AccuKnox

CSPM

Cloud Security Posture Management

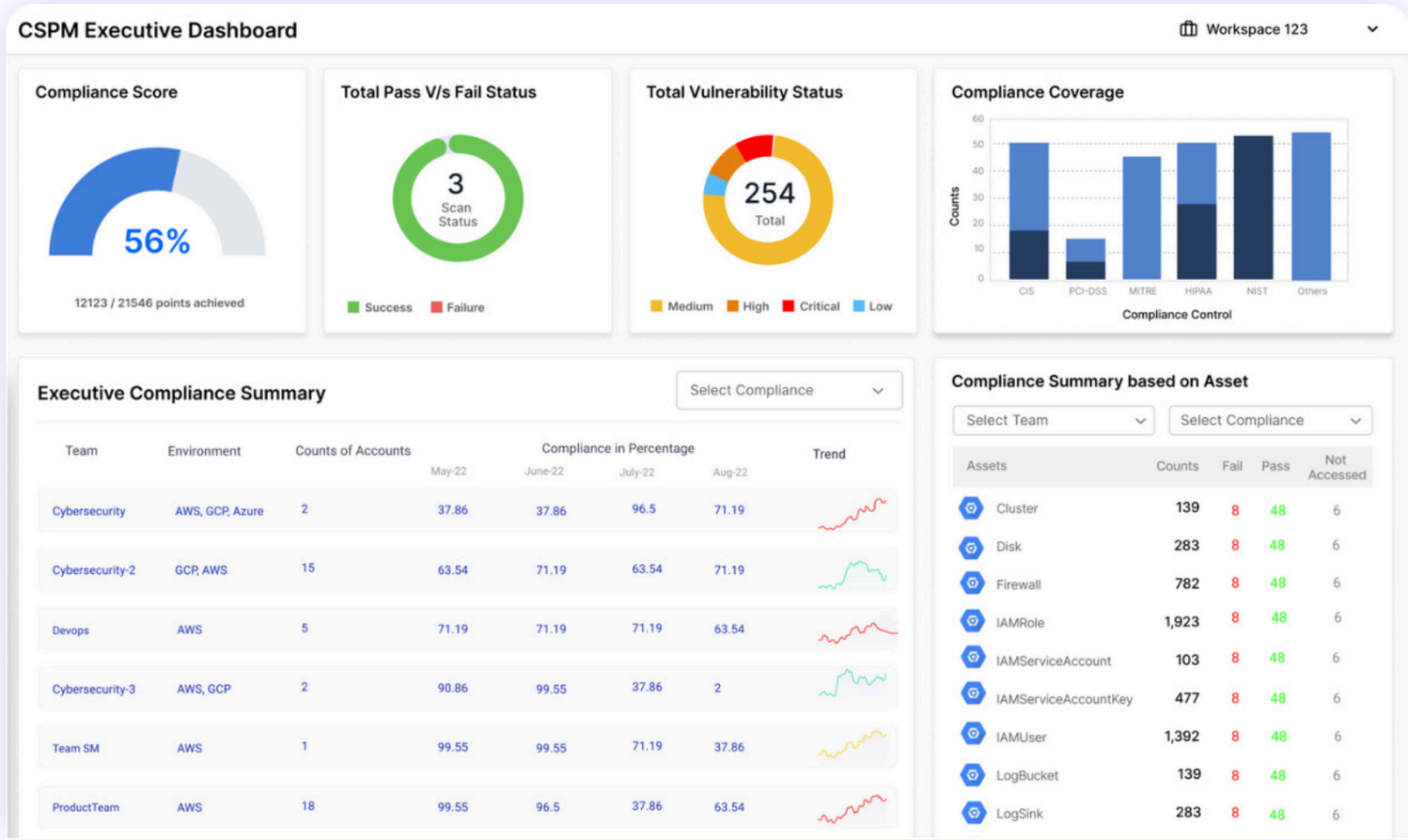
Achieve Full Transparency of your Cloud Security Posture

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

Contents

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

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

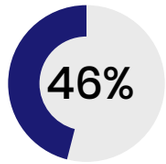
AccuKnox CSPM Tooling Is Your Best Bet

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.

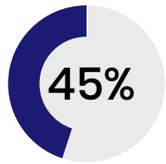
1	Unidentified Misconfigurations	CSPM quickly detects and fixes misconfigurations to align cloud infrastructure with security best practices and reduce the risk of data exposure.
2	Inadequate Visibility	CSPM offers real-time insights to detect vulnerabilities, unauthorized access, and potential threats 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

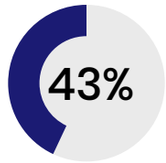
Commonly cited challenges in managing cloud misconfigurations. Source: 2020 Fugue State of Cloud Security Survey



Missing critical misconfigurations due to human error



Human error during remediation

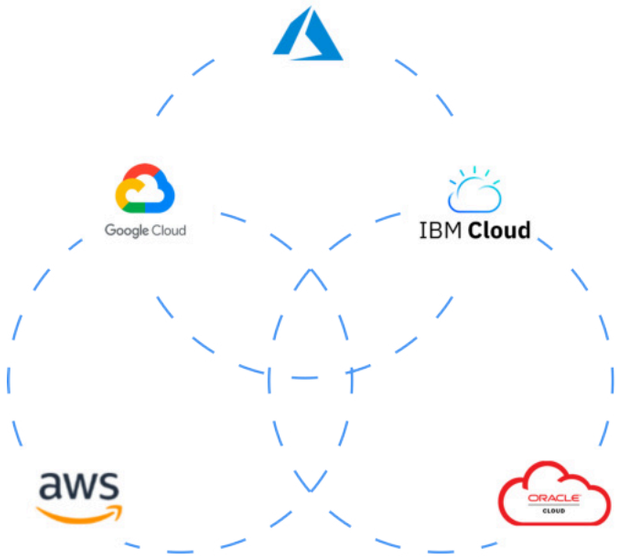


Difficulty training team members

Agentless CSPM Platform

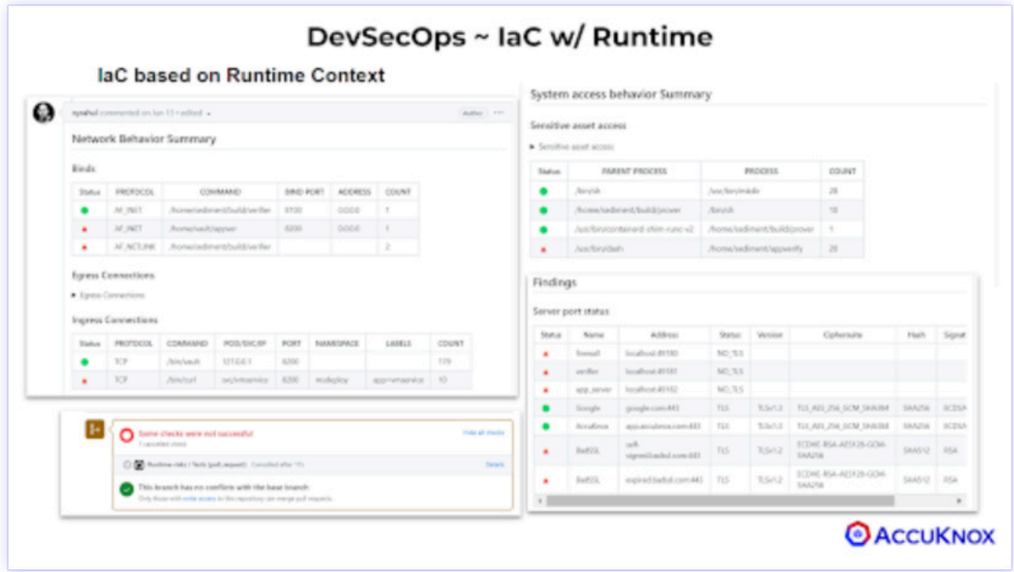
Basic Security

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



CSPM Features

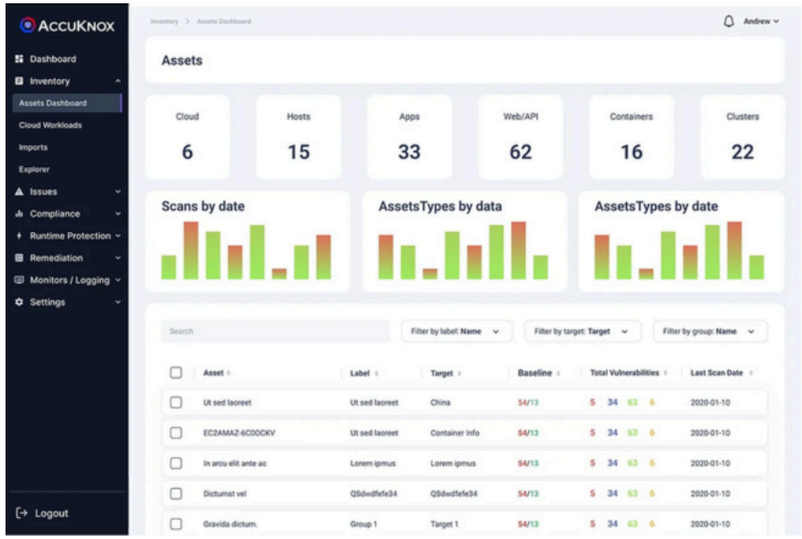
- Cloud
- Continuous Compliance
- Misconfiguration
- Asset Heirearichal View (AHV)
- Assets Inventory
- CSPM DevOps Integrations
- Baseline and Drift Detection
- Reporting and Governance

