ACCUKNOX

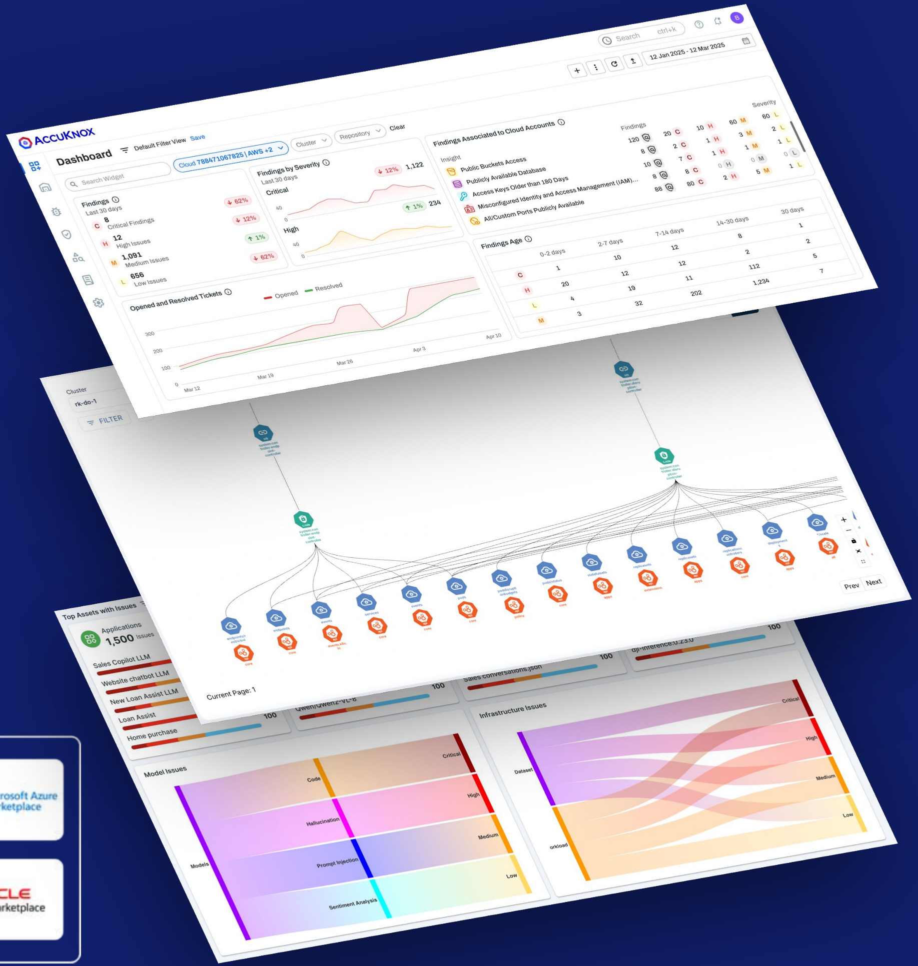
Secure Code to Cognition™

AI-Powered
Zero Trust CNAPP

DevSecOps Engineers Love Our CNAPP

G ★★★★★ Rated 4.5/5

G2 ★★★★★ Rated 4.3/5



Certified & Accredited by

NVIDIA INCEPTION PROGRAM

aws PARTNER Containers Software

NETAPP EXCELLERATOR

OPEN HORIZON

NASSCOM Emerge 50 Awards

NUTANIX

As Featured in

Gartner

IBM Cloud

ORACLE

aws

LF EDGE

NEPHIO

Available on

aws marketplace

Microsoft Azure Marketplace

Red Hat Marketplace

ORACLE Cloud Marketplace

Outline

1. What Problems do we solve?
2. Customer Wins
3. Product Offerings
4. Platformization - Integrated Security
5. Support Matrix
6. Unique Differentiation
7. Architecture & Deployment Models
8. POC Timelines

What problem do we solve?

ACCUKNOX

PROBLEM

Advanced attacks in Public and Private Clouds are hard to detect and even harder to prevent

SOLUTION

We deliver Zero Trust Security for Public and Private Cloud

AGENTLESS SECURITY

AND

Delivers Zero Trust Security for:

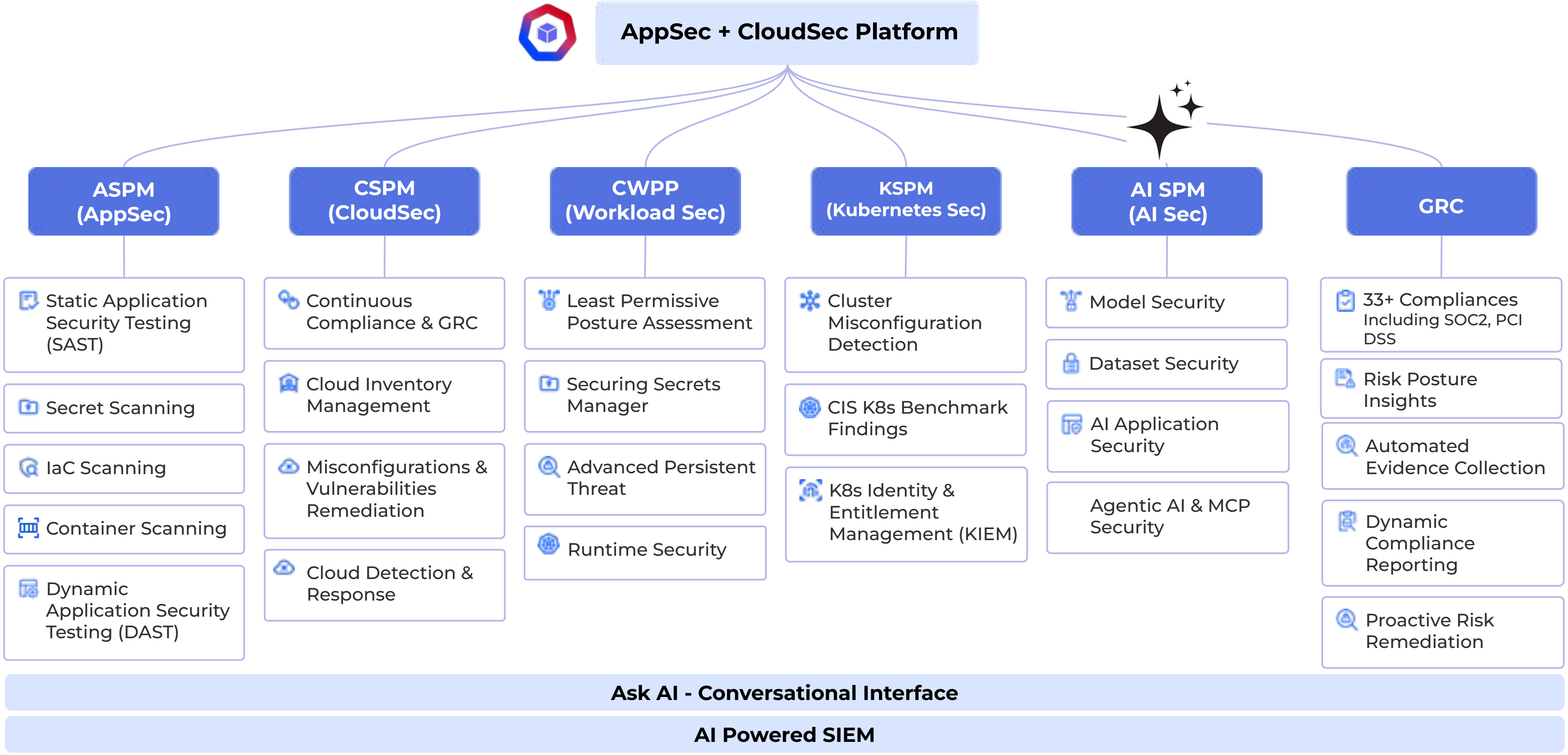
- All Public Clouds aws Azure Google Cloud ORACLE CLOUD
- All Private Clouds Red Hat OpenShift openstack. RANCHER BY SUSE NUTANIX. VMware Tanzu
- Managed Kubernetes Distros Amazon EKS Azure Kubernetes Service (AKS) Google Kubernetes Engine
- Modern Workloads (kubernetes { api } LLM LARGE LANGUAGE MODEL) and Legacy Workloads ( )

Furthermore..

- Inline Security as opposed to Post-attack Mitigation
- We deliver integrations with 50+ Enterprise Platforms (EDR, SIEM, SOAR, Ticketing/Notification, CI/CD, Supply Chain)
- We deliver 30+ Compliance Reports and Continuous Compliance

Platformization

ACCUKNOX



AppSec + CloudSec Platform

ASPM (AppSec)
- Static Application Security Testing (SAST)
- Secret Scanning
- IaC Scanning
- Container Scanning
- Dynamic Application Security Testing (DAST)

CSPM (CloudSec)
- Continuous Compliance & GRC
- Cloud Inventory Management
- Misconfigurations & Vulnerabilities Remediation
- Cloud Detection & Response

CWPP (Workload Sec)
- Least Permissive Posture Assessment
- Securing Secrets Manager
- Advanced Persistent Threat
- Runtime Security

KSPM (Kubernetes Sec)
- Cluster Misconfiguration Detection
- CIS K8s Benchmark Findings
- K8s Identity & Entitlement Management (KIEM)

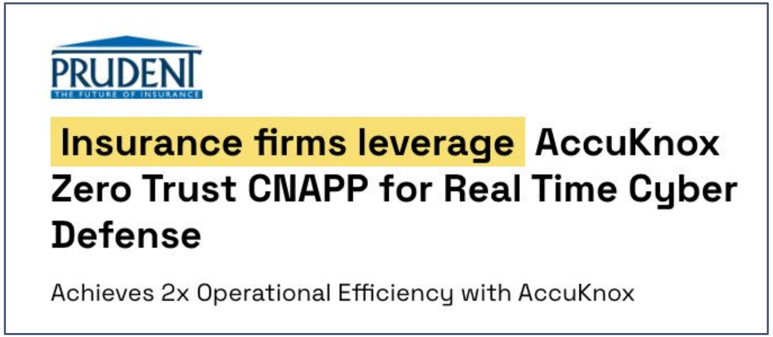
AI SPM (AI Sec)
- Model Security
- Dataset Security
- AI Application Security
- Agentic AI & MCP Security

GRC
- 33+ Compliances Including SOC2, PCI DSS
- Risk Posture Insights
- Automated Evidence Collection
- Dynamic Compliance Reporting
- Proactive Risk Remediation

