AccuKnox

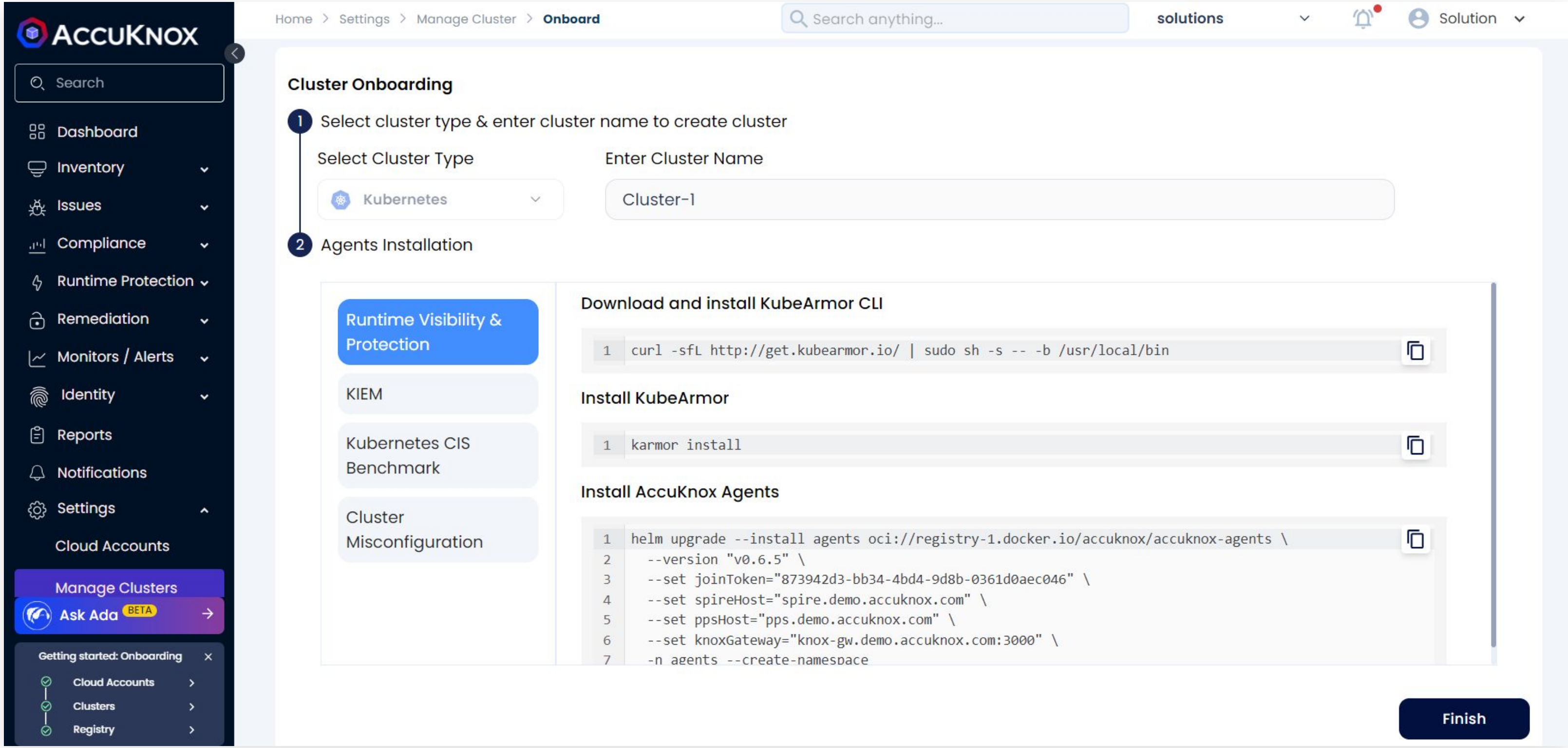
CWPP Playbook

Table of Contents

- Realtime Protection for K8s Shared Network
    - Onboarding
    - App Behavior Monitoring
    - Policies
    - Pod Security Admission (PSA)
- Container Registry Scanning
- Forensics

Cluster Onboarding (Agent Based)

- Navigate to Settings → Manage Cluster and click on Onboard Now
- Provide a name for the cluster and install the agents via the commands on screen



Cluster Onboarding

1. Select cluster type & enter cluster name to create cluster

Select Cluster Type: Kubernetes

Enter Cluster Name: Cluster-1

2. Agents Installation

Download and install KubeArmor CLI

```
curl -sfL http://get.kubearmor.io/ | sudo sh -s -- -b /usr/local/bin
```

Install KubeArmor

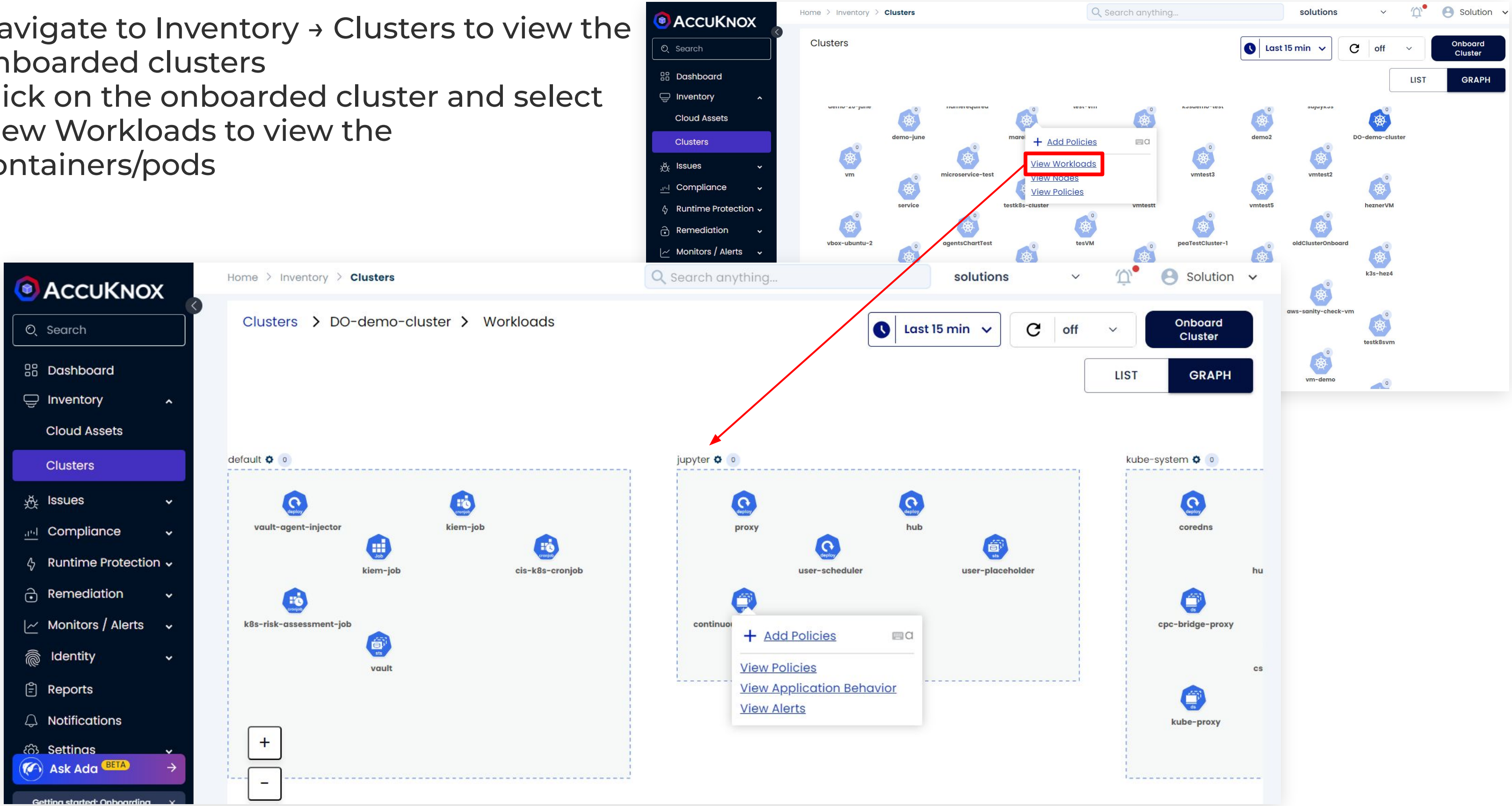
```
karmor install
```

Install AccuKnox Agents

```
helm upgrade --install agents oci://registry-1.docker.io/accuknox/accuknox-agents \
  --version "v0.6.5" \
  --set joinToken="873942d3-bb34-4bd4-9d8b-0361d0aec046" \
  --set spireHost="spire.demo.accuknox.com" \
  --set ppsHost="pps.demo.accuknox.com" \
  --set knoxGateway="knox-gw.demo.accuknox.com:3000" \
  -n agents --create-namespace
```

