AccuKnox

CNAPP Features v2.2

AccuKnox ASPM & CSPM

ASPM - Code

Static Code Analysis	Detect critical software quality defects and security vulnerabilities in code as it's written, early in the development process. Leverage Veracode, Fortify, SonarQube.
Software Composition Analysis	Manage the security, quality, and license compliance risks that come from the use of open source and third-party code in applications and containers. Leverage Sonatype, trivy and Snyk SCA
Secret Scanning	We leverage Sonarqube, checkmarx
DAST	Burp, Zap and Nuclei
CI/CD Integration	Github Actions, Gitlab, Jenkins plugins,AWS pipeline, GCP code build pipeline, Azure Devops pipeline
Vulnerability Management	Segregation of False Positives

CWPP - Image

Images Risk Assessment	Ability to onboard and Scan registries like; Nexus, GCR, ECR, DockerHub
Vulnerability Scanning	Ability to automatically set periodic scans to identify vulnerabilities in the cloud assets and images present in the registries
Risk Based Prioritization	Accept risk for false positivies. The risk prioritization will work across future scans as well.
Compliance & Reporting	Compliance & Reporting
CI/CD Integration	Scan the container images in the CI/CD pipeline and report vulnerabilities. The scan reports can be sent to the SaaS dashboard for future reference.
Vulnerability Management	Segregation of False Positives. Ability to identify assets with most risks. Identify assets that have similar risks.

CSPM - Cloud

CSPM Executive Dashboard	Ability to provide a dashboard view of cloud resource's overall Compliance Score in % , Pass / Fail criteria, Compliance summary based on each asset associated to infrastructure.
Misconfiguration Detection	Ability to Support for Misconfigurations Detection in Public Clouds (**AWS, GCP, Azure**).
Inventory Assessment	Ability to assess for cloud resources categorizions in terms of total Cloud Accounts, Hosts, Applications, WEB APIs, Clusters, Containers with an organized view into your cloud resources across multi-cloud.
Continuous Compliance	Ability to review the cloud infrastructure health and compliance posture by leveraging frameworks like **STIG, CIS, NIST CSF, HIPAA, MITRE**
CI/CD Integration	Github Actions, Gitlab, Jenkins plugins,AWS pipeline, GCP code build pipeline, Azure Devops pipeline

Integrations

Tools integrations	Nessus, Nipper, Fortify, Sonarqube, Veracode, Burp, Zap, AWS Security Hub, Prowler, AWS Macie, Clair, Trivy, KubeBench, KubeHunter, DroopeScan, LambaGuard, SonaType, CLOC, KubeRBAC, Synk
Ticketing Integrations	Ability to comment-analysis on the ticket. Support for Ticketing integration - Jira Cloud/Server, FreshService, ConnectWise
Reports	Ability to generate comprehensive report for sensitive assets to perform detailed Compliance Audit

AccuKnox CWPP

Observability

Workload Observability	Ability to observe the behaviour of workloads with granular control of clusters, namespaces and pods at Runtime posture (Managed & Unmanaged clusters, Containerized, VMs & Baremetal supported)

Compliance

Workload Hardening Policies	Recommended policies for runtime protection for different workloads.

Monitoring

Logs & Alerts	Ability to view raw logs. Ability to trigger alerts in an automated / customized way.

Zero Trust

Auto Discovered Zero Trust Policy	Ability to Recommend Automatically generated Hardening Policies based on standard compliance framework - **MITRE, NIST, PCI-DSS, CIS**
Custom Zero Trust Policy	Ability to Customize the Policy creation using Policy Editor Tool
Inline Remediation	Ability to execute inline remediation against runtime attacks like APT vulnerability, log4j, etc. with robust declarative Policy by ensuring uptime and Zero Trust posture of applications.
Network Microsegmentation	Ability to isolate workload and restrict traffic to prevent any malicious lateral movements

Orchestration

Multi User, Multi Tenant, Multi Cluster management	Ability to onboard & handle multiple tenants(users) and set RBAC control for User Management

Integrations

Channel Integrations	Ability to enable integration with SIEM Tools, Ticketing Backends & Notification applications. Splunk (with specialized AccuKnox app support), Slack (send policy violations to slack channels), Jira, AWS CloudWatch, rsyslog

Deployments

k8s workloads support	On prem and managed k8s support, including x86 and ARM architectures (for detailed support matrix check here).
VM & Bare-Metal support	Policy engine works on vm and bare-metal as well. Limited support in SaaS dashboard for VM/Bare-metal (ref)

Compliance

File Integrity Monitoring	Ability to not just monitor but block any write access to system folders.
Continuous Compliance	PCI-DSS, NIST, CIS, MITRE, DISA-STIG

