BUSINESS PARTNERSHIP PROPOSAL

라온시큐어의 Agentic AI 제품이 통제할 AI 에이전트를 공급합니다

그리고 그 대가로, 라온시큐어 제품 안에 상주하며 유지보수와 CS를 수행할 **AI 담당자**를 함께 제안합니다. 원격 접속이 아니라 상주입니다 — 접속하지 않습니다, 이미 안에 있습니다.

제안
genver / NeuralStudio

수신
라온시큐어

대상 제품
ONE Access · ONE Shield · ONE SOAR · ONE Hacker
OnePass · OmniOne Access · OmniOne Chain

문서
v1.0

00 — EXECUTIVE SUMMARY

제안 요지

두 회사가 서로에게 없는 것은 대칭이 아닙니다. 한쪽이 다른 쪽을 보완하는 관계가 아니라, **서로가 서로의 성립 조건**인 관계입니다.

라온시큐어의 조건

통제할 대상이 필요합니다

Agentic AI 라인업 넷은 모두 "AI 에이전트가 이미 있다"를 전제로 그것을 통제합니다. 그런데 지금 시장에 있는 것은 챗봇이고, **챗봇에는 DID를 발급할 이유가 없습니다** — 행위하지 않으므로 권한이 필요 없고, 권한이 없으면 권한 관리 제품이 앉을 자리가 없습니다.

genver의 조건

규제 시장의 자격이 필요합니다

genver는 AI 직원이 메일을 보내고 파일을 쓰고 셸을 실행하고 외부 사이트에 로그인하는 시스템입니다. 통제 대상 그 자체입니다. 그러나 **신원·가드레일·감사·검증 체계가 없어** 공공·금융 시장에 들어가지 못합니다.

그래서 진짜 제안

운영 인력을 드립니다

라온 제품 넷의 기대효과는 전부 "보안 담당자·IT 운영자"를 전제합니다. **AI가 대응하는데 그 AI를 사람이 운영합니다.** genver의 AI 직원이 그 자리에 앉습니다 — 고객사 안에 상주하면서.

한 문장

genver는 라온이 팔 제품의 대상을 만들고, 라온은 genver가 못 들어가는 시장의 자격을 만듭니다. 그리고 genver의 AI 직원이 라온 제품의 운영자가 됩니다.

제안하는 네 개의 결합점

#	라온 제품	genver의 대응 자산	결합 후
1	**ONE Access** OnePass · OmniOne Access	`agent_tokens` · `approvals` `sessions`	AI 직원이 **DID를 갖고 외부 시스템에 스스로 로그인**합니다
2	**ONE Shield**	LLM 호출 경로 (필터 0건)	프롬프트 인젝션 · Jailbreak · **나가는 PII** 방어 단, 값어치가 판마다 다릅니다 — §6.0
3	**OmniOne Chain**	감사 원장 3종 본사 보고 경로	AI 행위 감사 로그의 **위변조 불가 증명**
4	**ONE Hacker**	운영 점검 체인 (보안 점검 0개)	AI 에이전트 대상 모의 침투의 **첫 실전 타깃**
+	Upstage Solar 온프레미스 RAON x Upstage	온프레미스 모델 서버 이미 vLLM으로 동작 중	**옵션.** 공공·국방이 "국산 파운데이션 모델"을 요건으로 걸 때 **입찰 자격**을 만듭니다 — 성능 교체가 아닙니다

다만 먼저 갈라야 할 것 — genver는 판이 둘입니다

genver는 **인터넷 연결 판**과 **온프레미스(폐쇄망) 판**이 있고, 두 판은 LLM이 회사 밖에 있느냐 랜 안에 있느냐가 다릅니다. **그 차이가 라온 제품의 값을 뒤집습니다.**

인터넷 판에서는 데이터가 실제로 밖으로 나가므로 **ONE Shield의 PII 차단이 최우선**입니다. 온프레미스 판에서는 나갈 곳이 없어 **"유출 방지" 논거가 성립하지 않고**, 대신 **프롬프트 인젝션과 RAG 문서 오염**이 남습니다 — 폐쇄망일수록 그것이 더 위험합니다. **같은 제품을 두 판에 같은 말로 팔 수 없습니다.** 상세는 §6.0에 적었습니다.

그리고 역방향

OnePass·OmniOne Access 표준제안서에 SLA·원격지원·상주·장애대응 조항이 없습니다. 인증 제품이 멈추면 전 직원이 로그인을 못 하는데, 제안서가 약속하는 것은 "SE 배정" 한 줄입니다. 못해서가 아니라 **팔 것이 없어서**입니다 — 사람 엔지니어 상주는 원가가 맞지 않고, 원격지원은 폐쇄망에서 약속할 수 없습니다.

상주 AI가 그 칸을 채웁니다. 채우는 순간 유지보수가 비용에서 상품이 됩니다.

---

01 — PRODUCT UNDERSTANDING

라온시큐어 제품 이해

이 제안이 다루는 제품은 일곱입니다. **기존 라인업 셋(사람의 신원)**과 **Agentic AI 라인업 넷(AI의 통제)**으로 성격이 갈립니다.

기존 라인업 — 사람의 신원

OnePass

MFA 지원 통합 인증 플랫폼

사내 업무 시스템의 로그인을 하나로 묶습니다. FIDO(생체·PIN)·OTP·인증서와 **Windows Credential Provider**(OS 로그인)를 포함하고, SSO는 SAML 데이터 포맷과 JWT를 씁니다. **온프레미스 중심**이며 **폐쇄망 FIDO 인증을 명시적으로 지원**합니다.

OmniOne Access

클라우드 통합 계정 관리(SSO/IdP)

여러 SaaS를 한 번의 로그인으로 씁니다. **SAML · OAuth 2.0 · OIDC** 표준 IdP이고 **SCIM** 프로비저닝과 LDAP 인사 연동을 지원합니다. 네이버클라우드 기반 SaaS로 제공되며 사용자당 월정액입니다.

OmniOne

DID · VC 분산신원 플랫폼

분산신원(DID)과 검증가능자격증명(VC)의 발급·검증 인프라입니다. 모바일 신분증 **4,500만 발급** 실적을 갖고 있고, **OmniOne Chain**이라는 블록체인 원장이 함께 있습니다.

이 문서에서 계속 중요한 구분

OnePass는 인증수단이고, OmniOne Access는 IdP입니다. "어떻게 본인임을 증명하는가"와 "누가 신원을 발급해 표준 프로토콜로 넘겨주는가"는 다른 층이고, 겹치지 않고 위아래로 쌓입니다. 뒤의 §6에서 이 구분이 **genver의 두 판**과 정확히 대응합니다.

Agentic AI 라인업 — AI의 통제

ONE Access

AI 에이전트의 신분증 · 권한 관리

AI 에이전트에게 **DID를 발급**하고, 할 수 있는 일을 **VC로 위임**하고, 접근할 때마다 **VP로 검증**하고, 문제가 생기면 **즉시 회수**합니다. 겨냥하는 문제는 **Shadow Agent** — 개별 식별자 없는 AI는 사고가 나도 누가 했는지 추적할 수 없습니다. Human → AI Agent → Sub-Agent로 이어지는 위임 체인과 MCP 기반 리소스 접근을 다룹니다.

