



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

Contents

Overview

CSPM Features

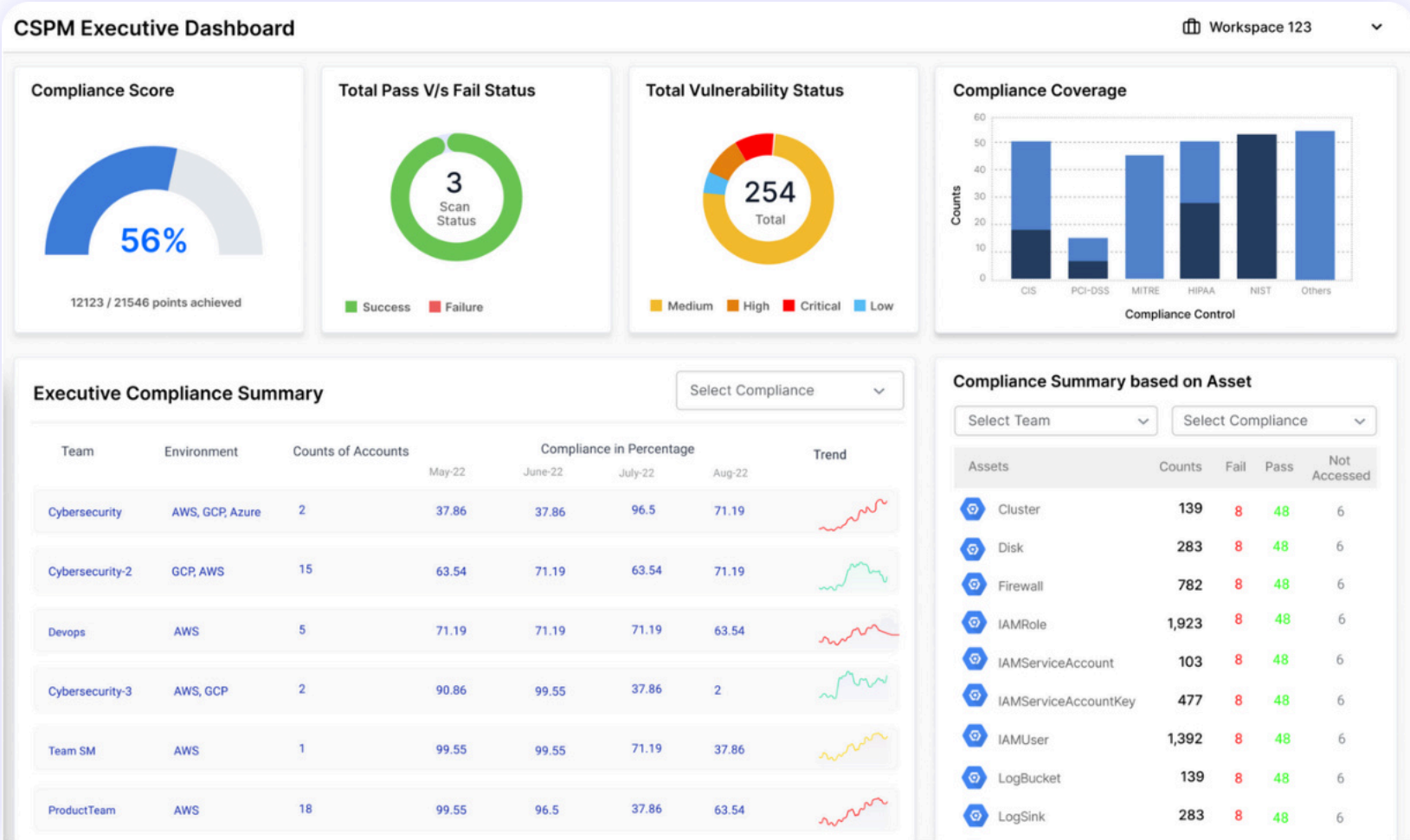
AccuKnox CSPM vs Hyperscalers

Dashboard Tour

Summary

About

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

CSPM Features

AccuKnox CSPM vs
Hyperscalers

Dashboard Tour

Summary

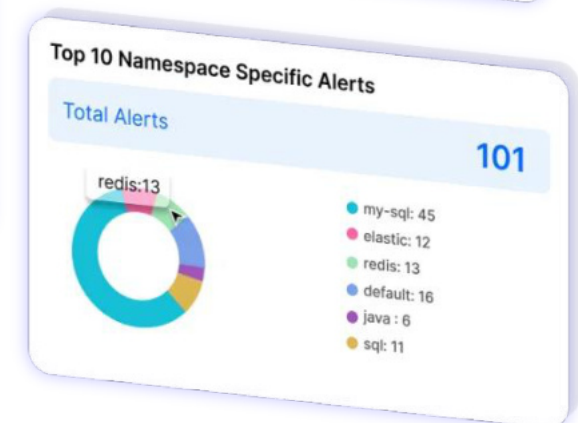
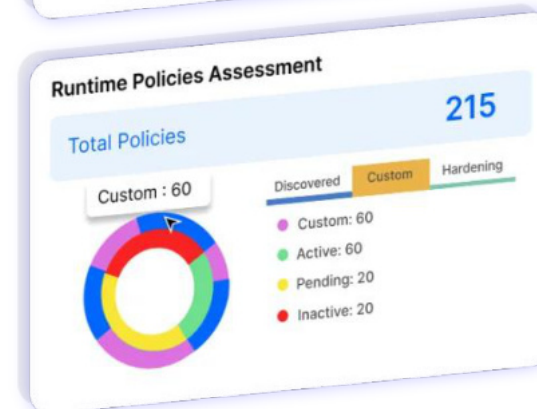
About

Overview

Compliance, Drift Detection & Vulnerability Scanning with Advanced CSPM Tool

Our CSPM architectural guidelines concur with best practices Zero Trust Cloud Security guidelines espoused by US Department of Defense NSA (National Security Agency), CNCF (Cloud Native Computing Foundation), GSA Zero Trust Architecture guidelines, and comprehensive functional and operational guidelines as outlined by Gartner.

- Continuous Compliance Monitoring
- Reporting and Governance
- Asset Inventory
- Incident Response
- Detect Misconfigurations
- Drift Detection
- DevOps Integrations



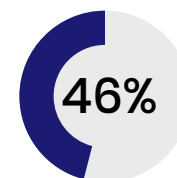
AccuKnox CSPM Tooling Is Your Best Bet

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.