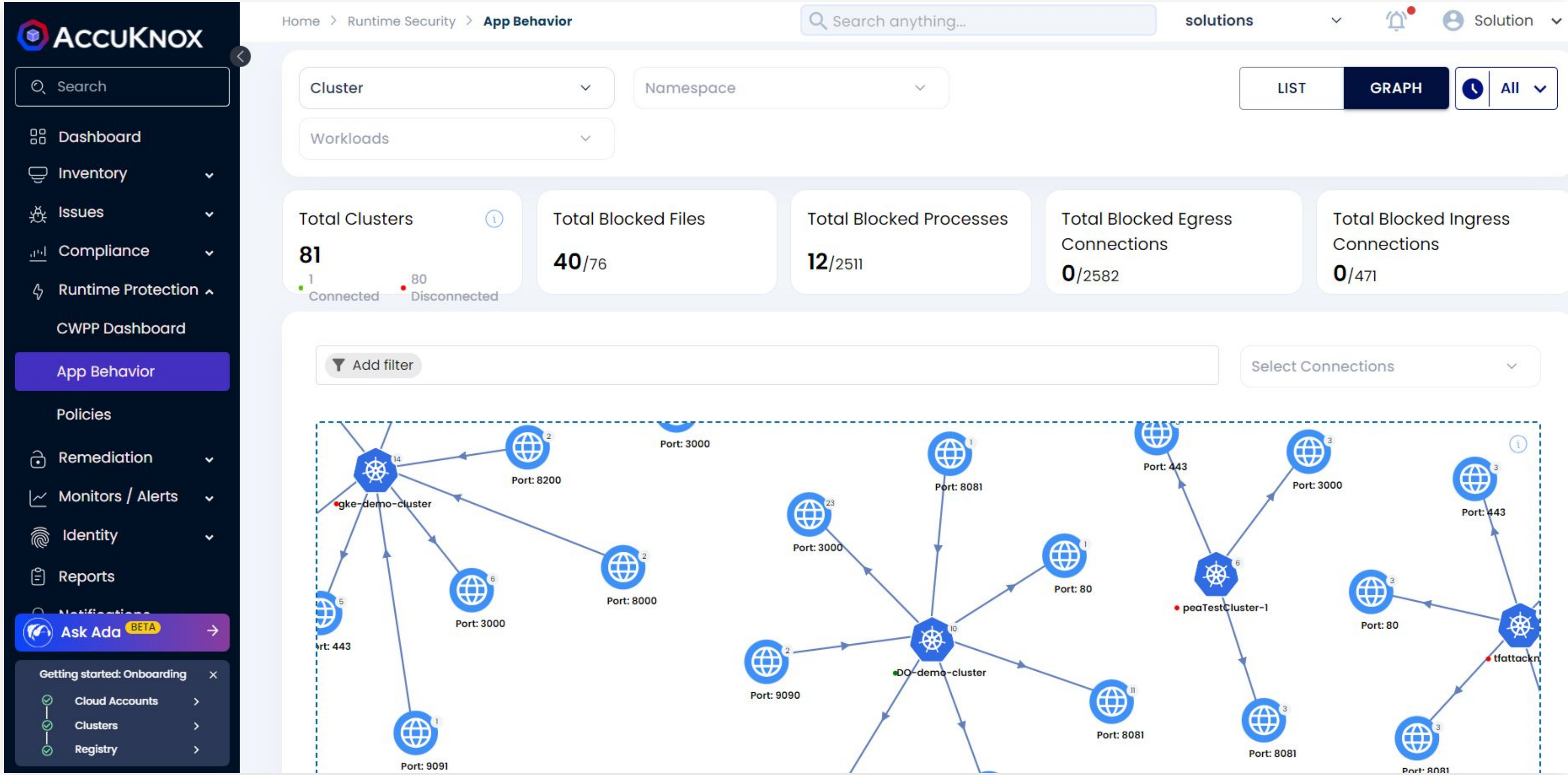
View Clusters

- Navigate to Inventory → Clusters to view the onboarded clusters
- Click on the onboarded cluster and select View Workloads to view the containers/pods



Application Behavior - Graph view

Navigate to Runtime Protection → App Behavior to view a Network Graph

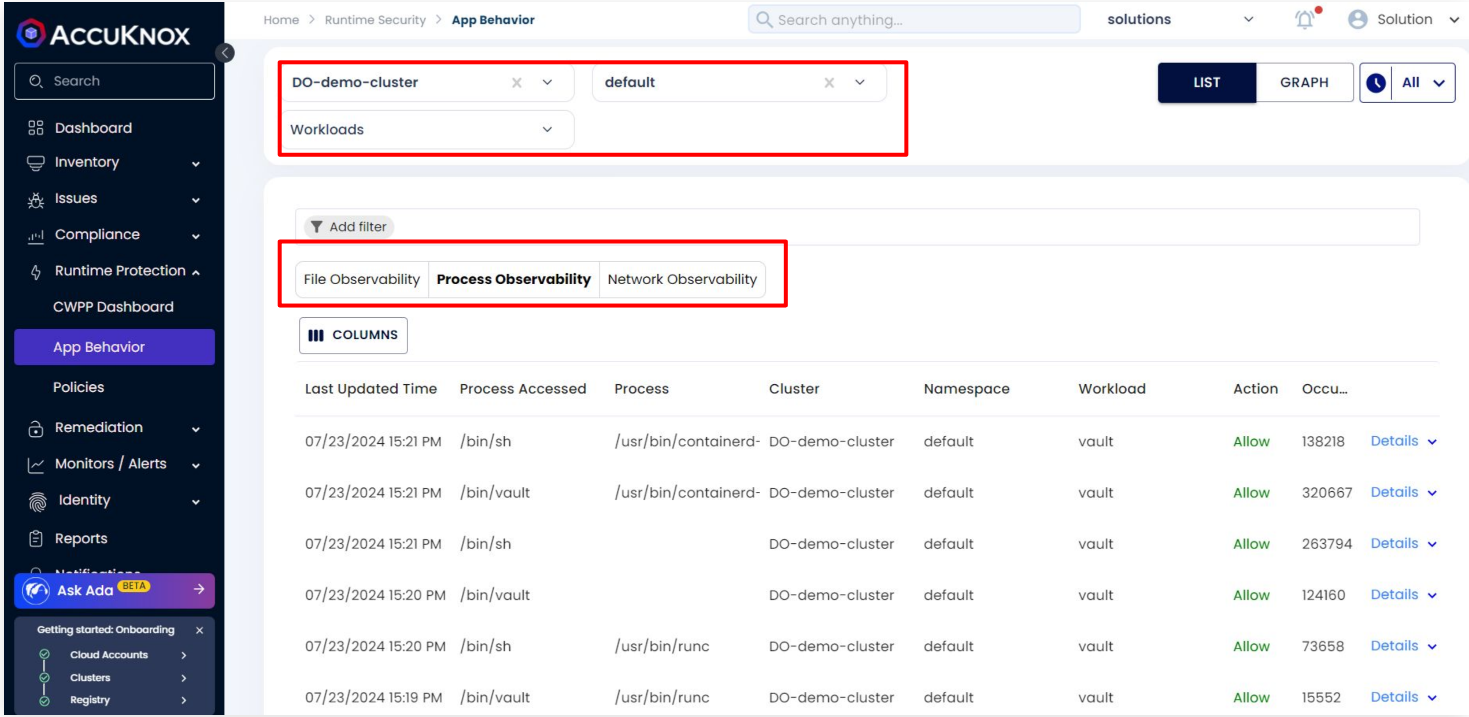


Home > Runtime Security > App Behavior

Total Clusters	Total Blocked Files	Total Blocked Processes	Total Blocked Egress Connections	Total Blocked Ingress Connections
81 1 Connected 80 Disconnected	40/76	12/2511	0/2582	0/471

Application Behavior - List view

The behavior can be filtered for particular workloads by selecting a specific cluster, namespace or workload. The data can also be provided in a list view including the network, file access and process execution observability.



DO-demo-cluster | default

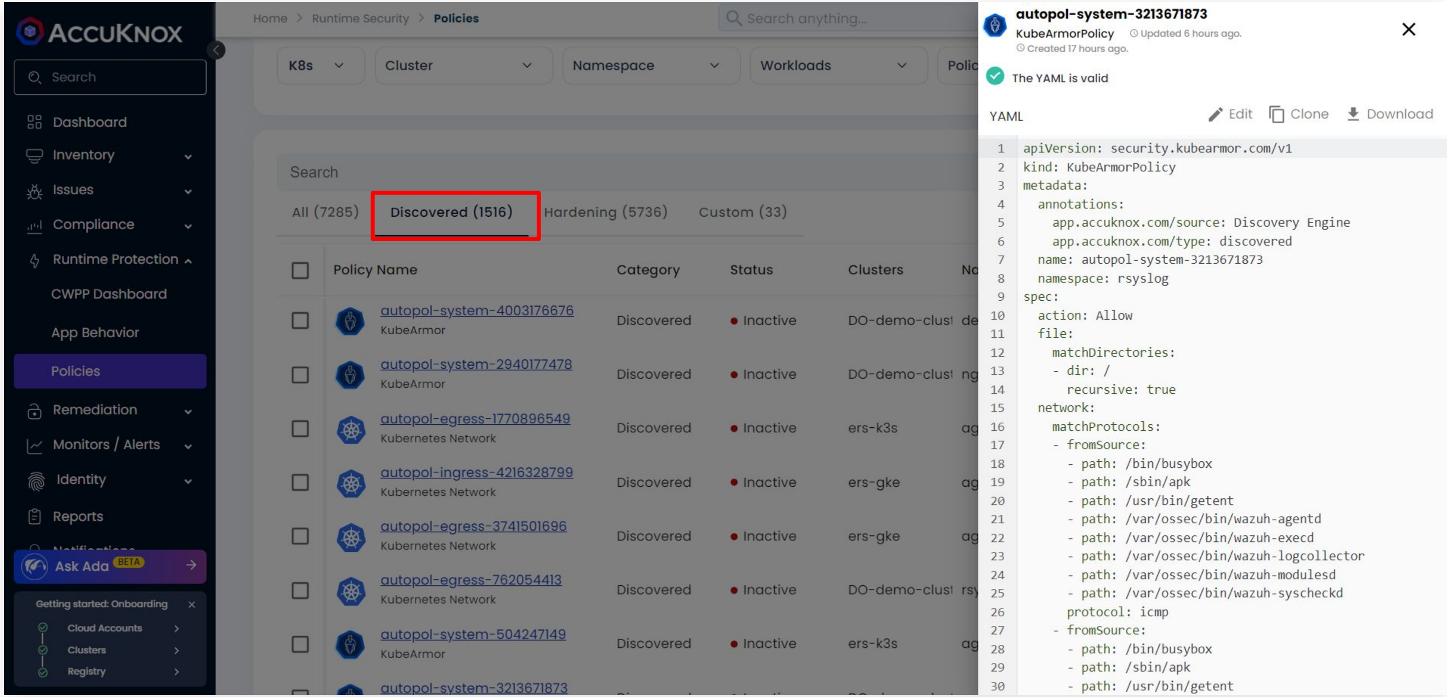
Workloads

File Observability | **Process Observability** | Network Observability

Last Updated Time	Process Accessed	Process	Cluster	Namespace	Workload	Action	Occu...	
07/23/2024 15:21 PM	/bin/sh	/usr/bin/containerd-	DO-demo-cluster	default	vault	Allow	138218	Details ⌄
07/23/2024 15:21 PM	/bin/vault	/usr/bin/containerd-	DO-demo-cluster	default	vault	Allow	320667	Details ⌄
07/23/2024 15:21 PM	/bin/sh		DO-demo-cluster	default	vault	Allow	263794	Details ⌄
07/23/2024 15:20 PM	/bin/vault		DO-demo-cluster	default	vault	Allow	124160	Details ⌄
07/23/2024 15:20 PM	/bin/sh	/usr/bin/runc	DO-demo-cluster	default	vault	Allow	73658	Details ⌄
07/23/2024 15:19 PM	/bin/vault	/usr/bin/runc	DO-demo-cluster	default	vault	Allow	15552	Details ⌄

Policies - Discovered

- Navigate to Runtime Protection → Policies and click on Discovered tab
- These discovered policies are generated based on the app behavior identified and whitelist the detected behavior. Click on any of the policies to view the whitelisted behavior



