

AccuKnox VS Semgrep



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.

Parameters



Platform Type

✓
Full Cloud-Native Application Protection Platform (CNAPP).

—
Static Application Security Testing (SAST) tool.

Primary Objective

✓
End-to-end security across build, deploy and runtime.

—
Detects vulnerabilities in source code before deployment.

Attack Surface Coverage

✓
Source Code + Infrastructure + Containers + Kubernetes + APIs + Runtime.

—
Source code only.

Application Security Posture Management (ASPM)

✓
Covers a broad spectrum of scanning capabilities across the entire application lifecycle, going beyond traditional code scanning to provide full-stack visibility and risk correlation.

At the core, AccuKnox performs SAST to analyze source code for vulnerabilities such as potential SQL injection queries, insecure coding practices and logic issues early in the development phase. It complements this with DAST, which scans running applications to identify real time vulnerabilities like authentication issues, misconfigurations and exposed endpoints. In addition, AccuKnox includes SCA to detect vulnerabilities in open-source libraries and dependencies, mapping them to known CVEs and identifying outdated or risky components.

Beyond application code, AccuKnox extends ASPM into infrastructure by performing Infrastructure-as-Code (IaC) scanning, identifying misconfigurations in Terraform, Kubernetes manifests, and other deployment templates before they reach production. It also includes container image scanning to uncover vulnerabilities, malware and misconfigurations within container images, as well as KSPM to assess cluster configurations, RBAC policies and workload security settings.

—
ASPM capabilities are code-centric and developer-driven. It aggregates findings primarily from its SAST engine (and some supply chain/security rule packs) into dashboards that help teams track vulnerabilities, triage issues and monitor remediation progress over time. While it provides useful features like rule customization, deduplication and workflow-based triaging, its visibility is largely limited to source code and static analysis results, without deeper correlation to runtime behavior, cloud posture, or infrastructure exposure.

Parameters



Deployment Model



SaaS, On-prem, air-gapped, hybrid.



CLI, SaaS, CI/CD integrations.

False positive management



Manages false positives by going beyond traditional, isolated scanning and instead validating findings in real runtime context. It leverages eBPF-based runtime observability to understand real application behavior and baseline normal activity.



Semgrep manages false positives primarily through rule tuning, developer control, and context-aware pattern matching, rather than runtime validation like CNAPP platforms.

Semgrep reduces false positives by allowing highly customizable rules written in its own pattern syntax, enabling teams to precisely define what should and should not be flagged in their codebase. It supports rule constraints such as metavariables, pattern combinations and logical conditions (AND/OR/NOT), which help narrow detections and avoid overly broad matches.

Auto Fixes and suggestions



Gives context-aware guidance where AI-Assisted remediation explains the root cause of each security issue, provides step by step fix guidance.
Can be enabled for all sorts of findings.



Auto fix capabilities are only applicable to basic 1 line fixes.

Data Retention



Retains all historical data on the platform from the time of onboarding until the customer requests its deletion.



For Semgrep open source edition (Opengrep), only CLI based logs are available as part of historical data.

IDE integration



Primarily CI/CD focused.



Supported. Eg: VS Code, IntelliJ, pre-commit hooks.

SIEM Integration



Native + integrated SIEM along with external integrations.
Supported SIEM platforms: Splunk, QRadar, Azure Sentinel, CloudWatch, Syslog etc.



No native SIEM integration capability.

Parameters



Ticketing tool integration



Supports: Jira, ServiceNow, Freshservice, ConnectWise, ServiceDesk Plus etc..
Bidirectional Sync (status tracking, updates reflected back)



Primarily Jira only.

Future Proof Security



5G Workloads and IoT/Edge Security, AI Security with ModelKnox (AI-SPM) and API Security. Bidirectional Sync (status tracking, updates reflected back)



Does source code scanning only. No future proof security.
Limited bidirectional sync (mainly ticket creation, not full sync)

SBOM Generation



Supports up to CycloneDX 1.7 format. SBOM generation can be done via CI/CD Integration. Automation supported via pipeline-integrated generation. Third party SBOM ingestion possible if uploaded in supported formatted.



CycloneDX 1.4 support only. SBOM generated primarily from scans. Automation is directly via UI or API. Third party SBOM ingestion is not supported.

SBOM Capabilities



Users can upload CycloneDX JSON files into a project and select two versions to compare. The interface highlights added packages, removed packages, and version changes between the two files. This aids in tracking dependency drift and supply chain changes over time.