Ask AI - Conversational Interface

AI Powered SIEM

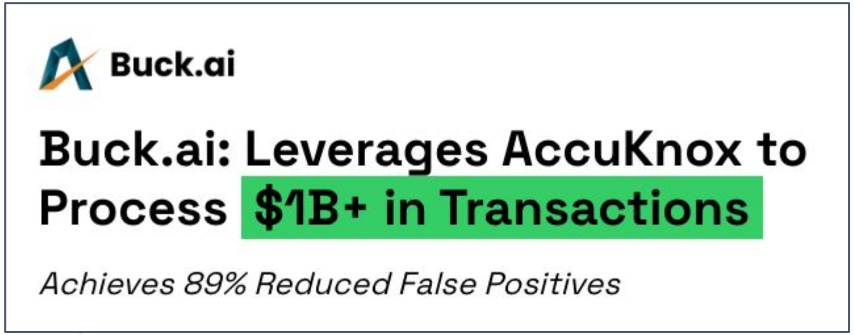
Customer Wins | Case Studies



PRUDENT
THE FUTURE OF INSURANCE

Insurance firms leverage AccuKnox Zero Trust CNAPP for Real Time Cyber Defense

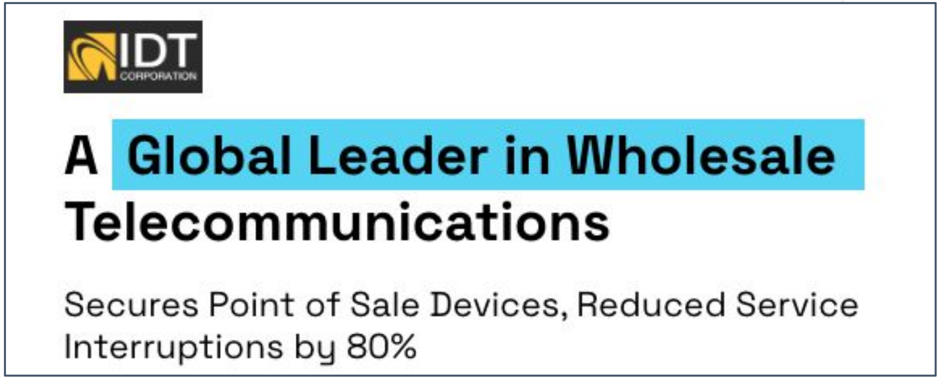
Achieves 2x Operational Efficiency with AccuKnox



