ACCUKNOX | Gartner®

AccuKnox Zero Trust CNAPP

Compliance with Gartner Recommendations

Prevent Zero Day Attacks

as featured in:

aws ORACLE Gartner NEPHIO IBM LF EDGE

Table of Content

Executive Summary

Gartner authored 2 definitive documents on CNAPP in 2021 and 2023 . In our view these 2 documents cover virtually all aspects of CNAPP from a functional and technical perspective. Gartner's documents provide a very nice framework for customers and partners to evaluate different vendors, in a structured and holistic manner and make informed decisions.

At the outset we will provide a brief overview of AccuKnox CNAPP. In a subsequent section, we will address salient aspects of AccuKnox CNAPP and presents it in the context and framework as discussed in the Gartner documents[1].

[1] PLEASE NOTE: Our goal is not to paraphrase Gartner's documents. Readers would be best served by going through the in-depth documents authored by Gartner. Rather, this aims to present our capabilities in a framework, context and lexicon outlined by Gartner.

Overview

Kubernetes Pod security

Network separation and hardening

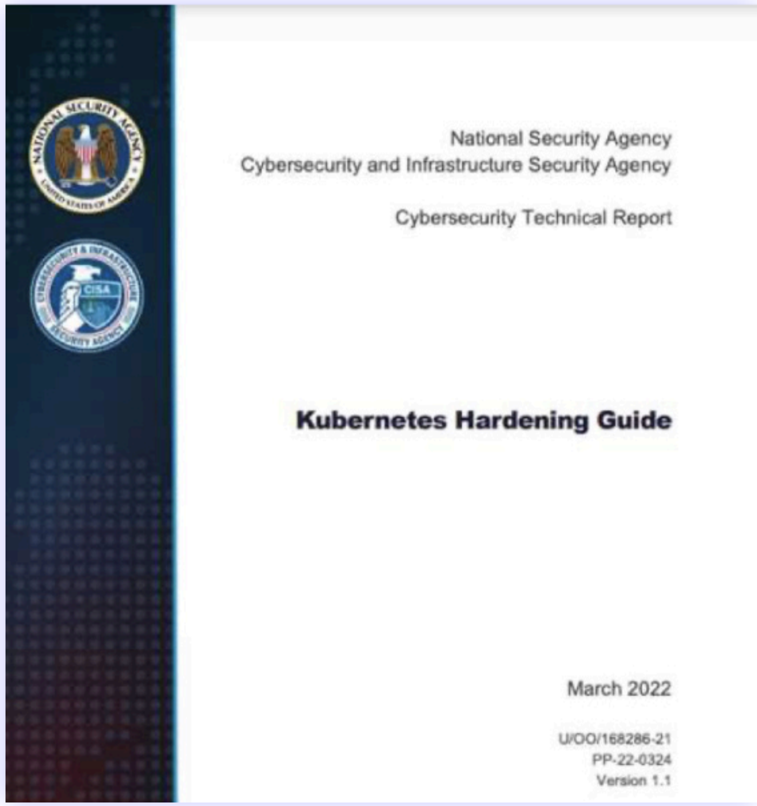
AccuKnox Zero Trust CNAPP - Overview

AccuKnox combines CNAPP capabilities with Zero Trust principles. Zero Trust principles include:

1. Assume a hostile cyber ecosystem
2. Presume you have been breached
3. Remove trust assumption for apps, libs, and infrastructure
4. Apply a least-permissive security policy against every application
5. Monitor every policy violation that the app performs

In summary, Zero Trust shifts the focus from trying to identify what is bad and stopping it, to identifying what is good and allowing it.

In order to implement Zero Trust principles AccuKnox implements some of the core principles outlined in Kubernetes run-time Security as outlined in US Department of Defense National Security Agency (NSA) Kubernetes Hardening Guide and CNCF Cloud Native Security White Paper



National Security Agency
Cybersecurity and Infrastructure Security Agency

Cybersecurity Technical Report

Kubernetes Hardening Guide

March 2022

U/OO/168286-21
PP-22-0324
Version 1.1

Kubernetes Pod security

- Use containers built to run applications as non-root users.
- Where possible, run containers with immutable file systems.
- Scan container images for possible vulnerabilities or misconfigurations.
- Use a technical control to enforce a minimum level of security including:
- Preventing privileged containers.
- Denying container features frequently exploited to breakout, such
- as hostPID, hostIPC, hostNetwork, allowedHostPath.
- Rejecting containers that execute as the root user or allow
- elevation to root.
- Hardening applications against exploitation using security services such as SELinux®, AppArmor®, and secure computing mode (seccomp).

CLOUD NATIVE COMPUTING FOUNDATION

CLOUD NATIVE SECURITY WHITEPAPER

May 2022

Runtime

The runtime environment of a container needs to be monitored and secured from a process, file, and network perspective. Only sanctioned capabilities and system calls (e.g. seccomp filters), should be allowed to execute or be invoked in a container by the host operating system. In some cases, the usage of sandboxing container runtimes is worth consideration to enable more strict host isolation. Changes to critical mount points and files should be monitored and prevented. Configuration must prevent changes to binaries, certificates, and remote access configurations. The configuration must also prevent ingress and egress network access for containers to only what is required to operate. Additionally, network traffic to malicious domains should be detected and denied.

Network separation and hardening

- Lock down access to control plane nodes using a firewall and role-based
- access control (RBAC). Use separate networks for the control plane
- components and nodes.
- Further limit access to the Kubernetes etcd server.
- Configure control plane components to use authenticated, encrypted
- communications using Transport Layer Security (TLS) certificates.
- Encrypt etcd at rest and use a separate TLS certificate for communication.
- Set up network policies to isolate resources. Pods and services in different
- namespaces can still communicate with each other unless additional
- separation is enforced.
- Create an explicit deny network policy.
- Place all credentials and sensitive information encrypted in Kubernetes Secrets rather than in configuration files. Encrypt Secrets using a strong encryption method. Secrets are not encrypted by default.

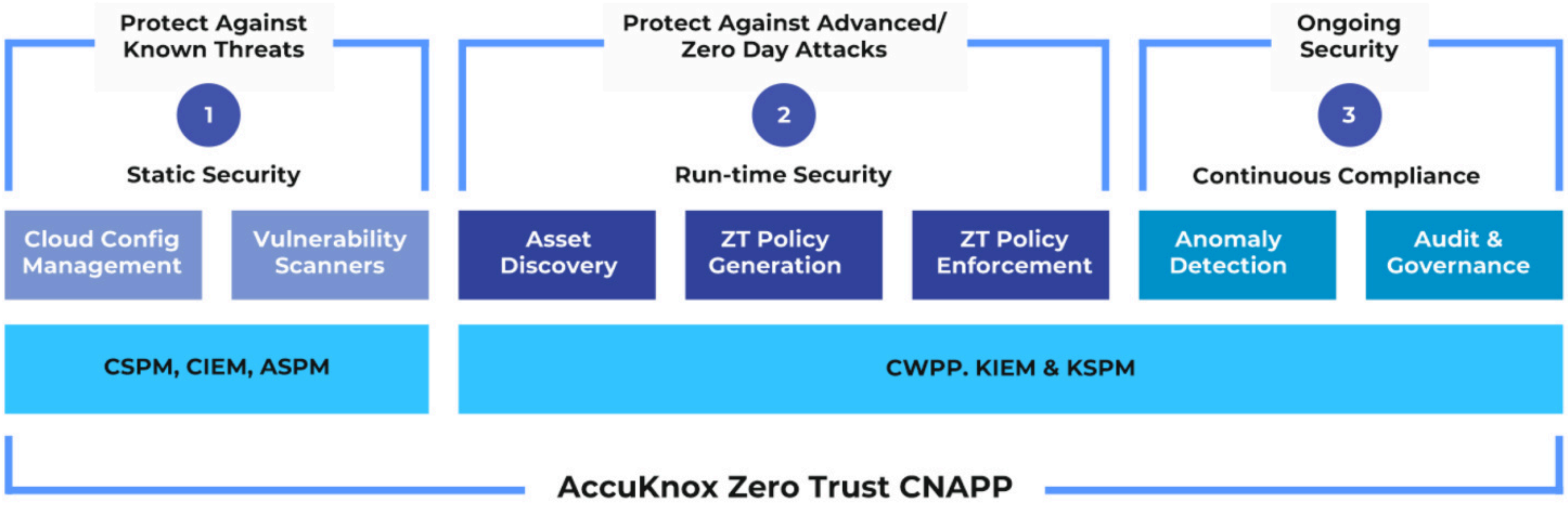
AccuKnox Zero Trust CNAPP combines

AccuKnox Zero Trust CNAPP combines:

- CSPM/KSPM - Cloud/Kubernetes Security Posture Management
- CWPP - Cloud Workload Protection Platform

Please Note: AccuKnox is currently developing CIEM/KIEM and this will be released in late Q3/early Q4 2023. The following is a high-level overview AccuKnox Zero Trust CNAPP.