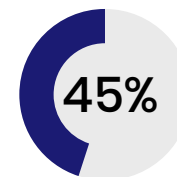
1	Unidentified Misconfigurations	CSPM quickly detects and fixes misconfigurations to align cloud infrastructure with security best practices and reduce the risk of data exposure.
2	Inadequate Visibility	CSPM offers real-time insights to detect vulnerabilities, unauthorized access, and potential threats in your cloud environment that could otherwise remain hidden.
3	Compliance Challenges	Automate compliance checks with CSPM to ensure adherence to regulatory standards and reduce the risk of legal consequences and reputational damage.
4	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.

Cloud misconfiguration Challenges

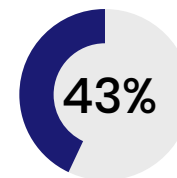
Commonly cited challenges in managing cloud misconfigurations. Source: 2020 Fugue State of Cloud Security Survey



Missing critical misconfigurations due to human error



Human error during remediation

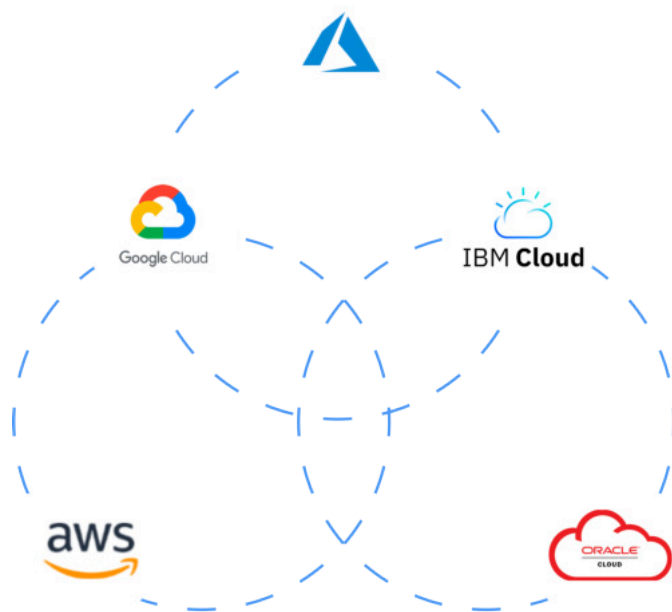


Difficulty training team members

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

DevSecOps ~ IaC w/ Runtime

IaC based on Runtime Context

System access behavior Summary

Sensitive asset access

Status	PARENT PROCESS	PROCESS	COUNT
●	/bin/bash	/usr/bin/rsync	28
●	/home/hadmend/build/powershell	/bin/bash	10
●	/usr/bin/containerd-shim-runc-v2	/home/hadmend/build/powershell	1
●	/usr/bin/dash	/home/hadmend/appwrite	28

Findings

Server port status

Status	Name	Address	Status	Version	Cyberark	Hash	Signal
●	smtpd	localhost:8110	MD, SSL				
●	webdav	localhost:8111	MD, SSL				
●	app_server	localhost:8112	MD, SSL				
●	Google	google.com:443	TLS	7.54/1.2	TLS_AES_128_GCM_SHA256	SHA256	SC25A
●	Apple	apple.com:443	TLS	7.54/1.2	TLS_AES_128_GCM_SHA256	SHA256	SC25A
●	SubSOL	api.subsol.com:443	TLS	7.54/1.2	SC256_RSA_AES128_GCM_SHA256	SHA256	SC25A
●	SubSOL	api.subsol.com:443	TLS	7.54/1.2	SC256_RSA_AES128_GCM_SHA256	SHA256	SC25A
●	SubSOL	api.subsol.com:443	TLS	7.54/1.2	SC256_RSA_AES128_GCM_SHA256	SHA256	SC25A

Network Behavior Summary

Findings

Some checks were not successful

Runtime info / Name (path, request) / Consider also / ...

This branch has no conflicts with the base branch

This issue will only occur in this repository on merge pull requests

CSPM Features

Cloud

Continuous
Compliance

Misconfiguration

Asset Hierarchy
View (AHV)

Assets Inventory

CSPM DevOps
Integrations

Baseline and Drift
Detection

Reporting and
Governance

CSPM Features – 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 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.

Continuous Compliance

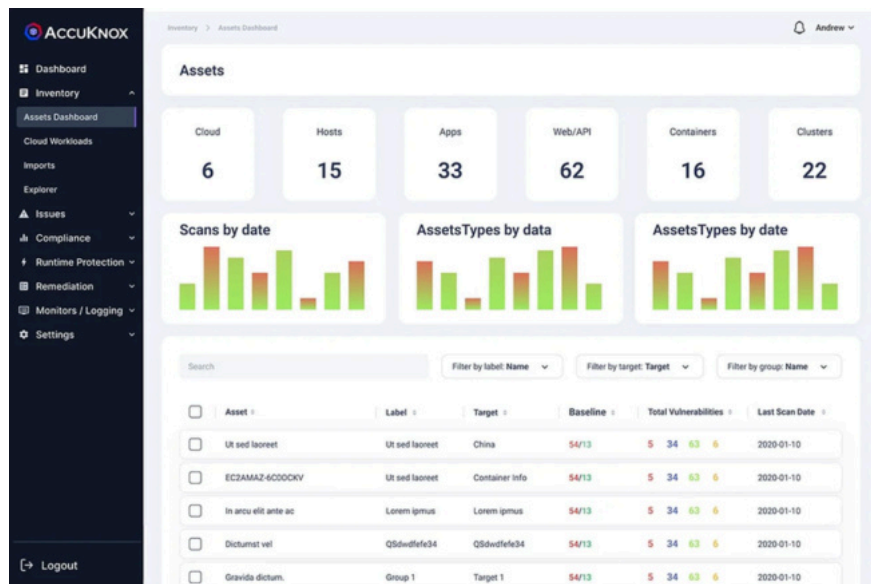
Ability to review the cloud infrastructure health and compliance posture by leveraging frameworks like STIG, CIS, NIST CSF, HIPAA, MITRE

Baseline for Drift Detection

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.

