HS 효성인포메이션시스템 | Hitachi Vantara

[Cyber Resilience Insight 2026]

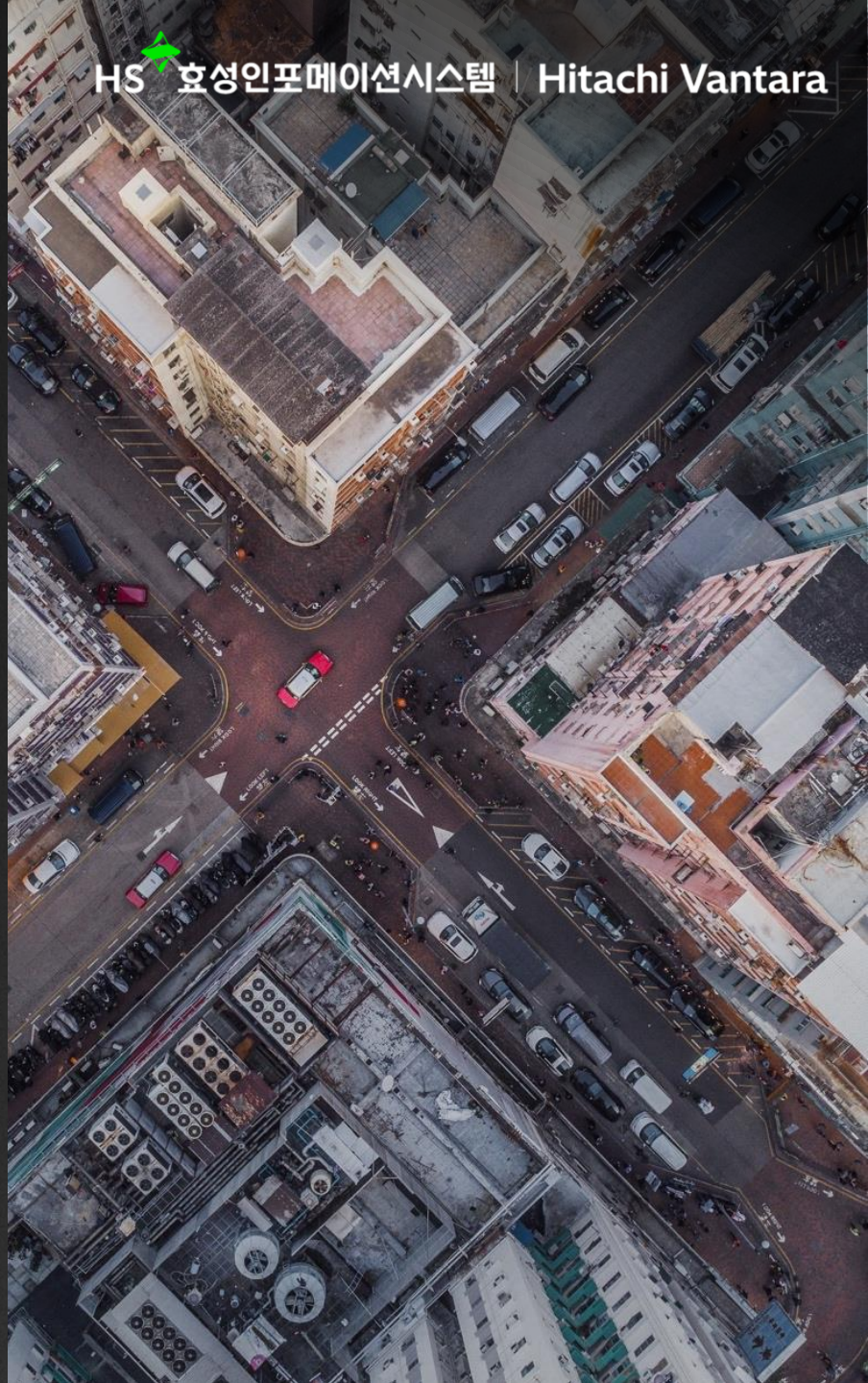
무중단 서비스를 위한 Cyber Resilience 완성 전략

양 경 모 PM
HS효성인포메이션시스템 SA팀

Agenda

1. IT 시스템 장애의 현주소
2. 비즈니스 연속성 확보방안
3. 사이버 공격으로부터 데이터 보호방안

Ⅰ.
IT 시스템 장애의 현주소



Black Swan의 오늘날

IT 시스템의 블랙스완(Black Swan) 시대

블랙스완(Black Swan) 현상은
도저히 일어날 것 같지 않지만 일단 발생하면 엄청난 충격과 파급력을 가져오는 예측 불가능한 사건을 의미함

25년 주요 IT 시스템 장애 사례

IT 시스템 장애 사례

24년 Crowd Strike 장애 글로벌 금융 및 항공 서비스 장애	23년 공공기관 인프라 장애로 인한 행정업무 중단	22년 데이터 센터 화재로 인한 대형 플랫폼 서비스 중단
21년 안드로이드 Web view 오류로 인한 메신저, 플랫폼 앱 대규모장애	13년 3.20 방송·금융 전산 대란 (3.20 사이버공격)	09년 7.7 디도스(DDoS) 대란
20년 K증권 전산장애 (프로그램 오류, 대규모 투자자피해)	11년 N은행 전산망 장애 뱅킹/카드 승인 등 서비스 마비	07년 증권 거래소 전산 장애
18년 KT 아현지사 통신구 화재	11년 9.15 대규모 정전사태	06년 A은행 전국 영업점 전산마비
14년 거래소 국고채 3년물 매매중단 전산장애	10년 금융회사 동파로 인한 전산마비	05년 거래소 주식 매매 지연

최근의 IT 시스템 장애는

화재, 시스템 장애, 해킹 등 ... 디지털 재해는 예고 없이 찾아옵니다.

과거

정전, 화재, 인프라 및 센터 장애

오늘

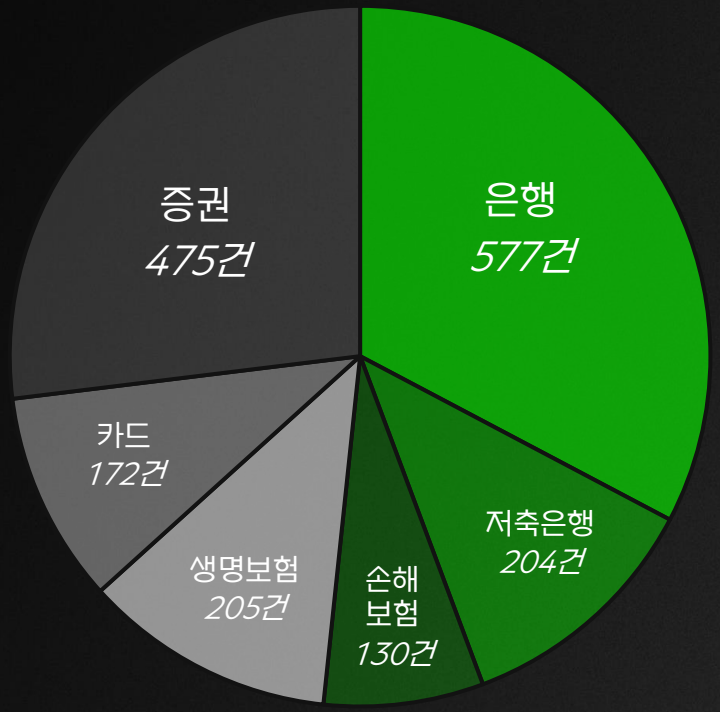
사이버 공격, 랜섬웨어, 해킹 및 데이터 유출

재해복구(DR)의 중요성 증대

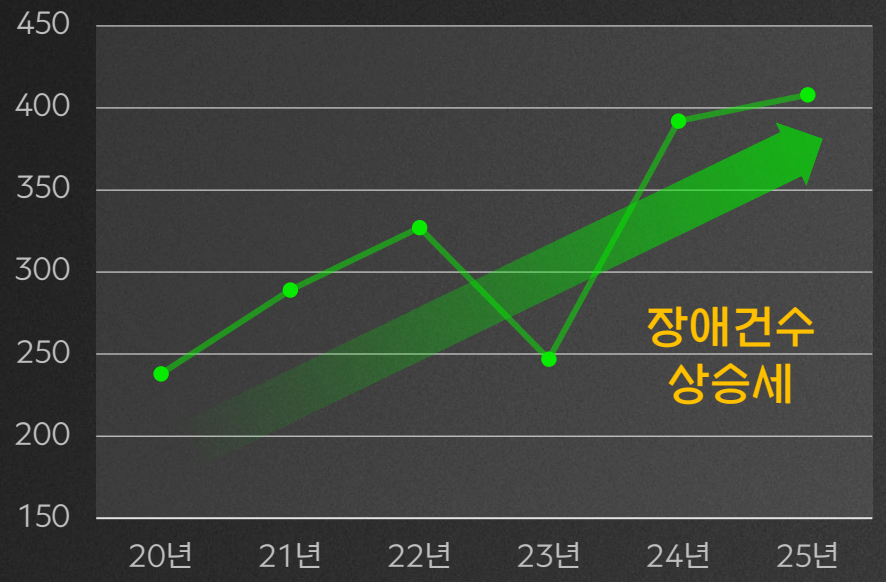
증가하는 IT 시스템 장애 피해규모

- 최근 5년간 금융부문 IT 시스템 장애 총 1,763건
- IT 시스템 장애 피해금액 약 259억원

업종별 최근 5년간 누적 장애건수

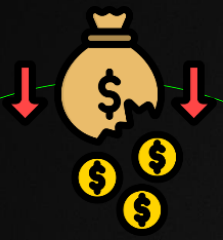


최근 5년간 장애 발생 건수



자료 출처 : 금융감독원 '국내 금융업권 전산장애 발생현황 '

