AccuKnox

Zero Trust CNAPP

Cloud Native Application Protection Platform

Definitive Guide

Secure

Build → Runtime
Public Cloud (AWS, Azure, GCP), Private / Air gapped, Edge/IoT
Kubernetes, Virtual Machine
Static, Dynamic workloads

Contents

CSPM

AccuKnox Cloud Security Posture Management (CSPM) leverages agentless technology to revolutionize cloud security by proactively identifying, prioritizing vulnerabilities, providing a seamless or chestration and management platform.

CWPP

Runtime Protection Reinvented: AccuKnox Cloud Workload Protection Platform (CWPP) has a differentiated solution built for runtime security, namely, KubeArmor (opensource,now a part of CNCF sandbox project) which leverage eBPF for observability of App Behavior and LSMs for enforcement / in-line mitigation from unknown Zero Day attacks.

Code to Cloud Security

AccuKnox AppSec offers a unique solution, seamlessly integrating open source and commercial security scanning tools. Our flexible security posture approach efficiently prioritizes critical vulnerabilities, ensuring a comprehensive protection journey from code to cloud.

Zero Trust Security

- Why Zero Trust
- History of Zero Trust
- Definition of Zero Trust
- Government Recommendations

Notable Cloud Breaches

The bigger you are, the bigger the hack.

A day does not go by when we don't hear about major cyber attacks against Cloud Assets. Given that the workloads are moving to the cloud at rapid rate it is only natural that attacks are shifting to the cloud. In addition to the number of attacks the severity and sophistication of the attacks in the cloud are also very advanced.

The Global Cloud Computing Market Size Is Estimated To

Be Valued At	And Reach	With CAGR of
$405.29 Billion	**$1,465.81 Billion**	**23.9%**
in 2022	by 2028	by 2028

TESLA

Kubernetes console was vulnerable, and hackers were able to take control and find the credentials to AWS cloud. They were able to gain access to S3 buckets with sensitive data, as well as run cryptocurrency mining in Kubernetes pods.

WeightWatchers

An insecure Kubernetes cluster console was found by scanning publicly available IPs on kubelet TCP port 10250.

shopify

Exploited containers allowed attackers to overwrite host runc library and gain root access to the container hosts

amazon

Technology

Amazon Gets Record $888 Million EU Fine Over Data Violations

By Stephanie Bodoni

July 30, 2021, 5:03 AM MDT *Updated on July 30, 2021, 5:43 AM MDT*

T-Mobile

THE WALL STREET JOURNAL.

BUSINESS

T-Mobile Says Hackers Stole Data on More Than 40 Million People

Theft included Social Security numbers and driver's license data for current and prospective customers

Key Takeaway

It is only logical that attackers will be increasing the volume, velocity and sophistication of their cyber attacks. Hence it is prudent to instill pertinent security measures.

Revolutionizing Security – The Timely Renaissance of Zero Trust

Despite being conceived in 1974 with the introduction of Least Privilege, the true potential of Zero Trust principles only emerged a decade ago. It took the impactful SolarWinds breach to propel Zero Trust into mainstream acceptance. This transformative approach shifts the security paradigm from merely thwarting the bad to recognizing the good – a philosophy embodied by Zero Trust.

1974

MIT professor, Saltzer coins the term "Least privilege" Every program should operate using the least set of privileges necessary to complete the job.


Protection and the Control of Information Sharing in Multics

Jerome H. Saltzer
Massachusetts Institute of Technology

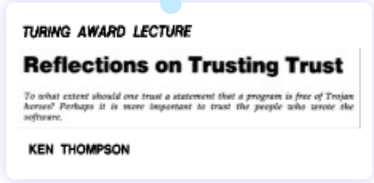
1977

PKI
RSA (Rivest Shamir Adelman), DiffieHelman Invent public key infrastructure (PKI)

(PKI) is a needed to manage digital certificates and manage public-key encryption. Required for activities where simple passwords are an inadequate and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

1984

MIT Professor Ken Thompson delivers a seminal lecture on **Trusting Trust**


TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

2003

UK Royal Mail organizes Jericho Forum where a new term **DEPERIMETERIZATION** is introduced

Security Must:

1. Be specific to the asset being protected
2. Pervasive, simple and scalable
3. Leverage Open Protocols
4. Transparent
5. Portable
6. Allow for separation of duties
7. Apply at rest, in transit and in use

2010

John Kindervag, Forrester coins the term Zero Trust

Tenets

1. Network is assumed to be hostile
2. Threat actors are in your network
3. Network segmentation is not enough
4. Policies must be dynamic
5. Device is no longer at the border
6. Containers, Serverless and Cloud are new disruptors

2019

SolarWinds leveraged for several high-profile breaches.

CISA issues Emergency Directive 21-01 "The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales.

Focus

Remote work has accelerated Zero Trust adoption, with 81% of organizations implementing or considering Zero Trust initiatives to secure remote access.

Zero Trust Tenets

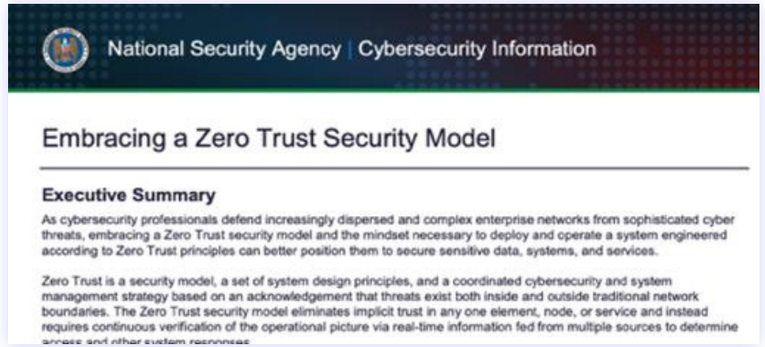
1. The network is always assumed to be hostile
2. Assume threat actors are already inside your network
3. Network locality (segmentation) is not sufficient for deciding trust in a network
4. Every device, user and network flow is authenticated and authorized
5. Policies must be dynamic and calculated from as many sources of data as possible
6. The device is no longer the border. A user/service' identity is the net border
7. Containers, serverless and cloud are the new disruptors of traditional security architecture

ZERO TRUST ADAGE
Verify, Then Trust, Continuously Verify

Zero Trust Devices, Networks and Users

"If organizations don't adapt to the new development and adopt the Zero Trust principles, "they probably will be going out of business in this digital world."

July 2023 pwc

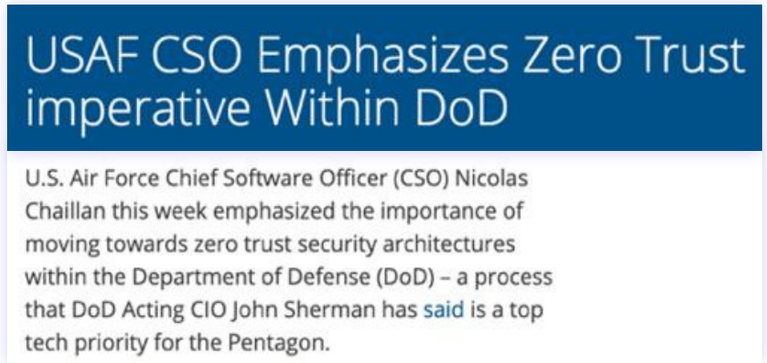

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

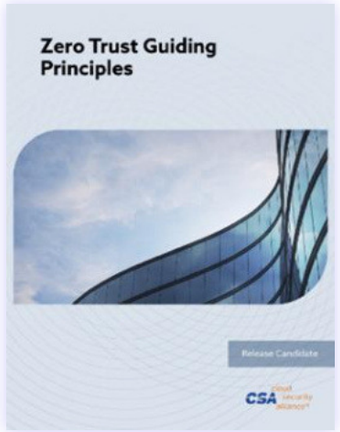
Executive Summary

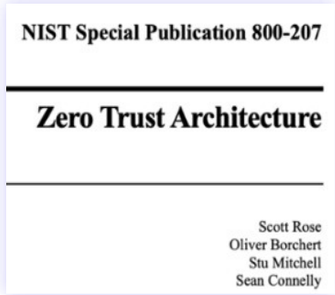
As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine


USAF CSO Emphasizes Zero Trust imperative Within DoD

U.S. Air Force Chief Software Officer (CSO) Nicolas Chaillan this week emphasized the importance of moving towards zero trust security architectures within the Department of Defense (DoD) – a process that DoD Acting CIO John Sherman has said is a top tech priority for the Pentagon.


Zero Trust Guiding Principles


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

Newsflash

Zero Trust is not an entirely new idea. The concept of least privilege has been around for a long time. However, the recent Zero Day attacks has brought board room visibility to this.