Asset Inventory

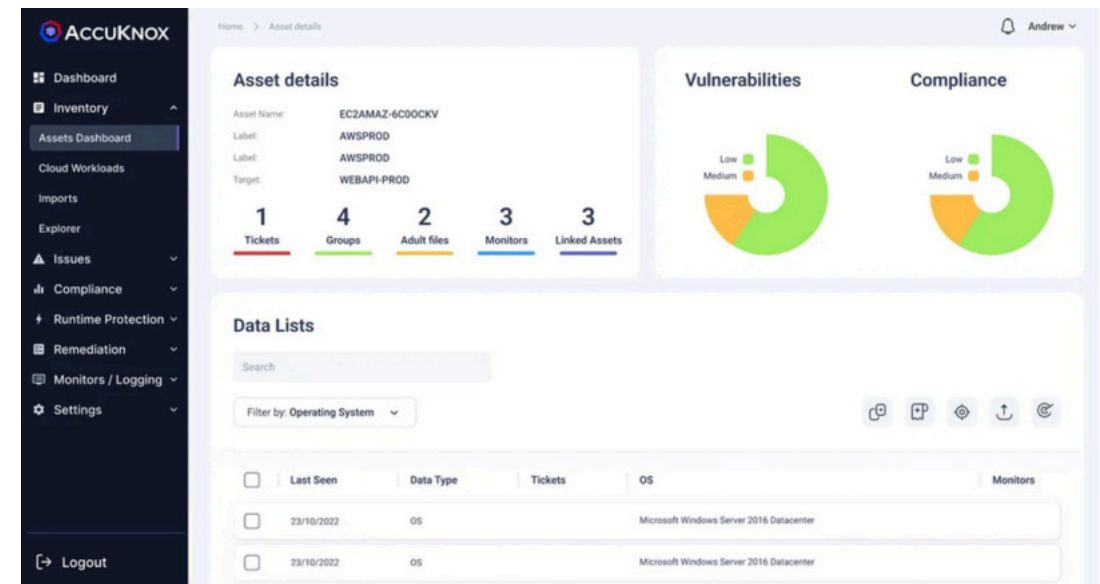
- Identifies assets and provides visibility across a multi-cloud infrastructure
- Associates misconfigurations and vulnerabilities with asset
- Categorize assets in type of cloud resource and further allow assets to be in a customized group
- Segregated assets based on different environments (dev/test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

Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
aws-compliance-baseline	CloudSploit	0	0	2	0/0	-
RickBase	CloudSploit	0	0	0	0/0	-
Prowler Baseline	Prowler	1	0	0	0/0	-
Testing	CloudSploit	0	0	0	0/0	-
test	CloudSploit	0	0	0	0/0	-
cloudsploit-test	CloudSploit	0	0	0	0/0	-
twst	CloudSploit	0	0	0	0/0	-
AWS Baseline	CloudSploit	1	0	0	0/0	-
test	CloudSploit	0	0	0	0/0	-
cloudsploit-test	CloudSploit	0	0	0	0/0	-

62%

BUSINESSES EXPERIENCE CLOUD MISCONFIGURATIONS.

Knowledge and Competence Gap

49%

BUSINESSES LACK SECURITY VISIBILITY AND MONITORING CAPABILITIES.

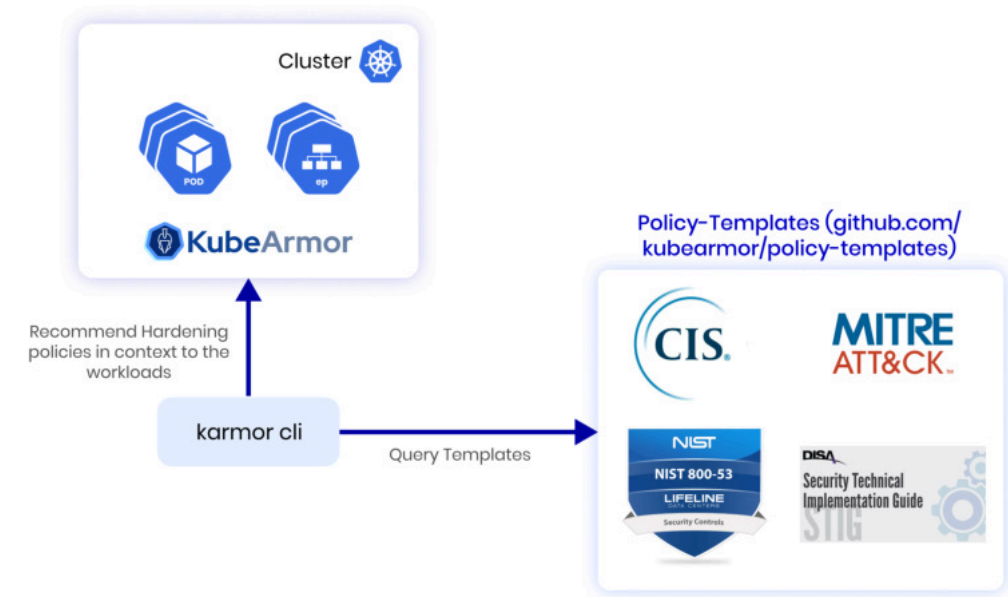
Visibility and Monitoring Hazard



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)



Compare

Finding	baseline-aws100723	aws-SH-auditfile-BL
AWS, Config should be enabled	✓	✗
Ensure, a log metric filter and alarm exist for unauthorized A...	✓	✗
Ensure, a log metric filter and alarm exist for S3 bucket polic...	✓	✗
Ensure, a log metric filter and alarm exist for CloudTrail confi...	✓	✗
Ensure, a log metric filter and alarm exist for security group c...	✓	✗
Ensure, a log metric filter and alarm exist for AWS Manageme...	✓	✗
PCI.RDS.1, RDS snapshot should be private, AWS Config eval...	✗	✓
PCI.S3.1, S3 buckets should prohibit public write access	✗	✓
PCI.RDS.2, RDS DB instances should prohibit public access	✗	✓

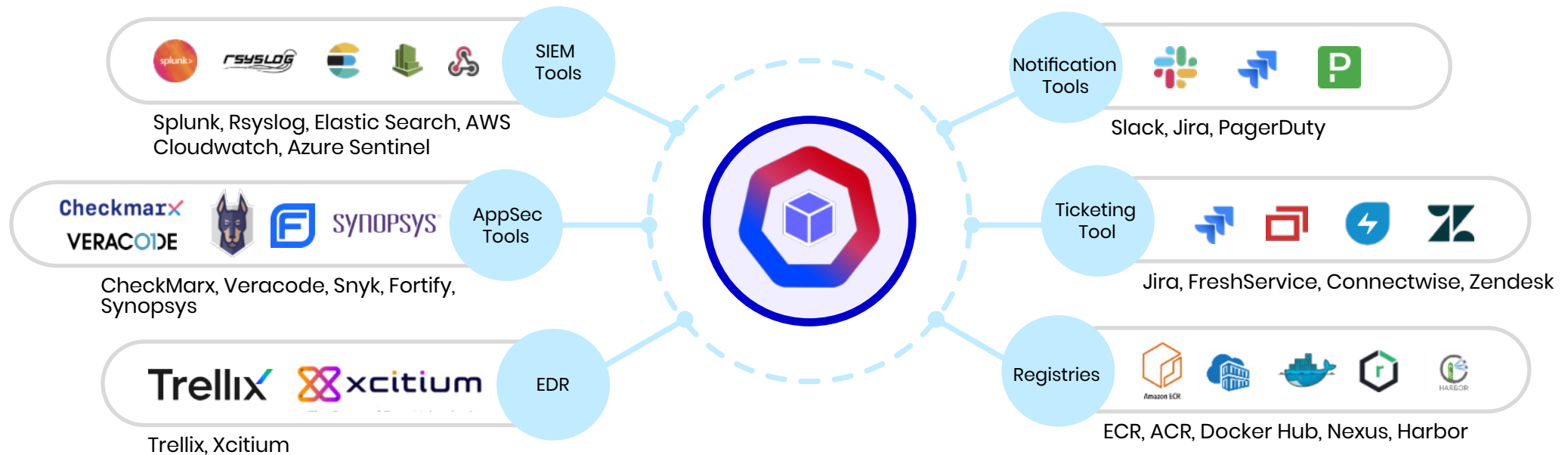
Asset Hierarchy View (AHV)

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.

