AccuKnox CSPM

Cloud Security Posture Management

Achieve Full Transparency of your Cloud Security Posture

Comprehensive Security Solution for Multi-Cloud and On-Premises

AccuKnox CSPM tool leverages agentless technology to deliver advanced cloud security. Proactively identify and prioritize vulnerabilities to deliver continuous compliance.
AccuKnox’s Cloud Native Application Protection Platform offers end-to-end cloud security, from development to production, by combining static and dynamic security measures using microservices. It securely stores data in S3 buckets and integrates with CI/CD pipelines and SIEM tools like Jira, Slack, Splunk, and Rsyslog for a comprehensive security system.
Overview
Compliance, Drift Detection & Vulnerability Scanning with Advanced CSPM Tool


- Continuous Compliance Monitoring
- Reporting and Governance
- Asset Inventory
- Incident Response
- Detect Misconfigurations
- Drift Detection
- DevOps Integrations
AccuKnox CSPM Tooling Is Your Best Bet

Gartner predicts that 99% of cloud security failures by 2025 will be due to customer misconfigurations. Are you willing to risk it all? Security Experts consider AccuKnox CSPM for airtight security.

### Cloud misconfiguration Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing critical misconfigurations due to human error</td>
<td>46%</td>
</tr>
<tr>
<td>Human error during remediation</td>
<td>45%</td>
</tr>
<tr>
<td>Difficulty training team members</td>
<td>43%</td>
</tr>
</tbody>
</table>

### Unidentified Misconfigurations
CSPM quickly detects and fixes misconfigurations to align cloud infrastructure with security best practices and reduce the risk of data exposure.

### Inadequate Visibility
CSPM offers real-time insights to detect vulnerabilities, unauthorized access, and potential threats in your cloud environment that could otherwise remain hidden.

### Compliance Challenges
Automate compliance checks with CSPM to ensure adherence to regulatory standards and reduce the risk of legal consequences and reputational damage.

### Dynamic Cloud Environments
CSPM offers a proactive defense against emerging threats by continuously monitoring, assessing, and adjusting security postures to adapt to the dynamic landscape of cloud infrastructure. This ensures resilient security.
Agentless CSPM Platform

**Basic Security**

Multi-Cloud Security & Compliance Posture Discovery, and protection through the use of native APIs.

**Application Security**

App Security from Code to Run
Mode of Deployment - DevSecOps, SaaS

Get a Demo
CSPM Features

- Cloud
- Continuous Compliance
- Misconfiguration
- Asset Hierarchy View (AHV)
- Assets Inventory
- CSPM DevOps Integrations
- Baseline and Drift Detection
- Reporting and Governance

AccuKnox Agentless CSPM Platform
## CSPM Features – Cloud

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CSPM Executive Dashboard</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Misconfiguration Detection</strong></td>
<td>Ability to Support for Misconfigurations Detection in Public Clouds (AWS, GCP, Azure).</td>
</tr>
<tr>
<td><strong>Inventory Assessment</strong></td>
<td>Ability to assess cloud resources categorized in terms of total Cloud Accounts, Hosts, Applications, WEB APIs, Clusters, Containers with an organized view into your cloud resources across multi-cloud.</td>
</tr>
<tr>
<td><strong>Continuous Compliance</strong></td>
<td>Ability to review the cloud infrastructure health and compliance posture by leveraging frameworks like STIG, CIS, NIST CSF, HIPAA, MITRE</td>
</tr>
<tr>
<td><strong>Baseline for Drift Detection</strong></td>
<td>Ability to detect drift in configuration. In the event of a potential security misconduct, baselines are critical to understand change from established expected behavior and raise an alert when it is violated.</td>
</tr>
</tbody>
</table>
Asset Inventory

- Identifies assets and provides visibility across a multi-cloud infrastructure
- Associates misconfigurations and vulnerabilities with asset
- Categorize assets in type of cloud resource and further allow assets to be in a customized group
- Segregated assets based on different environments (dev/test or prod) and tagging

Misconfiguration

The NSA has identified misconfiguration as a significant vulnerability in cloud environments, despite its less sophisticated nature, with critical implications.