Cloud Security at Scale with Runtime Protection



AccuKnox is a Core Contributor to KubeArmor, Zero Trust run-time security engine, a very popular CNCF project that has achieved 500,000+ downloads. KubeArmor leverages eBPF (Extended Berkeley Packet Filter) for observability and BPF-LSM, SELinux and AppArmor for Zero Trust Policy enforcement.
AccuKnox Enterprise run-time security engine is anchored on KubeArmor and delivers key areas that are needed in Enterprise Deployment:

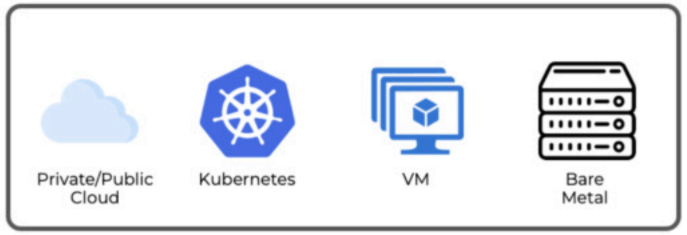
- Automated Zero Trust run-time policy generation
- Prioritization of vulnerabilities
- SIEM/SOAR integration
- Gitops integration
- Full UI/UX, Dashboards
- SAAS delivery, etc.

AccuKnox delivers flexible deployment options (Public Cloud, Private Cloud, Multi-Cloud) and secures a variety of workloads (K8, Virtual Machine, Functions/Services with a roadmap to support IoT/Edge, 5G, Data, etc.) because of its unique and differentiated competency in Kubernetes run-time security.

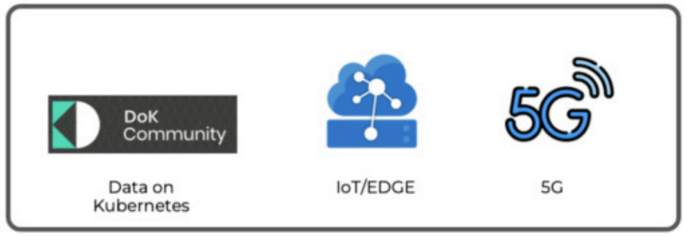
In summary, AccuKnox offers the following differentiated capabilities:

- Comprehensive Zero Trust CNAPP
- Core Contributor to KubeArmor: 500,000+ downloads, 500+ stars
- Enterprise offering anchored in KubeArmor
- Support for Public, Multi-Cloud and Private Clouds (on prem)
- Secure modern (Kubernetes) & traditional (Virtual Machine) workloads
- DevSecOps led
- Future proof roadmap: Support for IoT/Edge and 5G
- Proven track record of innovation:
- 10+ patents
- Incubated by SRI (previously Stanford Research International)
- On-going R&D partnership with SRI
- 5G Security R&D Award from NSF (National Science Foundation/US DoD
- Lighthouse Clients, Partners, 5G

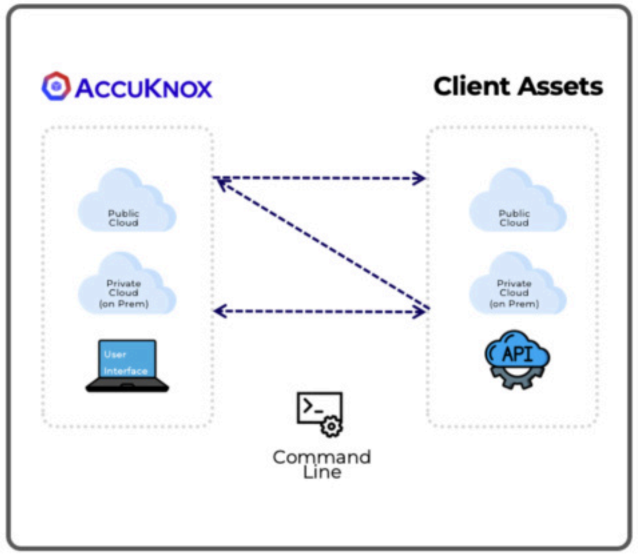
v1.0 Offering CNAPP



Roadmap



Support for Public & Private Cloud



Get a Demo

Mapping to Gartner CNAPP Guidelines

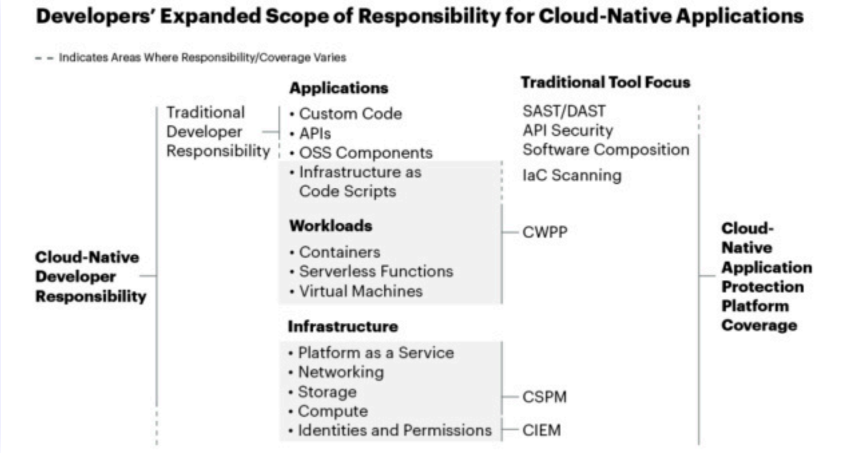
Get a Demo

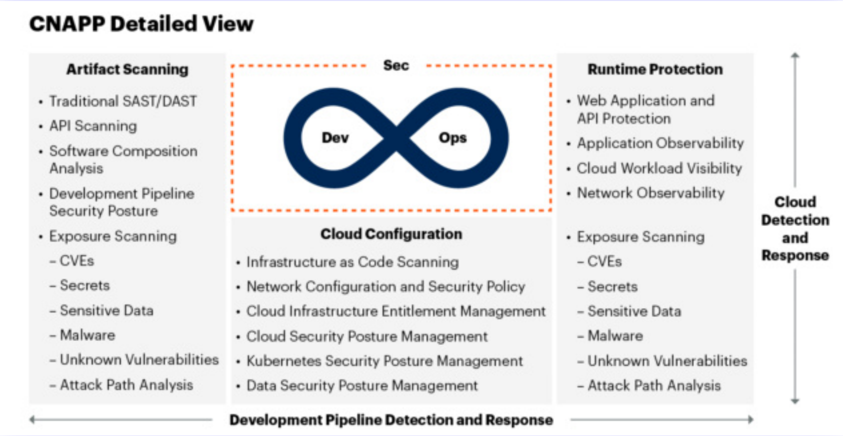
Mapping to Gartner CNAPP guidelines

Gartner discusses a number of the following areas that needs to be addressed in a CNAPP solution:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Cloud Identity Entitlement Management (CIEM)
- Their equivalents in Kubernetes: KSPM, KWPP, KIEM
- Container Lifecycle Security
- Software Supply Chain Security
  - Risk Based Prioritization
  - Forensics Intelligence
  - Anti-Malware Protection
  - Compliance and Configuration Drift
  - Vulnerability Management
  - Scalability and Performance
  - Non-intrusive Deployment
  - Flexible Integration with Workflow and Tools and more..

This following 2 diagrams provide a snapshot of key components of CNAPP


Developers' Expanded Scope of Responsibility for Cloud-Native Applications
- - Indicates Areas Where Responsibility/Coverage Varies
Cloud-Native Developer Responsibility
Traditional Developer Responsibility
Applications
• Custom Code
• APIs
• OSS Components
• Infrastructure as Code Scripts
Workloads
• Containers
• Serverless Functions
• Virtual Machines
Infrastructure
• Platform as a Service
• Networking
• Storage
• Compute
• Identities and Permissions
Traditional Tool Focus
SAST/DAST
API Security
Software Composition
IaC Scanning
CWPP
CSPM
CIEM
Cloud-Native Application Protection Platform Coverage


CNAPP Detailed View
Artifact Scanning
• Traditional SAST/DAST
• API Scanning
• Software Composition Analysis
• Development Pipeline Security Posture
• Exposure Scanning
– CVEs
– Secrets
– Sensitive Data
– Malware
– Unknown Vulnerabilities
– Attack Path Analysis
Sec
Dev
Ops
Cloud Configuration
• Infrastructure as Code Scanning
• Network Configuration and Security Policy
• Cloud Infrastructure Entitlement Management
• Cloud Security Posture Management
• Kubernetes Security Posture Management
• Data Security Posture Management
Runtime Protection
• Web Application and API Protection
• Application Observability
• Cloud Workload Visibility
• Network Observability
• Exposure Scanning
– CVEs
– Secrets
– Sensitive Data
– Malware
– Unknown Vulnerabilities
– Attack Path Analysis
Cloud Detection and Response
Development Pipeline Detection and Response

Source: Gartner

Summary of Gartner's viewpoints

The following is a high-level summary of Gartner’s viewpoints:

- CNAPP offerings bring together multiple disparate security and protection capabilities into a single platform focused on identifying and prioritizing excessive risk of the entire cloud-native application and its associated infrastructure.
- Optimal security of cloud-native applications requires an integrated approach that starts in development and extends to runtime protection. SRM leaders should evaluate emerging cloud-native application protection platforms that provide a complete life cycle approach for security.
- Developers are increasingly responsible for operational tasks, such as addressing vulnerabilities, deploying infrastructure as code, and deploying and tearing down implementations in production, thus requiring tools that address this expanded scope.
- Because security is often viewed as an obstacle to developers it is absolutely critical to prioritize risks identified and provide sufficient context for the developer to remediate it.

