

When AccuKnox Wins

- You need workload-level identity on every API call: which pod, which service account, which IAM role. Wallarm cannot answer this.
- You need air-gapped or fully offline deployment for government, defence, or highly regulated environments.
- You want CNAPP consolidation: one platform covering API security, CSPM, CWPP, and ASPM instead of separate point solutions.
- You need 5+ compliance frameworks mapped simultaneously from live traffic, not static audit snapshots.

Capability	 ACCUKNOX	 wallarm
API Discovery	<ul style="list-style-type: none"> ✓ Auto-discovers endpoints via live traffic through connected gateways (AWS API Gateway, Istio, Kong, NGINX, F5, Azure APIM). Classifies shadow, zombie, and orphan APIs against uploaded OpenAPI/Swagger specs. Filters inventory by PII/PHI sensitivity, auth type, and HTTP status codes. 	<ul style="list-style-type: none"> ✓ Full API and endpoint inventory with automatic risk scoring. Detects shadow and orphan APIs across all traffic flows. Sensitive Business Flow Identification flags endpoints tied to auth, account management, and AI-driven operations.
East-West Traffic	<ul style="list-style-type: none"> ✓ Covers both north-south and east-west traffic, including encrypted service-to-service calls that perimeter tools miss. No proxy insertion required for internal traffic observation. 	<ul style="list-style-type: none"> — East-west coverage available via Ingress Controller or Envoy sidecar — requires explicit proxy deployment. Security Edge option handles external traffic only via DNS change.
Runtime Enforcement	<ul style="list-style-type: none"> ✓ Real-time blocking with configurable policy modes per workload: alert, block, or quarantine. DoS mitigation included. 	<ul style="list-style-type: none"> ✓ Inline blocking natively built in from day one. API Session Blocking (2025) targets malicious sessions without disrupting legitimate traffic. Security Edge deploys in under 15 minutes via a single DNS change.
OWASP API Top 10	<ul style="list-style-type: none"> ✓ Full OWASP API Top 10 coverage at runtime. Compliance evidence tied to live traffic, not static snapshots. Maps to PCI-DSS, HIPAA, GDPR, and DORA simultaneously. Policy-as-code via OPA/Rego for CI/CD gating. 	<ul style="list-style-type: none"> ✓ Full OWASP API Top 10 plus business logic abuse, BOLA, and ATO. Schema-based DAST in CI/CD covers API1-API8 pre-production. Context-aware blocking reduces false positives versus signature-only tools.
Shadow API Detection	<ul style="list-style-type: none"> ✓ Compares live traffic against OpenAPI/Swagger spec to surface shadow, zombie, and orphan APIs. Auto-creates Jira tickets on new shadow API detection. Filters shadow inventory by PII, PHI, and credit card data exposure. 	<ul style="list-style-type: none"> — Shadow and orphan API detection across full traffic inventory. Assigns risk scores to all discovered endpoints automatically. No documented Jira auto-ticketing workflow for shadow API events.
Schema Validation	<ul style="list-style-type: none"> ✓ OpenAPI/Swagger spec upload drives real-time endpoint classification. Schema deviations trigger alert, block, or quarantine. Supports REST, GraphQL, gRPC, SOAP/WSDL. 	<ul style="list-style-type: none"> — Schema-based DAST enforces spec compliance pre-production (2025). Runtime enforcement stops non-compliant requests inline. CI/CD DAST is more mature and more explicitly documented than AccuKnox's shift-left tooling.
Protocol Support	<ul style="list-style-type: none"> — REST, GraphQL, gRPC, SOAP/WSDL across north-south and east-west. Covers K8s API Server, AWS CloudTrail, Azure Functions, Google Anthos. No documented WebSocket support. 	<ul style="list-style-type: none"> ✓ REST, GraphQL, gRPC, WebSocket, and other modern protocols. Does not document K8s control plane API or cloud-native event stream coverage.
CI/CD Integration	<ul style="list-style-type: none"> — Scans IaC, Helm charts, K8s manifests, and API specs pre-deployment. OPA/Rego policy enforcement gated in CI/CD. Integrates with Jenkins, GitLab, Argo CD. Auto-generates compliance evidence per pipeline run. 	<ul style="list-style-type: none"> ✓ Schema-based DAST integrates directly into CI/CD pipelines. Finds API vulnerabilities and catches BOLA, broken auth, and spec mismatches in staging before production. CI/CD DAST is more explicitly documented than AccuKnox's shift-left tools.
Workload Identity Context	<ul style="list-style-type: none"> ✓ Correlates every API call with Kubernetes pod identity, service account, and cloud IAM binding. Links API findings to the exact process generating the traffic, not just the endpoint. Key for Zero Trust enforcement in multi-tenant K8s clusters. 	<ul style="list-style-type: none"> ✗ API risk scored against traffic patterns and endpoint risk. No documented workload identity correlation at the pod or IAM level. Cannot attribute API calls to a specific K8s pod, service account, or IAM role.
Compliance Mapping	<ul style="list-style-type: none"> ✓ Out-of-the-box: OWASP, PCI-DSS, HIPAA, GDPR, DORA, SOC2, CIS Benchmarks, NIST SP 800-190. Maps 5+ frameworks simultaneously in a single control plane. DORA 24-hour reporting supported via SBOM and tamper-evident audit trails. 	<ul style="list-style-type: none"> — OWASP API Top 10 with compliance reporting. PCI-DSS and HIPAA referenced in customer use cases. GDPR data flow mapping via sensitive data identification. DORA and multi-framework simultaneous mapping not explicitly documented.
Deployment Options	<ul style="list-style-type: none"> ✓ SaaS, AWS/GCP/Azure, private cloud, on-prem, air-gapped. Works on VMs, bare metal, and K8s. No container runtime dependency. 	<ul style="list-style-type: none"> — SaaS, public/private/hybrid cloud, on-prem. Deploys via DNS change (Security Edge) or pre-built marketplace images on AWS, GCP, Azure, IBM Cloud. No documented air-gapped or fully offline deployment.

About AccuKnox

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



in [linkedin.com/accuknox](https://www.linkedin.com/company/accuknox)

X @AccuKnox