

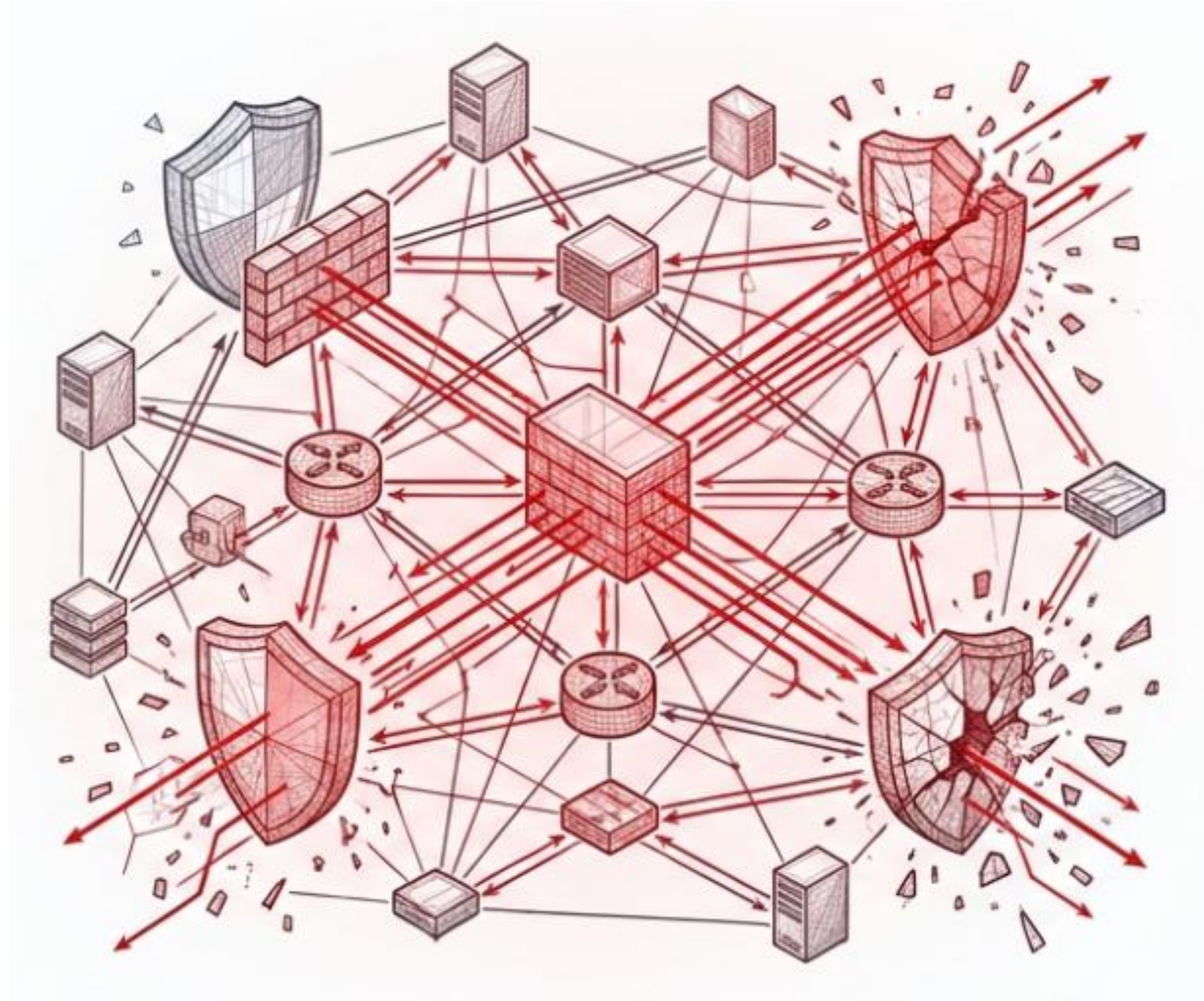
AI 해킹 자율화 시대, 사이버 복원력의 완성

소프트웨어 보안 공식이 붕괴하는 지금,
최후의 보루가 될 수 있는 물리적 에어갭(Air-Gap) 데이터 금고 - 디포트리스



연결된 이상, 소프트웨어 방어망은 결국 뚫립니다.