As a security and risk management (SRM) leader responsible for infrastructure security, you should:

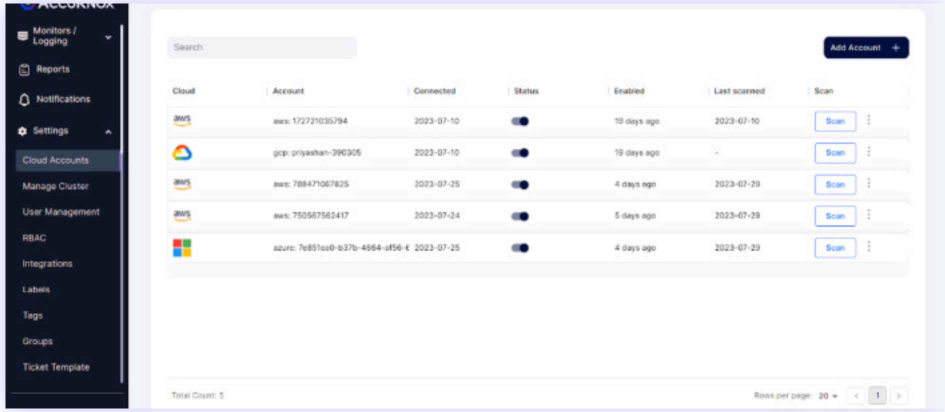
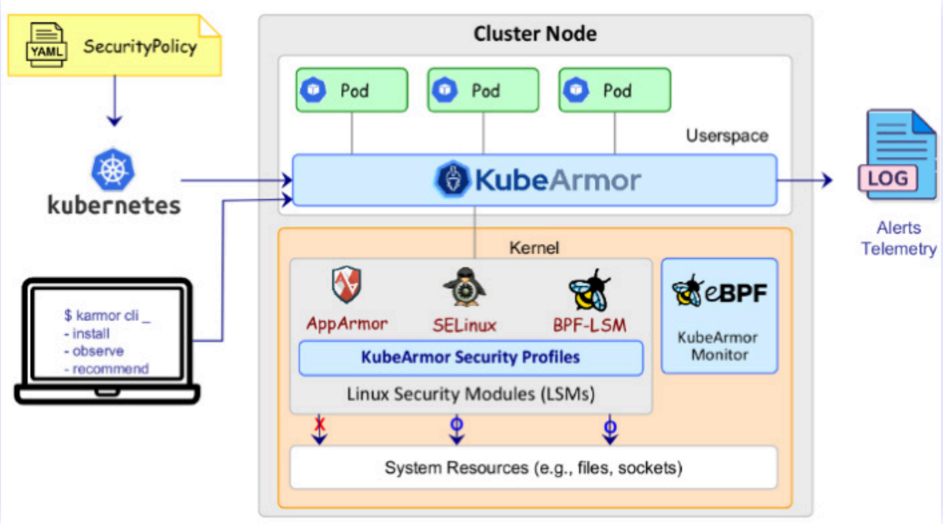
- Implement an integrated security approach that covers the entire life cycle of cloud-native applications, starting in development and extending into production.
- Integrate security into the developer’s toolchain so that security testing is automated as code is created and moves through the development pipeline, reducing the friction of adoption.
- Acknowledge that perfect apps aren’t possible and focus developers on highest severity, highest confidence and highest risk vulnerabilities to avoid wasting developer’s time.
- Scan development artifacts and cloud configuration comprehensively and combine this with runtime visibility and configuration awareness in order to prioritize risk remediation.
- Reduce complexity and improve the developer experience by choosing integrated CNAPP offerings that provide complete life cycle visibility and protection of cloud-native applications across development and staging and into runtime operation.
- Favor CNAPP vendors that provide a variety of runtime visibility techniques, including traditional agents, Extended Berkeley Packet Filter (eBPF) support, snapshotting, privileged containers and Kubernetes K8s integration to provide the most flexibility at deployment

Gartner Recommendations for CNAPP

- Infrastructure
- Application Security
- Policy Governance
- Runtime Security
- Registry Scan
- Deployment
- Forensics
- Ease of Use
- Pricing and Licensing
- Integration with Tools
- GRC

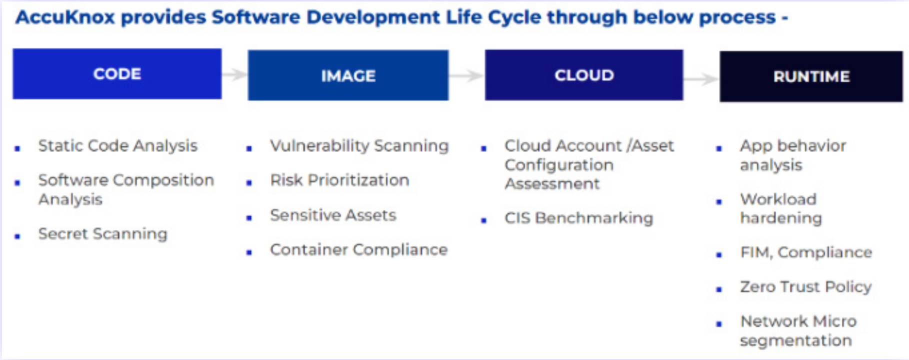
Gartner Recommendations for Cloud-Native Application Protection Platforms

Gartner's CNAPP recommendations give fundamental instructions for enterprises to effectively secure their cloud-native apps agnostic to underlying infrastructure. These recommendations address the specific issues of cloud-native apps, such as their dynamic nature, microservices design, and continuous deployment. They supply perspectives into key security capabilities to prioritize, guaranteeing security threats, data protection, industry compliance, and user and stakeholder confidence. Here are the top recommendations from Gartner along with how AccuKnox goes above and beyond to fulfill it.

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
Infrastructure	Major Cloud Providers	AccuKnox provides multi-cloud security with coverage to all major cloud providers such as AWS, AZURE & GCP. We also additionally support GCP, Oracle Cloud and Private Cloud platforms like VMWare, OpenStack etc. Visit help to know more.	
Application Security	Application layer observability/monitoring	AccuKnox built KubeArmor (now a CNCF donated sandbox project) which leverage eBPF for observability of App Behavior and automatically discovers Zero Trust Least permissive Policies	

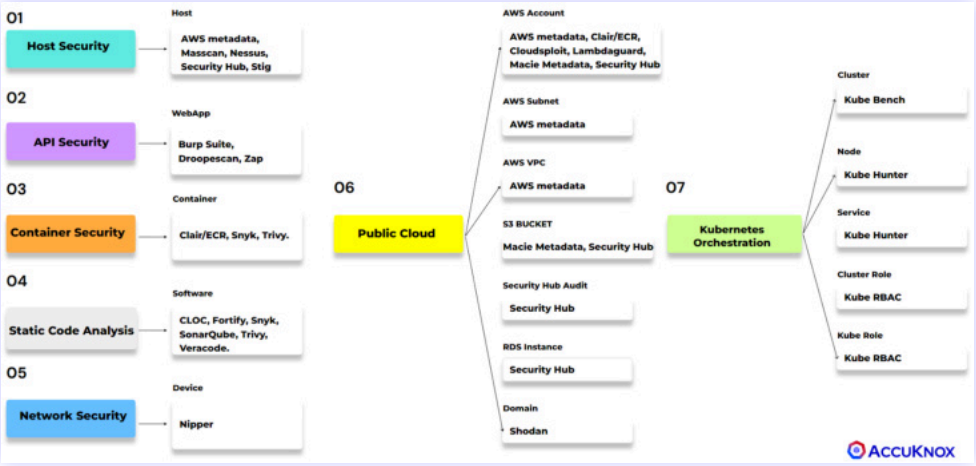
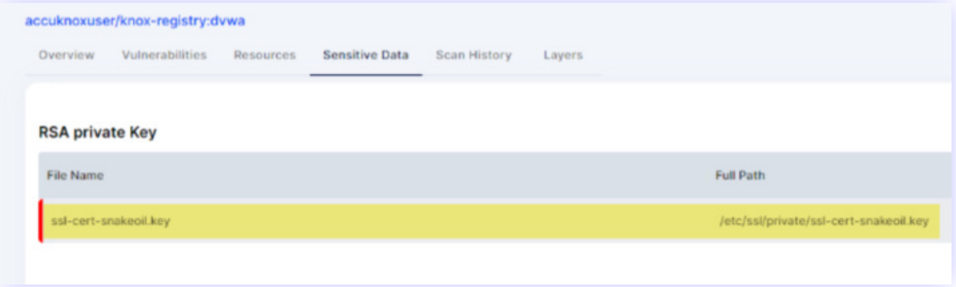
Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	●	19 days ago	2023-07-10	Scan
	gcp: priyashan-390305	2023-07-10	●	19 days ago	-	Scan
aws	aws: 788471067825	2023-07-25	●	4 days ago	2023-07-29	Scan
aws	aws: 750567562417	2023-07-24	●	5 days ago	2023-07-29	Scan
	azure: 7e851ea0-b37b-4664-af56-€	2023-07-25	●	4 days ago	2023-07-29	Scan

Total Count: 5

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Support for VMware-based infrastructure (on-premises and public-cloud-based)	AccuKnox provides security for on-prem infrastructure such as VMware, private cloud such as IBM Private Cloud, Openshift and public cloud infrastructure.	
	Support for other cloud and container environments such as Red Hat OpenShift and SUSE's Rancher		
	Traditional static analysis of custom code for unknown vulnerabilities	AccuKnox analyzes source code for potential security vulnerabilities without at development stage for finding common CVE, coding errors, security best practices and it can also help to fail the build early in CI pipeline to save cost and effort	
	Traditional dynamic scanning for unknown vulnerabilities	AccuKnox can not just detect unknown vulnerabilities or zero-day attacks but can actually prevent it from execution. It can assess and generate default posture of application and can prevent any anomaly that could potentially be an attack through its one of a kind in-line mitigation approach using LSMs	