ONE Shield

AI 안전 가드레일

AI와 LLM 사이에 앉아 입출력을 검사합니다. **L1** 인코딩·난독화 탐지 / **L2** Jailbreak 시그니처 / **L3** OWASP LLM Top10 정책 / **L4** PII 익명화 / **L5** 유해콘텐츠. RAG 문서 포이즈닝과 MCP 도구 호출 가로채기도 범위입니다. 구조는 `Client → Inbound Filter → LLM → Outbound Filter` 입니다.

ONE SOAR

AI 자율 보안 관제 타워

자연어 명령을 받아 보안 제품들을 조종합니다 ("김라온 사원 개발팀 입사처리 해줘"). AI Agent 오케스트레이션 + 보안 RAG + 워크플로 엔진 + Tool Registry(MCP) 구성입니다. 차별점으로 **Upstage Solar와의 공동 사업 기반 온프레미스 소버린 AI 플랫폼**과 라온 보안 특화 SLM을 내세웁니다.

ONE Hacker

AI 모의 침투 테스터

PTG(Penetration Testing Graph)로 컴포넌트가 아닌 경로 단위 공격을 수행하고, **Oracle Verification**이 "실제로 뚫렸는지"를 비-LLM 백엔드로 확정합니다. 확장 영역으로 **기존 웹을 넘어 AI Agent 대상 모의 침투**를 제시하고 있습니다.

02 — DIAGNOSIS

진단 — 넷 다 통제 대상이 있어야 성립합니다

제품이 부족해서가 아닙니다. **먹일 것이 아직 없기 때문입니다.**

제품	무엇을 통제하나	성립 조건
ONE Access	AI 에이전트의 신원과 권한 (DID·VC·회수)	**권한을 위임받아 실제로 행위하는 AI**가 있어야
ONE Shield	AI ↔ LLM 사이의 입출력	**LLM을 반복적으로 부르는 AI**가 있어야
ONE SOAR	자연어 명령으로 보안 제품을 조종	**명령을 칠 운영자**가 있어야
ONE Hacker	AI Agent 대상 모의 침투	**공격할 AI Agent**가 있어야

ONE Access 자료가 말하는 **"수천 개의 AI 에이전트가 동시에 운영되는 환경"**은 고객이 스스로 만들어야 하는 것이고, 라온시큐어는 그것을 만들지 않습니다. 이것이 라인업의 구조적 공백입니다.

> **그리고 이 공백은 유리한 조건이기도 합니다**
>
> 대상이 없다는 것은 **레퍼런스가 아직 없다**는 뜻입니다. 첫 end-to-end 레퍼런스를 만드는 파트너를 지금 확보하면, 시장이 형성될 때 **표준이 그 레퍼런스의 모양을 따릅니다.**

03 — WHAT IS GENVER

genver — 챗봇이 아니라 AI 직원입니다

genver는 고객사 VPS 한 대에 **사용자 100명과 AI 직원 100명**을 함께 앉히는 업무 협업 플랫폼입니다. AI가 답을 주는 것이 아니라, **직원처럼 일을 끝까지 가져갑니다.**

VPS 한 대 기준
100 명 AI 직원

컨테이너
19 개

HTTP API
187 개

앱 단계 도구
63 종

DB 테이블
50 개

AI 직원이 실제로 하는 일

행위	구현	통제 필요성
메일을 보낸다	`Mail_send` · MTA 실물	대외 발송 = 되돌릴 수 없음
파일을 읽고 쓴다	`Drive_read` · 오브젝트 스토리지	고객 데이터 접근
업무 앱을 조종한다	앱 단계 도구 63종	업무 시스템 변경
외부 사이트에 스스로 로그인한다	Playwright · 자격증명 저장소	**현재 비밀번호 주입 방식**
다른 AI에게 일을 넘긴다	협의 · 위임 · 깨우기	위임 체인 추적
셸을 실행한다	`Bash`	임의 코드 실행
앱을 배포한다	배포 파이프라인	운영 환경 변경

> 핵심
>
> **이것이 ONE Access가 기다리던 통제 대상입니다.** 챗봇은 행위하지 않아 DID가 필요 없지만, 메일을 보내고 셸을 실행하고 외부 시스템에 로그인하는 개체는 **신원 없이는 운영될 수 없습니다.**

반대로, genver가 규제 시장에 못 들어가는 이유

솔직하게 적습니다. 이 표가 이 제안의 다른 절반입니다.

영역	genver의 현재	필요한 라온 제품
사람 인증	ID/PW 단일 인증	OmniOne Access · OnePass
MFA · SSO	**없음**	OnePass FIDO
AI 신원	단기 베어러 토큰 (2시간, 턴마다 발급)	ONE Access
AI 상호 검증	**없음** — 검증자가 발급자와 같은 DB를 봐야 함	ONE Access (VC/VP)
LLM 입출력 필터	**없음** — 정책 엔진은 부수효과만 검사	ONE Shield
프롬프트 인젝션 방어	**0건**	ONE Shield L2·L3
RAG 포이즈닝 방어	**없음** — 고객 문서를 통째로 색인함	ONE Shield
감사 무결성	평문 DB. 위변조 방지 장치 없음	OmniOne Chain
외부 사이트 로그인	**비밀번호를 브라우저에 주입**	ONE Access (VP 제시)
취약점 점검	**0건** — 운영 점검 체인에 보안 항목 없음	ONE Hacker
AI 기본법 대응 문서	**0건**	라온 컨설팅

패턴

genver는 대응할 자산을 절반 이상 갖고 있는데, 그것을 규제 언어로 번역한 문서가 0건입니다. 승인 체계·전결규정 엔진·근거 원장·감사 로그가 모두 구현되어 있습니다. 문서가 없을 뿐입니다. **라온시큐어는 그 번역을 20년 해 온 회사입니다.** §9에서 이것이 가장 먼저 돈이 되는 지점임을 설명합니다.

---

04 — SYNERGY I

시너지 I — 위임 체인이 실물로 있습니다

ONE Access 자료의 위임 체인 그림은 개념도입니다. **그 그림의 네 칸이 genver에 전부 대응물을 갖고 있습니다.**

ONE Access 자료의 개념	genver의 실물
(4)(5)(6) **Human → AI Agent 위임 VC**	사람이 특정 AI 직원을 호출하면 **그 직원 범위로 좁힌 토큰**이 발급됩니다
(7)(8)(9) **AI Agent → Sub-Agent 위임 VC**	위임 기능이 구현되어 있고, 데모에서 문서 작성 에이전트를 서브 에이전트로 호출합니다
Agent 간 A2A 상호 검증	협의(consultation) 체계 — 역할 기준으로 다른 AI에게 질의하고 응답받습니다
MCP를 통한 Resource Server 접근	앱 단계 도구 63종이 이미 그 형태로 동작합니다

AI 토큰 구조가 이미 VC의 모양을 절반 갖고 있습니다

genver의 현재 구조	ONE Access 대응
AI 직원 식별자	DID subject (Step 1 — 활성화)
권한 범위(scopes)	권한 VC의 주장 (Step 2 — 역할 위임)
만료 시각 — **2시간**	단기 자격증명
발급자 기록	Issuer
회수 시각 · 회수자	(Step 5 — 회수)
턴마다 재발급	**최소 권한 원칙(PoLP)이 이미 구현되어 있습니다**

없는 것은 하나입니다

검증 가능성. 지금은 토큰 해시를 genver 데이터베이스에서 조회해 검증합니다 — 즉 **검증자가 발급자와 같은 DB를 봐야 합니다.** 그래서 genver 밖의 어떤 시스템도 genver의 AI 직원을 검증할 수 없습니다.