양방향 연결(TCP/IP)의 태생적 한계



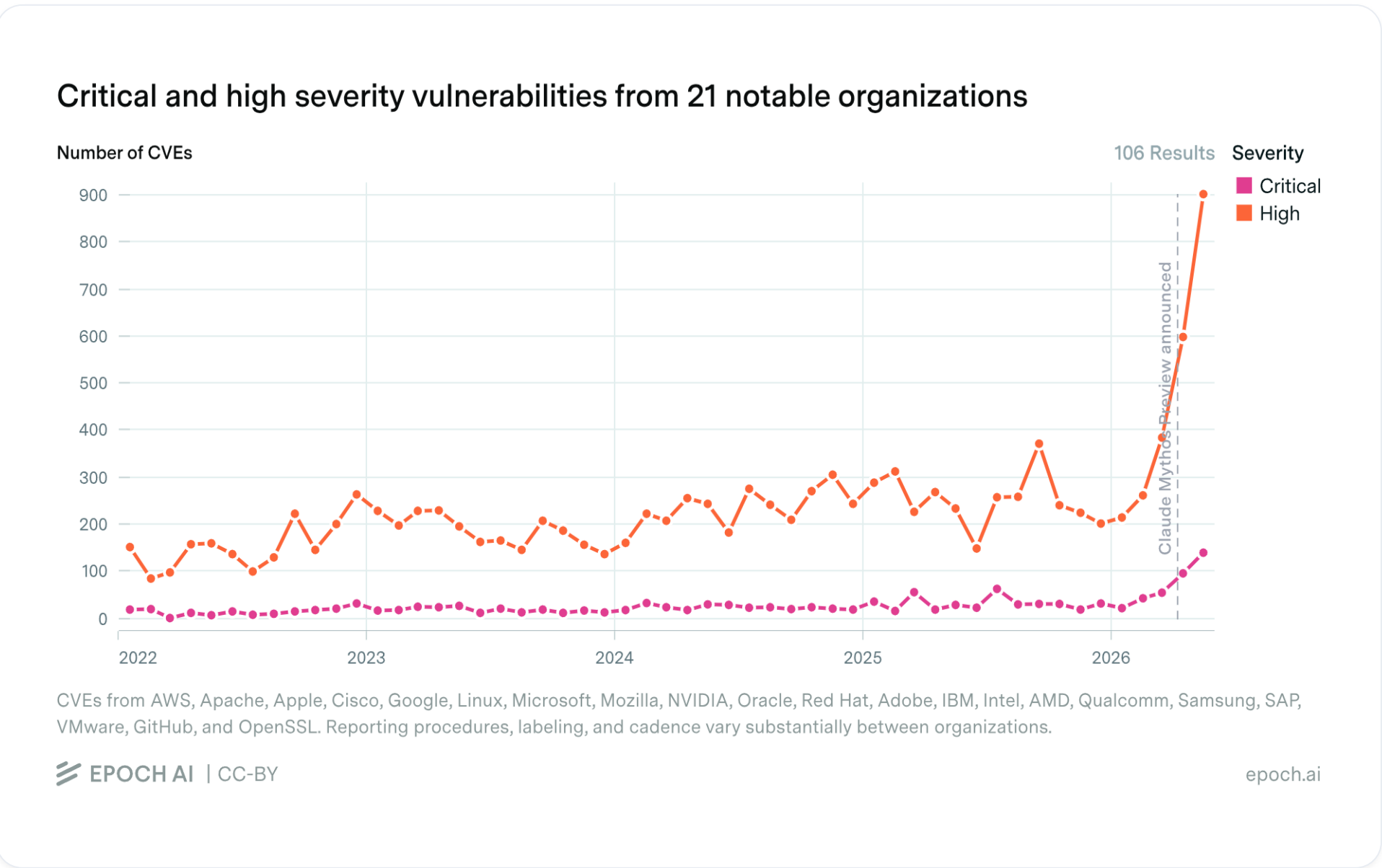
∴ 양방향 연결의 함정

수많은 노드가 TCP/IP로 연결된 채, 오직 소프트웨어 방어망에만 의존합니다.

**방어자의 소프트웨어가 한 번 뚫리는 순간,
연결된 모든 자산이 노출됩니다!**

AI 해킹의 시대: 글로벌 선도기업도 위기!

