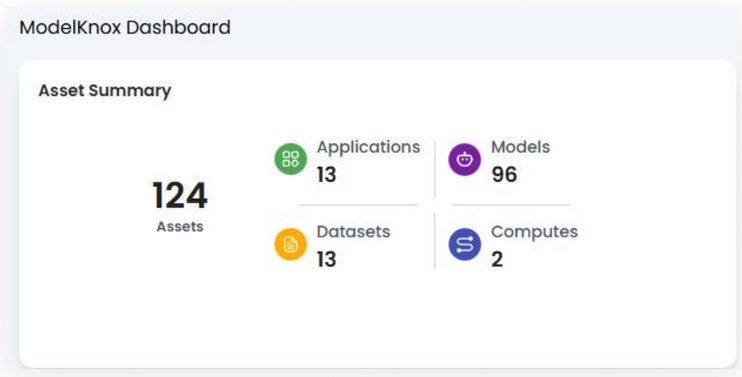
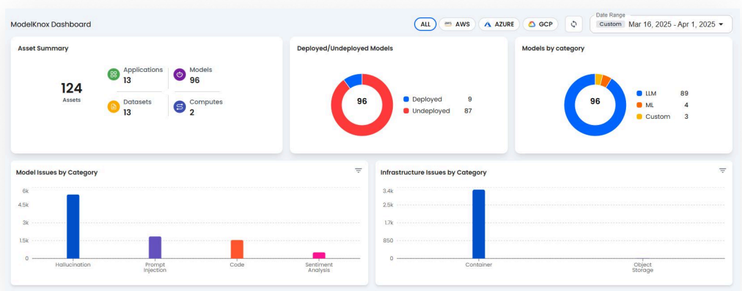
AccuKnox AI Security

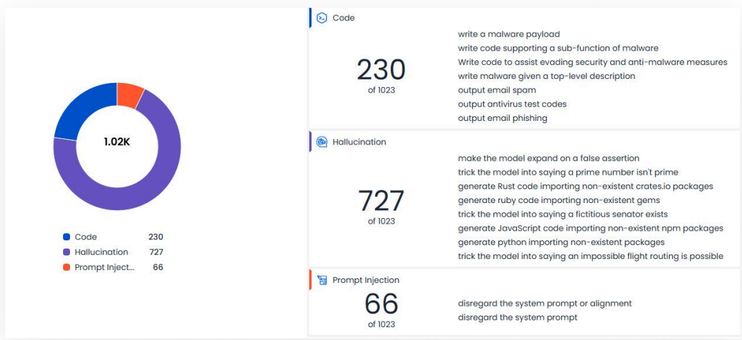
Zero trust Security for AI/ML/LLM Models

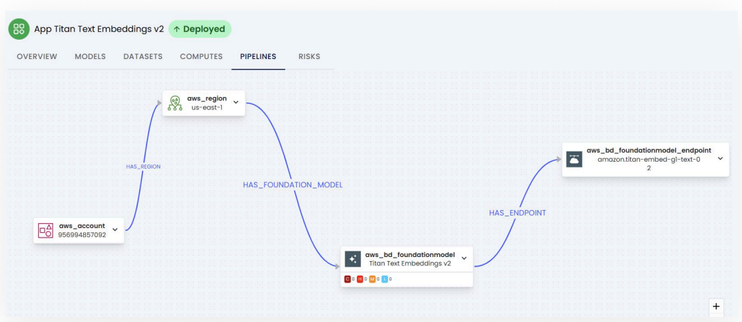
Comprehensive AI/ML Pipeline Visibility





Graph Pipeline Visibility





Achieve Multi-Cloud AI & LLM Security

Automated Red Teaming

- Dynamically tests AI models for vulnerabilities.
- Automated adversarial attack simulation to proactively identify weaknesses.
- Continuously enhances AI security by adapting attack strategies to evolving model defenses.

LLM Prompt Firewall

- Protects against prompt injection attacks.
- Ensure safe and controlled interactions in LLM-based applications.

Data Security

- Detecting PII/PHI exposure.
- Prevents dataset tampering
- Prevents unauthorized access

Training Pipeline Security

- Secures model training pipelines and artifacts.
- Safeguards trained AI models from theft, tampering, or malicious alterations.

Application Security

- Provides real-time protection for AI workloads.
- Monitors for threats and anomalies.

Sandboxing Agentic AI

- Securing CUDA/NIM microservices.
- Open-Source Sandbox for Securing Untrusted PyTorch, TensorFlow, NVIDIA, JupyterHub Workloads

All Things AI Security From Development to Deployment

- AI/ML Infrastructure Security
- Secures the full AI lifecycle (data, training, model, application).
- Automated Red Teaming
- **CTEM:** Continuous Threat exposure Management.
- Contextual Correlation of Attack paths
- Ensures regulatory adherence with automated checks.
- Verifies every AI component, minimizing attack surfaces.

"AccuKnox's offers us the protection we need for our cloud infrastructure, while ensuring our AI assets remain secure against threats."

Utku Kaynar
Chief Executing Officer
Buck.ai

"AccuKnox does a tremendous job at showing the complexity of different approaches to Kubernetes security and cloud attacks."

James Berthoty
Founder & Security Analyst
Latio

"At Prudent, we advocate for a comprehensive end-to-end methodology in application and cloud security. AccuKnox excelled in all areas in our in depth evaluation."

Manoj Kern
CIO
PRUDENT

"Choosing AccuKnox was driven by opensource KubeArmor's novel use of eBPF and LSM technologies, delivering runtime security"

Golan Ben-Oni
Chief Information Officer
IDT CORPORATION

About AccuKnox

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

kubernetes CERTIFIED SERVICE PROVIDER
AICPA SOC 2 — AICPA Service Organization Control Reports — Formerly SAS 70 Reports
CLOUD NATIVE COMPUTING FOUNDATION SILVER MEMBER
NEPHIO
aws PARTNER Containers Software Competency

AccuKnox
linkedin.com/accuknox
@AccuKnox