☐	Policy Name	Category	Status	Clusters	Na
☐	autopol-system-4003176676 KubeArmor	Discovered	● Inactive	DO-demo-clust	de
☐	autopol-system-2940177478 KubeArmor	Discovered	● Inactive	DO-demo-clust	ng
☐	autopol-egress-1770896549 Kubernetes Network	Discovered	● Inactive	ers-k3s	ag
☐	autopol-ingress-4216328799 Kubernetes Network	Discovered	● Inactive	ers-gke	ag
☐	autopol-egress-3741501696 Kubernetes Network	Discovered	● Inactive	ers-gke	ag
☐	autopol-egress-762054413 Kubernetes Network	Discovered	● Inactive	DO-demo-clust	rsy
☐	autopol-system-504247149 KubeArmor	Discovered	● Inactive	ers-k3s	ag
☐	autopol-system-3213671873				

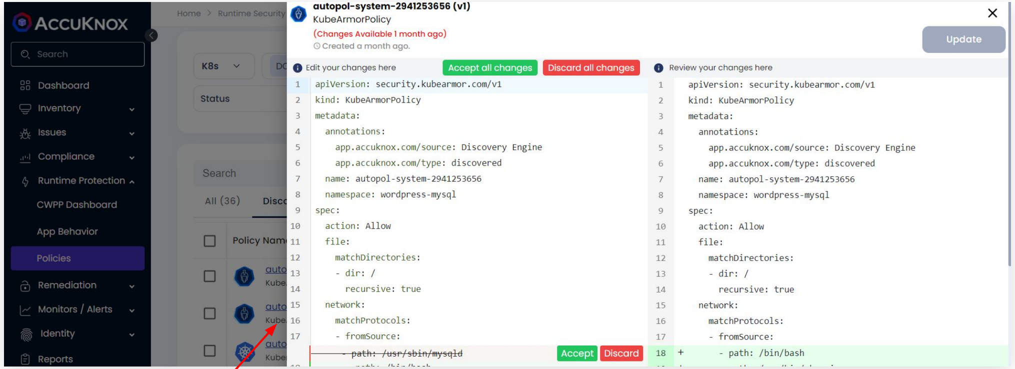
autopol-system-3213671873
KubeArmorPolicy Updated 6 hours ago.
Created 17 hours ago.

✓ The YAML is valid

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  annotations:
    app.accuknox.com/source: Discovery Engine
    app.accuknox.com/type: discovered
  name: autopol-system-3213671873
  namespace: rsyslog
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /
      recursive: true
  network:
    matchProtocols:
    - fromSource:
      - path: /bin/busybox
      - path: /sbin/apk
      - path: /usr/bin/getent
      - path: /var/ossec/bin/wazuh-agentd
      - path: /var/ossec/bin/wazuh-execd
      - path: /var/ossec/bin/wazuh-logcollector
      - path: /var/ossec/bin/wazuh-modulesd
      - path: /var/ossec/bin/wazuh-syscheckd
      protocol: icmp
    - fromSource:
      - path: /bin/busybox
      - path: /sbin/apk
      - path: /usr/bin/getent
```

Policies - Zero Trust Journey

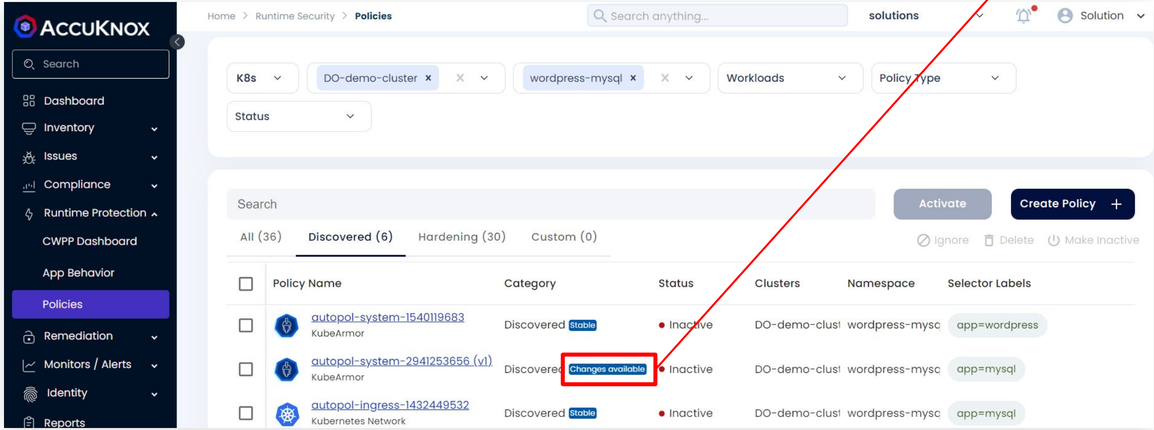
- The discovered policies will be applied in a learning/audit mode by default and will only alert for any violations
- Update the policy as required by selecting the Changes Available



autopol-system-2941253656 (v1)
KubeArmorPolicy
(Changes Available 1 month ago)
Created a month ago.

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  annotations:
    app.accuknox.com/source: Discovery Engine
    app.accuknox.com/type: discovered
  name: autopol-system-2941253656
  namespace: wordpress-mysql
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /
      recursive: true
  network:
    matchProtocols:
    - fromSource:
      - path: /usr/sbin/mysqld
```