VC/VP로 바꾸면 검증이 DB 조회가 아니라 **서명 검증**이 되고, 그 순간 **genver AI 직원이 고객사의 다른 시스템(그룹웨어·ERP·MCP 서버)에 스스로 접근할 수 있게 됩니다.** genver에게는 기능 확장이고, 라온시큐어에게는 **ONE Access의 첫 end-to-end 레퍼런스**입니다.

권장 PoC — 하나만 고른다면 이것입니다

> **AI 직원이 DID를 갖고 고객사 그룹웨어에 스스로 로그인합니다.**

지금 genver는 이것을 **브라우저 자동화 + 비밀번호 주입**으로 합니다. ONE Access를 붙이면 비밀번호가 사라지고 VP 제시가 됩니다.

데모가 강합니다

"이 AI가 누구인지 상대 시스템이 검증한다"가 화면에서 보입니다.

실제 약점이 없어집니다

비밀번호를 브라우저에 넣는 구조가 사라집니다.

첫 end-to-end 레퍼런스

자료의 위임 체인 그림이 실제로 돕니다.

Sub-Agent까지 한 번에

위임 기능이 이미 있어 (7)(8)(9)를 함께 시연합니다.

---

05 — SYNERGY II · 역제안

시너지 II — 드리는 것은 고객이 아니라 운영 인력입니다

라온 제품 넷의 "역할별 기대효과"를 다시 읽으면 전부 같은 전제를 깔고 있습니다 — **보안 담당자 · IT 운영자 · 관리자 · 사용자.**

ONE SOAR

누군가 자연어 명령을 **쳐야** 돕니다

ONE Shield

오탐이 나면 누군가 정책을 **고쳐야** 합니다

ONE Access

수천 에이전트의 라이프사이클을 누군가 **관리해야** 합니다

ONE Hacker

리포트를 누군가 **읽고 조치해야** 합니다

> **AI가 대응하는데, 그 AI를 사람이 운영합니다.**
> **genver의 AI 직원이 그 자리에 앉습니다.**

기존 유지보수와 무엇이 다른가

기존 — 원격 접속 모델

- 장애 발생 → 고객사에 **접속 승인 요청**
- 승인 대기 (폐쇄망은 방문 일정 조율)
- 접속 자체가 **감사 대상 이벤트**
- 세션 종료 후 맥락이 사라짐
- 엔지니어 1인이 여러 고객사를 순회
- SLA를 약속할 근거가 없음

제안 — 상주 모델

- 장애 발생 → **이미 안에 있습니다.** 접속하지 않습니다
- 대기 시간 **0**
- 접속 이벤트가 발생하지 않음
- 고객사별 맥락이 **지속적으로 누적**됨
- 고객사마다 전담 AI 담당자
- 상시 점검 결과가 **SLA의 근거**가 됨

일을 어디서 하는가는 이미 기준이 있습니다

genver의 CS 정책이 배치 기준을 한 문장으로 정해 두었습니다.

> **그 일에 필요한 입력 중, 옮길 수 없는 것이 어디에 있는가.**

OnePass 장애에 이 기준을 대면 이렇게 갈립니다.

이동 불가 — 고객사 쪽	이동 불가 — 라온 쪽
실패한 인증의 **그 순간** (타이밍·경합)	OnePass 소스와 저장소
사용자 단말의 FIDO 등록 상태	제품 전체 이력 (다른 고객사가 섞임)
인증 로그와 세션 상태	릴리스 권한
연동된 레거시 IAM의 실제 응답	—

양쪽에 다 있으므로 일을 쪼갭니다. 판단(범주 결정) · 디버깅(지점 특정) · 수정(코드 변경)으로 나누어, **디버깅은 고객사 상주 AI, 수정은 라온 본사**가 맡습니다. 둘을 잇는 것은 **진단서와 익명화된 재현 픽스처**입니다 — **고객 데이터는 나가지 않습니다.**

이 구조가 인증 제품에 특히 값진 이유

인증 장애는 곧 전사 마비입니다

대응 시간이 그대로 손실이고, 그 시간의 대부분은 **원격 접속 승인을 기다리는 시간**입니다. 상주 AI는 그 시간이 0입니다.

폐쇄망에서 원격 접속은 그 자체가 사고 경로입니다

라온의 주력 시장이 정확히 폐쇄망입니다. **폐쇄망은 기능 점검조차 밖에서 할 수 없습니다.** 지금 엔지니어가 폐쇄망 고객사에 들어가는 절차 자체가 감사 대상입니다.

그리고 여기에 라온시큐어만 풀 수 있는 역설이 있습니다

고객사가 "AI를 우리 망 안에 상주시킨다"를 받아들이려면 **그 AI를 신뢰할 근거**가 있어야 합니다. 상주 AI는 소스를 읽고 로그를 보고 컨테이너를 재시작합니다. "믿어 주세요"로는 공공·금융 계약이 되지 않습니다.

그 신뢰 근거를 라온시큐어가 팝니다

- 상주 AI에게 **고객사의 ONE Access 서버**가 DID를 발급합니다 (Step 1)
- 그 AI가 할 수 있는 일이 VC로 명시됩니다 (Step 2 — 소스 읽기 ○, 쓰기 ×)
- 접근할 때마다 VP를 제시하고 **고객사가 검증**합니다 (Step 3·4)
- 계약 종료 또는 이상 감지 시 **고객사가 즉시 회수**합니다 (Step 5)
- 모든 행위가 OmniOne Chain에 남습니다

발급자가 고객사이고 대상이 상주 AI라는 것이 핵심입니다. 자기 참조가 아닙니다. 고객사가 발급하고 고객사가 회수하는 신원 위에서만 상주가 도는 구조이고, **신원 발급 인프라와 상주 AI를 동시에 공급할 수 있는 회사는 라온시큐어뿐입니다.**

제안서의 빈 칸

항목	OnePass 표준제안서	OmniOne Access 표준제안서
SLA	**없음**	**없음**
원격지원	**없음**	**없음**
상주	**없음**	**없음**
장애대응 체계	**없음** (Cached Login 등 제품 기능만)	**없음** (Web OTP 비상용만)
기술지원	"안정적 기술 지원" 언급	"제품/시스템 기술 지원, SE 배정"

> **상주 AI가 이 칸을 채우면 유지보수가 비용에서 상품이 됩니다.** genver가 설계해 둔 SLA 체계 — 점검 체인 · 오류 예산 · 월간 SLO 달성률 — 이 **그대로 계약서의 숫자**가 됩니다.

