

보안 사고가 반복되는 지금, 운영 DB를 보호하는 연결 구조부터 다시 설계해야 합니다.

운영 DB 보호를 위한 새로운 신뢰 기준
N-FORTRESS

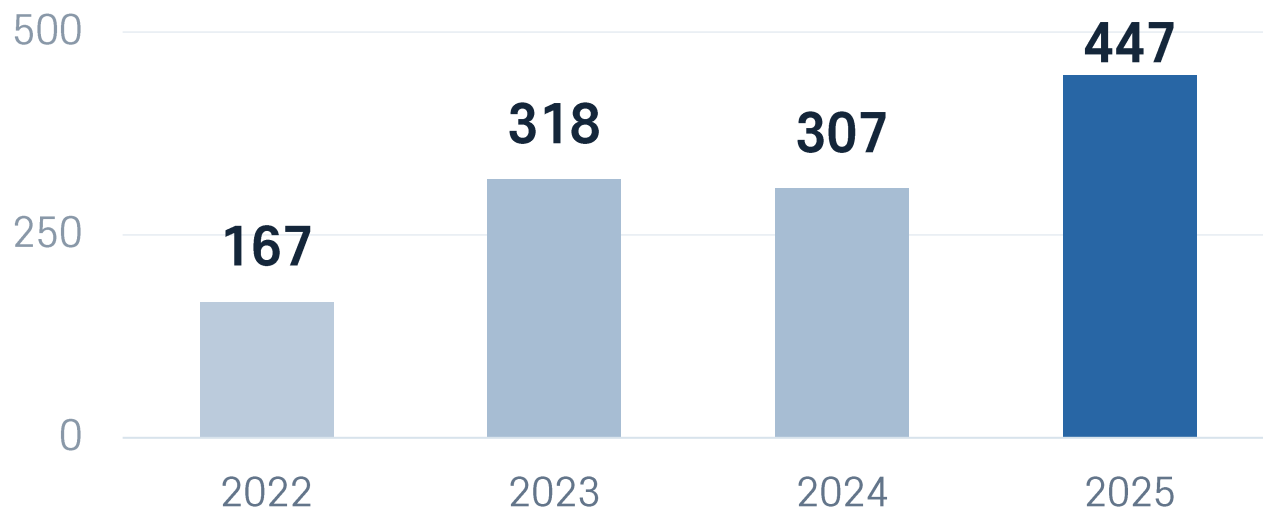


1. 현 상황 및 문제점

개인정보 유출 신고가 증가하고 있습니다

2026년 상반기 신고가 이미 전년도 연간 수준에 근접했습니다.

연도별 개인정보 유출 신고



출처: 개인정보보호위원회 발표 / 단위: 건 · 연간

2026년 상반기 유출 신고

432

전년도 연간 신고의

96.6%

1. 현 상황 및 문제점

AI는 공격의 효율과 규모를 높이는 도구로 악용되고 있습니다

AI 악용 사례와 위협 평가는 공격 환경이 달라지고 있음을 보여줍니다.

보고된 AI 악용 사례

AI 활용, 2~3시간 만에 침해

Anthropic은 AI를 이용한 침투·정보 탈취 및 다수 대상 병렬 공격 사례를 공개했습니다.

취약점 탐색·계정 탈취·정보 유출 자동화

Anthropic 위협 인텔리전스 · 2026.09.10

국내 금융권 실제 침해사고

금융권 약 10만 건 유출

금융당국은 금융사 16곳의 침해사고와 개인정보 유출을 발표했습니다.

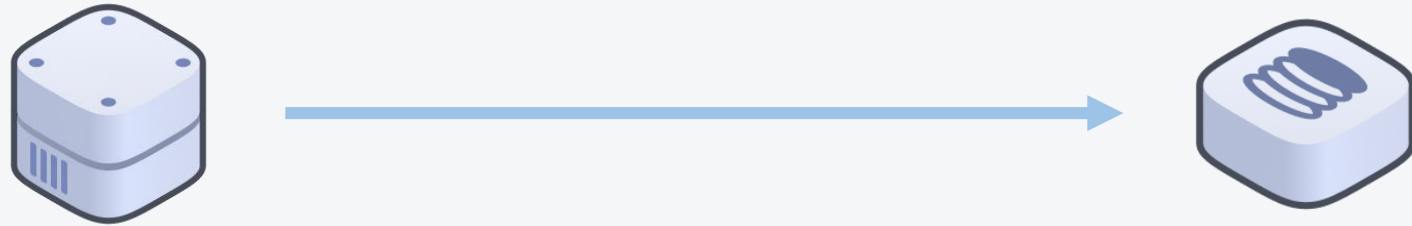
AI 활용 해킹은 더욱 증가할 전망

금융위원회·금융감독원 · 2026.10.14

2. 보호 방식의 재설계

서버가 침해되어도, 운영 DB 접근은 별도로 통제해야 합니다

기존 연결 구조



서버 침해 시 DB 접근 경로가 악용될 수 있습니다.