IT 시스템 장애의 영향



막대한 재정적 손실

- 서비스 마비 기간의 직접 매출/거래 손실, 복구 작업에 투입되는 비상인력
- 비용 및 장비 교체 비용

고객 신뢰도 추락

- 대고객 서비스 중단은 단순 불편을 넘어 일상 마비 초래
- 고객 불만이 폭주하고 기업 전체의 신뢰도 손상

법적 및 규제 준수 문제

- 데이터 보호의무 위반으로 인한 과징금, 금융감독기관 관련법규 미준수에 따른 행정 처벌

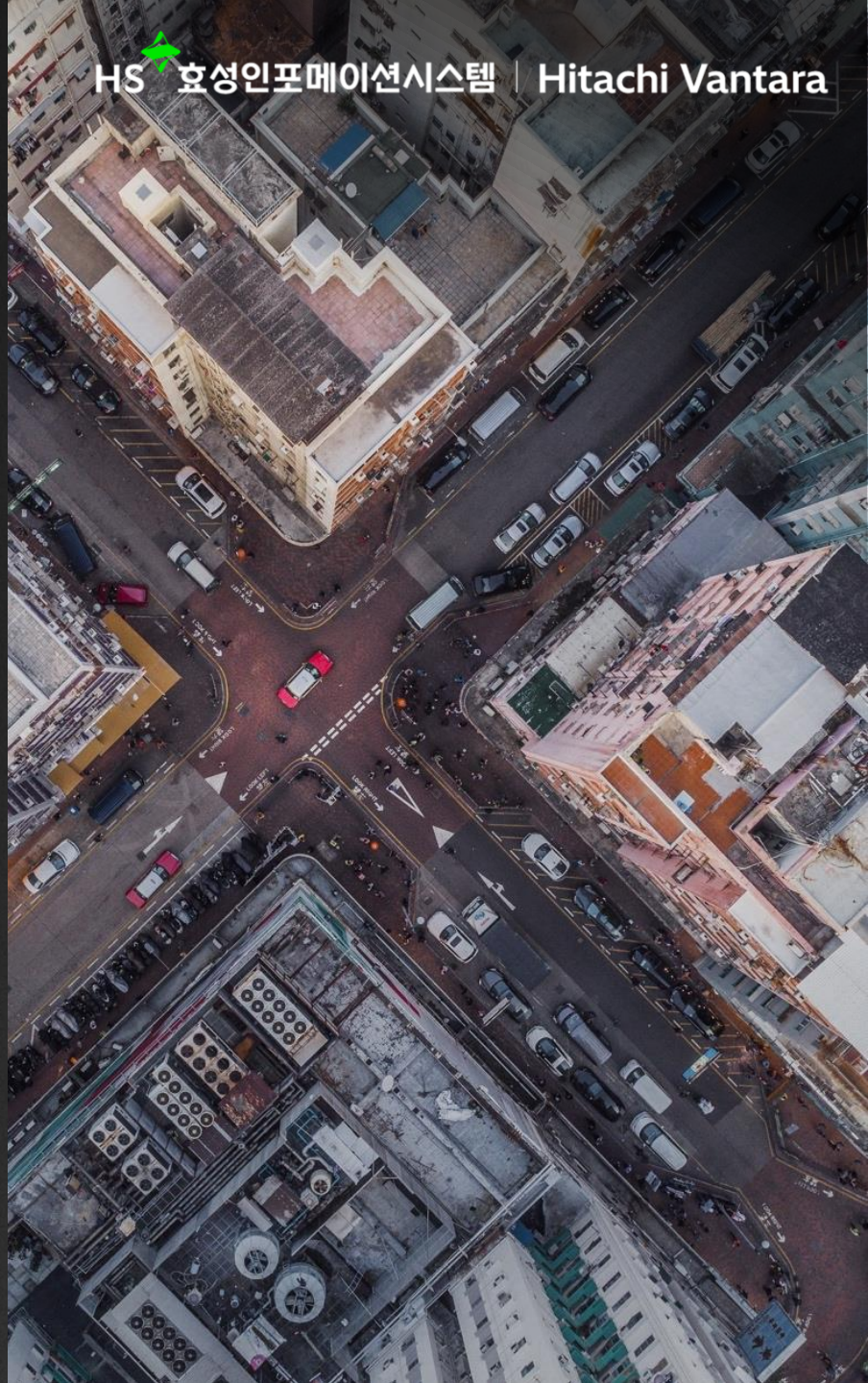
IT 시스템 장애가 발생하면

데이터 손실을 최소화 하며 **RPO = Zero**

서비스 복구를 신속히 **RTO = Zero**

비즈니스 연속성을 확보하는 것이 핵심

II.
비즈니스 연속성 확보방안



비즈니스 연속성을 위한 고려요소

- 재해복구는 DR시스템의 구축에 그치는 것이 아닌 서비스의 연속성을 확보하는 것이 핵심 전략

RPO
(Recovery Point Objective)

서비스 데이터를 복구할 때
어느 시점까지 복구할지에 대한 목표

재해발생 시점
(Disaster Event)

RTO
(Recovery Time Objective)

재해 발생 이후 서비스 복구에
걸리는 시간에 대한 목표

데이터 손실 (Lost Data)

서비스 중단 시간 (Down time)

Seconds	Seconds
Hours	Hours
Days	Days
Weeks	Weeks

업무 중요도별 재해복구 수준 결정

주센터와 재해복구센터는 1:1 자원 구성 필요

Mirror Site

- 주 전산센터와 동일한 시설/ 전산 기기/ 네트워크 등 확보
- 양 센터에서 동시에 데이터를 처리 및 운영하며, 재해발생 시 즉시 전환 가능

Hot Site

- 주 전산센터와 거의 동일한 수준의 시설/ 전산 기기/ 네트워크 자원 확보
- 데이터를 실시간 이중화 하며, 재해발생 시 수 시간 이내에 대체 가능

Warm Site

- 기본 시설, 주요 전산 기기 및 네트워크 확보
- 하루 전 데이터를 백업 센터로 소산하며, 재해 발생 시 수 일 내 대체 가동

Cold Site

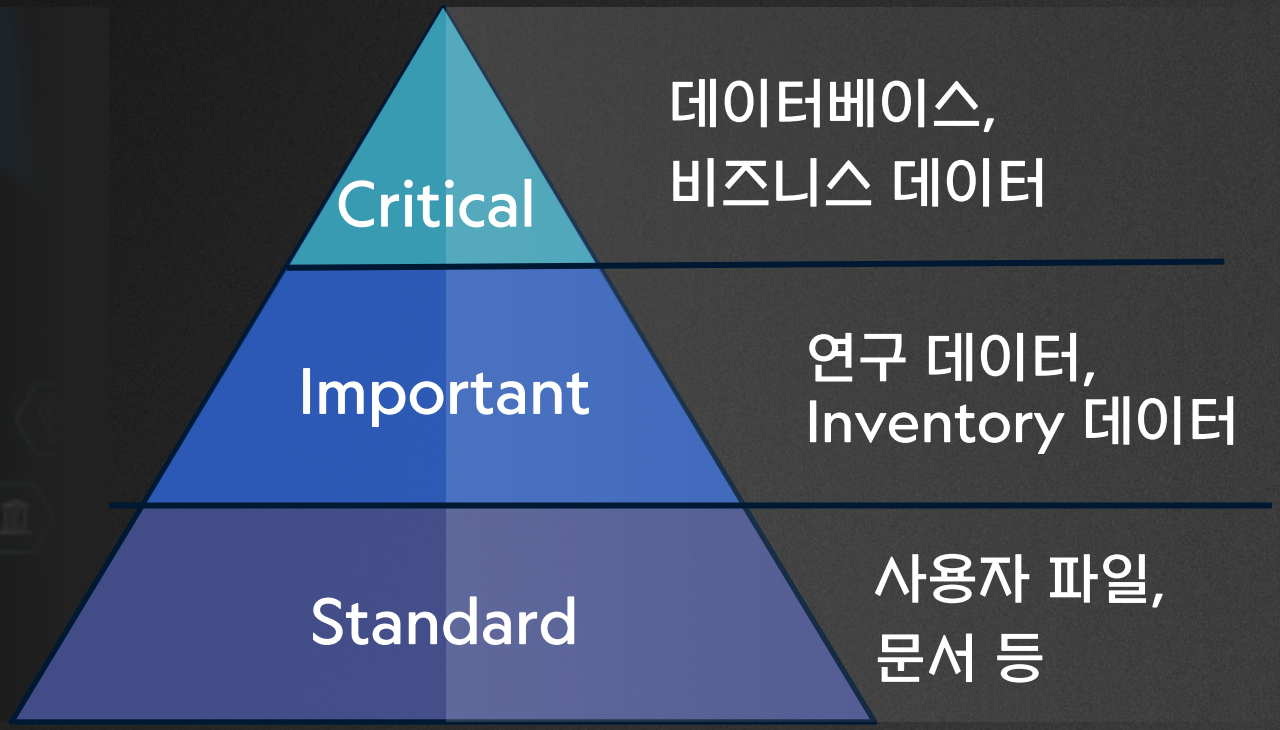
- 기본 시설만 확보
- 재해발생 시 전산 기기 도입 및 네트워크를 구축하여 대체 가동 (한 달 내외)

비용 및 난이도 증가

복구 소요시간 및 손실율 증가

핵심 데이터 보호의 중요성

핵심 데이터를 안전하게 보호 = 비즈니스 연속성 확보



실시간 데이터 보호의 중요성

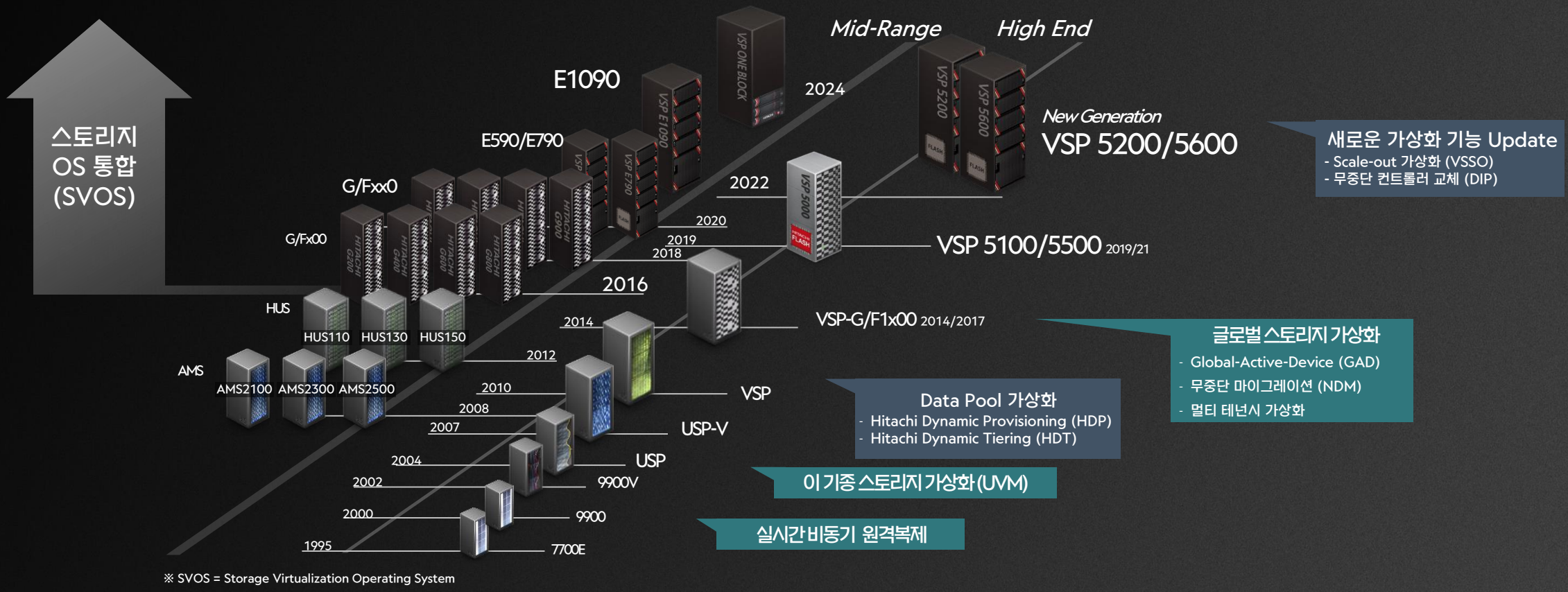
비즈니스 연속성의 핵심은 실시간 데이터의 보호

백업
시점 데이터 보관
데이터 복원

스토리지
실시간 데이터 보호
서비스 복구

30년 이상 진화한 Hitachi 스토리지 history

- 스토리지 컨트롤러기반 Active/Active 미러링 솔루션 (RTO & RPO = 0)
- 완벽한 스토리지 이중화 Active-Active구성으로 센터 장애에 대비한 서비스 연속성 제공
- 이중 쓰기 및 로컬 읽기 지원하여 스토리지 자원 100% 활용하여 성능 향상
- 국내 최다 Active-Active 구현 사례 보유 및 다양한 운영 환경에서 검증된 스토리지 솔루션

