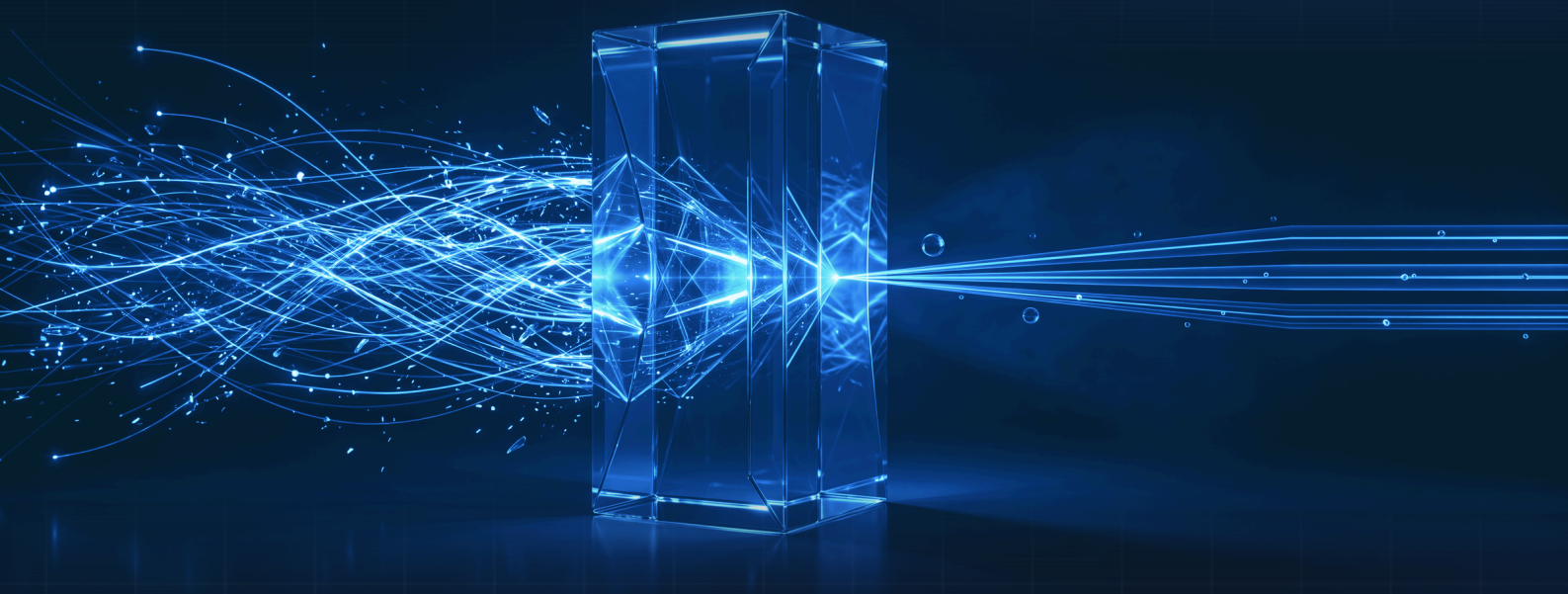
allclouds.pl
AI by design

SAIE PANTERA · 2026/Q3

WHITE PAPER



SAIE · KONTROLA · BEZPIECZEŃSTWO · ŁAD KORPORACYJNY AI

PROXY:AI

Centralna warstwa kontroli, bezpieczeństwa i ładu korporacyjnego dla sztucznej inteligencji

PROXY:AI działa jako ujednolicona brama między użytkownikami, aplikacjami i agentami AI a modelami językowymi - chmurowymi i lokalnymi. Eliminuje zjawisko Shadow AI, chroni dane wrażliwe i utrzymuje koszty pod pełną kontrolą - od chmury, przez On-Premises, po tryb Air-Gap

Niniejszy dokument przybliża architekturę i zasadę działania PROXY:AI: cykl życia żądania, moduły platformy, mechanizmy zgodności regulacyjnej oraz warianty wdrożenia. Adresatami są CISO, działy IT oraz kadra zarządzająca organizacji wdrażających AI

01

AI Gateway

Inteligentny router centralizujący cały ruch do modeli AI

02

AI Firewall

Zapora czasu rzeczywistego: analiza treści, polityki, maskowanie danych

03

Governance

Niezmienny rejestr WORM i automatyczne pakiety dowodowe dla audytorów

04

Cost Control

FinOps dla AI - zarządzanie kosztami AI: budżety, limity, pełna przewidywalność finansowa

