

AccuKnox

VS

Qualys TotalCloud



Better

AccuKnox offers superior protection across cloud, containers, and Kubernetes environments, supporting over 33 compliance frameworks and enhanced by open-source innovations like KubeArmor, trusted by over 1 million downloads.



Faster

AccuKnox speeds up security operations with real-time runtime protection, cutting remediation time by 91% and reducing false positives by 89%, making threat detection and response significantly more efficient.



Cheaper

AccuKnox delivers a unified Cloud Native Application Protection Platform (CNAPP) that lowers total cost of ownership by consolidating multiple security tools into one solution, offering flexible pricing that scales seamlessly for organizations of all sizes.

Application Security Coverage



Registry scan (ECR, GCR, Nexus, Docker Hub, ACR, Harbor, Quay, jFrog, OpenShift, GAR.)



Identify 3rd Party Dependencies and their Vulnerabilities (SCA), Scan for Vulnerability in Code (SAST), IaC and Evaluate Applications for Vulnerabilities (DAST)



Integrate with CI/CD for Shift Left Automation with Prioritization



Deep observability with context by making use of eBPF



Auto-generation of policies based on container activity to prevent anything that deviates from it



Graphical view of Kubernetes identities with customizable queries to define least-permissive posture



Supports Container Registry Scanning



Provides SCA, SBOM, and DAST (via WAS); No native SAST



CI/CD Integrations, mainly for DAST and IaC workflows, no SAST integration



Agent-based eBPF visibility for Linux/containers; robust observability via TruRisk, limited enforcement via QFlow



Supports detection, response, and remediation via QFlow; no auto policy generation



Detects RBAC misconfigurations; Kubernetes visualizations are less granular

Observability and Remediation

Hardening and Prevention



Hardening policies based on compliance and best practices to restrict activities at the kernel layer



Proactive prevention of attacks using LSMs (Linux Security Modules) to deny access at kernel level



Admission Controller and PSA (Pod Security Admission) to prevent vulnerable deployments



No kernel-layer hardening.



Enforces at runtime via InstaProtect and QFlow remediation.



Supports Admission Controller for policy checks during deployment

Deployment Models



Airgapped and On-Prem Support



Support for Hybrid environment of On Prem + Cloud



Agent Based Protection and Scanners for identifying vulnerabilities



Only SaaS model is supported; no airgapped deployment



Limited On-Prem support



Both Agentless and Agent-Based models supported, depending on the product

Open vs Proprietary



Built on KubeArmor, an open-source CNCF Sandbox project



Completely proprietary solution, closed source architecture

Parameters



Integrates with Open source scanners to provide a single platform view



No native support for OSS frameworks like Trivy or OPA; limited extensibility via APIs only



Integrates with both open-source and proprietary security tools for unified issue tracking



Integrates with commercial tools in the Qualys ecosystem, limited open-source external integrations



Unified platform view across tools - Consolidated dashboard for OSS and proprietary tools



Closed ecosystem; lacks OSS visibility



5G and IoT/Edge Security supported



No IoT/Edge/5G support; covers cloud, SaaS, Kubernetes, AI security



Built-in Kubernetes Security via KSPM & KIEM (Identity Enforcement Module)



KSPM supported for Kubernetes posture monitoring



AI Security with ModelKnox (AI-SPM) to secure AI pipelines



AI-SPM available for AI model/service risk management

Integrations

Future Proof Security

Summary of the AccuKnox vs. Qualys TotalCloud comparison:

- ✓ **Application Security:** AccuKnox offers complete coverage (SCA, SAST, DAST, IaC) with deep CI/CD integrations; Qualys lacks native SAST and primarily supports DAST and IaC.
- ✓ **Observability & Remediation:** AccuKnox provides deep eBPF-based observability with auto policy generation and granular Kubernetes identity mapping; Qualys offers limited enforcement and less granular RBAC visualizations.
- ✓ **Hardening & Prevention:** AccuKnox enforces proactive prevention using LSMs and kernel-layer controls; Qualys lacks kernel-level hardening but supports runtime enforcement and Admission Controllers.
- ✓ **Deployment Flexibility:** AccuKnox supports air-gapped, on-prem, hybrid, and agent-based models; Qualys is SaaS-first with limited on-prem options.
- ✓ **Open Source & Future-Readiness:** AccuKnox is built on open-source (KubeArmor) and supports 5G/IoT security; Qualys is closed-source with limited open-source integration and no IoT/5G coverage.

Featured by



Extra 30 Days Free Trial



*No strings attached, limited period offer!



Scan for Demo

About AccuKnox

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



in linkedin.com/accuknox

X @AccuKnox