Semgrep's SBOM capabilities are generally point-in-time and repository-centric, without lifecycle management, runtime correlation or centralized aggregation across environments. While it excels in ease of use, fast generation and integration into CI/CD pipelines, its SBOM remains a static output artifact, lacking deeper context such as exploitability, environment awareness, or continuous tracking.

Analytics and Reporting

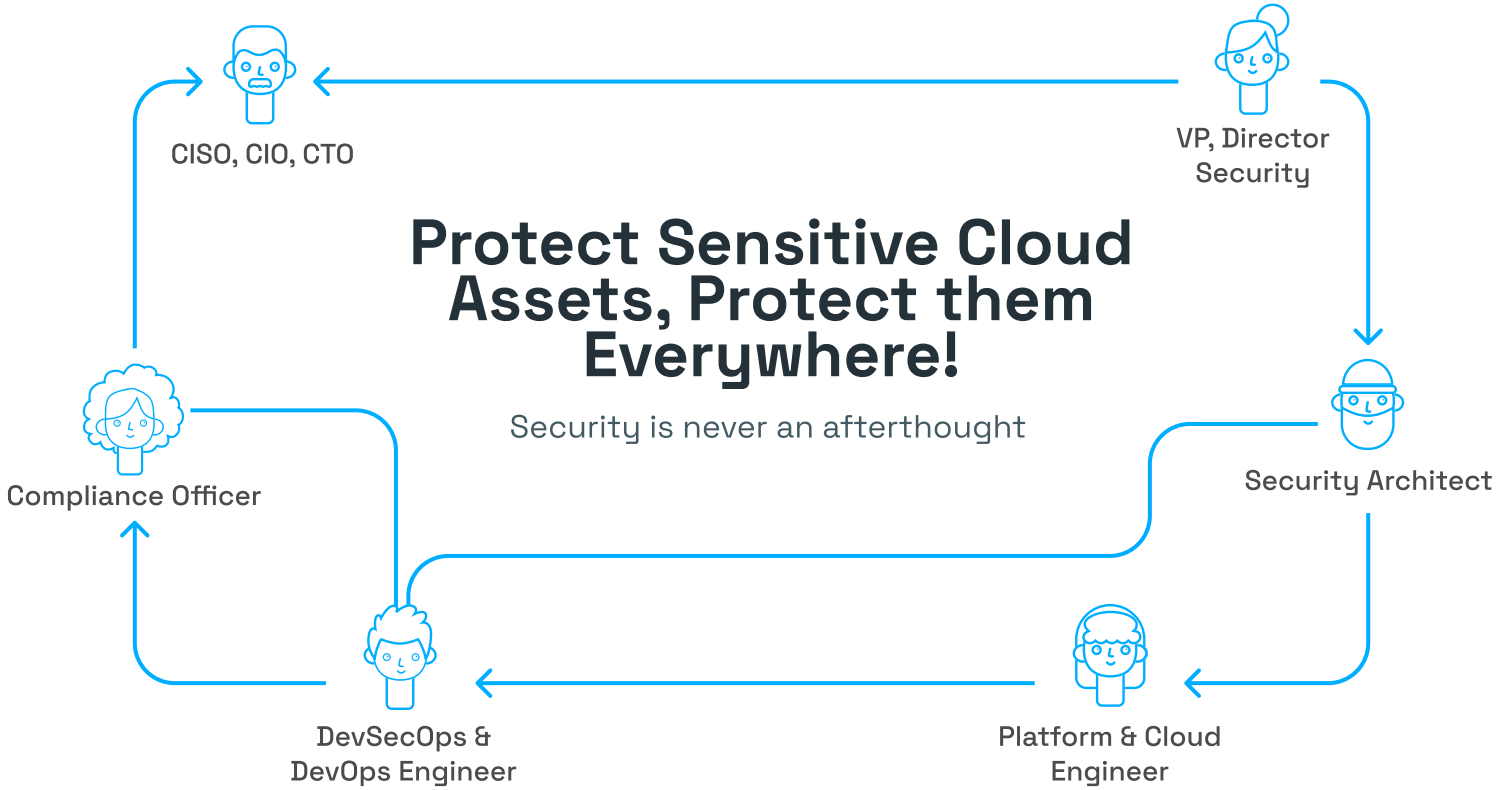


AccuKnox provides comprehensive reporting and analytics by aggregating and correlating security data across its entire CNAPP stack to deliver unified, context-rich insights. The platform offers centralized dashboards that present real-time visibility into vulnerabilities and misconfigurations. It supports customizable reports (pdf, docs, csv) aligned with industry standards.



Analytics on trends, historical issues available on enterprise version only.

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