---

06 — ARCHITECTURE

일체화 아키텍처 — 두 판과 축 넷

먼저 판을 갈라야 합니다. genver는 인터넷 연결 판과 온프레미스 판이 있고, **라온 제품의 값이 판마다 뒤집힙니다.**

※ 별도 대에 서는 것 셋 — OnePass 서버(권장 8Core/32GB) · ONE Shield L5(GPU) · 온프레미스 모델 서버(GPU). genver 표준 VPS에는 GPU가 없습니다.

0 먼저 — genver는 판이 둘이고, 라온 제품의 값이 판마다 뒤집힙니다

이것을 세우지 않으면 아래 네 축의 우선순위가 어긋납니다

genver는 코드가 한 벌이고 **환경변수가 판을 정합니다.** 그런데 두 판은 LLM 조달 구조가 근본적으로 다르고, 그 차이가 라온 제품의 값을 바꿉니다.

	인터넷 연결 판	온프레미스(폐쇄망) 판
LLM 위치	외부 게이트웨이 — **회사 밖**	고객 GPU 서버 — **랜 안**
소유자	본사	**고객**
실측 구성	상용 모델 + 폴백	DGX Spark 121GB · vLLM · ctx 32,768
프록시 자리	게이트웨이 자체	**이미 차 있습니다** — OpenAI 호환 프록시가 앉아 auth·usage를 계량
임베딩	채팅과 같은 URL	**별도 vLLM** — 다른 포트, 다른 호출자
웹검색	게이트웨이 플러그인	내부 메타검색 엔진
턴당 LLM 호출	**3회**	**20회** — 작은 모델이 턴당 한 걸음만 딛기 때문
AI SLO	본사 책임 — **계약 포함**	고객 책임 — **계약 제외**
데이터 외부 유출	있습니다	없습니다

맨 아랫줄 둘이 전부를 결정합니다.

인터넷 연결 판 — 나가는 데이터를 막는 것이 전부입니다

이 판에서는 고객사 문서와 대화가 **실제로 회사 밖으로 나갑니다.** 그리고 지금 genver가 그 경로에 가진 방어는 **0입니다** — 전결규정의 검토 계층은 메일 발송 직전에 정규식 한 겹을 걸 뿐이고, **프롬프트로 나가는 것은 아무도 보지 않습니다.**

ONE Shield L4 (PII 익명화)

최우선. 유일한 통제점이고 지금 비어 있습니다.

ONE Shield L1~L3

높음 — 외부 문서와 웹검색 결과가 그대로 프롬프트에 실립니다.

OmniOne Access

딱 맞습니다 — SaaS IdP에 SaaS 플랫폼. SCIM으로 조직도까지.

ONE Access · OmniOne Chain

유효. 앵커링 경로도 단순합니다.

온프레미스 판 — 유출 논거가 사라지고, 더 위험한 것이 남습니다

> **정직하게 적습니다. 이 판에서는 ONE Shield의 대표 논거인 "기밀·정보 유출 방지"가 성립하지 않습니다.** 데이터가 랜 밖으로 나가지 않기 때문입니다. **차단할 외부가 없습니다.**
>
> **그런데 남는 것이 있고, 그것이 오히려 폐쇄망에서 더 위험합니다.**

위협	폐쇄망에서 유효한가
PII 외부 유출	약해집니다 — 나갈 곳이 없습니다
프롬프트 인젝션	**그대로 유효** — 내부 문서·메일·웹페이지가 프롬프트에 실립니다
RAG 문서 포이즈닝	**더 위험합니다** — 폐쇄망은 "내부 문서는 안전하다"고 가정하기 쉽습니다
도구 오남용	**그대로 유효** — 셸·배포·메일 도구를 AI가 쥐고 있습니다
내부자 위협	**더 중요해집니다** — 외부 통제선이 없으므로

폐쇄망 고객사는 **"망이 닫혀 있으니 안전하다"**를 전제로 삽니다. 그 전제에서 가장 위험한 것은 **이미 안에 들어온 오염**입니다. 오염된 문서 하나가 색인되면 그것을 참조하는 직원 전원이 감염되고, **폐쇄망이라는 이유로 아무도 의심하지 않습니다.**

> **그래서 제안**
>
> **폐쇄망에서 ONE Shield의 논거를 "유출 방지"가 아니라 "오염 탐지"로 바꾸시길 제안합니다.** 논거를 바꾸면 주력 계층도 바뀝니다 — L4가 아니라 **L2·L3와 RAG 검사**입니다. 그리고 이 논거는 경쟁사가 따라 하기 어렵습니다. 망분리를 판 회사일수록 "닫힌 망 안의 오염"을 말하기 껄끄럽기 때문입니다.

자원 — 온프레미스 판에 L5를 넣을 자리가 없습니다

실측 구성이 이렇습니다. DGX Spark 통합메모리 **121GB**에서 채팅 vLLM이 45%를 쓰고, 나머지를 genver 스택과 임베딩 vLLM이 나눠 씁니다. ONE Shield L5는 여기에 L40S 1장을 더 요구합니다. **폐쇄망 고객사에 GPU를 추가로 요구하면 그것은 새 하드웨어 계약입니다.** L1~L4가 CPU로 도는 판이 없으면 이 판에서는 ONE Shield를 팔 수 없습니다.

그리고 역설 — 필터가 덜 필요한 판에서 비용이 6.7배 큽니다

판	턴당 LLM 호출	필터 지연 누적 (150ms 기준)
인터넷 연결 판	3회	**0.45초**
온프레미스 판	**20회**	**3초**

온프레 판이 20인 이유는 작은 모델이 턴당 한 걸음만 딛기 때문이고, 그 구조는 바뀌지 않습니다. **그래서 1단계 PoC를 인터넷 판에서 먼저 합니다**(§9).

Upstage Solar의 자리 — 축이 아니라 조달 옵션입니다

genver는 온프레미스 LLM을 이미 돌리고 있습니다. 그래서 Solar는 없는 것을 채우는 것이 아니라 기존 모델을 바꾸는 것이고, 교체 비용은 환경변수 두 줄입니다.

> **바꿀 이유는 성능이 아니라 자격입니다.** 현재 실측에 쓰는 것은 해외 오픈 모델입니다. 공공·국방 입찰이 **"국산 파운데이션 모델"**이나 **"AI 주권"**을 요건으로 걸면 이 구성으로는 답할 수 없습니다. 라온시큐어가 *RAON x Upstage — 국내 유일 소버린 AI 보안 체계*를 내세우는 것이 정확히 그 요건을 겨냥한 것입니다.
>
> **즉 Solar의 값은 기술 스택이 아니라 입찰 자격이고, 그래서 전제가 아니라 옵션입니다** — 필요한 고객사에만 켭니다. 켤 때 확인할 것은 vLLM의 도구 호출 파서 대응 여부와 컨텍스트 창입니다(§10).

1 신원 — 사람과 AI는 다른 제품이 맡고, 사람 쪽은 판이 둘입니다

OmniOne Access · OnePass · ONE Access

제안서를 대조하면 두 인증 제품의 역할이 갈립니다.