N-FORTRESS



직접 연결을 분리하고, 허용된 데이터 요청을 중계합니다.

2. 보호 방식의 재설계

정상 업무는 유지하고, 비인가 직접 접속은 차단합니다

홈페이지 주문 사례로 보는 N-FORTRESS의 요청 중계와 연결 분리 구조



허용 형식의 악용까지 자동으로 막는 것은 아니며, 업무 권한·요청 검증·DB 접근제어를 함께 적용합니다.

3. 솔루션 개요

N-FORTRESS: 운영 DB 보호 게이트웨이

Data Transistor를 기반으로 외부 연결과 DB 연결을 분리하고, 업무 요청과 응답을 전달합니다.

구현하는 보호 방식

외부 세션 종료와 요청 재구성
TX·RX 물리 분리 및 광 절연
이중 일방향 채널의 요청·응답 전달

3. 솔루션 개요

기존 보안 통제에, 운영 DB의 직접 연결 분리를 더합니다.

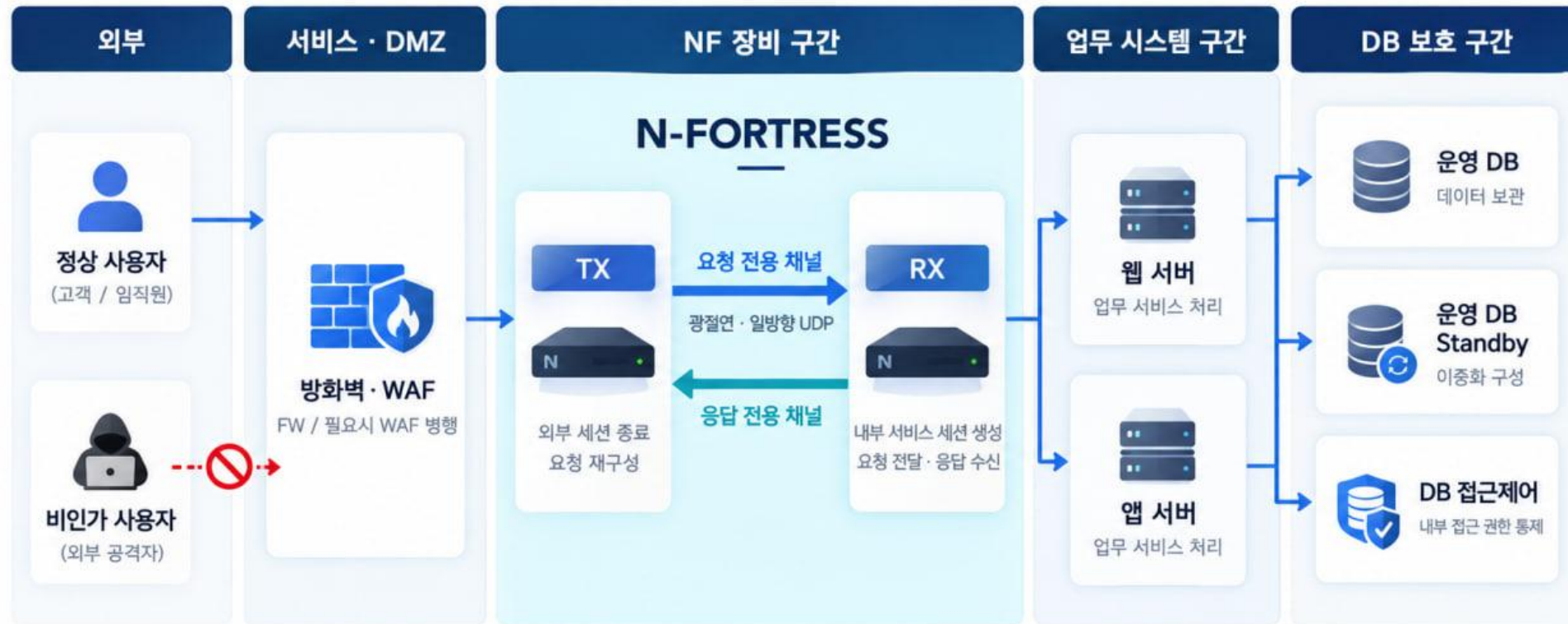
N-FORTRESS는 기존 보안 체계를 보완해 외부 세션과 DB 세션을 분리합니다.

