

# Global Aviation Leader: Secures AI Workflows Against Supply Chain Attacks

Enterprise-Grade AI Security Across a Multi-Cloud  
Agent Estate with AccuKnox

## Supported Clouds



## Deployment



“AccuKnox gives us the protection we need for our cloud AI infrastructure, while ensuring our agents and models remain secure against emerging threats.”

### Global Airline

Head of Cloud & AI Security

# Challenges

- ❗ Uncontrolled AI Agent Sprawl Across Three Clouds**  
40+ AI agents running across AWS Bedrock, Azure AI Foundry, and Copilot Studio with no unified visibility, behaviour discovery, or runtime controls.
- ❗ Production LLMs Exposed to Adversarial Attacks**  
SOC, SRE, FinOps, and DevOps agents running in production had zero guardrails against prompt injection, hallucination, abuse, and evolving threat tactics.
- ❗ Multi-Cloud AI Misconfiguration**  
ML workspace governance gaps, public notebook exposure, and critical CVEs in AKS clusters (CVE-2023-24301) with no single platform to correlate risks.
- ❗ No Compliance Posture for AI Regulations**  
Zero systematic tracking against OWASP LLM Top 10, NIST AI RMF, ISO 42001, or EU AI Act across sensitive aviation data flows.

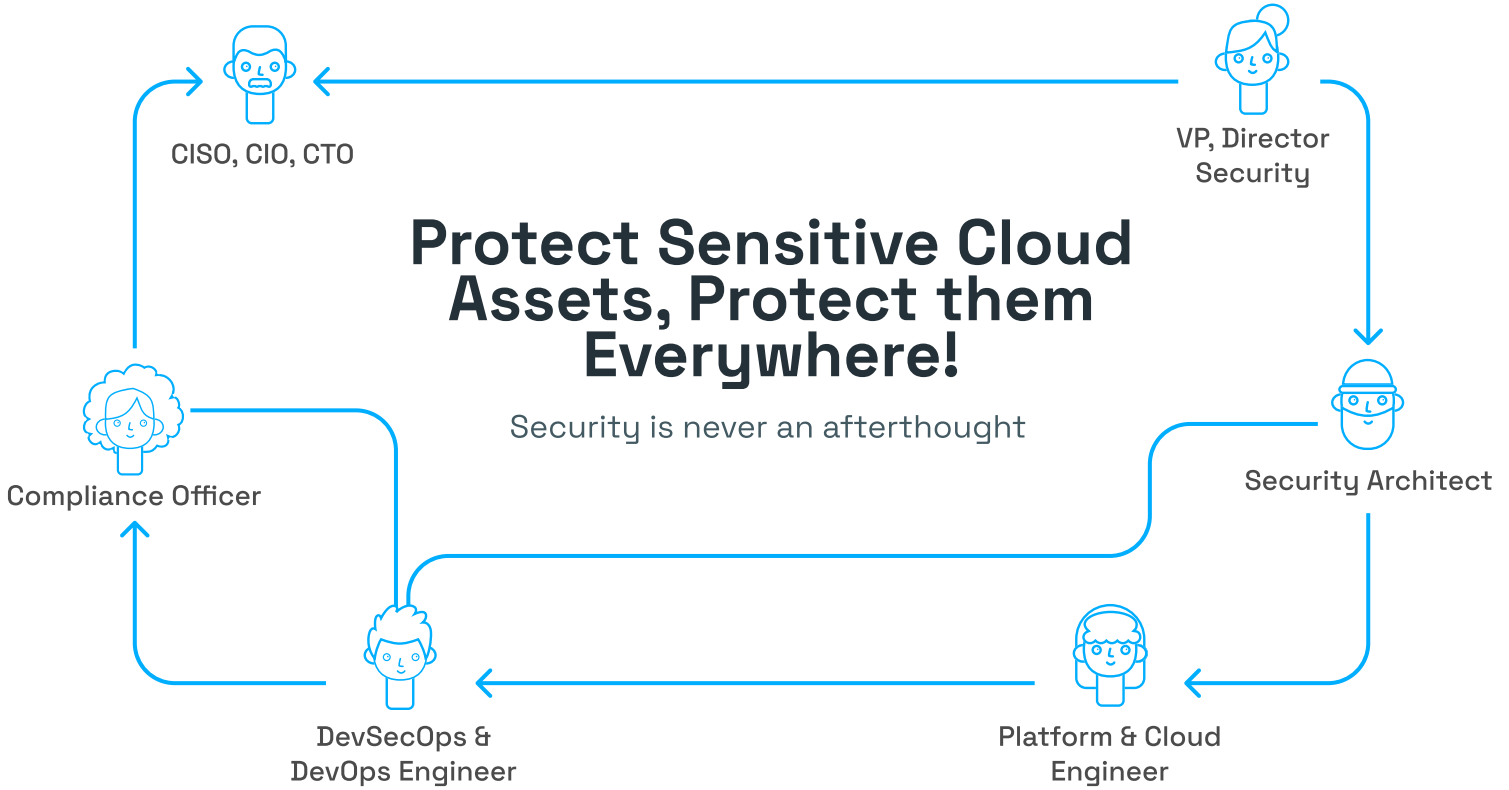
# Solutions

- ✓ **AI Asset Inventory:** Auto-discovered 40 shadow Copilot agents and 1,500+ ML models, eliminating shadow AI overnight.
- ✓ **Prompt Firewall:** Real-time LLM-as-a-judge inspection via Azure APIM and AWS API Gateway with session context.
- ✓ **Automated Red Teaming:** Continuous scanning of AI workloads across injection, toxicity, and model extraction.
- ✓ **Agent Behaviour Sandboxing:** eBPF-based runtime controls on AKS blocking unsafe tool usage and unauthorised outbound traffic.
- ✓ **AI Detection & Response (AI-DR):** Automated remediation workflows for public notebook exposure and unauthorised model changes.
- ✓ **AI Compliance Posture:** Mapping across 25+ frameworks, including ISO 27001, NIST AI RMF, and the EU AI Act.

# Outcomes

- ✓ Achieved full-stack AI security, **reducing runtime security risks by 90%** across the entire estate.
- ✓ Eliminated blind spots — **achieving live inventory of 1,500+ models** across three clouds within days.
- ✓ **Minimised data leakage risk by 85%** through Prompt Firewall guardrails and DSPM controls.
- ✓ **Reduced cloud security incidents by 70%** and achieved **95% fewer false positives**.
- ✓ Continuous posture tracking across SOC 2, GDPR, and **30+ AI-specific frameworks**.

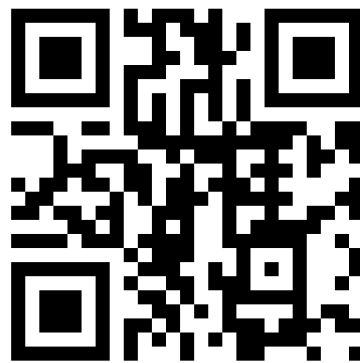
Featured by



Extra 30 Days Free Trial



\*No strings attached, limited period offer!



Scan for Demo

## About AccuKnox

AccuKnox is a Zero Trust Cloud Security Platform that protects Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.



in linkedin.com/accuknox

X @AccuKnox

