OnPress OS™ 보안 및 망분리 아키텍처 백서

문서 유형: 기술 백서 (PDF) | 버전: V1.0 | 작성일: 2026년 7월 24일
작성: Core Company | 대상: CTO, CIO, 보안 책임자, 인프라 아키텍트

Executive Summary

OnPress OS™는 외부망 데이터 전송 0바이트를 설계 원칙으로 하는 온프레미스 sLLM(소형 거대 언어 모델) 통합 플랫폼입니다. 모든 AI 추론 연산이 고객사 사내 서버 내에서 완결되며, 입력된 데이터는 단 1바이트도 외부로 유출되지 않습니다.

본 백서는 OnPress OS™의 3중 망분리 아키텍처(물리 계층 → 네트워크 계층 → 애플리케이션 계층)와 E2E 암호화 파이프라인을 상세히 기술하며, 방산·제조·의료 등 보안 규제 산업에서의 실 적용 방안을 제시합니다.

1. 배경: 왜 온프레미스 AI인가

1.1 클라우드 AI의 구조적 보안 위험

위험 요소	설명	실제 사례
데이터 전송 노출	모든 프롬프트·문서가 외부 API 서버를 경유	GPT API에 기밀 도면 업로드 시 제3자 서버 저장
토큰 과금 폭발	컨텍스트 길이에 비례한 무한 과금	30분 작업에 $62~$124 자동 청구
서비스 종속성	API 중단 시 업무 전체 마비	클라우드 장애로 공장 AI 시스템 다운
규제 미준수	방산·금융·의료 분야 외부망 AI 사용 금지 규정 위반	방위사업청 보안규정, 의료법 제19조 위반

1.2 온프레미스 sLLM의 비교 우위

항목	클라우드 LLM (GPT-5.6 / Fable 5)	OnPress OS™
데이터 전송	외부 서버 경유	0바이트 (폐쇄망)
비용 구조	종량제 (예측 불가)	고정비 (월 정액)
규제 컴플라이언스	위반 가능성 존재	완전 준수
레이턴시	인터넷 속도 의존	로컬 추론 12ms

2. 3중 망분리 아키텍처

2.1 물리 계층 (Physical Layer)

• 에어갭(Air-Gap): AI 추론 서버와 외부망을 물리적으로 완전 분리
• NAS 금고: 모든 학습·추론 데이터를 암호화된 로컬 스토리지에 저장. AES-256 적용
• 단방향 게이트웨이: 모델 업데이트 시 외부→내부 단방향 전송만 허용. 내부→외부 트래픽은 iptables로 완전 차단

2.2 네트워크 계층 (Network Layer)

구성 요소	사양	설명
VLAN 분리	802.1Q 표준	AI 트래픽 전용 VLAN 태깅, 일반 업무망과 분리
MAC 주소 필터링	화이트리스트 기반	등록된 디바이스만 AI 노드 접근 허용
mTLS 상호 인증	X.509 인증서	AI 노드 ↔ NAS ↔ 클라이언트 간 양방향 TLS
로컬 DNS	Pi-hole + Unbound	외부 DNS 쿼리 차단, 내부 전용 호스트명 해석

2.3 애플리케이션 계층 & SDK 예시

```
const node = new OnPressNode({
endpoint: "http://192.168.1.100:8080", // 로컬 IP 전용
aesKey: process.env.LOCAL_VAULT_KEY, // 환경변수 주입
});

const result = await node.infer({
model: "onpress-13b-v2",
protocol: "ONVIF_RTSP",
prompt: "라인 #3 CCTV 시각 감시 이상 징후 분석"
});
// → { tokenCost: 0, latencyMs: 12, egressBytes: 0, dataLeakRisk: "none" }
```

3. E2E 데이터 암호화 파이프라인

단계	암호화 방식	키 관리
센서 → 수집 노드	TLS 1.3 + PSK	사전 공유키, 기기별 고유 페어링
수집 → 저장 (NAS)	AES-256-GCM	HSM 또는 로컬 볼트
저장 → 추론	메모리 내 복호화	추론 완료 즉시 메모리 소거 (memset_s)
저장 데이터 (At Rest)	LUKS2 + dm-crypt	TPM 2.0 바인딩

4. 규제 컴플라이언스 매트릭스

규제/인증	요구사항	OnPress OS™ 준수 방식
방위사업청 보안규정	군사 기밀 외부망 전송 금지	물리적 에어갭 + 제로 이그레스
ISMS-P	개인정보 암호화·접근 통제	AES-256 + RBAC 접근 제어
GDPR Art.32	처리의 안전성 확보	E2E 암호화 + 데이터 현지화
HIPAA	의료정보 전송 시 암호화 필수	TLS 1.3 + 저장 데이터 암호화