인한 실패
- 전기 / 네트워크 / 스토리지 장애

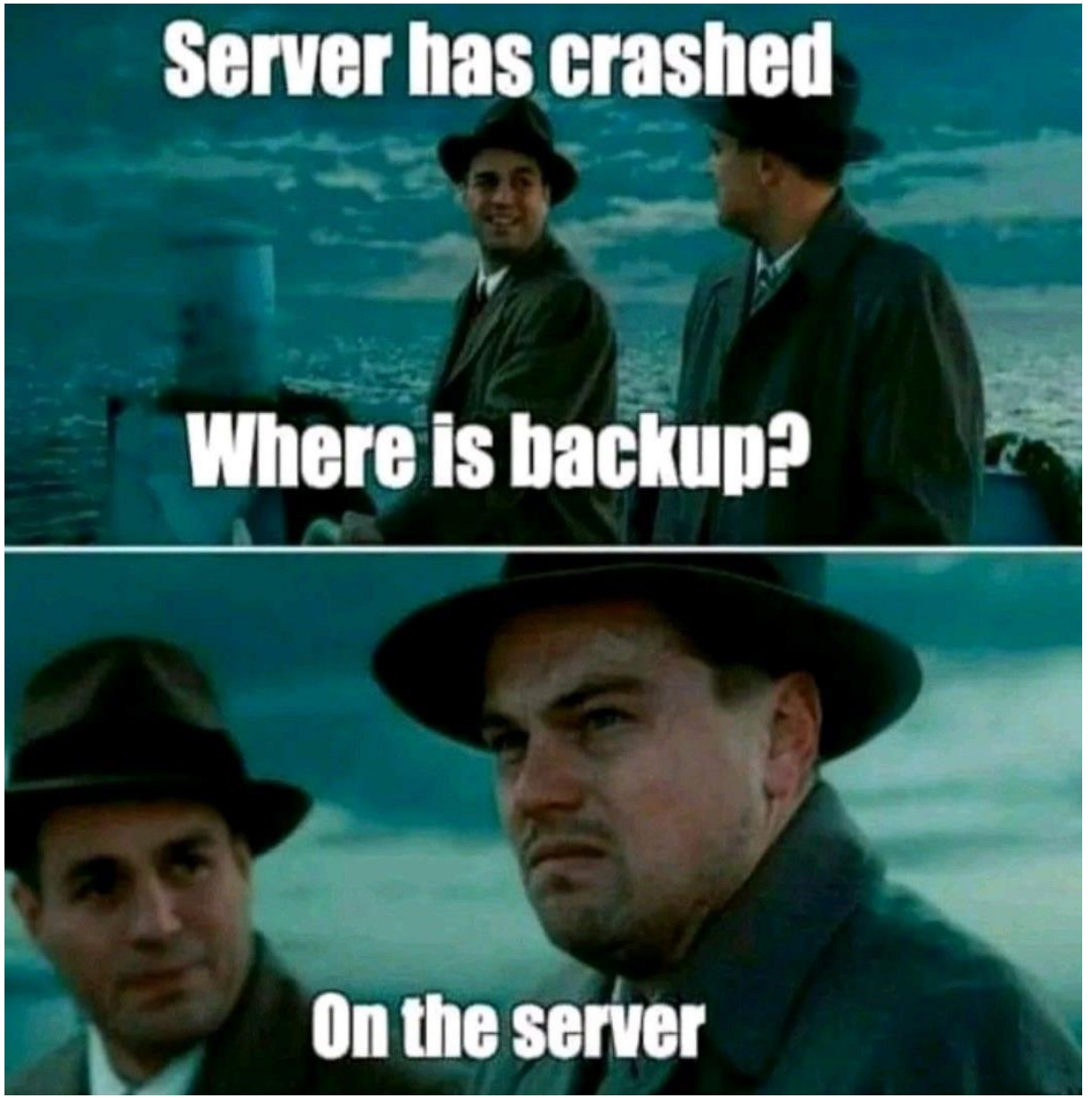
→ 하드웨어 이중화를 통한 무중단 운영

데이터 관점에서의 장애 유형

논리적 장애 [Logical Failure]
: 애플리케이션 또는 운영체제 상의
데이터 삭제 및 손상으로 발생되는 장애

- Human Fault
- 운영자 / DBA 에 의한 작업 실수
- 사이버 공격으로 인한 데이터 손실

→ 백업을 통한 데이터 복구



데이터 관리 인식의 변화

단순한 데이터 보호에서 초고속 복구를 통한 비즈니스 보호로의 백업 개념 변화

LEGACY BACKUP

- 단순한 데이터 보호 목적
- 데이터 손실에 대한 보험
- 느린 백업 윈도우 및 복구 불확실성

현대적 데이터 보호

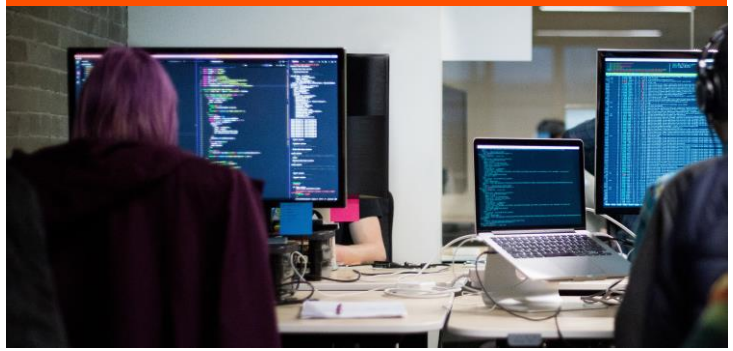
- 데이터 보호 → 비즈니스 보호
- 데이터 활용 → 새로운 가치 창출
- 초고속 성능 기반 복구 중심의 접근

