WHITE BOOK · CONFIDENTIAL REVIEW

The White Book of GNX Identity-to-Execution Logic Engine

검증·라이선스 계약용 설명서

입력·신원·표시상태·세션증거·실행권한을 하나의 검증 가능한 증거 체인으로 묶어, 조건 없는 실행을 fail-closed 방식으로 차단하는 실행통제 엔진

문서명	The White Book of GNX Identity-to-Execution Logic Engine
문서상태	Enterprise Review Draft · License Table Edition
버전	v1.0 · GNX Identity-to-Execution Edition
기준일	2026-05-02
작성주체	주식회사 지엔엑스_GNX Co., Ltd. · CEO Kim Chul
적용표면	logicnoid.co.kr · www.logicnoid.co.kr · api/admin/verify/docs.logicnoid.co.kr · AWS EC2 · CloudFront · AWS WAF
문서 통제	본 문서는 계약 전 검토 및 엔터프라이즈 보안 심사 목적의 공식 설명 자료이며, 운영 secret, admin private key, DB 원본 dump, 장기 토큰을 포함하지 않습니다.

목차

1. 문서 목적과 계약 테이블 포지션

1.1 목적

본 백서는 GNX Identity-to-Execution Logic Engine 을 엔터프라이즈 라이선스 테이블에 올리기 위한 검증·계약용 설명서다. 기존 청서와 백서는 로직노이드.com 의 실체를 “사이트가 아니라 작동하는 엔진”으로 설명했고, 첫 거래 단위를 Review, Trial, Production 의 단계로 분리해야 한다는 거래 원칙을 제시했다. 새 백서는 이 원칙을 유지하되, 신규 인스턴스에서 실제로 구현·검증된 WNS-bound execution gate, one-time execution handle, signed admin challenge, CloudFront 및 AWS WAF 구조를 기준으로 다시 정리한다.

계약 상대가 물을 핵심 질문은 “무엇을 사는가, 왜 지금 사야 하는가, 어떻게 검증할 수 있는가”이다. GNX 의 답은 명확해야 한다. 판매 대상은 웹사이트, PoC 화면, 단순 API 가 아니라 입력·신원·표시상태·세션증거·실행권한을 하나의 검증 가능한 증거 체인으로 묶어 조건 없는 실행을 fail-closed 방식으로 차단하는 실행통제 엔진이다.

1.2 비대체 포지션

본 제품은 IAM 대체재가 아니다. Okta, Microsoft Entra, CyberArk, Ping, SailPoint 와 정면 대체 경쟁하지 않는다. 본 엔진은 기존 IAM, API Gateway, AI Agent Runtime, 통신·금융 보안 시스템 앞단 또는 후단에 결합되는 execution evidence gate 다. 이 포지션은 고객사의 기존 보안 지출을 부정하지 않고, 인증 이후 또는 실행 직전의 증거 기반 통제 계층을 추가하는 방식으로 구매 저항을 낮춘다.

1.3 현재 검증 자산

- logicnoid.co.kr 루트 도메인은 EC2 A 레코드 기반 직접 랜딩 표면으로 유지한다.
- www, api, admin, verify, docs 표면은 CloudFront 및 AWS WAF 경유로 운영한다.
- origin.logicnoid.co.kr 은 CloudFront 원본 전용 EC2 표면이다.
- OpenAPI, Threat Model, Deployment Guide, Backup/Restore Runbook, Incident Response Runbook, Evidence Verification CLI 가 패키지화되어 있다.

요약문 본 백서의 첫 명제는 GNX 가 판매할 것은 페이지가 아니라 검증 가능한 실행통제 엔진의 실시권이라는 점이다. 고객은 기존 보안 체계를 버리는 것이 아니라 실행 직전의 evidence gate 를 추가로 검증한다.

2. 제품 정의와 IP 포지션

2.1 계약상 제품 정의

제품명은 GNX Identity-to-Execution Logic Engine 이다. 계약서상 표현은 “입력·신원·표시상태·세션증거·실행권한을 하나의 검증 가능한 증거 체인으로 묶어, 조건 없는 실행을 fail-closed 방식으로 차단하는 실행통제 엔진”으로 고정한다. 이 정의는 기능 나열이 아니라 구매 대상의 법적·기술적 경계를 규정한다.