Zero Trust CNAPP

- Why Zero Trust CNAPP?
- CNAPP
- CSPM, KSPM
- ASPM
- CIEM, KIEM
- Zero Trust
- GRC
- Integration
- Deployment
- Leveraging AI

Ephemeral and Transient Nature of Containers

ISACA Silicon Valley Chapter

Evolution of server workload abstractions

Physical

- Monolithic applications
- Physical servers as unit of scaling
- Life span of years

Virtual Machines

- Hardware virtualization
- VMs as unit of scaling
- Life span of months to years

Containers

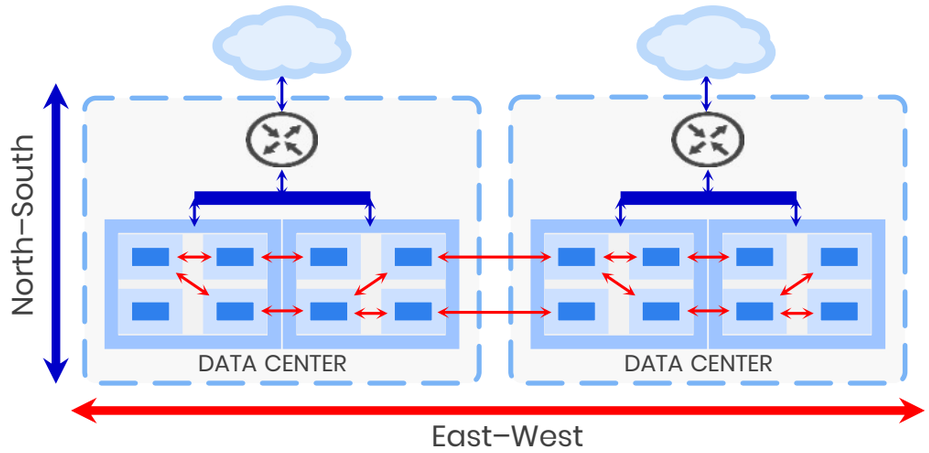
- OS Virtualization
- Applications/services as unit of scaling
- Lifespan of minutes to days

Serverless

- Lifespan of seconds to minutes

Unmonitored inter-container communication

Current
Perimeter Defenses
Firewalls, End Point
address only North-South
[17% of the traffic]



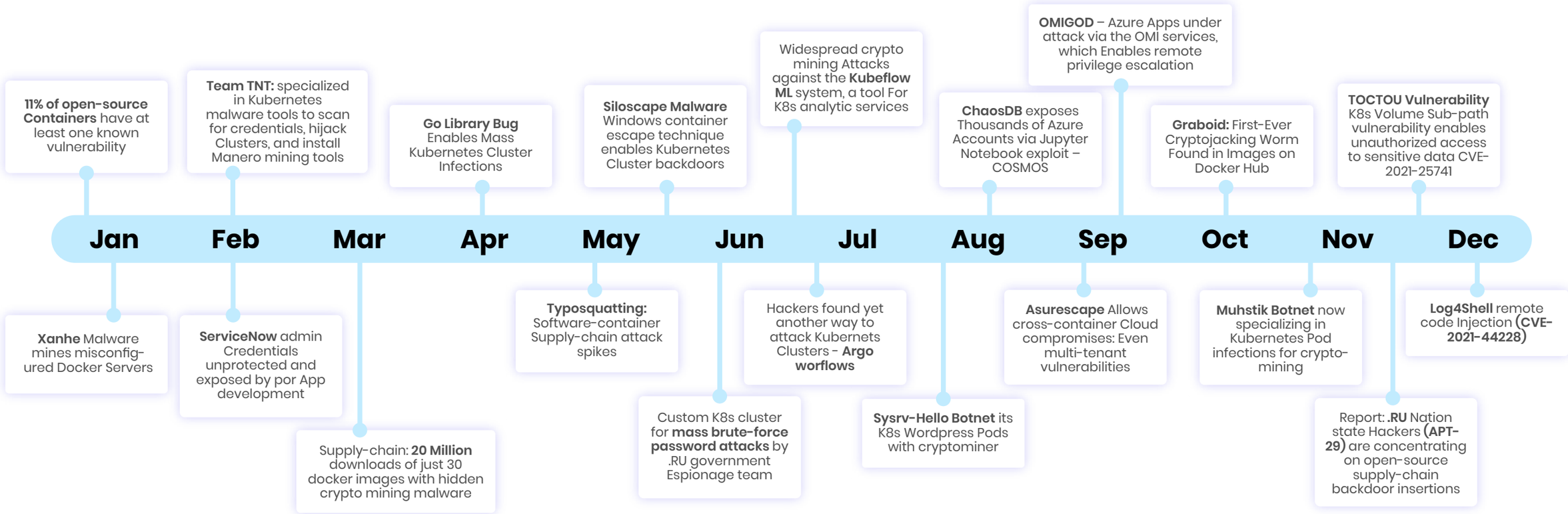
Current
Container Security Solutions
Do not have a mechanism to **affirmatively enforce Policy Compliance**

Source: Gartner 2019

Beware Almost all modern Zero Day threats originate in un-monitored East-West, lateral movement attack vectors.

What problem does CNAPP solve?
Overcoming Inadequacy of Traditional Perimeter Defenses Against Sophisticated Cloud Attacks

Top 20 Cloud Security Incidents In 2022



Brilliant Idea

"Average Time to Detect and Respond to Security Incidents" is a crucial metric. It indicates the effectiveness of security operations in identifying and addressing potential threats.

How CNAPP Neutralizes Advanced Threats?

Zero-Day Attacks Root Causes

- Privilege escalation
- Lateral movement
- Process subversion
- Rootkit attacks
- Embedded malicious logic
- Unauthorized file system manipulations
- Malicious network interface usage
- Unauthorized process execution, termination, thread hijacking
- Unauthorized administrative functions and command invocation

Zero Trust Mitigation Approaches

- Run-time Security
- Micro-segmentation
- Application Firewalling
- Kernel Hardening
- In-line Security

Beware

Zero-day attacks require proactive security measures, continuous monitoring, and rapid response to protect sensitive information and organizational integrity from unauthorized access, data breaches, and financial losses.

CNAPP – Cloud Native Application Protection Platform

- **Integrated Security Lifecycle -** Implement a holistic approach to secure cloud-native applications, spanning from development to runtime protection.
- **Developer Toolchain Integration -** Integrate security seamlessly into the developer's toolchain, automating testing throughout the development pipeline to enhance adoption efficiency.
- **Focus on Critical Vulnerabilities -** Prioritize the identification and remediation of highest severity, highest confidence, and highest risk vulnerabilities, optimizing developer efforts.
- **Comprehensive Artifact and Configuration Scanning -** Conduct thorough scans of development artifacts and cloud configurations, coupled with runtime visibility, to prioritize and remediate security risks effectively.
- **Diverse Runtime Visibility Techniques -** Choose CNAPP vendors offering a range of runtime visibility techniques, including traditional agents, eBPF support, snapshotting, privileged containers, and Kubernetes integration for deployment flexibility.

AccuKnox Zero Trust CNAPP meets all the guidelines outlined by Gartner

Certify-Verify

Cloud-native apps require automated testing. Prioritize critical vulnerabilities, and diverse runtime visibility for robust protection. Security should be dynamic and responsive to changes in the cloud environment.

CNAPP – Cloud Native Application Protection Platform

AccuKnox Enterprise CNAPP Suite

Shift Left Defense

- Thwart advanced "Zero Day" attacks with a proactive Shift Left approach.

Security Layers:

- Static Security: Leverage Cloud Security Posture Management (CSPM).
- Run-time Security: Utilize Cloud Workload Protection Platform (CWPP).

Integrated Testing

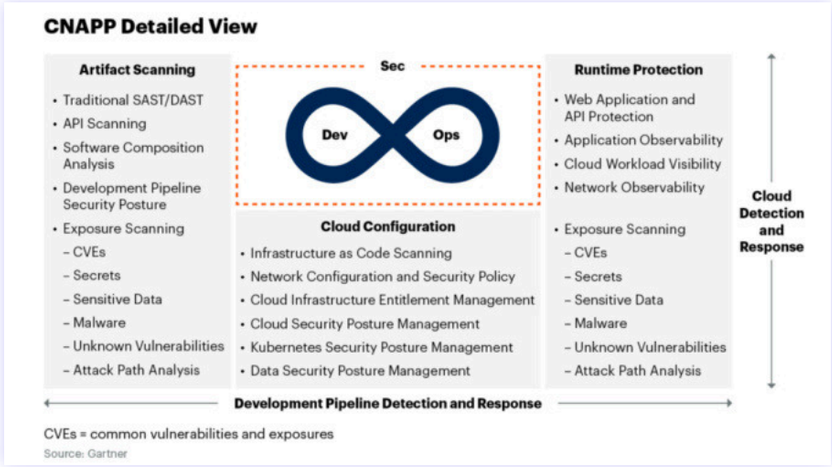
- Seamlessly integrate with Static Application Security Testing (SAST), Software Composition Analysis (SCA), and API Protection (DAST).