	OnePass	OmniOne Access
포지션	MFA 인증 통합 (업무·OS Level)	클라우드 SSO / IdP
SSO 표준	SAML **데이터 포맷** · JWT OIDC·OAuth는 제안서에 없음	**SAML · OAuth 2.0 · OIDC IdP**
배포	**On-Premise 중심** (Hybrid·Cloud 지원)	**네이버클라우드 SaaS**
폐쇄망	**FIDO 완벽 지원 명시**	제안서에 언급 없음
프로비저닝	조직/사용자 동기화	**SCIM** · REST API · LDAP 인사 연동

그래서 genver의 두 판에 그대로 대응합니다. genver는 이미 클라우드 판과 온프레미스 판으로 갈려 있고, 라온 제품도 같은 선에서 갈립니다.

	genver 클라우드 판	genver 온프레미스·폐쇄망 판
IdP	**OmniOne Access** (OIDC)	**OnePass** (SAML·JWT)
인증수단	OnePass FIDO	OnePass FIDO — 폐쇄망 지원
프로비저닝	**SCIM**	REST API
LLM	외부 게이트웨이	고객 GPU + vLLM (Solar는 옵션)

genver 쪽 작업은 어느 판이든 같습니다. 인증 API가 3개뿐이고 세션이 DB의 난수 토큰이므로 **발급 경로만 바뀌고 세션 구조는 그대로입니다.**

SCIM의 값이 생각보다 큽니다

genver는 조직도 구성원과 로그인 사용자를 일부러 분리해 두었습니다 — 조직도의 사람 대부분은 로그인하지 않기 때문입니다. 그런데 **그 조직도를 갱신할 경로가 지금 없습니다.** SCIM이 그 자리를 정확히 채웁니다.

Step-up이 붙을 자리가 이미 있습니다

genver에는 **사람 승인 게이트**가 구현되어 있습니다 — 메일 발송 · 배포 · 운영 조치 · 외부 공유 · 자격증명 입력. 되돌릴 수 없는 행위에 재인증을 거는 것은 자연스럽고, **승인 화면에 서명이 붙으면 그 승인이 부인방지 대상이 됩니다.** 라온 인증 제품이 **AI 승인 워크플로의 인증 수단**이 되는 첫 사례입니다.

AI 쪽 — DID를 어디에 매다는가

설계 결정이 하나 있고, 이것을 틀리면 재파견이 깨집니다. genver의 AI 직원에는 두 개의 축이 있습니다.

축	범위	DID 체계에서의 역할
직군 job_family	전사 안정 — 카탈로그가 정의	**VC의 주장(claim)**으로 들어갑니다
개체 식별자 ai_id	VPS 로컬 — 고객사가 생성	**DID subject**가 됩니다

DID를 직군에 매달면 안 됩니다. 같은 직군의 직원 100명이 같은 DID를 갖게 되고, 그러면 ONE Access가 해결하려는 **Shadow Agent 문제가 그대로 재현됩니다.** DID는 개체 식별자에, 직군과 능력은 VC의 주장에 넣습니다.

이 배치가 **승급**과도 맞습니다. 같은 직원에게 새 직군을 주는 것은 **DID는 유지한 채 VC만 재발급**하는 것이라 기억과 신원이 함께 보존됩니다.

2 가드레일 — ONE Shield가 앉을 자리는 하나가 아닙니다

통합 설계에서 실제로 풀어야 할 것 셋

ONE Shield의 구조가 `Client → Inbound Filter → LLM → Outbound Filter`이므로 **OpenAI 호환 프록시 자리에 앉는다**는 점에서 genver와 맞습니다. 붙는 순간 얻는 것이 큽니다.

ONE Shield 계층	genver의 현재
L1 인코딩·난독화 탐지	**없음**
L2 Jailbreak 시그니처	**없음**
L3 OWASP Top10 for LLM	**없음**
L4 PII 익명화	발송 직전 **정규식 한 겹**뿐
L5 유해콘텐츠	**없음**
MCP 도구 호출 가로채기	정책 엔진이 **부수효과만** 검사

> **다만 "환경변수 하나로 끝난다"는 아닙니다**
>
> genver 코드를 확인한 결과 세 가지를 미리 풀어야 합니다. 협업 시작 후에 발견하면 일정이 밀리는 것들이라 먼저 공유합니다.

1. 호출자가 넷이고, ONE Shield는 넷을 구분하지 못합니다

LLM 기본 주소를 읽어 **직접** 호출하는 곳이 넷입니다 — 플랫폼, **에이전트 워커(플랫폼을 경유하지 않습니다)**, 업무 앱들, 색인기.

전부 같은 곳을 가리키면 **한 지점에서 보는 것 자체는 됩니다.** 문제는 그다음입니다 — **ONE Shield 입장에서 넷이 전부 같은 클라이언트로 보입니다.** 어느 AI 직원의 어느 턴에서 온 요청인지 알 수 없고, 그러면 **주체별·직군별 정책을 걸 수 없습니다.** 전역 임계값 하나로 돌면 오탐 시 전원이 막힙니다.

> **해법이 축 1과 이어집니다.** 헤더에 AI 직원 식별자와 직군을 실어 보내면 되고, 그것은 곧 **VC의 주장을 헤더로 내리는 것**입니다. 즉 축 1을 먼저 하면 축 2의 정책 입력이 생깁니다.

2. RAG 포이즈닝은 채팅 프록시 자리에서 잡히지 않습니다

genver의 임베딩은 **별도 경로**입니다. 채팅 vLLM이 아니라 별도 인스턴스로 가고, 호출자도 플랫폼이 아니라 **색인기**입니다. 그리고 문서가 오염되는 시점은 **색인 시점**이지 채팅 시점이 아닙니다.

채팅 프록시 자리에만 앉으면 오염된 문서를 **이미 색인이 끝난 뒤에야** 만나고, 그때는 "이 조각이 이상한가"만 볼 수 있어 문서 단위 판단이 안 됩니다. **색인 경로에 검사 지점이 하나 더 필요합니다.**

다행히 그 자리는 축 4에서 genver가 이미 식별해 둔 결함(문서 색인 범위 미검사)과 **같은 자리**라 한 번에 고칠 수 있습니다.

3. 온프레미스에서는 프록시 자리가 이미 차 있습니다

§6.0에 적은 대로 온프레미스에서는 OpenAI 호환 프록시가 이미 앉아 auth와 usage를 계량합니다. **ONE Shield를 앞에 체인할지, 그것을 대체할지**를 정해야 합니다. 대체하면 계량 기능을 ONE Shield가 대신해야 하고, 체인하면 §6.0의 지연 계산이 그대로 얹힙니다.

> **선행조건 셋**
>
> **1. 지연 실측** — 턴당 호출 수에 곱해집니다. 입력만인지 출력도인지, 호출마다인지 턴 경계인지를 실측 후 정합니다.
>
> **2. GPU** — L5는 L40S 1장. 온프레 GPU는 이미 vLLM 둘이 나눠 쓰고 있습니다. **L1~L4 CPU 판이 없으면 폐쇄망에서는 팔 수 없습니다.**
>
> **3. 자원 슬라이스** — genver 쪽 0단계 작업. 슬라이스 없이 컨테이너를 하나 더 넣으면 필터 폭주가 AI 직원 전체를 함께 죽입니다.