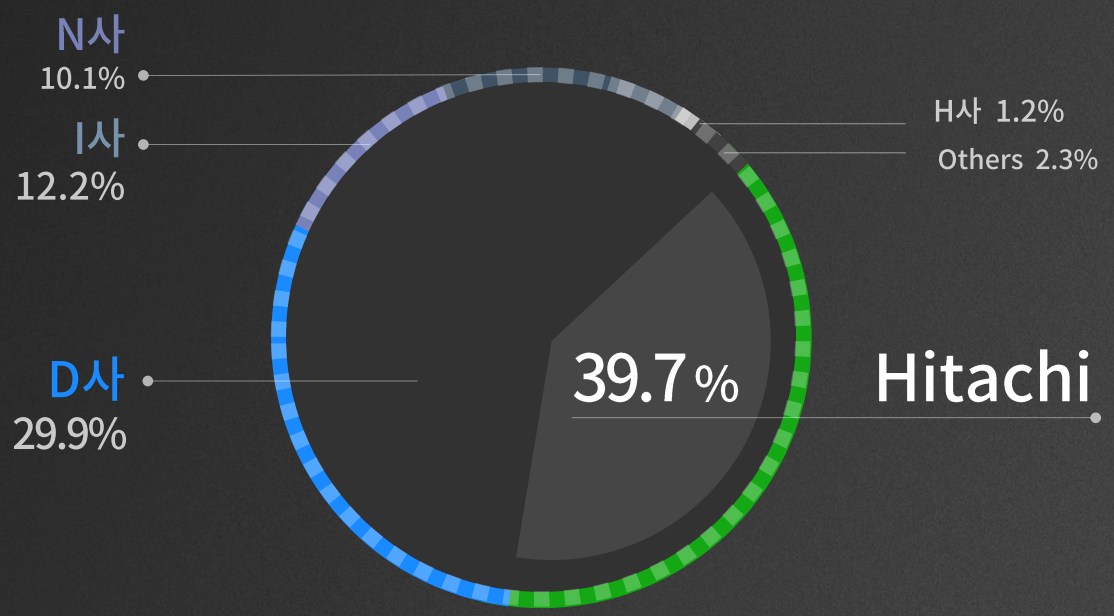


※ SVOS = Storage Virtualization Operating System

시장 점유율 1위의 Hitachi 스토리지

국내 스토리지 시장 선도

하이엔드 시장
12년 연속 *1위!*
2025년 *1위!*



하이엔드 벤더별 점유율	2022 Total	2023 Total	2024 Total	2025 Total
Hitachi	39.5%	42.1%	41.2%	39.7%
D사	39.2%	24.7%	25.7%	29.9%
I사	4.4%	16.4%	14.0%	12.2%
N사	8.7%	6.3%	11.1%	10.1%
H사	3.4%	3.6%	2.2%	1.2%
Others	4.9%	7.0%	5.8%	2.3%

검증된 최고의 데이터 보호 솔루션

Hitachi 스토리지 기반의 데이터 보호 솔루션

Sync
고속의 실시간 동기 복제

실시간 복제 솔루션

운영과 DR 스토리지에 동일한 데이터를 저장하는 복제 솔루션

Async
Hitachi Only

업계 유일 실시간 비동기 복제

전 모델 동일 DR솔루션 탑재

Hitachi 라인업 간 복제 지원, 유연하고 효율적 구성 지원

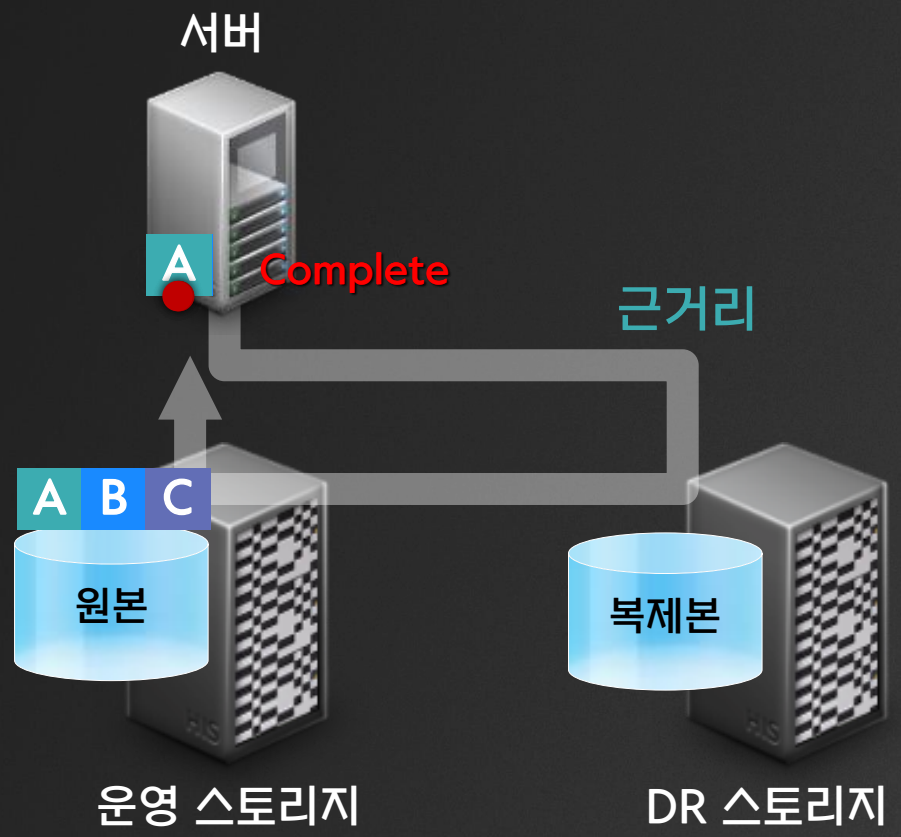
Sync
Hitachi Best!

국내 최다, Active-Active 미러링

무중단 스토리지 Active-Active 미러링

RPO/RTO=0
국내 최다 구축

Sync 방식의 데이터 보호 솔루션



☑ 응답 성능 영향 최소화가 중요

- 원본과 복제의 완벽히 일치
- RPO=0
- Low latency Protocol
  : Fiber Channel, DWDM …
- 거리: 100km 이내 (Latency)

Sync 방식의 한계

동기 복제가 성능에 미치는 영향에 대한 뼈 아픈 사례는
9/11 사태 이후 드러났다.

미국 규제 당국은 테러 공격 당시 드러난 취약점에 대응해
데이터 보호 및 재해 복구 기능을 강화하기 위해
금융 기관 300마일(480km) 이상의 거리에
동기식 복제를 구현하도록 의무화하려고 했다.
그러나 사이트 간 지연 시간이 엄청나게 길어
결국 이 계획을 포기했다.

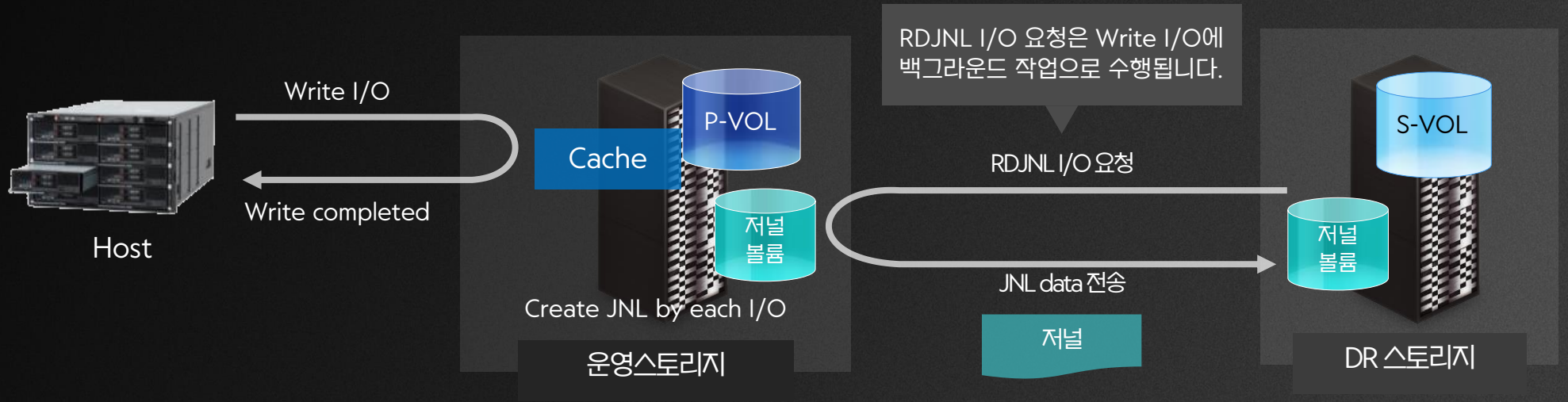
원문보기: https://www.itworld.co.kr/news/303595#csidxb1cc1dfc73a8a87abdbe9a9d86c29d5

Hitachi 원격지 재해복구 솔루션

Hitachi Only

업계 최고 실시간 비동기 DR 솔루션 Universal Replicator

- Async 방식이지만 실시간 데이터 전송을 통해 RPO를 Zero 지원
- 변경된 DATA의 시퀀스 넘버와 비트맵 관리를 통해 100% 데이터 정합성 보장
- 운영 스토리지의 별도 저널 영역에 변경 데이터를 보관하고 있어 전송 회선 장애 시에도 높은 저항력 확보
- 전송 대역폭 조절 기능을 통해 시스템의 영향을 최소화 하며 안전한 데이터 복제를 지원



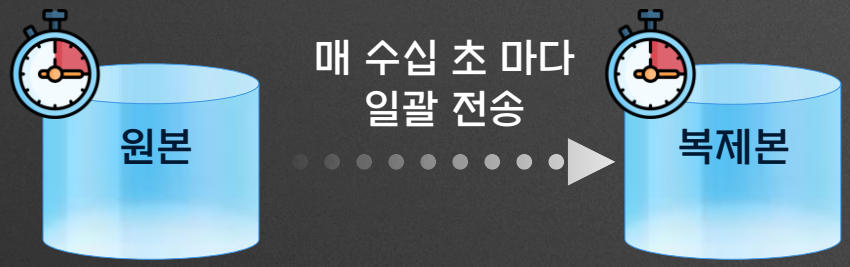
장거리 재해복구 전송 방식 비교

Hitachi UR 방식

- 데이터가 들어오면 바로 전송하는 방식으로 데이터 손실 없음 (Near RPO = 0)
- 별도의 저널 공간을 통해 회선 병목시에도 DR복제 지속 가능
- 데이터 전송 시 시퀀스 넘버를 통한 완벽한 데이터 정합성 보장

VS

타 사 방식



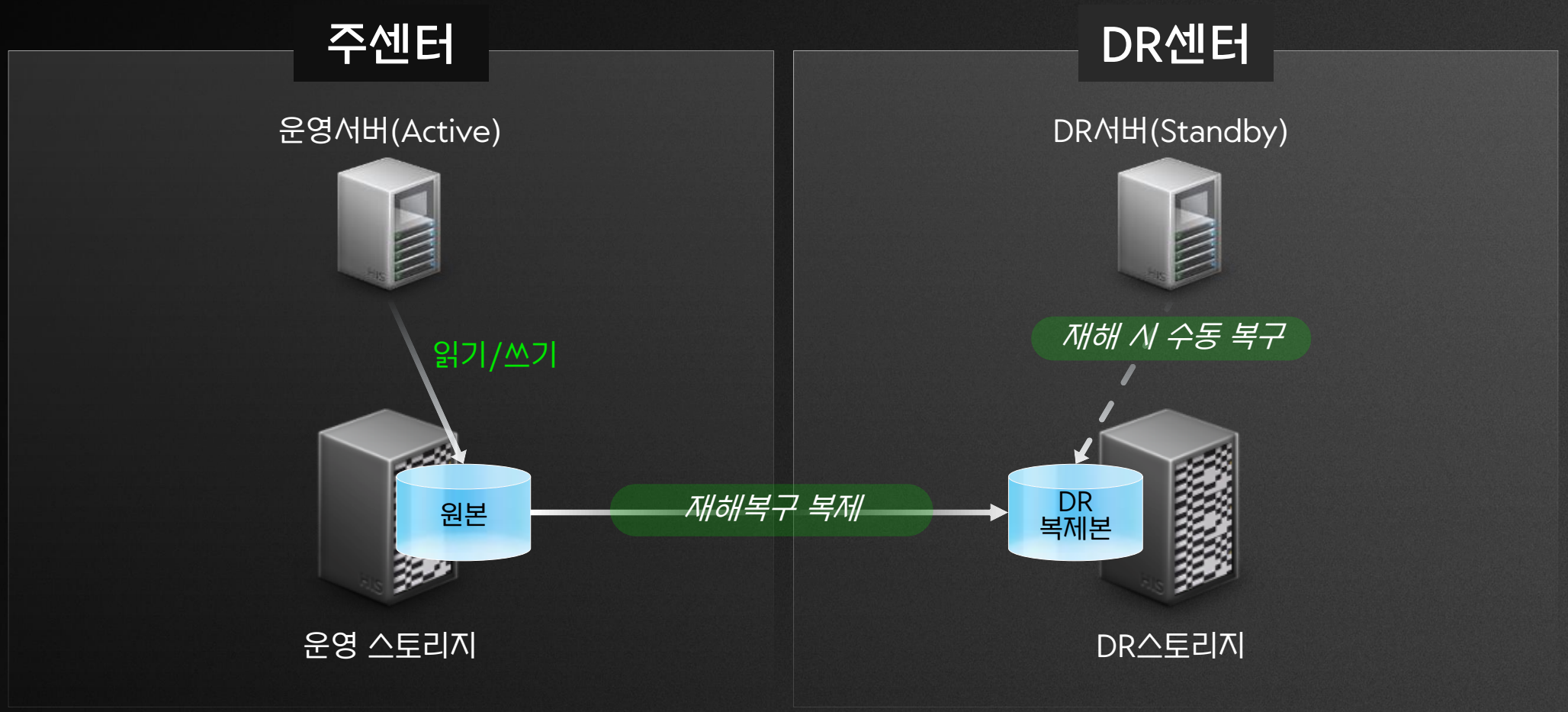
- 설정된 전송 주기(초~분) 마다 일괄 전송 (전송 주기 만큼 데이터 손실)
- 전송 거리에 따른 오버헤드 발생
- 변경량이 많은 경우에 회선 대역폭 병목이 생기면 DR복제가 끊어짐