The screenshot displays the AccuKnox dashboard interface. On the left is a dark sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, and Settings. The main panel shows the 'Assets (112)' list on the left, categorized by region (US-WEST-1, US-EAST-1, US-EAST-2). The selected asset is 'tfServicelessApiTest-3AspNetCoreFunction-1PT87CEI58JJ8'. The 'Asset Information' section shows: Name, Asset Type (AWS Lambda), Label (DEV), and Last Seen. A summary table indicates: Vulnerability (3), Compliance (6), Monitors (4), and Alerts (9). The 'DataList Information' section provides details like Description, Memory, Ephemeral Storage, Trigger, and VPC. The 'Permission' section shows 'lambda_basic_execution'. At the bottom, a 'Diff View' compares configurations from 14/07/2023 and 21/07/2023, highlighting changes in the 'ports' section.

CSPM DevOps 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

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

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

Risk Framework

Auditing, Automated Remediation & Reporting

60%

Hardening Policies

70%

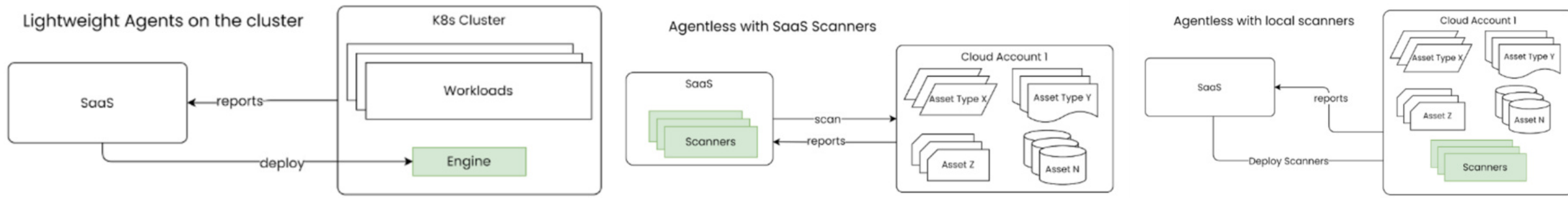
Any Security Policies

40%

Namespace with Policies

Secure Apps and Infrastructure

Organization, Multi-Tenancy, RBAC



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

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

- 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

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

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

CSPM Dashboard Tour

Onboarding

Asset View

Misconfigurations

Remediation

Identification Use Cases

Cloud Account Onboarding

Onboarding:

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

The screenshot displays the AccuKnox dashboard interface. On the left, a dark sidebar contains a menu with 'Cloud Accounts' highlighted. The main content area shows the 'Cloud Accounts' page with a search bar, a table of accounts, and an 'Add Account +' button. A red box highlights the 'Add Account +' button, and a red arrow points to it from below. Another red box highlights the 'Cloud Accounts' menu item, with a red arrow pointing to it from the right. The table contains one entry for an AWS account.

Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 956994857092	2023-08-14	<input checked="" type="checkbox"/>	a month ago	2023-09-13	Scan

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)

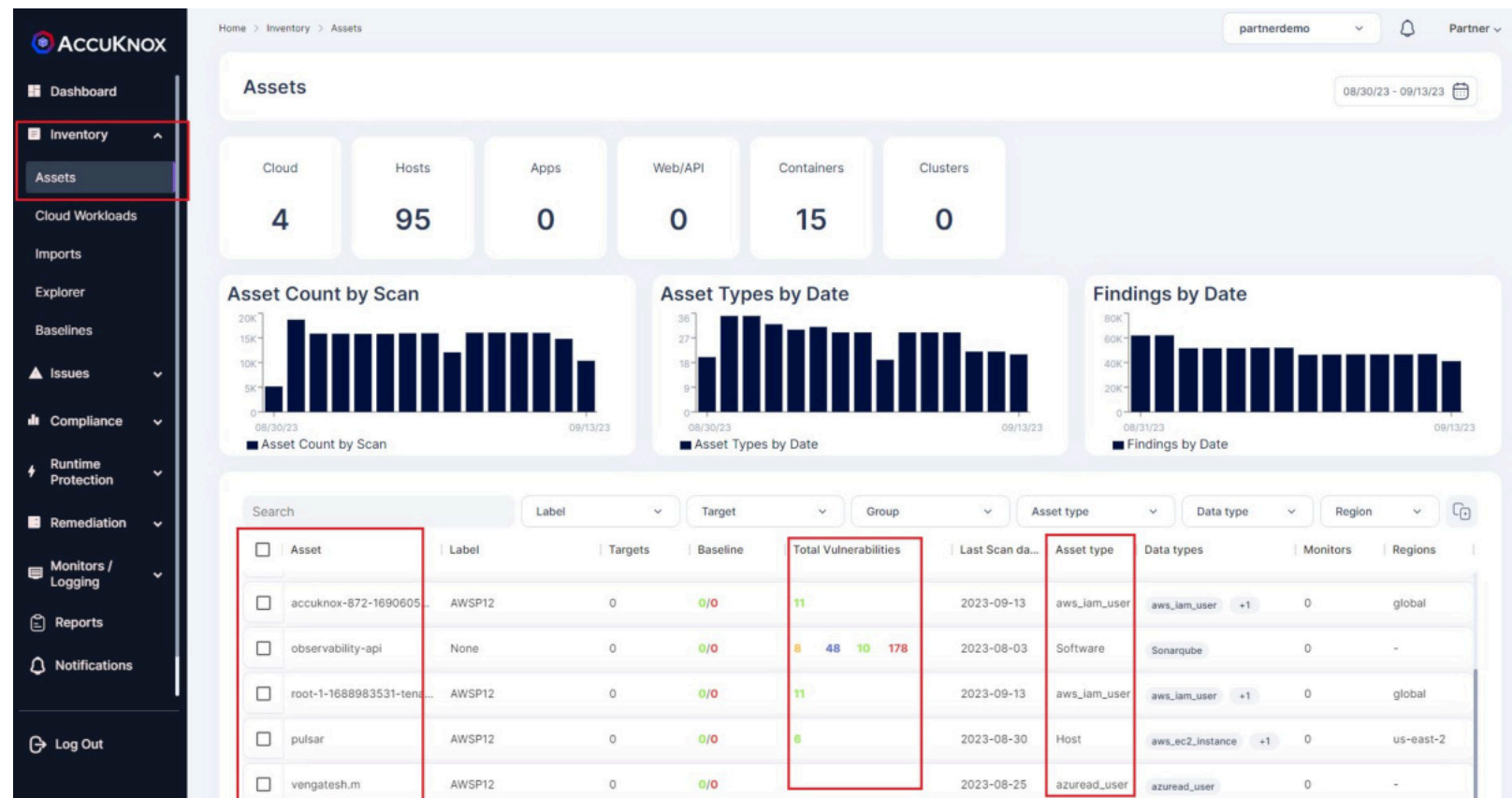
The screenshot shows the first step of the onboarding process, 'Cloud Account Details'. A progress bar at the top indicates three steps: 1. Cloud Account Details (checked), 2. Label & Tag, and 3. Set Up Connectivity. Below the progress bar, the text 'Select your Cloud Account' is centered. Three options are presented in a row, each with a logo and text: Amazon Web Service (AWS), Google Cloud Platform (GCP), and Microsoft Azure.