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  annotations:
    app.accuknox.com/source: Discovery Engine
    app.accuknox.com/type: discovered
  name: autopol-system-2941253656
  namespace: wordpress-mysql
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /
      recursive: true
  network:
    matchProtocols:
    - fromSource:
+     - path: /bin/bash
```

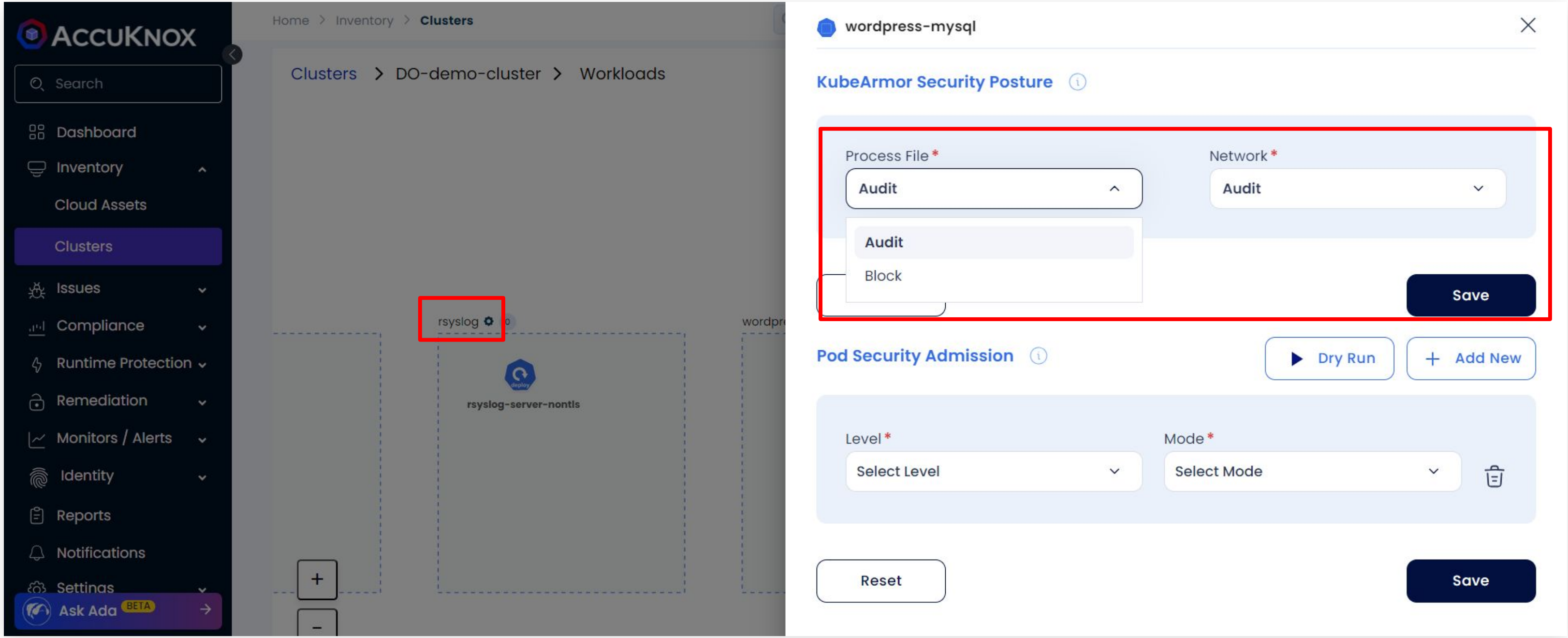


□	Policy Name	Category	Status	Clusters	Namespace	Selector Labels
□	autopol-system-1540119683 KubeArmor	Discovered Stable	● Inactive	DO-demo-clust	wordpress-mysq	app=wordpress
□	autopol-system-2941253656 (v1) KubeArmor	Discovered Changes available	● Inactive	DO-demo-clust	wordpress-mysq	app=mysql
□	autopol-ingress-1432449532 Kubernetes Network	Discovered Stable	● Inactive	DO-demo-clust	wordpress-mysq	app=mysql

- The discovered policies will be marked stable if no deviation is detected from the policy
- When the policies have become stable, they can be enforced in block mode

Policies - Enforce Zero Trust

- After applying the stable discovered policies for a namespace, navigate to Inventory → Clusters. Click on the Cluster → View Workloads
- Click on the Cog Icon next to the namespace, set the KubeArmor posture to Block
- When the application is updated, change back to Audit to learn new behavior



wordpress-mysql

KubeArmor Security Posture

Process File *: Audit

Network *: Audit

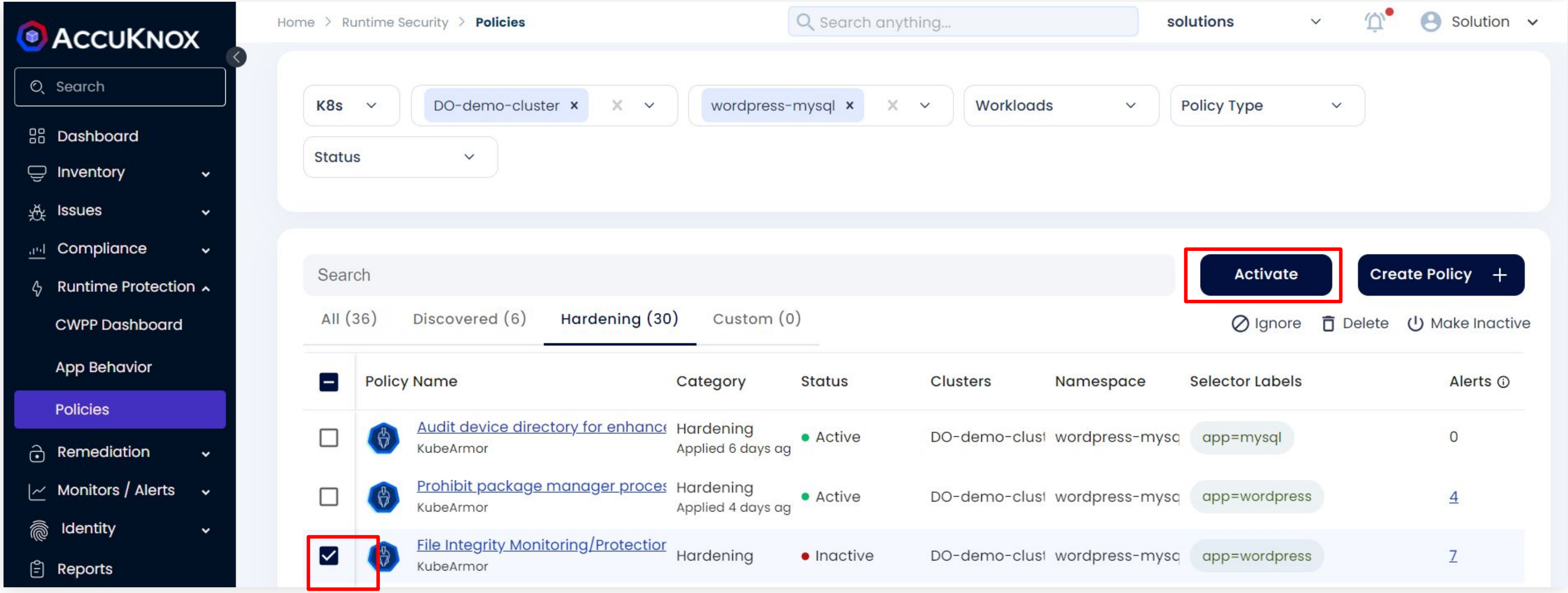
Pod Security Admission

Level *: Select Level

Mode *: Select Mode

Policies - Hardening

- Navigate to Runtime Protection → Policies and click on Hardening tab
- These discovered policies are based on frameworks like MITRE, CIS, NIST, etc... to improve security and compliance
- Select the Policy and click on Activate to apply it



☐	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Alerts ⓘ
☐	Audit device directory for enhance KubeArmor	Hardening Applied 6 days ag	● Active	DO-demo-clust	wordpress-mysq	app=mysql	0
☐	Prohibit package manager proces KubeArmor	Hardening Applied 4 days ag	● Active	DO-demo-clust	wordpress-mysq	app=wordpress	4
☑	File Integrity Monitoring/Protectior KubeArmor	Hardening	● Inactive	DO-demo-clust	wordpress-mysq	app=wordpress	7

Pod Security Admission (PSA)

- Pod Security admission places requirements on a Pod's Security Context and other related fields according to the three levels defined by the Pod Security Standards:

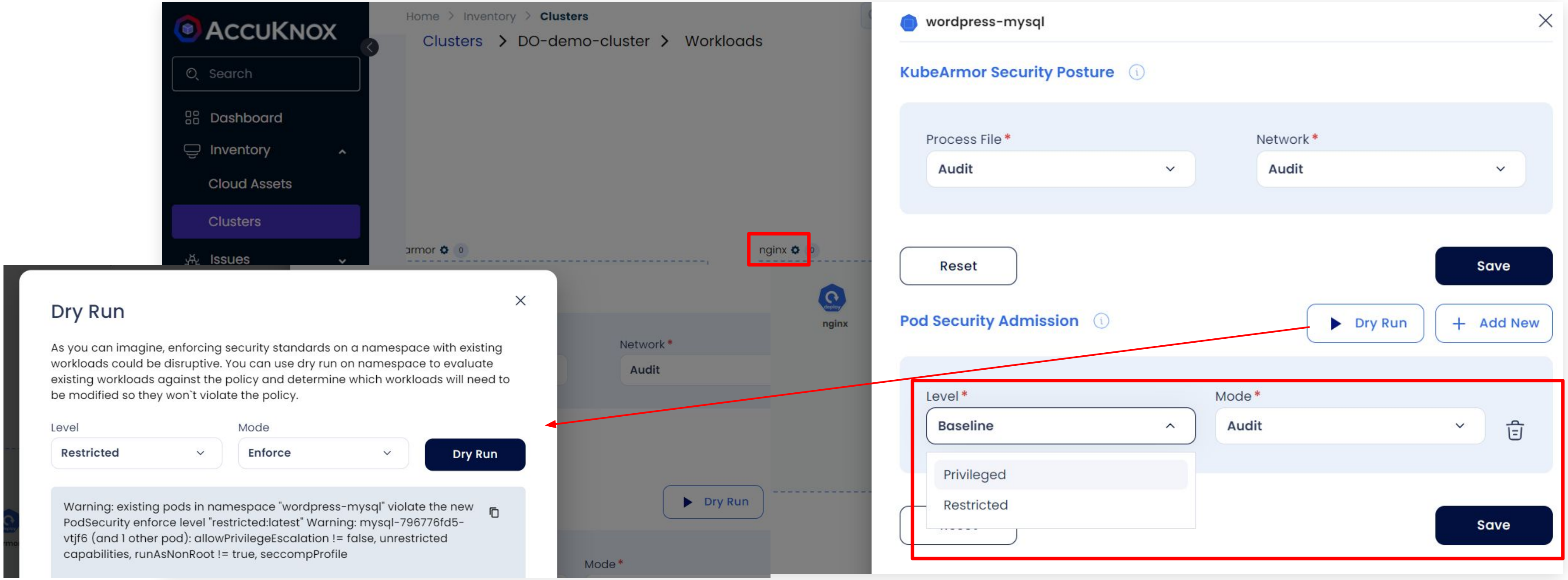
Level	Description
Privileged	Unrestricted policy,allows for known privilege escalations.
Baseline	Minimally restrictive policy. Allows the default (minimally specified) Pod configuration.
Restricted	Heavily restricted policy, following current Pod hardening best practices.

- PSA can be enabled in two modes:

Mode	Description
enforce	Policy violations will cause the pod to be rejected.
audit	Policy violations will trigger an alert but will otherwise be allowed

Enabling Pod Security Admission (PSA)

- Navigate to Inventory → Clusters and click on the cluster, select View Workloads
- Click on the cog icon next to the namespace
- Select a Level and Mode for the PSA. In case of Enforce mode, click on Dry Run to view potential effects before applying



Dry Run