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

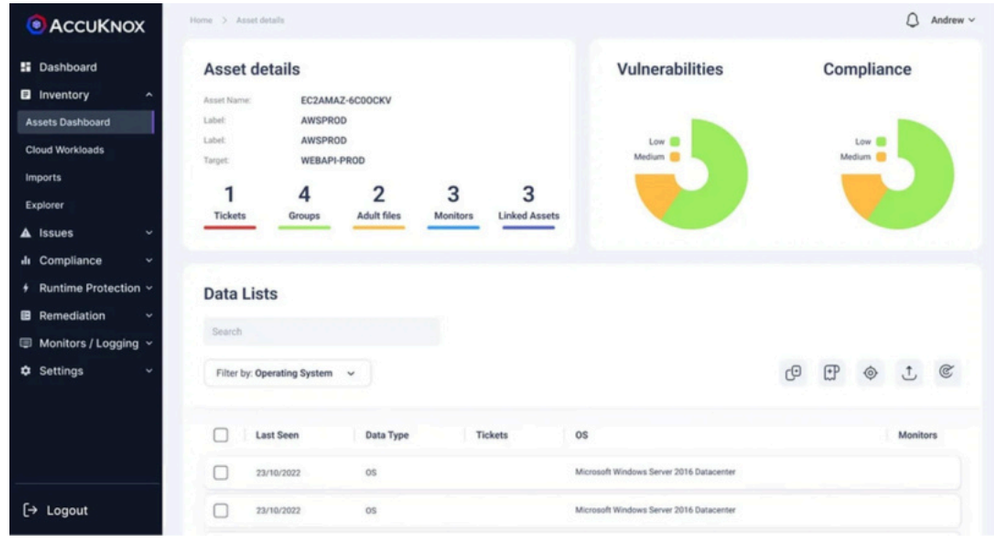
- Identifies assets and provides visibility across a multi-cloud infrastructure
- Associates misconfigurations and vulnerabilities with asset
- Categorize assets in type of cloud resource and further allow assets to be in a customized group
- Segregated assets based on different environments (dev/test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

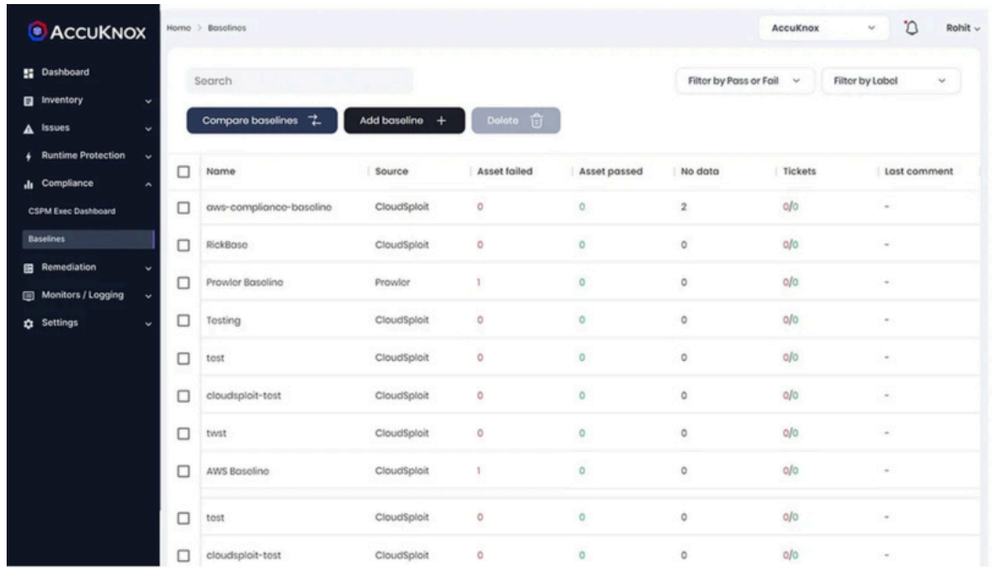
- AccuKnox provides a unified view with clear action items and a tracking of findings in a multi-cloud environment.
- Continuous compliance trends of the categorized assets of interest to see the conformance or deviation from the custom baselines or standard technical or governance framework in general.



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.



62%

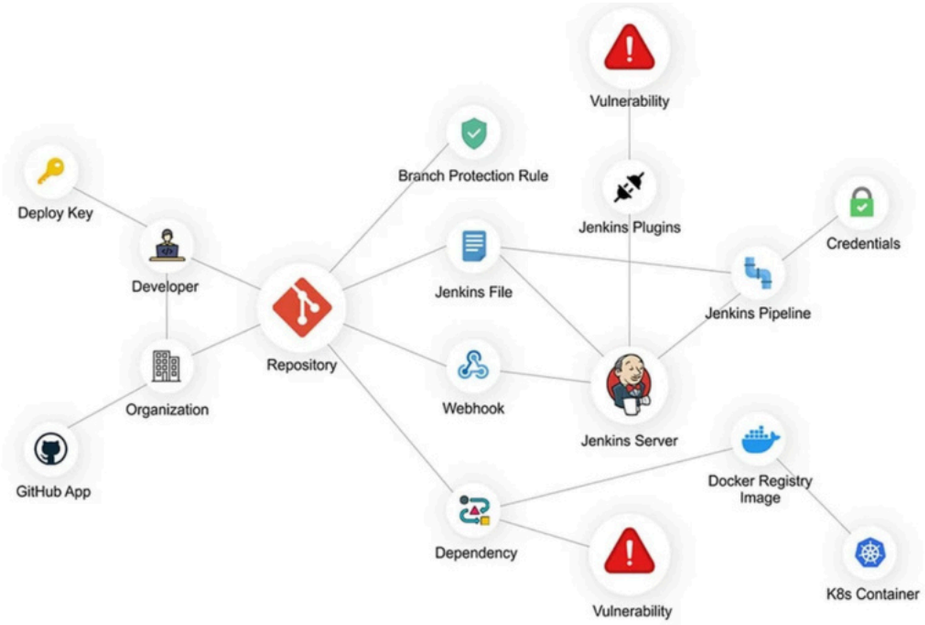
BUSINESSES EXPERIENCE CLOUD MISCONFIGURATIONS.

Knowledge and Competence Gap

49%

BUSINESSES LACK SECURITY VISIBILITY AND MONITORING CAPABILITIES.

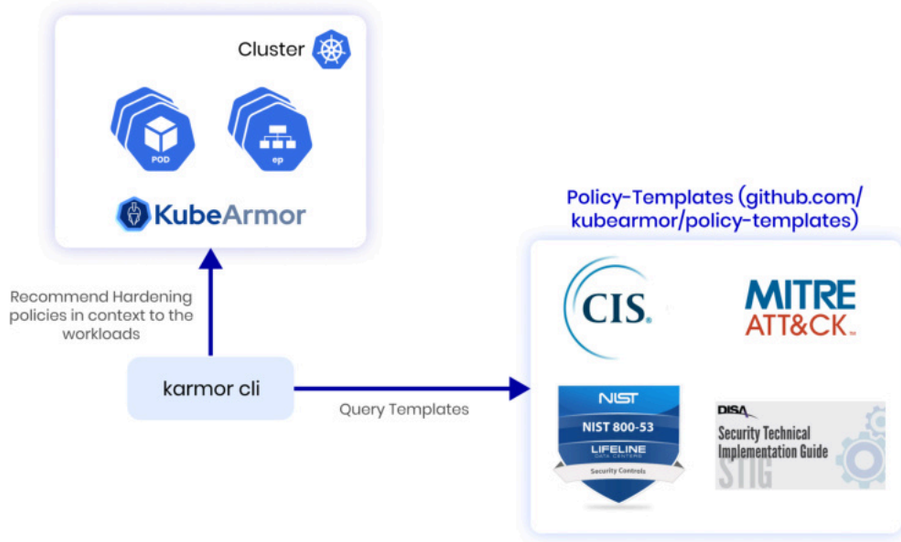
Visibility and Monitoring Hazard



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)