The screenshot shows the second step of the onboarding process, 'Label & Tag'. The progress bar at the top shows three steps: 1. Cloud Account Details (checked), 2. Label & Tag (checked), and 3. Set Up Connectivity. Below the progress bar, the text 'Label & Tag' is centered. The form contains three dropdown menus: 'Connection Method *' with 'Access Keys' selected, 'Label *' with 'AWSDEV14AUG' selected, and 'Tag' with 'TESTJULYAWS' selected. At the bottom, there are three buttons: 'Back', 'Cancel', and 'Next'.

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

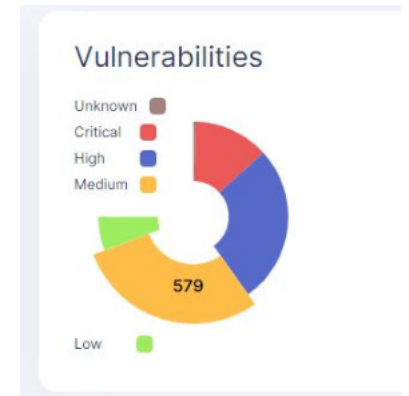
You may further choose to view the misconfigurations associated with a particular Asset from Asset View

The screenshot shows the AccuKnox dashboard with a sidebar on the left containing navigation items: Dashboard, Inventory, Assets, Cloud Workloads, Imports, Explorer, Baselines, Issues, Compliance, Runtime Protection, Remediation, and Monitors / Logging. The main content area is titled 'Asset details' and shows the following information:

- Asset Name: TESTBRIAN
- Label: DEMO14AUG
- Type: Host
- Last Seen: Wednesday, September 13, 2023 05:44 AM
- Region: us-east-1

Below the details are four summary cards: Tickets (1), Groups (0), Audit Files (0), and Monitors (0). The 'Explorer' section below has a search bar and filter options for Ticket Configuration and Filter by. A table lists assets with columns for Last seen, Data Type, Tickets, and OS. One asset is highlighted with a red box:

Last seen	Data Type	Tickets	OS
2023-09-11	aws_ec2_instance	0	



The 'Findings' section includes a search bar and filter options for Ticket Configuration, Group by, Data Type, Risk Factor, Ignored, Status, Tickets, and Exploit Available. A table lists findings with columns for Last seen, Risk Factor, Finding, Status, Ignored, Exploit Avail..., Tickets, and Data Type. Three findings are highlighted with red boxes:

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2023-09-12	Low	Instance Detailed Monitoring: us-east-1	Active	False	False	0	cloudsploit
2023-09-12	Low	EC2 has Tags: us-east-1	Active	False	False	0	cloudsploit
2023-09-12	Low	Insecure EC2 Metadata Options: us-eas	Active	False	False	0	cloudsploit

Findings/Misconfigurations

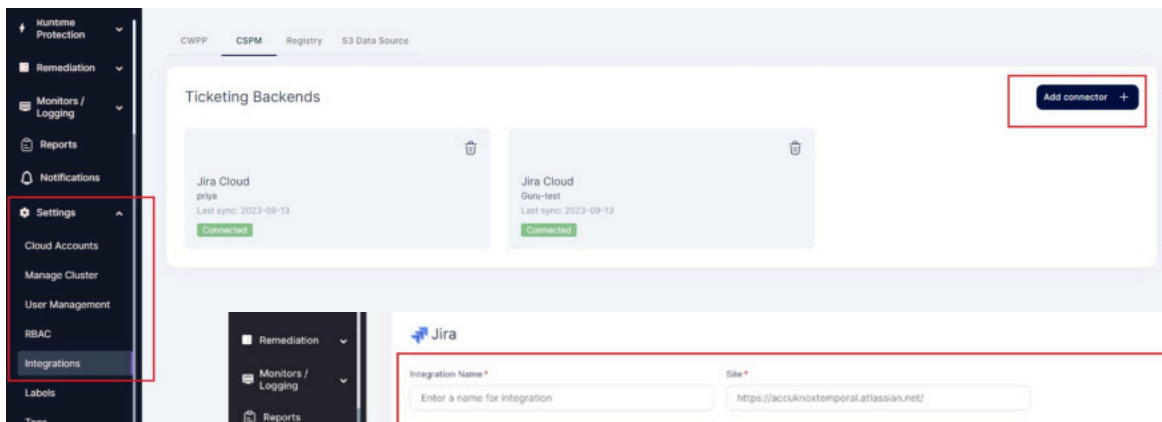
To see the findings and misconfigurations associated with the Onboarded Cloud Account, Please navigate to Issues -> Vulnerabilities

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

The screenshot shows the AccuKnox interface for viewing vulnerabilities. The left sidebar contains navigation options: Dashboard, Inventory, Issues (with Vulnerabilities selected), Registry Scan, Risk-based Prioritization, Compliance, Runtime Protection, Remediation, Monitors / Logging, Reports, Notifications, and Settings. The main content area is titled 'Vulnerabilities' and includes several filter dropdowns: Risk factor (set to High), Ignored (set to Ignored), Status (set to Status), Tickets (set to Tickets), Group (set to Group), and Scan (set to Scan). There is an 'Edit' button and a 'Reset' button. Below the filters is a search bar and a table of findings. The table has columns for Group ids, Last seen, Finding, Status, Tickets, Ignored, Data Type, Exploit Avail..., and Asset. The table contains three rows of data:

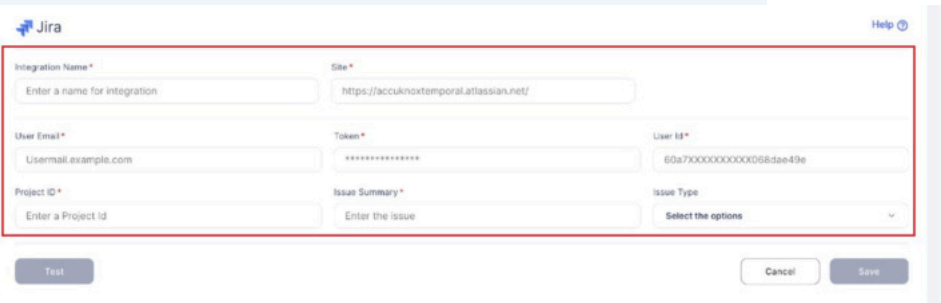
Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
1	2023-09-10	Block public access settings are disabled for the S3 bucket	Active	None	False	securityhub	False	vd-testing
1	2023-09-10	AWS Health - AWS_SECRETSMANAGER_SECURITY_NOTIFICA...	Active	None	False	securityhub	False	7884710678...
8	2023-08-26	CVE-2022-24771 - node-forge	Active	None	False	securityhub	False	\$LATEST

Remediation: Setup Ticketing Integration



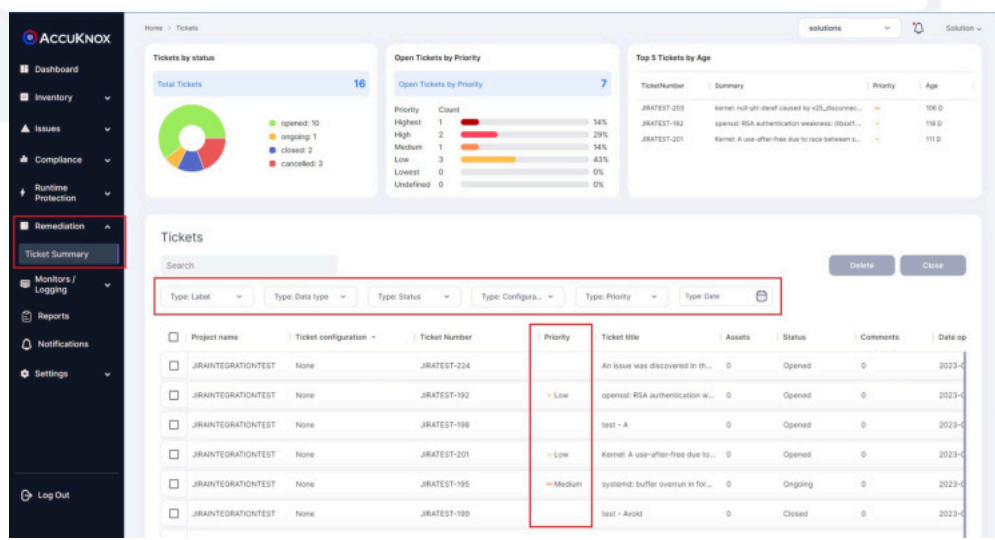
1

Setup Ticketing Configuration from Settings >> Integrations >> CSPM



2

You need to raise issues from Asset Detail page or Issues >> Vulnerability section to see Ticket Summary



3

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

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

The image shows two screenshots of the AccuKnox dashboard. The top screenshot shows the 'Issues >> Vulnerabilities' path. The left sidebar has 'Issues' selected, and 'Vulnerabilities' is highlighted. The main content area shows a 'Vulnerabilities' filter with 'Trivy' selected. Below is a table of findings with columns: Last seen, Finding, Status, Tickets, Ignored, Data Type, Exploit Avail., and Asset. One row is selected, and a 'Create a ticket' icon is visible in the top right of the table area.

The bottom screenshot shows the 'Inventory >> Asset' path. The left sidebar has 'Assets' selected. The main content area shows a table of findings with columns: Last seen, Data Type, Tickets, OS, and Monitors. One row is selected, and a 'Create a ticket' icon is visible in the top right of the table area.

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

The screenshot displays the 'Compliance Summary' page in the AccuKnox CSPM platform. The left sidebar contains navigation options, with 'Compliance Summary' highlighted. The main content area shows a filter configuration where 'Filter by Compliance' is set to 'CIS1' and the 'Result' filter is set to 'Failed'. A table below lists several failed compliance items, including IAM access keys, S3 buckets, and CloudTrail logging, with columns for Result, Info, Compliance, Control, Assets, Solution, and Description.

Result	Info	Compliance	Control	Assets	Solution	Description
FAILED	Category: IAM	CIS1 +1	Access Keys Last Used	5d8cc2b3-7199-46b3...	Detects access keys t...	Detects access keys t...
FAILED	Category: IAM	HIPAA +2	Access Keys Rotated	5d8cc2b3-7199-46b3...	Ensures access keys ...	Ensures access keys ...
FAILED	Category: S3	CIS1	S3 Bucket MFA Delete...	5d8cc2b3-7199-46b3...	Ensures MFA delete is...	Ensures MFA delete is...
FAILED	Category: CloudTrail	HIPAA +2	CloudTrail Enabled	5d8cc2b3-7199-46b3...	Ensures CloudTrail is ...	Ensures CloudTrail is ...
FAILED	Category: CloudTrail	HIPAA +2	CloudTrail Enabled	5d8cc2b3-7199-46b3...	Ensures CloudTrail is ...	Ensures CloudTrail is ...
FAILED	Category: CloudTrail	CIS1	CloudTrail To CloudW...	5d8cc2b3-7199-46b3...	Ensures CloudTrail lo...	Ensures CloudTrail lo...

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.

The screenshot displays the 'Compliance Summary' interface. On the left, a dark sidebar menu has 'Compliance Summary' highlighted with a red box. The main content area shows a 'Compliance Summary' header with several filters: 'Select Provider', 'Select Clo...', 'Region', 'Group by', and a 'FAIL...' filter highlighted with a red box. A date range filter shows '09/01/23 - 09/14/23'. Below the filters is a search bar and a 'Filter by Compliance' section where 'HIPAA' is selected and highlighted with a red box. A 'COLUMNS' button is visible above a table of results. The table has columns for 'Result', 'Info', 'Compliance', 'Control', 'Assets', 'Solution', and 'Description'. The table lists six failed compliance items, each with a checkbox, a 'FAILED' status, a category, a compliance standard (HIPAA or CIS2), a count, a control name, an asset ID, a solution, and a description.