Hitachi 장거리 복제 구성 사례

고객사	주센터	DR센터	거리(직선)
금융권 OO은행	서울 역삼	대전	132 km
금융권 OO중앙회	대전	서울 역삼	131 km
금융권 OO거래소	서울 여의도	부산	327 km
금융권 OOOO결제원	서울 여의도	부산	326 km
대형 제조사	경북 구미	미국 뉴저지	수 천 km

기존 재해복구 시스템 구조

- Active-Standby 형태의 재해복구 구조



기존 재해복구 시스템 구조

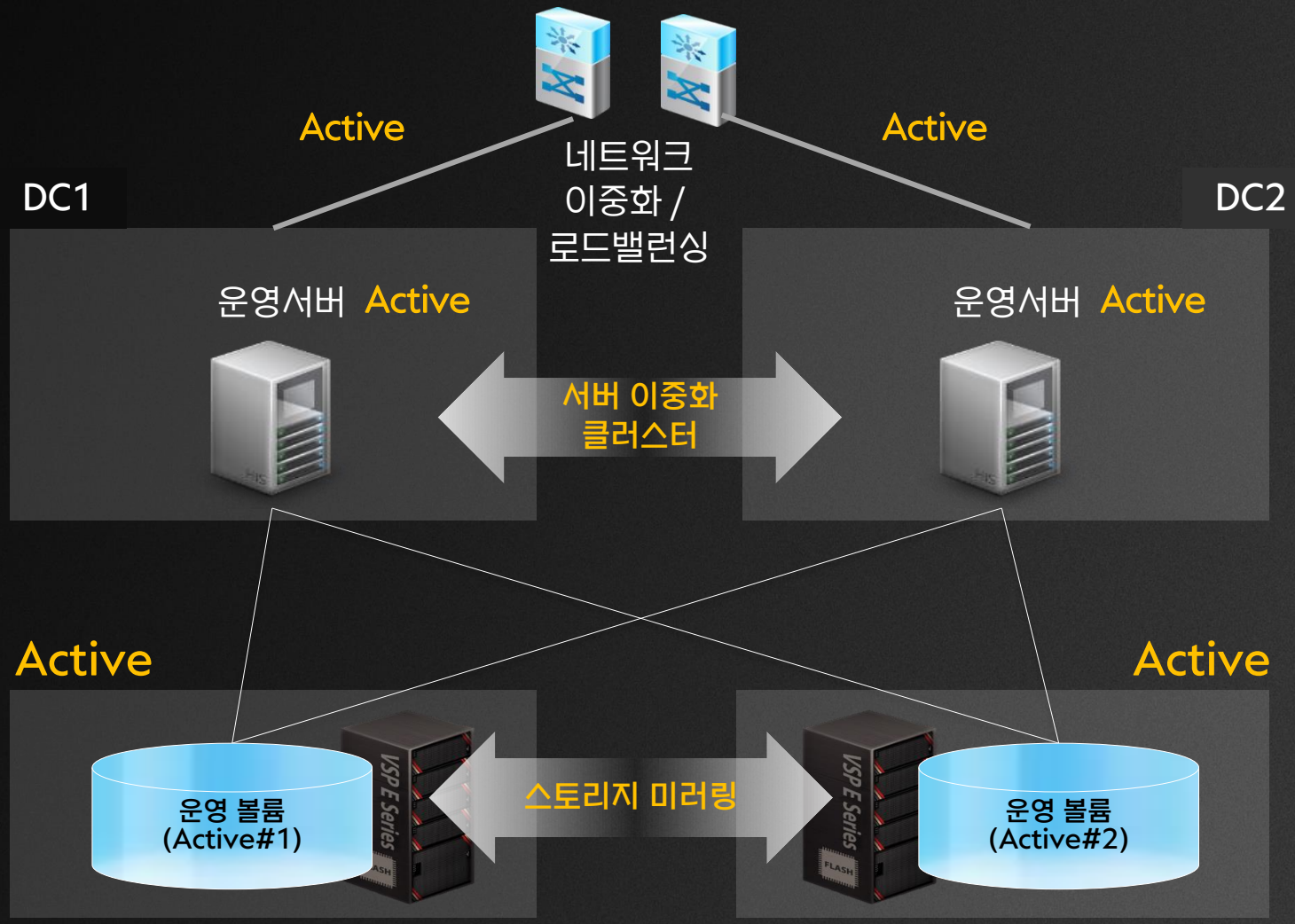
- Active-Standby 형태의 재해복구 구조

Active-Standby 재해복구의 한계점

- 장애로 인한 DR(Stand-by) 전환 시 **서비스 중단 발생**
- DR센터로 서비스 전환 시 수동 개입에 따른 **복구시간 증가**
- 비동기 방식의 데이터 보관을 수행함으로 **데이터 손실 우려 (RPO 증가)**
- DR센터 전환 후 기존 운영 서비스 **성능저하 우려**
- 실제 재해 상황에서의 전환 **절차 및 운영의 복잡성**

재해복구 시스템의 진화

- Active-Active 형태의 재해복구 구조



Active 데이터 센터를 위한 스토리지 요건

- Active-Active 데이터 센터 구축을 위해 갖춰야 할 스토리지 구축 요건

저지연 고성능 아키텍처 구조

Active-Active LUN (Dual-Access) 제공

DATA 쓰기 동시성 및 정합성 보장여부

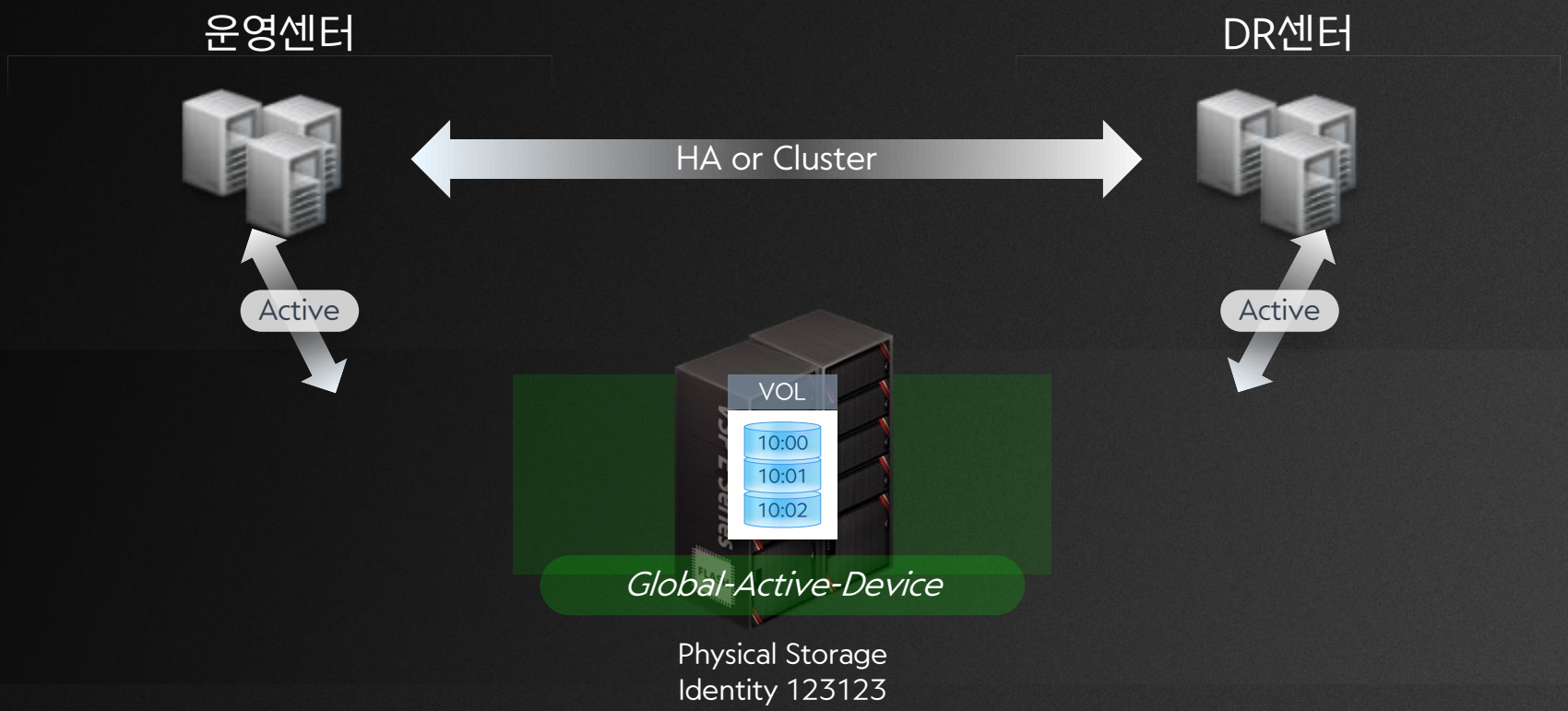
목표 RPO/RTO 충족 가능 여부

자동 장애 전환(Fail-over) 지원

Hitachi Active-Active 솔루션

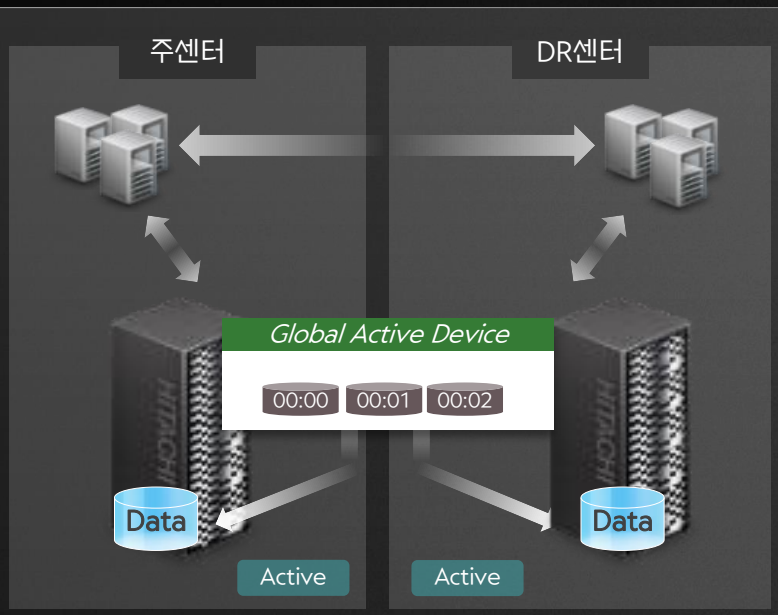
- 스토리지 컨트롤러기반 Active/Active 미러링 솔루션 (RTO & RPO = 0)
- 완벽한 스토리지 이중화 Active-Active구성으로 센터 장애에 대비한 서비스 연속성 제공
- 이중 쓰기 및 로컬 읽기 지원하여 스토리지 자원 100% 활용하여 성능 향상
- 국내 최다 Active-Active 구현 사례 보유 및 다양한 운영 환경에서 검증된 스토리지 솔루션