방화벽·백신·EDR 같은 소프트웨어 보안만으로는 AI 해킹과 지능형 랜섬웨어를 막을 수 없습니다.
글로벌 선도기업의 취약점이 AI와 함께 수직 폭증했습니다.



≈900건 High 심각도 CVE

200~300건대에 머물던 선도기업 취약점이
2026년 자율형 AI 발표 시점 과 함께 급증.

거인도 못 막는데, 중소기업이?

보안에만 수조 원을 쓰는 빅테크도 뚫립니다.
중소 제조기업이 **방화벽으로 막는 것은 불가능!**

그래서, 물리적 백업이 정답

소프트웨어 보안 솔루션은 무조건 뚫린다는 가정하에
백업 데이터를 물리적으로 격리하여 사이버 복원력을
확보하는 것이 최우선과제!

사람의 속도로는 막을 수 없습니다.

공격은 자동화되어 한 번만 성공하면 되고, 방어는 사람이 매번 성공해야 합니다.

방어 불가능의 수학: Human vs. AI Agent



하루 평균 50개 취약점 테스트 한계.
패치 개발 및 적용에 수 주 소요.



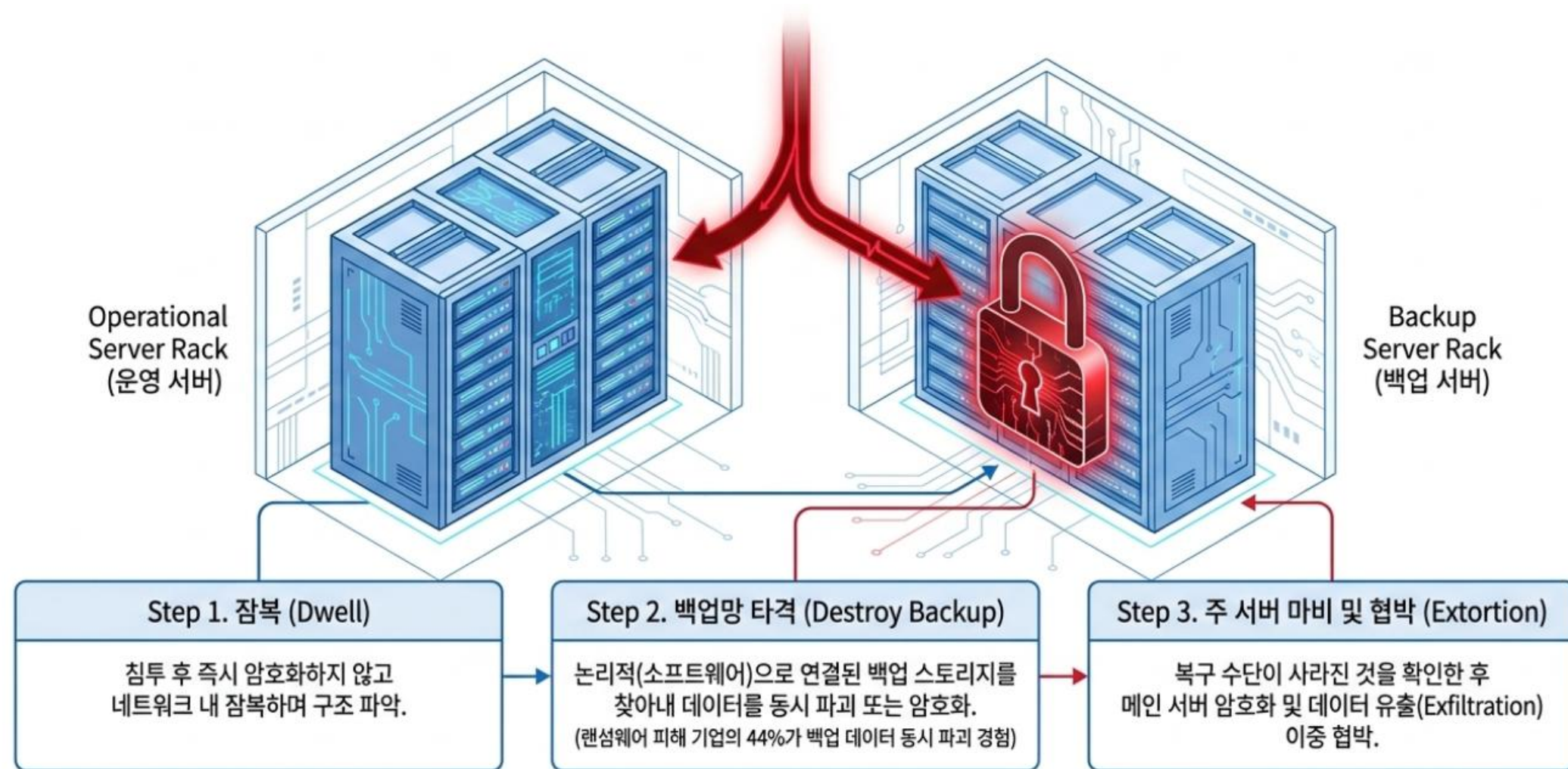
시간당 50,000개 취약점 동시 테스트.
방어벽 탐지 시 실시간으로 코드를
우회 변이 (밀리초 단위 공격).