3 감사 — 해시 체인 + OmniOne Chain 앵커링

기술 작업보다 계약 작업이 큽니다

genver의 감사 자산은 셋입니다 — **감사 로그**(누가 무엇을 했나, 거부도 남습니다), **근거 원장**(모든 수치가 지나갑니다), **전결 판정 기록**(규칙이 막거나 통과시킨 기록).

셋 다 고객사 VPS 안의 평문 데이터베이스에 있습니다. **그 VPS의 root를 가진 사람은 고칠 수 있고, 고쳤는지 알 방법이 없습니다.** AI 기본법의 투명성 요건과 금융권 감사 요구에 이 상태로는 답할 수 없습니다.

제안하는 형태는 이렇습니다.

1. 고객사 VPS에서 감사 원장 3종에 **해시 체인**을 겁니다 (앞 행의 해시를 다음 행에 넣습니다)
2. 주기적으로 **체인의 머클 루트만** 본사에 밀어 올립니다
3. 본사가 그 루트를 **OmniOne Chain에 앵커링**합니다

> **내용은 나가지 않고 해시만 나갑니다.** 이것이 고객사 동의를 받을 수 있는 유일한 형태입니다 — 계약서에 적을 것이 **"감사 로그의 해시" 한 줄**이면 고객사가 동의할 수 있습니다.
>
> **폐쇄망 앵커링은 정책 문제이지 기술 문제가 아닙니다.** 고객사 안에 체인 노드를 두면 고객이 위변조할 수 있는 체인이라 "위변조 불가"의 근거가 약해집니다. 밀기 경로로 해시만 올려 본사가 앵커링하는 구조가 현실적입니다.

4 검증 — ONE Hacker가 빈 칸을 채웁니다

그리고 첫 회차 시나리오를 genver가 제공합니다

genver는 운영 점검 체인 15개를 설계했는데 **보안 점검이 하나도 없습니다.** 그리고 그 점검 설계의 원칙이 ONE Hacker와 같습니다.

> **점검은 컴포넌트가 아니라 체인 단위이고, 실제 경로를 써야 한다 — 점검용 특별 엔드포인트는 그 경로만 검증한다.**

ONE Hacker의 **PTG**가 정확히 체인 단위 점검이고, **Oracle Verification**이 "실제로 뚫렸는지"를 확정합니다. genver의 점검 목록에 보안 체인을 추가하면 **하나의 상황판에서 가용성과 보안 태세를 함께 봅니다.**

제안 — 첫 회차 타깃 목록을 genver가 제공합니다

genver는 자체 설계 검토에서 **공격 표면 12개를 이미 문서로 식별해 두었습니다** — 스토리지 키 이름공간, 문서 색인 범위 검증, 앱 토큰 스코프, 부트스트랩 엔드포인트, 관리자 폴백 경로, HTML 렌더 후 PII 검사, 도구 게이트 누락, 브라우저 오리진 검증, 토큰 스코프 단일 검사점, 셸 도구 격리, 봉인 파일 목록 드리프트 등입니다.

일부는 이미 알려진 결함입니다. 그래서 첫 회차는 발견이 아니라 확인입니다 — 그리고 그것이 오히려 좋습니다. 알려진 것을 잡지 못하면 도구를 믿을 수 없고, 잡으면 미지의 영역으로 갈 근거가 생깁니다. **ONE Hacker의 정확도를 객관적으로 증명할 수 있는 벤치마크 세트**를 genver가 제공하는 셈입니다.

---

07 — BOUNDARY

경계 — ONE SOAR와 genver-agent는 같은 자리를 노립니다

이것을 먼저 정리하지 않으면 통합이 실패합니다. 둘 다 "자연어 명령 → 계획 → 도구 호출 → 실행"이고, 둘 다 오케스트레이션 레이어입니다.

	ONE SOAR	genver-agent
오케스트레이션	AI Agent	supervisor + 워커
추론	Upstage Solar · 보안 특화 SLM	게이트웨이 모델
지식	보안 RAG	문서 색인 + 전결규정(OJT)
실행	워크플로 엔진 · Tool Registry(MCP)	도구 레지스트리 · 앱 단계 63종
통제	제안서에 명시 없음	정책 엔진 · 승인 게이트 · 전결규정

겹치는 채로 통합하면 **도구 레지스트리가 둘이 되고 감사 로그가 갈라집니다.** 그러면 "누가 무엇을 했나"에 두 개의 답이 생기고, 둘 다 불완전합니다.

제안하는 경계

ONE SOAR는 genver의 전문앱으로 들어옵니다.

genver-agent가 직원이고, **ONE SOAR의 워크플로 엔진이 그 직원의 도구**입니다. 판단 근거는 genver의 기존 기준 그대로 — **주문자가 누구인가.** 보안 워크플로의 주문자는 고객사 보안팀이고, 그것은 파트너 소유의 전문앱입니다.

반대 방향이 안 되는 이유는 하나입니다. ONE SOAR의 대응 대상은 **보안 사건**이고 genver의 대상은 **업무**입니다. 업무를 보안 컨트롤 타워 밑에 두면 모든 업무가 보안 사건으로 모델링되고, 그러면 CS 원인 분류가 심각도 등급으로 뭉개집니다.

이 배치의 부수 효과가 라온시큐어에게 유리합니다

ONE SOAR의 시나리오("김라온 사원 개발팀에 입사처리 해줘")는 **genver의 사람 사용자가 치는 명령**이 되고, 그 명령이 genver의 승인 게이트를 지납니다. **ONE SOAR 제안서에 없는 것이 승인 체계인데, genver가 그것을 갖고 있습니다.** 퇴사 Kill-Switch처럼 되돌릴 수 없는 행위에 사람 승인이 붙는 것은 금융·공공 심사에서 반드시 요구되는 항목입니다.

---

08 — BUSINESS MODEL

사업 모델 — 본사 · 파트너 · 고객사 3층

genver는 **스튜디오(AI 직원 양성소) 자체를 파트너에게 판매하는 모델**을 이미 설계해 두었습니다. **라온시큐어가 그 파트너의 첫 사례로 가장 적합합니다.**

1 · 도메인이 보안이라 전 고객 공통입니다

파트너 모델의 대표적 함정은 "파트너 전문앱이 고객마다 달라 표준 배포에 못 들어가는 것" 입니다. **보안 전문앱은 전 고객 공통이라 이 함정에 걸리지 않습니다.**

2 · 파견할 곳이 있습니다

국내외 고객사 1,000곳 이상, 공공·금융 레퍼런스, 모바일 신분증 4,500만. **genver가 스스로 뚫을 수 없는 시장입니다.**

3 · 전문앱이 자기 제품의 운영앱입니다

파트너 모델 중 **유일하게 앱의 정확성을 파트너가 보증할 수 있는 경우**입니다. OnePass 운영앱의 동작이 틀리면 라온이 책임집니다 — 자기 제품이니까.