Result	Info	Compliance	Control	Assets	Solution	Description
<input type="checkbox"/> FAILED	Category: IAM	HIPAA +2	Access Keys Rotated	5d8cc2b3-7199-46b3...	Ensures access keys ...	Ensures access keys ...
<input type="checkbox"/> FAILED	Category: S3	HIPAA +1	S3 Bucket Logging	5d8cc2b3-7199-46b3...	Ensures S3 bucket lo...	Ensures S3 bucket lo...
<input type="checkbox"/> FAILED	Category: CloudTrail	HIPAA +2	CloudTrail Enabled	5d8cc2b3-7199-46b3...	Ensures CloudTrail is ...	Ensures CloudTrail is ...
<input type="checkbox"/> FAILED	Category: CloudTrail	HIPAA +2	CloudTrail Enabled	5d8cc2b3-7199-46b3...	Ensures CloudTrail is ...	Ensures CloudTrail is ...
<input type="checkbox"/> FAILED	Category: CloudTrail	CIS2 +1	CloudTrail File Validati...	5d8cc2b3-7199-46b3...	Ensures CloudTrail fil...	Ensures CloudTrail fil...
<input type="checkbox"/> FAILED	Category: EC2	HIPAA +1	EBS Encryption Enabl...	5d8cc2b3-7199-46b3...	Ensures EBS volumes ...	Ensures EBS volumes ...

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

The screenshot shows the AccuKnox dashboard with a sidebar on the left containing navigation options like Dashboard, Inventory, Assets, Cloud Workloads, Imports, Explorer, Baselines, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Reports, and Notifications. The main content area features several summary cards for Cloud (4), Hosts (95), Apps (0), Web/API (0), Containers (15), and Clusters (0). Below these are three bar charts: 'Asset Count by Scan', 'Asset Types by Date', and 'Findings by Date'. A table at the bottom displays asset details, filtered by 'S3Bucket'. The table has columns for Asset, Label, Targets, Baseline, Total Vulnerabilities, Last Scan date, Asset type, Data types, Monitors, and Regions. The row for 'vd-testing' is highlighted with a red box, showing 1 total vulnerability. The 'S3Bucket' filter in the table header and the 'S3Bucket' column in the table are also highlighted with red boxes.

Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan date	Asset type	Data types	Monitors	Regions
dvsa-website-78847106...	DEMO14AUG	0	0/0	0	2023-09-03	S3Bucket	None	0	us-east-1
vd-testing	DEMO14AUG	0	0/0	1	2023-09-13	S3Bucket	aws_s3_bucket +1	0	us-east-1
s3public-bucket	DEMO14AUG	0	0/0	0	2023-09-14	S3Bucket	jobs +3	0	us-east-1
dvsa-receipts-bucket-7...	DEMO14AUG	0	0/0	0	2023-09-03	S3Bucket	None	0	us-east-1
config-bucket-78847106...	DEMO14AUG	0	0/0	0	2023-09-14	S3Bucket	jobs +4	0	us-east-1
do-not-delete-awsgoat-...	DEMO14AUG	0	0/0	0	2023-09-14	S3Bucket	jobs +4	0	us-east-1

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

The screenshot displays the AccuKnox interface for finding vulnerabilities. The left sidebar contains navigation options like Dashboard, Inventory, Issues, and Remediation. The main area is titled 'Vulnerabilities' and includes search filters for Risk factor (set to 'Critical'), Ignored (set to 'Ignored'), Status, Group, and Scan. Below the filters is a search bar containing 'ebs' and a table of results. The table has columns for Group ids, Last seen, Finding, Status, Tickets, Ignored, and Data Type. Three entries are visible, all with the finding 'EBS Encryption Enabled: us-east-2' and status 'Active'. To the right, a details panel for the selected finding shows 'Asset Type: AwsEc2Volume' and 'Severity: Low'. A description at the bottom states: 'Ensures EBS volumes are encrypted at rest, EBS volume is not encrypted to awscmk'.

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.

The screenshot displays the AccuKnox 'Vulnerabilities' page. The left sidebar contains navigation items: Dashboard, Inventory, Issues, Vulnerabilities (highlighted), Registry Scan, Risk-based Prioritization, Compliance, Runtime Protection, Remediation, and Monitors / Logging. The main panel shows filter tabs for 'SecurityHub' and 'TESTBR...'. Under 'Risk factor', 'Critical' is selected. The 'Asset Type' is set to 'Host'. A 'Finding' filter is also applied. Below the filters is an 'Edit' button and a search bar. A table lists findings with columns for Group ids, Last seen, Finding, Status, Tickets, Ignored, and Data Type. One finding is highlighted: Group id 1, Last seen 2023-09-10, Finding '103.105.23.45 is performing SSH brute force attacks against i-03b6098477fa7d26a', Status Active, Tickets 1, Ignored False, Data Type securityhub. To the right, a detailed view of this finding is shown, including its description: '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.' The detailed view also shows fields for Asset (TESTBRIAN), Asset Type (Host), Location (N/A), Status (Active), Ignored (False), Tickets (1), and Severity (Low), along with a 'Save' button.

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

The screenshot shows the AccuKnox interface. On the left is a navigation sidebar with 'Vulnerabilities' highlighted. The main panel has filters for 'Trivy' (data-type), 'Critical' (Risk factor), and 'Finding' (Ticket Configuration). Below the filters is a table of vulnerabilities:

Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type
2	2023-08-01	aom_image.c in libaom in AOMedia before 2021-04-07 frees ...	Active	1	False	trivy
1	2023-08-01	Buffer Overflow in uv_encode(): (libtiff5@4.2.0-1+deb11u4)	Active	1	False	trivy
1	2023-08-01	Buffer Overflow via /libtiff/tools/tiffcrop.c: (libtiff5@4.2.0-1+d...	Active	1	False	trivy
1	2023-08-29	CVE-2022-29361: (Werkzeug@2.0.3)	Active	1	False	trivy
1	2023-08-29	heap-based buffer over-read and overflow in inflate() in inflat...	Active	1	False	trivy

The detailed view on the right shows the selected vulnerability: 'Buffer Overflow in uv_encode(): (libtiff5@4.2.0-1+deb11u4)'. It includes details like Asset Type: Container, Severity: Critical, and a description: 'libtiff 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

The screenshot shows the AccuKnox dashboard interface. On the left is a navigation sidebar with options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, and Settings. The main content area displays 'Assets (112)' with a list of asset IDs and names. A selected asset's details are shown, including its name, type (AWS Lambda), label (DEV), and last seen time. A summary bar shows counts for Vulnerability (3), Compliance (6), Monitors (4), and Alerts (9). Below this, 'DataList Information' provides details about the asset's configuration, such as memory, storage, and permissions. A 'Permission' section shows the current configuration for 'lambda_basic_execution'.