- AccuKnox provides a unified view with clear action items and a tracking of findings in a multi-cloud environment.
- Continuous compliance trends of the categorized assets of interest to see the conformance or deviation from the custom baselines or standard technical or governance framework in general.
Baseline and Drift Detection

AccuKnox creates Baseline from multiple sources and tools

- Use scan results to establish a baseline on Day1++ of your infrastructure. Allow comparison on any subsequent day to determine induced "delta" difference.
- Deviation from the baseline could trigger an alert for integration methods supported by Slack or Jira.
- A custom baseline can be established, and customized alerts can be issued when security controls are breached.
Continuous Compliance

Ready to Use Compliance Templates

• AccuKnox CNAPP comes equipped with predefined templates.
• Organizations may assess their compliance against common standards such as CIS, NIST, PCI, GDPR, and HIPAA.
• By automating compliance checks against these benchmarks, AccuKnox enables organizations to identify gaps and deviations from best practices.
• This feature simplifies the compliance auditing process.
• We help you meet regulatory requirements and maintain a robust security posture.
• AccuKnox can help protect your workloads and infrastructure from attacks and threats.
• It does this by providing a set of hardening policies that are based on industry-leading compliance and attack frameworks (CIS, MITRE, NIST-800-53, and STIGs)
Asset Heirarchical View (AHV)

IT HELPS TO IDENTIFY DELTA DIFFERENCE OF CONFIGURATIONS.

First-time users can access their cloud account settings using the "Settings" button. The sidebar shows their assets categorized by Cloud Accounts, Asset Category, Region, and Asset. They can access assets using the global search bar or by expanding the tree. The user interface allows them to compare datalists from different dates and toggle the diff view to see changes.
CSPM DevOps Integrations

- SIEM Tools: Splunk, Rsyslog, Elastic Search, AWS Cloudwatch, Azure Sentinel
- AppSec Tools: CheckMarx, Veracode, Snyk, Fortify, Synopsys
- Notification Tools: Slack, Jira, PagerDuty
- Ticketing Tool: Jira, FreshService, ConnectWise, Zendesk
- Registries: ECR, ACR, Docker Hub, Nexus, Harbor

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:
- Our platform offers a range of ticketing integrations including Jira Cloud/Server, FreshService, ConnectWise, and ServiceNow. Plus, with our comment-analysis capabilities, you can easily analyze and manage tickets with ease.

Reports:
- Generating Comprehensive Reports for Sensitive Assets to Conduct a Thorough Compliance Audit
# Reporting and Governance

<table>
<thead>
<tr>
<th>Auto-Discover Posture</th>
<th>GH repo security status</th>
<th>App security posture &amp; vulnerability</th>
<th>Issues in Cloud Infra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>Cloud-&gt; current Cloud Posture</td>
<td>GH repo -&gt; scan</td>
<td>APP -&gt; auto generated policies</td>
</tr>
<tr>
<td>Continuous Observability</td>
<td>Multi-Cloud View</td>
<td>Application Behavior</td>
<td>Integration to SIEM tools</td>
</tr>
<tr>
<td>Mode of Enforcement</td>
<td>Auto Remediate and report violations</td>
<td>Detect Drift in cloud and get alerts</td>
<td>Audit and report suspicious behavior</td>
</tr>
<tr>
<td>Reporting, Analytics &amp; Auditing</td>
<td>Reporting for 3PAO</td>
<td>Real-time Log Monitoring</td>
<td>Audit Trail &amp; Deep Telemetry</td>
</tr>
</tbody>
</table>

- **Lightweight Agents on the cluster**
- **K8s Cluster**
- **Workloads**
- **Engine**
- **Agentless with SaaS Scanners**
  - **Cloud Account I**
  - **Asset Type Y**
  - **Asset Type Z**
  - **Asset N**
  - **Saas Scanners**
  - **Scan**
  - **Reports**
- **Agentless with local scanners**
  - **Cloud Account I**
  - **Asset Type Y**
  - **Asset Type Z**
  - **Asset N**
  - **Deploy Scanners**
  - **Saas Scanners**
  - **Scan**
  - **Reports**

**AccuKnox CSPM Features**

**AccuKnox Agentless CSPM Platform**

**Get a Demo**
AccuKnox CSPM vs Hyperscalers
Where HyperScalers Miss, AccuKnox Delivers

CSPM from HyperScalers

- Cloud Asset Inventory
- Web Application Firewall
- Secrets Manager & IAM Policies
- Container Security
- Vulnerabilities as part of SCA, SAST but without runtime context

AccuKnox CPM

- Multi-Cloud Support, Single Dashboard O&M, Consolidated Overview
- Complete visibility into entire Infrastructure & Application
- Misconfigurations detection
- Ability to leverage or define custom Baseline for Compliance
- Continuous compliance trends for your resources and workloads
- Detect sensitive assets
- Automated Issue tracking and management workflow
- Proactive monitoring and notified for alerts on configuration change
- Empower, Secure & Excel your Code → Cloud security
- Comprehensive Reporting for third party audits (3PAO)
- Manage full lifecycle of security processes not just identification