AccuKnox provides Software Development Life Cycle through below process -

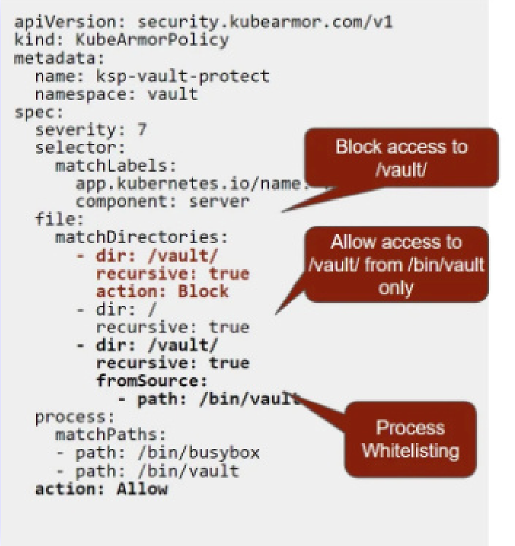
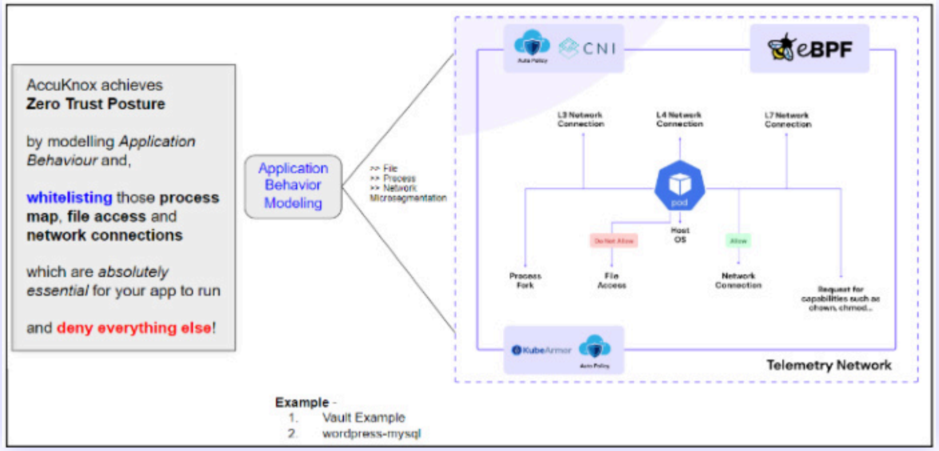
CODE	IMAGE	CLOUD	RUNTIME
Static Code Analysis	Vulnerability Scanning	Cloud Account /Asset Configuration Assessment	App behavior analysis
Software Composition Analysis	Risk Prioritization	CIS Benchmarking	Workload hardening
Secret Scanning	Sensitive Assets		FIM, Compliance
	Container Compliance		Zero Trust Policy
			Network Micro segmentation

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	API scanning for unknown vulnerabilities	AccuKnox can detect application attack scenarios at running app to find vulnerabilities of application post-deployment based on OWASP Top10 for finding common CVE and security best practices	
	Development pipeline/ software supply chain security beyond SCA (see Note 4)	AccuKnox can help to detect 3rd party dependencies/lib in open source which are used during dev, test or production to identify vulnerable 3rd party software and identify open-source component risks. Protecting against supply chain attacks.	
	Development pipeline hardening	AccuKnox can help to detect vulnerability early in the CI pipeline using its static code analysis, software composition analysis and secret scanning. Vulnerabilities that are detected are prioritized based on the runtime context and exploitability	
Policy Governance	Sensitive data in structured data repositories	AccuKnox can detect hard coded secrets in repositories and can fail a build in the CI pipeline	

accuknoxuser/knox-registry:dvwa

RSA private Key

File Name	Full Path
ssl-cert-snakeoil.key	/etc/ssl/private/ssl-cert-snakeoil.key

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Single Security Policy for All Artifacts	AccuKnox streamlines security policies across all components of the application. No matter if it's a container, a VM, a serverless function, or storage. The rules remain consistent. Ensure a uniform set of rules for everyone in the organization. See example policies.	
Runtime Security	Extended Berkeley Packet Filter (eBPF) support.	Our solutions leverage eBPF for kernel events and LSMs for enforcement. This makes visibility into runtime activities that much easier. Our architecture (eBPF - Extended Berkeley Packet Filter based) is one of the most efficient Cloud Native architectures. It is used to support Facebook's Katran Load Balancer, one of the largest in the world. Consequently we don't have architectural and performance limitations of older legacy Cloud Security platform architectures	