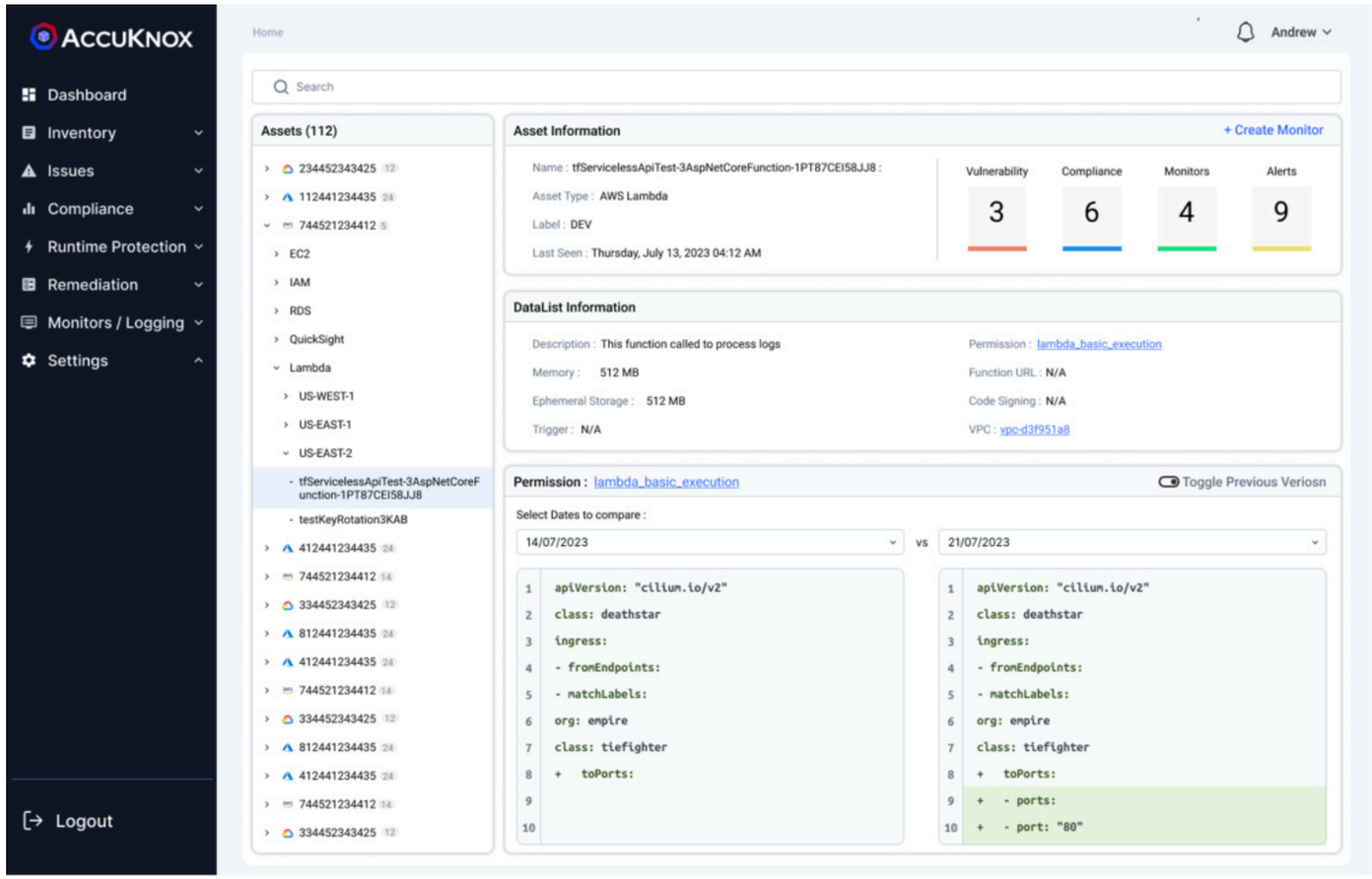
Compare

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	✗	✓

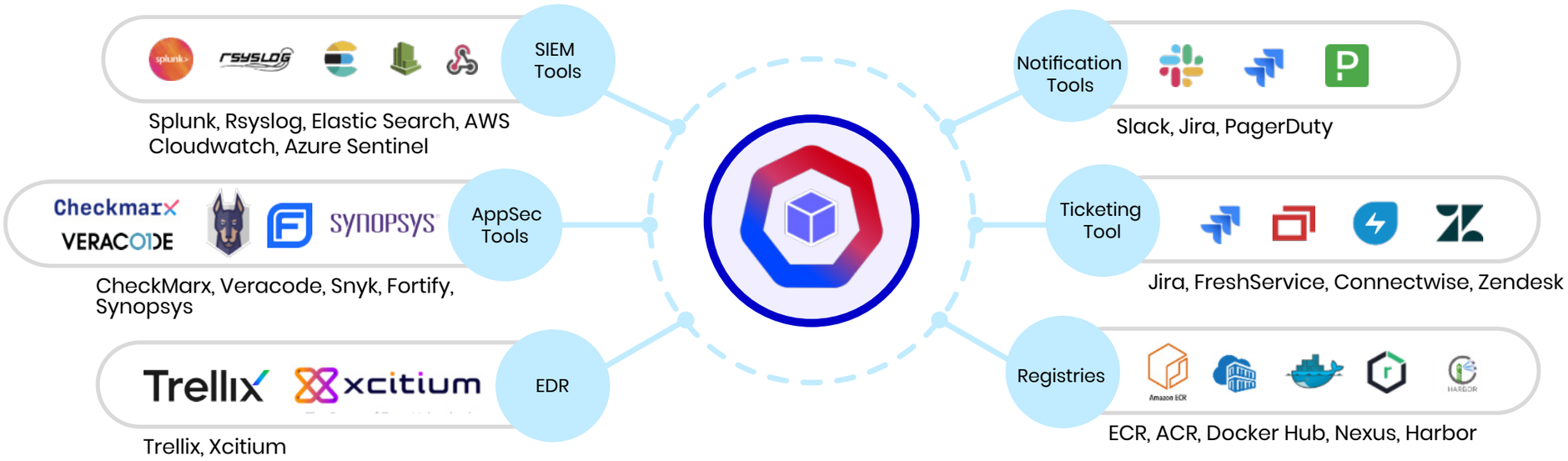
Asset Heirearichal View (AHV)

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.



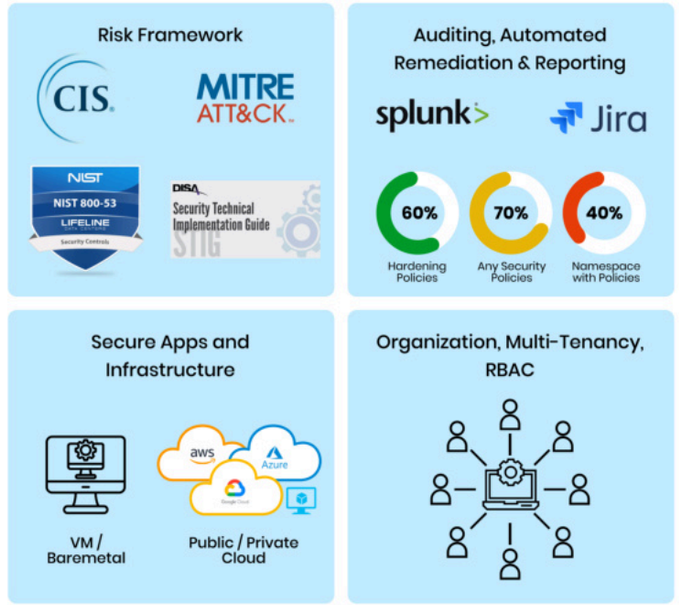
CSPM DevOps Integrations

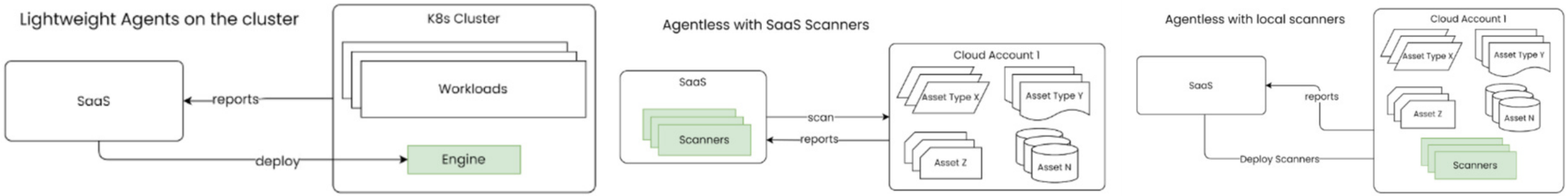


Tools integrations	Nessus, Nipper, Fortify, SonarQube, Veracode, Burp, Zap, AWS Security Hub, Prowler, AWS Macie, Clair, Trivy, KubeBench, KubeHunter, DroopeScan, LambaGuard, SonaType, CLOC, KubeRBAC, Synk
Ticketing Integrations	Our platform offers a range of ticketing integrations including Jira Cloud/Server, 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





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

Summary

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.

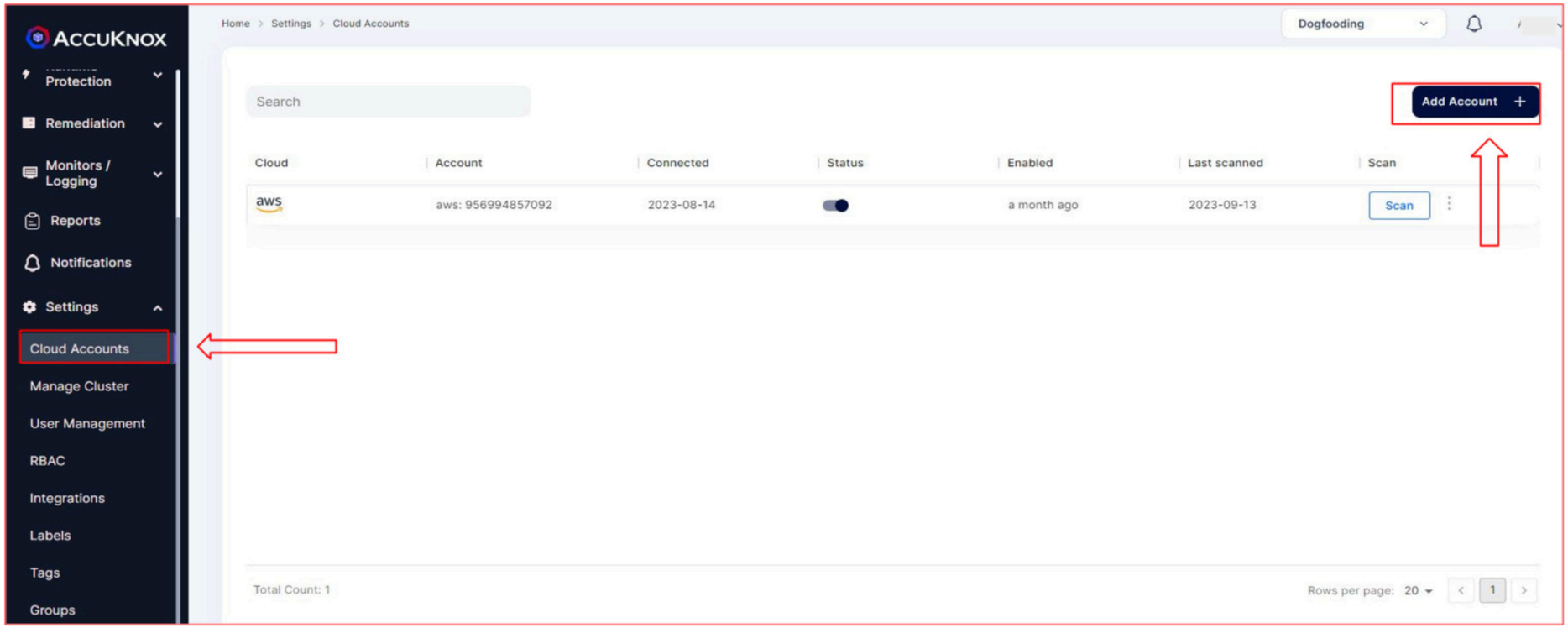
CSPM Dashboard Tour

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

Cloud Account Onboarding

Onboarding:

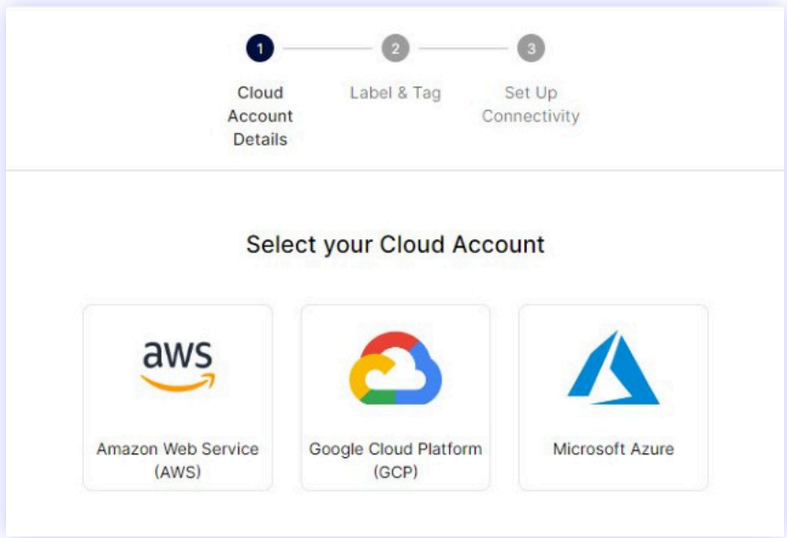
- Navigate to Settings
- Click on Cloud accounts
- Click on Add Account to add a new cloud account

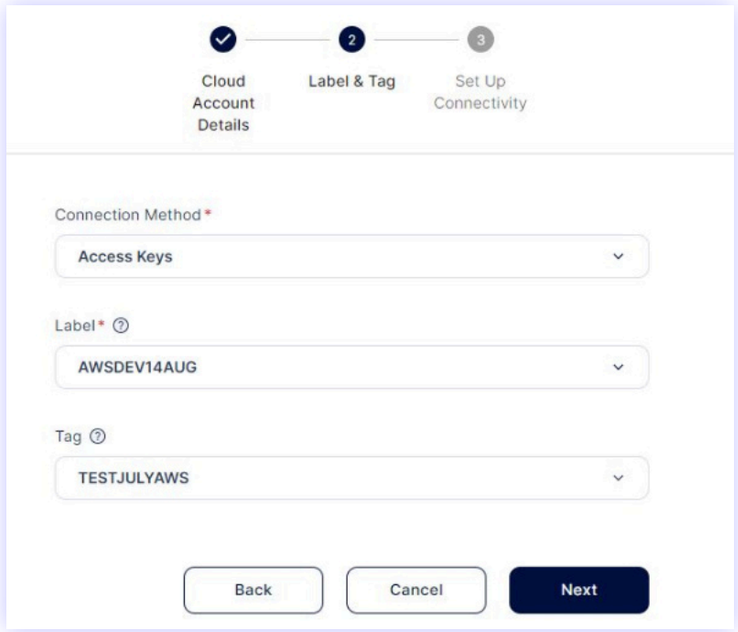


Cloud Account Onboarding

Choose the Cloud provider (AWS | GCP | Azure)

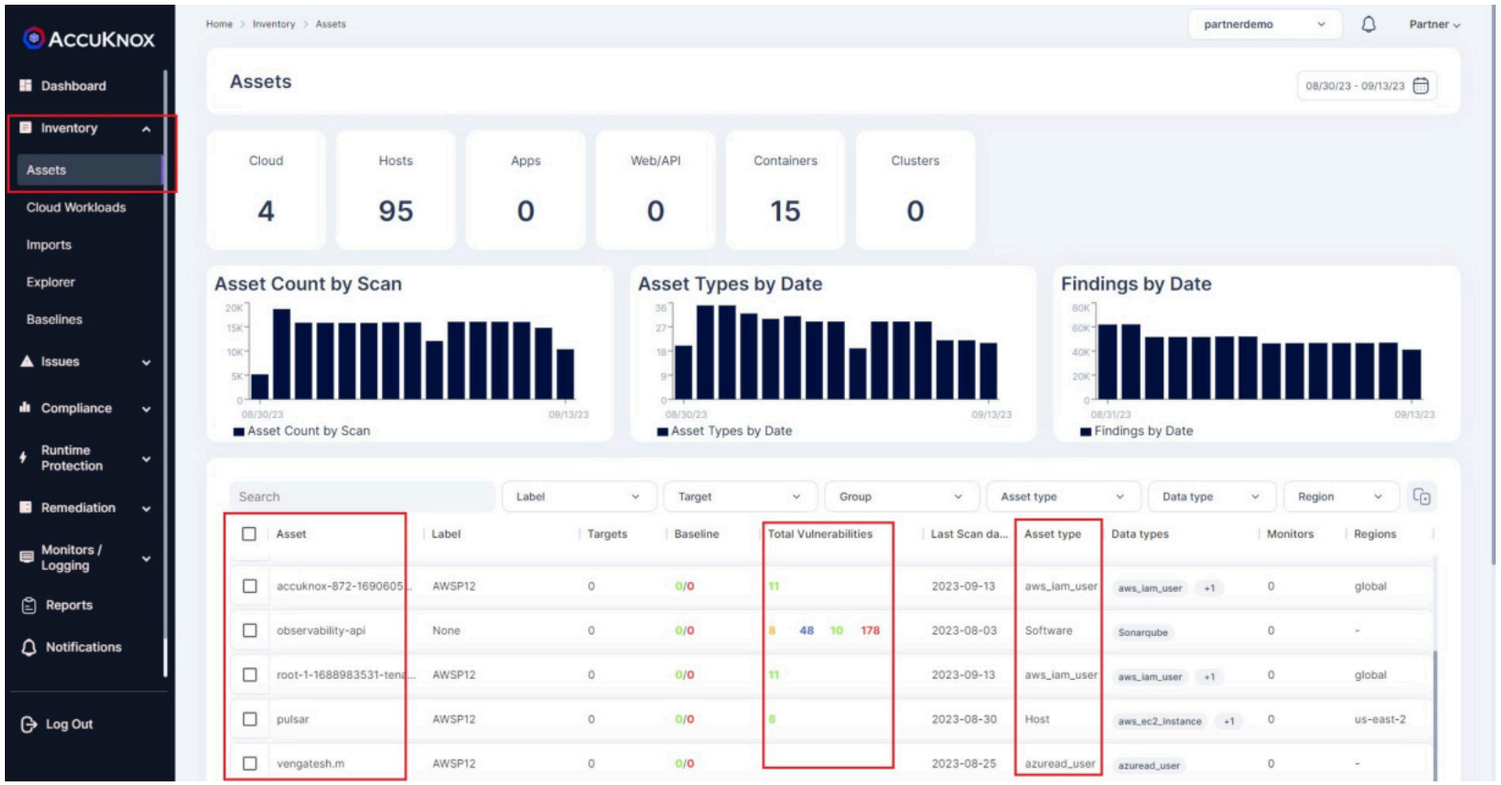
- Select AWS
- Choose connection method -> Access keys
- Select Label and Tag (It will be used to identify the assets)





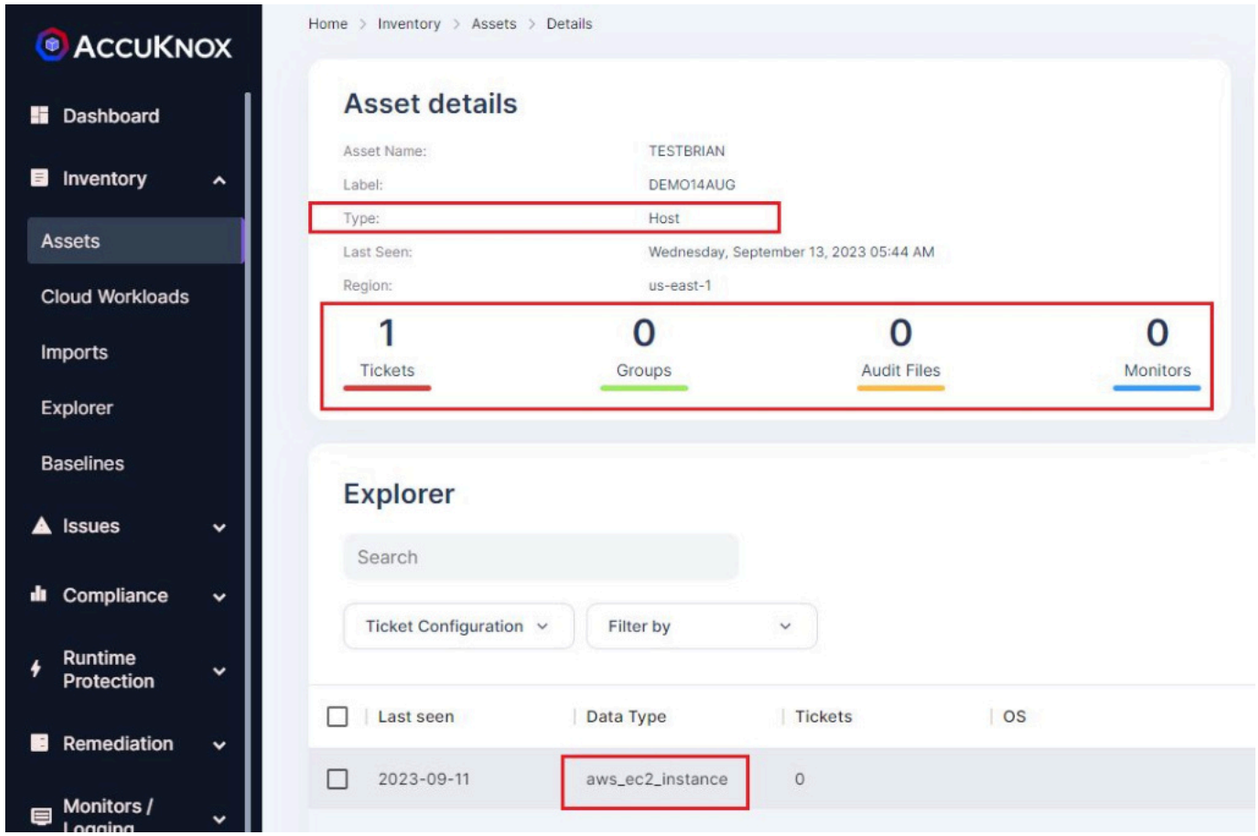
Asset View

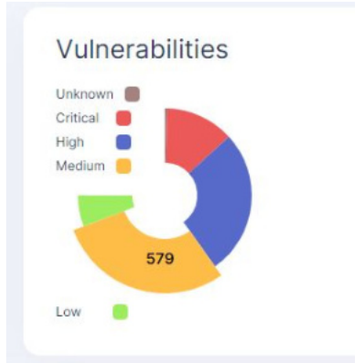
- After Onboarding the cloud account wait for the scan to complete
- Scan is triggered instantly on account onboarding, but the scan completion might take at-least an hour or more. You will get an email after the successful scan executes.
- Once Scan completed, you should be able to see the cloud assets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

