



# AccuKnox Capabilities

Code to Cloud Security



Agentless      Agentless + eBPF sensor

**CSPM**      **ASPM**      **KSPM**      **CWPP**

OnPrem & SaaS Deployment Options

Findings & Ticketing Lifecycle

Compliance & GRC

Projects, Tags, Groups

AI CoPilot AskAda

Rules Engine (IFTTT for Findings)

Dashboards, Reporting, RBAC

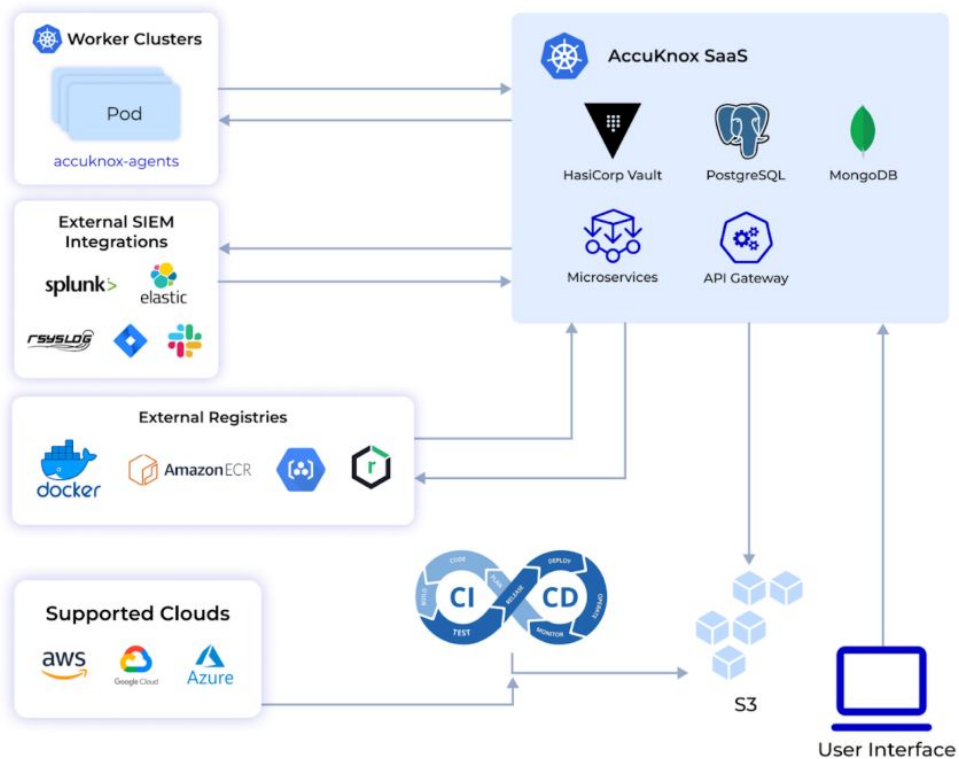
SIEM/SOAR Integrations

CI/CD DevSecOps



# AccuKnox Architecture (HLD)

ACCUKNOX Enterprise Architecture





## Code Scanning

- Code Smells
- Security Issues
- Quality Issues



## IaC Scanning

- Terraform, Ansible
- K8s manifests, Dockerfiles
- Azure Templates, AWS CloudFormation



## Container Scans

- Using Trivy / Clair
- Sensitive asset detection in images



## Rules Engine based WorkFlows for Findings



## Prioritization & Aggregation



## SCA

- Checkmarx SCA
- Using Trivy SCA

Integration: Agentless, CICD



## Secrets in Container Images



## Secrets in Kubernetes ConfigMaps



## Secrets in IaC

- Using checkov in terraform, helm-charts, ansible, k8s-manifests

## **Secrets in Code Repos** (Roadmap: Jan 2025)

## **Secrets in S3 buckets, GCS, File System** (Roadmap: Jan 2025)



## Runtime Secrets Protection

- Protect secrets exposed through:
  - env variables
  - config files

**Integration: Agentless, CICD**



### Host & Endpoint scanning



### API Scanning

- Using ZAPProxy, burpsuite



### VM / Bare Metal STIGs and CIS

- AccuKnox developed Risk Assessment Tool (RAT)