데이터 활용 필요성 증가

단순한 데이터 보호에서 초고속 복구를 통한 비즈니스 보호로의 백업 개념 변화

비즈니스 보호

TEST/DEV



GDPR & 컴플라이언스

악성코드 감지

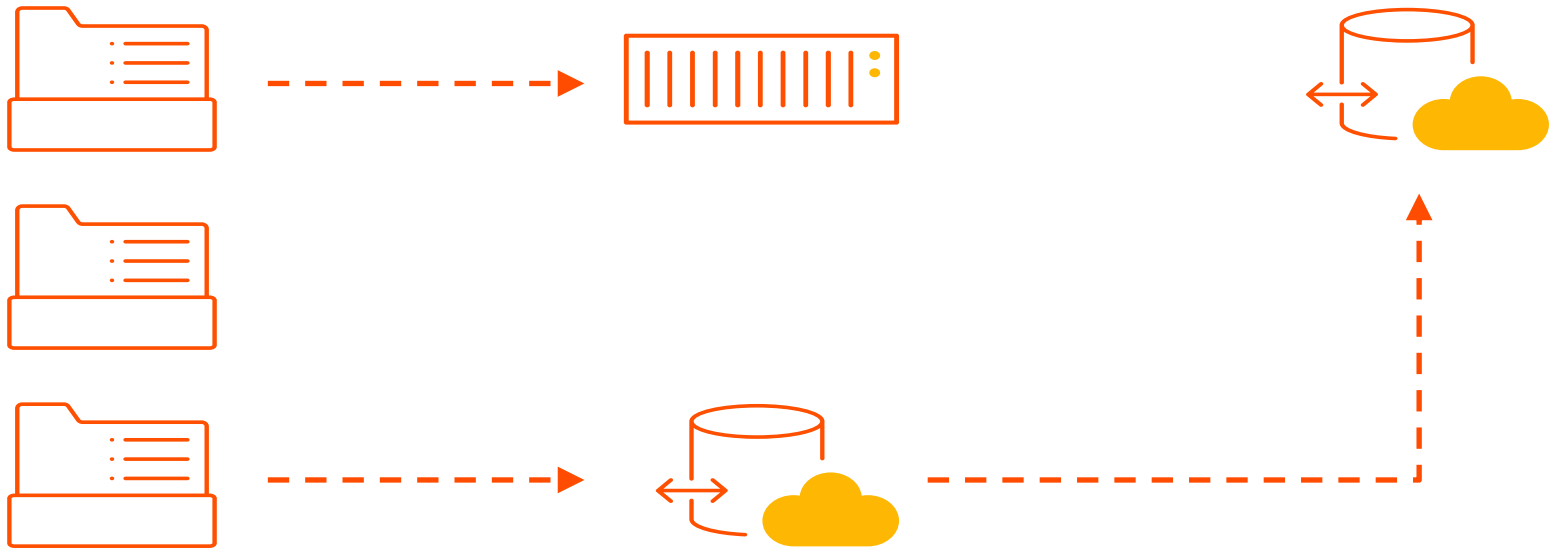
데이터 분석

데이터 보호 전략 변화 필요

3개 이상의
복제본

2개 이상의
스토리지 저장소

1개 이상의
오프사이트 소산



D2D2T 에서 F2F2C로의 전환

무중단 서비스를 위한 데이터 보호 아키텍처

1

ActiveCluster

AADC 구현
실시간 데이터 이중화
물리적 장애 보호

2

SafeMode

랜섬웨어 보호
다운타임 최소화
논리적 장애 보호

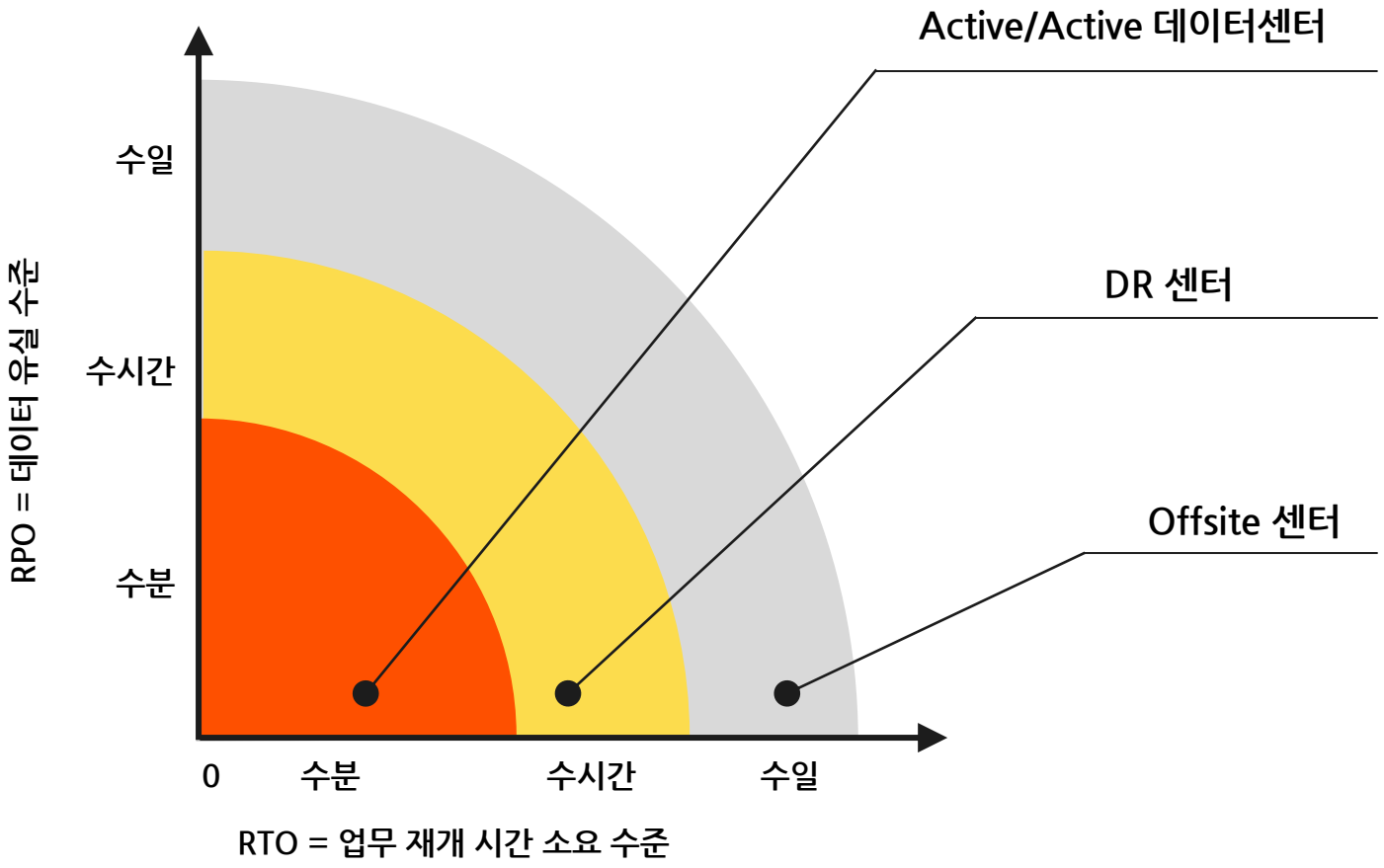
3

RapidRestore

비즈니스 보호
초고속 백업/복구
데이터 활용성 향상

ActiveCluster

재해 복구 RPO/RTO 수준 정의



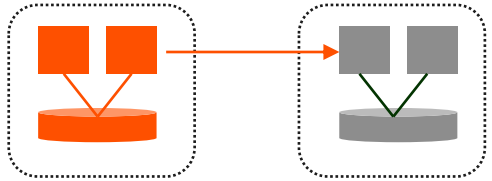
CONTINUOUS AVAILABILITY
- 서비스 무중단 (Zero Downtime)
- 최소중단(Near Zero Downtime)

DISASTER RECOVERY
- 중단 → 복구 → 서비스 재개
- Hour ~ Day

BACKUP & RECOVERY
- 중단 → 복구 → 서비스 재개
- Days

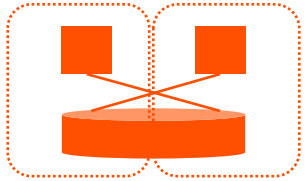
비즈니스 연속성을 위한 새로운 아키텍처

Active/Standby → Active/Active 로의 전환



Active/Standby

복잡한 페일오버 절차



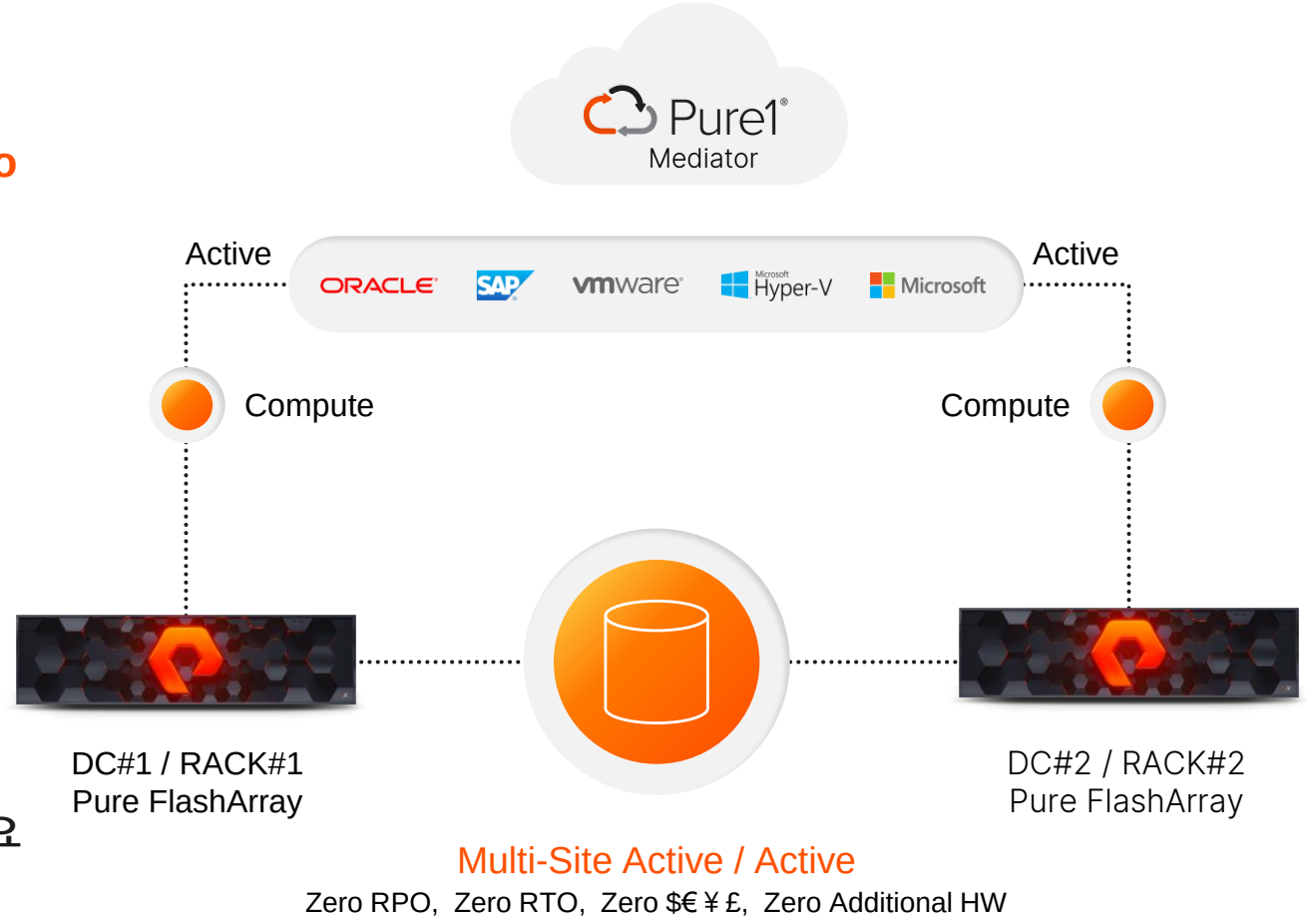
Active/Active

무중단 서비스 지원

DR 구성을 위한 스토리지 이중화 아키텍처 전환

ActiveCluster Overview

- **Active-Active 기반 데이터센터 장애 보호 RPO = Zero**
- **데이터 손실 없는 즉시 Failover RTO = Zero**
- **사용자 개입 없는 자동화된 장애 조치**
- **Round Trip Time(RTT) = 11ms 내에서의 구성**
- **Async 스냅샷 방식에서 Sync 모드로 자동 전환**
- **클라우드 기반 Mediator 제공으로 별도 Witness 불필요**