In the shared security model, hyperscalers are responsible for providing basic security, while customers are tasked with ensuring the protection of their applications. To provide advanced CSPM tool, AccuKnox builds upon the security capabilities of hyperscalers by offering multi-cloud and multi-cluster cloud asset protection.
AccuKnox CSPM Value Add over what hyperscalers provide

- Multi-cloud support
- Analyze Baseline Compliance for All Regions, even unconfigured ones
- Review and address findings ignoring repetitive issues, no need to re-review things which have been identified as not being real issues
- Allow security analyst to review policies, configuration, and findings without granting console access

- Monitor assets for changes to indicate when a re-review is necessary or if an undesirable condition has been detected.
- Analyze findings from other sources within context of an asset, i.e. static code analysis results grouped with container findings
- Report across groups that represent real world structures (business units, applications, departments, etc.)

- Provide reports demonstrating activity to governing agencies or 3PAO
- Assess pass/fail and remember status producing a true Baseline
- Manage full lifecycle of security processes not just identification
- Take action on findings by opening tickets with responsible party to resolve

Hyper Scalers

- AWS
  - Analyze Baseline Compliance for All Regions, even unconfigured ones
  - Generate findings for potential security issues
  - Perform service specific security analysis (Macie, Analyzer, Detective, etc.)
  - Collect vulnerability data and manage patching

AccuKnox CSPM tool uses agentless technology to enhance cloud security. It actively identifies and prioritizes vulnerabilities. Easy to achieve compliance with regulations. Tightly coupled integration with SIEM/SOAR platforms.
CSPM Dashboard Tour

- Onboarding
- Asset View
- Misconfigurations
- Remediation
- Identification Use Cases

AccuKnox Agentless CSPM Platform
Cloud Account Onboarding

Onboarding:
- Navigate to Settings
- Click on Cloud accounts
- Click on Add Account to add a new cloud account
Cloud Account Onboarding

Choose the Cloud provider (AWS | GCP | Azure)

- Select AWS
- Choose connection method -> Access keys
- Select Label and Tag (It will be used to identify the assets)
Asset View

- After Onboarding the cloud account wait for the scan to complete
- Scan is triggered instantly on account onboarding, but the scan completion might take at-least an hour or more. You will get an email after the successful scan executes.
- Once Scan completed, you should be able to see the cloud assets by navigating to Inventory -> Assets
Asset Detail View

You may further choose to view the misconfigurations associated with a particular Asset from Asset View.
Findings/Misconfigurations

To see the findings and misconfigurations associated with the Onboarded Cloud Account, please navigate to Issues -> Vulnerabilities.

- Apply SecurityHub/Cloudsploit in data-type filter
- You may choose the severity “Critical” or “High, Medium, Low” for the findings
Remediation: Setup Ticketing Integration

1. Setup Ticketing Configuration from Settings >> Integrations >> CSPM

2. Then go to the Remediation >> Ticket Summary to get Overview of the Issues

You need to raise issues from Asset Detail page or Issues >> Vulnerability section to see Ticket Summary
Remediation: Auto-Create Tickets

Two Approaches to Identify Issues: Inventory Asset Detail and Issues Vulnerabilities.
To generate a ticket, select the finding or misconfiguration from either the Inventory Asset Detail or Issues Vulnerabilities.

**Approach 1: Issues >> Vulnerabilities**
- Select the finding and Select the Ticket Configuration
- Create a ticket to get this issue logged

**Approach 2: Inventory >> Asset**
- Select the Asset and go to Asset Detail Page
- Select the ticket configuration (Jira etc.) and the finding then click on “Create a ticket” icon
Seeing only Failed Compliance in CIS

To see the compliance summary for the Failed results in CIS

- Click on Compliance Summary
- Select CIS from Filter by Compliance and select Failed from the Result filter.
- You can select filters by Compliance to see specific compliance
Seeing only Failed Compliance in HIPAA

To see the compliance summary for the Failed results in HIPAA

• Click on Compliance Summary
• Select HIPAA from Filter by Compliance and select Failed from the Result filter.
Identify S3 buckets accessible on public networks

- Go to Inventory >> Assets page and Filter for Asset Type as s3bucket
- Look for S3bucket with count in Total Vulnerabilities
Identify unencrypted EBS Volume

To identify the unencrypted EBS Volume associated with the Onboarded Cloud Account, Please navigate to Issues -> Vulnerabilities