방어자가 한 번이라도 실수할 때를 기다리는 것이 아니라, 수만 번의 공격을
동시에 쏟아부어 방어막을 찢어버리는 '제로-세컨드(Zero-Second)' 시대.

PHASE 02 · THE COMPLICATION

해커의 1순위 표적은 이미 '백업 서버'입니다.

“복구의 희망부터 끊는다” — 운영 서버를 암호화하기 전, 잠복하며 백업망을 먼저 파괴합니다.



● **96%**

랜섬웨어 공격이 백업 저장소를 표적 백업은 더 이상 안전지대가 아닙니다.

■ **76%**

표적이 된 백업의 실제 침해 성공률 표적이 되면 상당수가 무력화됩니다.

↗ **8x**

백업이 훼손됐을 때 복구 비용 그렇지 않은 경우 대비 약 8배

“백업이 있습니까?”가 아니라 — “관리자 권한이 탈취돼도 백업이 삭제·암호화되지 않는 구조입니까?”

국가 최상위 보안의 답: 물리적 단방향 통신

원자력 발전소는 인터넷이 차단된 절대 폐쇄망 — 외부와의 통신은 오직 일방향 다이오드(Data Diode)뿐입니다.



핵발전소 모델

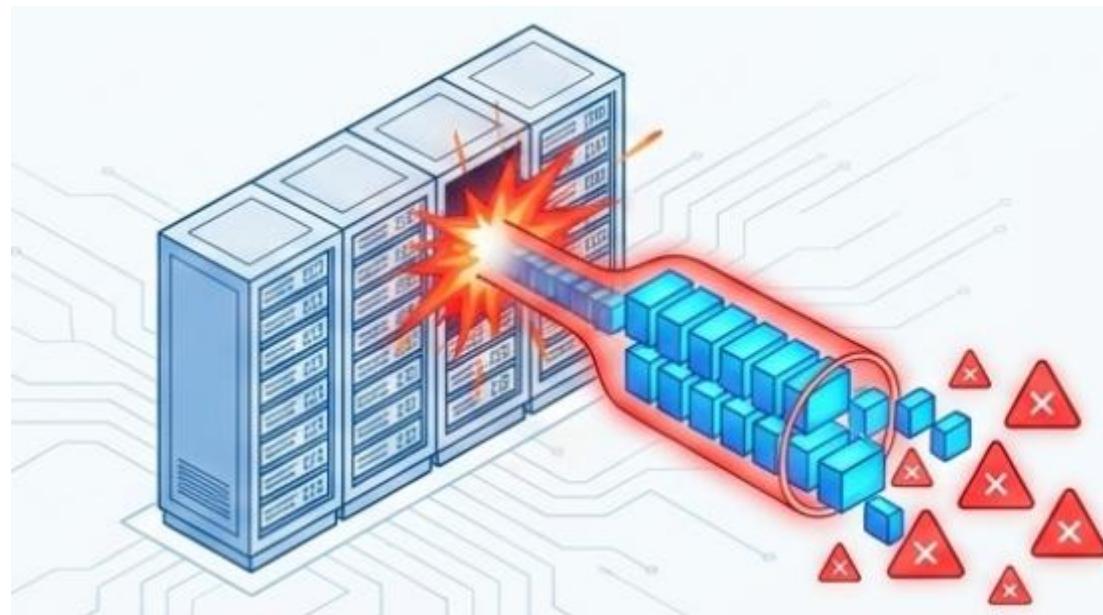
원자력 발전소는 외부망과 오직
‘일방향 광케이블(Data Diode)’로만 기계적 단절.
외부 해킹 원천 불가능.