PROBLEM: SZTUCZNA INTELIGENCJA POZA KONTROLĄ ORGANIZACJI

W większości organizacji dostęp do modeli językowych rozwija się oddolnie i bez planu. Zespoły łączą się bezpośrednio z API różnych dostawców, a pracownicy przenoszą dane firmowe do publicznych chatbotów. To zjawisko, Shadow AI, oznacza utratę kontroli nad tym, kto, z jakiego narzędzia i z jakimi danymi korzysta

Konsekwencje narastają w trzech wymiarach: **bezpieczeństwo** (dane wrażliwe trafiają do zewnętrznych modeli poza polityką), **koszty** (agent w pętli generuje lawinowe rachunki - Denial-of-Wallet) i **uzależnienie technologiczne** (vendor lock-in)

Równolegle rośnie presja regulacyjna: AI Act, RODO, DORA, NIS2/KSC, KRI oraz ISO/IEC 42001 wymagają wykazania nadzoru nad AI wraz z dowodami. Przy rozproszonym dostępie zebranie takich dowodów jest praktycznie niewykonalne



SEDNO PROBLEMU

Organizacja nie może chronić, rozliczać ani udowadniać tego, czego nie widzi. Warunkiem kontroli, przewidywalnych kosztów i zgodności jest jeden punkt, przez który przechodzi cały ruch AI

BEZPIECZEŃSTWO DANYCH

AI Firewall - maskuje dane wrażliwe i blokuje ataki na model (Prompt Injection)

UZALEŻNIENIE OD DOSTAWCY

Zero-Code Switch - zmiana modelu bez przepisywania aplikacji

NIEKONTROLOWANE KOSZTY

Cost Control - budżety i limity, ochrona przed lawiną kosztów (Denial-of-Wallet)

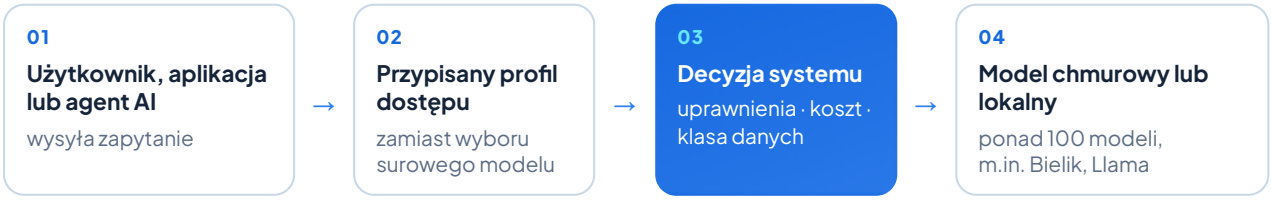
PRESJA REGULACYJNA

Governance - rejestr WORM i pakiety dowodowe

CZYM JEST PROXY:AI

PROXY:AI to jeden punkt wejścia między użytkownikami, aplikacjami i agentami AI a ponad 100 modelami - chmurowymi i lokalnymi. Użytkownicy korzystają z przypisanego profilu dostępu, a o tym, który model obsłuży zadanie, decyduje system

ZARZĄDZANIE PROFILAMI, NIE MODELAMI - ZERO-CODE SWITCH



JAK TO DZIAŁA – CYKL ŻYCIA ŻĄDANIA

Wartość PROXY:AI najlepiej widać w drodze pojedynczego zapytania. Każde żądanie – od człowieka, aplikacji czy agenta – przechodzi ten sam, pełny cykl kontroli

01 **Uwierzytelnienie**
RBAC: role, grupy, klucze – bez bezpośrednich kluczy API

02 **Ocena kontekstu**
ABAC: kto, skąd, o jaki model, jakie ryzyko

03 **Skan wejścia**
AI Firewall: maskowanie danych, blokada ataków na model (Prompt Injection, Jailbreak)

04 **Routing i budżet**
dobór modelu wg wyniku skanu, kontrola limitów

05 **Wywołanie modelu**
lub bufor semantyczny dla powtarzalnych pytań

06 **Skan wyjścia**
analiza odpowiedzi modelu

07 **Akceptacja człowieka**
operacje wysokiego ryzyka (human-in-the-loop)

08 **Zapis audytowy**
niezmienny rejestr WORM

MODUŁY PLATFORMY

Etapy cyklu realizuje dziesięć modułów, pogrupowanych w cztery filary platformy

AI GATEWAY

- **Model Registry** – katalog modeli i profili dostępu
- **ABAC Gateway** – ocena żądania na podstawie atrybutów
- **RBAC i tożsamość** – role, grupy i klucze; rotacja bez przestojów
- **MCP Gateway** – nadzór nad autonomicznymi agentami AI

AI FIREWALL

- **AI Firewall** – skanowanie w 12 językach, maskowanie danych
- **Bariery ochronne** – filtry Prompt Injection / Jailbreak