- Apply Cloudsploit in data-type filter
- Choose the severity “Critical” for the Findings Search for “ebs volume” in the search field
Identify Hosts with Critical Findings

To identify Hosts with the Critical Findings, Please navigate to Issues -> Vulnerabilities

- Apply SecurityHub in data-type filter
- Choose the severity “Critical” for the Findings

103.105.23.45 is performing SSH brute force attacks against i-03b6098477fa7d26a. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.
Identify Container Images with critical vulnerabilities

To see the vulnerabilities associated with the Container Images, Please navigate to Issues -> Vulnerabilities

- Apply Trivy in data-type filter
- Choose the severity “Critical” for the Findings

Buffer Overflow in uv_encode(): (libtiff5@4.2.0-1+deb11u4)

ibftiff 4.5.0 is vulnerable to Buffer Overflow in uv_encode() when libtiff reads a corrupted little-endian TIFF file and specifies the output to be big-endian.
Summary of CSPM Toolkit
Summary of CSPM Features

- Asset discovery on Multi-Cloud
- Mapped misconfigurations and vulnerabilities to each asset
- Detect critical assets with highest severity and group findings based on asset
- Group critical assets together and do proactive monitoring for configuration change
- Multi-Cloud Support for Drift Detection
- Full scans generates lot of noise and information that could be redundant
- Baselining Infrastructure with respect to particular controls by CIS, PCI-DSS or multiple data sources that AccuKnox supports
- Delta difference over time will be recorded and generated as an alert
- Provides proactive Monitoring vs Point-in-time snapshot
About AccuKnox

- Why AccuKnox
- Customer Accolades
- Innovation Patents
- Analyst praise
- Power of partnerships
Why AccuKnox

Introducing One of the Most Comprehensive Zero Trust CNAPP Platforms in the Industry. Look no further for the ultimate solution – our platform provides unparalleled coverage. With support for public clouds like AWS, GCP, and Azure, as well as private clouds such as OpenStack and Tanzu, you can trust our platform to handle all your workload needs. We cater to modern workloads, like K8 and Serverless, and traditional workloads, like Virtual Machine and Bare Metal. Our platform is even equipped to handle futuristic workloads like IoT/Edge and 5G.

We also delivers both Static and Runtime Security, anchored on innovations in Cloud Security and AI/ML-based Anomaly Detection. With over 15 patents, we’re proud to offer an OpenSource, DevSecOps-led delivery model. To top it off, we have an ongoing R&D partnership with the esteemed Stanford Research Institute.

### Misconfiguration Detection
Scan for misconfigurations in IoC templates. Auto-remediate at the source with a pull request

- Misconfigurations in Multi-Cloud
- Runtime Security
- Detect threats leveraging KubeArmor and get auto-recommended Behavioural & Hardening Policies and get in-line remediation
- Auto Policy
- Custom Alert
- Microsegmentation
- LSMS Enforcement
- Activity audit

### Troubleshooting
Accelerate troubleshooting with a single source of truth

- Kubernetes Context
- eBPF backed telemetry
- Logs Aggregation
- Proactive Monitoring on Sensitive Assets

### Image Scanning
Scan for vulnerabilities and misconfigurations across static code, containers and hosts

- Registry / Image Scan
- Static Code Analysis
- Host scanning

### CSPM, KSPM & Compliance
Most comprehensive security posture by leveraging different security scanning tool. Custom Playbooks to cover all kind of Environments

- Security Tool integration
- Compliance frameworks
- Risk Based Prioritization

### Drift Detection
Get customized alerts based on deviation from baseline

- Custom Baseline
- Baseline Comparison
- Alerts on Drift
Customer testimonials

**Large US Government Contractor**

“We performed an extensive analysis of comparable industry offerings and selected AccuKnox due to its support for public and private cloud and highly differentiated capabilities in the areas of Risk Prioritization, Drift Detection, and Advanced Compliance. Furthermore, we were very impressed with AccuKnox’s integration with leading Vulnerability Management platforms like Nessus.”

**Large Cyber Insurance Provider**

“Their comprehensive and integrated offering; flexible deployment options; ongoing R&D commitment; Open Source foundations; and their track record of successful partnerships made them a clear winner.”

**Large Digital Health Provider**

“Zero Trust security is a Clint Health imperative and commitment we have to our customers. AccuKnox’s leading product combined with their successful track record of partnering with their customers forms the foundation for this objective.”

