

Behörde / Institution
Sebastian Weiss
Projektname
Sentinel
Verwaltungsebene
Bund
Website / URL
https://github.com/sebastianweiss83/sentinel-kernel
Einreichungskategorie
Künstliche Intelligenz
Möchten Sie das Projekt noch in einer zweiten Kategorie einreichen?
Transformation
Projektbeschreibung
Sentinel ist eine Open-Source-KI-Middleware für souveräne Entscheidungen und Nachweise, entwickelt für die Nachweispflichten des EU AI Acts (Art. 12, 13, 14 und 17).
Beschreiben Sie den technischen Innovationsgrad des Projektes und den Beitrag zur Verwaltungsmodernisierung.
Der technische Innovationsgrad von Sentinel liegt in der Architektur als „AI-Decision-Middleware“, die den deterministischen Nachweis stochastischer KI-Entscheidungen direkt im Code verankert. Anstatt Logs nachträglich über externe Monitoring-Tools zu aggregieren, fängt Sentinel den execution flow autonomer Agenten über native Python-Dekoratoren ab. Das System erzwingt eine In-Process-Validierung von Policies und schreibt Entscheidungspfade mathematisch verkettet und manipulationssicher in ein lokales, kryptografisch signiertes Datenformat. Die eigentliche Innovation ist die Entkopplung von globalen Cloud-Diensten: Sentinel realisiert diese Governance vollständig zustandslos und offline (Air-Gapped) und bricht das Paradigma, dass KI-Traceability rechenintensive Cloud-Schnittstellen benötigt. Für die öffentliche Verwaltung ist dieses Design ein digitaler Befreiungsschlag. Behörden scheitern beim KI-Einsatz oft an den Hürden des Datenschutzes und der Nachweisbarkeit bei automatisierten Bescheiden. Sentinel löst dieses Dilemma auf drei Ebenen: Erstens sichert die Offline-Fähigkeit absolute digitale Souveränität. Da keine Daten an US-Cloud-Infrastrukturen fließen, unterstützt das System die Anforderungen aus DSGVO, KRITIS und NIS2. Zweitens automatisiert Sentinel die Transparenzpflicht: Bei Widersprüchen gegen KI-gestützte Verwaltungsakte generiert das System auf Knopfdruck ein signiertes, auditfähiges PDF-Nachweispaket, das den Entscheidungsweg für Bürger und Gerichte lückenlos offenlegt. Drittens senkt es die Integrationshürde in veraltete staatliche IT-Infrastrukturen (Legacy-Systeme). Durch den minimalen Code-Overhead können Behörden moderne KI-Agenten agil auf eigener Hardware einführen, ohne langwierige IT-Modernisierungsprojekte starten zu müssen.
Welchen ökonomischen Nutzen hat das Projekt?
Der ökonomische Nutzen des Sentinel-Kernels von Sebastian Weiss liegt in der Vermeidung existenzbedrohender finanzieller Risiken und der drastischen Senkung operativer Compliance-Kosten. Angesichts drohender Bußgelder unter dem EU AI Act von bis zu 15 Millionen Euro oder 3 Prozent des weltweiten Jahresumsatzes fungiert Sentinel als direkte Absicherung. Die Middleware stellt die regulatorisch geforderte, lückenlose Rückverfolgbarkeit autonomer KI-Entscheidungen nach Artikel 12 automatisiert und manipulationssicher bereit. Gleichzeitig optimiert das Framework die interne Wertschöpfung in der Softwareentwicklung. Statt wertvolle Entwicklungsressourcen monatelang für den Aufbau einer eigenen Logging- und Audit-Infrastruktur aufzuwenden, lässt sich das System per One-Decorator-Integration in wenigen Minuten einbinden. Als Open-Source-Lösung spart Sentinel zudem teure, wiederkehrende SaaS-Lizenzgebühren von Drittanbietern und senkt so die Gesamtbetriebskosten (TCO).

Ein weiterer finanzieller Hebel liegt in der Effizienzsteigerung bei Prüfprozessen. Die Fähigkeit, auf Knopfdruck signierte, auditfähige PDF-Nachweispakete zu generieren, verkürzt die Vorbereitungszeit für Audits von Wochen auf wenige Stunden. Dies reduziert die Honorare für externe Berater und beschleunigt die Markteinführung (Time-to-Market) neuer KI-Produkte. In regulierten Märkten wie dem Finanzwesen oder bei kritischen Infrastrukturen (KRITIS) sichern sich Unternehmen so einen Wettbewerbsvorteil, da sie konforme KI-Systeme schneller produktiv schalten können. Zudem bietet der Verzicht auf US-Cloud-Abhängigkeiten infrastrukturelle Vorteile. Sentinel läuft vollständig offline und lokal. Unternehmen sparen dadurch unvorhersehbare Cloud-Traffic-Gebühren und nutzen kosteneffizient ihre bestehende Hardware, ohne sensible Daten an externe Server übertragen zu müssen.

