AlonicOS

Agentic AI • Digitale Souveränität

SOUVERÄNE KI-AGENTEN · MADE IN EUROPE

Wenn KI zur Pflicht wird, ist Souveränität kein Feature — sondern die Voraussetzung.

AlonicOS ist das EU-gehostete, Single-Tenant-Betriebssystem für KI-Agenten. Auditierbar von der ersten Sekunde, produktiv in Tagen — und gebaut für eine Regulierung, die 2026 scharf gestellt wird.

DSGVO · EU AI Act · EU Data Act nativ

Ausgerichtet an BSI-C3A

2026 wird die Regulierung verbindlich. Der Markt rennt trotzdem.

Zwei Kräfte treffen aufeinander: ein scharf gestellter Rechtsrahmen und eine Adoptionswelle, die sich nicht aufhalten lässt. Wer KI-Agenten jetzt produktiv setzt, muss beides gleichzeitig bedienen — Tempo und Nachweisbarkeit.

DIE PFLICHT

02.08.2026

EU AI Act wird voll anwendbar. Verstöße: bis zu **35 Mio. €** oder 7 % des weltweiten Jahresumsatzes.

DER MARKT

+141 %

Anstieg der Agentic-AI-Ausgaben 2026 auf **201,9 Mrd. $** (Gartner). 40 % der Unternehmensanwendungen binden bis Jahresende Agenten ein.

90 %

der DACH-Unternehmen stärken aktiv ihre digitale Souveränität.

69 %

setzen auf EU-Rechenzentren, um Drittstaaten-Zugriffe zu vermeiden.

C3A

BSI-Kriterien für Cloud-Souveränität, seit April 2026 als Maßstab.

> **„Im Zeitalter der KI gewinnt nicht der Größte — sondern der Automatisierteste."**
>
> Die Frage ist nicht mehr *ob* Agenten — sondern auf welcher Plattform sie auditierbar laufen.

02 · DIE ANTWORT

Eine Plattform statt eines Dutzends Werkzeuge zum Selbst-zusammenbauen.

AlonicOS liefert das fertige Ergebnis — den laufenden Workflow, nicht den Bausatz. **~65 Dienste** als eine Auslieferung: Orchestrierung, Memory, Security, Observability und Geschäftskonnektoren.

RUNTIME

Agenten statt Chats

Mehrstufige Abläufe laufen als kontrollierte Workflows mit Temporal-Orchestrierung — nicht als lose Prompt-Ketten.

GOVERNANCE

Audit by design

Jeder Agentenschritt trägt Rolle, Modell, Tool-Aufruf, Kosten und Ergebnis im revisionssicheren Audit-Ledger.

SOUVERÄNITÄT

EU-Single-Tenant

Dediziertes Deployment im eigenen EU-Rechenzentrum, optional air-gapped. Cross-Tenant-Zugriff ist baulich ausgeschlossen.

ÖKONOMIE

Kosten pro Lauf — in €

Durchgängiges Kosten-Ledger, Budget-Bremse vor dem Lauf, ROI je Geschäftsprozess statt Pro-Sitz-Lizenz.

~65	~2 Tage	21 / 8	9
Dienste, eine Auslieferung	bis zum produktiven Workflow	Modelle über Provider	Security-Schichten

03 · GOVERNANCE IST TEIL DER RUNTIME

Nicht nachträglich zertifiziert. In die Laufzeit eingebaut.

KI-Sicherheit ist 2026 nicht mehr Input-Validierung. Neue Angriffsklassen — Prompt-Injection, Memory-Poisoning, Tool-Rug-Pulls — erfordern neue Schichten. AlonicOS integriert neun Verteidigungsebenen in die Runtime, nicht als Plug-in.

PROMPTGUARD · 9-SCHICHTEN-DEFENSE-IN-DEPTH

- L9 PromptGuard
- L8 Output-Filter
- L7 Memory-Quarantine
- L6 MCP-Integrity
- L5 Credential-Vault
- L4 Data-Residency-Gate
- L3 Tool-ACL & CaMeL-Tokens
- L2 Audit-Ledger
- L1 Temporal-Orchestration

RED-TEAM-BENCHMARK · GARAK

Angriffs-Erfolgsrate	8,76 % → 6,70 %
promptinject-Suite	73 % → 0 %

Interner Benchmark, keine externe Zertifizierung. Sieben Schichten produktiv aktiv, weitere im Shadow-Mode. Methodik auf Anfrage.

RECHTSSICHERHEIT

Eine renommierte deutsche Wirtschaftskanzlei prüft unsere KI-Implementierungen — von DSGVO bis EU AI Act. Art. 73-Tabletop-Drill am 12. Mai 2026 erfolgreich durchlaufen.

AlonicOS ist compliance-unterstützend, nicht compliance-zertifizierend, und ersetzt keine Rechtsberatung. Die Ausrichtung an BSI-C3A-Kriterien bedeutet keine Zertifizierung; die Hochrisiko-Einstufung nach EU AI Act verantwortet der Kunde als Betreiber.

04 · BEWEIS & ÖKONOMIE

Jeder Euro nachvollziehbar. Auf den Cent, pro Lauf.

Eine Transparenz, die kein Wettbewerber öffentlich zeigt: reale Kosten pro Ausführung. Vier produktive Workflows, wie sie heute bei Kunden laufen.

WORKFLOW	ERGEBNIS	PRO LAUF
Sales-Pipeline	Qualifizierte Leads, CRM-angereichert, mit Antwort-Entwurf	~0,08 €
Legal & Compliance	Strukturiertes Gap-/Konflikt-Memo mit Zitaten	~0,14 €
Markt-Resonanz	Wöchentliche Tiefen-Analyse, Delta + belegbare Quellen	~0,30 €
Content-Pipeline	Compliance-geprüftes Kurzvideo — Entwurf, nie auto-publiziert	~0,62 €

MODELLWAHL PRO SCHRITT

21 Modelle · 8 Provider · EU-Allowlist

Mistral & Aleph Alpha aus EU-Rechenzentren, Ollama lokal, dazu Claude, Gemini & GPT pro Arbeitspaket — mit automatischem Fallback. US-Modelle werden bei „EU-only" baulich blockiert.

LIVE-RAG · DAS DIFFERENZIERUNGSMERKMAL

Ihre Daten bleiben im Mandanten

Verträge, Preise und Datenblätter werden live zum Zeitpunkt der Frage gezogen — nicht hochgeladen, nicht kopiert, nicht trainiert. Qdrant + Apache-AGE-Knowledge-Graph.

05 · AUS DER PRAXIS FÜR DIE PRAXIS

Montag Pilot. Mittwoch validierter Workflow.

TAG 1 · VM

Design

Anforderung → YAML, Modell pro Schritt.

TAG 1 · NM

Integration

MCP-Adapter für SAP, Oracle, CRM.

TAG 1 · ABD

Validierung

Preflight + Kostenprognose.

TAG 2

Launch

Live in der Kunden-Oberfläche.

GF

Gerald Fehringer · KI-Praktiker

„Wir tragen AGENTIC nicht nur im Firmennamen — wir leben es. Jeden Tag." Praxiswissen macht er auf dem YouTube-Kanal **PraKItisch** verständlich: echte AGENTIC-Praxis statt KI-Bubble-News.

Use Case durchrechnen

30 Minuten mit Fachanwender — wir rechnen einen realen Anwendungsfall konkret durch, auf Wunsch mit Live-Demo.

Kontakt

coach@startvisor.ai

+49 1522 189 7460

startvisor.ai/aionicos

NC AGENTIC GmbH · Lilienstraße 11 · 20095 Hamburg · HRB 191086