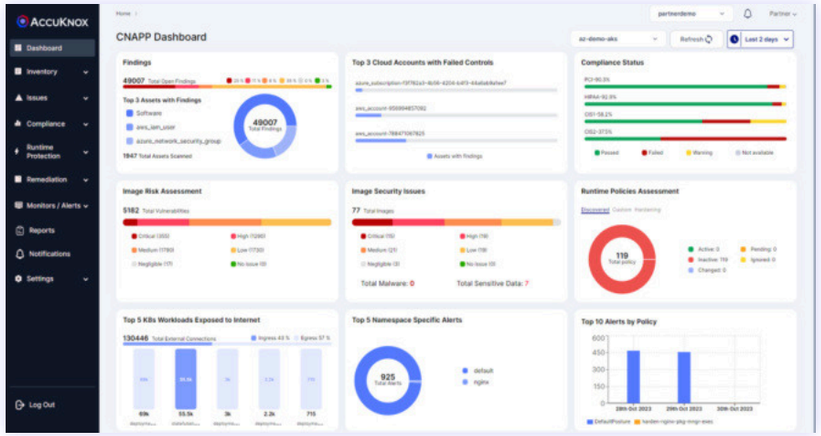
Identity Management:

- Cloud Identity and Entitlement Management (CIEM).
- Kubernetes Identity and Entitlement Management (KIEM).

Real-Time Protection

- Stay one step ahead with real-time defense against zero-day attacks.





Strategy

One needs to take a comprehensive and holistic approach to cloud security. Fragmented and disjointed approaches results in "alert deluge", inefficient and ineffective security operations.

Zero Trust Security From Code → Cloud

Code

- Static Code Analysis
- Software Composition Analysis
- Secret Scanning
- API Sec

Image

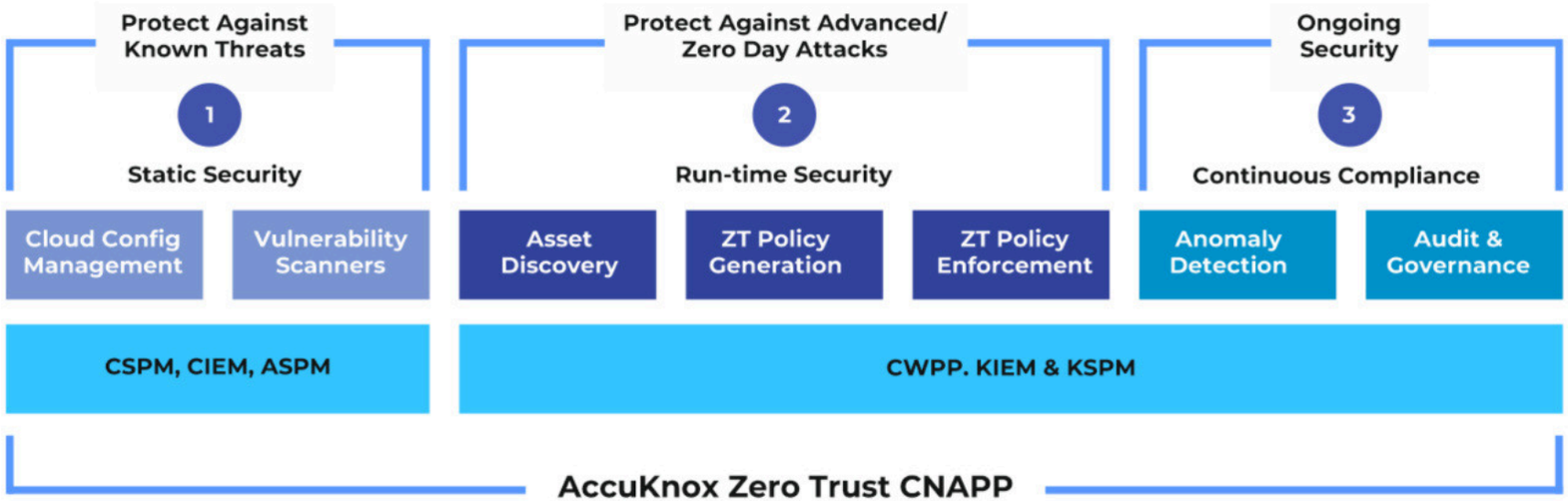
- Vulnerability Scanning
- Risk Prioritization
- Secret Scanning
- Container Compliance

Cloud

- Cloud Account /Asset Configuration Assessment
- CIS Benchmarking

Runtime

- App behavior analysis
- Workload hardening
- FIM, Compliance
- Zero Trust Policy
- Network Micro segmentation

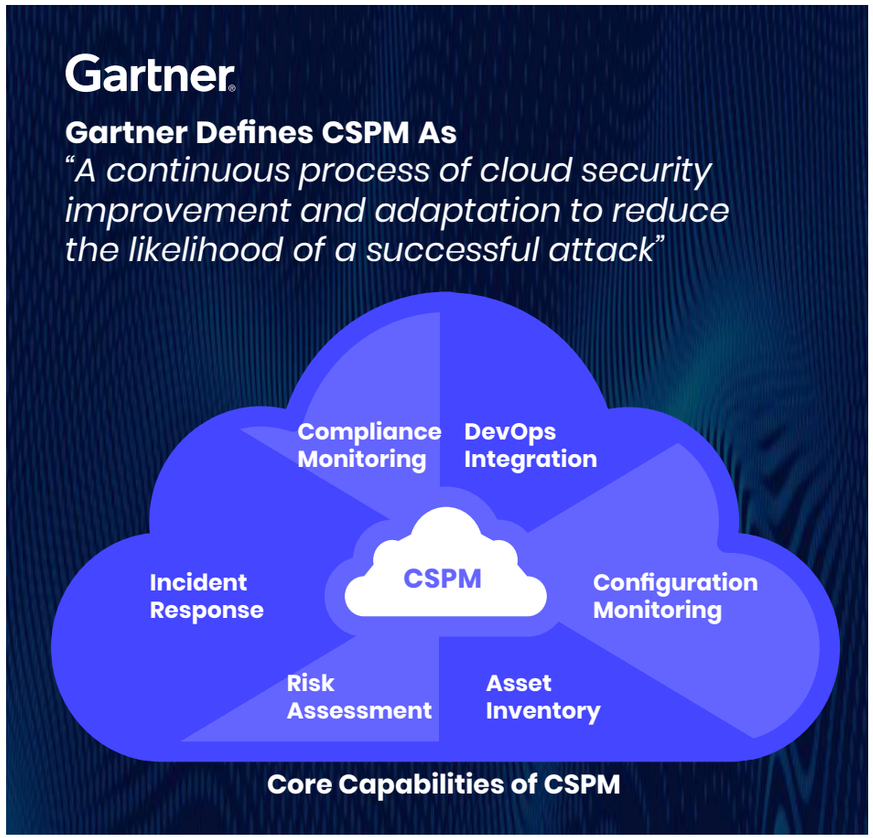


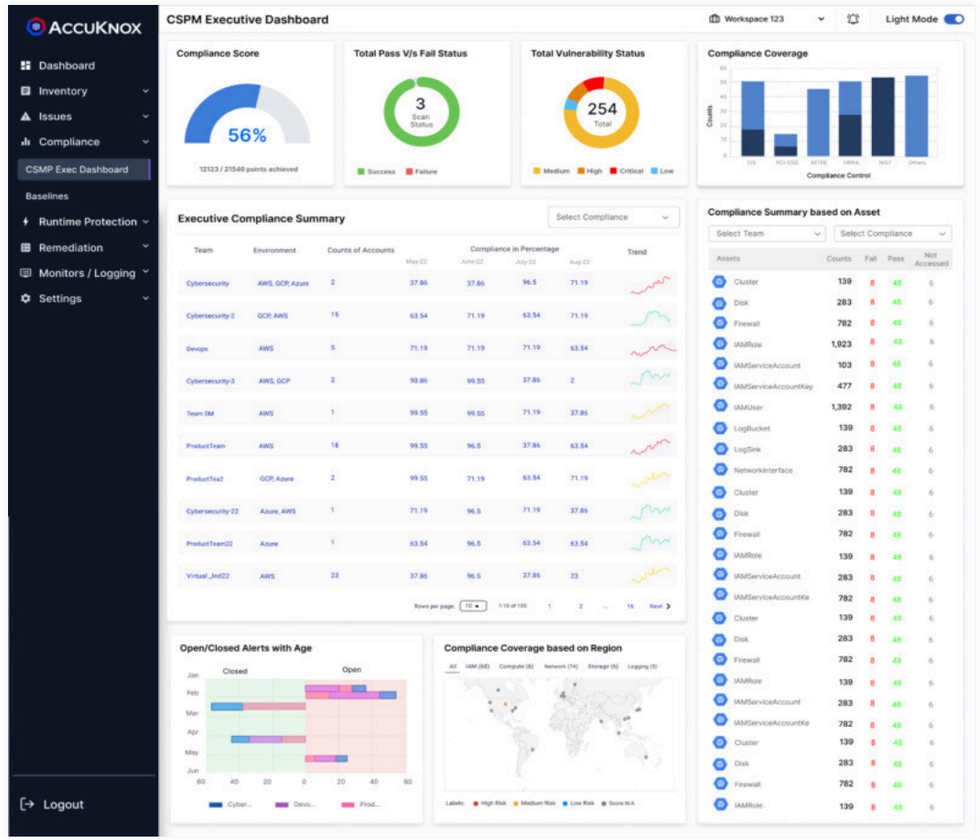
Technical Stuff

Cloud-native apps require automated testing. Prioritize critical vulnerabilities, and diverse runtime visibility for robust protection. Security should be dynamic and responsive to changes in the cloud environment.