책임 배분

	genver 본사	라온시큐어 (파트너)	고객사
플랫폼 개발 · 배포 · 운영	●	—	—
보안 전문앱 제작	—	●	—
보안 AI 직원 양성 · 검정	—	●	—
신원 · 가드레일 · 감사 제품 공급	—	●	—
규제 대응 문서 (AI 기본법 등)	—	●	—
AI 직원 배치 (작업방)	—	—	●
전결규정 결정	—	—	●
DID 발급 · 회수	—	—	●
1차 CS (VPS 상주)	●	—	—
2차 CS — genver 버그	●	—	—
2차 CS — 라온 제품 버그	—	●	—

두 가지를 미리 합의해야 합니다

1. 배포·운영 권한은 본사가 유지합니다. 파트너가 배포 권한을 갖는 순간 형상의 정본이 둘이 되고, 트리 해시 기반 드리프트 감지가 무의미해집니다. 이것은 기술적 제약입니다.

2. CS 라우팅이 3자가 됩니다. genver의 CS 원인 분류에 **"라온 제품 버그"** 칸이 하나 늘고, 2차 판단이 *VPS → (genver 본사 / 라온)* 분기가 됩니다. 협의 체계가 이미 "받는 쪽 개인을 몰라도 역할로 넘긴다"를 지원하므로 구조 변경 없이 역할만 추가하면 되지만, **진단서에 "어느 제품의 형상인가"가 칸으로 있어야** 합니다.

---

09 — ROADMAP

로드맵 — 각 단계가 독립적으로 가치를 냅니다

PoC가 데모로 끝나지 않도록, **어느 단계에서 멈춰도 그 자체로 성과가 남게** 쪼갰습니다.

0단계 — genver 내부 선행작업

협업 전 · 자체 수행

신원 체계를 얹기 전에 genver 쪽에서 정리해야 할 것들입니다. **비용은 genver가 부담합니다.**

- AI 직원의 **직군 축 명시화** — 지금은 직함 문자열 매칭이라 권한 부여가 부정확합니다. 이 상태로 VC를 발급하면 **틀린 권한이 서명되어 나갑니다**
- **승인 만료 처리 연결** — 만료 로직이 있으나 호출되지 않아 승인이 무기한 대기 상태입니다. 여기에 Step-up 서명을 붙이면 무기한 유효한 서명이 됩니다
- **격리 관련 선결 항목** — 신원은 인가를 강하게 할 뿐 격리를 만들지 않습니다. **서명된 신원으로 뚫리면 사고가 감사 로그에 정당한 접근으로 남습니다**
- **자원 슬라이스 도입** — ONE Shield 컨테이너를 넣을 자리. 슬라이스 없이 넣으면 필터 폭주가 AI 직원 전체를 함께 죽입니다
- **형상 정보 노출** — 3자 CS 라우팅에서 "어느 제품의 형상인가"를 판정할 근거

1단계 — ONE Shield, 인터넷 연결 판에서 먼저 2~3주

두 판 중 인터넷 판을 먼저 하는 것이 이 단계의 핵심입니다. 이유가 셋입니다 — ① 이 판에서만 데이터가 실제로 회사 밖으로 나가고 그 경로의 방어가 0이라 **L4의 값이 최대**입니다. ② 턴당 호출이 3회라 **지연 부담이 6.7배 작습니다.** ③ **프록시 자리가 비어 있습니다** — 온프레는 이미 차 있어 체인 설계가 필요합니다.

- **genver 산출** — 프롬프트 인젝션 · Jailbreak · **나가는 PII** 방어
- **라온 산출** — ONE Shield의 **첫 AI 직원 환경 레퍼런스**. 챗봇이 아니라 한 턴에 도구를 여러 번 부르는 에이전트 트래픽입니다
- **결정할 것** — 입력만인가 출력도인가 · 호출마다인가 턴 경계인가 · **호출자 식별을 어떤 헤더로 넘기는가**
- **함께 해야 하는 것** — 색인 경로에 RAG 검사. **채팅 프록시 자리에서는 잡히지 않습니다**(§6 축 2)

온프레미스 판은 3단계 뒤로 미룹니다 — L1~L4 CPU 판의 존재 여부와 체인 설계가 확정되어야 하고, 논거도 **유출 방지에서 오염 탐지로 다시 써야** 합니다. **Upstage Solar는 이 단계에 넣지 않습니다** — 국산 파운데이션 모델을 요건으로 거는 입찰이 나올 때 켜는 옵션입니다.

2단계 — 사람 인증 2~4주 · 판에 따라 갈림

클라우드 판은 **OmniOne Access OIDC + SCIM**, 폐쇄망 판은 **OnePass SAML/JWT**. 세션 구조는 어느 쪽이든 그대로이고 발급 경로만 바뀝니다.

- 추가로 **승인 게이트에 Step-up 인증** — 되돌릴 수 없는 행위에 서명이 붙어 부인방지가 성립
- **라온 산출** — 라온 인증 제품이 **AI 승인 워크플로의 인증 수단**이 되는 첫 사례

3단계 — ONE Access 2~3개월 · 가장 값이 크고 가장 어려움

AI 토큰 체계를 DID/VC로 전환합니다. 열 대응은 §4의 표대로 이미 되어 있습니다. **권장 PoC는 "AI 직원이 DID로 고객사 그룹웨어에 스스로 로그인"**입니다. 위임 기능이 이미 있어 **Sub-Agent 위임까지 한 번에 시연**됩니다.

4단계 — 감사 앵커링 1~2개월 · 계약 작업이 더 큼

감사 원장 3종에 해시 체인 → 머클 루트를 본사 보고 경로에 태워 → OmniOne Chain 앵커링. **보고 항목이 고객 동의 범위라 계약서 작업이 기술 작업보다 큽니다.**

5단계 — ONE Hacker 상시 · 3단계 이후

운영 점검 체인에 보안 체인을 추가합니다. 봉인·스코프·격리가 선언에서 검증으로 바뀝니다. **3단계 이후인 이유는 점검 주체도 신원이 있어야 하기 때문입니다** — ONE Hacker의 접근 자체가 인가받지 않은 것이면 감사 로그가 오염됩니다.

6단계 — 역방향: 라온 제품의 상주 CS 사업 계약

genver의 CS 역할 체계를 라온 제품에 적용합니다. 진단서·픽스처 구조 그대로. **매출 규모로는 이 단계가 가장 클 수 있습니다** — 기존 고객사 1,000곳에 "제품 + 그 제품을 아는 AI 담당자"를 판매하고, **유지보수 계약을 구독으로 전환**합니다.

그런데 가장 빨리 돈이 되는 것은 제품 통합이 아닐 수 있습니다

즉시 착수 가능 · 개발 없음

genver의 AI 직원은 고영향 AI일 가능성이 높습니다. 투자심의·기업가치평가·자산관리 앱이 사람의 권리와 재산에 영향을 주는 판단을 합니다. AI 기본법(2026-01-22 시행)이 요구하는 것과 genver의 현재를 대조하면 패턴이 하나 보입니다.