구분	기존 보안 체계에 운영 DB 연결 분리를 추가합니다.
WAF·방화벽	웹 공격과 네트워크 통신 통제
DB 접근제어	계정·권한과 SQL 실행 통제
N-FORTRESS	외부 세션 종료, 요청 재구성 및 별도 DB 세션으로 전달
백신·EDR	호스트의 악성코드·이상 행위 탐지 및 대응
백업	장애·사고에 대비한 데이터 보관과 복구

4. 시스템 구조

Data Transistor의 통신 구조

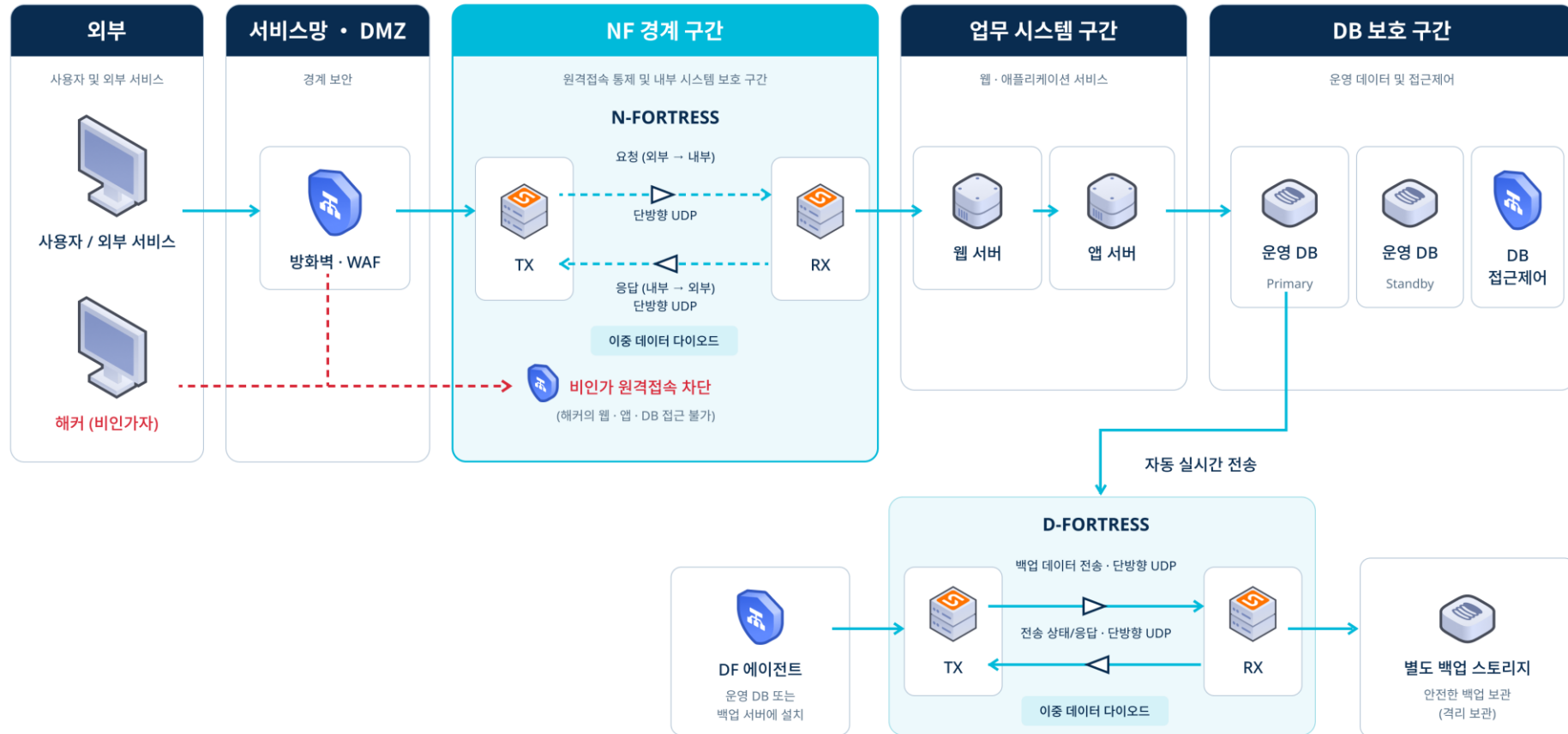
요청과 응답을 각각 독립된 광절연 일방향 채널로 전달합니다.