CSPM – Cloud Security Posture Management

CSPM – Definition, Features, and Dashboard





Technical Stuff

CSPM, finds and fixes cloud environment misconfigurations. It precisely and efficiently improves security posture and offers proactive remedial recommendations.

CSPM – Cloud Security Posture Management

AccuKnox CSPM value add over what hyperscalers provide

Multi-cloud support

Analyze Baseline Compliance for All Regions, even unconfigured ones

Review and address findings ignoring repetitive issues, no need to re-review things which have been identified as not being real issues

Allow security analyst to review policies, configuration, and findings without granting console access

Monitor assets for changes to indicate when a re-review is necessary or if an undesirable condition has been detected.

Analyze findings from other sources within context of an asset, i.e. static code analysis results grouped with container findings

Report across groups that represent real world structures (business units, applications, departments, etc.)

Provide reports demonstrating activity to governing agencies or 3PAO

Assess pass/fail and **remember** status producing a true Baseline

Manage full lifecycle of security processes not just identification

Take action on findings by opening tickets with responsible party to resolve

Hyper Scalers

Analyze Baseline Compliance for All Regions, even unconfigured ones

Generate findings for potential security issues

Perform service specific security analysis (Macie, Analyzer, Detective, etc.)

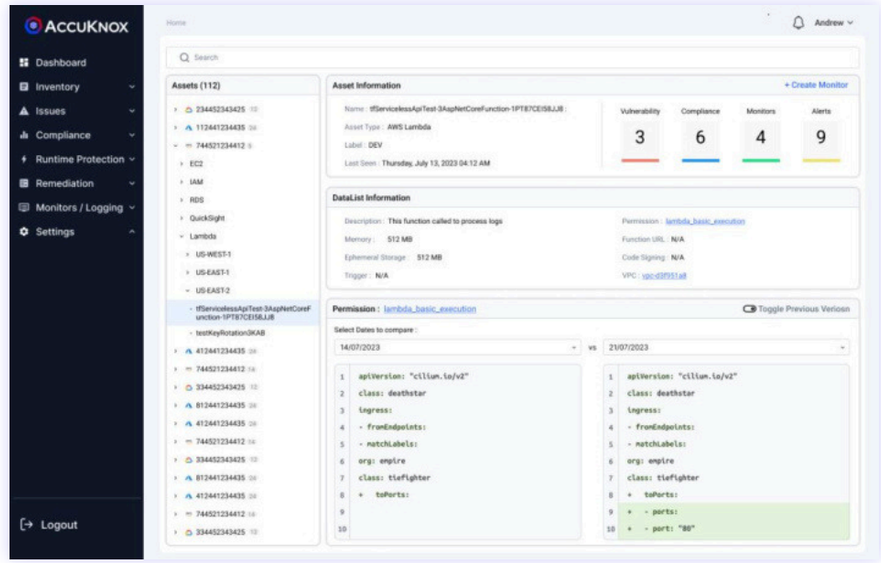
Collect vulnerability data and manage patching

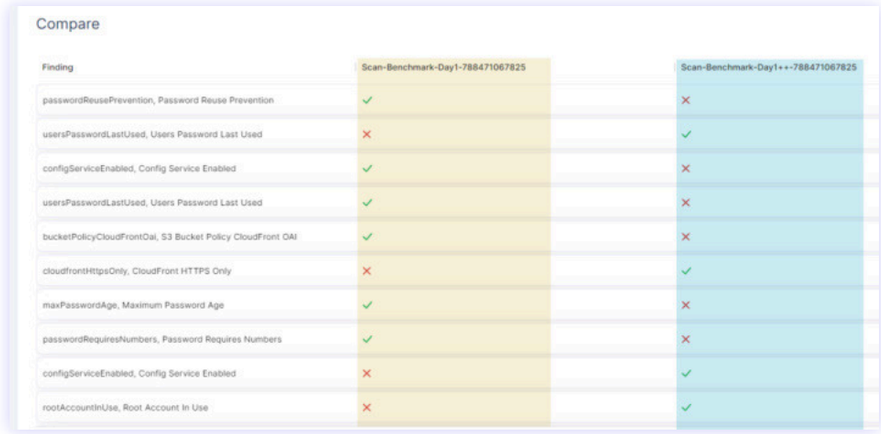
Summary

AccuKnox CSPM tool uses agentless technology to enhance cloud security. It actively identifies and prioritizes vulnerabilities. Easy to achieve compliance with regulations. Tightly coupled integration with SIEM/SOAR platforms.

CSPM – Cloud Security Posture Management

- Asset discovery on Multi-Cloud
- Mapped misconfigurations and vulnerabilities to each asset
- Detect critical assets with highest severity and group findings based on asset
- Group critical assets together and do proactive monitoring for configuration change
- Multi-Cloud Support for Drift Detection
- Full scans generates lot of noise and information that could be redundant
- Baselining Infrastructure with respect to particular controls by CIS, PCI-DSS or multiple data sources that AccuKnox supports
- Delta difference over time will be recorded and generated as an alert
- Provides proactive Monitoring vs Point-intime snapshot





Focus

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

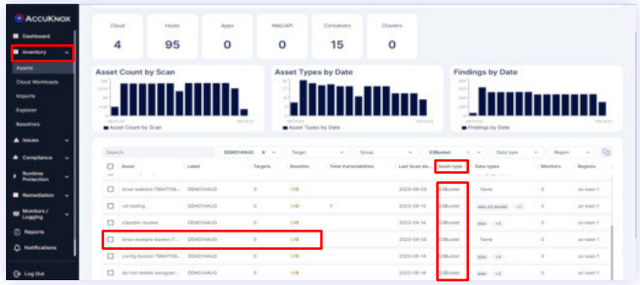
Exposed Treasures

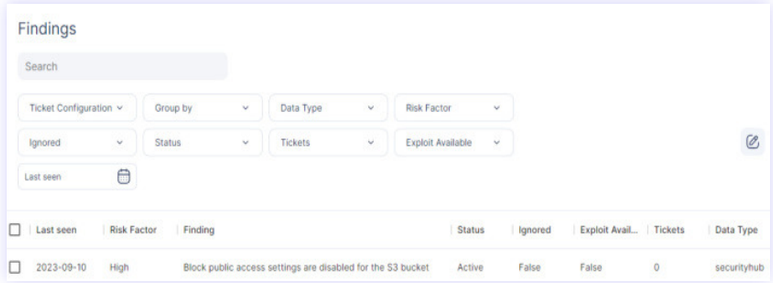
Identifying Publicly Accessible S3 Buckets

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

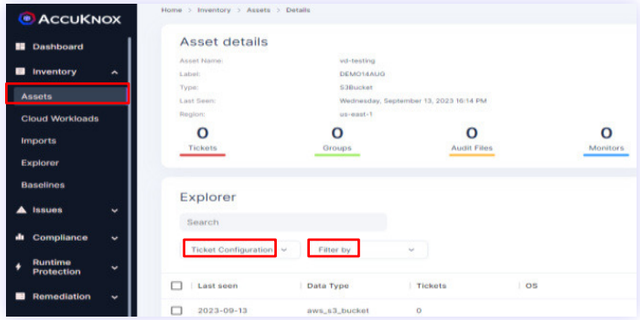
After Identification of S3bucket with misconfiguration, click on the bucket with misconfiguration(vd-testing) to see the detailed view.