**Integration: Agentless, CICD**



### K8s Misconfiguration detection



### K8s Security Risk assessment



### K8s CIS Benchmarks



### K8s Identities & Entitlements

- Unused service accounts
- Excessive Permissions for Service accounts



### Admission Controller support

- Pod Security Admission support
- Kyverno based support
- OPA support (roadmap)



### K8TLS (TLS Posture)

- Inhouse built tool
- TLS best practices use
- Certificates best practices

**Integration: Agentless, CronJob mode**



## Kubernetes, Containers, VM, Baremetal



## Application Behavior Monitoring

- File, Process, Network, Capabilities
- Network Graph of workloads



## Workload Hardening

- File Integrity Monitoring
- Cryptomining, Malware Protection
- Root certs, sensitive assets protection



## Zero Trust Policy

- ZTNA
- Zero Trust Process Whitelisting



## K8s Network Microsegmentation

- Automated ingress, egress network policy discovery



## Auto Remediation, Preemptive Mitigation

**Integration: Agent based (eBPF sensors)**





Container  
Image/Registry  
Scanning

(9+ registries supported)



Application  
Hardening



Github/Jenkins Plugins



DevSecOps/CICD  
Model



Host Scanning

Integration: Agentless, CICD



## Ticketing

- Jira, FreshService, ConnectWise, ServiceNow
- Bidirectional ticket sync



## Notification Channels

- Slack, Email
- Suppressions



## SIEM

- Azure Sentinel
- Splunk, CloudWatch,
- Rsyslog, ...



## Extensive (+Custom) Reporting



## Code Repos

- GitHub
- GitLab
- BitBucket



## DevSecOps

- [Jenkins](#)
- [GitHub Actions](#)
- Azure DevOps



Asset Inventory



Support for all major  
CSPs



Rules Engine based  
Workflow



Compliance

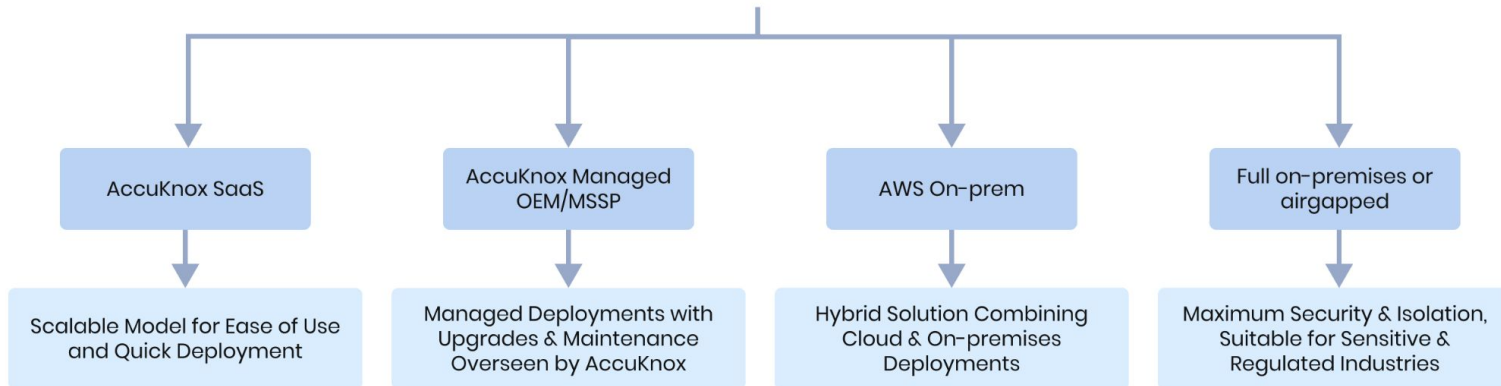
(30+ compliance types)