스토리지 미러링 기술 'GAD'



Hitachi Active-Active 솔루션 비교

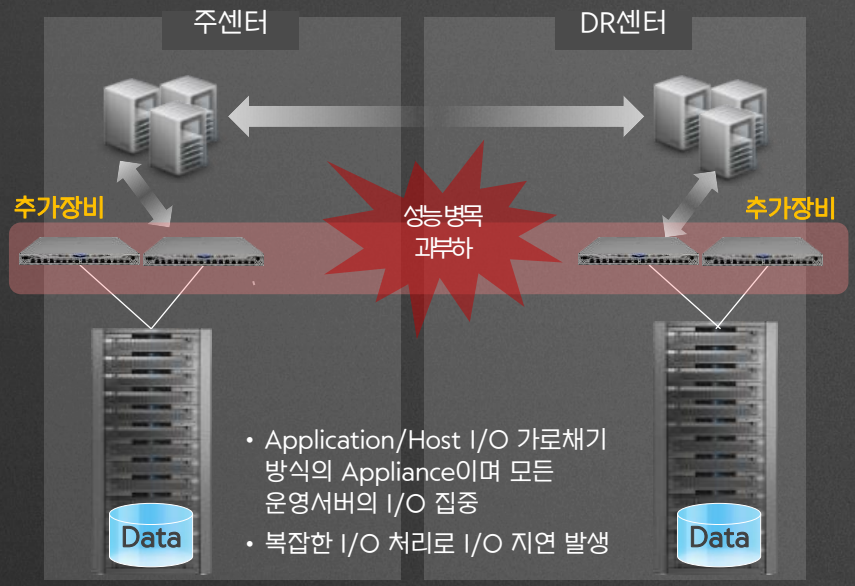
Hitachi GAD 방식



- 별도의 어플라이언스 추가 없이 스토리지 컨트롤러에서 스토리지 미러링(GAD) 제공
- 모든 I/O를 스토리지 레벨에서 처리하게 되므로 I/O지연 없이 고성능 제공

VS

타 사 방식



- Application/Host I/O 가로채기 방식의 Appliance이며 모든 운영서버의 I/O 집중
- 복잡한 I/O 처리로 I/O 지연 발생

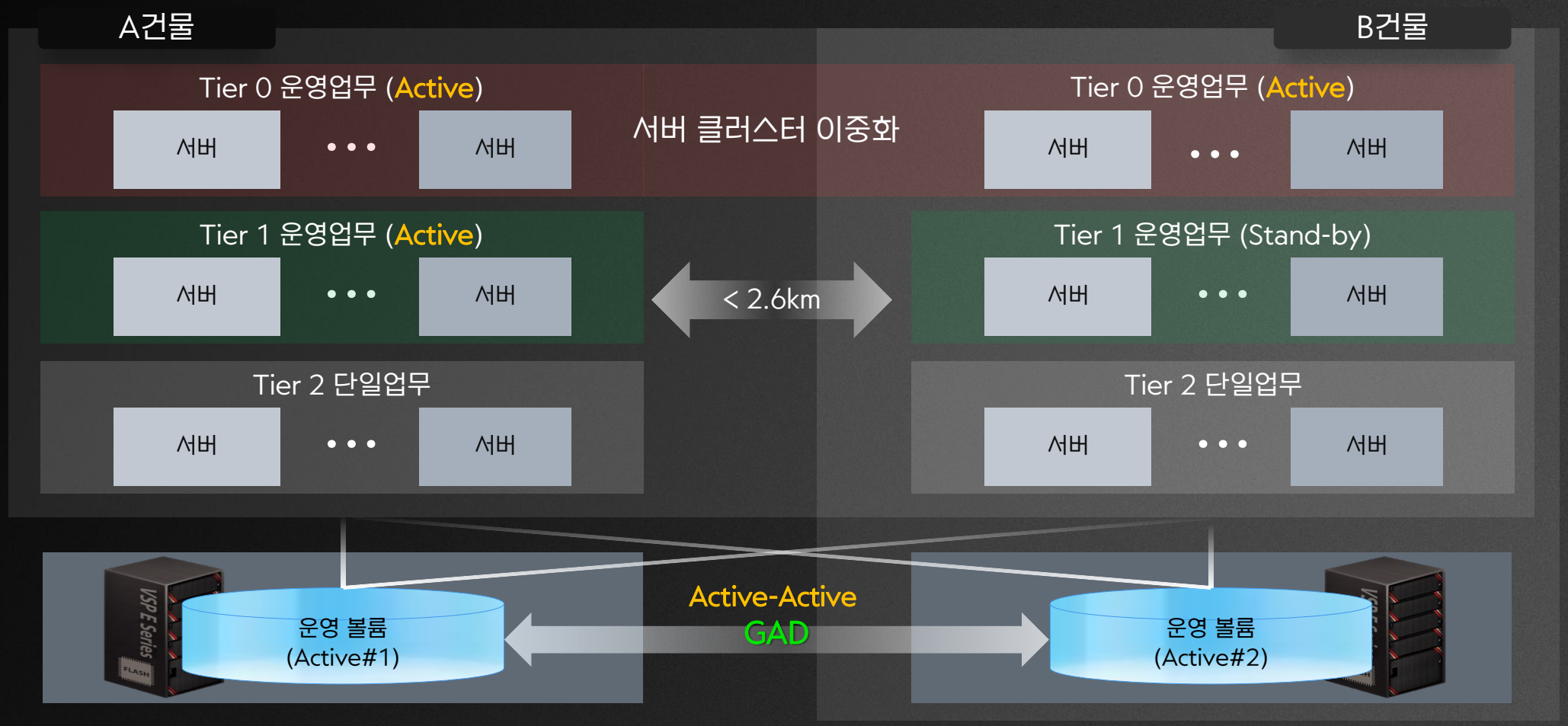
- 스토리지 미러링을 지원하지 않으므로 별도의 어플라이언스 필요
- 모든 I/O를 별도 어플라이언스에서 처리하게 되는 구조로, 성능 병목현상을 갖는 요소가 됨
- 2대의 스토리지의 정합성 및 운영관리를 위한 심판자 역할을 하는 쿼럼이 외부 클라우드에 위치

Hitachi Active-Active 솔루션 적용사례

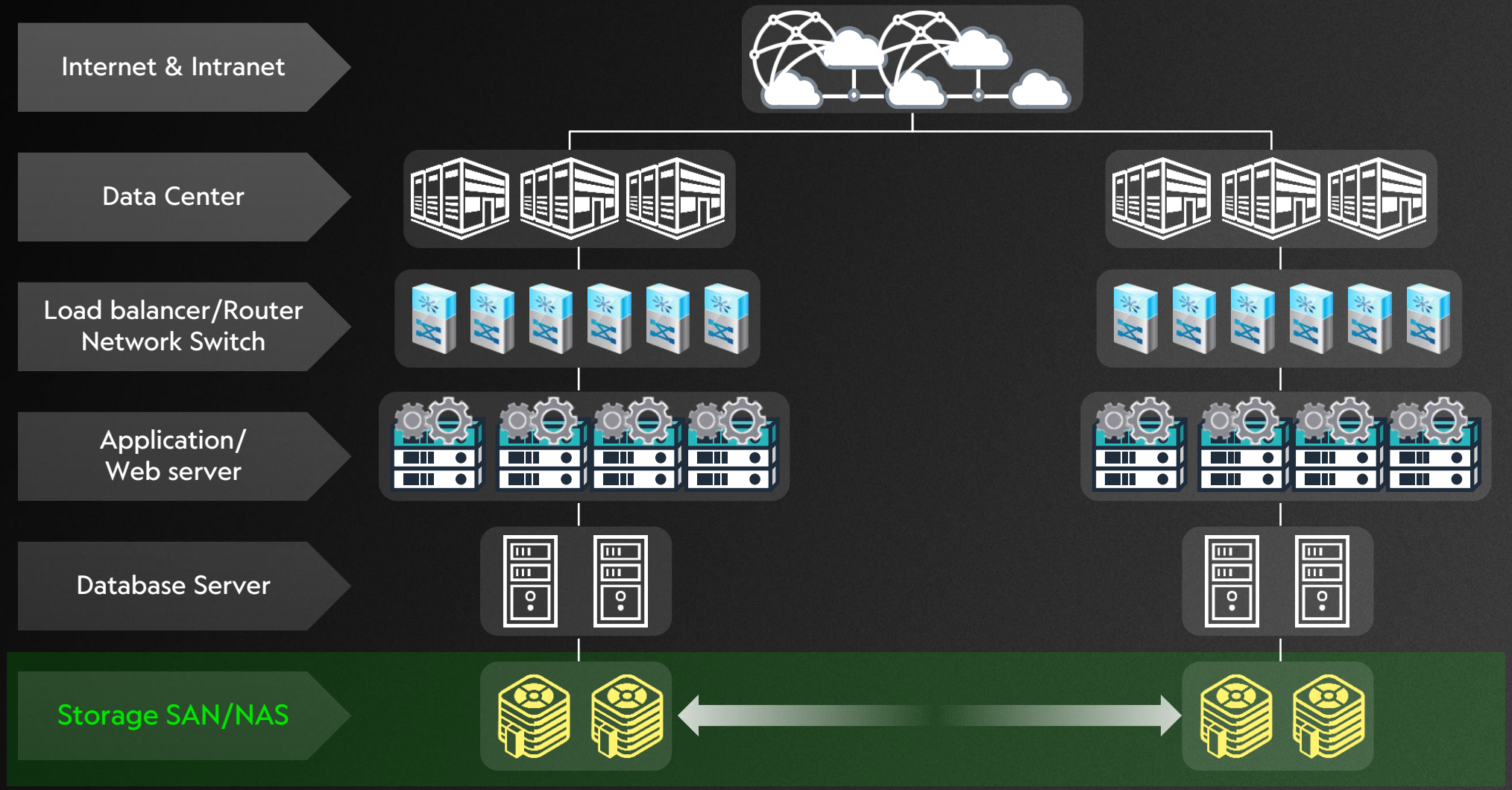
구분	고객사	도입장비	비고
금융	OO은행	VSP 5500	
금융	OOO은행	VSP 5600	
금융	OO중앙회	VSP 5600	
금융	OO카드	VSP F1500	
금융	OO생명	VSP G1000	
금융	OO증권	VSP 5500	
금융	OO화재	VSP 5500	
금융	OOO금고	VSP F1500	
공공	OOOOOO관리원	VSP F1500	
공공	OOOO연구소	VSP F1500	
공공	OOOOOO연구원	VSP E1090	
통신	OO텔레콤	VSP F1500	
병원	OOOO병원	VSP E790	
기업	방송사	VSP E590	
기업	OO홈쇼핑	VSP E1090	
원격지 구축 사례			
제조	반도체 제조사	VSP F1500	공장간 GAD 구성 (~5KM)
제조	OOOO해양	VSP G1500	공장간 GAD 구성 (~2KM)
병원	OO대학교병원	VSP G600	병원간 GAD 구성 (~1KM)