1





2



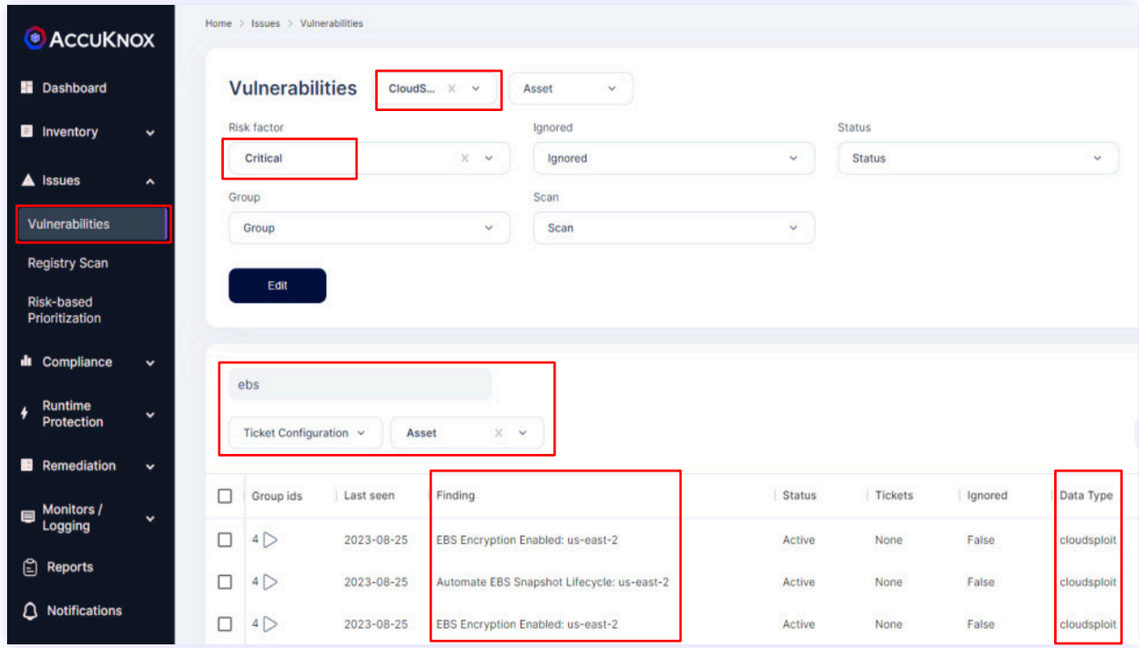
Considerations

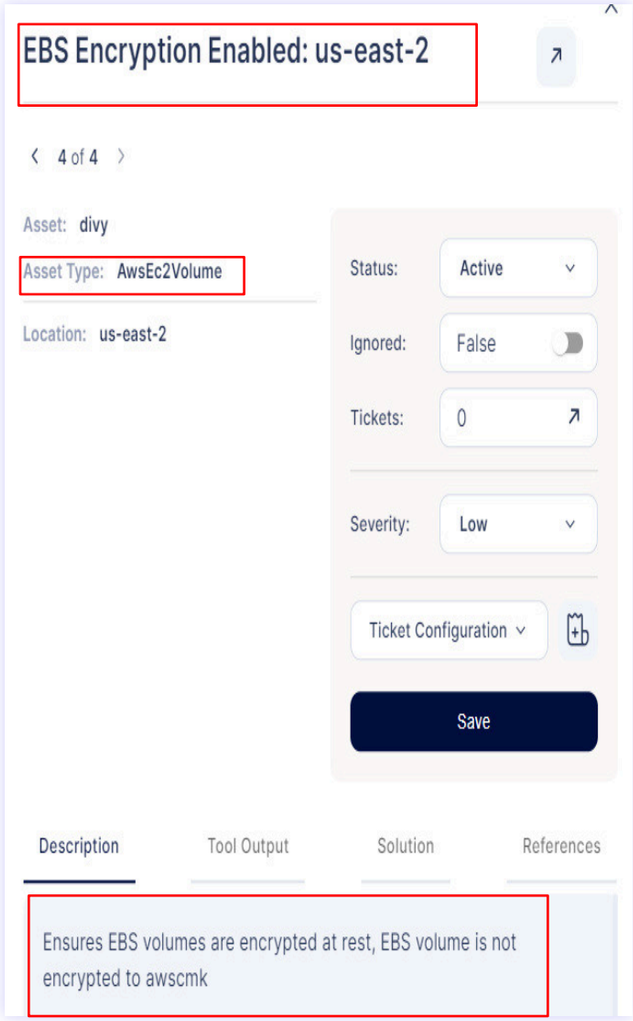
Implement an automated monitoring system for S3 bucket changes. Regularly audit permissions using AWS Config Rules. Promptly identify and rectify potential data leaks.

Spotting Unencrypted EBS Volumes

To identify the unencrypted EBS Volume associated with the Onboarded Cloud Account, please navigate to Issues → Vulnerabilities

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





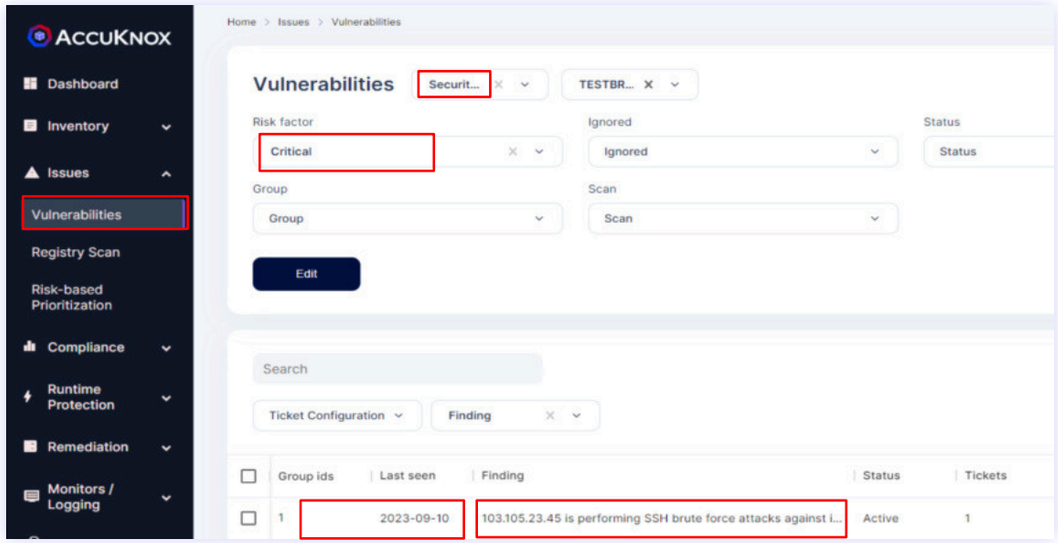
Focus

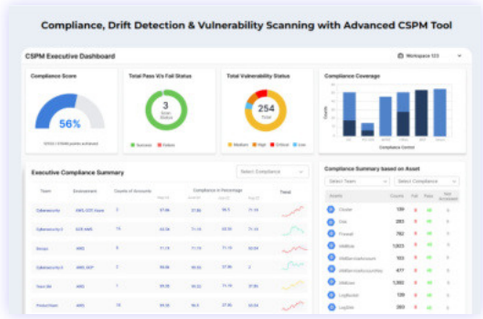
Cloudsploit's robust data-type filtering and granular search capabilities enable the easy identification of critical vulnerabilities. Streamlining security measures and protecting cloud infrastructure against potential risks is simple as it gets.

Identify Hosts with Critical Findings

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

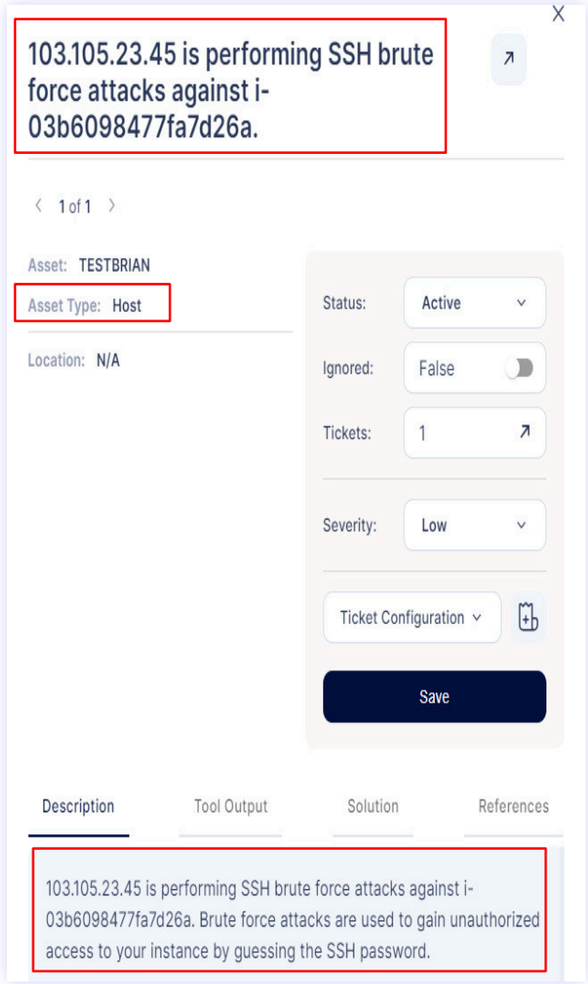
- Apply **SecurityHub** in data-type filter
- Choose the severity "Critical" for the Findings





The global market for CSPM is projected to grow at a CAGR of 15.3% from $4.2 billion in 2022 to $8.6 billion by