As you can imagine, enforcing security standards on a namespace with existing workloads could be disruptive. You can use dry run on namespace to evaluate existing workloads against the policy and determine which workloads will need to be modified so they won`t violate the policy.

Level: Restricted

Mode: Enforce

Dry Run

Warning: existing pods in namespace "wordpress-mysql" violate the new PodSecurity enforce level "restricted:latest" Warning: mysql-796776fd5-vtjf6 (and 1 other pod): allowPrivilegeEscalation != false, unrestricted capabilities, runAsNonRoot != true, seccompProfile

wordpress-mysql

KubeArmor Security Posture

Process File *: Audit

Network *: Audit

Reset | Save

Pod Security Admission

Dry Run | + Add New

Level *: Baseline

- Privileged
- Restricted

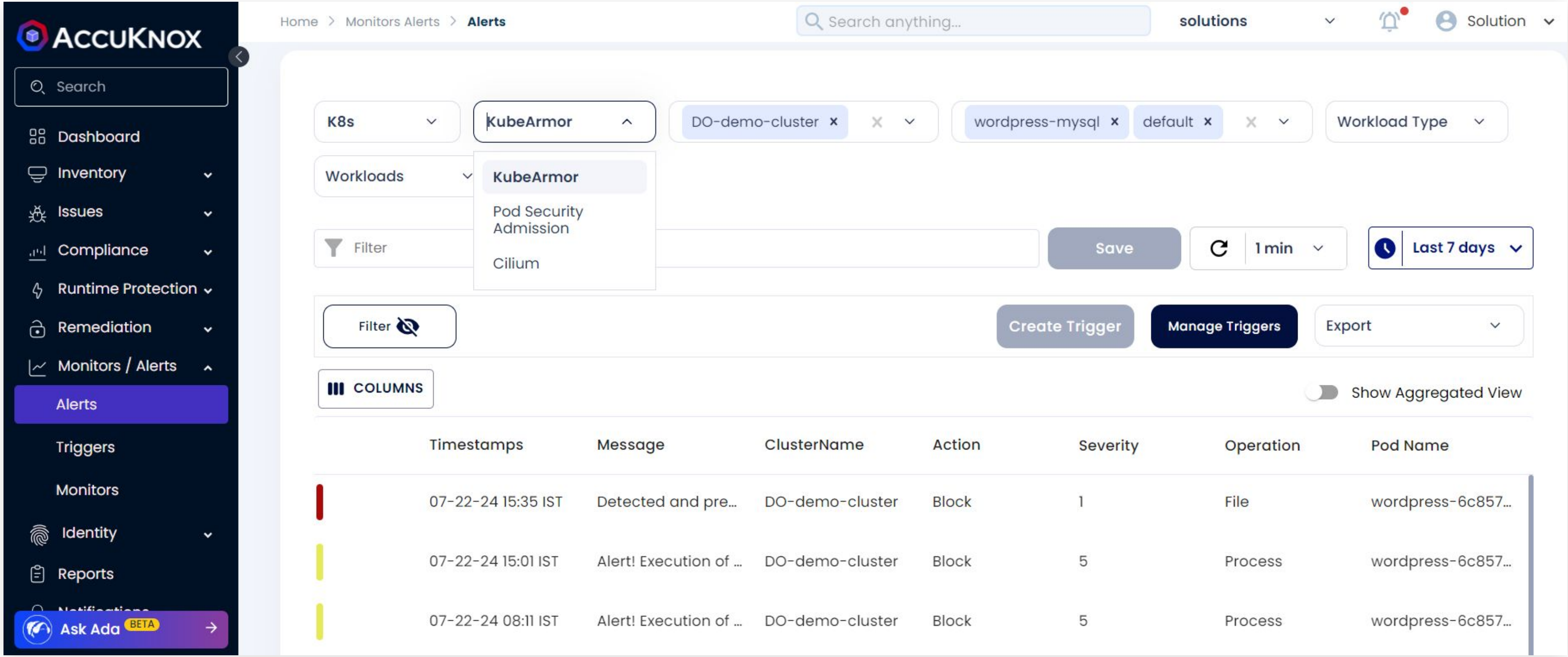
Mode *: Audit

Reset | Save

Logs and Alerts for Policy Violation

ACCUKNOX

- Navigate to Monitors/Alerts → Alerts to view the alerts generated for policy violations
- Custom Filtering can be performed on this screen and saved for quick filtering



Home > Monitors Alerts > Alerts

K8s | KubeArmor | DO-demo-cluster × | wordpress-mysql × | default × | Workload Type

Workloads

KubeArmor
Pod Security Admission
Cilium

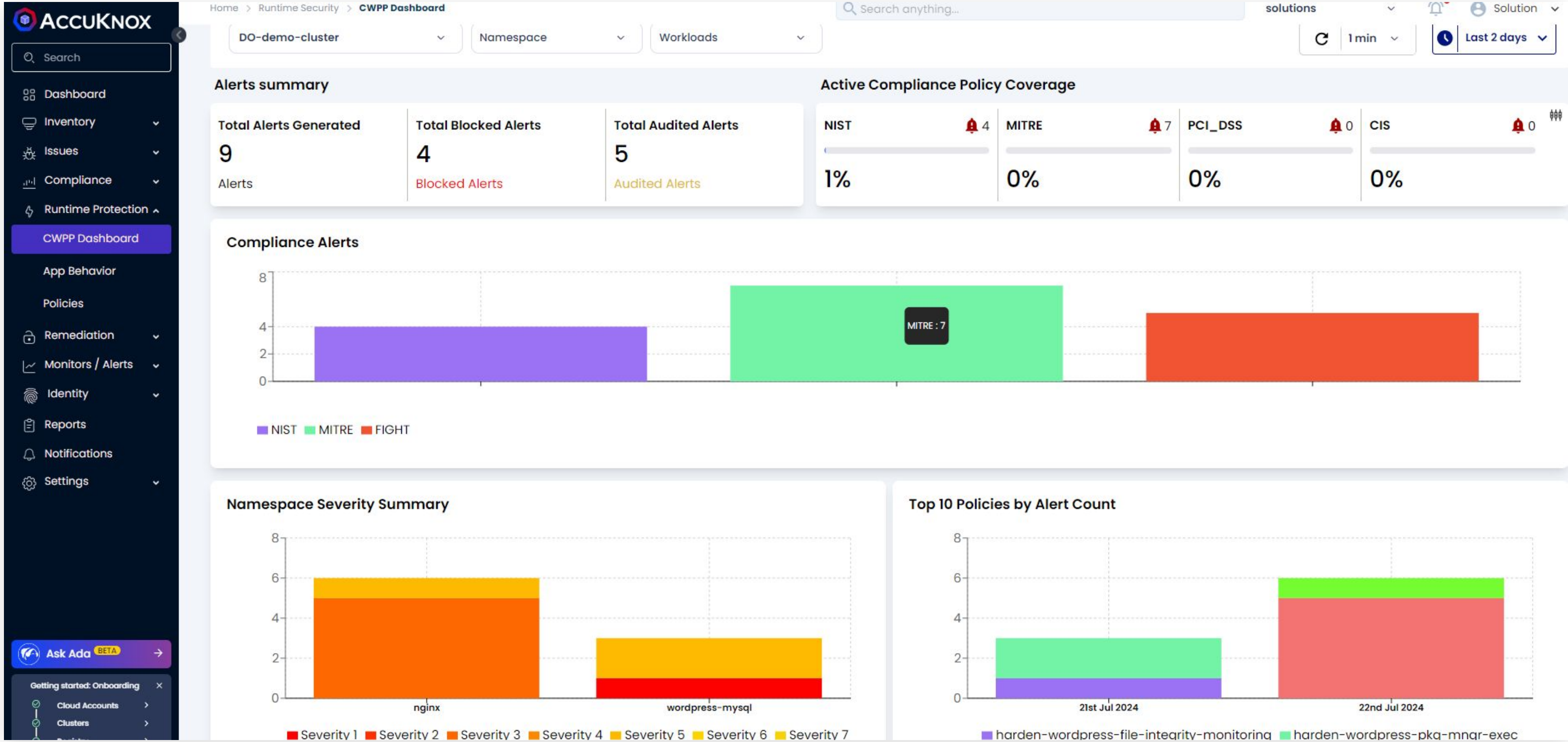
Filter

1 min | Last 7 days

	Timestamps	Message	ClusterName	Action	Severity	Operation	Pod Name
🟥	07-22-24 15:35 IST	Detected and pre...	DO-demo-cluster	Block	1	File	wordpress-6c857...
🟨	07-22-24 15:01 IST	Alert! Execution of ...	DO-demo-cluster	Block	5	Process	wordpress-6c857...
🟨	07-22-24 08:11 IST	Alert! Execution of ...	DO-demo-cluster	Block	5	Process	wordpress-6c857...

CWPP Dashboard

After applying policies and some alerts have been triggered, navigate to Runtime Protection → CWPP Dashboard and select the cluster for a comprehensive view



Alerts summary

Total Alerts Generated	Total Blocked Alerts	Total Audited Alerts
9	4	5
Alerts	Blocked Alerts	Audited Alerts

Active Compliance Policy Coverage

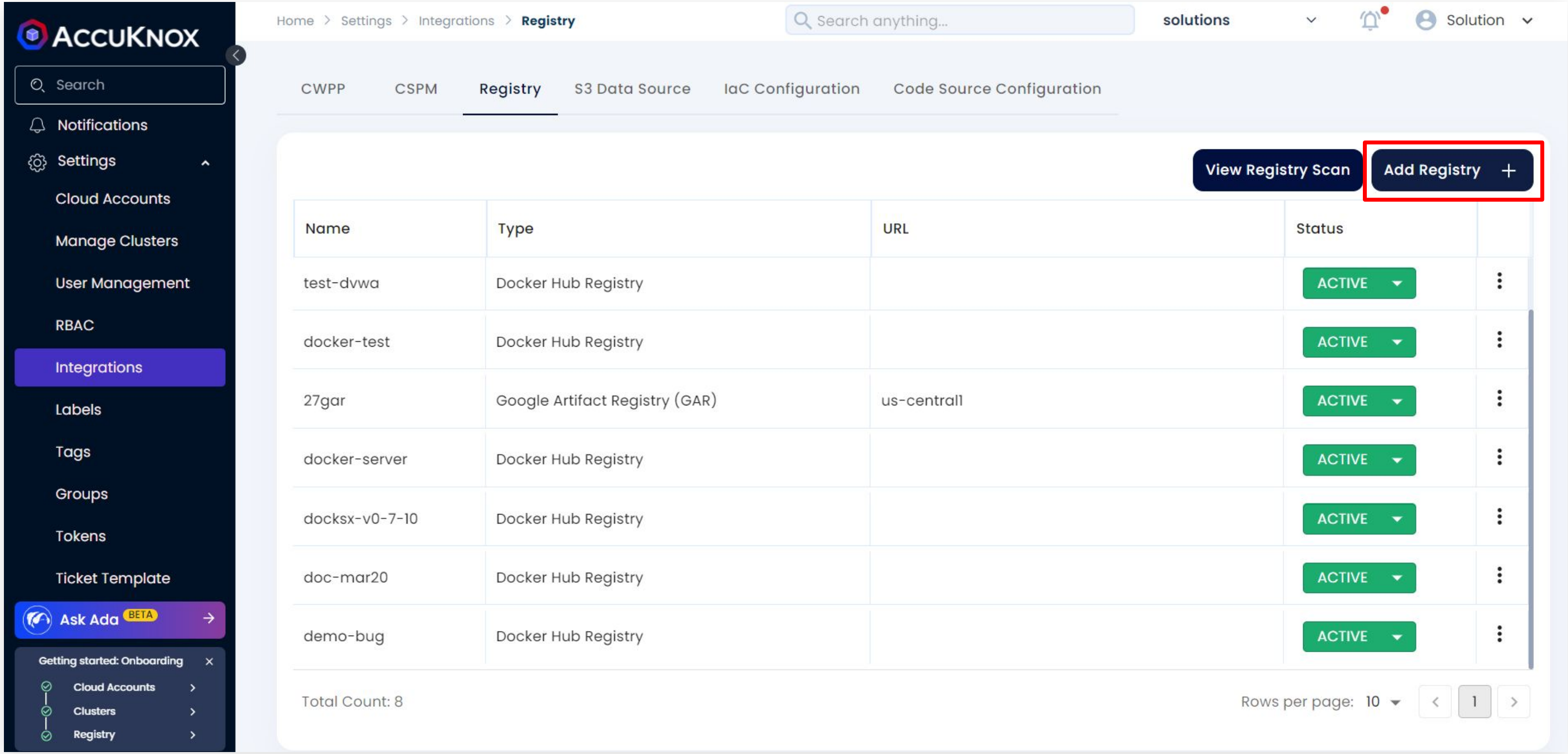
NIST	MITRE	PCI_DSS	CIS
4	7	0	0
1%	0%	0%	0%

ACCUKNOX

Vulnerability Management for Containers

Onboard Container Image Registries

- Navigate to Settings → Integrations → Registry tab
- Click on Add Registry



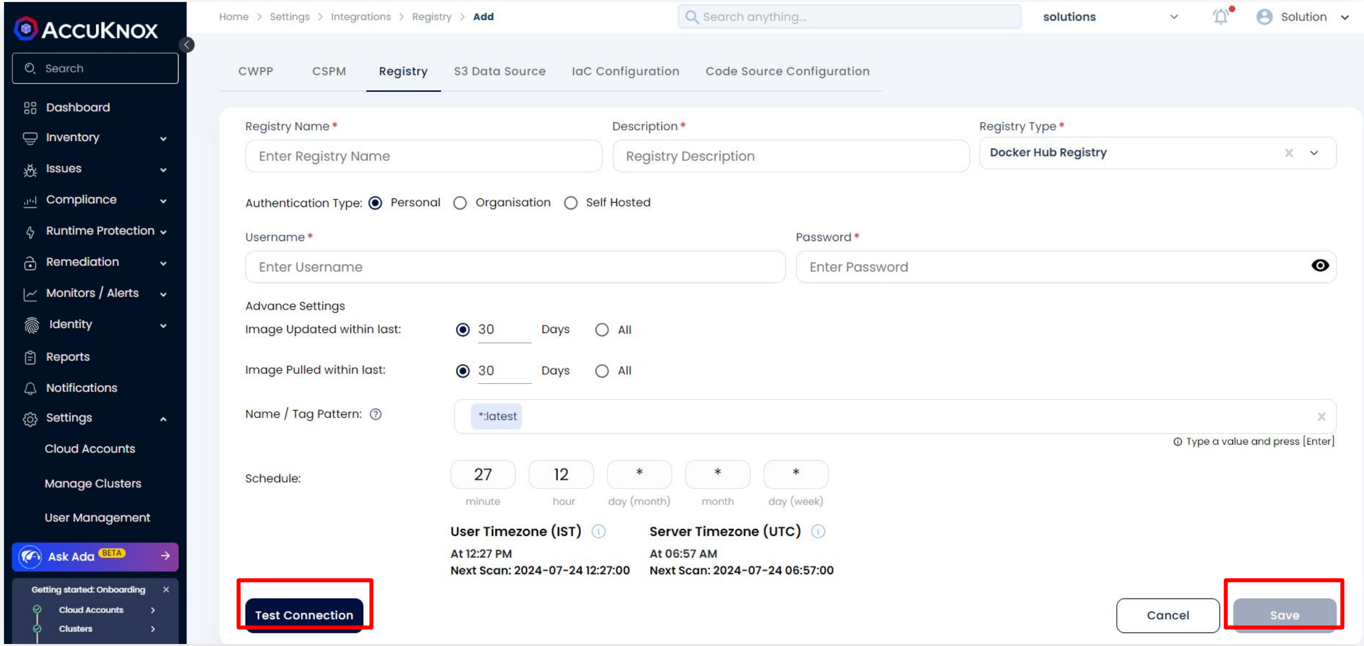
Name	Type	URL	Status
test-dvwa	Docker Hub Registry		ACTIVE
docker-test	Docker Hub Registry		ACTIVE
27gar	Google Artifact Registry (GAR)	us-central1	ACTIVE
docker-server	Docker Hub Registry		ACTIVE
docksx-v0-7-10	Docker Hub Registry		ACTIVE
doc-mar20	Docker Hub Registry		ACTIVE
demo-bug	Docker Hub Registry		ACTIVE

Total Count: 8

Rows per page: 10

Onboard Container Image Registries

- Input a Name and Description of the registry. Select the Registry Type
- Provide Auth Credentials as per the selected registry



Registry Name * : Enter Registry Name

Description * : Registry Description

Registry Type * : Docker Hub Registry

Authentication Type: ● Personal ○ Organisation ○ Self Hosted

Username * : Enter Username

Password * : Enter Password

Advance Settings

Image Updated within last: ● 30 Days ○ All

Image Pulled within last: ● 30 Days ○ All

Name / Tag Pattern: *:latest

Type a value and press [Enter]

Schedule: 27 minute, 12 hour, * day (month), * month, * day (week)

User Timezone (IST)
At 12:27 PM
Next Scan: 2024-07-24 12:27:00

Server Timezone (UTC)
