AccuKnox

MANAGED SERVICES PROPOSAL

Managed Cloud Security Services

Unified CNAPP Security, Delivered and Operated as a Service

Table of Contents

Table of Contents

1. Executive Summary

Cloud environments have outgrown the tools most security teams use to defend them. Multi-account, multi-cluster, multi-cloud estates now carry misconfigurations, exposed data, vulnerable workloads, and increasingly AI models and agents, all changing faster than a lean internal team can monitor manually.

AccuKnox Managed Cloud Security Services pairs our CNAPP (Cloud-Native Application Protection Platform) and AI security stack with a dedicated AccuKnox delivery team that operates it on the customer's behalf: continuous posture management, runtime protection, data security, application security, and AI/LLM security — monitored, tuned, and reported on as an ongoing service rather than a one-time deployment.

This document outlines the service scope, delivery model, service tiers, SLAs, and engagement process for a managed offering built on the AccuKnox platform.

2. The Cloud Security Challenge

Organizations adopting cloud-native and AI-driven architectures consistently face the same operational gaps:

- Security tooling sprawl across CSPM, CWPP, and AppSec point solutions that don't share context.
- Alert volume that exceeds what a lean internal SecOps team can triage, let alone remediate.
- Runtime environments that change faster than manual policy review can keep up with.
- New exposure from AI models, prompts, and agentic workflows that traditional CNAPP tooling was never built to see.

A managed service model addresses these gaps by pairing the platform with the people, process, and operational coverage needed to run it continuously.

3. Service Overview

AccuKnox Managed Cloud Security Services is delivered on top of the AccuKnox CNAPP platform and covers five core security pillars. Each pillar maps to a purpose-built AccuKnox capability, deployed, tuned, and operated by the AccuKnox delivery team.

3.1 What's Included

- Platform deployment, configuration, and lifecycle management across the customer's cloud accounts and clusters.
- Continuous monitoring and triage of findings by AccuKnox security analysts.
- Policy authoring and tuning (including KubeArmor runtime policies) to reduce false positives over time.
- Guided and, where contracted, assisted remediation.
- Advisory Reporting. AccuKnox will send advisories based on the customer asset inventory and its exposure.
- Scheduled reporting, compliance mapping, and quarterly business reviews.
- A named delivery engineer, lead and defined escalation path for the life of the engagement.

3.2 Cloud Security Posture Management (CSPM)

Continuous misconfiguration and compliance monitoring across AWS, Azure, and GCP.

- Continuous Security posture assessment against cloud-provider security best practices.
- Drift detection across accounts, with prioritized remediation guidance.
- Handling in-scope advisories for the cloud or application environments.

3.3 Runtime & Workload Protection (KubeArmor)

eBPF-based runtime security for containers, Kubernetes, and hosts.

- Zero-trust runtime policy enforcement at the process, file, and network level.
- Least-permissive policy generation from observed workload behavior, tuned by AccuKnox engineers.
- Real-time blocking/alerting on anomalous runtime behavior, with managed policy lifecycle as workloads evolve.

3.4 Application Security Posture Management (ASPM)

Unified visibility into code, dependency, and pipeline risk from commit to runtime.

- Aggregation of SAST, SCA, and pipeline findings into a single, de-duplicated risk view.
- Risk-based prioritization that correlates code-level findings with other vectors.
- Managed triage to cut through duplicate and low-value findings before they reach engineering.

3.5 AI & Model Security

Security and governance for models, prompts, and agentic workloads.

- Guardrails and a prompt firewall for LLM-facing applications
- Discovery and posture management for models and AI pipelines running in the customer's environment.

4. Service Tiers

Three tiers accommodate teams at different stages of cloud maturity. Scope, cloud account count, and cluster count are finalized during scoping and reflected in the commercial proposal.

Capability	Foundation	Advanced	Premium
CSPM continuous monitoring	•	•	•
Managed runtime policy authoring	•	•	•
ASPM pipeline & code risk aggregation	—	•	•
AI/LLM security & guardrails	—	—	•
Monitoring coverage	Business hours (8 hours from Mon-Fri)	Extended hours (12 hours from Mon-Sat)	24x7x365
Runtime Alert triage by AccuKnox analysts	•	•	•
Assisted remediation	—	•	•
Named delivery lead	—	•	•
Quarterly business reviews	•	•	•
Monthly reporting	•	•	•
Dedicated Slack/Teams channel	— (only by email)	— (only by email)	•

Pricing is scoped to environment size (cloud accounts, clusters, data stores, and model endpoints in scope) and is provided separately in the commercial proposal.