2027



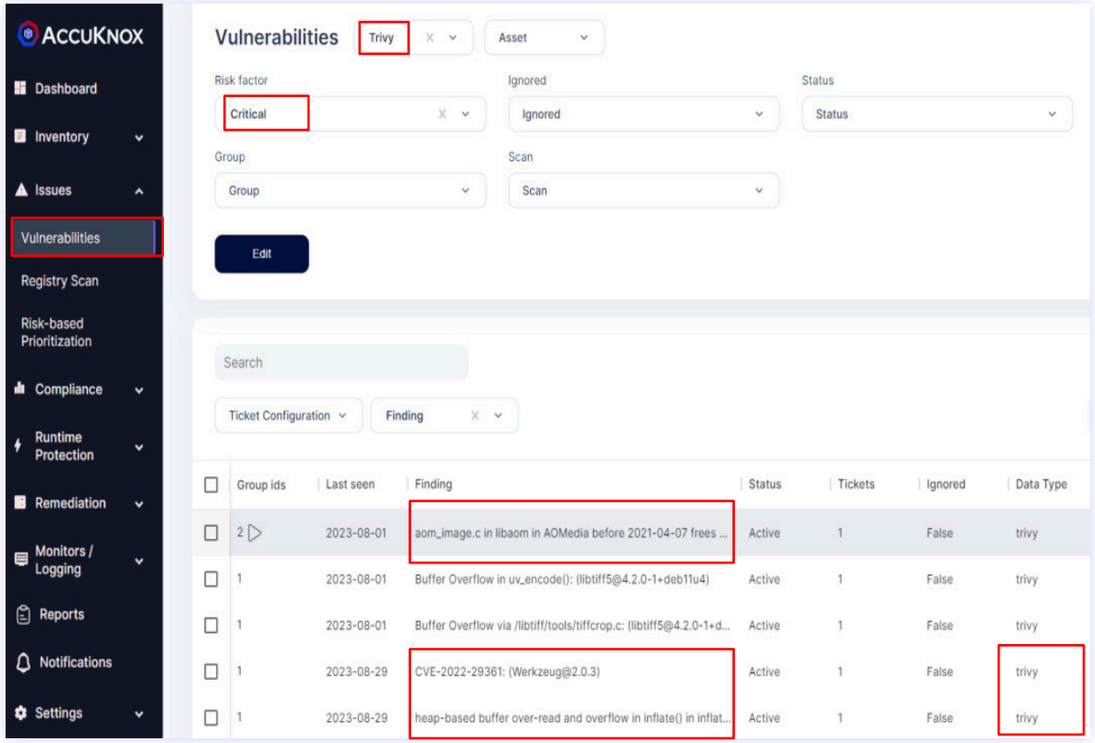
Beware

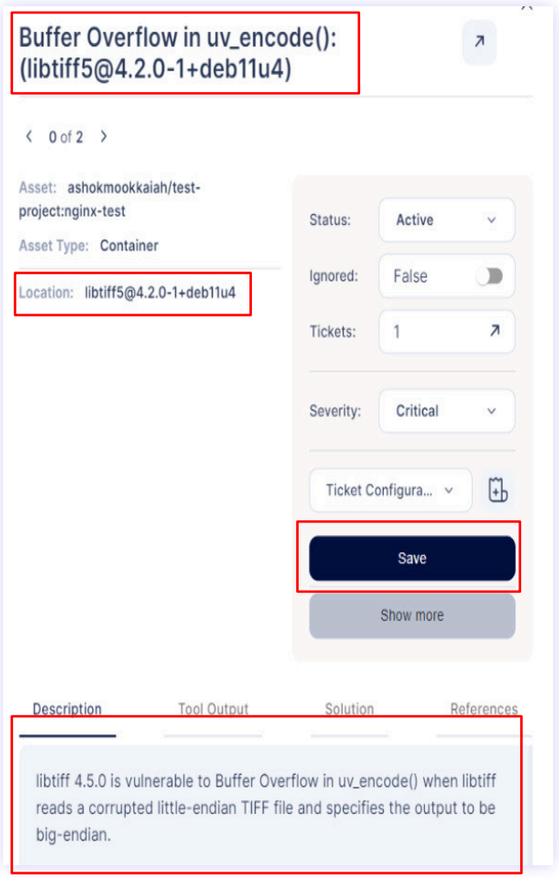
As the adage goes "an ounce of prevention is worth a pound of cure". Identifying basic and critical vulnerabilities in one's infrastructure is the first step in the cloud security journey.

Identify Container Images with Critical Vulnerabilities

To see the vulnerabilities associated with the Container Images, navigate to Issues → Vulnerabilities

- Apply **Trivy** in data-type filter
- Choose the severity "Critical" for the Findings



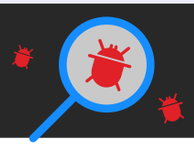


Focus

Cloudsploit's robust data-type filtering and granular search capabilities enable the easy identification of critical vulnerabilities. Streamlining security measures and protecting cloud infrastructure against potential risks is simple as it gets.

Shift Left – AccuKnox AppSec's Unified Approach

Problem: Noise



Most Vulnerabilities are **Noise** due to

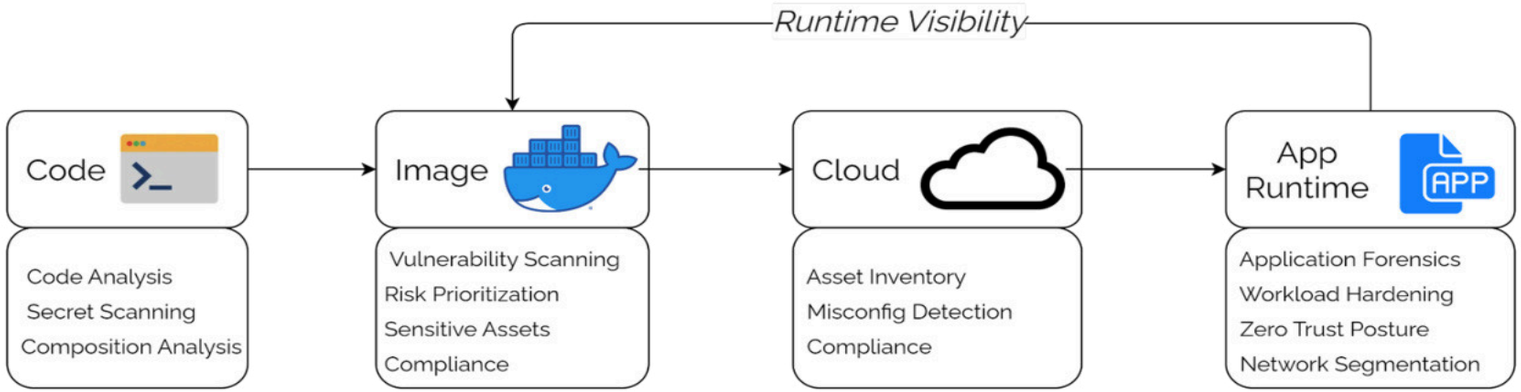
- False Positives
- Unexploitable
- Unused at Runtime
- **Too many** findings with no Runtime Context!!

AppSec and CloudSec works in silos and don't have contextual understanding of Vulnerabilities

Solution: AccuKnox AppSec

Revolutionizing Application Security

AccuKnox AppSec integrates best in class Vulnerability Management, SCA, SAST and DAST tools. Our flexible security posture approach efficiently prioritizes critical vulnerabilities, ensuring a comprehensive protection journey from code to cloud



Strategy

A critical part of Cloud Security journey is to integrate with AppSec (SAST, DAST, SCA) platforms. this ensures that any issues, vulnerabilities in the development phase is fully addressed during the deployment and run-time phases.

ASPM – Application Security Posture Management

SAST

Definition – analyzes source code for potential security vulnerabilities without running application
Used at – during development
Advantages – ability to fail a build in CI pipeline
Disadvantages – lots of false positives, runtime context
Cost – significant
Use-case:
- finding common CVE
- coding errors
- security best practices

Tools Supported

sonarqube, FORTIFY, VERACODE, $

DAST or API Sec

Definition – simulate attack scenarios at running app to find vuln
Used at – post-development (test or production)
Advantages – identify vuln in running environment
Disadvantages – may miss some vuln, false positives, slow down app
Cost – significant
Use-case:
- finding common CVE
- coding errors
- security best practices

Tools Supported

OWASP Zed Attack Proxy, Burp Suite

Tools WIP

VERACODE, $, nuclei, WAS, TSUNAMI, HCL AppSca

Key Takeaway

SAST analyzes source code during development, allowing failures in the CI pipeline. It is costly and prone to false positives. DAST simulates attack scenarios post-development, identifying vulnerabilities and aligning with AccuKnox's security offerings.

SAST

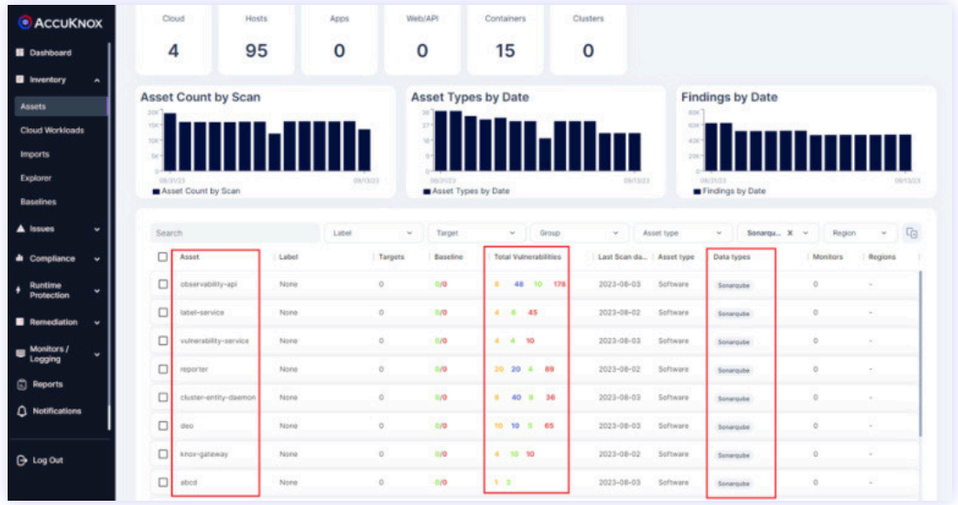
Integrate **Sonarqube** with your code repository through a JWT session-based token from AccuKnox SaaS