기계적 단절

나갈 수는 있어도, 들어올 수는 없습니다. 소프트웨어는 해킹돼도, 물리 법칙은 해킹되지 않습니다.

그런데 왜 기업 백업망에는 쓰지 못했을까?

기존 산업용 다이오드의 치명적 딜레마 — 피드백 채널이 없어 대용량 파일 전송이 불가능했습니다.



기존 산업용 다이오드의 한계

- 피드백 채널 부재: ACK 패킷을 받을 수 없어 양방향 통신(TCP/IP) 단절.
- I/O 마비 및 패킷 유실: 대용량 엔터프라이즈 백업 전송 시 데이터가 깨지고 스토리지 메모리 초과로 시스템 다운.



재전송 요청 불가

데이터가 유실되어도 수신 측에서 '다시 보내달라'는 피드백을 줄 수 없습니다.



소용량에 국한

소규모 텍스트·로그 전송에만 사용 가능
— 극심한 패킷 유실이 발생합니다.



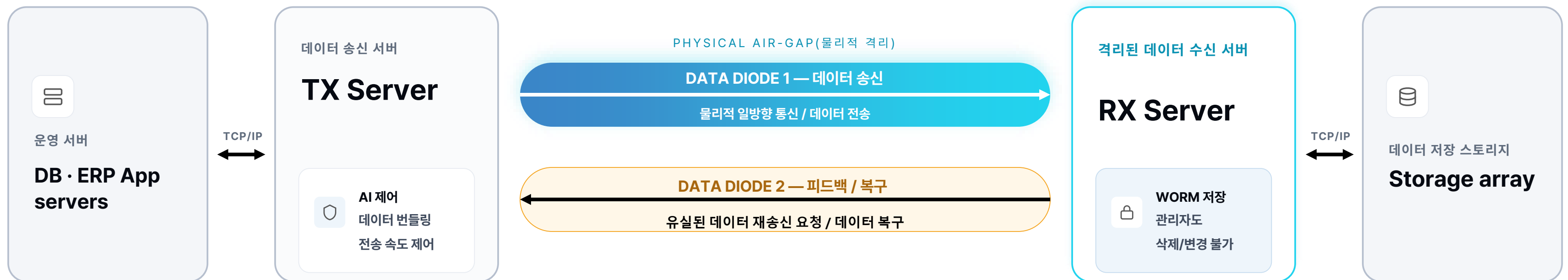
대용량 데이터 전송 불가

테라바이트급 DB·서버 백업에 적용하면 파일이 깨져 전송이 불가능합니다.

PHASE 03 · THE RESOLUTION

데이터 다이오드의 한계를 돌파한 D-FORTRESS

이중 데이터 다이오드: 일방향 통신의 보안성은 지키고, 대용량 파일 전송이 가능!



각 다이오드는 물리적으로 분리된 일방향 통신 채널입니다.

다이오드 2는 오직 전송 피드백과 복구 데이터만 전달합니다.

따라서 송신서버(TX)가 침해당하더라도 수신서버(RX) 내부로 진입할 수 있는 양방향 통신 채널은 존재하지 않습니다

PHASE 03 · THE RESOLUTION

뚫는 것을 막는 대신, 들어올 길 자체를 없앴습니다

디포트리스는 외부에서 해커가 침입할 양방향(TCP/IP) 침입 경로 **자체를 물리적으로 제거**한 데이터 금고입니다.

해커가 최고관리자 권한을 탈취해도 **백업 데이터 파괴(삭제 및 암호화) 자체가 불가능**해집니다. (관리자도 데이터를 네트워크 상에서 삭제/변경 불가)



D-FORTRESS 3대 핵심 가치

절대적 격리, 완벽한 무결성, 그리고 비즈니스 연속성을 통해 최종 방어선을 구축합니다



물리적 망분리 (Air-Gap)

하드웨어 수준의 일방향 격리를 통해
공격 표면(Attack Surface)을
원천적으로 제거합니다.