Beschreiben Sie die Nachhaltigkeit der Lösung.

Die Nachhaltigkeit von Sentinel lässt sich in drei Dimensionen unterteilen: ökologische Ressourceneffizienz, technologische Langlebigkeit und digitale Souveränität für den Staat.

1. Ökologische Nachhaltigkeit (Grüne IT)

Sentinel bricht mit dem Trend, jede regulatorische Prüfung über energieintensive Cloud-Plattformen abzuwickeln. Da die Richtlinienprüfung (In-Process-Validation) vollständig lokal im Arbeitsspeicher erfolgt, entfällt der CO₂-intensive Datenverkehr zu externen Servern. Statt riesige, unstrukturierte Datenberge anzuhäufen, komprimiert das System Entscheidungsdaten sofort in kompakte, mathematisch verkettete Audit-Pakete. Durch den minimalen Rechenaufwand können Behörden bestehende Hardware ressourcenschonend weiternutzen, anstatt neue Serverfarmen aufzubauen.

2. Technologische Langlebigkeit und Investitionsschutz

Als quelloffene Software unter der freien Apache-2.0-Lizenz ist Sentinel unabhängig vom wirtschaftlichen Schicksal eines einzelnen Herstellers. Die Community kann den Code über Jahrzehnte pflegen. Das Framework bietet zudem Investitionsschutz: Ändert sich der Unterbau der verwendeten KI-Modelle, bleibt die Auditierungsebene von Sentinel unberührt. Da das System modular aufgebaut ist, lassen sich zukünftige Novellen des EU AI Acts über einfache Regel-Updates einpflegen, ohne die IT-Infrastruktur neu aufzusetzen.

3. Nachhaltige Verwaltung ohne Vendor-Lock-in

Für die öffentliche Verwaltung verhindert Sentinel die Abhängigkeit von privaten, monopolartigen Technologie-Konzernen und eskalierenden Abo-Gebühren (SaaS-Dilemma). Der Staat behält die volle Kontrolle über seine Prüfalgorithmen. Zudem sichert das System das demokratische Prinzip der Nachprüfbarkeit: Die manipulationssicheren Nachweise garantieren, dass automatisierte Verwaltungsakte auch noch nach Jahren lückenlos für Bürger und Gerichte nachvollziehbar bleiben.

Wie trägt das Projekt zur Stärkung der Digitalen Souveränität bei?

Das Projekt stärkt die Digitale Souveränität europäischer Unternehmen und Behörden, indem es die technologische und rechtliche Abhängigkeit von außereuropäischen Plattformen bei der KI-Regulierung vollständig auflöst.

Das Framework erzielt diesen Souveränitätsgewinn durch drei zentrale Architekturmerkmale:

Vollständige Cloud-Unabhängigkeit (Air-Gapped Operationalization): Sentinel bricht mit dem Zwang, Überwachungs- und Compliance-Daten an US-amerikanische Hyperscaler zu übermitteln. Die gesamte In-Process-Validierung und die Generierung der Audit-Spuren erfolgen

lokal im Arbeitsspeicher und auf eigener Hardware. Sensible Daten, Geschäftsgeheimnisse und personenbezogene Daten verbleiben physisch in der Hoheit der eigenen Organisation.

Schutz vor dem Vendor-Lock-in durch Open-Source-Governance: Da die Kernsoftware unter der freien Apache-2.0-Lizenz steht und eine Stewardship unter der Linux Foundation Europe angestrebt wird, entzieht sie sich der Kontrolle proprietärer Monopole. Organisationen erlangen die volle strategische Autonomie zurück: Sie können den Quellcode selbst auditieren, modifizieren und zeitlich unbegrenzt betreiben, ohne das Risiko von abrupten Lizenzänderungen, Preiseskalationen oder der plötzlichen Abkündigung von Software-Komponenten durch Drittanbieter (SaaS-Dilemma) fürchten zu müssen.

Autonomie bei der Durchsetzung europäischer Rechtsstandards: Anstatt darauf zu warten, dass globale Tech-Konzerne Compliance-Tools für europäische Gesetze entwickeln, stellt Sentinel ein maßgeschneidertes, heimisches Werkzeug für den EU AI Act bereit. Der Staat und regulierte Industrien behalten die absolute Deutungs- und Kontrollhoheit über die Algorithmen, die zur Überprüfung von KI-Entscheidungen herangezogen werden.

Die Software verwandelt Digitale Souveränität von einem theoretischen Konzept in ein sofort einsetzbares, technisches Werkzeug. Sie stellt sicher, dass Europa die Kontrolle über die Governance seiner kritischen KI-Infrastrukturen behält.

Projektwebsite
https://github.com/sebastianweiss83/sentinel-kernel
Umsetzungspartner
BWI, T-Systems, Quantum Systems, diverse deutsche CTOs
Zusätzliche Dokumente
Keine