장애 타입 별 조치 시나리오

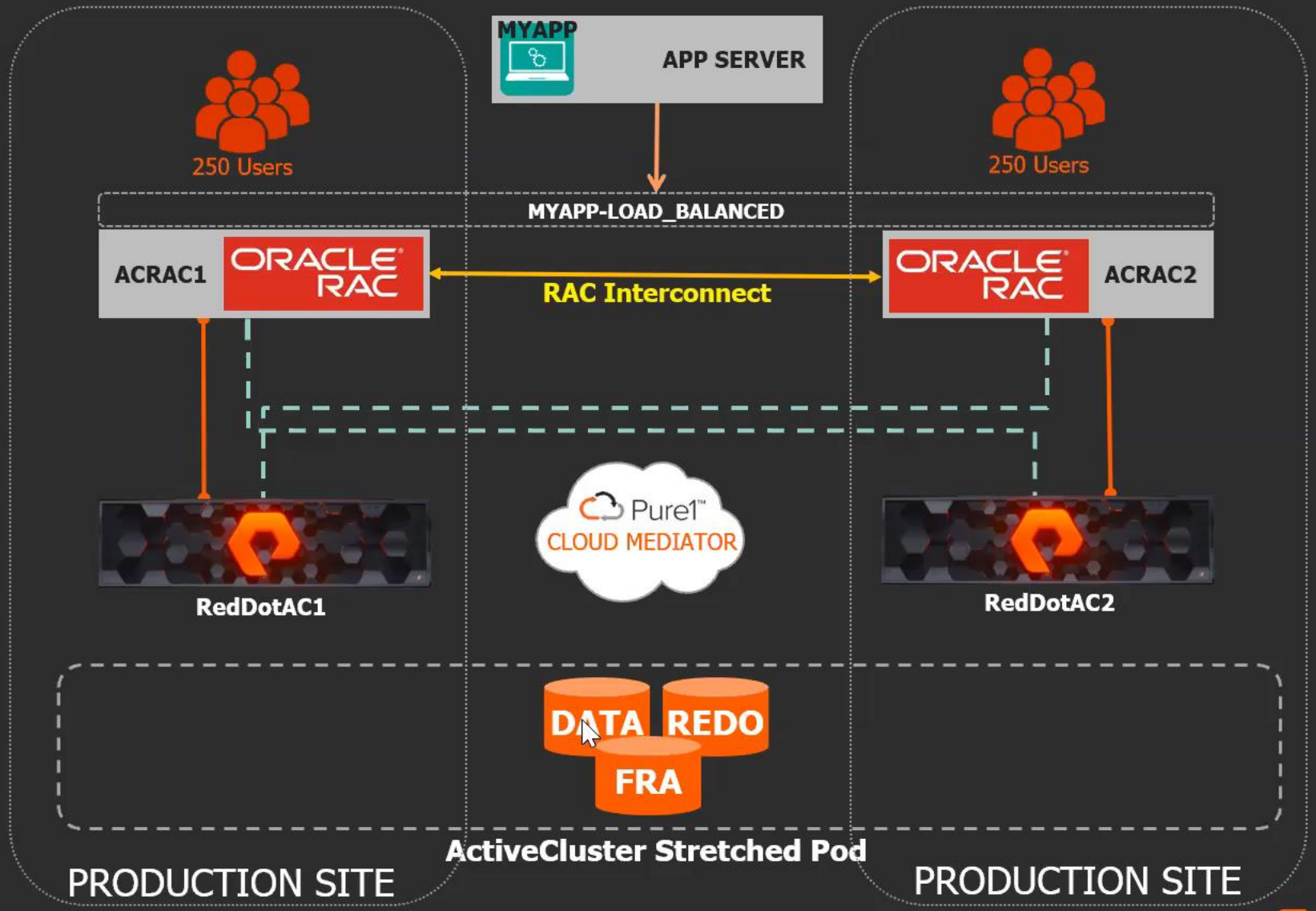
장애 타입						
FlashArray	Replication Connections	Cross-site host connectivity	Management network connectivity	Replication + Cross-site host connectivity	All Cross-site Connectivity	Site Loss

Green 애플리케이션 서비스 무중단. 일부 하위 스토리지 경로 실패 발생.

Yellow 실패 시, 라이브 Array와의 연결 경로가 없는 서비스들의 다운타임 발생 → 수동 또는 자동으로 서비스 재개 가능

Grey 사이트 간 연결이 없는 Non-Uniform 구성에서의 Pod Offline 에 따른 서비스 다운 발생

BUSINESS CONTINUITY WITH RAC ON ACTIVECLUSTER



PURESTORAGE®

ActiveCluster Summary

Symmetric Active-Active

데이터 미러링을 통해 동일 볼륨에 대한 읽기 / 쓰기 수행

Transparent Failover

자동화된 무중단 장애 조치 수행 및 Re-Sync 자동 수행

Active-Active-Async Replication

변경데이터에 대한 복제/재동기화 수행 및 async 통합

Software Defined & No License

별도 장비 없이 소프트웨어 만으로 구현

Simple Management

모든 어레이에서의 작업 지원(Uniform/Non-Uniform)

Pure1 Cloud Mediator

클라우드 기반 Witness 제공으로 별도 구성 불필요

Safemode

SafeMode 를 통한 랜섬웨어 극복 사례

인도의 MSP 기업

FlashArray를 운영 스토리지로 사용

스냅

1. 랜섬웨어 감염 / 스냅샷 삭제 확인
2. Eradication Bucket 스냅샷 복원 및 서비스 재개

Status : Ransomware attack occured on 14th.