데이터 무결성 (Data Integrity)

제로 트러스트 아키텍처 기반으로,
관리자도 백업 데이터의
수정 및 삭제가 불가능합니다.



비즈니스 연속성 (Zero RTO)

사고 발생 즉시 사전에 무결성이 검증된 데이터
를 복구하여 다운타임을 최소화합니다.

D-FORTRESS 기술적 차별성

물리적 격리에 기반한 데이터 보호 방식이 시스템 최고 관리자 권한이 뚫려도 원천적 데이터 보존을 가능하게 해줍니다.

	소프트웨어 보안(기존)	D-FORTRESS (물리적 격리)
보안 기반	논리적 & 정책적 - 결함 발견시 우회 가능	물리 법칙에 기반 - 논리적 우회 불가
루트 권한 손상 시	전체 보안 시스템이 일시에 붕괴	데이터 삭제 및 수정이 원천적 차단됨
위협 방어 범위	시그니처 종속적 — 미지의 제로데이(zero-days) 위협에 무방비	시그니처와 무관 — 접근 경로 자체가 제거됨
유지보수	지속적인 패치 및 업데이트 필요	한번 구축으로 끝 - 끊임없는 시그니처 업데이트 불필요

PHASE 03 · THE RESOLUTION

일반 백업 · WORM 스토리지 · D-FORTRESS 비교분석

관리자 권한이 탈취됐을 때, 백업 데이터가 실제로 지켜지는 구조인지가 핵심 기준입니다.

비교 기준	일반 백업 (NAS·클라우드·동기화 DR)	WORM 스토리지 (논리적 불변 저장)	D-FORTRESS (물리적 에어갭 + 이중 데이터 다이오드)
연결 구조	상시 양방향(TCP/IP) 연결 — 원본과 동일 네트워크에 상주	상시 양방향 연결 유지, 삭제 정책만 소프트웨어로 잠금	물리적으로 분리된 일방향 채널(이중 데이터 다이오드)만 존재
관리자 권한 탈취 시	백업본까지 삭제·암호화 가능	보존기간 내 삭제는 막지만, 정책 자체를 관리자가 변경·해제 가능	관리자도 네트워크상에서 삭제·변경 자체가 물리적으로 불가능
랜섬웨어 동시 감염 위험	실시간 동기화 시 원본 감염이 그대로 복제됨	이미 손상된 파일도 검증 없이 그대로 저장됨	물리적 단방향 구조상 원본 감염이 넘어올 경로 자체가 없음
사고 발생 시 복구	재감염 방지를 위한 스캔·검증에 수일~수주 소요	삭제는 막혀 있어도 오염 여부는 별도로 확인해야 함	평시 정상 데이터만 수신하는 구조라 별도 검증 없이 즉시 복구
대용량 전송 성능	네트워크 대역폭·백업 정책에 따라 상이	오브젝트 락 처리 오버헤드로 대용량 전송 시 성능 저하	이중 다이오드로 대용량 전송 한계 해결 - 100TB/6천만 파일 손실률 0%, 30Gbps
위협 방어 범위	시그니처·정책 종속적 — 신종·제로데이 위협에 취약	삭제·변조는 막지만 침입 경로 자체는 그대로 열려 있음	접근 경로 자체가 물리적으로 제거되어 시그니처와 무관
유지보수	지속적인 패치·백업 정책 업데이트 필요	지속적인 정책·권한 관리 필요	한번 구축으로 끝 - 시그니처·필터링 로직 업데이트 불필요

* 무결성 보장은 AI 기반 콘텐츠 필터링이 아니라, 이중 데이터 다이오드의 물리적 단방향 구조 자체로 확보합니다. (2026.08 최신 아키텍처 기준 — 별도 AI 랜섬웨어 필터링 모듈은 현재 제품 구성에 포함되지 않습니다.)