Buck.ai

Buck.ai: Leverages AccuKnox to Process $1B+ in Transactions

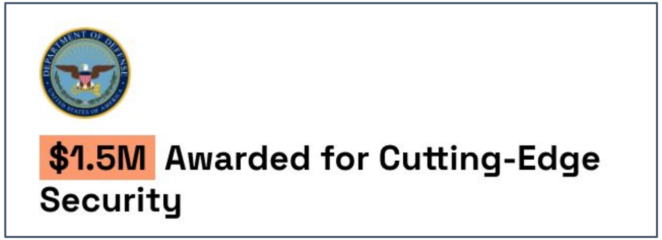
Achieves 89% Reduced False Positives



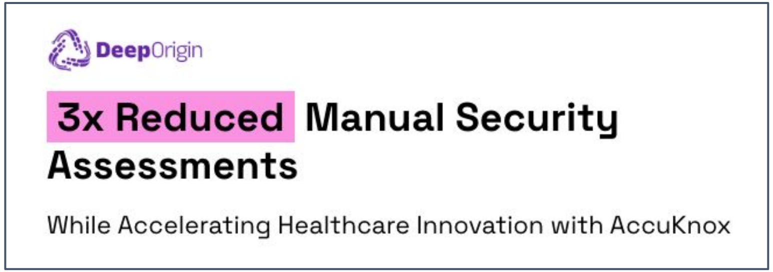
IDT
CORPORATION

A Global Leader in Wholesale Telecommunications

Secures Point of Sale Devices, Reduced Service Interruptions by 80%



$1.5M Awarded for Cutting-Edge Security



DeepOrigin

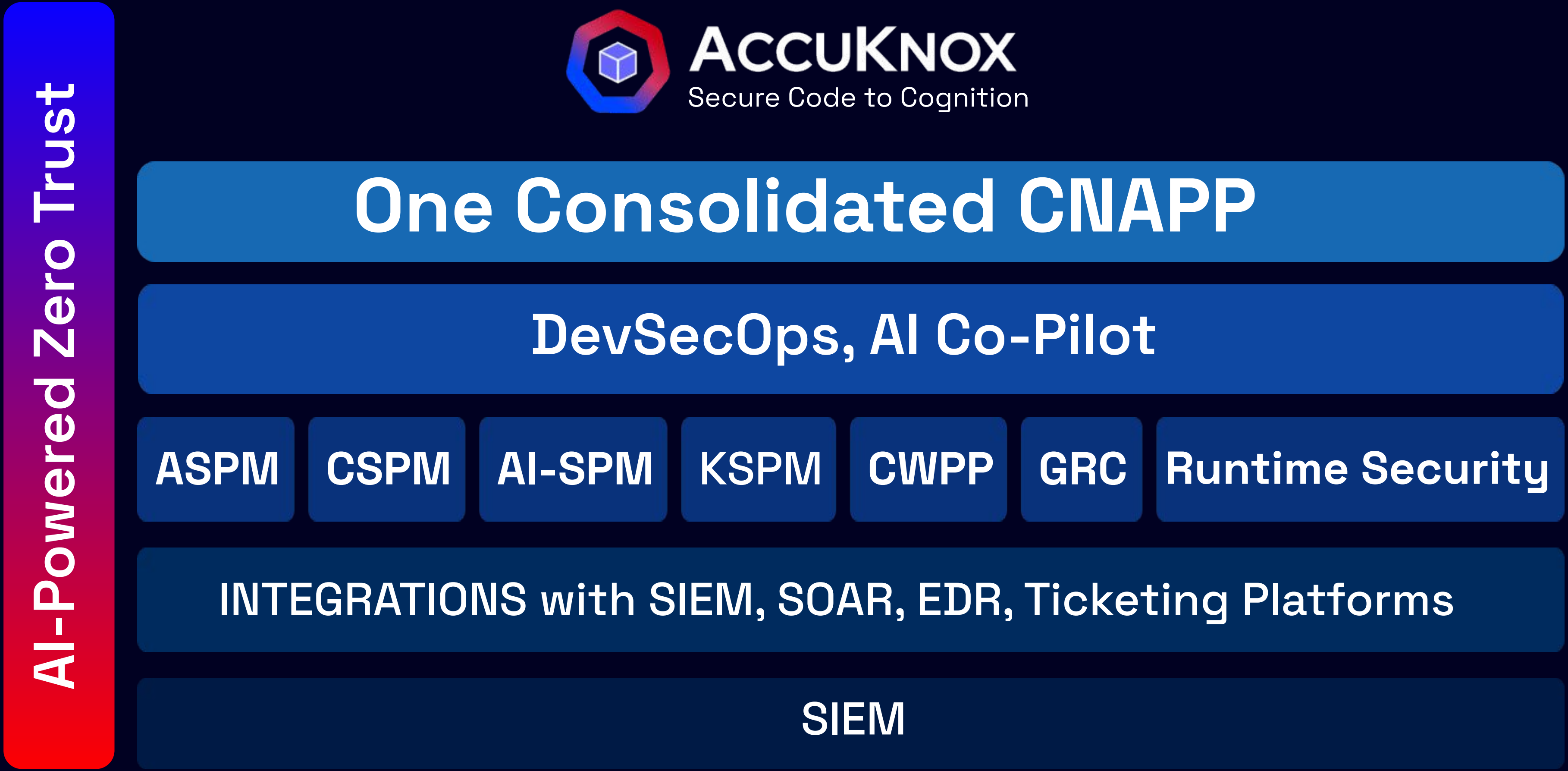
3x Reduced Manual Security Assessments

While Accelerating Healthcare Innovation with AccuKnox

Refer - accuknox.com/case-studies

ACCUKNOX

Secure Code to Cognition



AI-Powered Zero Trust

One Consolidated CNAPP

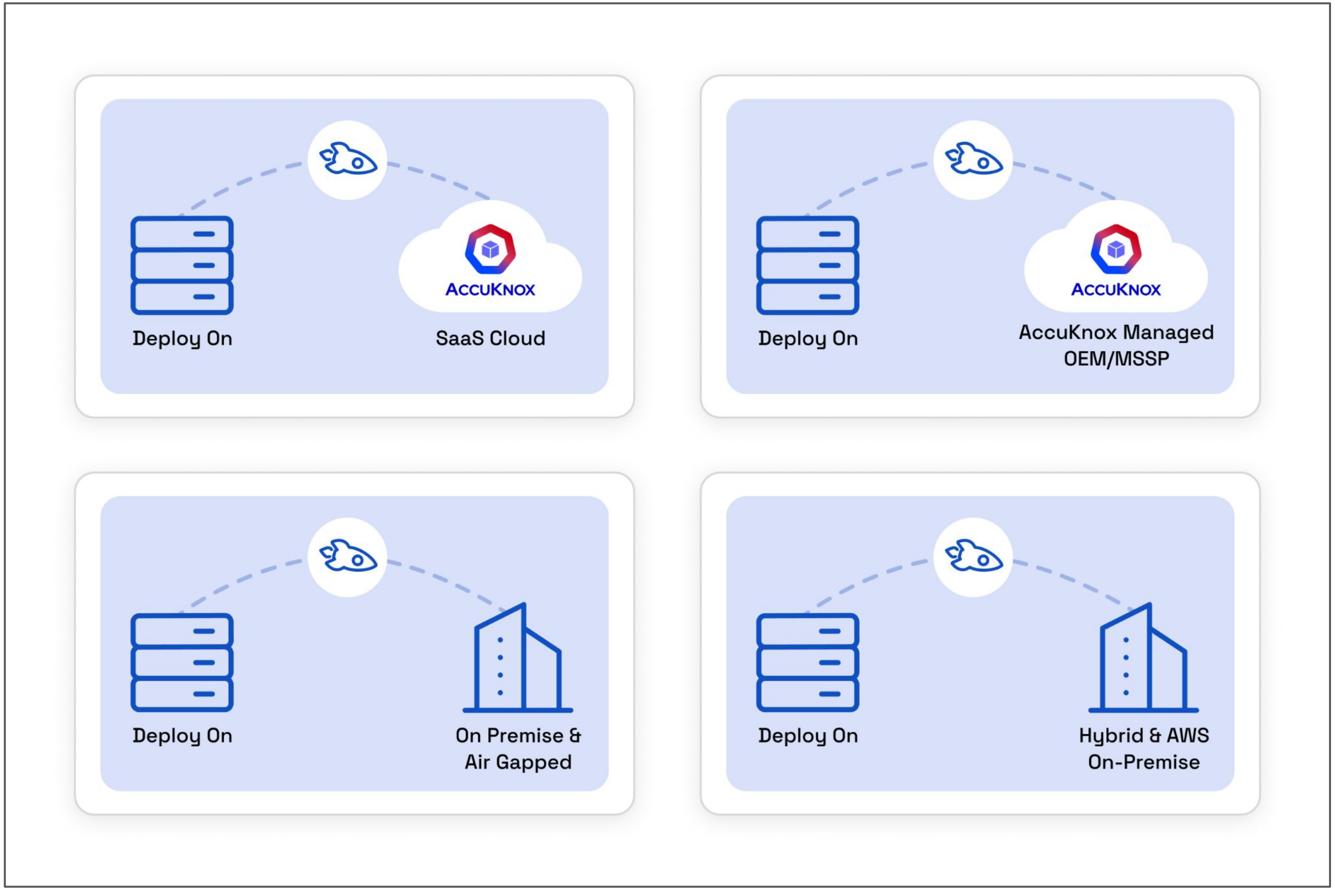
DevSecOps, AI Co-Pilot

ASPM | CSPM | AI-SPM | KSPM | CWPP | GRC | Runtime Security

INTEGRATIONS with SIEM, SOAR, EDR, Ticketing Platforms

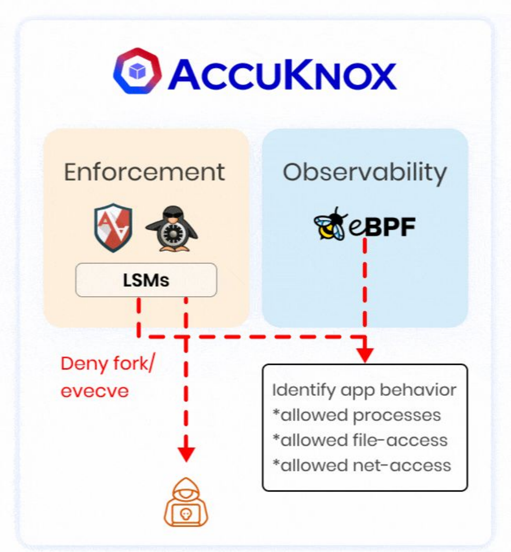
SIEM

Flexible Deployment Models



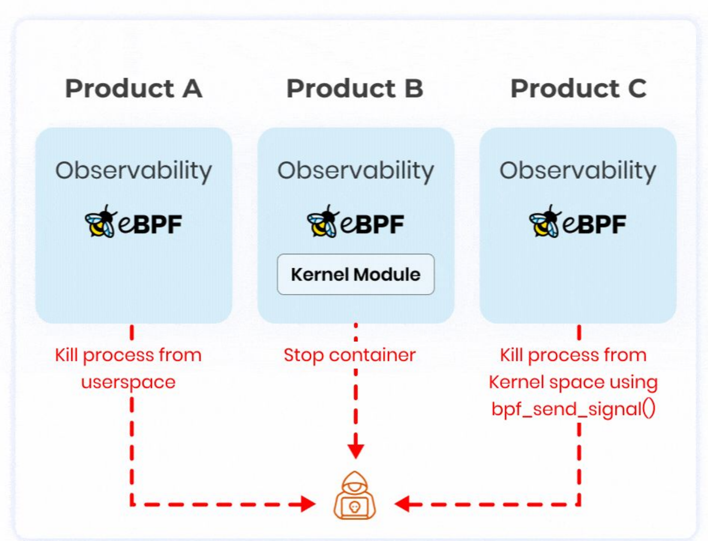
Unique Differentiation

AccuKnox can “ Observe ” >>
“Enforce ” during Attack time >> Automatically Generate “ Policies” >



Inline Mitigation

(vs)



Post Attack Mitigation

***We defend against real time**
Zero Day Attacks !

Support Matrix

1) Clouds

- Azure
- DigitalOcean
- aws
- IBM Cloud
- ORACLE CLOUD
- Red Hat
- Google Cloud
- Alibaba Cloud

2) Clusters (On-Prem, VMs)

- SUSE
- debian
- CentOS
- archlinux
- Raspberry Pi
- Rocky Linux™
- ORACLE
- Amazon EKS
- Amazon Linux
- IBM Cloud Kubernetes Service
- Bottlerocket
- Azure Kubernetes Service (AKS)
- RANCHER BY SUSE
- On-prem
- RED HAT OPENSHIFT Container Platform
- Google Kubernetes Engine
- fedora
- Oracle Kubernetes Engine
- Red Hat Enterprise Linux

**Linux based Operating Systems*

3) Container Registries

- Amazon ECR
- Azure Container Registry
- QUAY
- docker hub
- DOCKERHUB
- docker REGISTRY
- Google Cloud Artifact Registry
- Google Container Registry
- HARBOR
- JFrog Artifactory
- OPENSHIFT
- sonatype nexus repository

ACCUKNOX

Unique Differentiation

ACCUKNOX

- → **One Platform** - comprehensive coverage from *Code → Cloud*
- → **Automatic Zero Trust Policies** - for inline remediation
- → **Flexible Deployment** - Public and Private Cloud
- → **SOAR platform** - with 50+ integrations out of the box

Cloud

CSPM Executive Dashboard

Misconfiguration Detection

Inventory Assessment

Continuous Compliance

Baseline for Drift Detection

Code

Static Code Analysis

Software Composition Analysis

Secret Scanning

CI/CD Integration to Build cycle

Vulnerability Management

Image

Image Risk Assessment

Vulnerability Scanning

Risk Based Prioritization

Compliance & Reporting

CI/CD Integration

Vulnerability Management

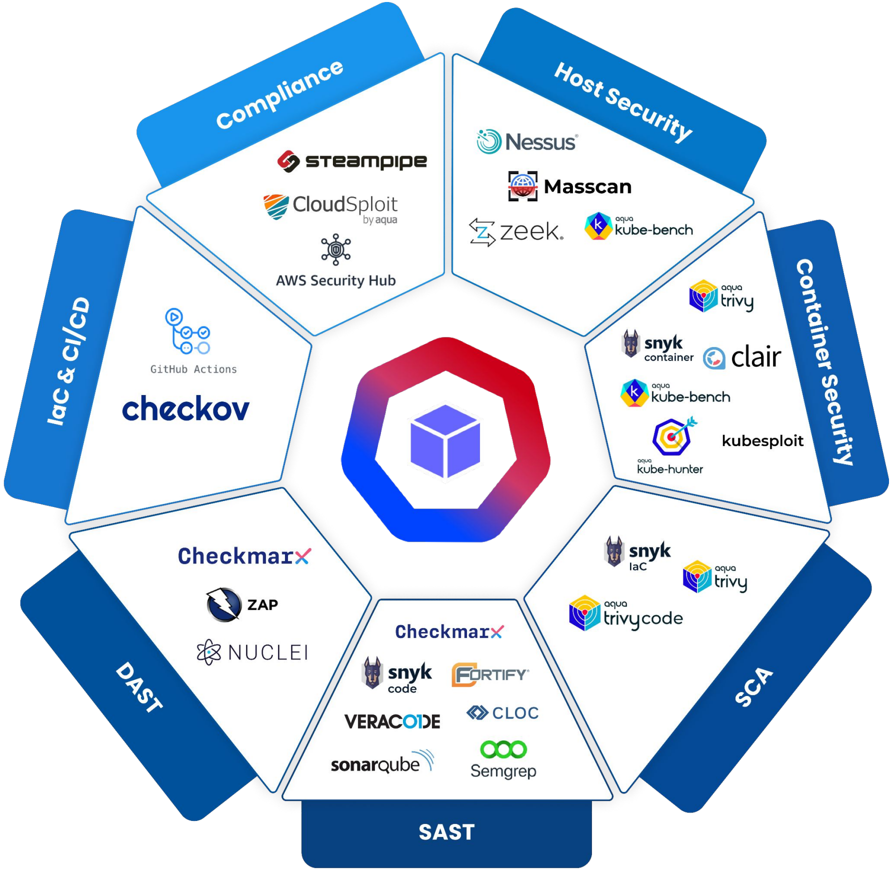
Security Area	Feature
Observability	Workload Observability
Compliance	Workload hardening Policies
Monitoring	Logs and Alerts
Zero Trust	Auto Discovered Zero Trust Policy Custom Zero Trust Policy Inline Remediation Network Microsegmentation
New features	Admission Controller Support KIEM (K8s Identities & Entitlements Management) ECS/EKS Fargate Support

Tools Supported Out of the box!

ACCUKNOX

Shift Left and Secure Right

1. Host security
2. Container security
3. Compliance
4. IaC & CI/CD Scanning
5. SAST
6. DAST
7. SCA



DevSecOps with AccuKnox

SAST

- Check app source code or bytecode for insecure constructs.
- Proactive scan, when app is not running, inside access.

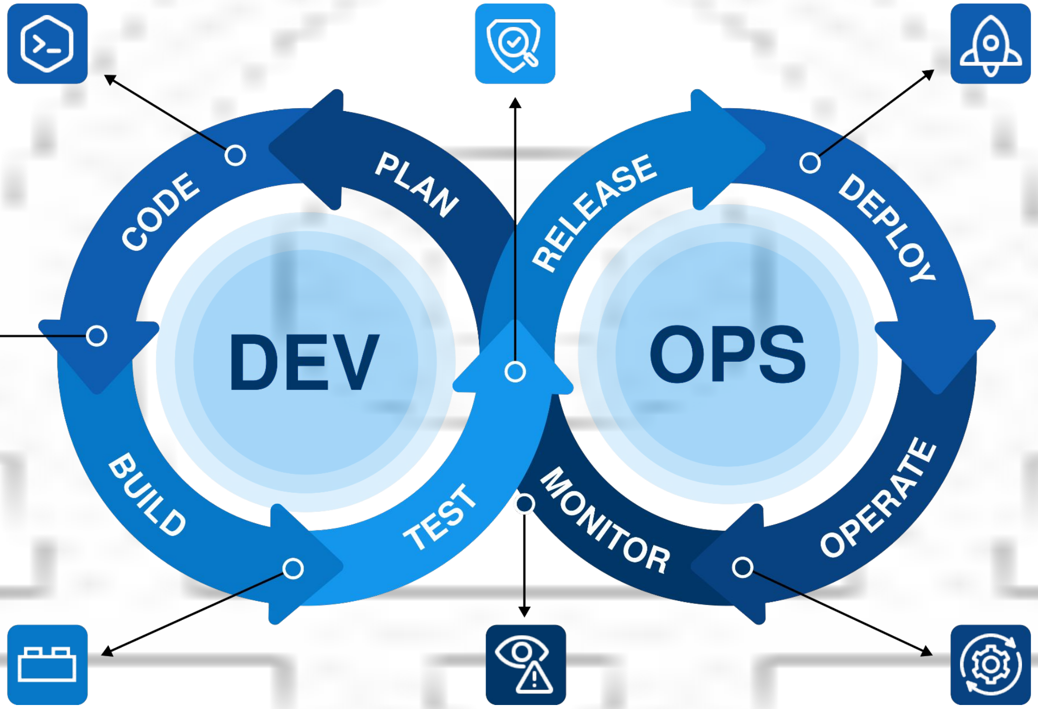
SCA

- Check app source code or bytecode for insecure constructs.
- Proactive scan, when app is not running, inside access.