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-vault-protect
  namespace: vault
spec:
  severity: 7
  selector:
    matchLabels:
      app.kubernetes.io/name:
      component: server
  file:
    matchDirectories:
      - dir: /vault/
        recursive: true
        action: Block
      - dir: /
        recursive: true
      - dir: /vault/
        recursive: true
        fromSource:
          - path: /bin/vault
  process:
    matchPaths:
    - path: /bin/busybox
    - path: /bin/vault
  action: Allow
```

AccuKnox achieves **Zero Trust Posture**

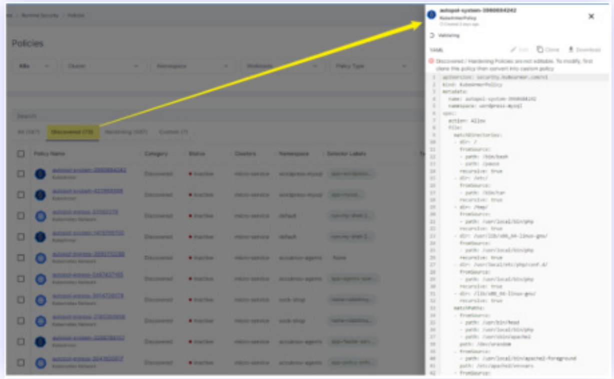
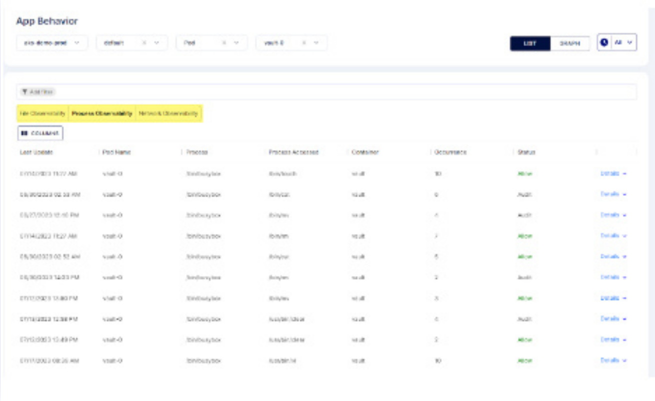
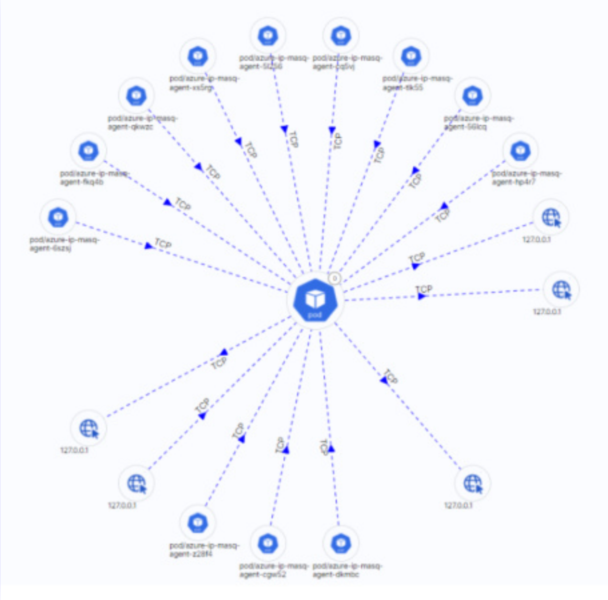
by modelling *Application Behaviour* and,

whitelisting those **process map**, **file access** and **network connections**

which are *absolutely essential* for your app to run

and **deny everything else**!

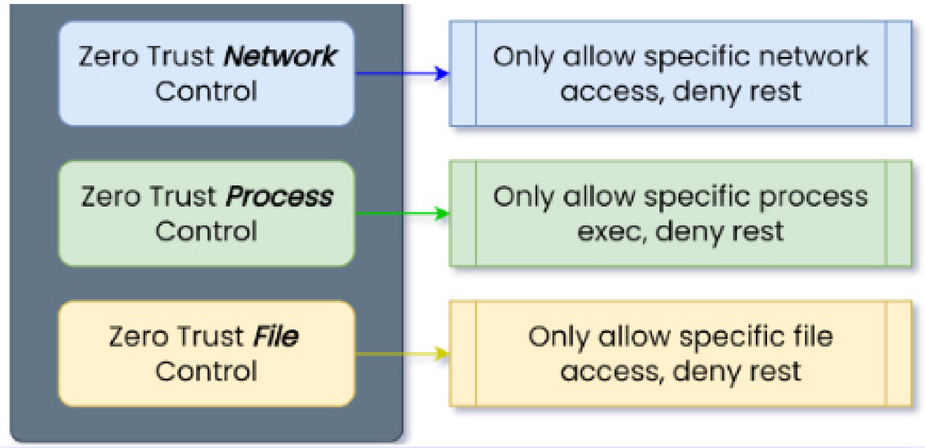
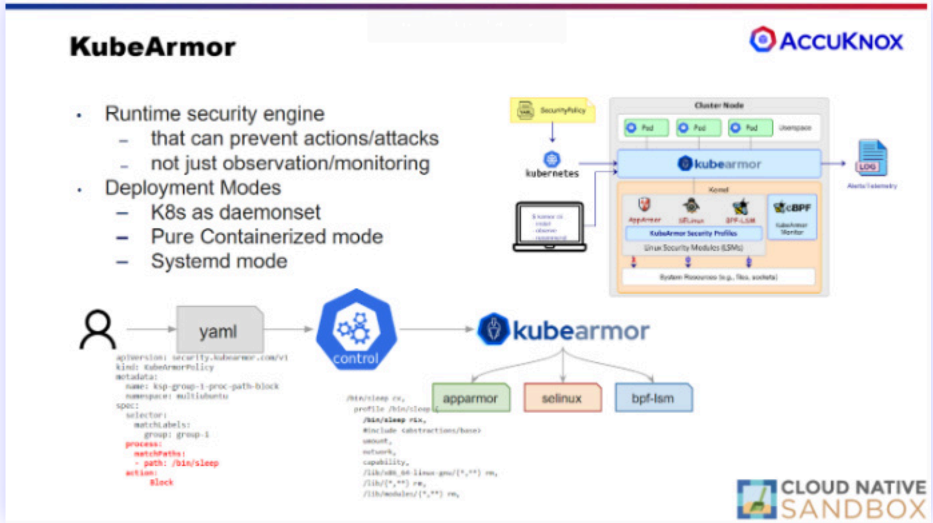
Example -
1. Vault Example
2. wordpress-mysql

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Deep Knowledge of Application Elements	Our CNAPP makes sense of connections between application components deep at kernel-level. Think of it as an astute investigator who understands how everything in your application meshes together. Nothing falls through the gaps.	
	Runtime visibility into virtual machine (VM) and container workloads.	AccuKnox CNAPP protects pure-containerized, Kubernetes, VM, and Bare Metal environments. Top-notch security solutions for diverse infrastructures across various deployment scenarios. We leverage eBPF for monitoring of the workloads at kernel level and provide rich telemetry of the application behavior in an aggregated view 	

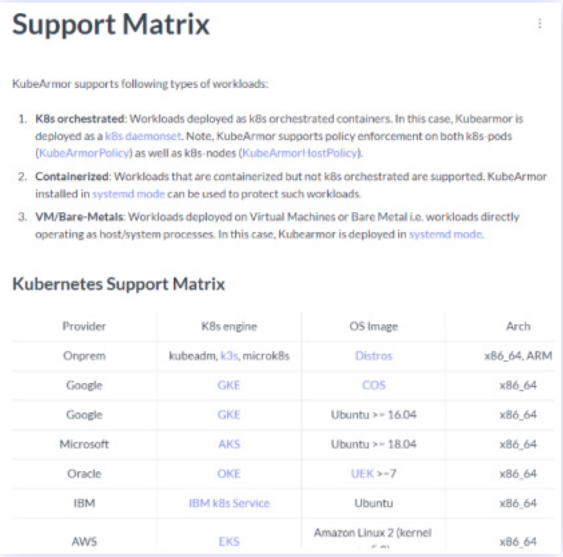
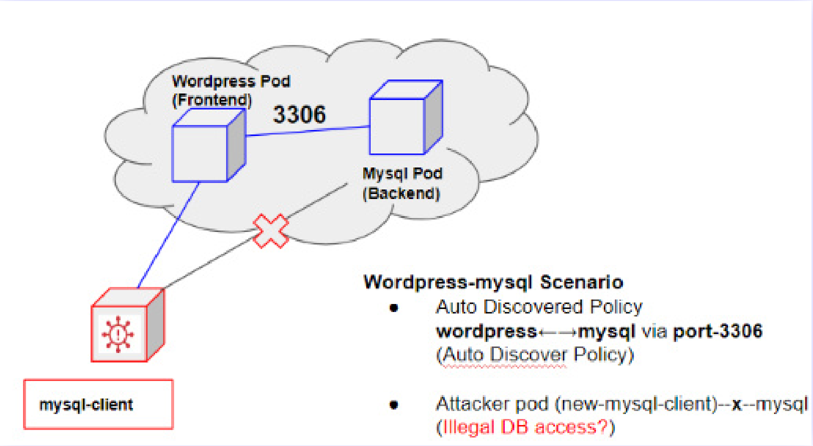
App Behavior

Last Update	Pod Name	Process	Process Accessed	Container	Occurrence	Status	
[illegible]	vault-0	/bin/busybox	[illegible]	vault	10	Allow	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	[illegible]	Audit	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	[illegible]	Audit	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	7	Allow	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	5	Allow	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	2	Audit	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	3	Allow	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	[illegible]	Audit	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	2	Allow	Details
[illegible]	vault-0	/bin/busybox	[illegible]	vault	10	Allow	Details

pod/azure-ip-masq-agent-5l2s6
pod/azure-ip-masq-agent-cq5vj
pod/azure-ip-masq-agent-xs5rg
pod/azure-ip-masq-agent-tlk55
pod/azure-ip-masq-agent-qkwzc
pod/azure-ip-masq-agent-56lcq
pod/azure-ip-masq-agent-fkq4b
pod/azure-ip-masq-agent-hp4r7
pod/azure-ip-masq-agent-6szsj
127.0.0.1
TCP
pod
pod/azure-ip-masq-agent-z28f4
pod/azure-ip-masq-agent-cgw52
pod/azure-ip-masq-agent-dkmbc

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Runtime visibility techniques like traditional agents	AccuKnox insights help you to understand what exactly is happening to your workload at runtime by providing visibility into: • What network connections have been established and across what ports; • What process forking is happening and by how many times • What files were accessed, directories, and how many times • What processes have even attempted network connections?	 Zero Trust ***Network*** Control → Only allow specific network access, deny rest Zero Trust ***Process*** Control → Only allow specific process exec, deny rest Zero Trust ***File*** Control → Only allow specific file access, deny rest
	Mentions LD_PRELOAD: Linux System Call Interception	AccuKnox employs Linux Security Modules (LSMs) which is an even more efficient and effective approach for intercepting system calls, enhancing container security, and mitigating zero-day attacks at kernel level. However, LD_PRELOAD is only relevant from user-level which will allow attack to execute in some cases if there is any unknown vulnerabilities	 **KubeArmor** • Runtime security engine – that can prevent actions/attacks – not just observation/monitoring • Deployment Modes – K8s as daemonset – Pure Containerized mode – Systemd mode apiVersion: security.kubearmor.com/v1 kind: KubeArmorPolicy metadata: name: ksp-group-1-proc-path-block namespace: multiubuntu spec: selector: matchLabels: group: group-1 process: matchPaths: - path: /bin/sleep action: Block /bin/sleep rx, profile /bin/sleep { /bin/sleep rix, #include <abstractions/base> umount, network, capability, /lib/x86_64-linux-gnu/{*,**} rm, /lib/{*,**} rm, /lib/modules/{*,**} rm,

Get a Demo

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Recommends use of DaemonSets for securing application	AccuKnox deploys KubeArmor as a DaemonSet on nodes. Full security monitoring and policy enforcement across the Kubernetes cluster	