법이 요구하는 것	genver의 현재
사전 고지	화면 표시는 있으나 **문서 없음**
위험 관리 방안	**없음**
설명 방안	근거 원장이 이미 근거를 남깁니다 — **자산은 있고 문서가 없음**
이용자 보호방안	**없음**
사람의 관리감독 체계	승인·전결규정·협의가 구현됨 — **자산은 있고 문서가 없음**
안전사고 모니터링	설계 완료, 구현 전

라온시큐어가 genver의 기존 자산을 AI 기본법 고영향 AI 대응 체계로 번역한 문서 한 벌을 만들면, 그것만으로 genver가 지금 못 들어가는 공공·금융 입찰에 들어갑니다. 개발 없이.

그리고 이것은 라온시큐어에게도 이득입니다 — **번역하다 보면 빈 칸이 드러나고, 그 빈 칸이 §6의 축 넷입니다.** 즉 컨설팅이 제품 판매의 진입로가 됩니다.

---

10 — OPEN QUESTIONS

확인 요청 — 로드맵이 이 답에 달려 있습니다

공개 자료만으로는 답할 수 없는데, **답에 따라 단계 순서와 일정이 바뀌는 것들**입니다.

#	질문	왜 이것이 순서를 바꾸는가
1	**ONE Access(AI 신분증)의 현재 성숙도** 표준제안서 또는 GA 여부	라인업 소개 자료에는 있으나 표준제안서를 확인하지 못했습니다. **3단계가 "붙이기"가 아니라 공동 개발이면 일정이 자릿수로 달라집니다.** 나쁜 소식이 아닙니다 — 요구사항을 함께 쓰게 된다는 뜻이고, genver의 기존 토큰 구조가 이미 그 요구사항의 초안입니다
2	**ONE Shield가 클라우드(SaaS)로도 서는가**	1단계를 인터넷 연결 판에서 먼저 하기로 잡았습니다(§9). **온프레미스 어플라이언스 형태만 있으면 그 순서가 깨집니다**
3	**ONE Shield에 호출자 식별을 넘길 수단** 헤더 · API 키 · 테넌트	genver는 LLM을 부르는 곳이 넷인데 **지금은 ONE Shield가 그 넷을 구분하지 못합니다.** 구분이 안 되면 전역 임계값 하나로 돌아야 하고, 오탐 시 AI 직원 전원이 막힙니다
3b	**임베딩·색인 경로도 검사하는가**	RAG 포이즈닝은 채팅 프록시 자리에서 잡히지 않습니다(§6 축 2). **문서 단위 검사 API**가 따로 있는지가 관건입니다
4	**ONE Shield의 배포 단위와 자원 요구**	L5가 GPU(L40S) 1장을 요구합니다. **L1~L4만 CPU로 분리 배포가 가능한가**가 폐쇄망 판의 성립 여부를 정합니다
5	**ONE Shield가 OpenAI 호환 프록시로 설 수 있는가**	1단계가 "코드 0줄"인지 "어댑터 개발"인지가 여기서 갈립니다
6	OnePass의 **OIDC 지원 여부**	제안서에는 SAML 데이터 포맷과 JWT만 확인됩니다. OIDC를 지원하면 폐쇄망 판의 연동이 훨씬 단순해집니다
7	**OmniOne Access의 온프레미스 구축 가능 여부**	현재는 네이버클라우드 SaaS입니다. 불가하면 폐쇄망 IdP는 OnePass 단독입니다
8	**OnePass 서버의 설치 위치**	권장 사양이 8Core/32GB인데 genver 표준 VPS가 8vCPU/32GB입니다. **같은 대에 올릴 수 없습니다.** 별도 서버 또는 IdP의 SaaS 사용을 전제해야 합니다
9	OmniOne Chain의 **폐쇄망 앵커링 방식**	축 3의 구체적 형태가 여기서 정해집니다
10	기존 **유지보수 계약 구조**	6단계는 기술이 아니라 계약 재설계입니다. 현재 유지보수 매출의 구조와 고객사 수를 알아야 상주 모델의 원가를 계산할 수 있습니다

미리 적어 두는 함정

정책은 어떻게 깨지는지를 함께 적어야 집행됩니다. 협업에서 실패할 수 있는 지점을 먼저 공유합니다.

오케스트레이션 레이어가 둘이 됩니다

ONE SOAR는 전문앱으로 들어옵니다(§7). **계약 전에 못 박습니다.**

감사 로그가 갈라집니다

도구 호출은 반드시 genver 정책 엔진을 지납니다. **라온 제품 호출도 예외 없이.**

가드레일 지연이 AI 직원을 못 쓰게 만듭니다

1단계에서 **호출별 실측**부터 합니다. 안 되면 턴 경계에만 겁니다.

폐쇄망에 GPU를 요구하게 됩니다

L1~L4 CPU 판을 기본으로 잡고 L5는 옵션으로 둡니다.

VC로 틀린 권한이 서명되어 나갑니다

0단계의 직군 축 명시화가 선행조건입니다.

폐쇄망에서 "유출 방지"로 ONE Shield를 팝니다

그 판에는 나갈 곳이 없습니다. 논거를 **오염 탐지**로 바꿉니다.

"환경변수 하나로 붙는다"고 약속합니다

호출자가 넷이고 **RAG는 채팅 프록시에서 안 잡힙니다.**

Upstage Solar를 전제로 놓습니다

온프레 LLM은 이미 돕니다. Solar는 **입찰 자격 옵션**입니다.

파트너가 배포 권한을 갖습니다

형상 정본이 둘이 되면 드리프트 감지가 죽습니다. **배포·운영은 본사 유지.**

VPS 한 대에 전부 올리려 합니다

OnePass 서버와 ONE Shield L5는 별도 대입니다. **자원 계산을 다시 해야 합니다.**

CS 라우팅에 라온 칸이 없어 전부 genver로 옵니다

진단서에 **제품 축**을 추가합니다(§8).

PoC가 데모로 끝납니다

각 단계가 독립적으로 가치를 내게 쪼갰습니다(§9).

11 — NEXT STEP

제안하는 다음 단계

STEP 1

기술 실무 미팅 (1회, 2시간)

§10의 확인 요청에 대한 답을 맞춥니다. 특히 **ONE Access 성숙도 · ONE Shield의 클라우드 제공 여부 · 호출자 식별 수단** 셋이 전체 일정을 정합니다.

STEP 2

genver 실물 데모

AI 직원 두 명이 시장조사 → 사업계획서 작성 → 상사에게 메일 검토 요청 → 전결규정 준수까지 수행하는 과정을 보여드립니다. **"통제 대상"이 실제로 어떤 모양인지**가 이 자리에서 확인됩니다.

STEP 3

1단계 PoC 착수

ONE Shield를 genver LLM 경로에 연결합니다. **코드 변경 없이 1~2주.** 결과가 좋으면 그 자체로 라온시큐어의 첫 AI 에이전트 환경 레퍼런스가 됩니다.

마지막으로

라온시큐어의 Agentic AI 라인업은 아직 통제할 대상이 없습니다.
genver는 아직 규제 시장에 들어갈 자격이 없습니다.
그리고 두 문제는 서로의 답입니다.

genver × 라온시큐어 협업 제안서

본 문서는 라온시큐어 공개 자료(Agentic AI 제품 라인업 소개 · OnePass 표준제안서 · OmniOne Access 표준제안서)와 genver 시스템 설계·구현 문서를 대조해 작성되었습니다.

genver / NeuralStudio

제안서 v1.0