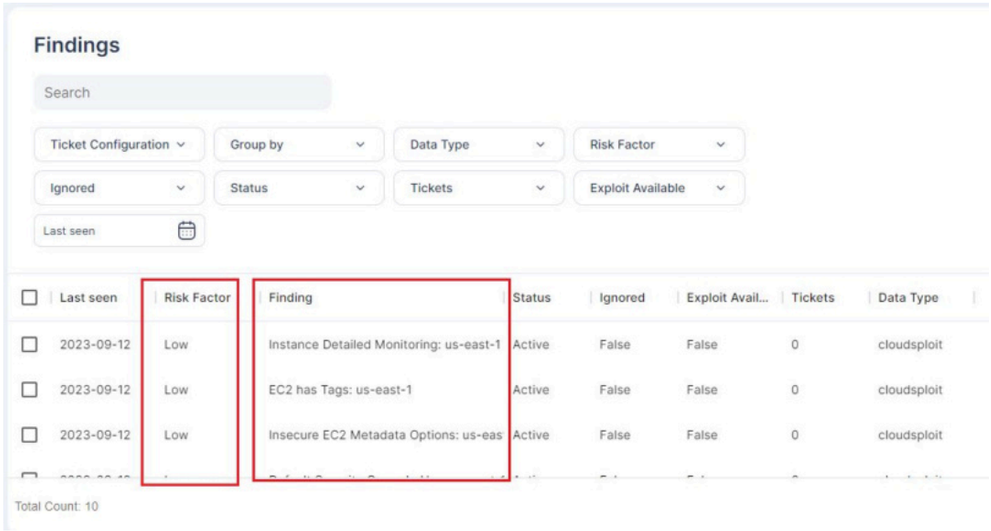


Asset Detail View

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



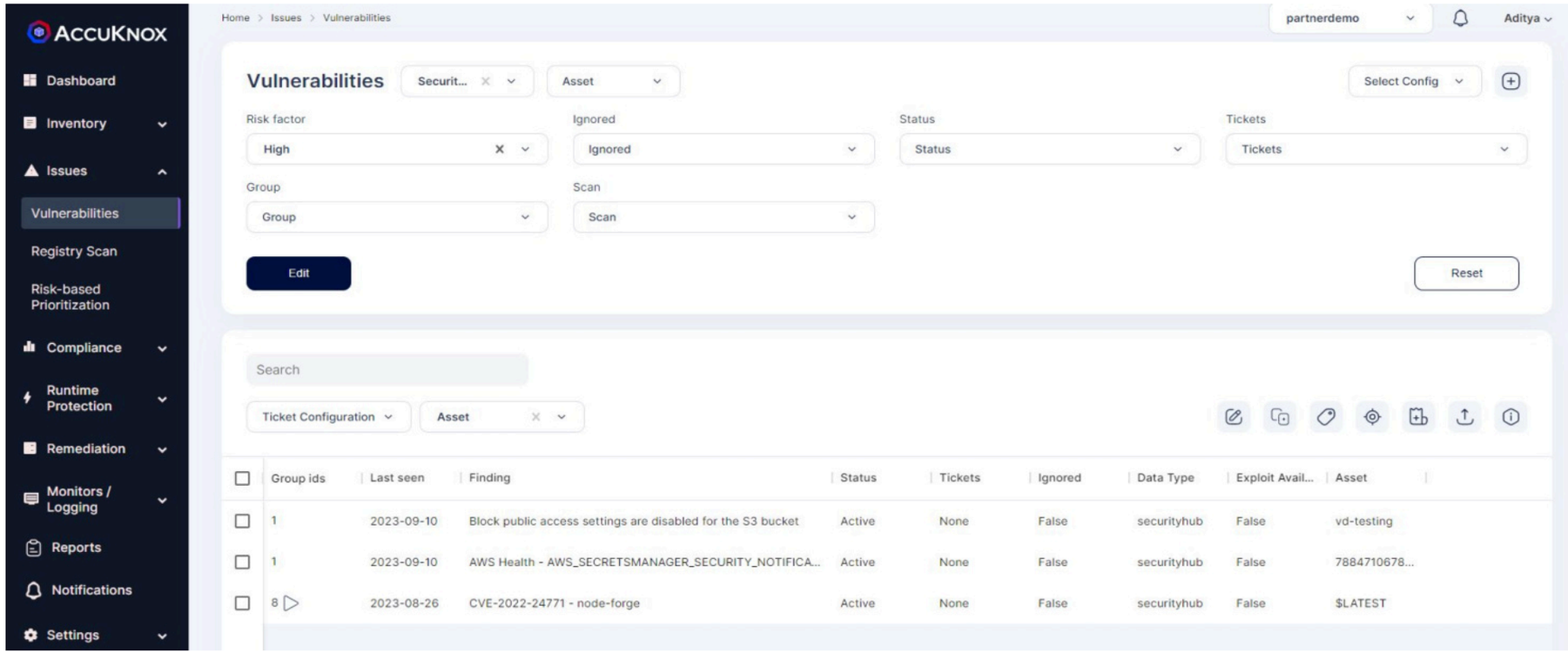




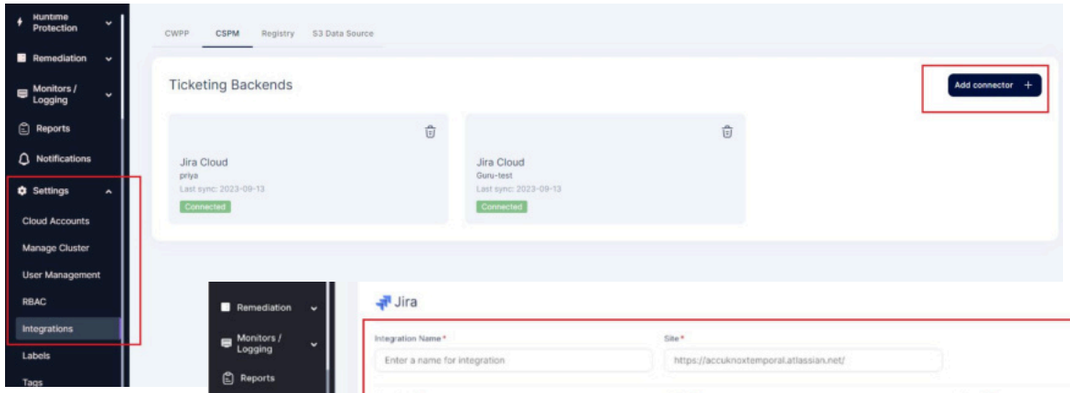
Findings/Misconfigurations

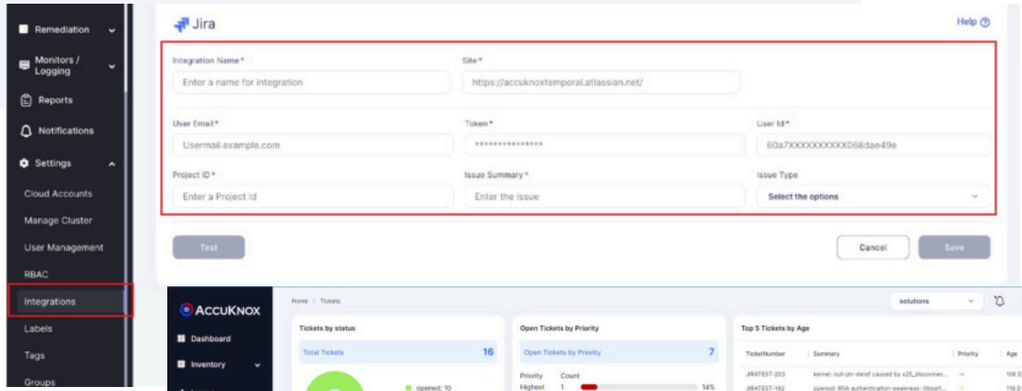
To see the findings and misconfigurations associated with the Onboarded Cloud Account, Please navigate to Issues -> Vulnerabilities

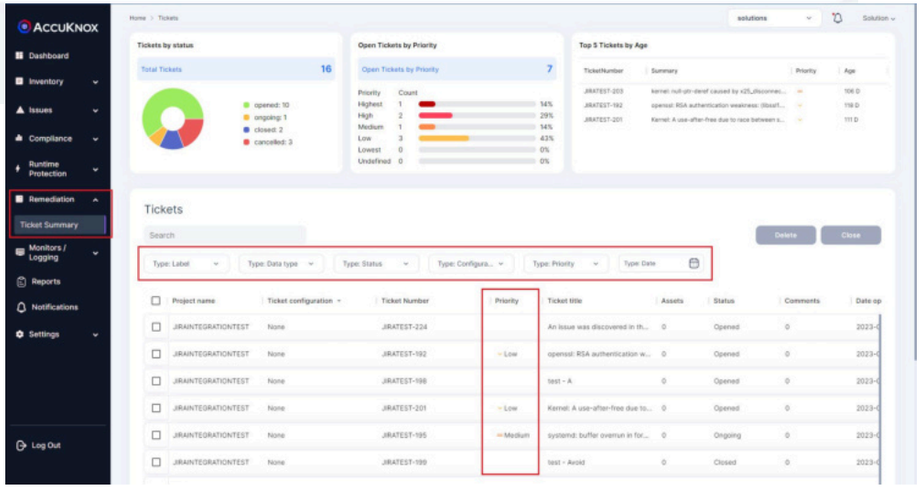
- Apply SecurityHub/Cloudsploit in data-type filter
- You may choose the severity “Critical” or “High, Medium, Low” for the findings



Remediation: Setup Ticketing Integration







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

2.