	Network connectivity mapping and real-time workload visibility for critical VMs and containers.	AccuKnox provides micro-segmentation in cloud workload security to enhance network security and protect workloads from lateral movement and unauthorized access. It involves dividing a network into smaller segments, or microsegments, and applying security policies to control communication between these segments.	

Support Matrix

KubeArmor supports following types of workloads:

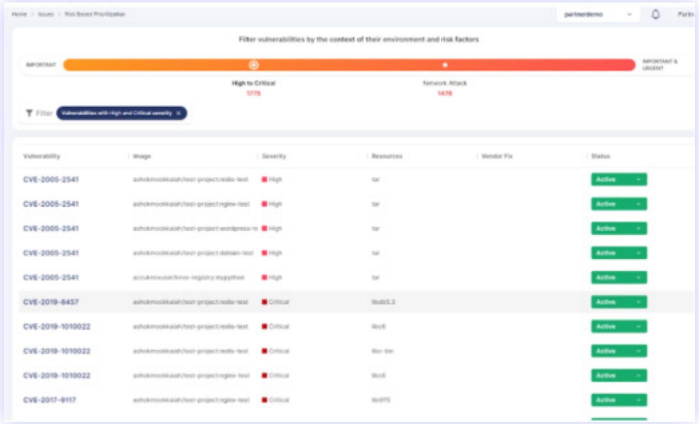
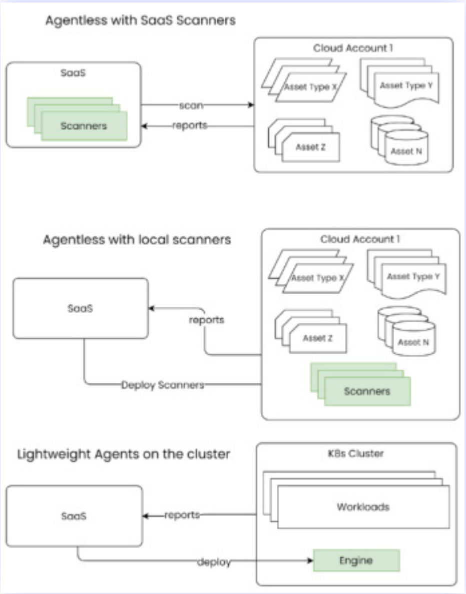
1. **K8s orchestrated**: Workloads deployed as k8s orchestrated containers. In this case, Kubearmor is deployed as a k8s daemonset. Note, KubeArmor supports policy enforcement on both k8s-pods (KubeArmorPolicy) as well as k8s-nodes (KubeArmorHostPolicy).
2. **Containerized**: Workloads that are containerized but not k8s orchestrated are supported. KubeArmor installed in systemd mode can be used to protect such workloads.
3. **VM/Bare-Metals**: Workloads deployed on Virtual Machines or Bare Metal i.e. workloads directly operating as host/system processes. In this case, Kubearmor is deployed in systemd mode.

Kubernetes Support Matrix

Provider	K8s engine	OS Image	Arch
Onprem	kubeadm, k3s, microk8s	Distros	x86_64, ARM
Google	GKE	COS	x86_64
Google	GKE	Ubuntu >= 16.04	x86_64
Microsoft	AKS	Ubuntu >= 18.04	x86_64
Oracle	OKE	UEK >=7	x86_64
IBM	IBM k8s Service	Ubuntu	x86_64
AWS	EKS	Amazon Linux 2 (kernel	x86_64

Wordpress-mysql Scenario

- Auto Discovered Policy **wordpress←→mysql** via **port-3306** (Auto Discover Policy)
- Attacker pod (new-mysql-client)--**x**--mysql (Illegal DB access?)

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
Registry Scan	Scanning of containers and container registries for risk assessment	AccuKnox helps in prioritizing vulnerability across container image scan, secrets information, sensitive data, or malware through runtime context. The risk scanning is by deploying scanners in an agentless way and provide the workload security posture It supports container and registry scanning for risk assessment. Get proactive security measures and risk mitigation strategies for containerized applications. We support Nexus, ECR, GCR, DockerHub etc.	
Deployment	Agentless workload scanning as a core capability.	AccuKnox provides best of the worlds i.e., it leverages agentless scanning for cloud account findings, vulnerability scanning, asset inventory etc. For runtime it uses a lightweight agent that is no different that how all the CNIs operate in the k8s cluster today. AccuKnox solution does not require any changes in the actual workload pods/ containers itself i.e., it does not use sidecar models nor does it inject any sensors/agents inside the actual workload pods/containers.	

Home > Issues > Risk Based Prioritization

partnerdemo

Filter vulnerabilities by the context of their environment and risk factors

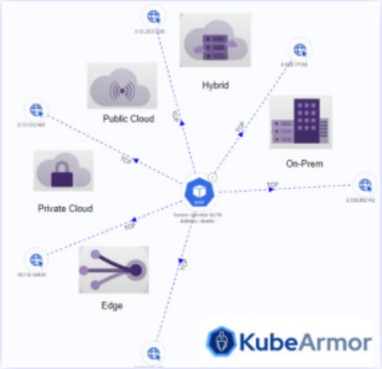
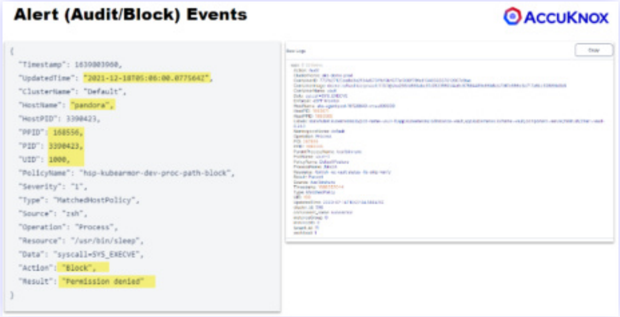
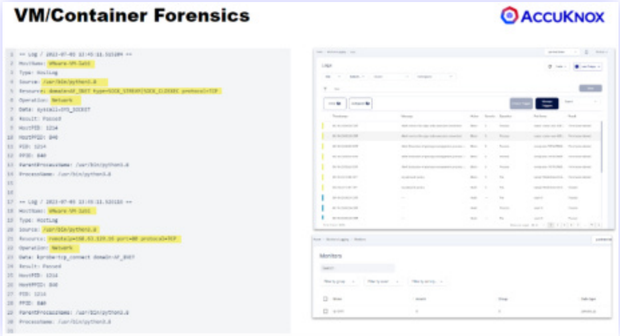
IMPORTANT — IMPORTANT & URGENT

High to Critical 1775

Network Attack 1476

Filter: Vulnerabilities with High and Critical severity ×

Vulnerability	Image	Severity	Resources	Vendor Fix	Status
CVE-2005-2541	ashokmookkaiah/test-project:redis-test	🟥 High	tar		Active
CVE-2005-2541	ashokmookkaiah/test-project:nginx-test	🟥 High	tar		Active
CVE-2005-2541	ashokmookkaiah/test-project:wordpress-te	🟥 High	tar		Active
CVE-2005-2541	ashokmookkaiah/test-project:debian-test	🟥 High	tar		Active
CVE-2005-2541	accuknoxuser/knox-registry:mypython	🟥 High	tar		Active
CVE-2019-8457	ashokmookkaiah/test-project:redis-test	🟥 Critical	libdb5.3		Active
CVE-2019-1010022	ashokmookkaiah/test-project:redis-test	🟥 Critical	libc6		Active
CVE-2019-1010022	ashokmookkaiah/test-project:redis-test	🟥 Critical	libc-bin		Active
CVE-2019-1010022	ashokmookkaiah/test-project:nginx-test	🟥 Critical	libc6		Active
CVE-2017-9117	ashokmookkaiah/test-project:nginx-test	🟥 Critical	libtiff5		Active

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Adaptable Deployment	AccuKnox offers one of the most flexible deployment options: Public Cloud, Private Cloud, Multi-Cloud. We have one of the most flexible architecture which allows us to offer a durable roadmap that covers Zero Trust Security for IoT/ Edge and 5G workloads • Hybrid/Multi Cloud • On-prem/DC • Public Cloud • Private Cloud • Edge Workload • 5G workloads	 AccuKnox App Behavior Network Graph View  Alert (Audit/Block) Events
Forensics	Deep understanding of Application Elements	AccuKnox can detect and aggregate your application behavior at process level granularity. It discovers your current posture of your application and automatically captures the logs for process executed, file accessed and network connections made in the application at real-time. Continuous monitoring of the same helps in creating governing policies of the default posture.	 VM/Container Forensics

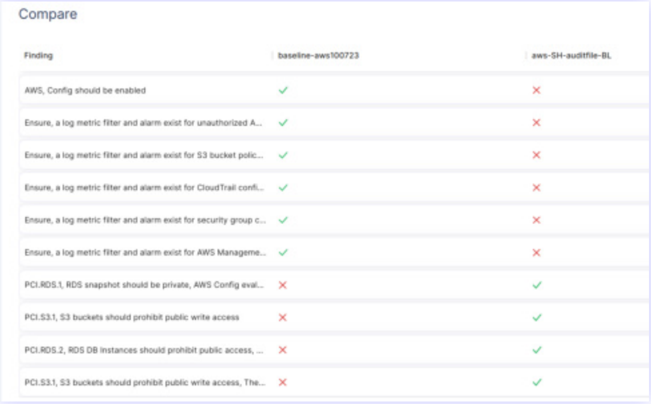
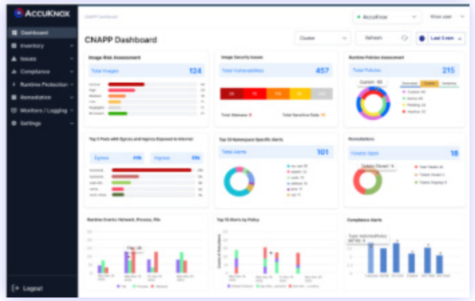
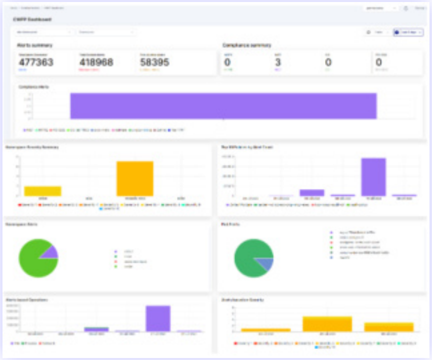
Alert (Audit/Block) Events