IaC

- Infrastructure Provisioning (Create, modify & delete IaC)
- Config Management (Express state of Infra using code/APIs) [KICS, Tfsec, Checkov]

Container Vulnerabilities



MONITOR, ALERT, CONTROL, BLOCK, LOG Application

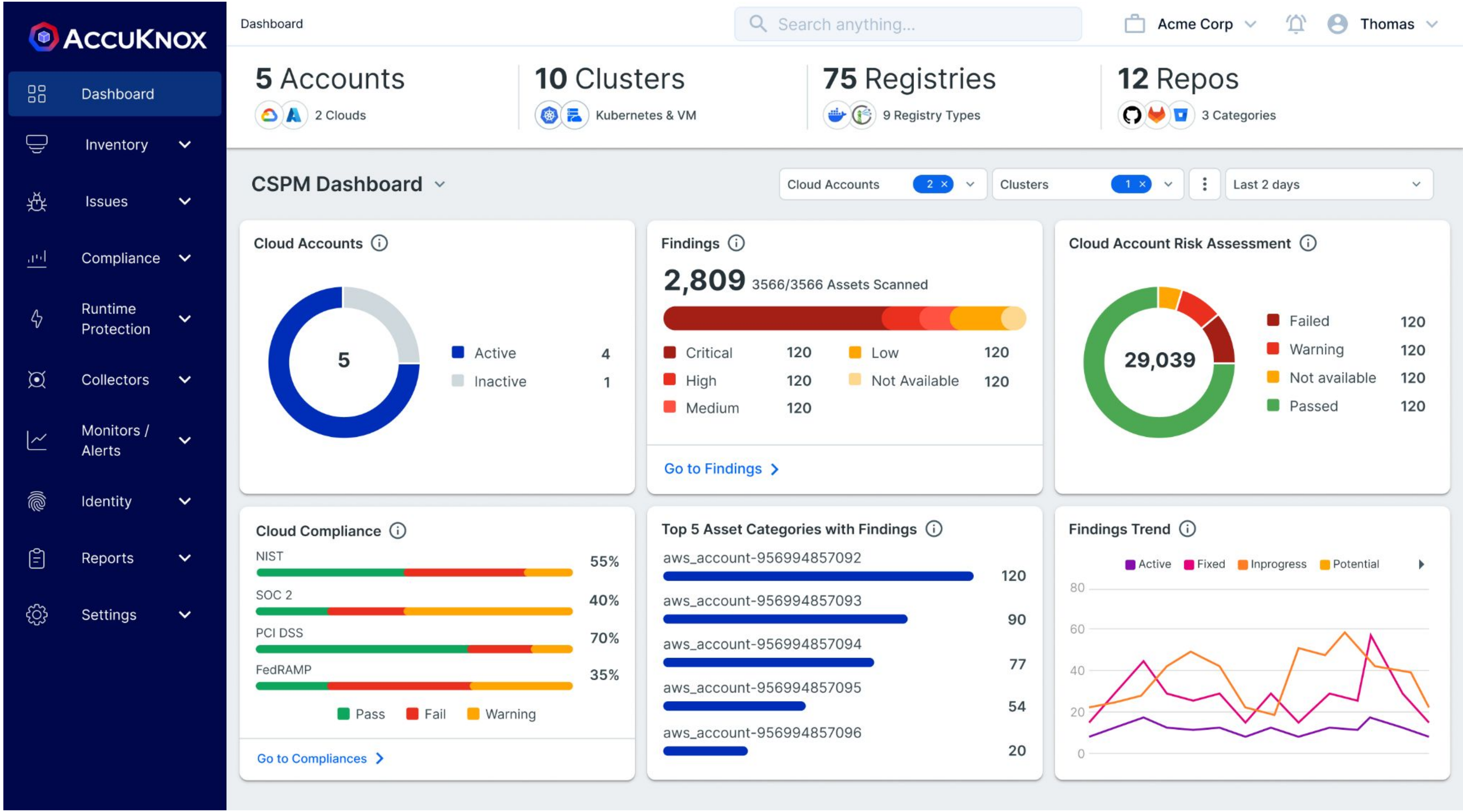
DAST

- Automated & continuous scans which invoke malicious http requests to web-ui & API covering wide range of attacks.
- Proactive scan, when app is running, outside access.

IAST

- They attach to running app passively and run when triggered.
- Reactive scan, when app is running, inside access.

01 DASHBOARD



Dashboard

5 Accounts
2 Clouds

10 Clusters
Kubernetes & VM

75 Registries
9 Registry Types

12 Repos
3 Categories

CSPM Dashboard

Cloud Accounts 2 × | Clusters 1 × | Last 2 days

Cloud Accounts

5

Active	4
Inactive	1

Findings

2,809 3566/3566 Assets Scanned

Critical	120	Low	120
High	120	Not Available	120
Medium	120		

Go to Findings >

Cloud Account Risk Assessment

29,039

Failed	120
Warning	120
Not available	120
Passed	120

Cloud Compliance

NIST	55%
SOC 2	40%
PCI DSS	70%
FedRAMP	35%

Pass Fail Warning

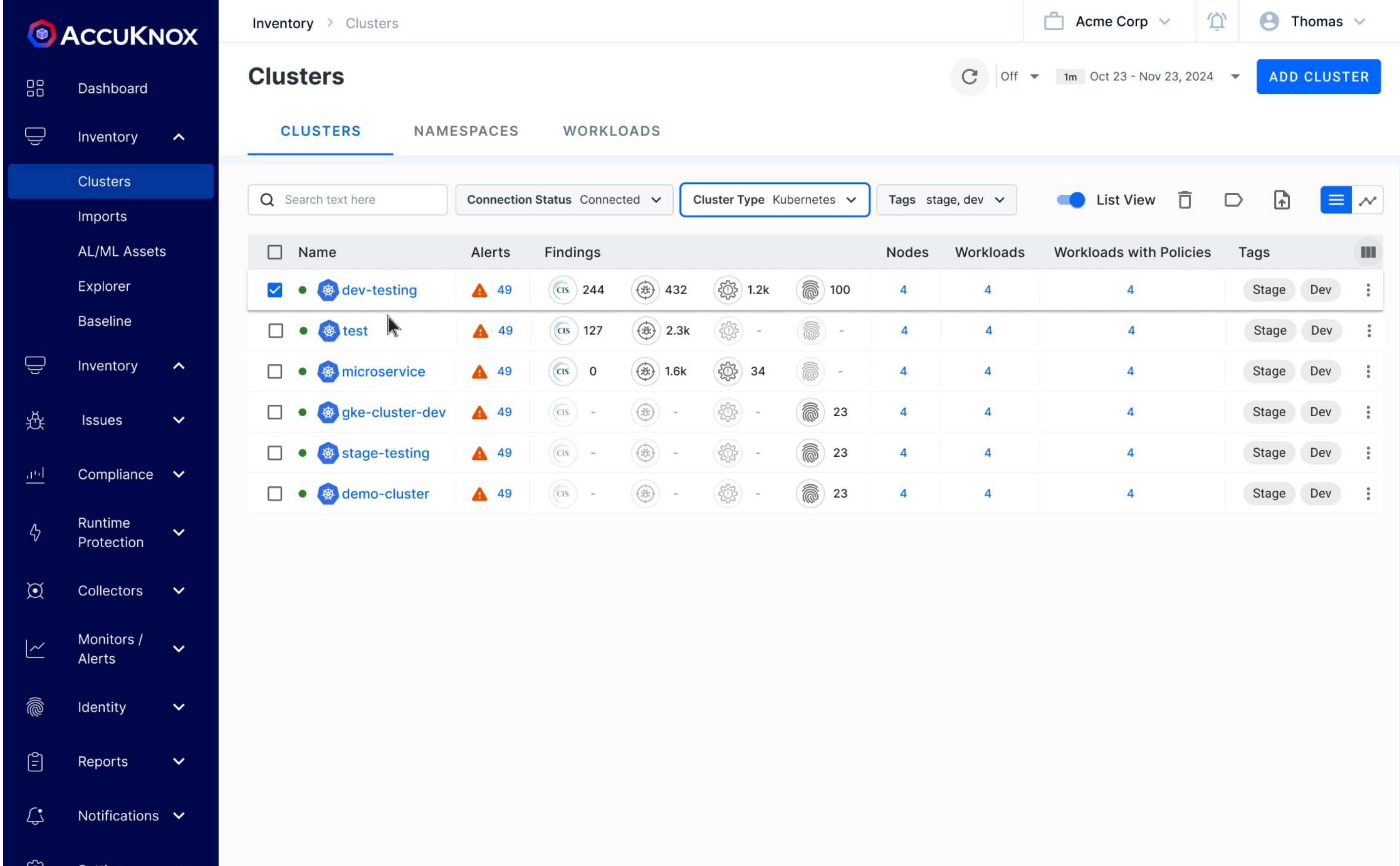
Go to Compliances >

Top 5 Asset Categories with Findings

aws_account-956994857092	120
aws_account-956994857093	90
aws_account-956994857094	77
aws_account-956994857095	54
aws_account-956994857096	20

Findings Trend

02 Clusters



Inventory > Clusters

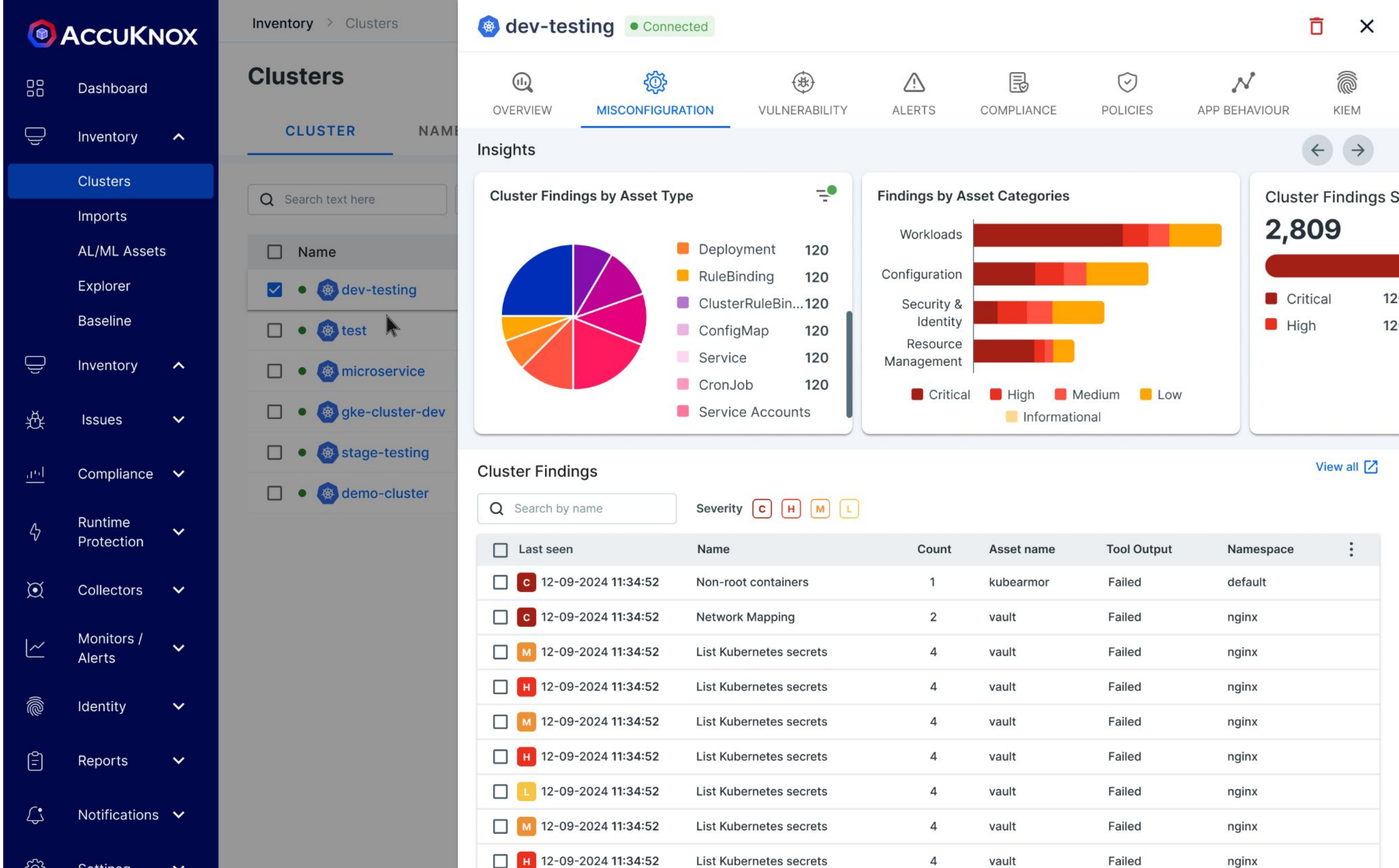
Clusters

Off 1m Oct 23 - Nov 23, 2024

Connection Status Connected | Cluster Type Kubernetes | Tags stage, dev

☐	Name	Alerts	Findings				Nodes	Workloads	Workloads with Policies	Tags
☑	● dev-testing	49	CIS 244	432	1.2k	100	4	4	4	Stage Dev
☐	● test	49	CIS 127	2.3k	-	-	4	4	4	Stage Dev
☐	● microservice	49	CIS 0	1.6k	34	-	4	4	4	Stage Dev
☐	● gke-cluster-dev	49	CIS -	-	-	23	4	4	4	Stage Dev
☐	● stage-testing	49	CIS -	-	-	23	4	4	4	Stage Dev
☐	● demo-cluster	49	CIS -	-	-	23	4	4	4	Stage Dev