2022- 14 02:59:54 | 1949506 | customer | pureuser | purepgroup destroy

2022- 14 03:00:00 | 1949507 | customer | pureuser | purepgroup destroy

2022- 14 03:00:06 | 1949512 | customer | pureuser | purepgroup destroy

RANSOM

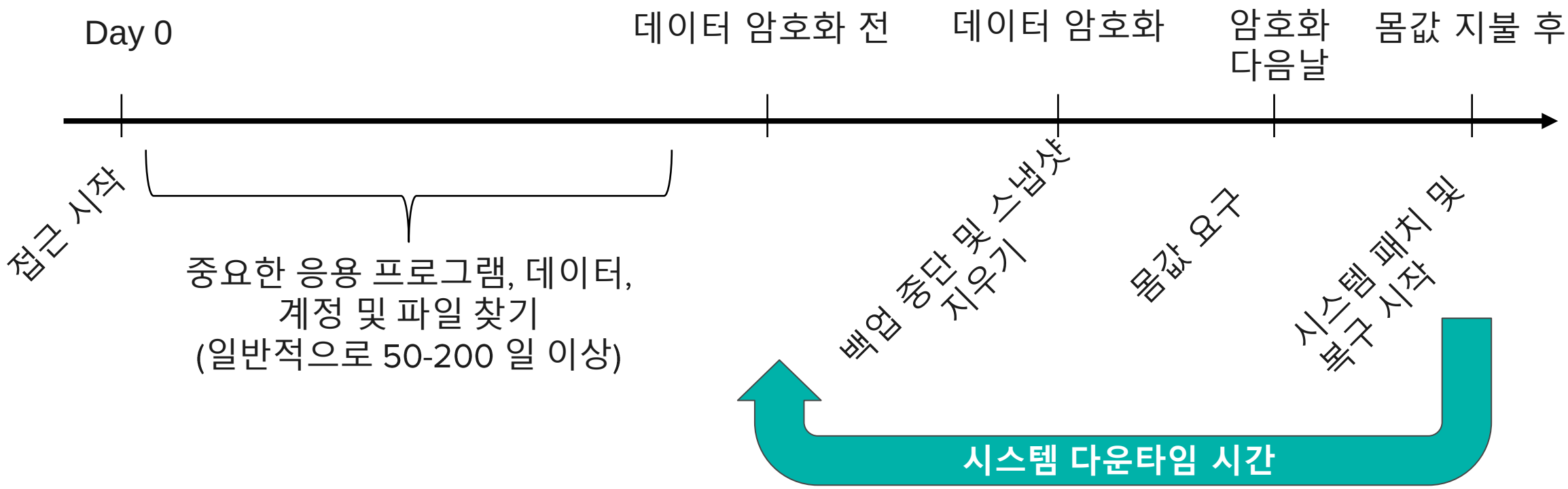
몸값, 몸값을 치르고 석방됨

MALWARE

악성 소프트웨어

일정 금액을 지불 할 때까지 컴퓨터 시스템에 대한 액세스를 차단하도록 설계된 일종의 악성 소프트웨어

랜섬웨어 공격 구조



랜섬웨어 공격화면 예시

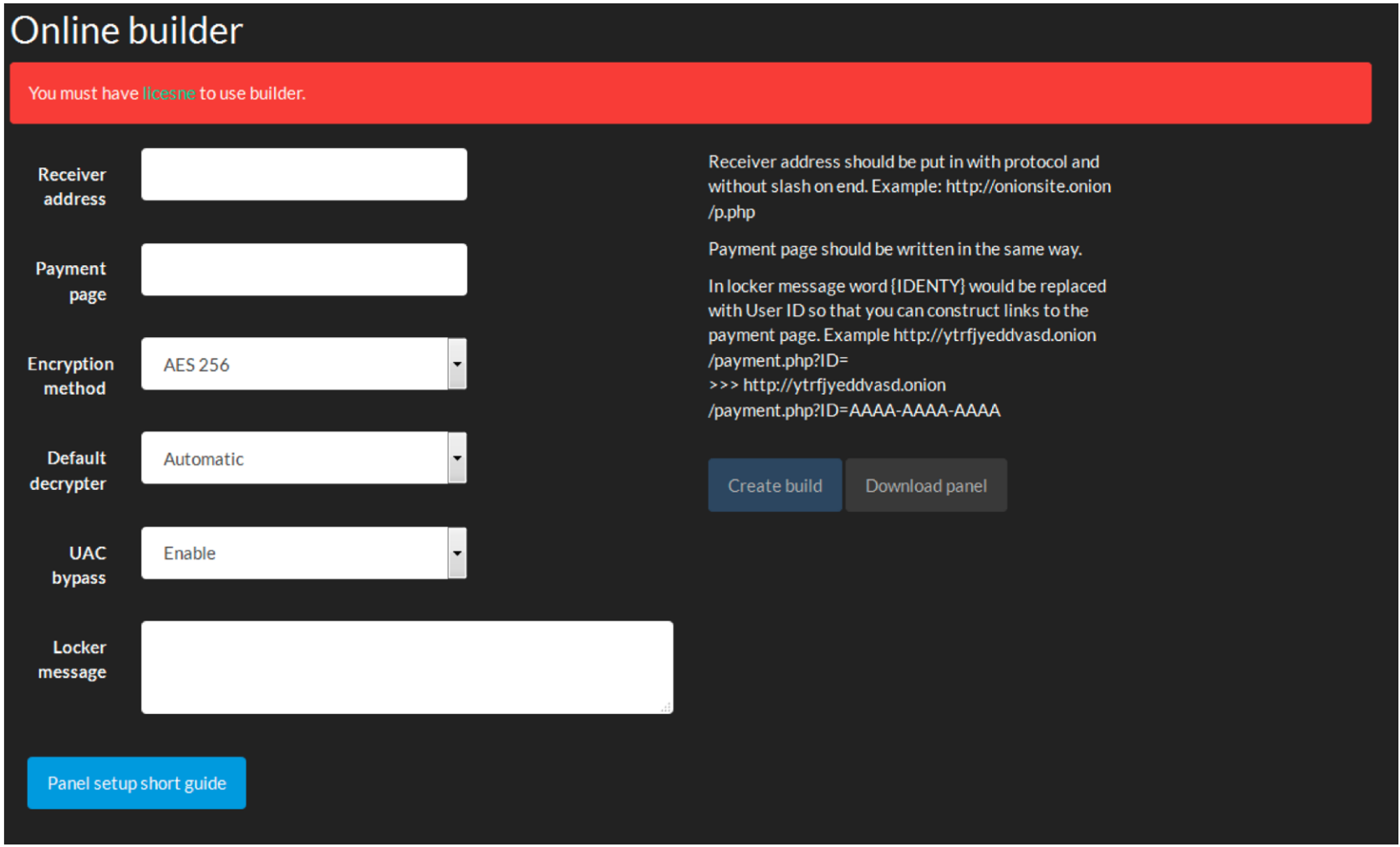
랜섬웨어는
항상 우리를
위협하고
있습니다

누구나 해커가 될 수 있습니다..

서비스 형 랜섬웨어는

누구든지 쉽게

악성코드를 만들 수 있습니다.



백업이 최후의 방어선 입니다.

랜섬웨어 감염 시
유일한 복구 방법은,

백업본에서 복원하거나

몸값을 지불하고
기도하는 것입니다..

해커는 당신의 백업을 찾고 있습니다

해커는 데이터를 암호화하기 **전에** 시스템에서 200 일 이상을 보냅니다.

그리고 그 시간은 백업 복사본을 찾는데 사용됩니다...

97% 백업본 감염을 위한 랜섬웨어 공격 시도

73% 백업본에 대한 랜섬웨어 공격 성공

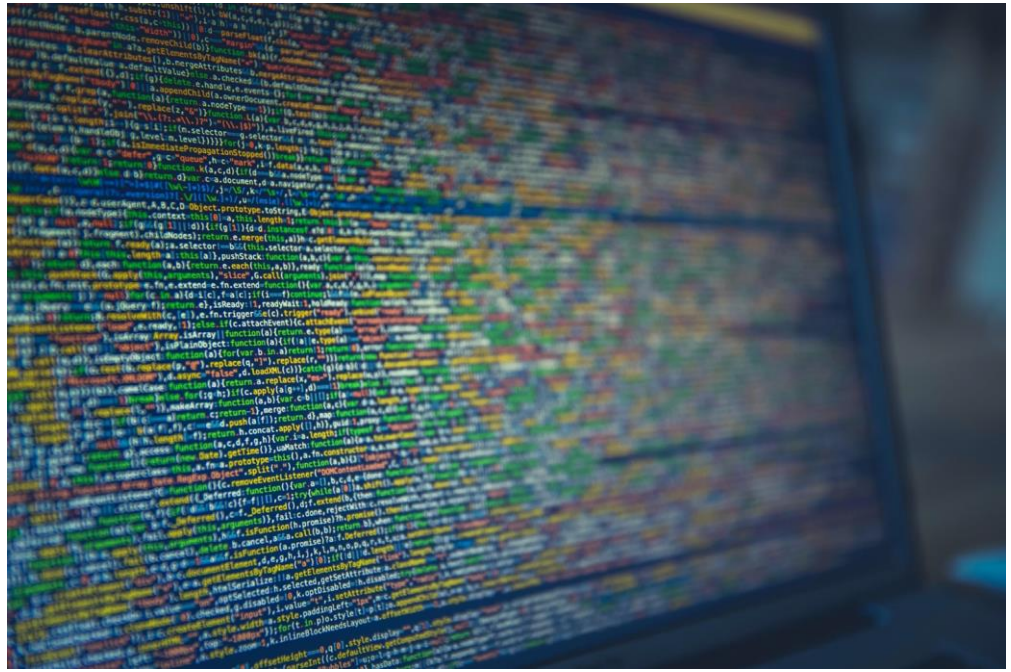
36% 조직에서 몸값을 지불했으나 데이터 복구 실패

Source: Veeam 2022년 랜섬웨어 동향 보고서

PURESTORAGE®

PURE//ACCELERATE® techfest22 seoul

공격을 받았다면 다음 두 가지 대응이 필요합니다.