2.2 WNS String-to-Execution Evidence Layer

WNS 의 핵심은 문자열 식별자를 네트워크 주소, 도메인 이름, 자원 위치, 외부 레지스트리 조회 키로 취급하지 않는다는 점이다. 문자열은 실행 제어를 위한 입력 증거로 수신되고, 정규화·fingerprint·receipt·상태 결합 판단을 거쳐 실행권한 판단의 전단 증거가 된다. 따라서 WNS Commit 은 단순 등록, URL routing, API key 발급이 아니라 string-to-execution evidence layer 다.

2.3 Evidence Chain 과 실행권한

엔진은 WNS receipt, Bident session proof, display 또는 policy condition, target identity, audience, nonce 를 결합한다. 이 조건이 충족될 때만 one-time opaque executionHandle 을 발급하고, consume 후 재사용을 차단한다. raw tunnelTicket, raw admin token, public vault, gnxceo fallback 은 새 엔진의 금지 구조다.

요약문 제품의 IP 포인트는 문자열·신원·표시·세션·정책·실행을 분리된 로그가 아니라 하나의 실행 증거 체인으로 결합하는 데 있다. 핵심은 “실행 허용”보다 조건 부족 시 “실행권한 미발급”을 기술적으로 강제하는 구조다.

3. 검증 아키텍처와 Evidence Surface

3.1 검증 표면

검증 표면은 www.logicnoid.co.kr, api.logicnoid.co.kr, admin.logicnoid.co.kr, verify.logicnoid.co.kr, docs.logicnoid.co.kr 로 분리된다. www 는 공개 검증 표면, api 는 엔진 API 표면, admin 은 signed admin challenge 기반 관리자 표면, verify 는 evidence verification 확장 표면, docs 는 제출 문서 표면이다.

3.2 검증 흐름

표준 흐름은 WNS commit, CSRF 발급, ZKV registration, Bident resonance, display lock, execution authorize, execution consume, audit receipt verification 순서다. 인수시험은 허용 경로만 확인하지 않는다. WNS 누락, Bident 누락, display 누락, nonce replay, handle replay, public vault probe, old policy endpoint 를 모두 차단해야 한다.

3.3 보안 게이트

Security Acceptance Test 는 CSRF, session proof, WNS requirement, display requirement, one-time handle, audit receipt, public vault removal, old policy migration 을 검증한다. Admin Signed Challenge 는 raw admin token 없이 관리자 세션을 바인딩한다. CloudFront 와 AWS WAF 는 public vault path 를 origin 에 도달하기 전 403 으로 차단한다.

요약문 검증 아키텍처의 핵심은 “보이는 데모”가 아니라 “재현 가능한 차단 증거”다. 고객은 API 응답, receipt, hash chain, WAF 차단, signed admin challenge 를 통해 엔진 실체를 확인한다.

검증 게이트 현황표

게이트	상태	증거/비고
Runtime Health	PASS	health/ready, DB READY, Redis READY
Security Acceptance Test	PASS	CSRF, WNS, Bident, Display, Replay, Vault 제거 확인
Admin Signed Challenge	PASS	raw admin token 미반환, ADMIN_SESSION_BOUND
WNS-bound Execution Gate	PASS	WNS receipt, Bident, display condition 결합
One-time Opaque Execution Handle	PASS	1 회 consume 및 replay 차단
Audit Hash Chain	PASS	prev_hash, event_hash, receipt 구조
CloudFront / AWS WAF	PASS	api/admin/verify/docs/www 보호 및 vault path 403 차단
OpenAPI / Threat Model / Runbook / CLI	PASS	문서와 검증 도구 패키지화
Apex CloudFront Cutover	PENDING	logicnoid.co.kr apex 는 EC2 A 레코드 랜딩 표면 유지

4. 라이선싱 상품 구조와 거래 단위

4.1 Enterprise Review License

Review 단계는 고객이 기술 실체를 검토할 권리를 사는 단계다. 제공 범위는 제한 문서, OpenAPI, Threat Model, Evidence Verification CLI, Security Acceptance 결과, 제한 기술 질의응답이다. 제외 범위는 전체 소스코드, 운영 secret, admin private key, DB 원본 dump, 특허권 전체 양도, 무제한 독점권이다.