**European Cyber Service Provider**

“AccuKnox’s powerful combination of CSPM and CWPP; OpenSource foundations; In-line Zero Trust Security; Support for Public and Private Clouds; made them the ideal partner for us. Our client, a Large European CyberSecurity agency, was looking for a Zero Trust Security Solution that supports Private Cloud platforms. Our win is a clear testament to the value our clients see in this partnership. We look forward to many more successes ahead.”

---

**Key Takeaway**

Because of its sophisticated skills in Risk Prioritization, Drift Detection, and Compliance, AccuKnox is a reliable option for a wide range of sectors. It provides comprehensive, adaptable, Zero Trust security solutions and is recognized by government contractors, cybersecurity vendors, and innovators in digital health.
Pioneering Security Solutions with Patents

10+ Patents

- Deep Learning Algorithm for Ultra-scale Container Forensics and Stability Assessment.
- Federated peer-based container anomaly detection using variational auto-encoders.
- Container Function Virtualization: high-performance L7 protocol analysis.
- eBPF-based container-aware live sensitive data flow tracking, policy specification, and enforcement.
- System and method for predefined policy specification for containerized workloads.
- MUD (Manufacturer User Description) based Policy Controls for containerized workloads.
- Sensitive Data Flow tracking in container-based environments using unified forensic streams.
- Sensitive data flow tracking in container-based environments using trusted brokered transaction-based Provenance Graphs.

With more than ten patents to its name, AccuKnox is a proud innovator in the fields of deep learning for ultra-scale container forensics, federated peer-based anomaly detection, and live eBPF-based data flow tracing across dynamic container clusters. Get a free demo of our state-of-the-art products on the AWS Marketplace right now.
Security Experts Laud AccuKnox Innovations

“Zero Trust run-time Cloud Security has become an organizational imperative for Companies and Governments. AccuKnox’ highly differentiated approach, their eBPF foundations and their seminal innovations developed in partnership with Stanford Research Institute (SRI) positions them very well to deliver a highly efficient Zero Trust Cloud Security platform.”

Frank Dickson
Vice President
Security and Trust, IDC

“Run-time Cloud Security is extremely important to detect Zero Day attacks, Bitcoin Miners, DDOS attacks, etc. AccuKnox delivers a critical component of the CWPP (Cloud Workload Protection Platform). Their ability to deliver Network, Application and Data Security makes AccuKnox a unique and differentiated offering.”

Chris Depuy
Technology Analyst
650 Group Analyst

“AccuKnox’ foundational capabilities are innovative in the areas specific to Kubernetes security. By combining technologies like un-supervised Machine Learning and Data Provenance, AccuKnox is positioned to deliver a comprehensive and robust cloud native Zero-Trust security platform to their customers.”

Chase Cunningham
Renowned Cyber Security Analyst and Zero-Trust Expert

AccuKnox, a pioneer in cloud-native security, is renowned for its innovative Zero Trust runtime security, Cloud Workload Protection, and Kubernetes-specific capabilities, backed by a groundbreaking partnership with Stanford Research Institute.
Power of Partnerships

AccuKnox joins mimik Technologies, IBM as Open Horizon project partner

Overview of KubeArmor

KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operations) of containers and nodes (VMs) at the system level. KubeArmor leverages Linux security modules (LSMs) such as AppArmor, SELinux, or BPF to enforce the security policies.

Secure Bletorocket deployments on Amazon EKS with KubeArmor

News Flash

AccuKnox, brings together a range of industry partnerships (Software Vendors, Hyperscalers, Systems Integrators, MSSP, Resellers, etc.) to deliver customers with the most optimal solution, quick implementation approach and best ROI (Return on Investment).
About AccuKnox

AccuKnox provides a Zero Trust Cloud Native Application Protection Platform (CNAPP). AccuKnox is the core contributor to Kubernetes Run-time security solution, KubeArmor®, a very popular CNCF (Cloud Native Computing Foundation) project. AccuKnox was developed in partnership with SRI (Stanford Research Institute) and is anchored on seminal inventions in the areas of Container Security, Anomaly Detection, and Data Provenance. AccuKnox can be deployed in Public, Private and Hybrid Cloud environments. AccuKnox is funded by leading CyberSecurity Investors like National Grid Partners, MDSV, Avanta Venture Partners, Dolby Family Ventures, DreamIT Ventures, 5G Open Innovation Lab and Seedop.

www.accuknox.com contact@accuknox.com
You cannot secure what you cannot see.

Your most sensitive information is stored on cloud and on premise infrastructure. Protect what is most important from cyber attacks. Real-time autonomous protection for your network’s edges.

Ready to get started? Get Free Trial →