랜섬웨어 공격에도
유효하고 사용가능한 데이터 복사본

대량의 데이터에 대한
초고속 데이터 복구

#1. 랜섬웨어 공격에도 유효하고 사용가능한 데이터 복사본

Snapshot Policy	Authorization	Tune Eradication Timer	Disable Eradication
위/변조 불가능한 스냅샷	권한 있는 사용자 제한	완전 삭제 타이머 설정	변경되지 않는 안전한 데이터
유연하고 세분화된 스냅샷 정책	최대 5명까지 승인된 컨택포인트, PIN code 제공	24시간에서 최대 30일까지 스냅샷 보관	볼륨 수동 완전삭제 비활성화

Purity SafeMode 스냅샷

삭제 불가능한 골든-카피 스냅샷으로 신속한 데이터 복구 수행

- 사용자 실수 또는 사이버 공격으로 인한 영구적 데이터 손실 방지
- 관리자 권한으로도 삭제 불가능한 보안 스냅샷
- 올-플래시 기반 초고속 복구
- 어레이간 복제를 통한 3-2-1 데이터 보호 전략

Rapid Restore

#2. 대량의 데이터에 대한 초고속 데이터 복구

최대 백업 시간:
90 TB/HR

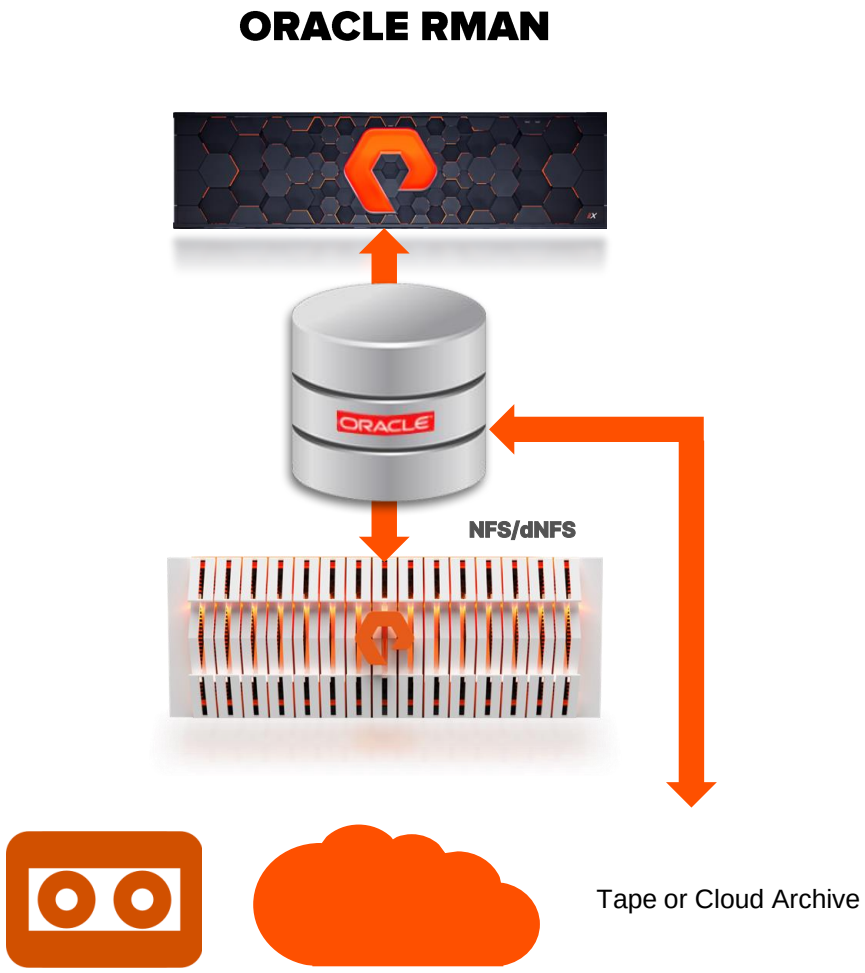
최대 복구 시간:
270 TB/HR

Scale-out 아키텍처:
용량 및 성능 확장

SMB, NFS, S3

오라클 환경의 데이터 보호 전략

Oracle 에서 직접 제공하는 복구 솔루션인 “RMAN" 연동을 통한 최적의 DB 백업 복구 구성

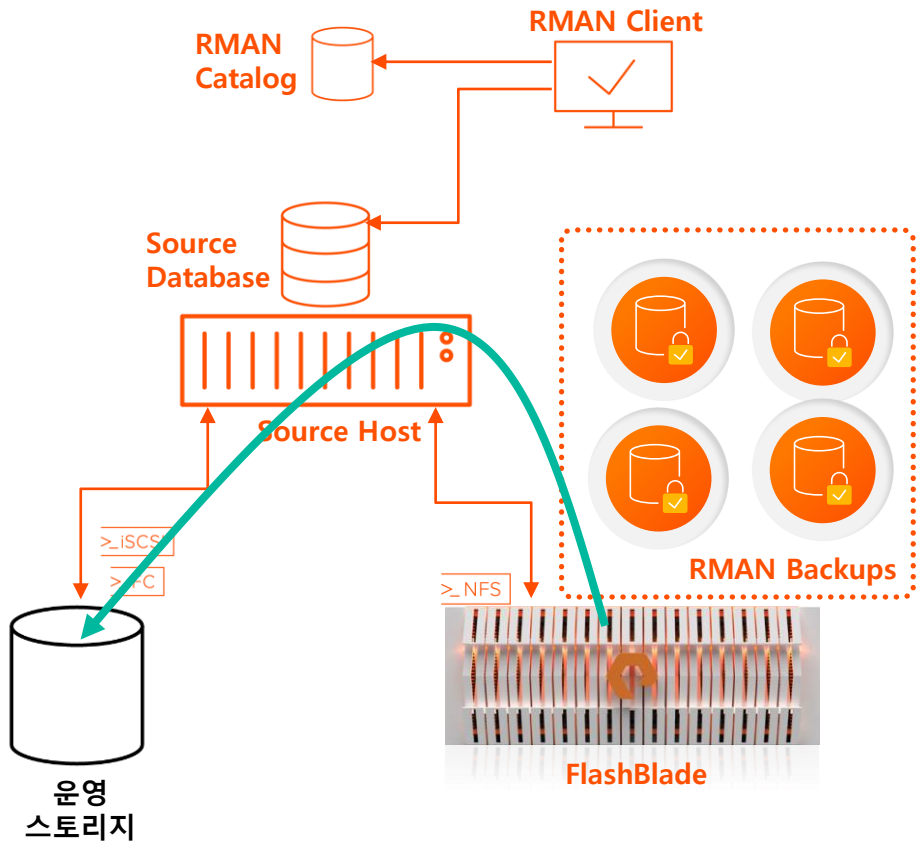


Oracle Recovery Manager(RMAN)

1. Oracle 에서 직접 제공
2. Oracle ZFS Appliance 와 동일 아키텍처
3. dNFS 기반 초고속 백업 성능 지원
4. DBA 최적화 백업 방안
5. Oracle Enterprize Manager 로 관리
6. Incremental Merge 기반 증분 백업 수행

데이터 및 비즈니스 보호 – 초고속 백업 복구

대용량 Oracle DB에 대한 RMAN 기반 dNFS 기반 초고속 백업 복구



Oracle RMAN + dNFS

- 단일 파일 시스템 (15블레이드 기준)
- 초당 **4.5GB 백업** 성능(15TB/hr, 최대 90TB/hr)
- 초당 4GB 복구 성능 (최대 270TB/hr)

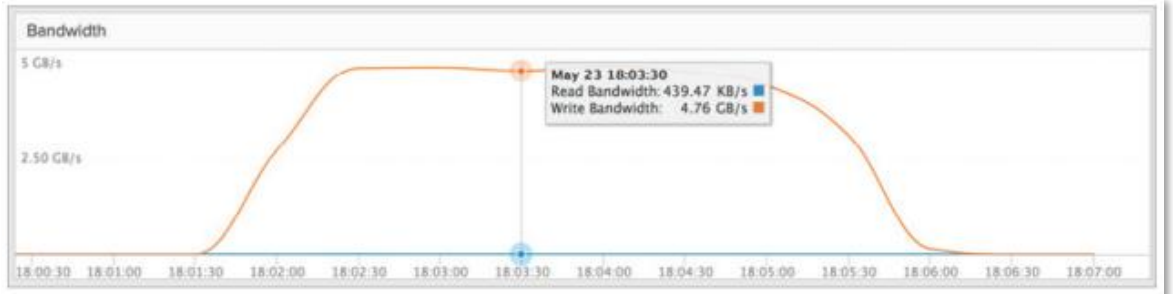


Figure 6. FlashBlade bandwidth

Figure 12. FlashBlade bandwidth

오라클 RMAN 구성 효과

- **dNFS(Direct NFS) 최적화** : 4배 이상 빠른 성능 (백업 90TB/hr, 복구 270TB/hr)
- **백업 데이터 용량 절감** : 3~4배 데이터 절감 효과
- **자유로운 스케일링** : 용량 및 백업/복구 성능 요건에 따라 유연한 확장
- **백업 데이터 활용** : 쉽고 빠르게 테스트/개발을 위한 CloneDB 생성
- **엔터프라이즈 백업** : 데이터베이스 백업 및 다양한 용도로의 데이터 활용성 제공