02 Clusters



Cluster Findings by Asset Type

🟧 Deployment	120
🟧 RoleBinding	120
🟪 ClusterRoleBin...	120
ConfigMap	120
Service	120
CronJob	120
Service Accounts	

Findings by Asset Categories

Cluster Findings S

2,809

🟥 Critical	12
🟥 High	12

Cluster Findings

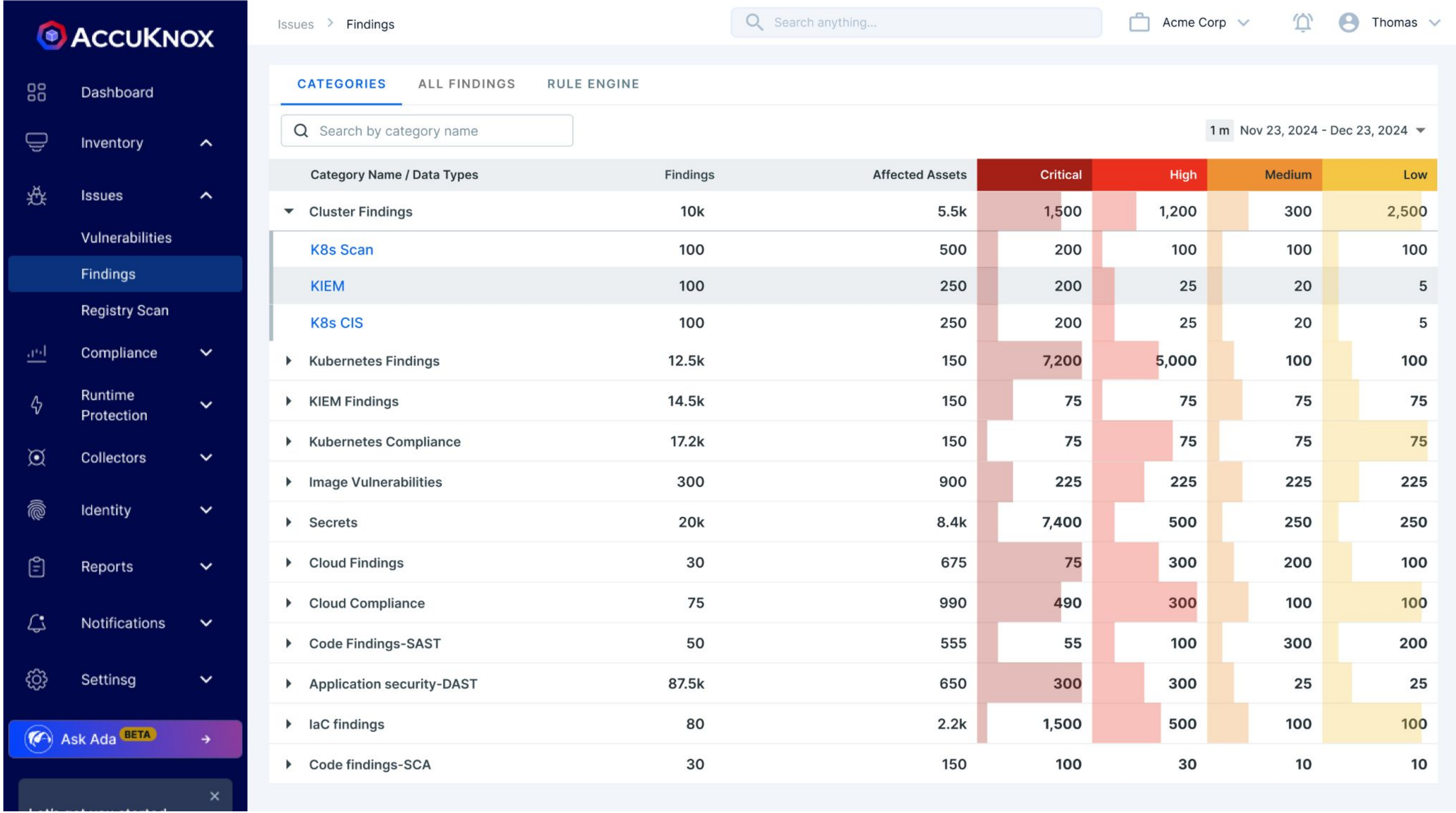
View all

Search by name

Severity C H M L

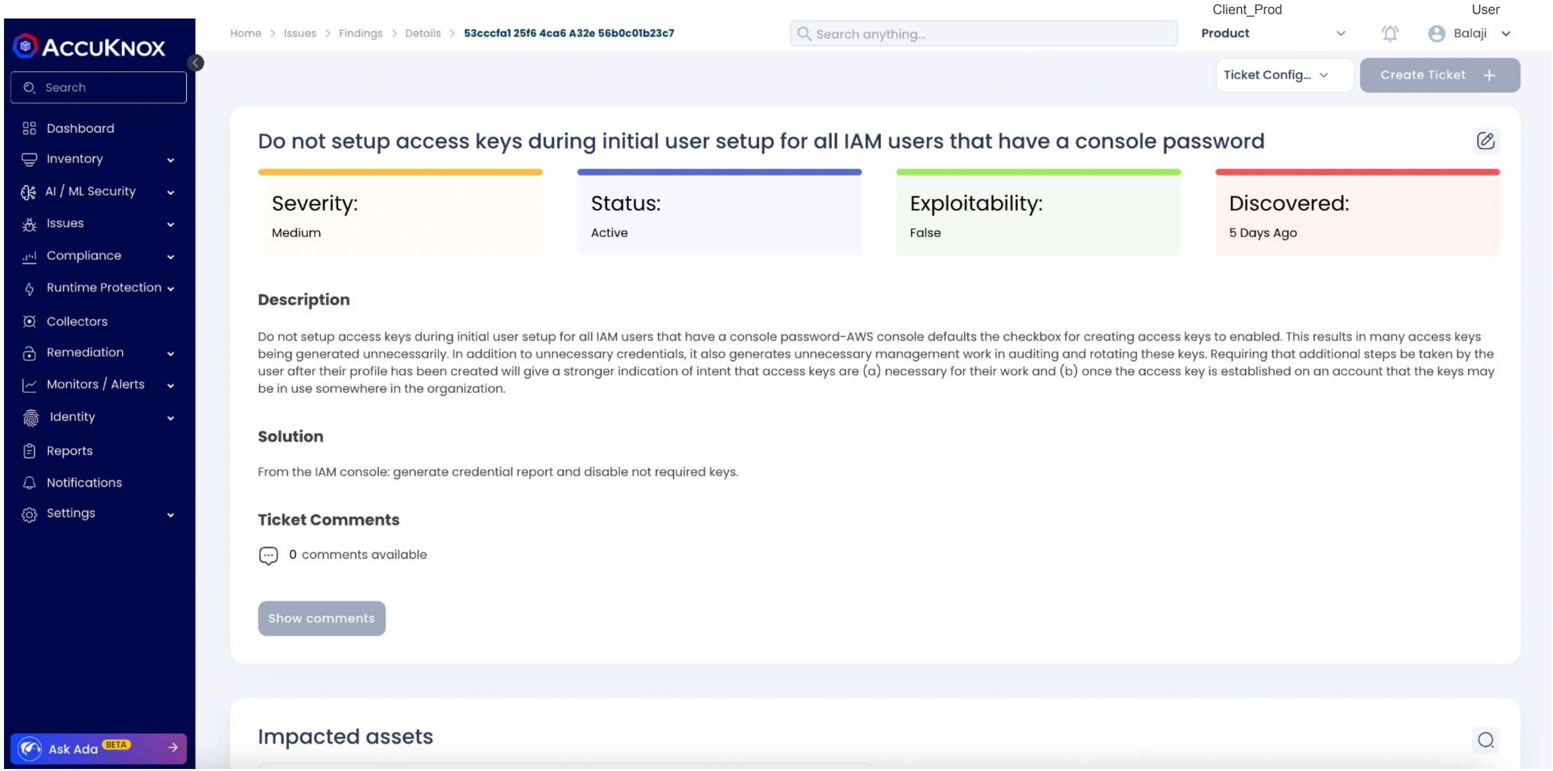
□	Last seen	Name	Count	Asset name	Tool Output	Namespace
□	C 12-09-2024 11:34:52	Non-root containers	1	kubearmor	Failed	default
□	C 12-09-2024 11:34:52	Network Mapping	2	vault	Failed	nginx
□	M 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	H 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	M 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	H 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	L 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	M 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx
□	H 12-09-2024 11:34:52	List Kubernetes secrets	4	vault	Failed	nginx

03 Findings



Category Name / Data Types	Findings	Affected Assets	Critical	High	Medium	Low
Cluster Findings	10k	5.5k	1,500	1,200	300	2,500
K8s Scan	100	500	200	100	100	100
KIEM	100	250	200	25	20	5
K8s CIS	100	250	200	25	20	5
Kubernetes Findings	12.5k	150	7,200	5,000	100	100
KIEM Findings	14.5k	150	75	75	75	75
Kubernetes Compliance	17.2k	150	75	75	75	75
Image Vulnerabilities	300	900	225	225	225	225
Secrets	20k	8.4k	7,400	500	250	250
Cloud Findings	30	675	75	300	200	100
Cloud Compliance	75	990	490	300	100	100
Code Findings-SAST	50	555	55	100	300	200
Application security-DAST	87.5k	650	300	300	25	25
IaC findings	80	2.2k	1,500	500	100	100
Code findings-SCA	30	150	100	30	10	10

03 Findings



Do not setup access keys during initial user setup for all IAM users that have a console password

Severity: Medium

Status: Active

Exploitability: False

Discovered: 5 Days Ago

Description

Do not setup access keys during initial user setup for all IAM users that have a console password-AWS console defaults the checkbox for creating access keys to enabled. This results in many access keys being generated unnecessarily. In addition to unnecessary credentials, it also generates unnecessary management work in auditing and rotating these keys. Requiring that additional steps be taken by the user after their profile has been created will give a stronger indication of intent that access keys are (a) necessary for their work and (b) once the access key is established on an account that the keys may be in use somewhere in the organization.