3. 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.

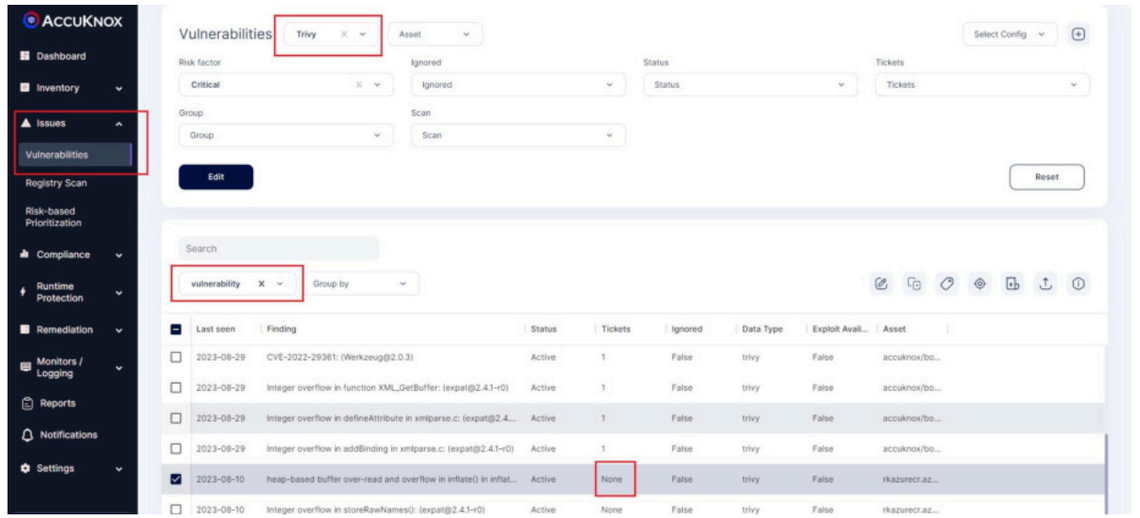
To generate a ticket, select the finding or misconfiguration from either the Inventory Asset Detail or Issues Vulnerabilities.

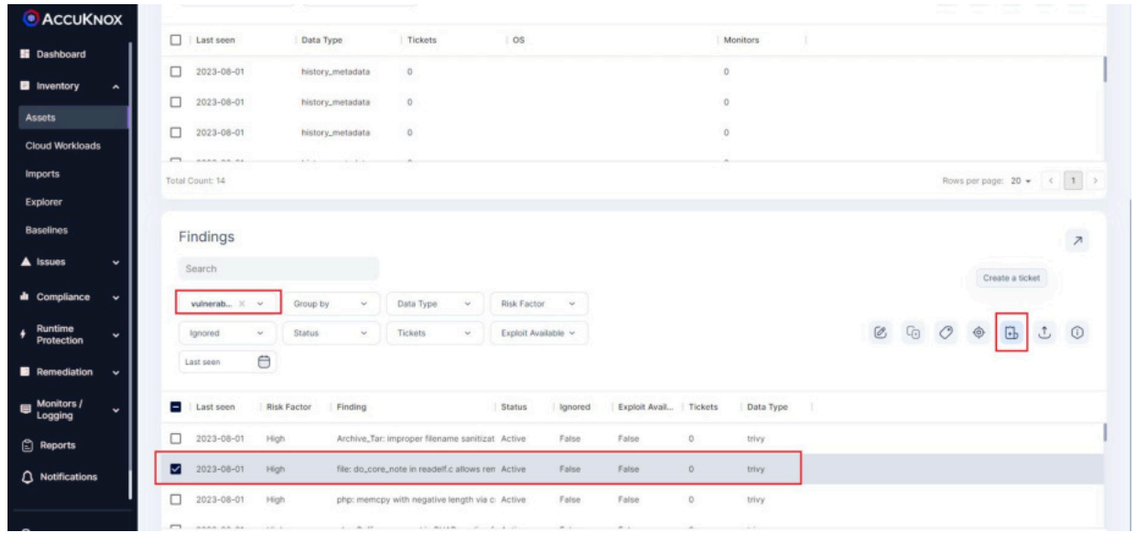
Approach 1: Issues >> Vulnerabilities

- 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

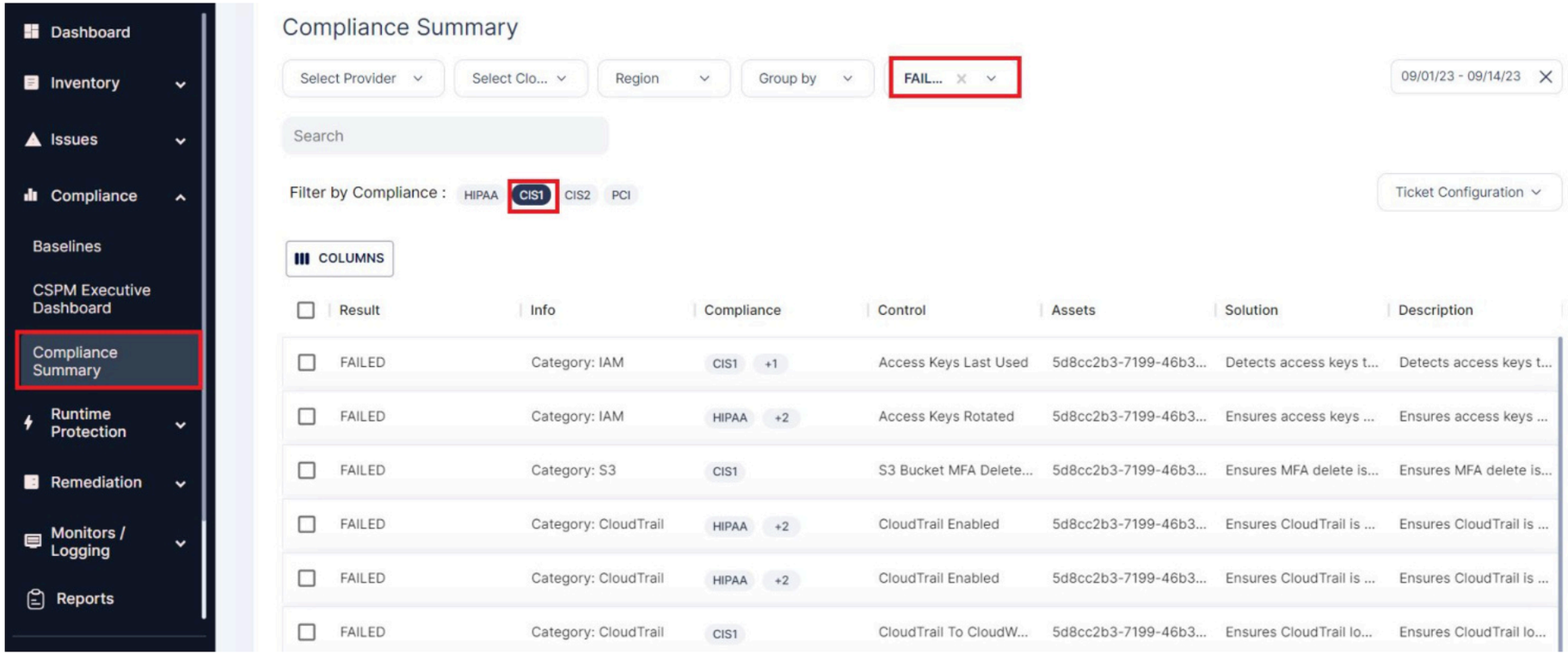




Seeing only Failed Compliance in CIS

To see the compliance summary for the Failed results in CIS

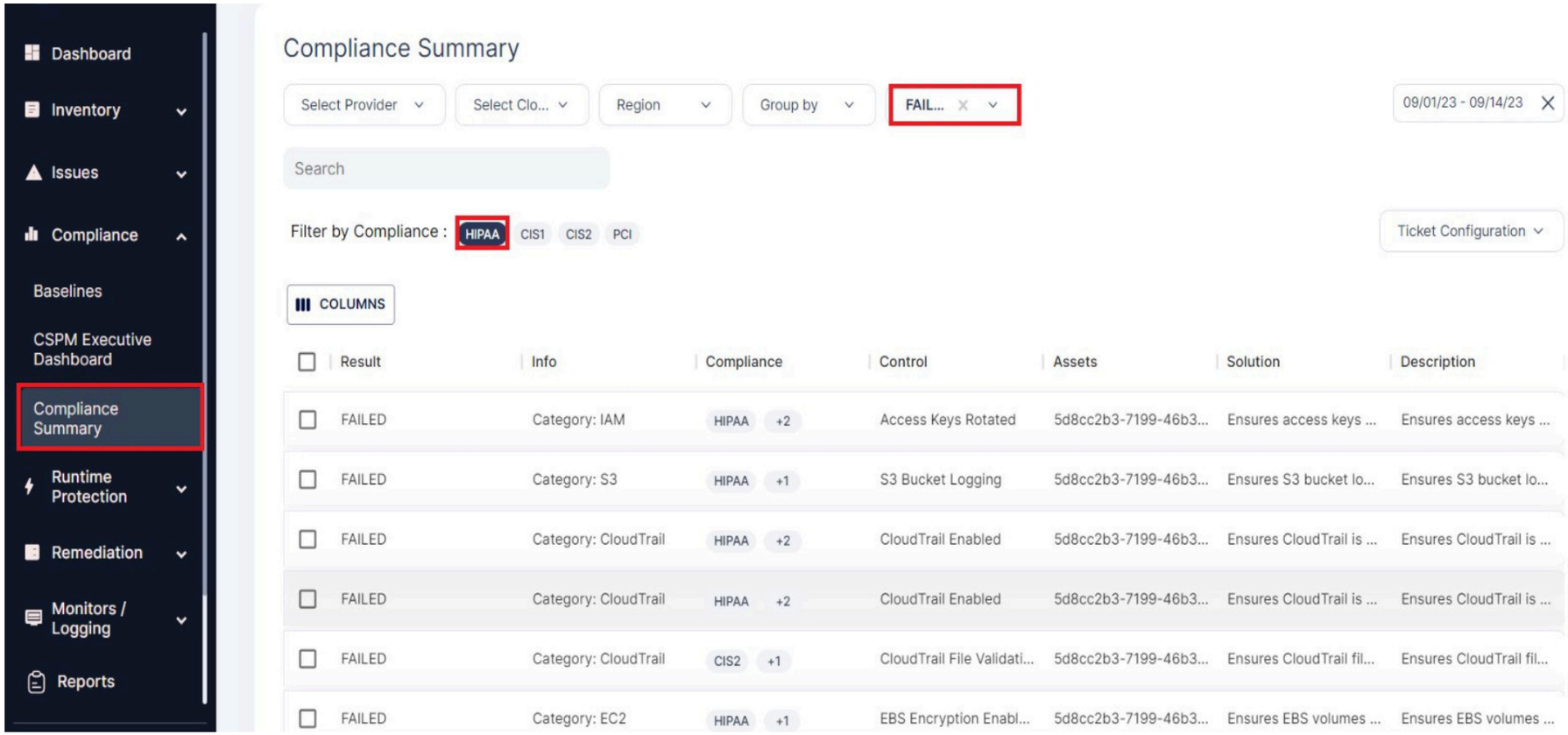
- Click on Compliance Summary
- Select CIS from Filter by Compliance and select Failed from the Result filter.
- You can select filters by Compliance to see specific compliance