Active-Active 센터 구축 사례

- 두개의 운영 센터를 구축하여 Active-Active 스토리지 미러링 구성
- 업무별 중요도를 고려하여 Tier를 구분하여 재해복구 구축



데이터센터의 인프라 구성요소



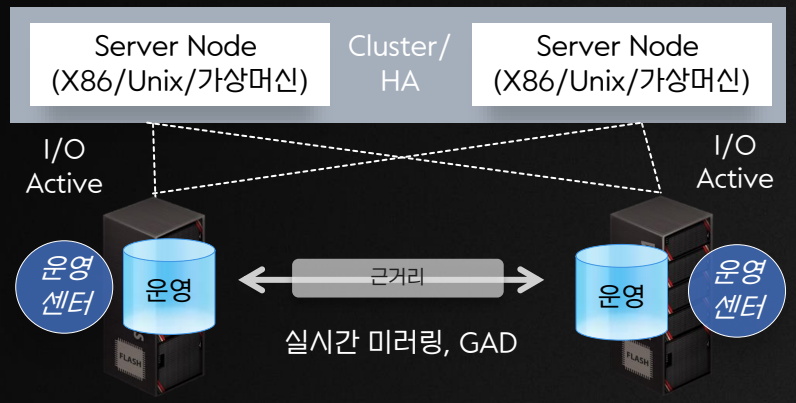
해결해야할 고려사항

높은 투자비용		• Active 데이터 센터 구축을 위해서는 주센터와 동일한 1:1 스펙의 장비 구성필요 • 네트워크 지연을 해결하기 위한 고대역폭 회선 비용 • 기타 고가용성을 위한 Cluster 소프트웨어 및 라이선스 비용
거리제한 및 Latency		• 2개 사이트 Write완료 후 응답에 따른 응답 지연 • 솔루션별 권장 Latency 충족을 위한 고속 전용회선 구성필요 • 물리적 Latency 극복을 위한 네트워크 가속 장비 필요
DBMS		• DB Lock을 방지하기 위한 데이터 일관성 유지 및 데이터 충돌 해결 • 거리에 따른 응답 지연 및 Split-Brain등 네트워크 단절 이슈해결 • 데이터 분할(Shard)등 구조 변경 필요
기타 사항		• Cluster File system 적용 및 어플리케이션 레벨의 충돌 제어 필요 • 운영 복잡성 증가에 따른 관리 역량 성숙도 필요

재해복구 구성 보완방안

- Active-Active 이중화를 확장하여 추가로 원거리 DR센터 구성 시 광범위한 지역에 걸친 재해 상황까지 대응 가능

Active-Active 센터 (2DC)

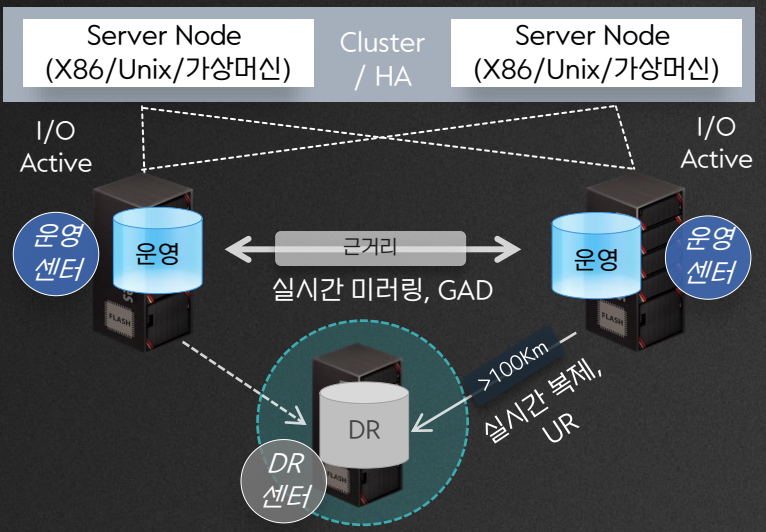


2Data Center 방식의 Active-Active 구성

GAD는 센터간 **최대 500KM & 최대 20ms** 이내의 Latency 구축 지원

근거리 이중화 운영 센터 구축 시 해당 반경에 재해가 발생했을 시 데이터 Loss를 대비한 대책이 필요

Active-Active & DR센터 (3DC)



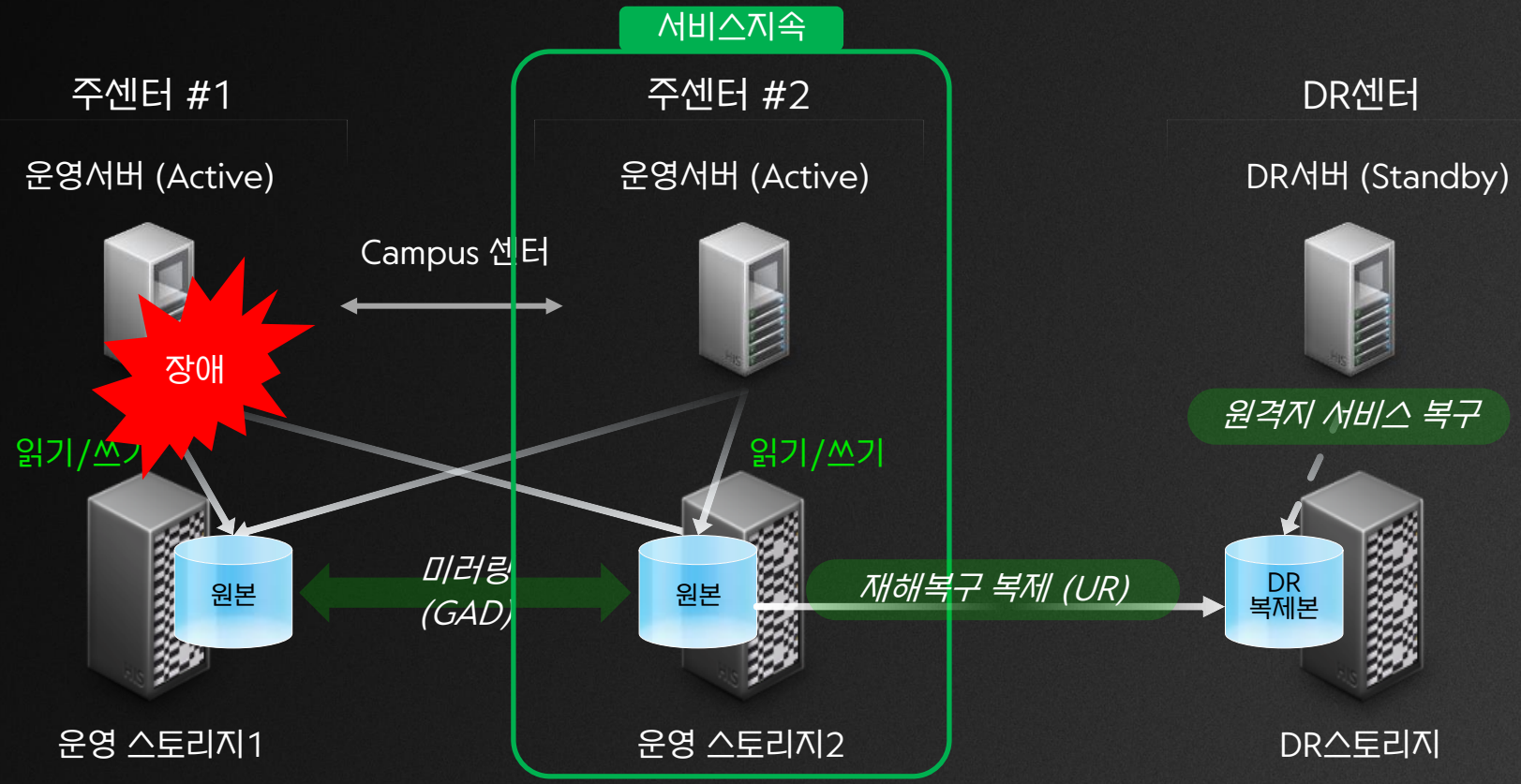
3Data Center 방식 Active-Active-Standby 구성

*추가로 **수백Km이상 원격지에 UR솔루션으로 실시간 DR구축***

운영 스토리지가 다운되어도 복제 연속성 및 데이터 보호

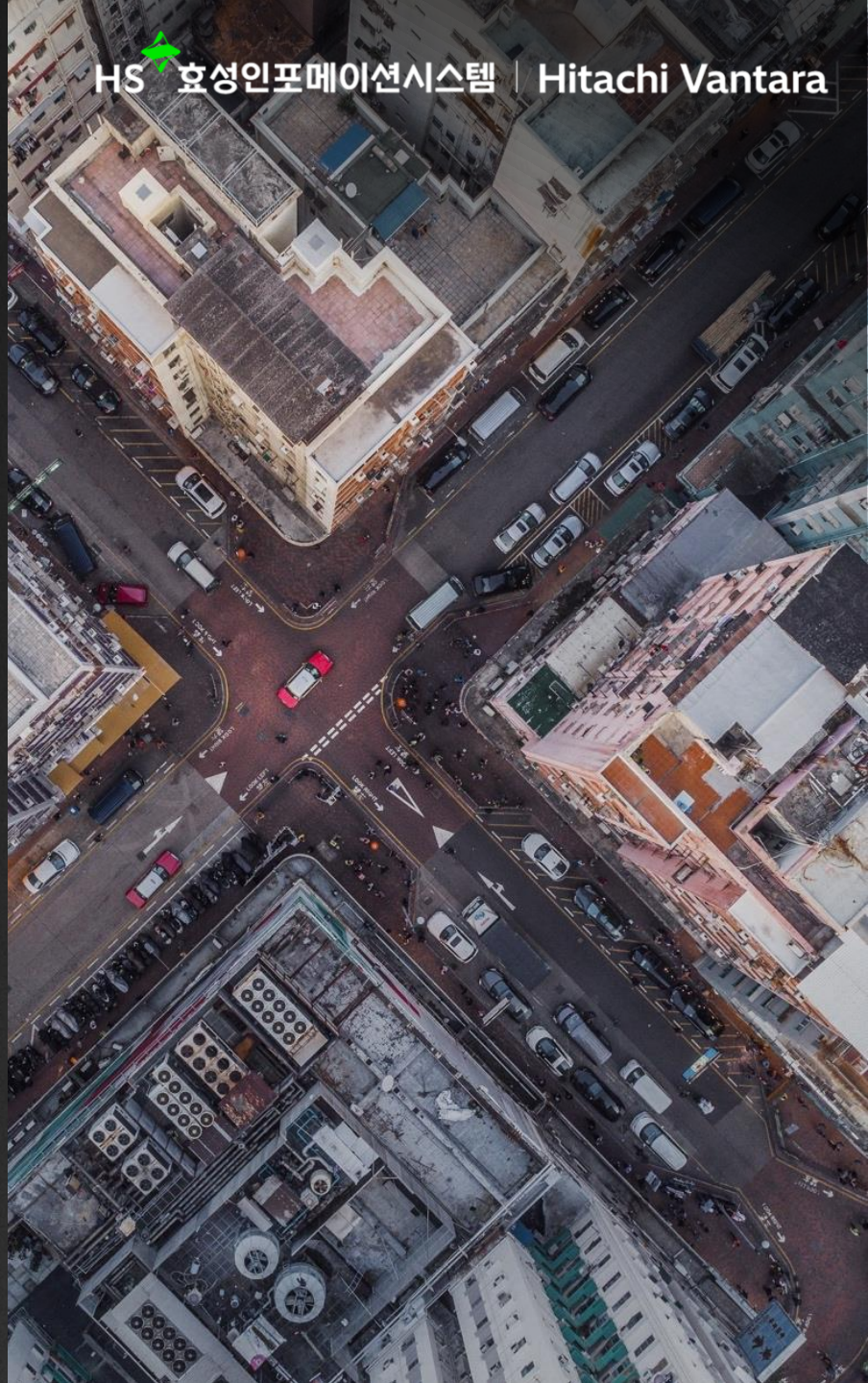
데이터센터 재해복구 구성

- 근거리 운영 데이터센터 구축을 통한 가용성 증대



- 운영센터와 근거리에 별도의 운영센터를 추가 구성하여 시스템 이중화 구성
- 근거리 네트워크(Campus Network)를 통한 서비스 Delay 최소
- 지리적인 재해상황시 데이터 보호를 위한 별도의 백업센터 필요