At 06:57 AM
Next Scan: 2024-07-24 06:57:00

Optionally, the following can be configured:

- Images to be scanned via
  - Regex
  - Update date
  - Pull date
- Scan schedule

- Click on Test Connection to verify and then Save

confidential and proprietary - limited distribution under NDA

View Results

- Navigate to Issues → Registry Scan to view the scanned registries
- Click on any of the images to view detailed scan results

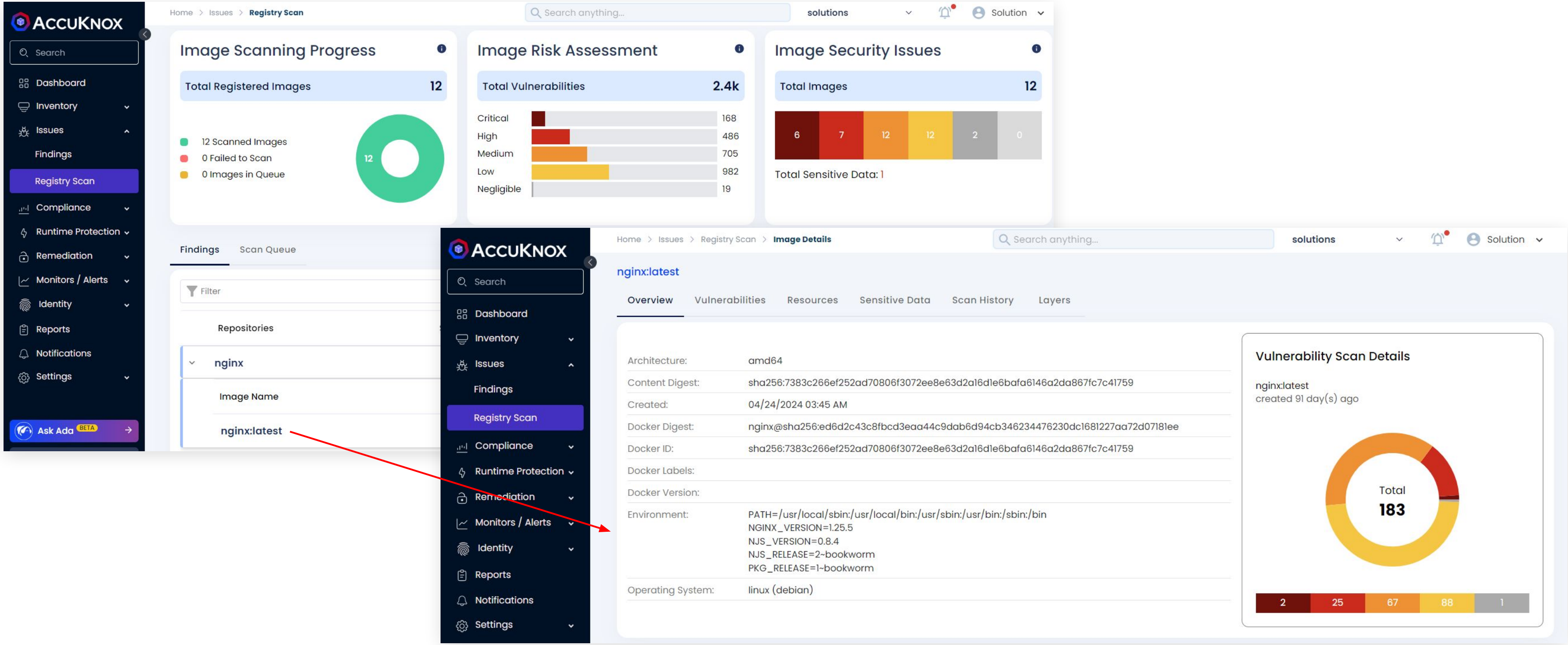


Image Scanning Progress

Total Registered Images	12

- 🟩 12 Scanned Images
- 🟥 0 Failed to Scan
- 🟨 0 Images in Queue

Image Risk Assessment

Total Vulnerabilities	2.4k
Critical	168
High	486
Medium	705
Low	982
Negligible	19

Image Security Issues

Total Images	12

6	7	12	12	2	0

Total Sensitive Data: 1

Repositories
nginx
Image Name
nginx:latest

nginx:latest

Architecture:	amd64
Content Digest:	sha256:7383c266ef252ad70806f3072ee8e63d2a16d1e6bafa6146a2da867fc7c41759
Created:	04/24/2024 03:45 AM
Docker Digest:	nginx@sha256:ed6d2c43c8fbcd3eaa44c9dab6d94cb346234476230dc1681227aa72d07181ee
Docker ID:	sha256:7383c266ef252ad70806f3072ee8e63d2a16d1e6bafa6146a2da867fc7c41759
Docker Labels:	
Docker Version:	

Environment:	PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
	NGINX_VERSION=1.25.5
	NJS_VERSION=0.8.4
	NJS_RELEASE=2~bookworm
	PKG_RELEASE=1~bookworm

Operating System:	linux (debian)

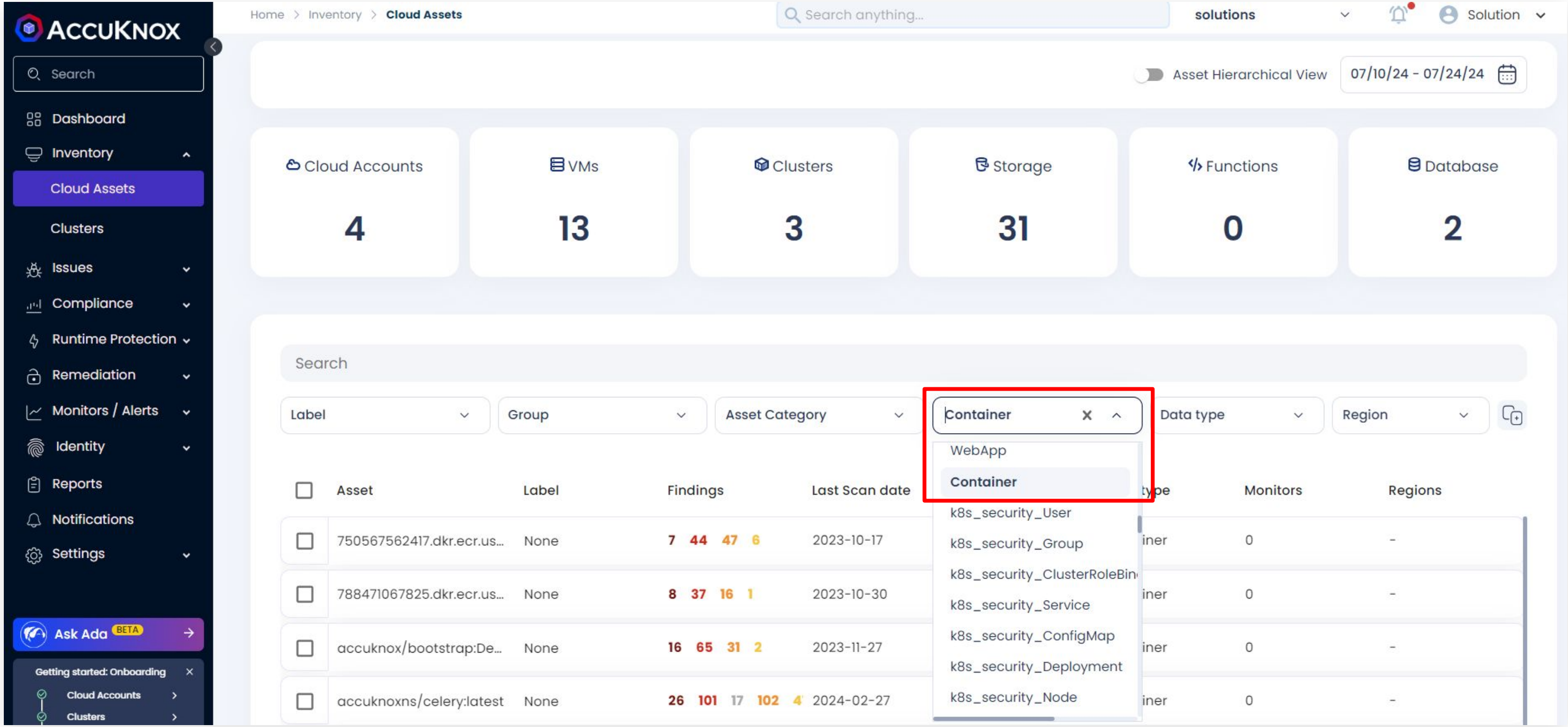
Vulnerability Scan Details

nginx:latest
created 91 day(s) ago

2	25	67	88	1

Inventory of Container Images

- Navigate to Inventory → Cloud Assets
- Filter Asset Type as Container to view list of all scanned images and associated findings



Home > Inventory > Cloud Assets

Asset Hierarchical View 07/10/24 - 07/24/24

Cloud Accounts	VMs	Clusters	Storage	Functions	Database
4	13	3	31	0	2

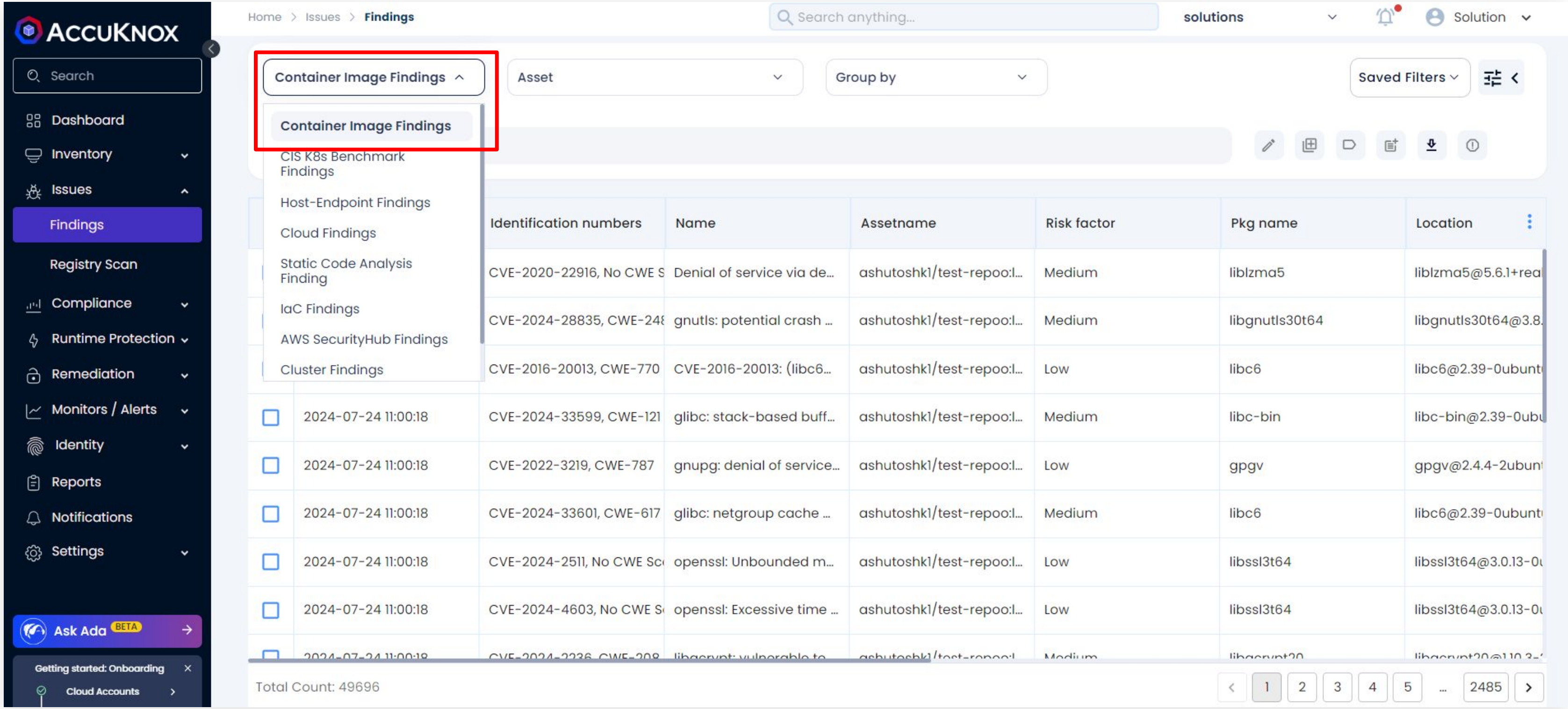
Search

Label | Group | Asset Category | Container | Data type | Region

□	Asset	Label	Findings	Last Scan date	type	Monitors	Regions
□	750567562417.dkr.ecr.us...	None	7 44 47 6	2023-10-17	iner	0	-
□	788471067825.dkr.ecr.us...	None	8 37 16 1	2023-10-30	iner	0	-
□	accuknox/bootstrap:De...	None	16 65 31 2	2023-11-27	iner	0	-
□	accuknoxns/celery:latest	None	26 101 17 102 4	2024-02-27	iner	0	-

View all Findings in Container Images

- Navigate to Issues → Findings
- Select top-left filter as Container Image Findings to get a list of all findings



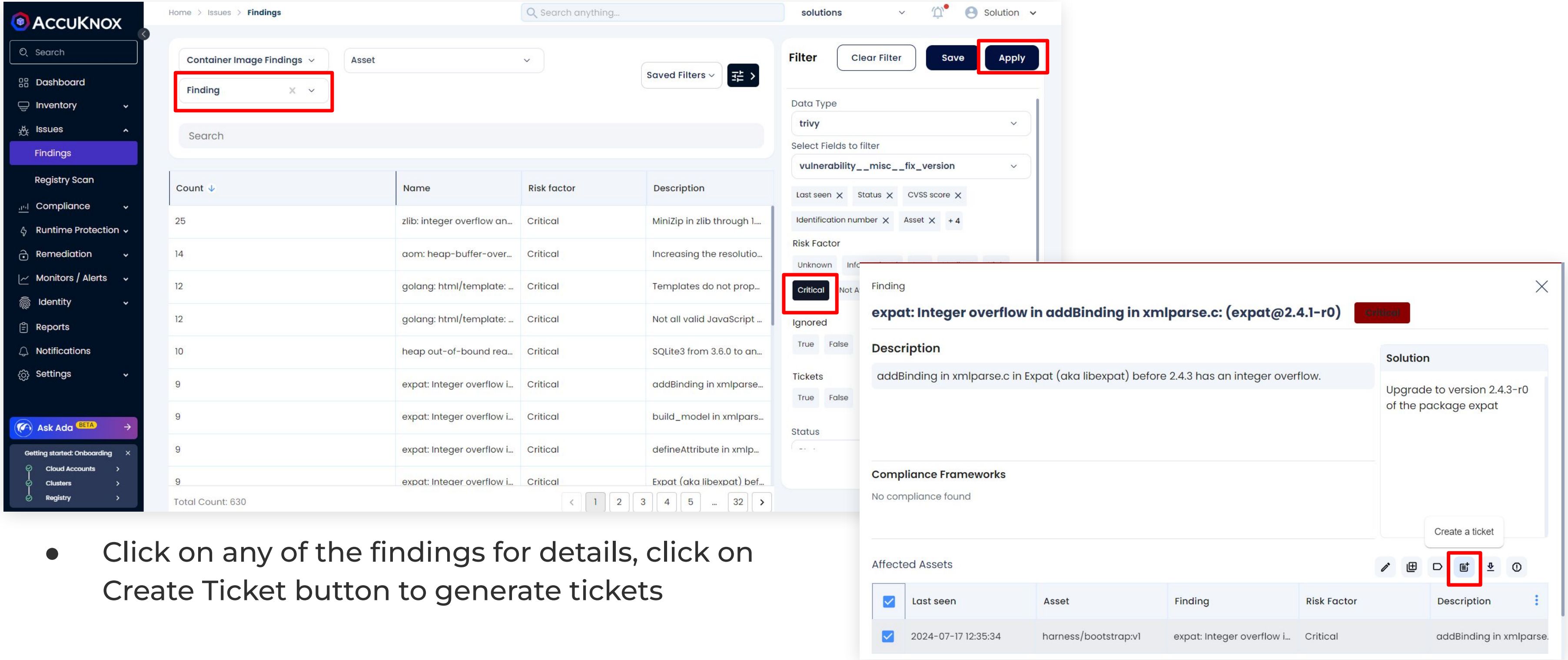
		Identification numbers	Name	Assetname	Risk factor	Pkg name	Location
		CVE-2020-22916, No CWE S	Denial of service via de...	ashutoshkl/test-repoo:l...	Medium	liblzma5	liblzma5@5.6.1+rea
		CVE-2024-28835, CWE-24	gnutls: potential crash ...	ashutoshkl/test-repoo:l...	Medium	libgnutls30t64	libgnutls30t64@3.8.
		CVE-2016-20013, CWE-770	CVE-2016-20013: (libc6...	ashutoshkl/test-repoo:l...	Low	libc6	libc6@2.39-0ubunt
□	2024-07-24 11:00:18	CVE-2024-33599, CWE-121	glibc: stack-based buff...	ashutoshkl/test-repoo:l...	Medium	libc-bin	libc-bin@2.39-0ubu
□	2024-07-24 11:00:18	CVE-2022-3219, CWE-787	gnupg: denial of service...	ashutoshkl/test-repoo:l...	Low	gpgv	gpgv@2.4.4-2ubun
□	2024-07-24 11:00:18	CVE-2024-33601, CWE-617	glibc: netgroup cache ...	ashutoshkl/test-repoo:l...	Medium	libc6	libc6@2.39-0ubunt