Solution

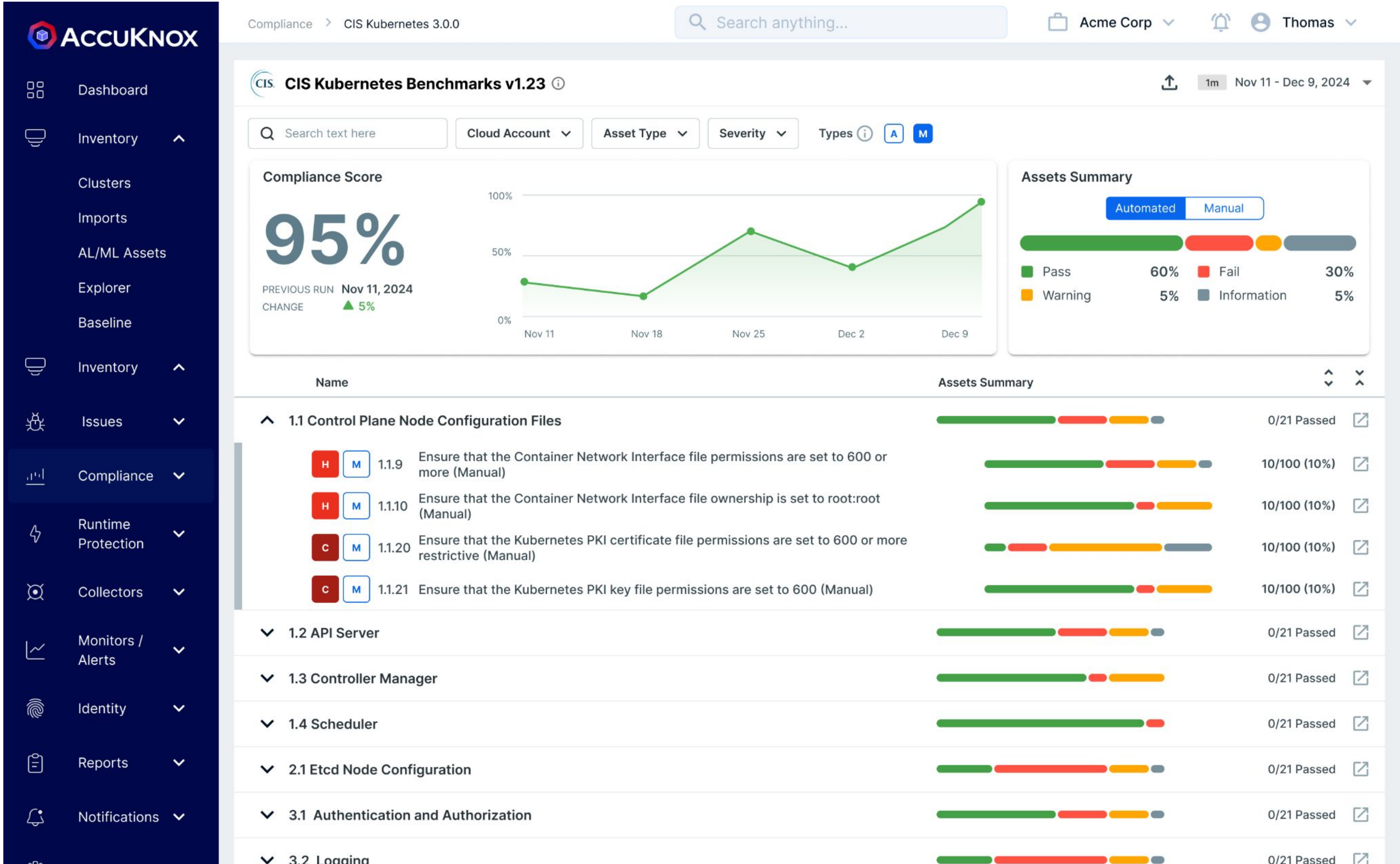
From the IAM console: generate credential report and disable not required keys.

Ticket Comments

0 comments available

Impacted assets

04 Compliance



Compliance > CIS Kubernetes 3.0.0

CIS Kubernetes Benchmarks v1.23

Nov 11 - Dec 9, 2024

Compliance Score

95%

PREVIOUS RUN Nov 11, 2024

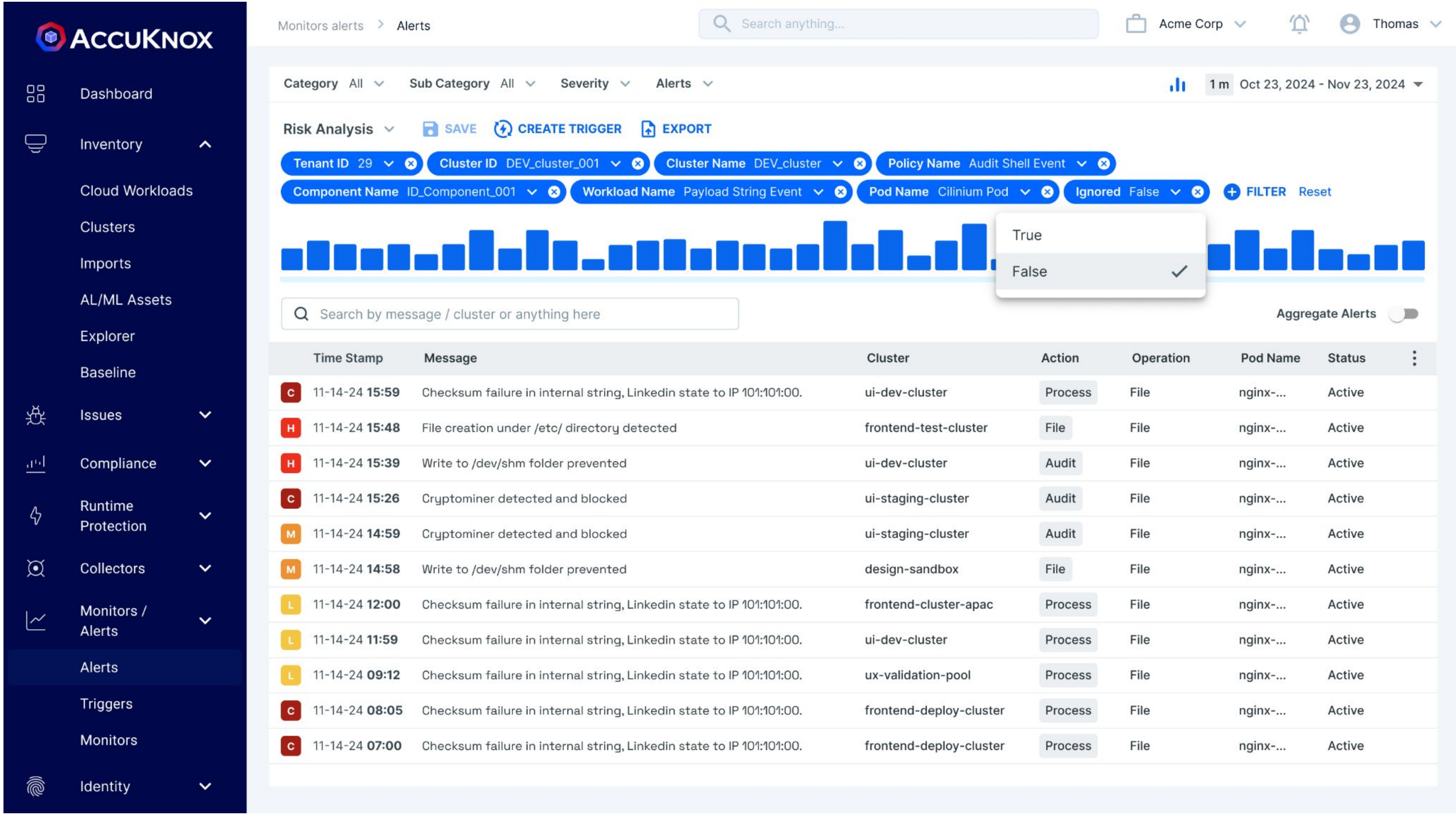
CHANGE ▲ 5%

Assets Summary

🟩 Pass	60%	🟥 Fail	30%
🟧 Warning	5%	⬛ Information	5%

Name	Assets Summary
1.1 Control Plane Node Configuration Files	0/21 Passed
H M 1.1.9 Ensure that the Container Network Interface file permissions are set to 600 or more (Manual)	10/100 (10%)
H M 1.1.10 Ensure that the Container Network Interface file ownership is set to root:root (Manual)	10/100 (10%)
C M 1.1.20 Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive (Manual)	10/100 (10%)
C M 1.1.21 Ensure that the Kubernetes PKI key file permissions are set to 600 (Manual)	10/100 (10%)
1.2 API Server	0/21 Passed
1.3 Controller Manager	0/21 Passed
1.4 Scheduler	0/21 Passed
2.1 Etcd Node Configuration	0/21 Passed
3.1 Authentication and Authorization	0/21 Passed
3.2 Logging	0/21 Passed

05 Alerts



Category All | Sub Category All | Severity | Alerts

Risk Analysis

Tenant ID 29 · Cluster ID DEV_cluster_001 · Cluster Name DEV_cluster · Policy Name Audit Shell Event · Component Name ID_Component_001 · Workload Name Payload String Event · Pod Name Cilinium Pod · Ignored False