고성능 SQL 백업

SafeMode를 이용하여 향상된 랜섬웨어 복구 기능 제공

빠른 SQL 백업 및 복원을 통해 가장 까다로운 대규모 SLA 충족

4배 백업 성능 개선
70TB/hr 백업, 43TB/hr 복구 성능
6x9 엔터프라이즈 가용성
성능 영향 없는 상시 데이터 암호화

Backup Speeds

>70 TB/hr

Restore Speeds

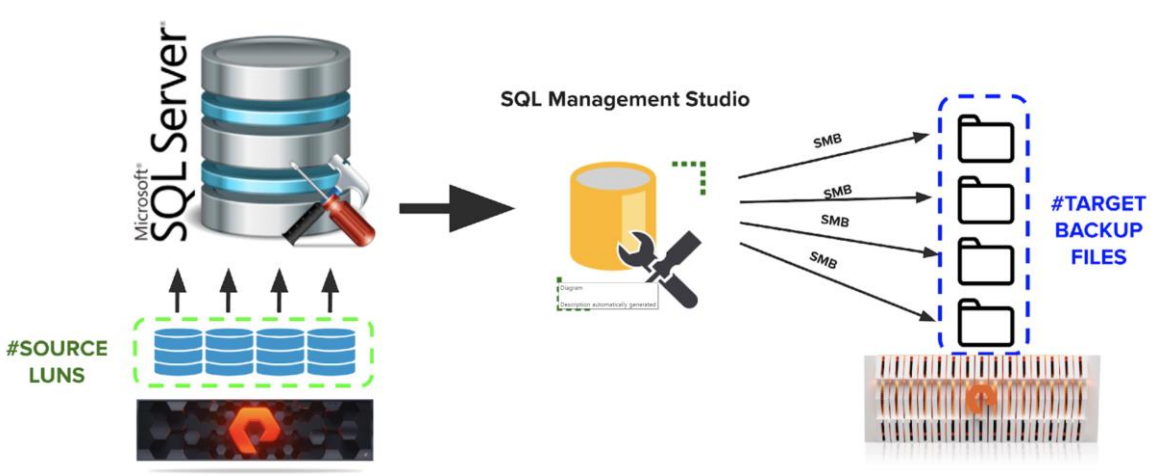
Up to 43.78 TB/hr*

*Restore Speeds may vary depending on SQL Server source storage array

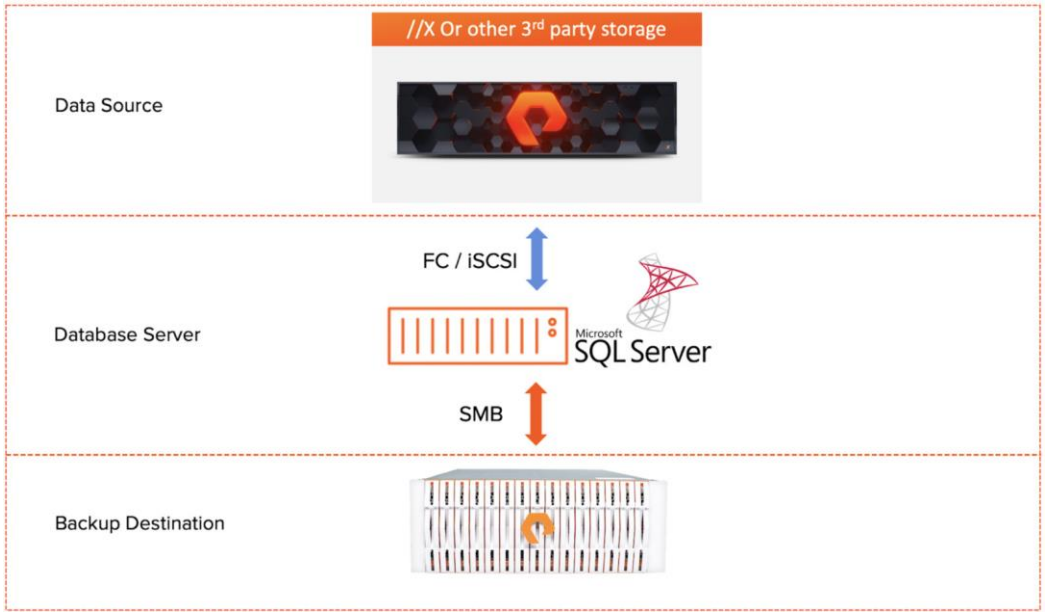
MSSQL 백업 구성 상세

SQL Server Management Studio(SSMS) 를 통해 모든 백업과 복구 수행을 하며, 별도의 백업 소프트웨어 불필요

[물리 구성도]



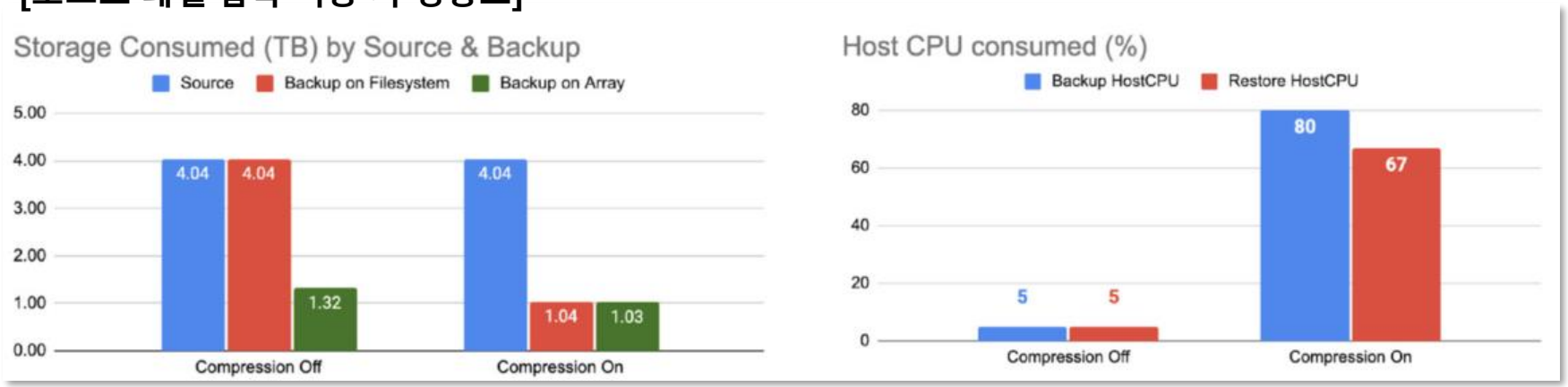
[논리 구성도]



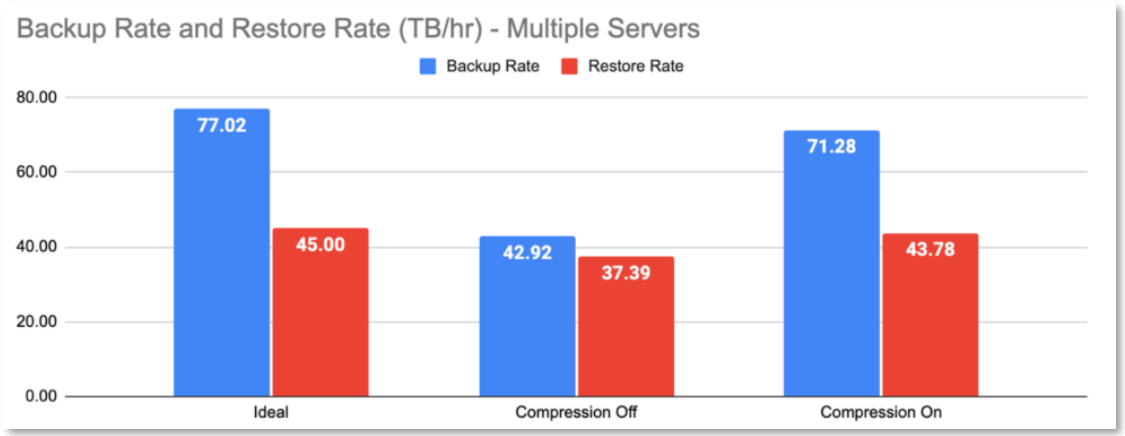
- 운영 스토리지로 FlashArray 또는 3rd Party 스토리지로 구성
- FlashArray 구성 시, SSMS Extension Kit 설치를 통해 SSMS에서 모든 작업에 대한 스케줄링 구성 지원
- SQL Server Management Studio(SSMS)를 통해 모든 백업 및 복구 작업 수행
- FlashBlade의 SMB 프로토콜로 백업 타겟 디렉토리 지정 및 백업 복구 수행

MSSQL 백업 및 복구 성능

[호스트 레벨 압축 적용 시 영향도]



[멀티 SQL 서버 환경에서의 백업/복구 성능]