□	2024-07-24 11:00:18	CVE-2024-2511, No CWE Sc	openssl: Unbounded m...	ashutoshkl/test-repoo:l...	Low	libssl3t64	libssl3t64@3.0.13-0
□	2024-07-24 11:00:18	CVE-2024-4603, No CWE S	openssl: Excessive time ...	ashutoshkl/test-repoo:l...	Low	libssl3t64	libssl3t64@3.0.13-0
□	2024-07-24 11:00:18	CVE-2024-2236, CWE-208	libgcrypt: vulnerable to...	ashutoshkl/test-repoo:l	Medium	libgcrypt20	libgcrypt20@1.10.3-

Total Count: 49696

< 1 2 3 4 5 ... 2485 >

Work on Critical Findings in Container Images

- Select Group By as Findings
- In the Filters tab, select Critical under Risk Factor and click on Apply



Count	Name	Risk factor	Description
25	zlib: integer overflow an...	Critical	MiniZip in zlib through 1...
14	aom: heap-buffer-over...	Critical	Increasing the resolutio...
12	golang: html/template: ...	Critical	Templates do not prop...
12	golang: html/template: ...	Critical	Not all valid JavaScript ...
10	heap out-of-bound rea...	Critical	SQLite3 from 3.6.0 to an...
9	expat: Integer overflow i...	Critical	addBinding in xmlparse...
9	expat: Integer overflow i...	Critical	build_model in xmlpars...
9	expat: Integer overflow i...	Critical	defineAttribute in xmlp...
9	expat: Integer overflow i...	Critical	Expat (aka libexpat) bef...

Total Count: 630 ‹ 1 2 3 4 5 ... 32 ›

Data Type: trivy

Select Fields to filter: vulnerability__misc__fix_version

Last seen ✕ Status ✕ CVSS score ✕ Identification number ✕ Asset ✕ +4

Risk Factor: Unknown Inf... Critical Not A...

Ignored: True False

Tickets: True False

Status

Finding

expat: Integer overflow in addBinding in xmlparse.c: (expat@2.4.1-r0) Critical

Description

addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

Solution

Upgrade to version 2.4.3-r0 of the package expat

Compliance Frameworks

No compliance found

Affected Assets

☑	Last seen	Asset	Finding	Risk Factor	Description
☑	2024-07-17 12:35:34	harness/bootstrap:v1	expat: Integer overflow i...	Critical	addBinding in xmlparse.

- Click on any of the findings for details, click on Create Ticket button to generate tickets

AccuKnox

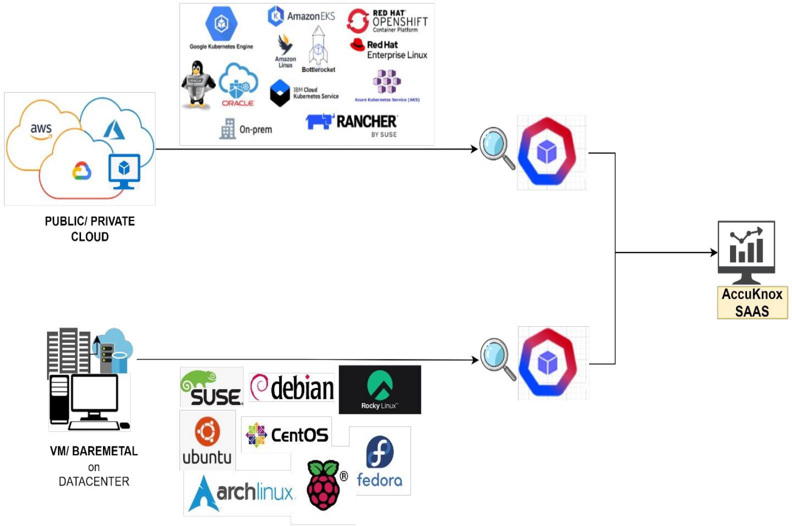
Forensics

How to perform Enhanced Forensics with eBPF and Splunk? [1]

ACCUKNOX

1- Telemetry Data Collection:

- **eBPF Instrumentation:**
    - KubeArmor uses eBPF (Extended Berkeley Packet Filter) to collect real-time data.
    - It Captures detailed telemetry, including:
        - **File Access Logs:** Records of all file interactions (reads, writes, modifications).
        - **Network Connections:** Details of network traffic, connections, and communications.
        - **Process Execution Logs:** Information about process start, stop, and activity.
    - It can generate:
        - **Audit** based Alerts
        - **Block** based Alerts
        - **Drift Detection** and Alerts



Telemetry Data Collection

Sample policies for aggregating telemetry events:

1- Process Based Telemetry

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-discovery-process-discovery
  namespace: wordpress-mysql
spec:
  tags: ["MITRE", "Discovery"]
  message: "Someone accessed running
process"
  selector:
    matchLabels:
      app: wordpress
  process:
    matchPaths:
      - path: /bin/ps
      - path: /usr/bin/ps
      - path: /usr/bin/pgrep
      - path: /usr/bin/top
      - path: /usr/bin/htop
    action: Audit
    severity: 5
```