III.
사이버공격 대응 방안



고도화 되는 사이버 공격

- 개인 PC 등을 암호화해 협박하던 것에서 기업은 물론 병원, 공공인프라 등을 겨냥한 무차별적 공격으로 진화
- 서비스형 랜섬웨어(RaaS) 키트가 저가에 공급되며 사이버 공격이 양상되고 있는 상황
- 디지털 트랜스포메이션과 클라우드 전환으로 공격표면이 넓어지면서 취약점도 크게 늘고 있는 상황

랜섬웨어 공격

락커(Locker)

데이터 및 기기를 잠금

크립토(Crypto)

파일을 암호화 →
Lockey감염 등의 사례

데이터 탈취

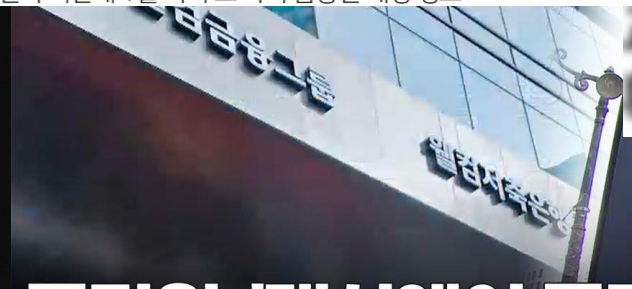
해킹을 통한 데이터 탈취
및 기존 데이터 감염

사이버 공격에 의한 피해 사례

국내 기업의 사이버위기... “랜섬웨어 피해 급증 "

은행도 랜섬웨어 당할 수 있다?...금융권 AI 공격 우려 확산

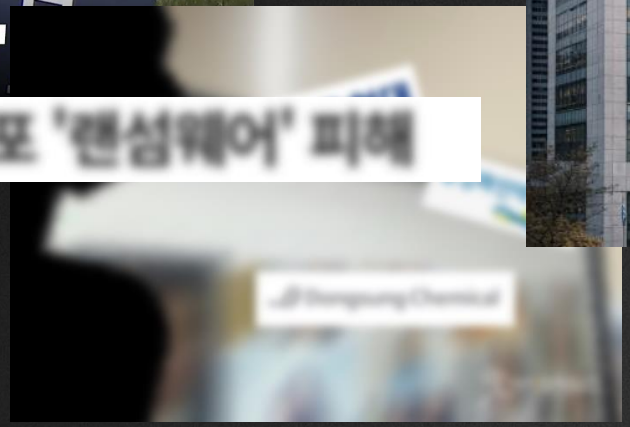
국제금융센터 지난해 1월 이어 또 다시 금융권 해킹 경고



교원그룹, 랜섬웨어 공격 의심 정황...데이터 외부 유출 '가능성' 확인 후 개인정보위 조사 착수

금감원, '랜섬웨어 공격'

현대중공업·동성그룹 해커 유포 '랜섬웨어' 피해



Ransomware 공격에 대한 대응

언제든 공격 당할 수 있다는 것을 인지하고 회복탄력성에 집중
“You Will Be Hacked, Embrace the Breach!”

대부분의 기업이 복구에 대한 확신 없음

랜섬웨어 대응 전략

- 사전에 데이터를 보호 및 접근제어 필요
- 랜섬웨어 공격의 사전 분석 및 탐지
- 감염 시 이전 데이터로 신속한 복구

변경 불가 스냅샷 (Thin Image Advanced)

- **Safe Snap (Immutable Snapshot)**
  Thin Image Advanced 기술 기반의 불변(Immutable) 스냅샷으로, Retention Lock(보존 잠금)을 적용하여 설정된 보관 기간 내 데이터의 수정 및 삭제를 원천적으로 차단하는 기술

관리자 권한 보호

관리자 계정(Admin/Root) 권한이 탈취되어도 데이터 삭제 불가능

랜섬웨어 차단

랜섬웨어가 스냅샷 삭제 명령을 내려도 실행되지 않음 (WORM 기능)

규정 준수 (COMPLIANCE)

데이터 보존 규정 및 감사(Audit) 요구사항 충족

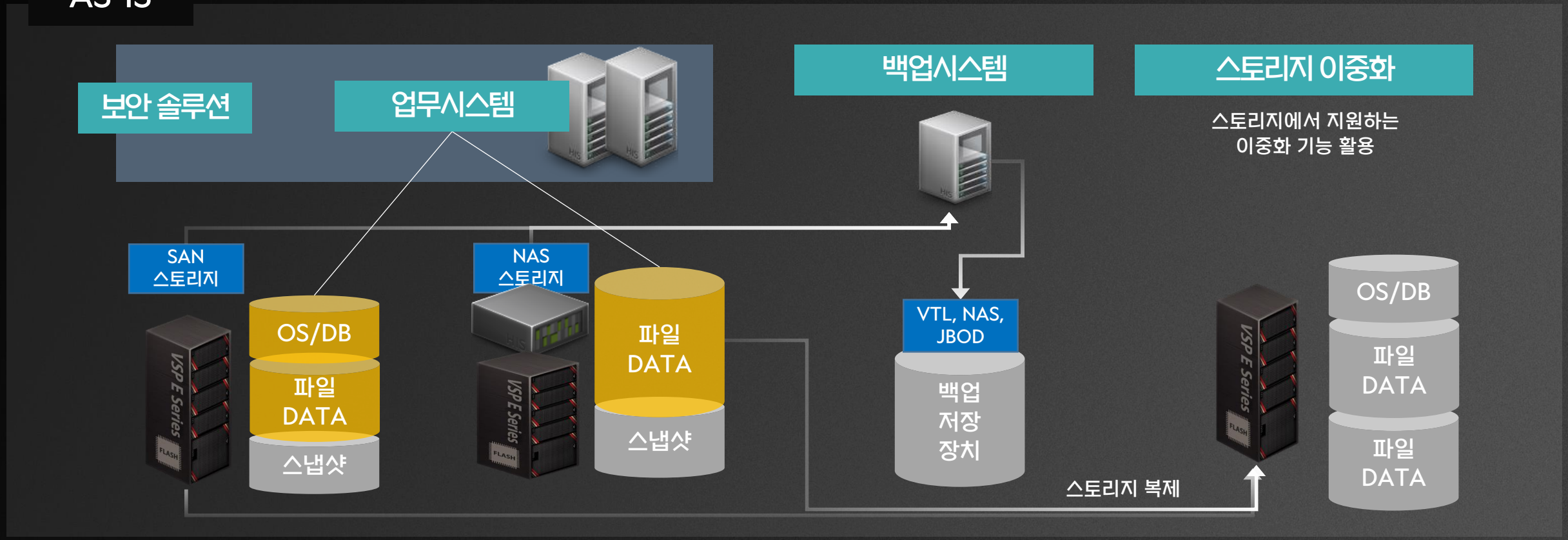
일반 스냅샷 vs Safe Snap 비교

구분 항목	일반 스냅샷 (Standard)	Safe Snap (Immutable)
제 가능 여부	관리자가 언제든 삭제 가능	잠금 기간 내 절대 불가
랜섬웨어 대응력	취약 (삭제 명령 시 삭제됨)	강력 (삭제/변조 시도 차단)
관리자 권한 탈취 시	데이터 전체 삭제 위험	데이터 보호 유지 (최후의 보루)
장기 보관 적합성	운영 목적 (단기)	보안 및 컴플라이언스 (중장기)

데이터 감염 방지를 위한 백업과 복구 전략

- 데이터 보호를 위해 스토리지 이중화 구성. SAN 혹은 SAN + NAS 복합 구성(파일 데이터가 많아지는 경우 NAS로 확장)
- 데이터 훼손 발생 후 스토리지 내 스냅샷을 이용하여 데이터 복구
- 백업 시스템을 이용한 데이터 보호와 장애 발생 시 복구 작업 수행