```
{
  "Timestamp": 1639803960,
  "UpdatedTime": "2021-12-18T05:06:00.077564Z",
  "ClusterName": "Default",
  "HostName": "pandora",
  "HostPID": 3390423,
  "PPID": 168556,
  "PID": 3390423,
  "UID": 1000,
  "PolicyName": "hsp-kubearmor-dev-proc-path-block",
  "Severity": "1",
  "Type": "MatchedHostPolicy",
  "Source": "zsh",
  "Operation": "Process",
  "Resource": "/usr/bin/sleep",
  "Data": "syscall=SYS_EXECVE",
  "Action": "Block",
  "Result": "Permission denied"
}
```

VM/Container Forensics

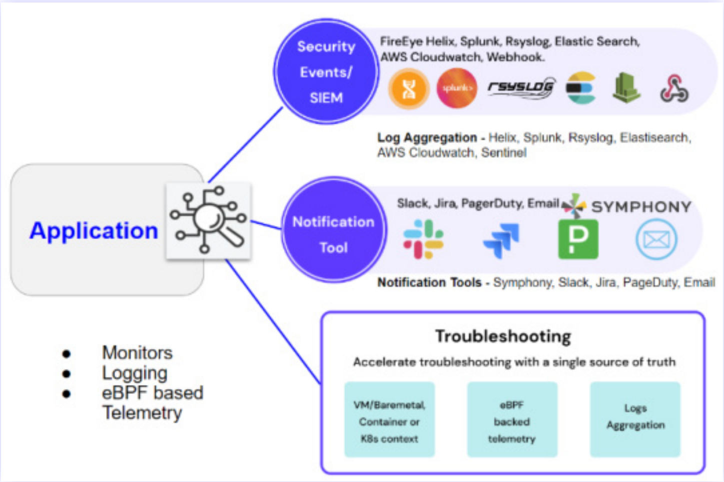
```
== Log / 2023-07-05 11:45:11.515184 ==
HostName: VMware-VM-1a01
Type: HostLog
Source: /usr/bin/python3.8
Resource: domain=AF_INET type=SOCK_STREAM|SOCK_CLOEXEC protocol=TCP
Operation: Network
Data: syscall=SYS_SOCKET
Result: Passed
HostPID: 1214
HostPPID: 840
PID: 1214
PPID: 840
ParentProcessName: /usr/bin/python3.8
ProcessName: /usr/bin/python3.8