4.2 Acceptance Trial License

Trial 단계는 고객사 지정 use case 에서 제한 연동과 인수시험을 수행하는 단계다. 통신사는 fraud signal adapter 와 display/session interlock, 금융권은 suspicious transaction gate 와 case evidence receipt, AI/API 고객은 agent action preflight 와 API Gateway Evidence Gate 를 시험한다.

4.3 Production License

Production 단계는 기간, 사용량, 적용 시스템, 계열사, SLA, 모듈, 배포 방식, 독점 옵션을 별도 산정하는 운영 실시권이다. 기술 전체 양도나 특허권 양도가 아니라, 지정 범위 내 실행통제 엔진 사용권을 부여한다.

요약문 거래 구조는 검증권, 시험권, 운영권을 분리한다. 고객이 검증할수록 다음 단계의 책임과 비용이 커지고, GNX 는 핵심 IP 와 운영 비밀을 보호한다.

5. 계약 전 실사·위험 통제·제출 패키지

5.1 제출 패키지

제출 패키지는 White Book, Blue Book, IP Summary, OpenAPI, Threat Model, Deployment Guide, Backup/Restore Runbook, Incident Response Runbook, Evidence Verification CLI, 산업별 라이선스 패키지, 표준 NDA, Evaluation License, Trial License, Production License, 가격표로 구성된다. 각 문서는 “완료 선언”이 아니라 검증 가능한 해시와 게이트 상태로 관리되어야 한다.

5.2 위험 통제

계약 전 실사에서 고객에게 필요한 만큼만 검증시키고 운영 비밀은 제공하지 않는다. public vault 는 제거되어야 하며, raw admin token 과 raw tunnelTicket 은 반환하지 않는다. 백업에는 admin private key 가 포함될 수 있으므로 운영 백업은 root-only 로 잠그고, 외부 제출용 패키지는 sanitized 형태로 분리한다.

5.3 법무·FTO 필요 범위

IAM 연동, API Gateway 배치, 통신 fraud signal 연동, 금융 이상거래 신호 연동, AI Agent tool-call preflight, 개인정보·신용정보·통신정보 처리, audit receipt 증거능력, 공동개발 IP 귀속, source escrow, 독점 옵션은 별도 법무 및 FTO 검토 대상이다.

요약문 계약 전 실사의 목표는 모든 것을 공개하는 것이 아니라, 검증 가능한 증거와 차단 정책으로 제품 실체를 보여주고 권리·비밀값·소스·특허를 단계별로 통제하는 것이다.

6. 산업별 진입 전략과 결론

6.1 통신사 패키지

통신사 버전은 Adama Display Interlock 과 fraud signal adapter 를 중심으로 한다. 보이스피싱, 스미싱, 유심 변경, 고객센터 본인확인, 착신전환, 고위험 통신 세션에 대해 탐지 이후 실행권한을 증거 체인으로 통제한다.

6.2 금융권 패키지

금융권 버전은 suspicious transaction gate 와 case evidence receipt 를 중심으로 한다. 고액 이체, 신규 수취인 등록, 인증수단 변경, API 기반 지급 지시, AI Agent 기반 금융 행위에서 조건 부족 시 execution handle 을 발급하지 않는다.

6.3 AI Agent / API Gateway 패키지

AI/API 버전은 agent action preflight SDK 와 API Gateway Evidence Gate 를 중심으로 한다. 외부 API 호출, 데이터 수정, 결제, 메시지 발송, 권한 상승, workflow 실행 전 증거 체인을 요구한다.

요약문 GNX Identity-to-Execution Logic Engine 은 기존 보안 제품군을 대체하지 않는다. 각 산업의 기존 탐지·인증·게이트웨이 뒤에 붙어 실행 직전의 증거 기반 통제를 제공하는 것이 첫 시장 진입 전략이다.

부록 A. 회사 및 문서 정보

주식회사 지엔엑스_GNX Co., Ltd. · CEO Kim Chul
이메일: gnxceo@naver.com
주소: 강원특별자치도 삼척시 도계읍 도상로 340, 주식회사 지엔엑스