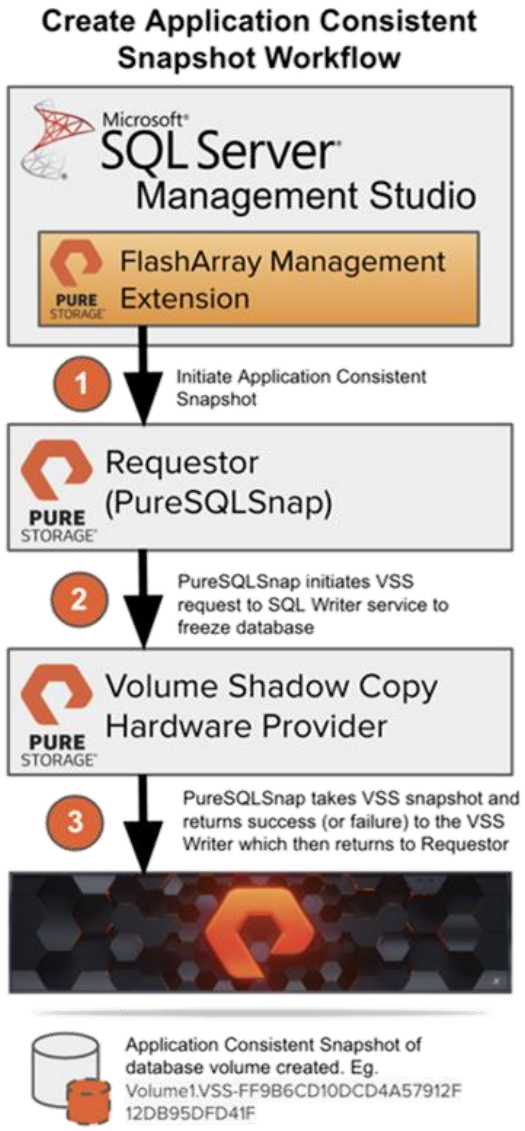


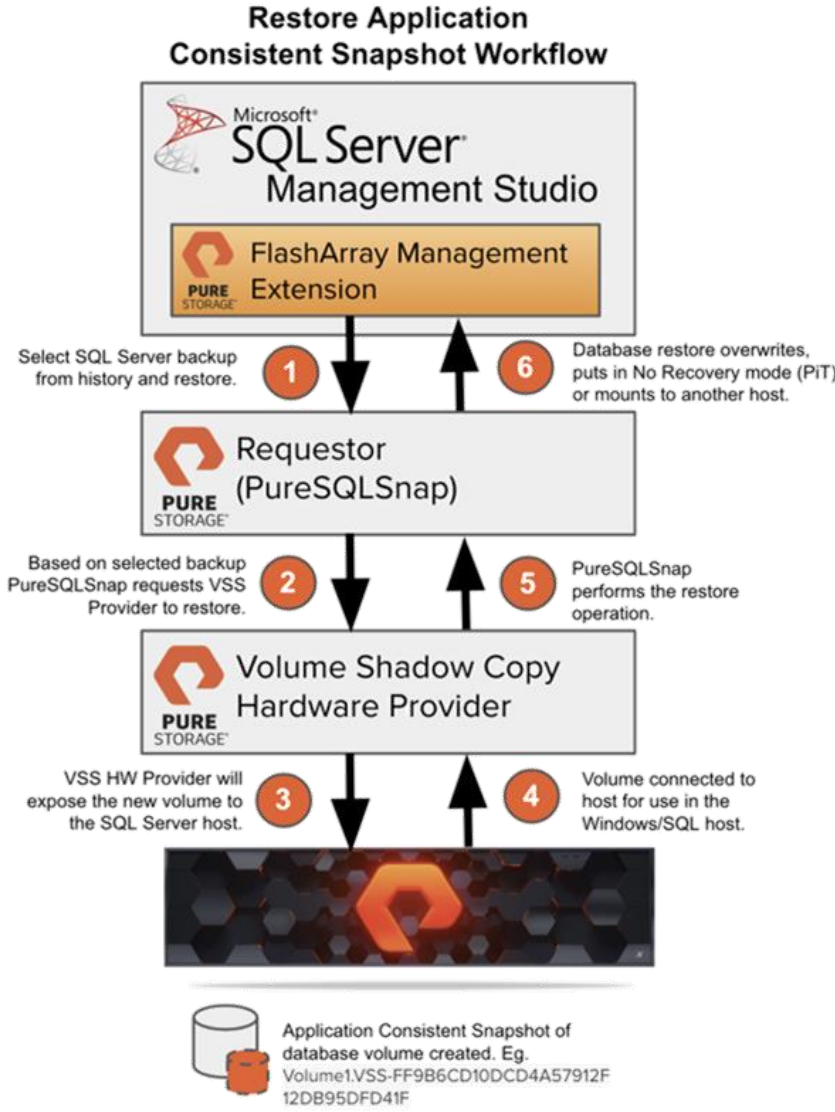
[SUMMARY]

- 호스트 레벨 압축 시 CPU 리소스 67~80% 이상 사용
- 스토리지 압축 사용 시, CPU 리소스 및 용량 절감 확인
- 멀티 SQL 환경에서 최대 77TB/hr 백업 성능 확인*
- 멀티 SQL 환경에서 최대 45TB/hr 복구 성능 확인*

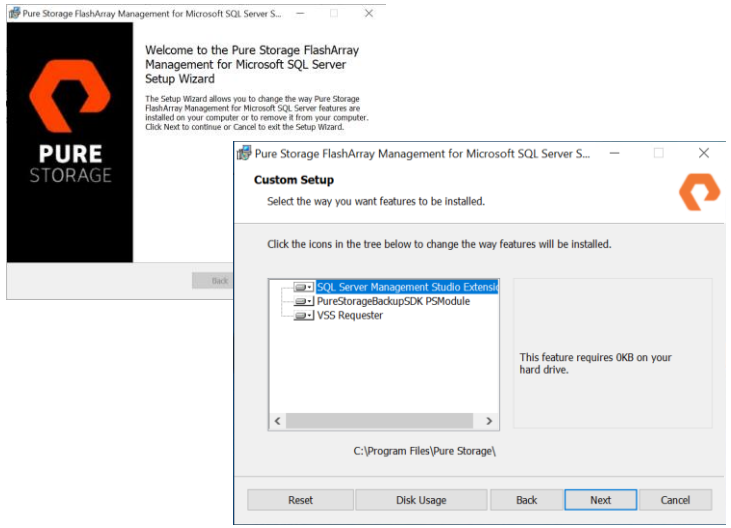
**** 30블레이드 환경에서 측정 및 SQL 서버 운영 스토리지의 read/write 성능에 영향을 받음***