Seeing only Failed Compliance in HIPAA

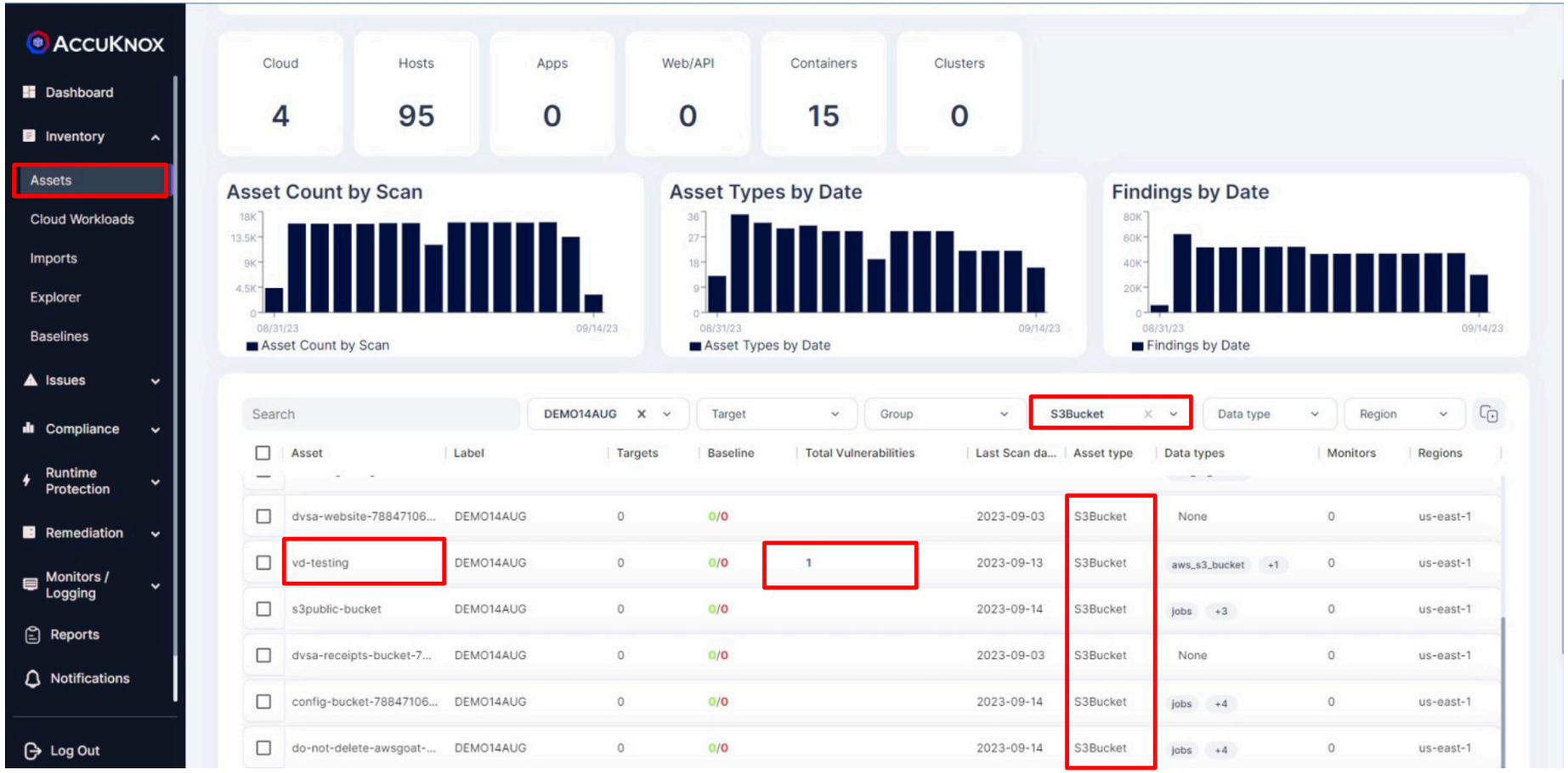
To see the compliance summary for the Failed results in HIPAA

- Click on Compliance Summary
- Select HIPAA from Filter by Compliance and select Failed from the Result filter.



Identify S3 buckets accessible on public networks

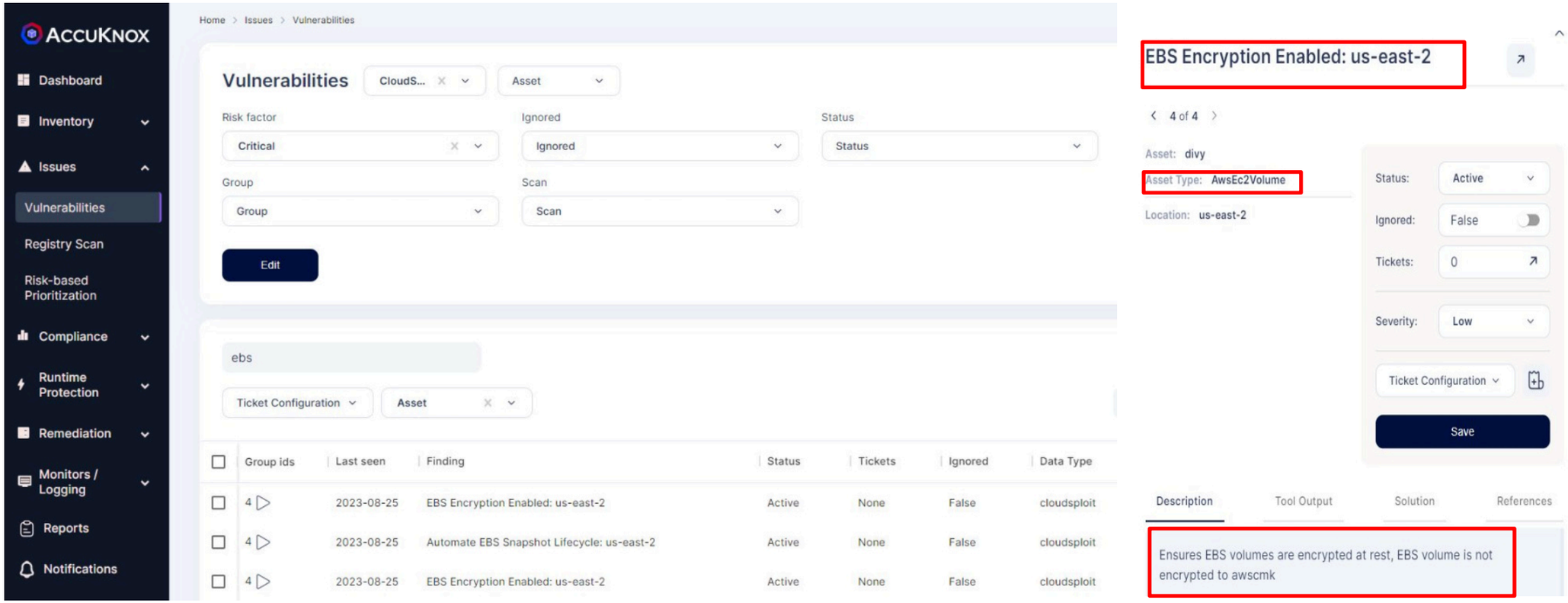
- Go to Inventory >> Assets page and Filter for Asset Type as s3bucket
- Look for S3bucket with count in Total Vulnerabilities