[외부 직접 연결은 분리하고, 정상 업무는 유지하는 N-FORTRESS 보호 구조]

4. 시스템 구조

NF 시스템 구성도



4. 시스템 구조

고객 환경에 맞춰 두 가지 위치에 적용합니다

A안은 외부→앱 서버, B안은 업무 앱→운영 DB 구간의 직접 연결을 분리합니다.

A안 | 웹·앱 앞단

외부에서 앱 서버로 향하는 직접 접속 경로 분리

WAF

N-FORTRESS

앱 서버

DB

B안 | DB 앞단

업무 앱과 운영 DB 사이의 직접 연결 분리

업무 웹

N-FORTRESS

운영 DB

기존 WAF·방화벽·DB 접근제어는 유지하며, 설치 위치와 호환성은 고객별 PoC에서 확정합니다.

물리적 연결 분리에도 빠른 응답

다이오드 왕복 상태 확인과 DB 응답 지연을 각각 측정했습니다.

다이오드 왕복 상태 확인

TX → RX → TX · 단일 표시값



0.22 ms

두 단방향 채널의
왕복 확인 시간

※ 실제 DB 응답 지연과 다른 시험입니다.

DB 요청 응답시간

SELECT 1 · 왕복 지연 중앙값(p50)



0.514 ms

실측 p50

※ 측정 기준: NF 경유 SELECT 1

64KB 응답

2.237 ms

평균 응답 · p95 2.407ms

1MB 응답

20.84 ms

RX 직접 20.73ms · 차이 0.11ms

30ms 초과 지연

0 건

이번 시험에서 미발생

6. 운영 적용

운영 DB 보호를 위한 우선 적용 대상

외부 서비스와 연결되고 개인정보·거래·업무 데이터를 처리하는 구간부터 검토합니다.

우선 적용 구간

외부 서비스와 주요 데이터가 연결된 시스템

- 고객 서비스의 웹·앱 서버
- 개인정보·거래정보 운영 DB
- 중요 내부 업무 시스템

고객 환경에서 확인할 사항

외부에서 내부 서버로 향하는 직접 접속 경로

- 정상 조회·입력·수정 요청의 호환성
- 관리망·백업망 등 우회 접속 경로
- 장애 시 서비스 영향과 복구 방식

적용 위치와 허용 업무는 고객 시스템별 사전 검토·PoC에서 확정합니다.

7. 적용 분야

중요한 운영 DB를 사용하는 분야

보호 대상 데이터와 실제 업무 흐름을 기준으로 적용 가능성을 검토합니다.

분야	보호 대상·업무	적용 시 확인할 사항
병원·의료	진료·검사 DB, 진료정보 연계	업무 조회 유지와 민감정보 접근 제한
금융·핀테크	고객·거래 DB, 거래·조회 서비스	트랜잭션 정합성과 응답 지연
제조·물류	생산·업무 DB, ERP 연계	업무 처리 호환성과 장애 영향
공공·국방	기관 업무 DB, 시스템 연계	허용 경계와 감사 기록