PHASE 03 · THE RESOLUTION

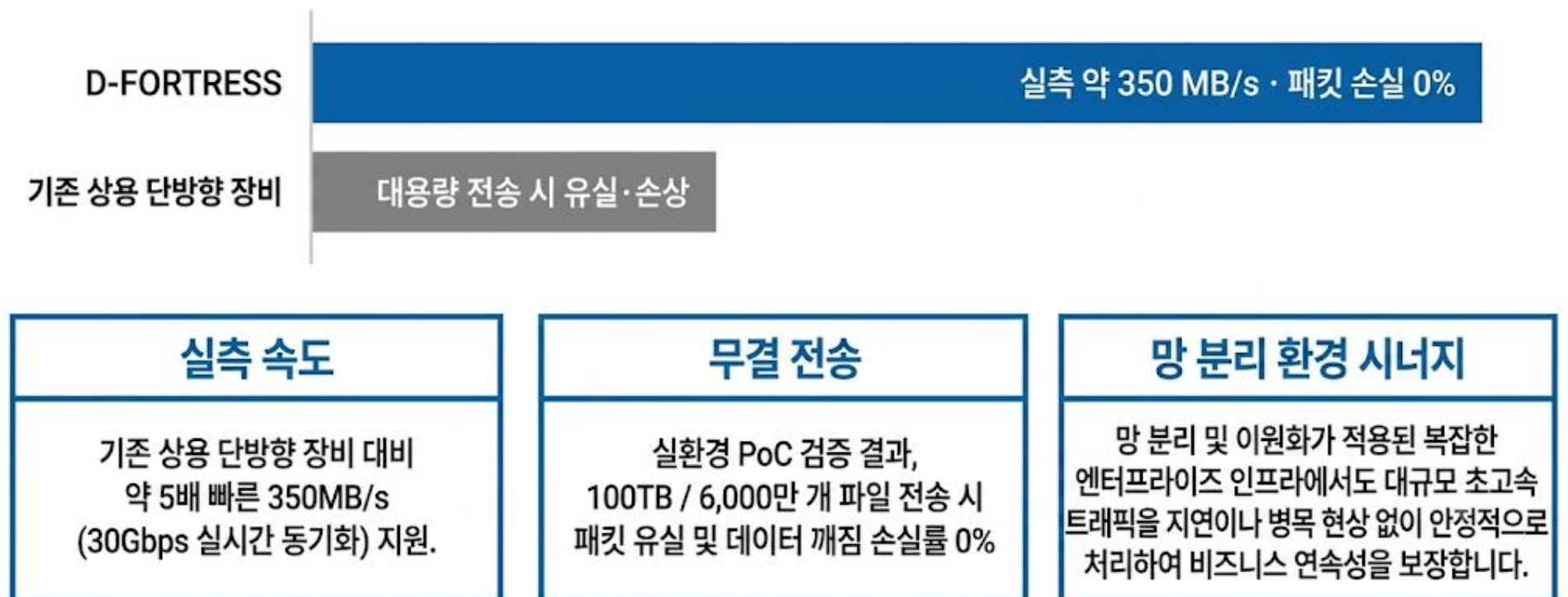
대용량 다수 파일도 안정적으로 전송

수백 TB 규모의 엔터프라이즈 환경에서도 데이터 손실 없는 안정적 전송 가능

가장 중요한 약속

데이터 손실률 0%

100TB 규모의 방대한 데이터도 **단 한 건의 손실(데이터 깨짐) 없이** 옮겨 담습니다.
 학생의 기록은 '완전한 원본'으로만 보존됩니다.



KISA도 '네트워크와 분리된 백업'을 권고합니다

한국인터넷진흥원(KISA) · 백업 관리 강화 권고

- “ 중요 자료는 **네트워크와 분리된 별도 저장소**에 정기적으로 백업할 것을 권고합니다.
- “ 클라우드에 보관된 자료에 대해서도 **정기적인 백업**을 수행해야 합니다.



참고 데이터백업 8대 보안수칙



디포트리스 = 물리적 격리 백업 | 디포트리스는 '네트워크와 분리된 별도 저장소'를, 소프트웨어가 아닌 물리적 하드웨어로 구현한 백업 금고입니다.