2- File Based Telemetry

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: audit-for-system-paths
  namespace: wordpress-mysql
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /bin/
      readOnly: true
      recursive: true
      action: Audit
    - dir: /sbin/
      readOnly: true
      recursive: true
      action: Audit
    - dir: /usr/sbin/
      readOnly: true
      action: Audit
      recursive: true
    - dir: /usr/bin/
      readOnly: true
      recursive: true
      action: Audit
    - dir: /etc/
      readOnly: true
      recursive: true
      action: Audit
  severity: 5
  tags:
  - NIST
  - PCI-DSS
  message: Access to network files detected. Possible
violation of NIST Controls
  selector:
    matchLabels:
      app: mysql
```

3- Network Based Telemetry

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-nist-ac-18-1-network-audit
  namespace: wordpress-mysql
spec:
  severity: 3
  tags: ["NIST-800", "AC-18(1)", "Networking",
"Access", "NIST_SA", "NIST_SA-20",
"NIST_SA-20-Customized Development of Critical
Components", "SA"]
  message: "Access to network files detected.
Possible violation of NIST Controls"
  selector:
    matchLabels:
      app: wordpress
  file:
    matchPaths:
      - path: /proc/net/tcp
      - path: /proc/net/udp
      - path: /proc/net/icmp
      - path: /proc/net/snmp
      - path: /proc/net/route
      - path: /proc/net/dev
      - path: /var/log/syslog
      - path: /var/log/audit/audit.log
      - path: /etc/hostapd/hostapd.conf
      - path: /etc/network/if-up.d
  action: Audit
```

Telemetry Data Collection

Sample forensics data generated by the policies:

```
ClusterName: default
HostName: gke-cluster-1-default-pool-37f4c896-8cn6
NamespaceName: wordpress-mysql
PodName: wordpress-7c966b5d85-wvtln
Labels: app=wordpress
ContainerName: wordpress
ContainerID: 6d09394a988c5cf6b9fe260d28fdd57d6ff281618869a173965ecd94a3efac44
ContainerImage: docker.io/library/wordpress:4.8-apache@sha256:6216f64ab88fc51d311e38c7f69ca3f9aaba621492b4f1fa93ddf63093768845
Type: MatchedPolicy
PolicyName: ksp-nist-ac-18-1-network-audit
Severity: 3
Message: Access to network files detected. Possible violation of NIST Controls
Source: /bin/ls
Resource: /etc/network/if-up.d
Operation: File
Action: Audit
Data: syscall=SYS_OPENAT fd=-100 flags=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC
Enforcer: eBPF Monitor
Result: Passed
ATags: [NIST-800 AC-18(1) Networking Access NIST_SA NIST_SA-20 NIST_SA-20-Customized Development of Critical Components SA]
HostPID: 1.275441e+06
HostPPID: 1.275298e+06
Owner: map[Name:wordpress Namespace:wordpress-mysql Ref:Deployment]
PID: 342
PPID: 336
ParentProcessName: /bin/bash
ProcessName: /bin/ls
Tags: NIST-800,AC-18(1),Networking,Access,NIST_SA,NIST_SA-20,NIST_SA-20-Customized Development of Critical Components,SA
```

How to perform Enhanced Forensics with eBPF and Splunk? [2]

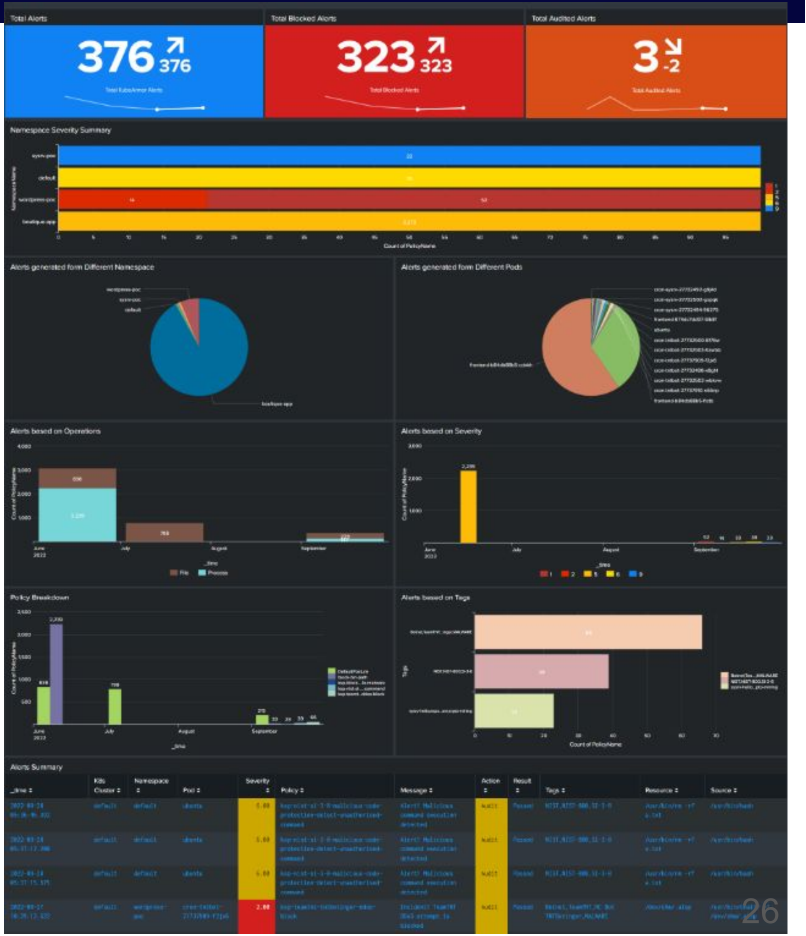
ACCUKNOX

2- Data Ingestion into Splunk:

- **Data Integration:**
  - By integrating splunk to Accuknox, eBPF-collected telemetry data is feeded into Splunk.

3- Reporting and Response:

- **Generate Reports:**
  - User can create detailed forensic reports highlighting findings and incident impacts.
- **Alert Configuration:**
  - User can set up alerts for immediate notification of suspicious activities or anomalies



Alerts Summary

_time	K8s Cluster	Namespace	Pod	Severity	Policy	Message	Action	Result	Tags	Resource	Source
2022-09-28 [illegible]	default	default	ubuntu	5.00	ksp-nist-si-3-8-malicious-code-protection-detect-unauthorized-command	Alert! Malicious command execution detected	Audit	Passed	[illegible]	/usr/bin/rm -rf a.txt	/usr/bin/bash
2022-09-28 [illegible]	default	default	ubuntu	5.00	ksp-nist-si-3-8-malicious-code-protection-detect-unauthorized-command	Alert! Malicious command execution detected	Audit	Passed	[illegible]	/usr/bin/rm -rf a.txt	/usr/bin/bash
2022-09-28 [illegible]	default	default	ubuntu	5.00	ksp-nist-si-3-8-malicious-code-protection-detect-unauthorized-command	Alert! Malicious command execution detected	Audit	Passed	[illegible]	/usr/bin/rm -rf a.txt	/usr/bin/bash
2022-09-27 [illegible]	default	wordpress-poc	[illegible]	2.00	[illegible]	[illegible]	Audit	Passed	[illegible]	[illegible]	[illegible]