**AWS CloudTrail, Azure  
Logs real time analysis**  
(Roadmap: Mar 2025)

**Integration: Agentless, CICD**




## AccuKnox Deployment Models






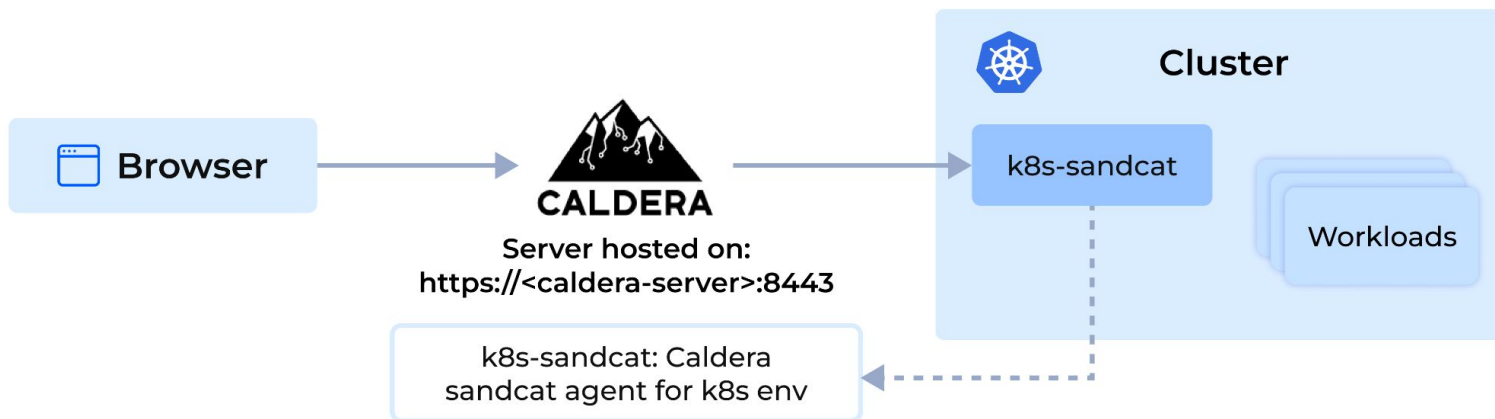
**Virtual Machine Attack Simulation**



**K8s Adversarial Emulation** ★



**AI/ML/GenAI Adversarial Emulation Red Teaming** ★





- ML/LLM visibility
- Models observability
- Security Posture Management

Vulnerability Scanning



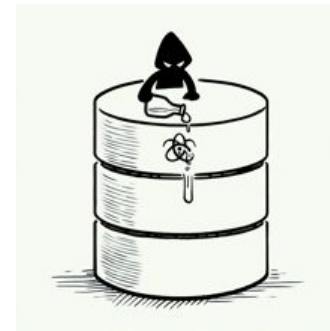
- Sandbox untrusted model execution
- PyTorch, TensorFlow, Jupyter Notebooks, MLOps

Runtime Protection



- Prompt Injection protection
- Observability into prompt usage

Security Posture Management



- Data Fencing
- Data poisoning protection
- ML Data Security

ML/LLM Model Security



- Model Hijacking Protection
- Model Usage view
- Unauthorized access

Infra & App Security

- **Complete Code to Cloud platform**
  - Best of breed tools in a single platform
  - Orchestrates findings/ticketing consistently across all dimensions
- **Differentiated offering for Cloud, K8s, Containers.**
- **SaaS, OnPrem, Air Gapped deployment options**
- **Extremely competitive Pricing/Licensing models**

- **Comprehensive Roadmap**
  - GenAI/ML security
  - API Security
  - Multi Layer Vulnerability Prioritization (Runtime visibility ⇒ ASPM)

For more information: <https://www.accuknox.com/information>



ACCUKNOX

**SEE USE CASES  
IN ACTION**

**[support@accuknox.com](mailto:support@accuknox.com)**