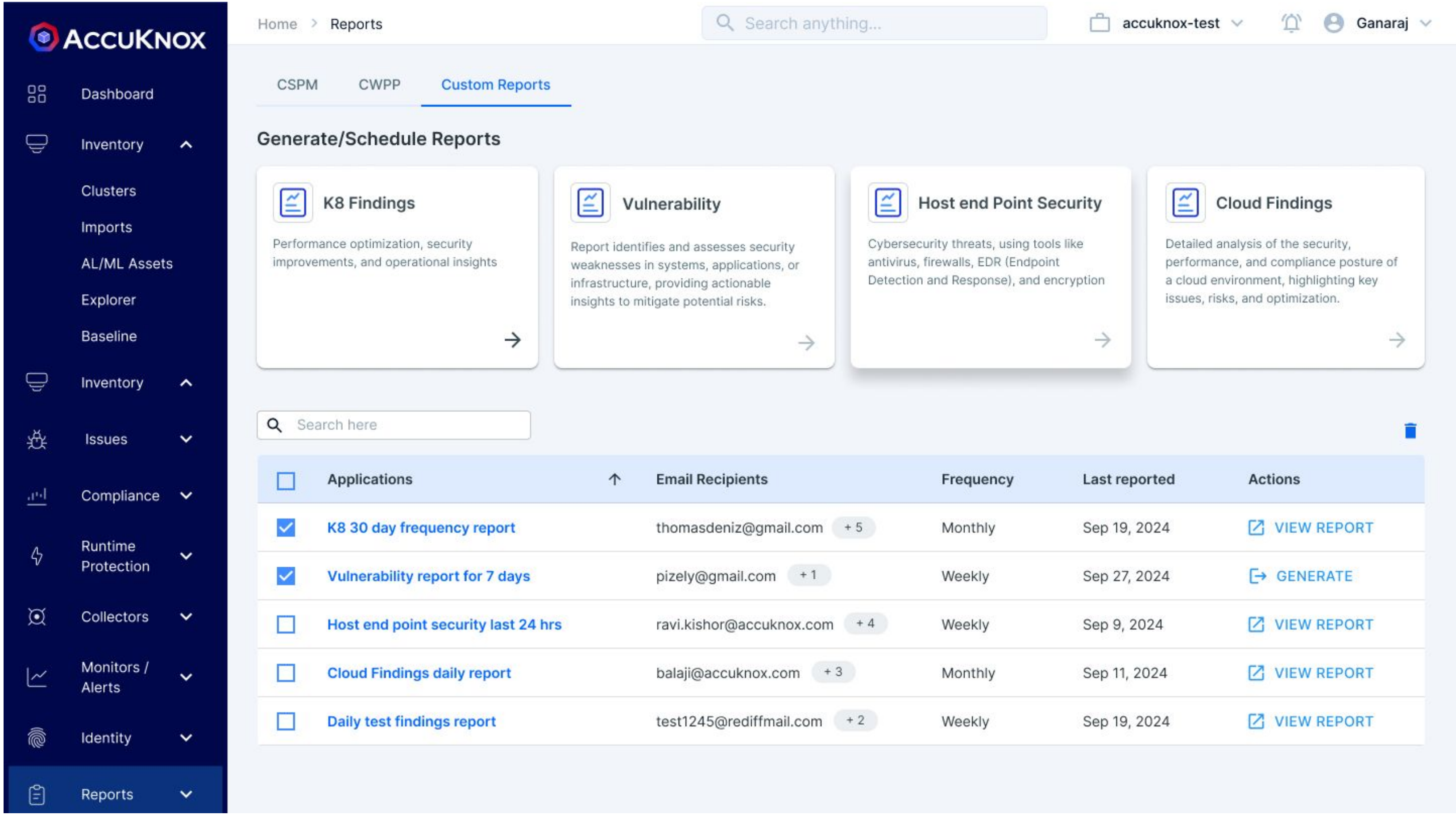
True

False ✓

Search by message / cluster or anything here

	Time Stamp	Message	Cluster	Action	Operation	Pod Name	Status
C	11-14-24 **15:59**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	ui-dev-cluster	Process	File	nginx-...	Active
H	11-14-24 **15:48**	File creation under /etc/ directory detected	frontend-test-cluster	File	File	nginx-...	Active
H	11-14-24 **15:39**	Write to /dev/shm folder prevented	ui-dev-cluster	Audit	File	nginx-...	Active
C	11-14-24 **15:26**	Cryptominer detected and blocked	ui-staging-cluster	Audit	File	nginx-...	Active
M	11-14-24 **14:59**	Cryptominer detected and blocked	ui-staging-cluster	Audit	File	nginx-...	Active
M	11-14-24 **14:58**	Write to /dev/shm folder prevented	design-sandbox	File	File	nginx-...	Active
L	11-14-24 **12:00**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	frontend-cluster-apac	Process	File	nginx-...	Active
L	11-14-24 **11:59**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	ui-dev-cluster	Process	File	nginx-...	Active
L	11-14-24 **09:12**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	ux-validation-pool	Process	File	nginx-...	Active
C	11-14-24 **08:05**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	frontend-deploy-cluster	Process	File	nginx-...	Active
C	11-14-24 **07:00**	Checksum failure in internal string, Linkedin state to IP 101:101:00.	frontend-deploy-cluster	Process	File	nginx-...	Active

06 REPORTS



Generate/Schedule Reports

K8 Findings
Performance optimization, security improvements, and operational insights

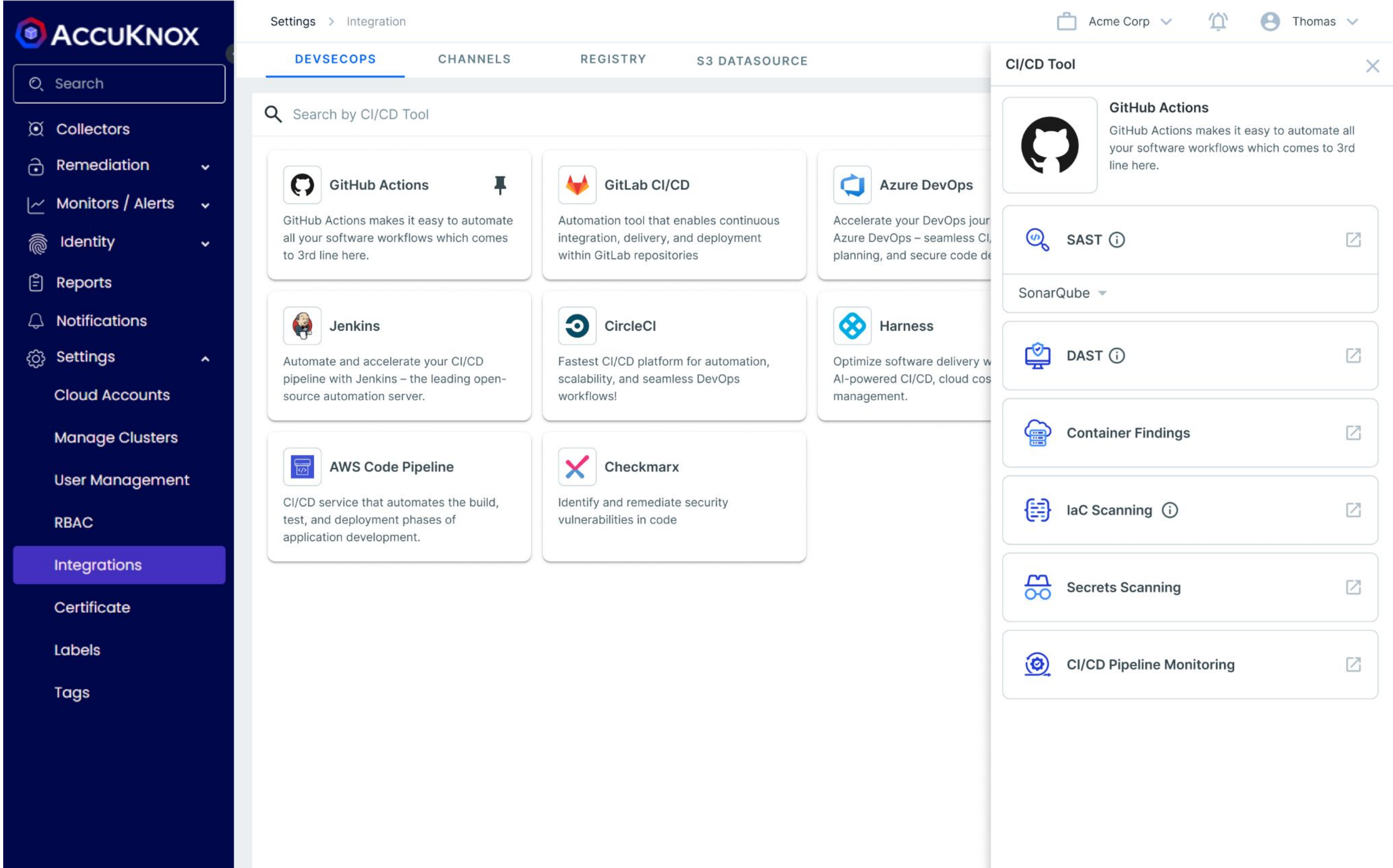
Vulnerability
Report identifies and assesses security weaknesses in systems, applications, or infrastructure, providing actionable insights to mitigate potential risks.

Host end Point Security
Cybersecurity threats, using tools like antivirus, firewalls, EDR (Endpoint Detection and Response), and encryption

Cloud Findings
Detailed analysis of the security, performance, and compliance posture of a cloud environment, highlighting key issues, risks, and optimization.

□	Applications ↑	Email Recipients	Frequency	Last reported	Actions
☑	K8 30 day frequency report	thomasdeniz@gmail.com + 5	Monthly	Sep 19, 2024	VIEW REPORT
☑	Vulnerability report for 7 days	pizely@gmail.com + 1	Weekly	Sep 27, 2024	GENERATE
□	Host end point security last 24 hrs	ravi.kishor@accuknox.com + 4	Weekly	Sep 9, 2024	VIEW REPORT
□	Cloud Findings daily report	balaji@accuknox.com + 3	Monthly	Sep 11, 2024	VIEW REPORT
□	Daily test findings report	test1245@rediffmail.com + 2	Weekly	Sep 19, 2024	VIEW REPORT

07 DevSecOps Integration



Settings > Integration

Acme Corp · Thomas

DEVSECOPS · CHANNELS · REGISTRY · S3 DATASOURCE

Search by CI/CD Tool

GitHub Actions
GitHub Actions makes it easy to automate all your software workflows which comes to 3rd line here.

GitLab CI/CD
Automation tool that enables continuous integration, delivery, and deployment within GitLab repositories

Azure DevOps
Accelerate your DevOps jour Azure DevOps – seamless CI, planning, and secure code de

Jenkins
Automate and accelerate your CI/CD pipeline with Jenkins – the leading open-source automation server.

CircleCI
Fastest CI/CD platform for automation, scalability, and seamless DevOps workflows!

Harness
Optimize software delivery w AI-powered CI/CD, cloud cos management.

AWS Code Pipeline
CI/CD service that automates the build, test, and deployment phases of application development.

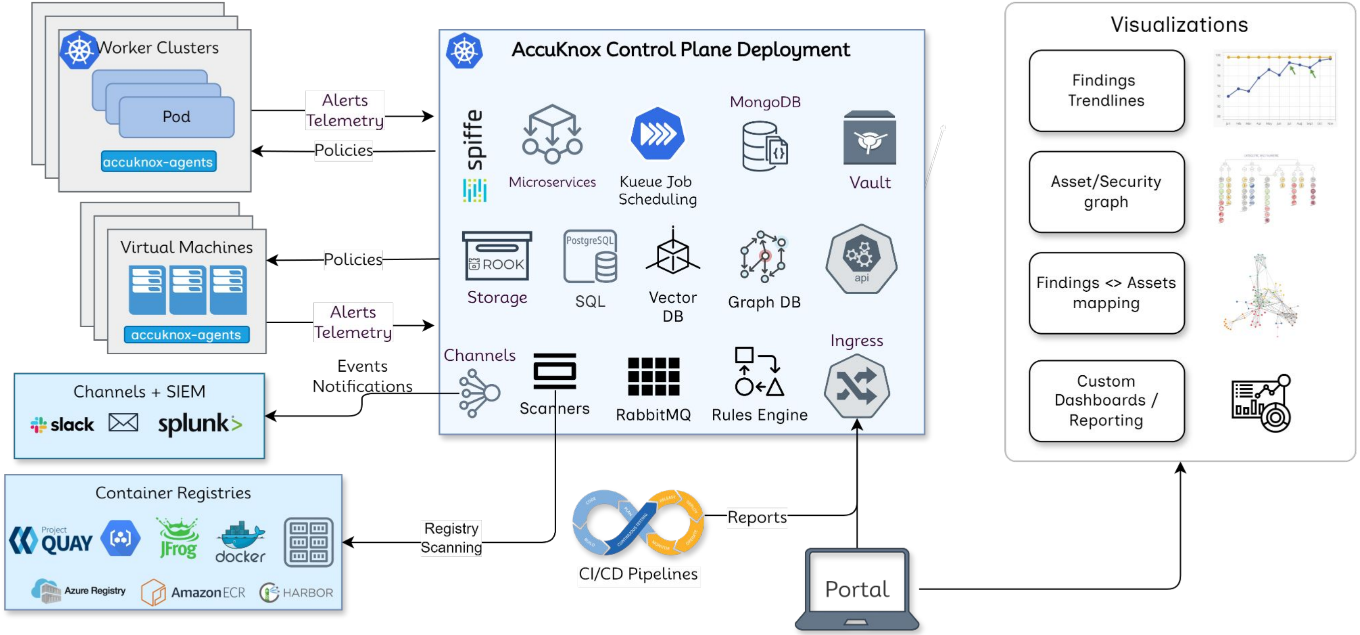
Checkmarx
Identify and remediate security vulnerabilities in code

CI/CD Tool

GitHub Actions
GitHub Actions makes it easy to automate all your software workflows which comes to 3rd line here.