Identify unencrypted EBS Volume

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

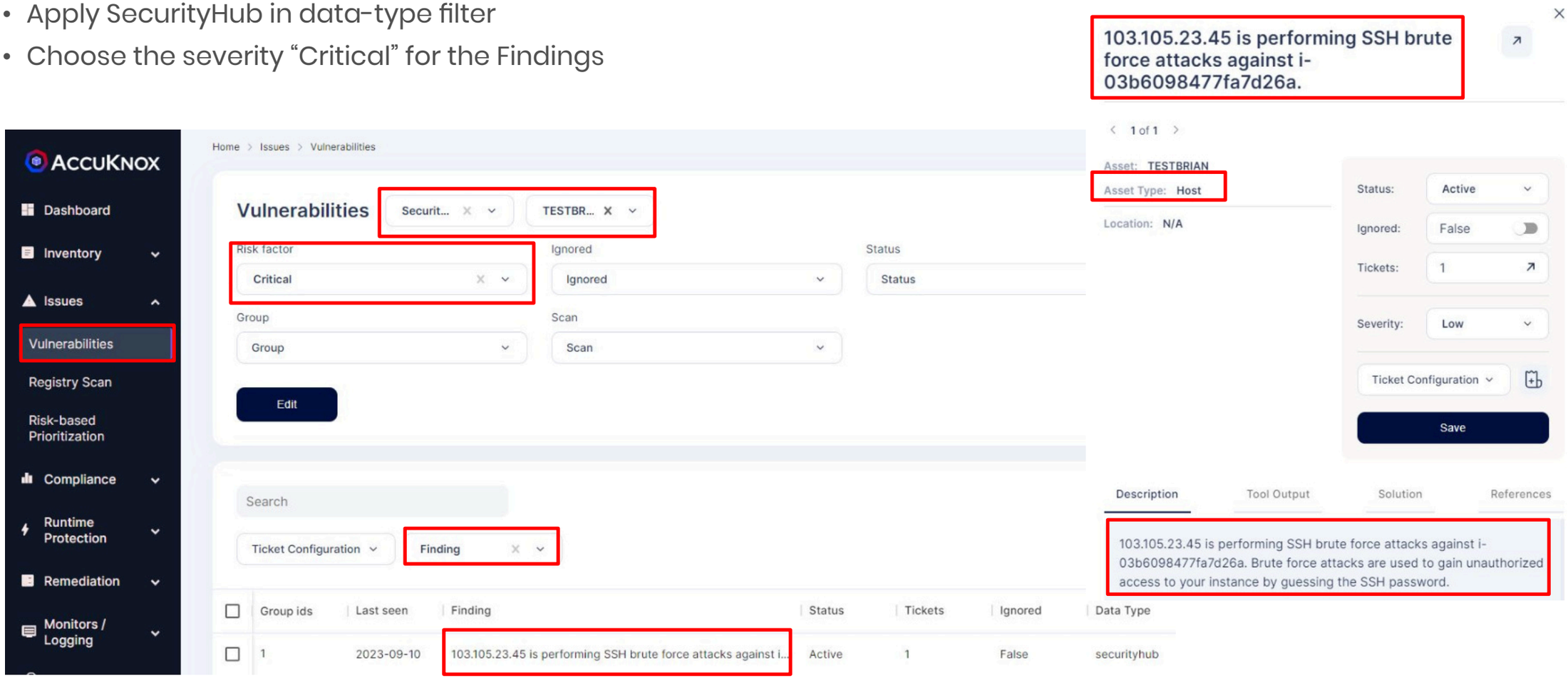
- Apply Cloudsploit in data-type filter
- Choose the severity “Critical” for the Findings Search for “ebs volume” in the search field



Identify Hosts with Critical Findings

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

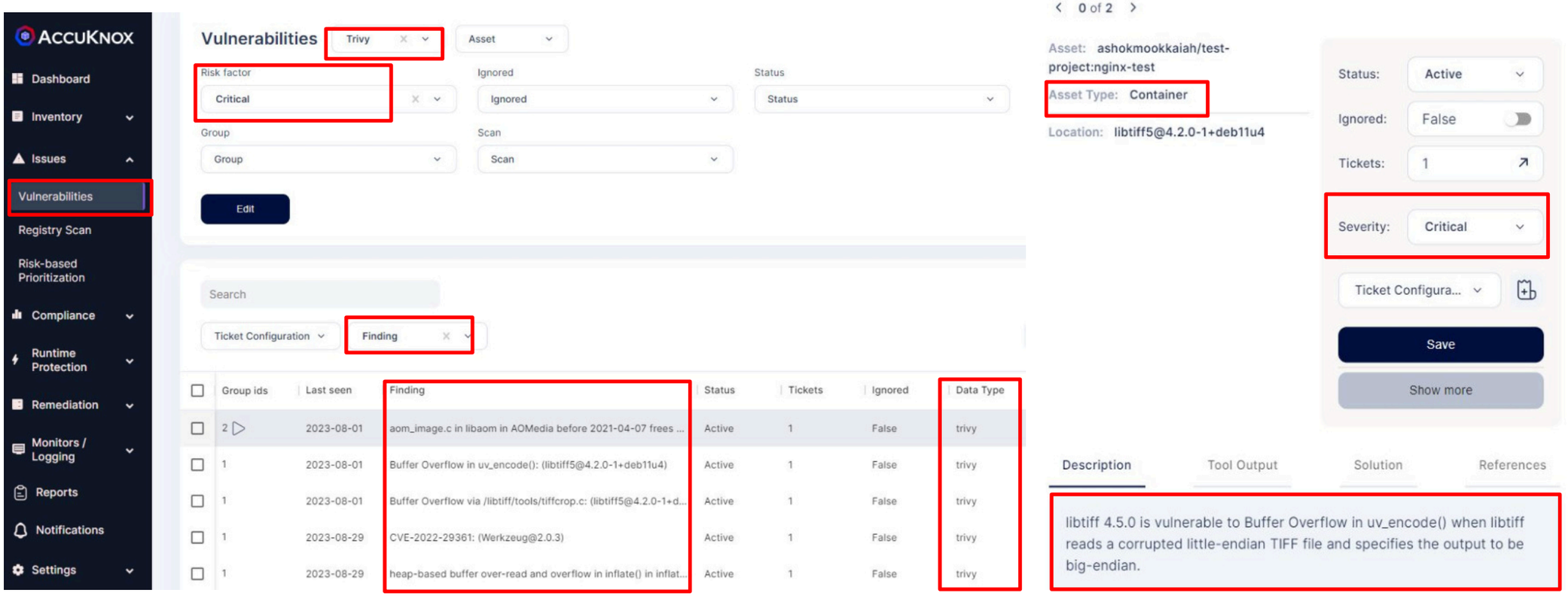
- Apply SecurityHub in data-type filter
- Choose the severity “Critical” for the Findings



Identify Container Images with critical vulnerabilities

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

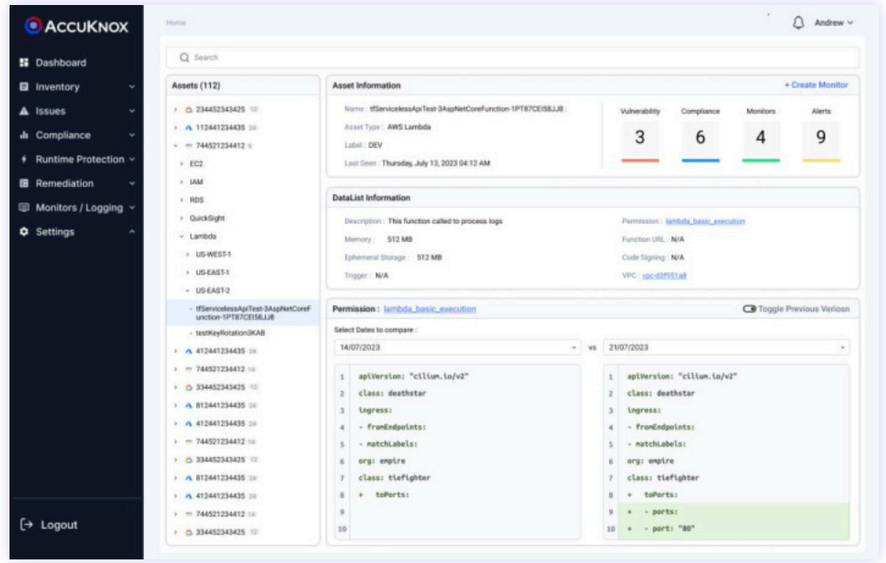
- Apply Trivy in data-type filter
- Choose the severity “Critical” for the Findings

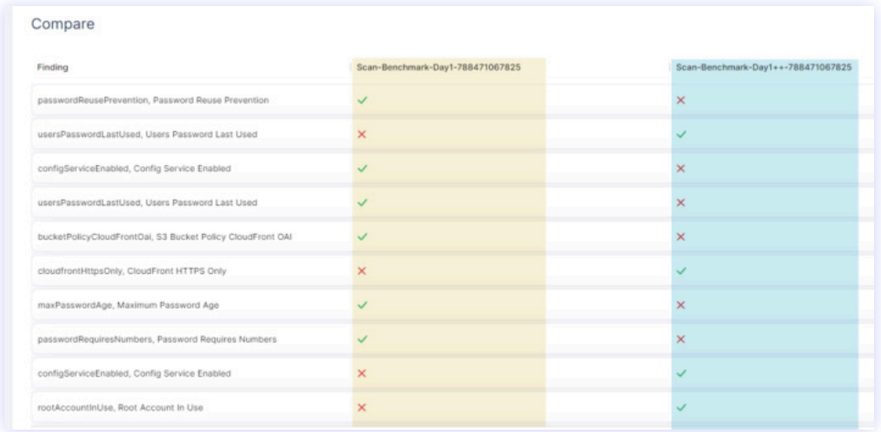


Summary of CSPM Toolkit

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





Focus

CSPM addresses the basic foundational “must have” elements of Cloud Security. Every organization needs to have one.

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 stateof-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

IBM

LF EDGE

AccuKnox joins mimik Technologies, IBM as Open Horizon project partner

Optimized for Intel® Smart Edge

Zero Trust Cloud Native Application Protection

ACCUKNOX intel

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 KubeArmorTM, 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)

KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)

5G OPEN INNOVATION LAB

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 500+ downloads. AccuKnox, Zero Trust Enterprise CNAPP is anchored on KubeArmor and is an integrated Cloud Native Security platform that includes:

SPM/KSPM (Cloud/Kubernetes Security Po
WPP (Cloud Workload Protection Platform
IEM/KIEM (Cloud/Kubernetes Identity and

aws

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

vmware troduction

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
LinkedIn

Phil Porras
Co-founder, Innovations
LinkedIn

Rahul Jadhav
Co-founder, VP of Engg
LinkedIn

Brian Burgess
Product
LinkedIn

Raj Panchapakesan
Global Head- Business Development& Partner Ecosystem
LinkedIn

Jen Wilson
Director, Operations& Customer Success
LinkedIn

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 →