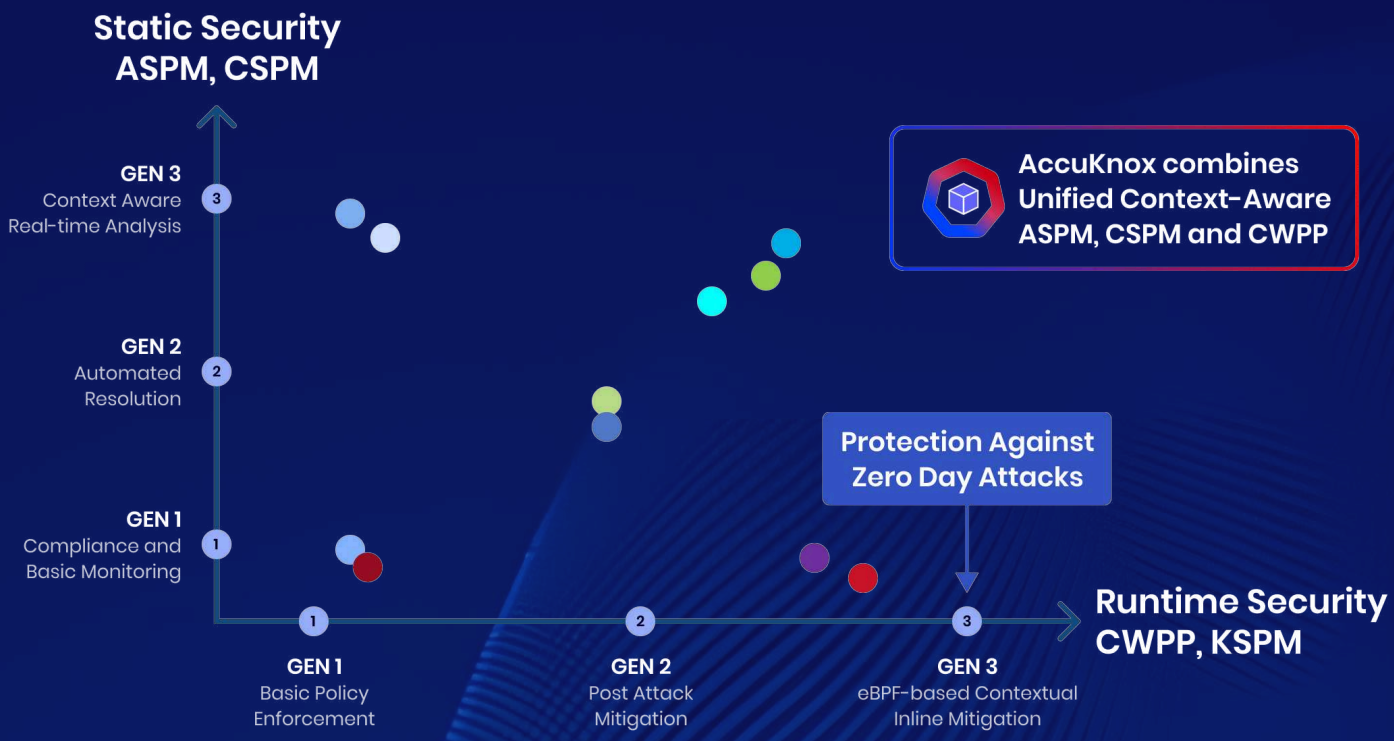
New Features

Admission Controller Support	Can integrated with Kyverno admission controller
KIEM (K8s Identities & Entitlements Management)	Ability to identify over-provisioned access. Identify service-accounts and users with different permissions.
Agentsless Risk Assessment	Ability to identify risks associated with Kubernetes Clusters with respect to misconfiguration and CIS benchmarks
ECS/EKS Fargate Support	Supported

AI-Co Pilot

ASK-ADA	AI LLM chatbot that answers queries related to the platform and gives information related to Assets and workloads onboarded in the platform

AccuKnox



Extra 30 Days Free Trial

aws

* No strings attached, Limited period offer!

Scan for Free Trial

About AccuKnox

AccuKnox is an AI-LLM-powered durable, reliable, and scalable Cloud Native Security Solution. Compliant with SOC2, STIG, PCI, HIPPAA, CIS, MITRE, NIST, and more. Enhances InfraSec & DevSecOps teams to Detect, Prioritize, and Protect Potential Cloud Attacks. Helps streamline Vulnerability triage and Alerts fatigue problems with GRC, Observability, and Inline Prevention. Provides Applications and Workloads resilience for both Public and Private Clouds by offering ASPM, CSPM, CWPP, CIEM & KIEM in one simplified Platform.