== Log / 2023-07-05 11:45:11.520118 ==
HostName: VMware-VM-1a01
Type: HostLog
Source: /usr/bin/python3.8
Resource: remoteip=158.43.129.35 port=80 protocol=TCP
Operation: Network
Data: kprobe=tcp_connect domain=AF_INET
Result: Passed
HostPID: 1214
HostPPID: 840
PID: 1214
PPID: 840
ParentProcessName: /usr/bin/python3.8
ProcessName: /usr/bin/python3.8
```

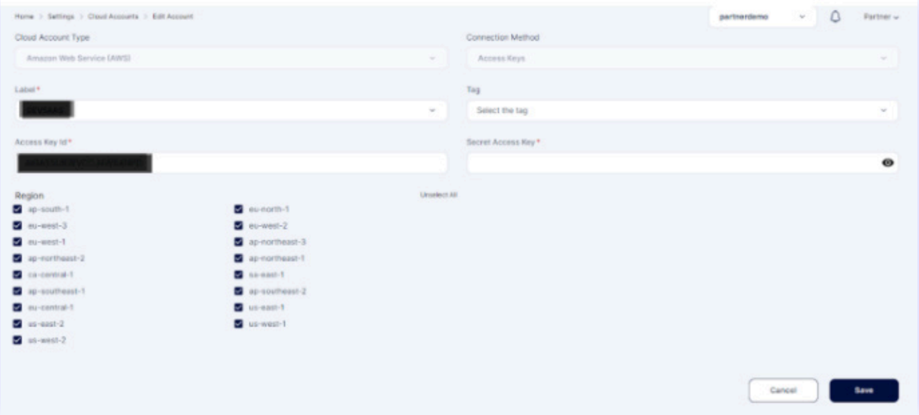
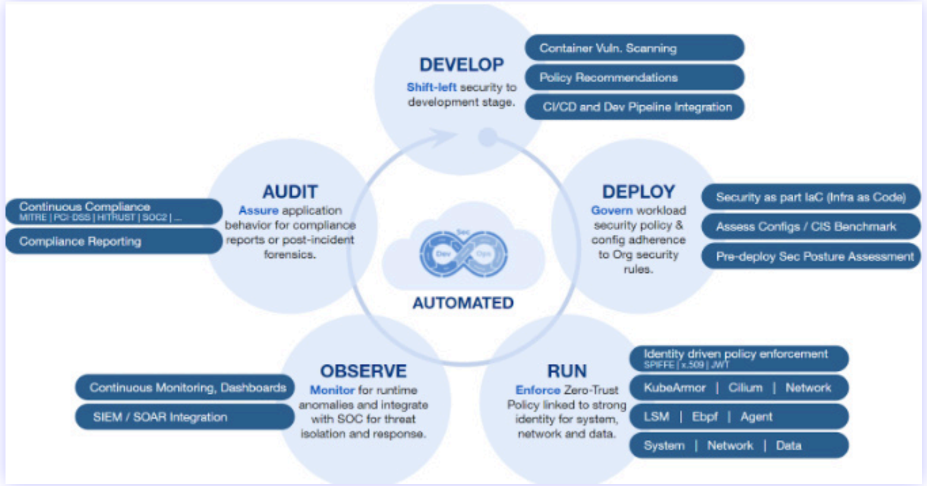
Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
Ease of Use	Predefined Compliance Templates	AccuKnox CNAPP comes equipped with predefined templates. Organizations may assess their compliance against common standards such as CIS, NIST, PCI, GDPR, and HIPAA. By automating 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.	
	Unified Management Plane	We have put together a single, easy-to-use management console. It is the control center for your application's security. It's where you oversee everything without juggling between numerous systems. Access our one stop shop solution.	 

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, ...	✗	✓
PCI.S3.1, S3 buckets should prohibit public write access, The...	✗	✓

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
Pricing and Licensing	Usage Pricing	AccuKnox offers a very simple pricing model as depicted here	
Integration with Tools & Workflows	Integration and Support for Key Tools	AccuKnox provides AccuKnox can integrate multiple Cloud Account, Registries, SIEM platform, Ticketing or Notifications Tools and the list is ever growing. Security Events/SIEM : Splunk, Rsyslog, AWS CloudWatch, Elastic Search, Webhooks Notification Tools: Slack, Jira, PagerDuty, Emails Ticketing Tools: Jira, FreshService, Connectwise, Zendesk, Registries: Nexus, ECR, GCR, DockerHub	
	Integrated Advanced Analytics	Integrations to SIEM tools such as Splunk, Sentinel or Chronicle will empower SOC team for forensics through deep telemetry that AccuKnox produces using its eBPF Technology	

Application
Security Events/ SIEM
FireEye Helix, Splunk, Rsyslog, Elastic Search, AWS Cloudwatch, Webhook.
splunk>
rsyslog
Log Aggregation - Helix, Splunk, Rsyslog, Elastisearch, AWS Cloudwatch, Sentinel
Notification Tool
Slack, Jira, PagerDuty, Email
SYMPHONY
Notification Tools - Symphony, Slack, Jira, PageDuty, Email
Troubleshooting
Accelerate troubleshooting with a single source of truth
VM/Baremetal, Container or K8s context
eBPF backed telemetry
Logs Aggregation
Monitors
Logging
eBPF based Telemetry

Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
	Cloud Control Plane API-based Integration	AccuKnox supports API-based integration with cloud control planes. This allows inspection of cloud account findings, vulnerability scanning, asset inventory etc.	 Home > Settings > Cloud Accounts > Edit Account partnerdemo Partner Cloud Account Type: Amazon Web Service (AWS) Connection Method: Access Keys Label *: [redacted] Tag: Select the tag Access Key Id *: [redacted] Secret Access Key * Region Unselect All ☑ ap-south-1 ☑ eu-west-3 ☑ eu-west-1 ☑ ap-northeast-2 ☑ ca-central-1 ☑ ap-southeast-1 ☑ eu-central-1 ☑ us-east-2 ☑ us-west-2 ☑ eu-north-1 ☑ eu-west-2 ☑ ap-northeast-3 ☑ ap-northeast-1 ☑ sa-east-1 ☑ ap-southeast-2 ☑ us-east-1 ☑ us-west-1 Cancel Save
	Integration into CI/CD Development Toolsets	Our product integrates into the CI/CD pipeline, supporting common development tool sets. This includes code repositories, build servers and container registries. This integration empowers continuous security monitoring and auditing throughout the development lifecycle. With telemetry data from these tools, AccuKnox verifies real-time insight into security risks. This allows you to fix problems early in the development process. Results in faster and more secure application deployments.	 DEVELOP Shift-left security to development stage. Container Vuln. Scanning Policy Recommendations CI/CD and Dev Pipeline Integration AUDIT Assure application behavior for compliance reports or post-incident forensics. Continuous Compliance MITRE | PCI-DSS | HITRUST | SOC2 | ... Compliance Reporting DEPLOY Govern workload security policy & config adherence to Org security rules. Security as part IaC (Infra as Code) Assess Configs / CIS Benchmark Pre-deploy Sec Posture Assessment Sec Dev Ops AUTOMATED OBSERVE Monitor for runtime anomalies and integrate with SOC for threat isolation and response. Continuous Monitoring, Dashboards SIEM / SOAR Integration RUN Enforce Zero-Trust Policy linked to strong identity for system, network and data. Identity driven policy enforcement SPIFFE | x.509 | JWT KubeArmor | Cilium | Network LSM | Ebpf | Agent System | Network | Data

Get a Demo

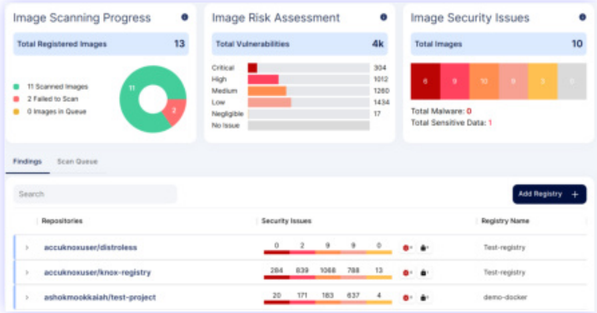
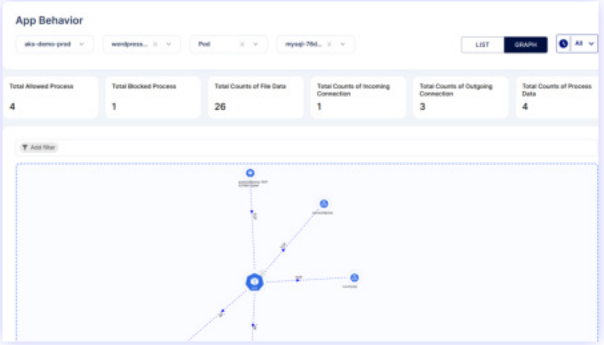
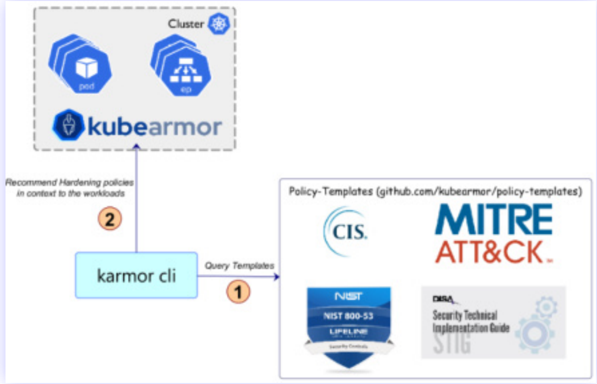
Category	Sub category	AccuKnox Compliance	Screen Shot, Table, Architecture Diagram
Compliance and Governance	Scanning of Containers and Container Registries for Risk	AccuKnox excels in container security by performing in-depth scanning of containers and container registries for potential risks. It supports various container registries, including Nexus, ECR, GCR, DockerHub, and clusters like EKS, GKE, AKS, RKE, and OKE. Proper visibility into containerized applications. By analyzing container images and registries, AccuKnox identifies vulnerabilities, configuration issues, and potential threats. Address security concerns before deployment, safeguarding their cloud-native applications.	
	Snapshots of Running Workloads	Get snapshot-based analysis with our AccuKnox. Real-time visibility into containerized applications and threat detection and response.	
	Ready To Use Compliance Templates	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 such as CIS, MITRE, NIST-800-53, and STIGs. These policies are designed to help you secure your workloads in a way that is compliant with these frameworks and recommended best practices.	

Image Scanning Progress

Total Registered Images 13

- 11 Scanned Images
- 2 Failed to Scan
- 0 Images in Queue

Image Risk Assessment

Total Vulnerabilities 4k

Critical	304
High	1012
Medium	1260
Low	1434
Negligible	17
No Issue	

Image Security Issues

Total Images 10

Total Malware: 0
Total Sensitive Data: 1

Findings | Scan Queue

Search | Add Registry +

Repositories	Security Issues					Registry Name
accuknoxuser/distroless	0	2	9	9	0	Test-registry
accuknoxuser/knox-registry	284	839	1068	788	13	Test-registry
ashokmookkaiah/test-project	20	171	183	637	4	demo-docker

App Behavior

aks-demo-prod | wordpress... | Pod | mysql-78d... | LIST | GRAPH | All

Total Allowed Process	Total Blocked Process	Total Counts of File Data	Total Counts of Incoming Connection	Total Counts of Outgoing Connection	Total Counts of Process Data
4	1	26	1	3	4

Add filter

Cluster
pod
ep
kubearmor
Recommend Hardening policies in context to the workloads
2
karmor cli
Query Templates
1
Policy-Templates (github.com/kubearmor/policy-templates)
CIS.
MITRE ATT&CK
NIST
NIST 800-53
LIFELINE
Security Controls
DISA
Security Technical Implementation Guide
STIG

Get a Demo

Proving Effectiveness against Zero Day Attacks

Get a Demo

In keeping with Layered Security approach that is recommended, our solution to Cloud Security is comprised of 4 steps:

1. **Basic Security** - Agentless - Cloud discovery, posture management and protection through the use of native APIs.
2. **Application security** - Lightweight Vulnerability Scanners based on proven open source technologies.
3. **Basic Workload Security category** - Lightweight Scanner - open-source industry standard scanner, eBPF* which is non-intrusive and is focused only at observability. It does not change anything in the application and has minimal performance footprint. As the user desires, one can flip the switch to enforcement ~ which advances workload security by invoking LSMs as guardrails at kernel level.
4. **Advanced workload security (Application Firewalling, Micro-segmentation)** - If enforcement is required to defend against zero-day attacks, AccuKnox triggers proven LSMs (Linux Security Modules) to move from observability "audit" to enforcement "block" mode.

*We use industry-standard eBPF (part of Linux Foundation, telemetry used by Google, Facebook, Cloudflare, etc.) to gain workload observability and rich telemetry.

Proving Effectiveness against Zero Day Attacks

AccuKnox has been field tested against advanced attack vectors that form the core of Zero Day attacks. They include:

- Detect and Prevent backdoor fetch-store-exec operations from subverted process or embedded malicious logic
- Prevent unauthorized network Interface usage
- Prevent unauthorized file system manipulations
- Prevent unauthorized process execution, termination, thread hijacking
- Prevent unauthorized administrative functions and command invocations
- Introduce strong identity management for all cross-container communications
- Produces fine-grain app-level audits and alerts for all permission violations

Summary

These are a few more examples that have been covered in greater detail in AccuKnox blogs:

Log4J - CVE-2021-44228 remediation policy for K8s clusters - Updated blog

Asif Ali – 8 min read

IntroductionOn December 9th, 2021, the world was made aware of a new vulnerability identified as CVE-2021-44228, affecting the Apache Java logging package log4j. This vulnerability earned a severity…

Protect Yourself Against CVE-2022-0185 with KubeArmor

Asif Ali – 1 min read

Now you can protect your workloads in minutes using AccuKnox, it is available to protect your Kubernetes and other cloud workloads using Kernel Native Primitives such as AppArmor,…

Defending Flask Workloads using Accuknox OpenSource

Vishnu Soman – 9 min read

IntroductionWith Python frameworks in play, developers get the freedom to focus on the logic of the application rather than worrying about all…

#Accuknox #open-source #kubearmor #cilium

Run-time protection from TNTBotinger Malware using Accuknox Open Source tools

Vishnu Soman – 11 min read

IntroductionWith the development of contemporary infrastructure, cryptocurrency mining has grown in popularity. It's very simple to target settings like Kubernetes since you…

Securing Java microservice workloads with AccuKnox Open-Source

Salman PJ – 4 min read

Microservices are small, self-contained, ready to run applications. Each will have a specific well-defined task. All of them are grouped together to…

#java #open-source #Accuknox #kubearmor #cilium

Protecting against CVE-2021-4034 Polkit Vulnerability using AccuKnox Opensource

IntroductionPolkit is a component for controlling system-wide privileges in Unix-like operating systems. It provides an organized way for non-privileged processes to communicate with privileged processes. It is also possible to use polkit to execute commands with elevated privileges using the command pkexec…

Summary

AccuKnox offers one of the most comprehensive, modern, proven Zero Trust CNAPP

CSPM	CWPP
1. Static Application Security Testing (SAST)	1. Runtime Kubernetes Security
2. Software Composition Analysis (SCA)	2. Runtime On-Prem Security
3. Network security	3. Zero Trust workload hardening policies
4. API Security	4. Inline Remediation
5. Host Security	5. Automatically Discovered Policies
6. Container Security	6. SIEM, Notifications, Ticketing tools integrations
7. Kubernetes Orchestration Security	7. Network micro-segmentation
8. Continuous Compliance	8. Container/VM Forensics
9. Baselines & Reporting	9. Support for emerging assets: IoT/Edge, 5G

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

About

Customer Accolades

Enterprise vs Open Source

Leadership

About AccuKnox

AccuKnox provides a Zero Trust Cloud Native Application Security (CNAPP) platform. 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 and Private 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.

Customer Accolades

70% INCREASE IN CRITICAL ISSUES RESOLUTION

5 SIEM TOOLS INTEGRATED

“ We are very pleased to partner with a Modern, Cloud Native, Zero Trust CNAPP innovator like AccuKnox. Zero Trust security is a commitment we have to our customers. Their work with AWS furthers the value that AccuKnox can deliver to us.”

ONDA

80% EFFICIENCY IN HANDLING FALSE POSITIVE ALERTS

5 MINUTES TO SOLVE KNOWN VULNERABILITIES

“ Zero Trust security is Clint Health's 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.”

clint™

50% TIME REDUCED IN HANDLING CI/CD PIPELINE ISSUES

1 MINUTE TO OBTAIN INSTANT REPORTS

“ 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.”

IXEL-INTERNATIONAL

Get a Demo

AccuKnox Enterprise vs KubeArmor OpenSource

AccuKnox Runtime Security Features	Open Source	Enterprise
Observability into the workload at granular level	✓	✓
In-line remediation for Zero Day Attacks	✓	✓
Manual apply of Security Policies using CLI	✓	✓
Integration to SIEM for security events and Notification tool	✓	✓
Network security using CNI	✓	✓
Auto-Discovered Behavioral Policies		✓
Recommendation of Hardening Policies based on standard compliance framework - MITRE, NIST, PCI-DSS, CIS		✓
Inventory View of Application		✓
Network Graph View of the Application		✓

AccuKnox Enterprise vs KubeArmor OpenSource

AccuKnox Runtime Security Features	Open Source	Enterprise
Network Micro segmentation in the application		✓
Hardening of the Secrets Managers like Hashicorp Vault, CyberArk Conjur		✓
GitOps based Version Control for Policy Lifecycle Management		✓
Rollback of recently changed Policy governing App Behavior		✓
On-the-fly detection of change in App Behavior through Policies		✓
Multi-Tenant, Multi-Cluster, RBAC for user-management		✓
Comprehensive Dashboard across workloads running in Managed/Unmanaged Cluster, Containerized environment, VM or Baremetal		✓
Integration with Registries for Container Image Vuln Scan		✓
Telemetry aggregation (Process executed, File accessed, Network connections made) and Alerts events (Audit, Block)		✓

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 ⟶**