Step 1: Create workflow action for GitHub with token

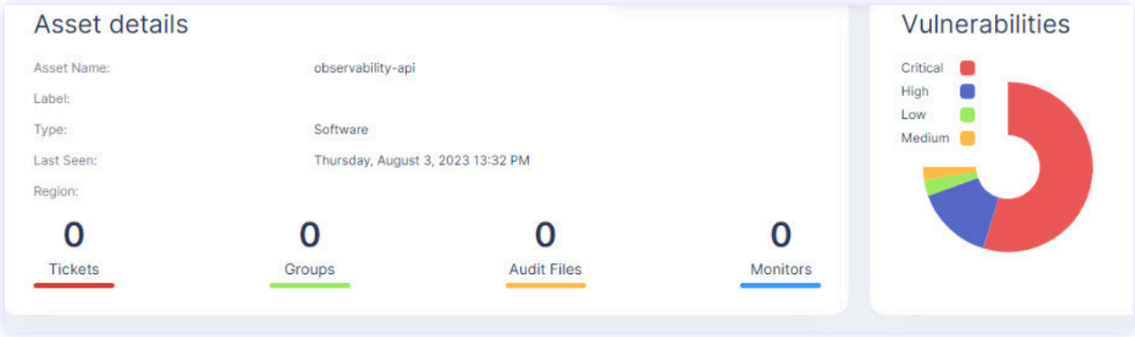
Step 2: Workflow will be triggered for every PR raised

Step 3: Push result to AccuKnox SaaS

Filter Data Source as **Sonarqube** and it will help to identify all the coding errors, common CVE etc. associated with your repository




```
40        - name: Push report to CSPM panel
41          run: |
42            curl --location --request POST 'https://${{env.CSPM_URL}}/api/v1/artifact/?tenant_id=${{ env.TENANT_ID }}&data_type=TR&save_to_s3=false'
43            --header 'Authorization: Bearer ${{ env.CSPM_TOKEN }}' --form 'file=@"./results.json"'
```



Get in touch with AccuKnox Team for assistance

Key Takeaway

Through a secure JWT token integration, AccuKnox and Sonarqube can analyze code automatically on GitHub pull requests. It finds common CVEs and coding errors for improved security and audit.

SCA

Definition – analyzes 3rd party dependencies/lib in open source
Used at – during dev, test or production
Advantages – identify vulnerable 3rd party sw
Disadvantages – no runtime context, limit 3rd party scope, does not scan code
Cost – – less significant
Use-case:

- Identifying open-source component risks.
- Protecting against supply chain attacks. Checking dependencies for vulnerabilities.

Tools Supported

sonatype
aqua trivy

Tools WIP

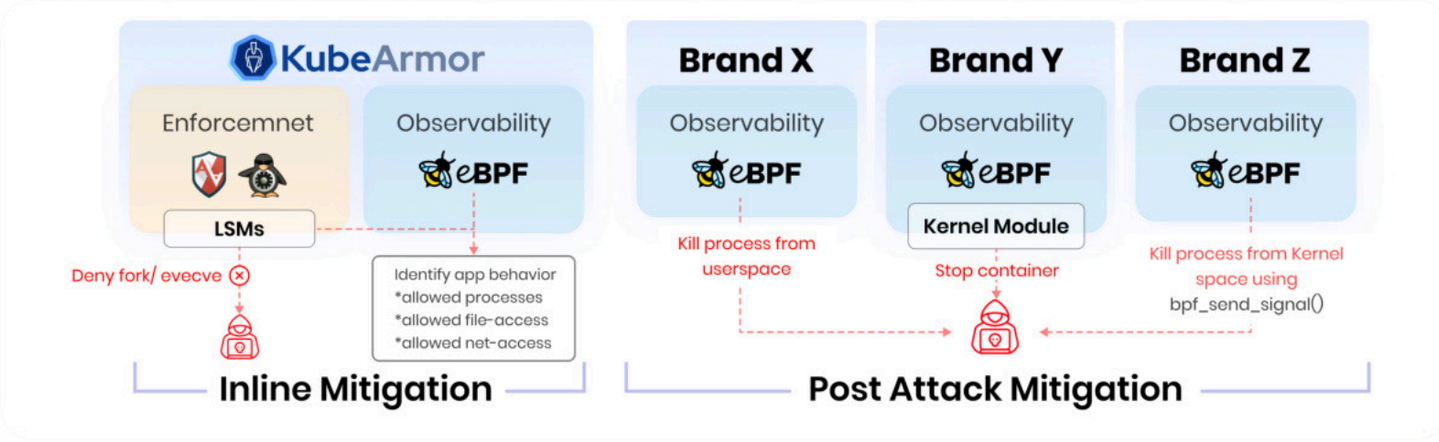
VERACODE
BLACKDUCK BY SYNOPSYS
snyk

Type	Vulnerability	Severity	Runtime Visibility	Final Severity	Actions
Vulnerability	ncurses: segfaulting OOB read: (ncursesterminfo-base@6.3_p20211120-ro)	7.1 (High)	ncurses module: Not used at runtime	Low	Virtual Patch Policy
Vulnerability	busybox: remote attackers may execute arbitrary code if netstat is used: (busybox@1.34.1-r3)	8.8 (High)	netstat module: In use at runtime	Critical	Upgrade busybox
Sensitive Asset	key.cert contains private key	Critical	key.cert: Not used at runtime	Low	Virtual Patch Policy
Sensitive Asset	root.pem contains sensitive key	Critical	root.pem is in use at runtime by /bin/vault process	High	Virtual Patch Policy

Key Takeaway

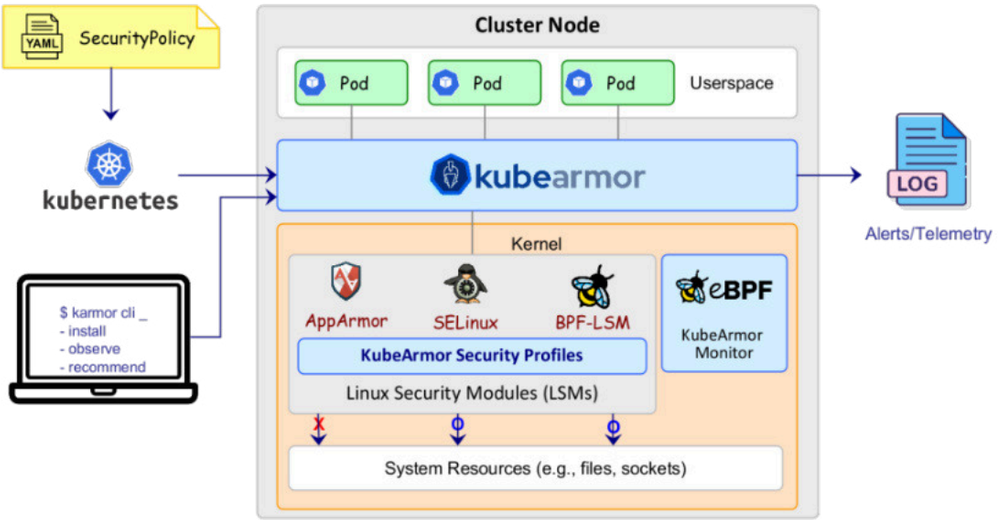
A secure software supply chain is ensured by AccuKnox's integration of Software Composition Analysis (SCA) into the development lifecycle. Simplified process to recognize and address vulnerabilities in open-source components.

KubeArmor's Distinctive Edge in Runtime Security Solutions



Differentiating Factors of KubeArmor:

- Restricts container behavior at the system level, covering process execution, file access, networking operations, and resource utilization.
- LSMs for security policies at runtime for each workload based on container or workload identities (e.g., labels).
- Generates logs for policy violations. eBPF-based monitoring to track container processes. Prompt alert on security policy breaches
- Simplifies policy management by handling internal complexities related to LSMs.
- Define and apply security policies based on metadata.



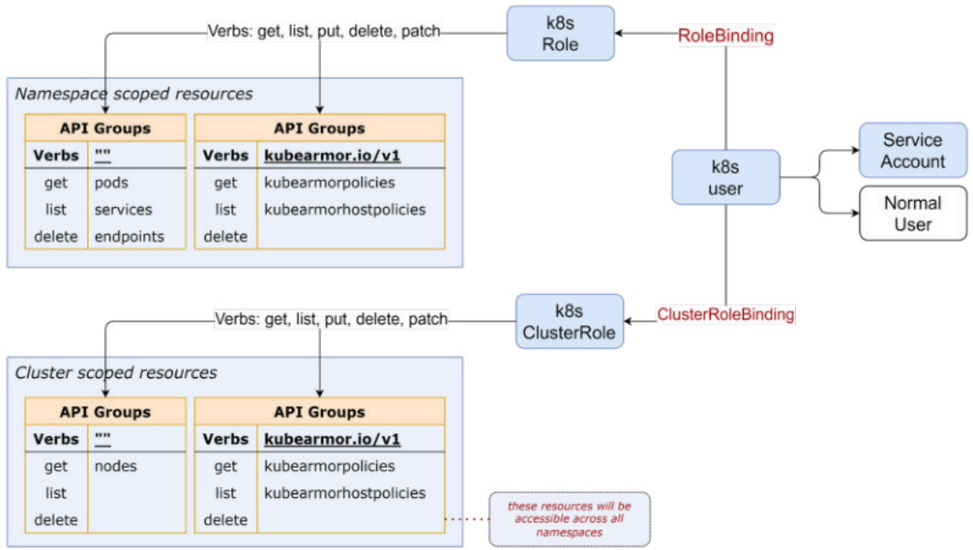
Key Takeaway

AccuKnox is powered by KubeArmor Discovery Engine. It simplifies policy management for effective, metadata-driven security solutions. Granular security policies are enforced at the system level with real-time monitoring for prompt alerts.