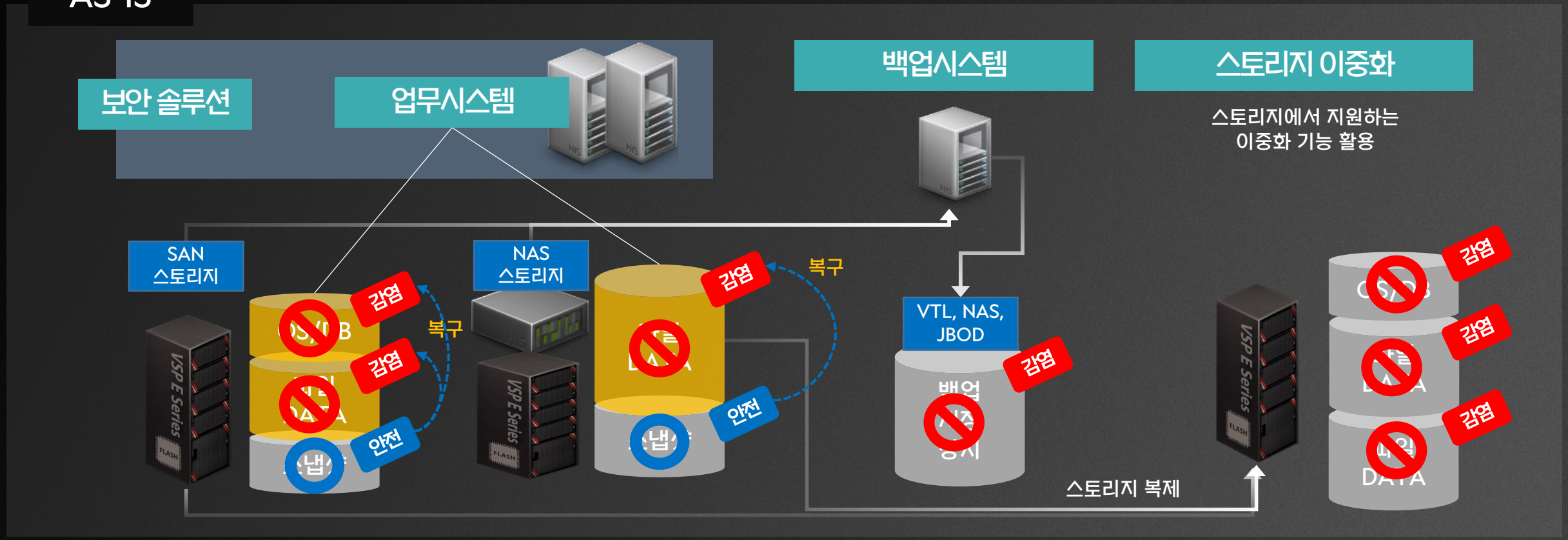
AS-IS



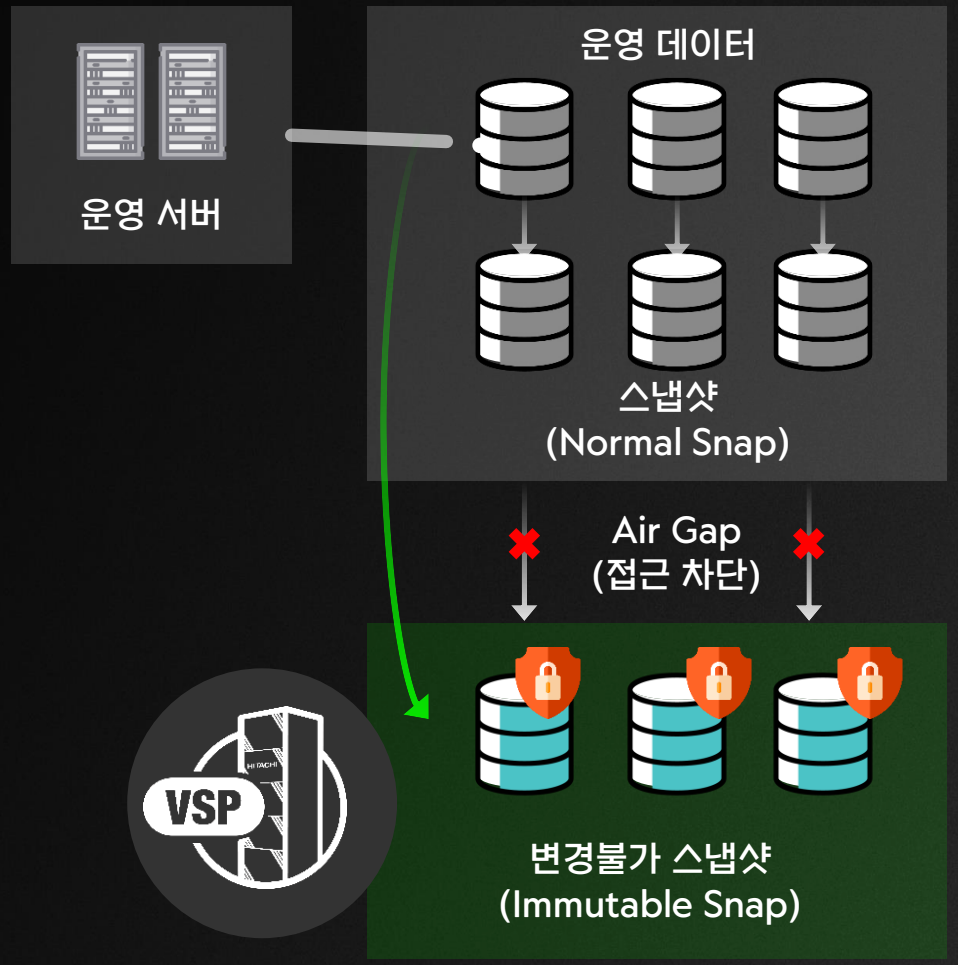
데이터 감염 방지를 위한 백업과 복구 전략

- 랜섬웨어 등의 공격으로 데이터가 손상되는 경우 실시간으로 이중화 된 스토리지에도 복제되어 전체 데이터 유실
- 스토리지 스냅샷으로 감염 시점 이전 데이터로 복구 가능 - 데이터 감염시점을 정확히 모르며 RPO, RTO 충족이 어려움
- 백업시스템으로 데이터 복구 - 단 백업서버가 랜섬웨어에 감염된 경우 데이터 복구 자체가 불가능

AS-IS



Hitachi 변경 불가 스냅샷 보호



- MFA(Multi-Factor Authentication)을 통한 접근 제어
- 변경 불가 스냅샷 생성과 복구 등의 관리를 완전 자동화 지원

- 특정 기간 보관 주기를 보장하는 변경 불가 스냅샷본 생성
- 외부 접근을 차단하는 논리적 Air-Gap 생성으로 스냅샷 데이터 보호

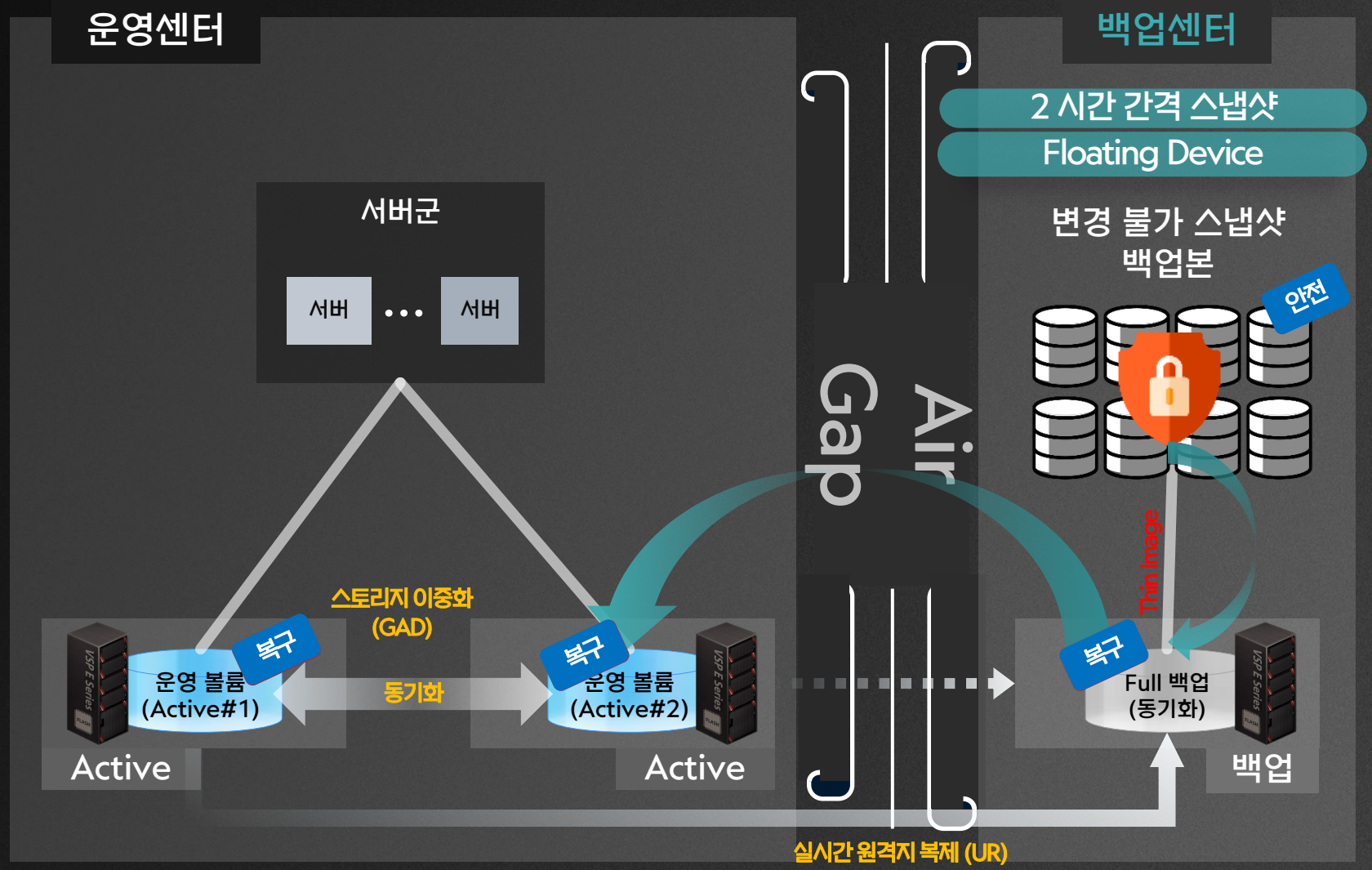
1. Normal Snap 방식
   - 스냅샷 생성/삭제 가능
   - 스토리지 관리자에 의해 스냅샷 삭제 가능
2. Immutable Snap 방식
   - Retention 기간 설정
   - 보존기간내 수정/삭제 불가
   - 관리자 권한으로도 삭제불가

랜섬웨어 감염에서 복구 사례

실 복구 예

- ✓ 백업: 백업 스토리지에서 2시간 마다 스냅샷 백업
- ✓ 복구(약2시간 30 분 소요):
  1) 마지막 Snapshot 백업본으로 데이터 복구
  2) Backup 스토리지로 서비스에서 운영 스토리지 복구

※ 특이점: 백업 서버 포함 대부분의 서버가 Ransomware 에 걸려 OS 재설치 작업등으로 복구가 지연됨
➔ OS에 대한 스냅샷 및 백업 복구 방안 추가 필요



TIA와 CyberSense와 통합한 AI탐지 모델

Hitachi Vantara Ransomware Detection Powered by CyberSense®

200+

탐지 규칙

암호화·삭제·변경 패턴 감지

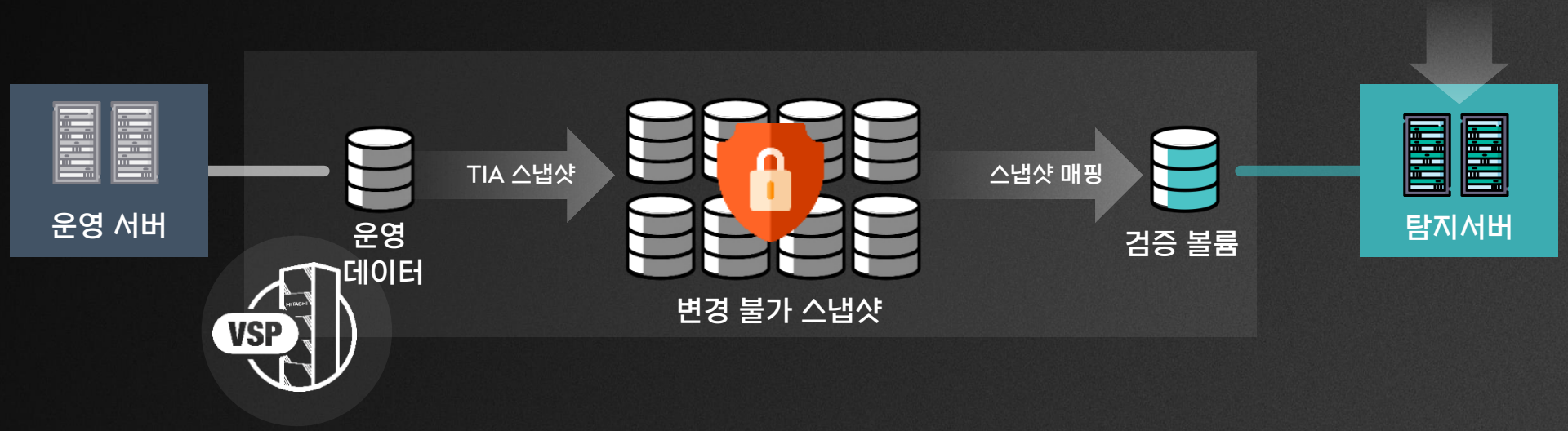
99.99%

탐지 정확도

정밀한 AI 기반 분석

1 AI 기반 무결성 분석
: 머신러닝 알고리즘으로 데이터 변조 패턴을 감지

2 감염 시점 자동 식별 + 정상 스냅샷 추천
: 공격 발생 시점을 정확히 파악하고 복구 지점을 추천



Hitachi 통합 데이터 관리 플랫폼

VSP 360

Revolutionize the Data Platform to fuel the AI Factory.

전문인력에 의한 직접 기술지원

제조사 전문엔지니어의 단일화 기술지원

전체 구성원 중
전문기술인력 비중, *60%*

필요 시

Global

Hitachi Vantara
본사

Hitachi Vantara
Korea

초기 설계부터 구축단계 및 장애상황까지
HS효성인포메이션시스템㈜ 전문 인력 지원!

고객사 별 전담 인력배정으로 체계적인 관리제공

재해와 사이버 위협에 대응하는 HIS의 제언

데이터 보호

- 실시간 원격지 재해복구(UR)를 통한 장거리 데이터 센터간 중요 데이터 보호 및 재해 복구 시스템 구축 지원
- 스토리지 기반의 Active-Active 이중화(GAD) 적용을 통한 무중단 스토리지 서비스 제공 (RPO & RTO=0)
- 변경 불가 데이터 보호 : Air-gap 생성, 보존 기간 설정(Safe Snap)
- 테스트 및 포렌식 : 별도의 Snapshot 복제(Snap on Snap)

AI 기반 자동 탐지

- CyberSense를 활용한 이상 I/O 감지 및 감염 여부 진단

운영 자동화

- AIOps기반의 데이터 통합 관리
- 데이터 복제 및 Snapshot 생성, 상황 시 복구 자동화

마무리하며

고객의 중요 데이터 보호를 최우선으로 생각하는

Hitachi 스토리지

스토리지
성능 및 안정성

1위의 업계
최고의 제품

강화된
사이버 복원력

스토리지
데이터 보호 솔루션

Hitachi Vantara

HS 효성인포메이션시스템

AIOPS
기반의

통합 데이터
관리플랫폼

파트너
지원이 아닌

벤더 전담 엔지니어
단일 통합 기술 지원

감사합니다.