8. 도입 검증

4주 PoC로 차단 효과와 업무 영향을 함께 검증합니다

사전 점검 3개 항목 · PoC 검증 7개 항목 · 고객별 합격 기준 사전 합의

사전 확인

연결 프로토콜·동시 연결
업무 변경 범위
우회 경로·장애 정책

보안 검증

직접 접속·탐색 차단
비인가 요청 제한
임의 외부 연결 차단

업무·운영 검증

조회·수정 정합성
처리량·응답시간
장애 복구·감사 추적

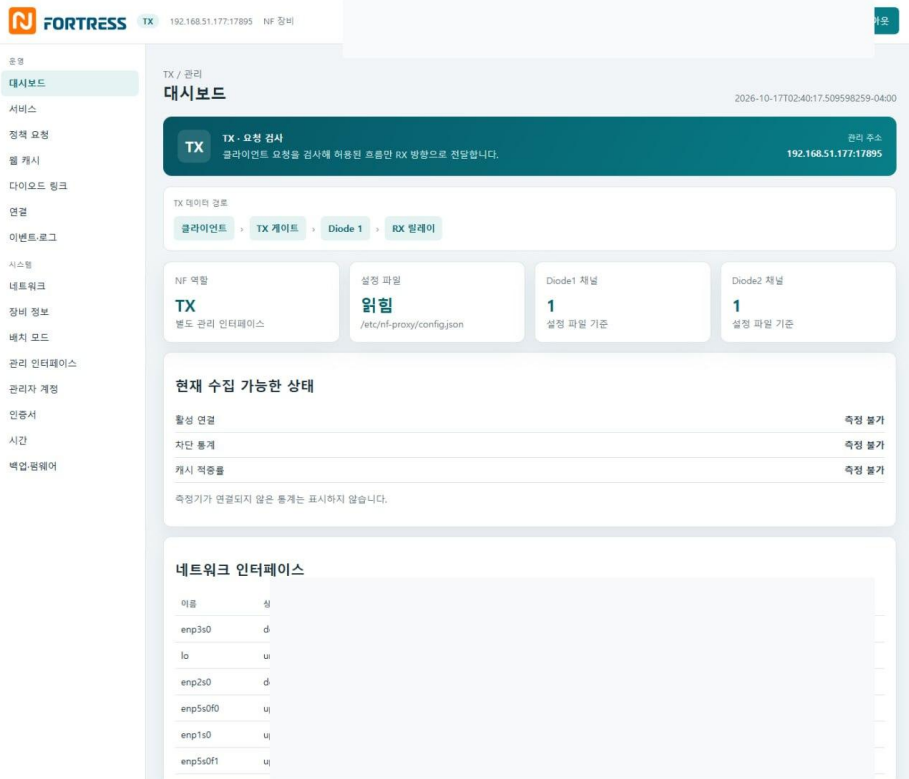
결과물: 차단된 것 · 허용된 것 · 업무 영향 / 합격 기준은 고객과 시험 전에 합의합니다.

NF 대시보드 화면

TX·RX의 분리된 관리 화면에서 연결 경로와 장비 상태를 확인합니다. (일부 운영 정보 비식별 처리)

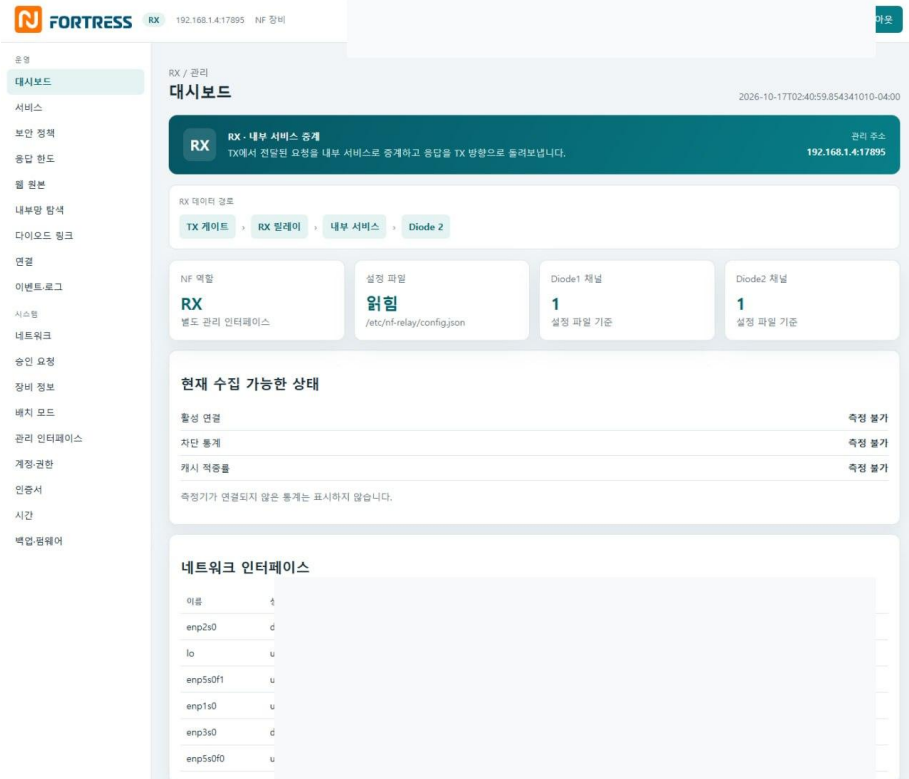
TX

관리 인터페이스



RX

관리 인터페이스



분리 운영: TX와 RX를 별도 UI로 관리
상태 점검: 설정·연결 상태 확인

경로 가시성: 데이터 흐름과 다이오드 채널 확인
관리 화면: 내부 운영 정보 비식별 처리

외부 직접 연결은 분리하고, 정상 업무는 유지합니다.

N-FORTRESS의 보호 경계와 업무 호환성을
고객 환경에서 함께 검증합니다.

ROCKGATE
CORE

PoC 및 기술 검토 문의 | rockgatecore.com | cmo@rockgatecore.com