The screenshot shows the 'Compare' feature in the AccuKnox dashboard. It displays a table with columns for 'Finding', 'Scan-Benchmark-Day1-788471067825', and 'Scan-Benchmark-Day1+-788471067825'. The findings are listed with green checkmarks for compliance and red X marks for non-compliance.

Finding	Scan-Benchmark-Day1-788471067825	Scan-Benchmark-Day1+-788471067825
passwordReusePrevention, Password Reuse Prevention	✓	✗
usersPasswordLastUsed, Users Password Last Used	✗	✓
configServiceEnabled, Config Service Enabled	✓	✗
usersPasswordLastUsed, Users Password Last Used	✓	✗
bucketPolicyCloudFrontOai, S3 Bucket Policy CloudFront OAI	✓	✗
cloudfrontHttpsOnly, CloudFront HTTPS Only	✗	✓
maxPasswordAge, Maximum Password Age	✓	✗
passwordRequiresNumbers, Password Requires Numbers	✓	✗
configServiceEnabled, Config Service Enabled	✗	✓
rootAccountInUse, Root Account In Use	✗	✓

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 IaC templates. Auto-remediate at the source with a pull request

Misconfigurations in Multi-Cloud

Proactive Monitoring on Sensitive Assets

Troubleshooting

Accelerate troubleshooting with a single source of truth

Kubernetes Context

eBPF backed telemetry

Logs Aggregation

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

Runtime Security

Detect threats leveraging KubeArmor and get auto-recommended Behavioural & Hardening Policies and get in-line remediation

Auto Policy

Custom Alert

LSMS Enforcement

Microsegmentation

Activity audit

Image Scanning

Scan for vulnerabilities and misconfigurations across static code, containers and hosts

Registry / Image Scan

Static Code Analysis

Host scanning

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



Patented

Deep Learning Algorithm for Ultra-scale Container Forensics and Stability Assessment.



Patented

Federated peer-based container anomaly detection using variational auto-encoders



Patented

Live eBPF Lightweight Provenance-based Data Flow tracking across Dynamic Topology Container Clusters



Patented

Container Function Virtualization: high-performance L7 protocol analysis



Patented

eBPF-based container-aware live sensitive data flow tracking, policy specification, and enforcement



Patented

System and method for predefined policy specification for containerized workloads



Patented

MUD (Manufacturer User Description) based Policy Controls for containerized workloads



Patented

Sensitive Data Flow tracking in container-based environments using unified forensic streams



Patented

Sensitive data flow tracking in container-based environments using trusted brokered transaction-based Provenance Graphs



Focus

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

Key Takeaway

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

Optimized for Intel® Smart Edge Zero Trust Cloud Native Application Protection



KubeArmor

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-LSM to enforce the

KubeArmor – an Open Source project by AccuKnox with 500k+ downloads, is now available in AWS Marketplace

CUPERTINO, Calif., June 22, 2023 /PRNewswire/ — AccuKnox™, a leader in Zero Trust CNAPP (Cloud Native Application Protection Platform), today announced KubeArmor™, an Open Source CNCF Kubernetes run-time security project, is now available in AWS Marketplace — a digital catalog with thousands of software listings from independent software vendors (ISVs) that make it easy to find, test, buy, and deploy software that runs on Amazon Web Services (AWS).

AccuKnox is now available in AWS Marketplace to provide application teams with greater access and scalability for Open Source CNCF Kubernetes run-time security project, KubeArmor.

"By making KubeArmor available in AWS Marketplace, we are taking steps towards achieving our goal of making Zero Trust Kubernetes Security project KubeArmor more widely available to the AWS community," said Rahul Jadhav, AccuKnox co-founder and chief technology & product officer.



KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)



September 13, 2022

AccuKnox Selected to Join 5G Open Innovation Lab Development Program, Bringing Zero Trust Security to the 5G Ecosystem

AccuKnox Forges Partnership with Touchstone Security, Managed Security Services Provider (MSSP) to deliver comprehensive Cloud Security Services

CUPERTINO, CA – July 24, 2023 AccuKnox, Inc announced a partnership with Touchstone Security, a seasoned Managed Security Services Provider (MSSP).

AccuKnox® offers a comprehensive Cloud Native Application Protection Platform (CNAPP) solution. AccuKnox delivers Zero Trust Security for Multi-cloud, Private/Public Cloud environments. In keeping with CI/CD best practices, AccuKnox focuses on finding vulnerabilities earlier in the software development process. AccuKnox is a comprehensive solution that delivers Cloud Security, Code Scanning, Container Security, API security, Host Security, Network Security and Kubernetes orchestration security. AccuKnox is a core contributor to Kubernetes run-time security solution KubeArmor which has been adopted by CNCF and has achieved 500k+ downloads. AccuKnox, Zero Trust Enterprise CNAPP is anchored on KubeArmor and is an integrated Cloud Native Security platform that includes:

WPP/KSPM (Cloud/Kubernetes Security Policy) WPP (Cloud Workload Protection Platform) IEM/KIEM (Cloud/Kubernetes Identity and Access Management)

Secure Bottlerocket deployments on Amazon EKS with KubeArmor

by Raj Seshadri | on 20 OCT 2022 | in Amazon Elastic Kubernetes Service, Containers, Customer Solutions, Technical How-To | Permalink | Share



August 1, 2022

AccuKnox Inc. joins the VMWare Technology Alliance Partner Program and announces the availability of AccuKnox Runtime Security on VMWare Marketplace

MENLO PARK, Calif. and CUPERTINO, Calif., Aug. 1, 2022 /PRNewswire/ -- AccuKnox Inc., The Zero Trust runtime security platform for Kubernetes, today announced it has joined

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



as featured in:



Leadership



Nat Natraj

CEO, Co-founder, Business



Phil Porras

Co-founder, Innovations



Rahul Jadhav

Co-founder, VP of Engg



Brian Burgess

Product



Raj Panchapakesan

Global Head- Business
Development & Partner Ecosystem



Jen Wilson

Director, Operations & Customer
Success



20+

TOOLS INTEGRATION

10+

PATENTS

30+

TRUSTED PARTNERS

10+

COMPLIANCE FRAMEWORKS

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 →