PHASE 04 · REFERENCE

[고객 도입 사례] A 건설사 : 랜섬웨어 위기를 극복한 '절대 데이터 금고' 구축

- A 건설사의 디포트리스 구축 사례

도입 배경 및 솔루션

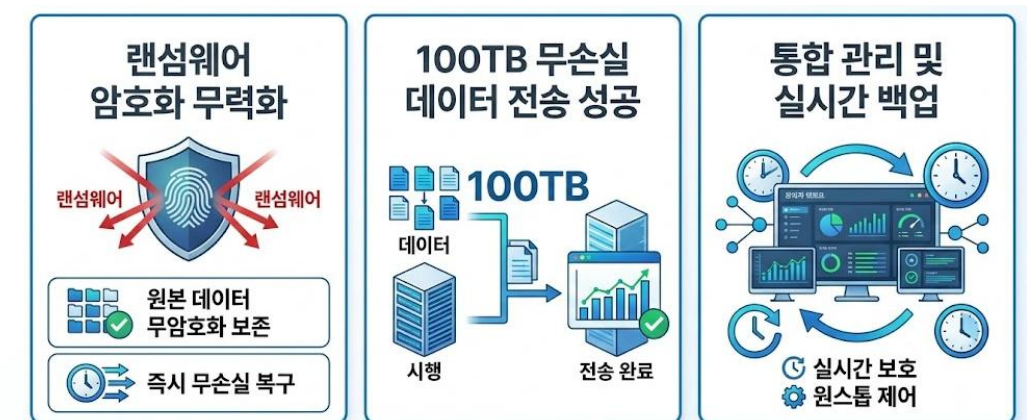
- 직면 과제: 랜섬웨어 감염으로 인한 DB 유실 및 전사 업무 마비 사태 발생
- 도입 목표: 해커의 재침투 시에도 데이터 오염·삭제가 원천적으로 불가능한 백업 시스템 확보
- 도입 제품: D-FORTRESS (물리적 데이터 금고 솔루션)

핵심 구축 성과

- 대규모 데이터 무손실 백업: 100TB(약 6천만 개 파일) 백업 완료 및 일평균 100GB 실시간 증분 백업
- 인프라 비용 획기적 절감: 고객사 기 보유 스토리지(200TB)를 D-FORTRESS에 마운트 (Bypass 방식)하여 스토리지 중복 투자 방지
- 유연한 환경 지원: Windows 및 Linux 이기종 서버 환경 동시 완벽 지원
- 랜섬웨어 면역: 사내망이 해킹당해도 백업 데이터는 절대 감염되지 않는 물리적 격리망 완성

아키텍처별 핵심 기능

구성 요소	역할	핵심 기능 요약
DF Agent (DB 서버 설치)	백업 실행 및 제어	실시간 백업 스케줄링, 파일 확장자 필터링, 전송 속도 제어, 백업 데이터 확인 및 즉각 복구
TX Server (송신 서버)	데이터 중계 및 모니터링	DF-RX 간 안전한 파일 중계(송수신), 에이전트 승인·관리, 실시간 네트워크 및 전송 상태 모니터링
RX Server (수신 서버)	최종 데이터 금고	TX 수신 데이터 격리 저장, 타임스탬프 기반 중복 파일 관리, 디스크 상태 및 백업 드라이브 중앙 제어



AI + SW + 물리적 에어갭 = 사이버 복원력(Cyber Resilience)의 완성

해킹의 두려움 없이 비즈니스 연속성을 보장하는 최후의 금고

- ☑ 미토스(Mythos), 딥시크 등 AI 주도 해킹은 인간의 방어(패치) 속도를 초월함.
- ☑ 미션 임파서블 보안 원칙: 인터넷 선이 차단된 서버에 보관하지 않는 한 100% 안전은 없음.
- ☑ D-FORTRESS의 역할: AI 모니터링 및 2차 인증(MFA)의 소프트웨어 통제 + 물리적 에어갭(Air-Gap)이 결합된 하이브리드 보호.
- ☑ 최악의 계정 탈취 상황에서도 백업 데이터를 절대 사수하는 기업의 생명선.



PHASE 05 · CONCLUSION

소프트웨어 방어가 실패할 때, D-FORTRESS는 최후의 보루가 됩니다.

UNBREAKABLE VAULT. UNSTOPPABLE BUSINESS.

더 이상 AI 해커의 속도를 소프트웨어로 따라잡으려 하지 마십시오.

해킹 경로 자체를 물리적으로 차단한 제로 트러스트 백업이 정답입니다.

ROCKGATE
CORE

(주)락게이트코어

마케팅총괄 김재원 이사

070-8080-4910 / cmo@rockgatecore.com

<https://dfortress.kr>