GOVERNANCE

- **Zarządzanie promptami** – repozytorium polityk odpowiedzi
- **Niezmienny audyt** – rejestr WORM, Prometheus i Grafana

COST CONTROL

- **FinOps i Anti-DoW – ochrona kosztowa** – budżety, Twin:Coin, klasy Basic/Advanced
- **AI Cost Forecast i Executive AI Dashboard** NOWE – prognoza kosztów (abonament czy API) i panel kosztów AI dla zarządu

<50 ms	100+	12	6+ mies.
ANALIZA W CZASIE RZECZYWISTYM	OBSŁUGIWANYCH MODELI	JĘZYKÓW SKANOWANIA	HISTORII AUDYTOWEJ

WIARYGODNOŚĆ PRODUCENTA

allclouds.pl wdrożyło własny system zarządzania AI i uzyskało certyfikat ISO/IEC 42001 – tej samej normy, której spełnienie PROXY:AI pomaga wykazać organizacjom

ISO/IEC 42001

WDROŻENIE REFERENCYJNE

LW Bogdanka – PROXY:AI w infrastrukturze krytycznej, w całości on-premises

ZGODNOŚĆ REGULACYJNA I DOWODOWOŚĆ

Fundamentem zgodności jest rejestr WORM: baza, która nieusuwalnie i z zabezpieczeniem kryptograficznym zapisuje każde wywołanie modelu, jego koszt i kontekst decyzji. Historia z ostatnich sześciu miesięcy jest dostępna na żądanie, a okres przechowywania można wydłużyć

Na tej podstawie PROXY:AI generuje pakiety dowodowe: dokumentację wg Załącznika IV AI Act, raporty ryzyka DORA, materiały NIS2/KSC oraz paczki audytowe ISO/IEC 42001 - jednym kliknięciem, z danych gromadzonych w toku normalnej pracy. Dowody wspierają wykazanie zgodności - nie zastępują opinii prawnej ani certyfikacji

WARIANTY WDROŻENIA I SUWERENNOŚĆ DANYCH

PROXY:AI oferuje trzy warianty wdrożenia, odpowiadające różnym poziomom wymagań co do suwerenności danych. Każde wdrożenie stanowi osobne, w pełni odizolowane środowisko. W wariantach On-Premises i Air-Gap dobór infrastruktury GPU pod modele lokalne jest częścią wdrożenia. W wariancie Air-Gap Offline Model Registry dobiera modele lokalne do posiadanego sprzętu, przygotowuje paczkę z Harbor i uruchamia model bez dostępu do internetu

SaaS

CHARAKTERYSTYKA
usługa zarządzana, najszybsze uruchomienie

LOKALIZACJA DANYCH
centrum danych usługodawcy (PL lub UE)

TYPOWE ZASTOSOWANIE
ewaluacje, brak własnej infrastruktury

On-Premises

CHARAKTERYSTYKA
instalacja we własnej infrastrukturze

LOKALIZACJA DANYCH
serwerownia organizacji

TYPOWE ZASTOSOWANIE
sektory regulowane, administracja publiczna

Air-Gap

CHARAKTERYSTYKA
środowisko odcięte, wyłącznie modele lokalne

LOKALIZACJA DANYCH
infrastruktura odizolowana

TYPOWE ZASTOSOWANIE
obronność, infrastruktura krytyczna

Platforma integruje się z rozwiązaniami DLP i SIEM, pozwala budować własne klasyfikatory danych i nakładać branżowe rozszerzenia. Typowe obszary: finanse, administracja publiczna, zdrowie, obronność, infrastruktura krytyczna

PODSUMOWANIE

Sztuczna inteligencja musi być widoczna, kontrolowana, rozliczalna i możliwa do wykazania przed audytorem. PROXY:AI dostarcza te cztery własności w jednej warstwie - z politykami w czasie rzeczywistym, budżetami i rejestrem, któremu nie sposób zaprzeczyć - zachowując pełną swobodę doboru modeli

PROXY:AI

Jeden punkt wejścia do świata modeli AI.
Kontrola, bezpieczeństwo i dowody zgodności

Umów demonstrację

Pilotaż w Państwa infrastrukturze

allclouds.pl
AI by design

allclouds.pl sp. z o.o.
ul. Jutrzenki 139, 02-231 Warszawa

KONTAKT
www.allclouds.pl · office@allclouds.pl
tel. +48 22 100 43 80 · fax +48 22 100 43 84
NIP: PL5223052539 · REGON: 363597531
KRS: 0000598708

CERTYFIKACJA
PN-EN ISO 9001 · PN-EN ISO/IEC 27001 · PN-EN ISO 14001 · PN-EN ISO 22301 · PN-EN ISO/IEC 27017 · PN-EN ISO/IEC 27018 · ISO/IEC 42001