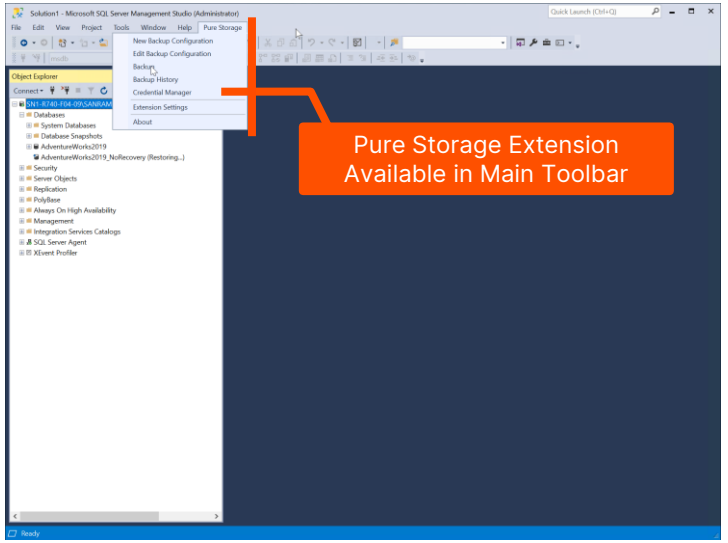
SSMS Extension Kit

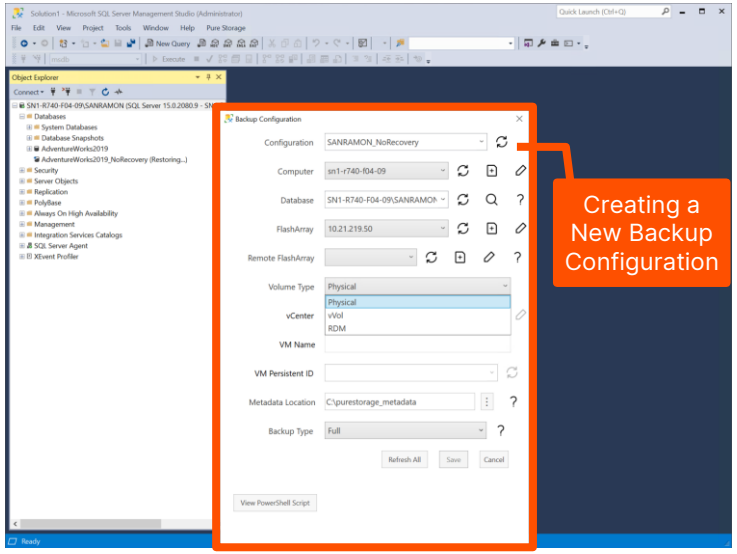


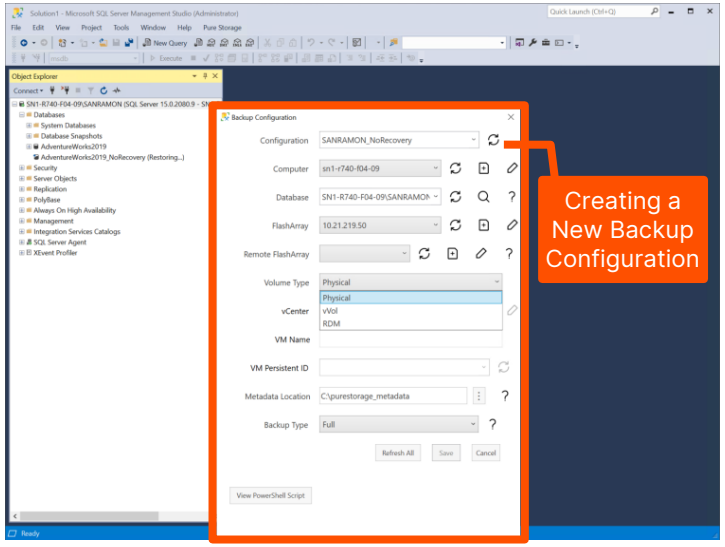


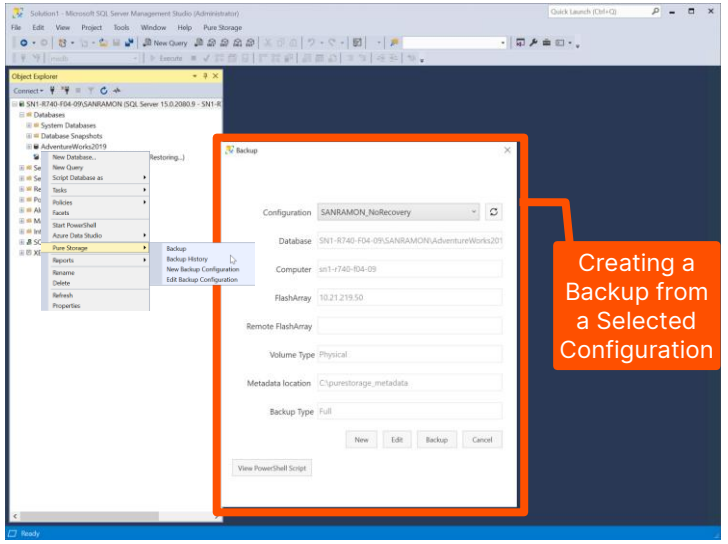
FlashArray 환경에서의 SSMS Extension 구성 예시

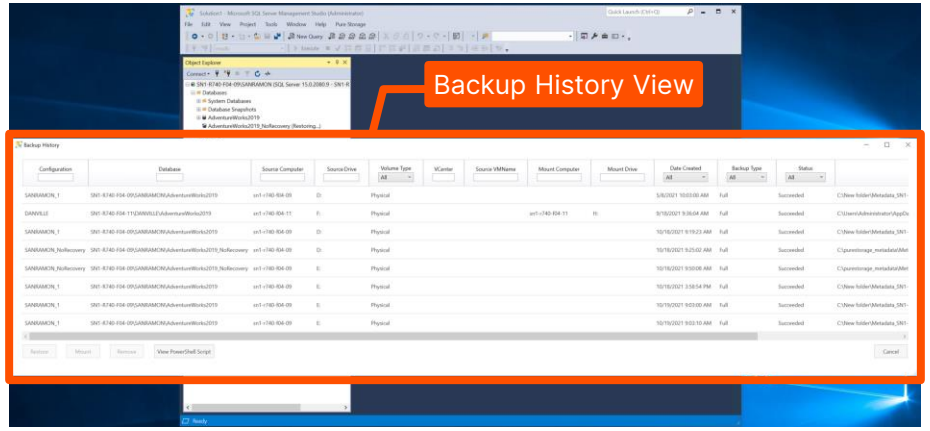




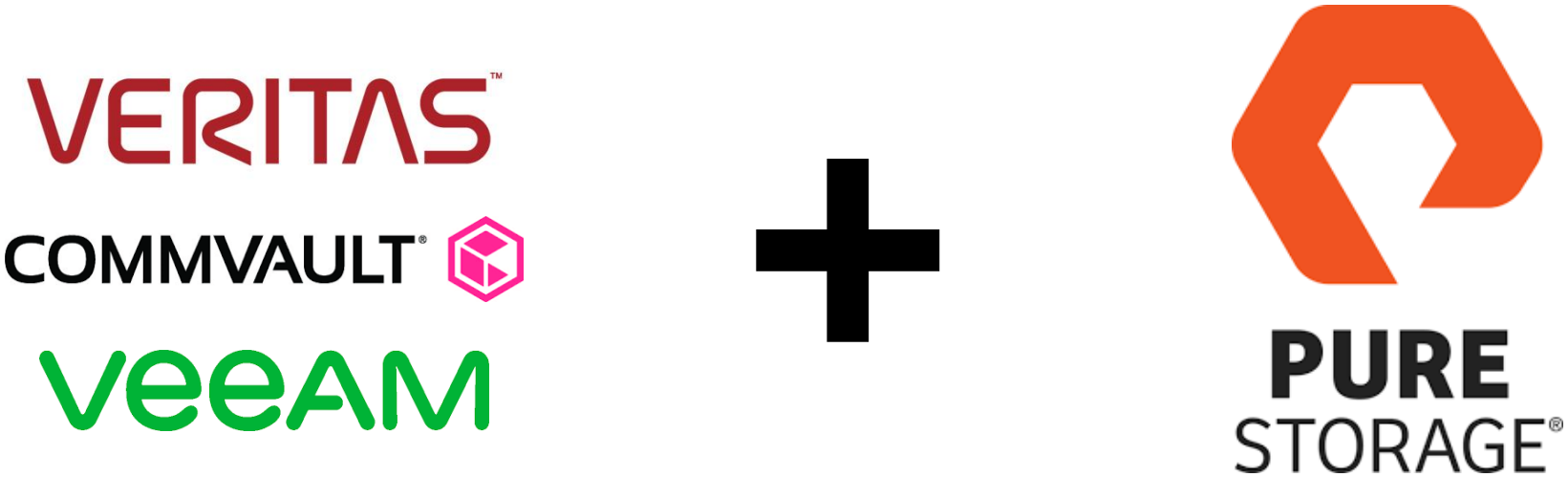








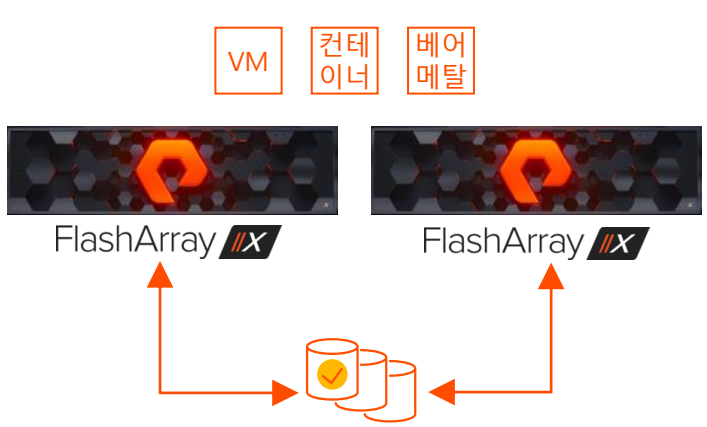
전략적 기술 파트너쉽



Rapid Restore 를 통한 비즈니스 보호

맺음말: 3-2-1 + F2F2C의 결합을 통한 서비스 무중단 완성

3개 이상의 복제본 | **2개 이상의 스토리지 저장소** | **1개 이상의 오프사이트 소산**



ActiveCluster 운영 스토리지 이중화

- 대상 업무: 운영 데이터
- 보호 방식: AADC 이중화 + 스냅샷 정책 설정
- 보호 용도: 논리적/물리적 장애
- 보호 레벨: 무중단 서비스

SafeMode를 통한 랜섬웨어 방지

DR 복제

3rd Party 백업 솔루션 연동

초고속 백업 / 복구

- 대상 업무: DB(Oracle/MSSQL/etc.)
- 보관 주기: ~ 2주
- 백업 용도: 최근 데이터 고속 복구

SafeMode 를 통한 랜섬웨어 방지

백업 솔루션 연동

- 대상 업무: 전체 통합 백업
- 보관 주기: 기업 SLA 준수(D/W/M/Y)
- 백업 용도: 백업 정책에 따른 데이터 보호

SafeMode 를 통한 백업 카탈로그 / 데이터 보호

Offsite 복제(온프렘/클라우드)

- 대상 업무: 전체 DR 통합
- 보관 주기: Daily / Monthly
- 백업 용도: 오프사이트 데이터 DR

SafeMode 를 통한 데이터 보호

Question?