- SAST — SonarQube
- DAST
- Container Findings
- IaC Scanning
- Secrets Scanning
- CI/CD Pipeline Monitoring

Architecture & Deployment Models



4 Types of Deployment Models:

1. Customer's On-prem (VMs, Bare metal)
2. Customer's Air-gapped infrastructure
3. Customer's Hosted Public & Private Cloud
4. AccuKnox's hosted SaaS

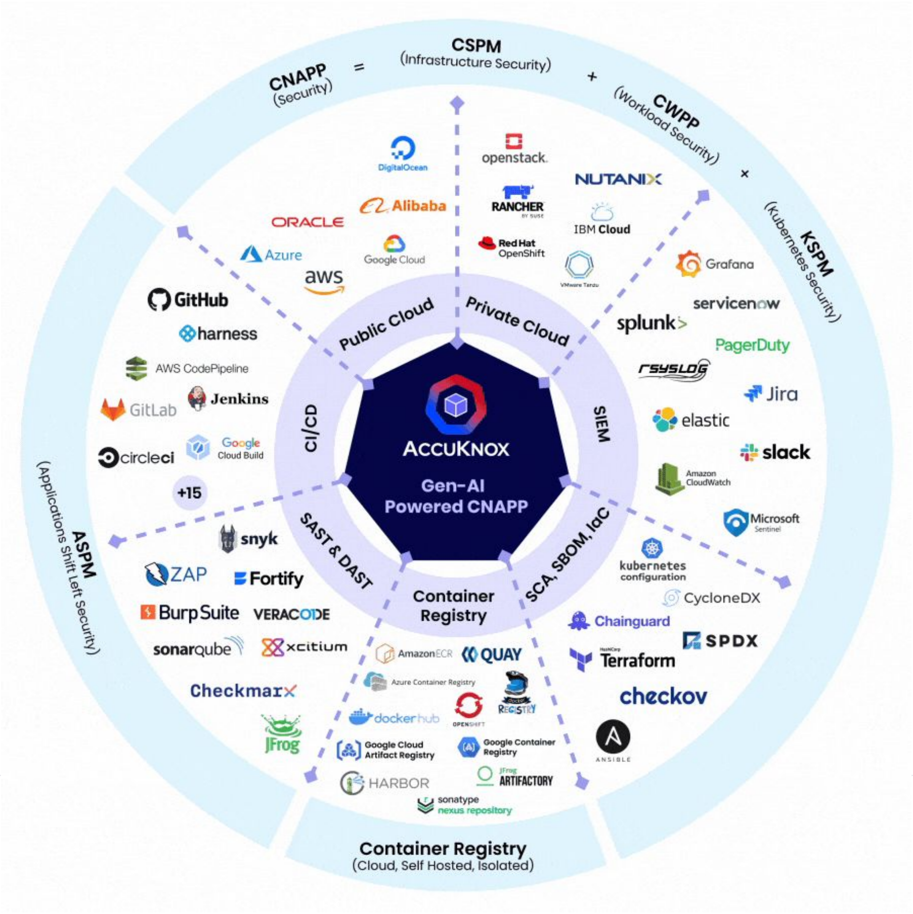
https://help.accuknox.com/getting-started/deployment-models/

Integrations Matrix

50+

Integrations

accuknox.com/integrations



ACCUKNOX

Industry Recognitions

ACCUKNOX

nationalgrid partners

Top Reasons why we invested in AccuKnox →

CLOUD SECURITY LIST

AccuKnox helps the Cloud security engineers notoriously overworked and under-resourced →

THENEWSTACK

AccuKnox's unique runtime security differentiation was emphasized by industry veterans →

Intellyx

An Intellyx Brain Candy Brief: AccuKnox stands apart in the Container security space →

Medium

It was inevitable that magic would happen when Nat and Phil met and shared their visions - says Raghuram, investor at AccuKnox →

NUTANIX

Announces AccuKnox as their 2024 AI Partner Program →

aws

AWS announces partnership with AccuKnox's Zero Trust CNAPP →

LF EDGE

AccuKnox joins mimik Technologies, IBM as Open Horizon project partner →

aiTechPark Connecting Insights with Individuals

Kubernetes Security Platform AccuKnox Secures $4.6M →

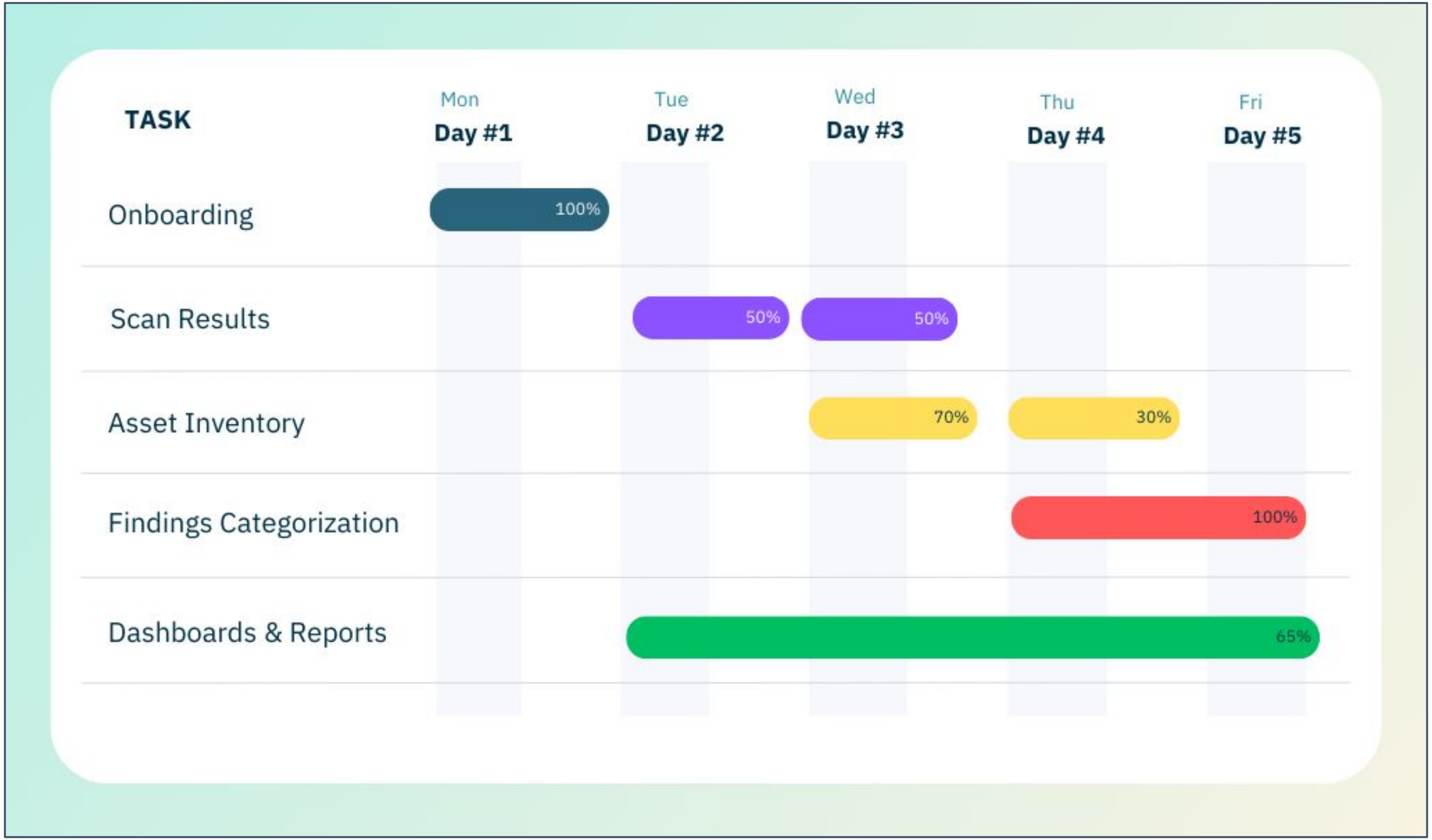
Red Hat

AccuKnox was verified and validated by RHEL operating systems security →

sjultra your cloud security partner

SJULTRA and AccuKnox collaborate to deliver CNAPP to the Enterprise →

POC Timelines



Summary

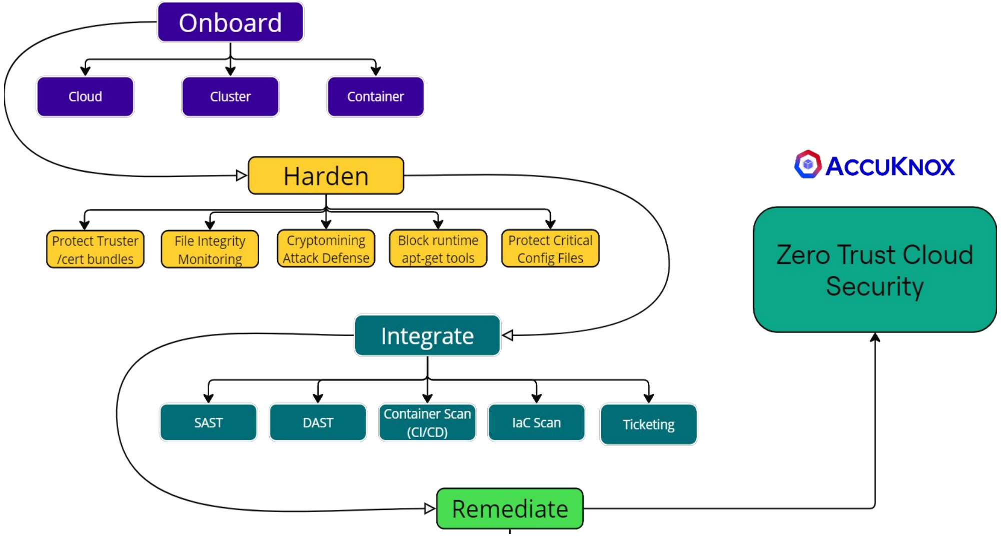
POC Execution:

Stage 1: Asset Inventory (Onboarding)

Stage 2: Discover Risk Assessment

Stage 3: Perform Risk Based Prioritization

Stage 4: Remediation (Policies, Ticketing)



Onboard

Cloud

Cluster

Container

Harden

Protect Truster /cert bundles

File Integrity Monitoring

Cryptomining Attack Defense

Block runtime apt-get tools

Protect Critical Config Files

Integrate

SAST

DAST

Container Scan (CI/CD)

IaC Scan

Ticketing

Remediate

ACCUKNOX

Zero Trust Cloud Security

aws Available in AWS Marketplace

Red Hat Marketplace Operated by IBM

Now available on Microsoft Azure MARKETPLACE

ORACLE Cloud Marketplace

accuknox.com/marketplace

Get AccuKnox CNAPP Demo

ACCUKNOX

ACCUKNOX

SEE US IN ACTION

support@accuknox.com

Certified by

kubernetes CERTIFIED SERVICE PROVIDER

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

CLOUD NATIVE COMPUTING FOUNDATION
SILVER MEMBER

NEPHIO

aws
PARTNER
Amazon EKS Ready

NUTANIX
READY
AHV