

Key Performance Improvements

Alert Management

89%



Fewer false positives → reduced alert fatigue

Remediation Speed

91%



Faster remediation → improved MTTR

Deployment Speed

<2 days



Deployment → vs weeks with Wiz

Compliance Coverage

33+



Compliance standards → improved audit readiness

Runtime Protection

Real-time



Blocking → inline runtime prevention, unlike Wiz

Deployment Flexibility

Hybrid & Air-gapped



Support → deployment flexibility

Customer	WIZ ⁺ Challenges	AccuKnox Solutions & Results
 <p>VEROGEN</p>	<p>Challenge: As a forensic genomics company, Verogen needed strong safeguards against PII/data exfiltration. Wiz's detection-only model flagged risks but could not prevent sensitive data from leaking in real-time.</p>	<p>Solution: Integrated directly with Verogen's on-premises Nessus instance to continuously scan their hosts, alongside deploying eBPF/LSM-based runtime enforcement. This provided both host-level vulnerability visibility and real-time blocking at the workload layer.</p> <p>Results: Achieved an ~85% reduction in PII leaks, strengthened compliance posture, and lowered the risk of insider-driven or zero-day data exfiltration.</p>
 <p>AUTHENTICID</p>	<p>Challenge: AuthenticID processes highly sensitive identity data in containerized pipelines. Wiz generated noisy alerts and lacked real runtime blocking, leaving critical ID apps exposed.</p>	<p>Solution: Connected with Nessus Cloud to scan all host assets, generating actionable security reports. Layered in runtime enforcement and AI-driven triage to reduce alert fatigue and strengthen zero-trust guardrails across ID processing workloads.</p> <p>Results: Realized a ~90% reduction in runtime threats across containerized ID pipelines, cut SOC triage time by over 60%, and improved audit-readiness for customer-facing compliance.</p>
 <p>Leading Indian Steel Manufacturer</p>	<p>Challenge: The steel giant needed to secure containerized OT + IT workloads across hybrid and air-gapped environments. Wiz's SaaS-only deployment and limited zero-trust enforcement created compliance gaps and high operational risk.</p>	<p>Solution:</p> <ol style="list-style-type: none"> 1. Completed CWPP onboarding for 2 Kubernetes clusters (QA & Dev). 2. Fixed multiple environment-level issues while supporting ongoing updates (e.g., migration to Prod, 2.3.2 release update, and export baseline fixes). 3. Enhanced visibility by resolving scan failures and aligning TSL Cloud assets. 4. Provided roadmap support for future production rollouts and compliance reporting. <p>Results: Strengthened supply-chain zero-trust enforcement, closed compliance gaps for OT integrations, and improved operational resilience with no current open issues post-update.</p>

Looking to Migrate from Wiz?

Evaluate how AccuKnox stands apart from Wiz security based on key features, pros and cons. We have compiled a list of solutions that leading organizations compare while considering AccuKnox as a potential Wiz alternative. While analyzing AccuKnox and Wiz side by side you can differentiate competencies, integration, deployment, service, support, and specific product capabilities that will influence your purchasing decision.

Better

AccuKnox provides a unified CNAPP that replaces multiple security tools with one platform, reducing cost and scaling easily for teams of any size.

Faster

AccuKnox accelerates security operations with real-time runtime protection, reducing remediation time by 91% and false positives by 89%.

Stronger

AccuKnox secures cloud, container, and Kubernetes environments with 33+ compliance frameworks and KubeArmor.

About AccuKnox

AccuKnox is a Zero Trust CNAPP provider protecting multi-cloud environments, Kubernetes, VMs, and edge infrastructure.