5. Service Delivery Model

5.1 Onboarding

A structured onboarding phase precedes steady-state monitoring:

- Week 1–2: Kickoff, access provisioning, and platform deployment across in-scope accounts and clusters.
- Week 2: Baseline assessment — initial CSPM/ASPM scan, Runtime Policy Authoring, Inventory of models and AI endpoints in scope.
- Week 3–4: Policy tuning to reduce noise, agreement on severity thresholds and escalation paths, and first steady-state report.

5.2 Steady-State Operations

- Continuous monitoring across all in-scope pillars, with coverage hours per the contracted tier.
- Alert triage and severity classification by AccuKnox analysts before escalation to the customer.
- Ongoing policy tuning as the environment changes (new services, clusters, models, or pipelines).
- Scheduled reporting cadence (monthly or quarterly, per tier) plus an always-on dashboard.
- Note that AccuKnox security team members responsible for providing the managed service would need access to the customer tenant containing the findings.

5.3 Incident Escalation

Findings above the agreed severity threshold are escalated directly to the customer's designated contact through the channel defined at onboarding (email, ticketing integration, or dedicated chat channel for Premium), alongside AccuKnox's recommended remediation.

5.4 Roles & Responsibilities

Activity	AccuKnox	Customer
Platform deployment & configuration	Responsible	Consulted
Cloud account / cluster access provisioning	Consulted	Responsible
Continuous monitoring & alert triage	Responsible	Informed
Policy tuning (CSPM, Runtime, ASPM, AI)	Responsible	Consulted

Activity	AccuKnox	Customer
Remediation execution	Consulted / Assisted*	Responsible
Reporting & business reviews	Responsible	Informed

**Assisted remediation scope (e.g., applying a pre-approved Runtime policy vs. code-level fixes) is defined per engagement.*

5.5 Security Personnel

Personnel	AccuKnox
Security Engineer/Analyst	Anmol Kumar (anmol@accuknox.com)
Security Lead	Gaurav Kumar Mishra (gaurav@accuknox.com)
Escalation	Rahul Jadhav (rahul@accuknox.com)

General Support Email: support@accuknox.com

6. Service Level Agreements

Response and update targets below apply to the Advanced and Premium tiers during contracted monitoring hours; Premium extends coverage to 24x7x365. Final SLAs are confirmed in the Statement of Work.

Severity	Initial Response
Critical	≤ 1 hour
High	≤ 4 hours
Medium	≤ 1 business day

7. Why AccuKnox

- Single platform, not a bundle: CSPM, ASPM, runtime protection, and AI security share one data model and one console, so managed analysts triage with full context instead of switching tools.
- eBPF-based runtime enforcement: KubeArmor enforces least-permissive policy at the kernel level, giving real-time blocking rather than after-the-fact detection.
- Built for what's next, not just what's deployed: AccuKnox AI Security extends the same posture and runtime discipline to models, prompts, and agentic workflows as they enter the environment.

- A team, not a ticket queue: a named delivery lead owns the relationship, the tuning, and the escalation path for the life of the engagement.

8. Engagement Model & Next Steps

Recommended next steps to move from this draft to a scoped proposal:

- Scoping call to confirm cloud accounts, cluster count, data stores, and any AI/model endpoints in scope.
- Environment walkthrough and confirmation of target service tier.
- Commercial proposal and Statement of Work, including final SLAs and reporting cadence.
- Onboarding kickoff per the timeline in Section 5.1.

Contact:

Gaurav Mishra,

Principal Product Manager,

gaurav@accuknox.com

ACCUKNOX

Next Step: A Scoping Call

We confirm cloud accounts, cluster count, data stores, and any AI or model endpoints in scope, then return a commercial proposal and Statement of Work with final SLAs and reporting cadence.

SOLUTIONS LEAD
Gaurav Mishra
gaurav@accuknox.com

GENERAL SUPPORT
AccuKnox Support
support@accuknox.com

WEB
AccuKnox, Inc.
accuknox.com

Secure Code to Cognition™