KubeArmor Enforcement Differentiation

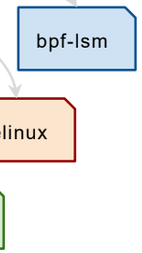
Runtime Security Engine Preventing Actions/ Attacks **Deployment Modes**

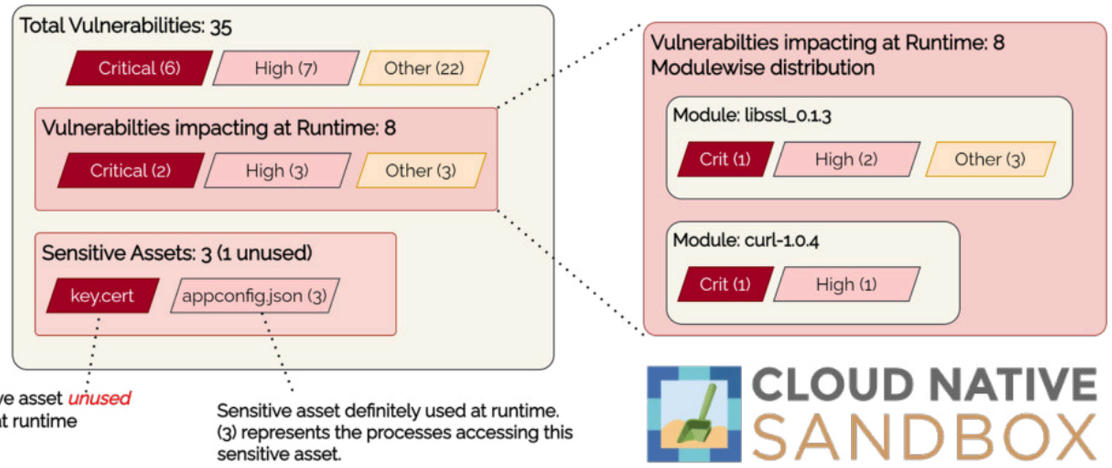
- K8s as DaemonSet
- Pure Containerized Mode
- Systems Mode




```
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 cx,
  profile /bin/sleep {
    /bin/sleep rix,
    #include
<abstractions/base>
    umount,
    network,
    capability,
    /lib/x86_64-linux-
gnu/{*,**} rm,
    /lib/{*,**} rm,
    /lib/modules/{*,**}
rm,
```





CLOUD NATIVE SANDBOX

Technical Stuff

KubeArmor generates human readable policies and is in keeping with modern practices “security as code”, “policy as code”. As a CNCF Open Source project it is being adopted by thousands of organizations globally.

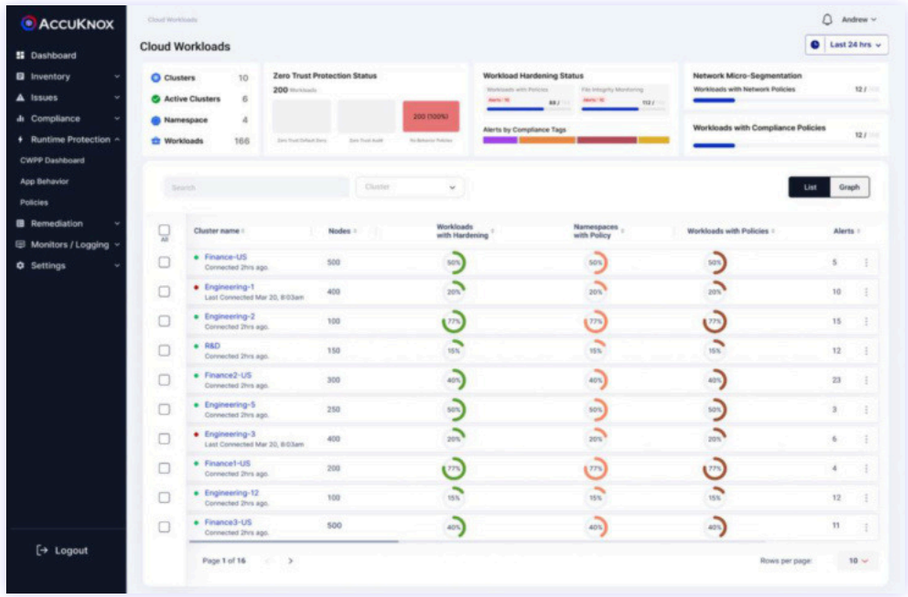
CWPP – Cloud Workload Protection Platform

Type	Vulnerability	
Zero Trust	Auto Discovered Zero Trust Policy	Custom Zero Trust Policy
	Inline Remediation	Network Microsegmentation
Recommendations	Workload Hardening Policies	
Monitoring	Logs and Alerts	
Orchestration	Multi User, Multi Tenant, Multi Cluster Management	
Integrations	Channel Integrations	
Deployments	k8s workloads support	VM and Bare-Metal support
Compliance	File Integrity Monitoring	Continuous Compliance
Roadmap	Admission Controller Support	KIEM (K8s Identities & Entitlements Management)
	Fargate Support	

Strategy

CWPP – Cloud Workload Protection Platform allows one to adopt the well-known approach of “Defense in Depth”. While CSPM delivers functionality to address static security issues, CWPP helps one address Zero Day attacks, run-time attacks.

CWPP – Fortifying Applications, Enforcing Zero Trust, Ensuring Security Resilience

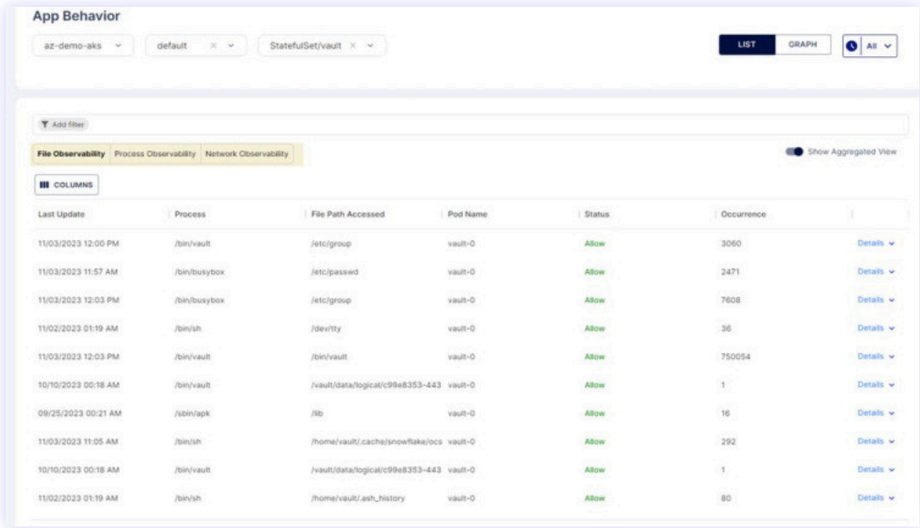


Application Security

1. Posture Discovery
2. Behavior Analysis
3. Remote Code Exec Protection
4. Cryptocurrency-mining Prevention
5. File Integrity Monitoring

Zero Trust Hardening

1. HashiCorp Vault
2. CyberArk Conjur



Security Measures

1. Man-in-the-Middle Attack Prevention
2. Denial-of-Service Protection

User Security

1. Covering Tracks Prevention
2. Impersonation Defense
3. Privilege Escalation Protection

Technical Stuff

CWPP helps one address Zero Day attacks, run-time attacks by delivering critical Zero Trust security capabilities like (1) Micro-segmentation (2) Application Firewalling (3) Kernel Hardening.

Agent or Agentless – YES is the answer!

Agentless
CSPM
(Cloud Security Posture Management)

Lightweight Industry Standard (eBPF) Sensor Agent
CWPP
Cloud Workload Protection Platform

Basic Security	Multi-Cloud Security and Compliance Posture Discovery, and protection through the use of native APIs
Application Security	App Security from Code to Run
Container Forensics and Auditing	eBPF (Extended Berkeley Packet Filter) based Observability with Auto-Discovery of App Behavior at process-level granularity
Workload Hardening, Zero Trust Security	Comply with NSA Kubernetes Hardening Guide. - Application Firewalling - Micro-segmentation - Kernel Hardening to defend against zero-day attacks. Use eBPF for observability and LSMs (Linux Security Modules) to move from observability (audit) to enforcement (block) mode

Brilliant Idea AccuKnox CNAPP delivers immense functionality without requiring an agent and provides advanced run-time functionality using an industry standard agent.

Beware of solutions that require proprietary agents, kernel modifications, etc.

Defense in-Depth – Multi Layer Zero Trust Security

Q. Why Multi Layer Zero Trust?

A. Zero Trust philosophy at every level

Application

- Least permissive access to secrets and data
- Fine grain monitoring and Application Hardening
- Application Isolation and containing blast radius

Transport

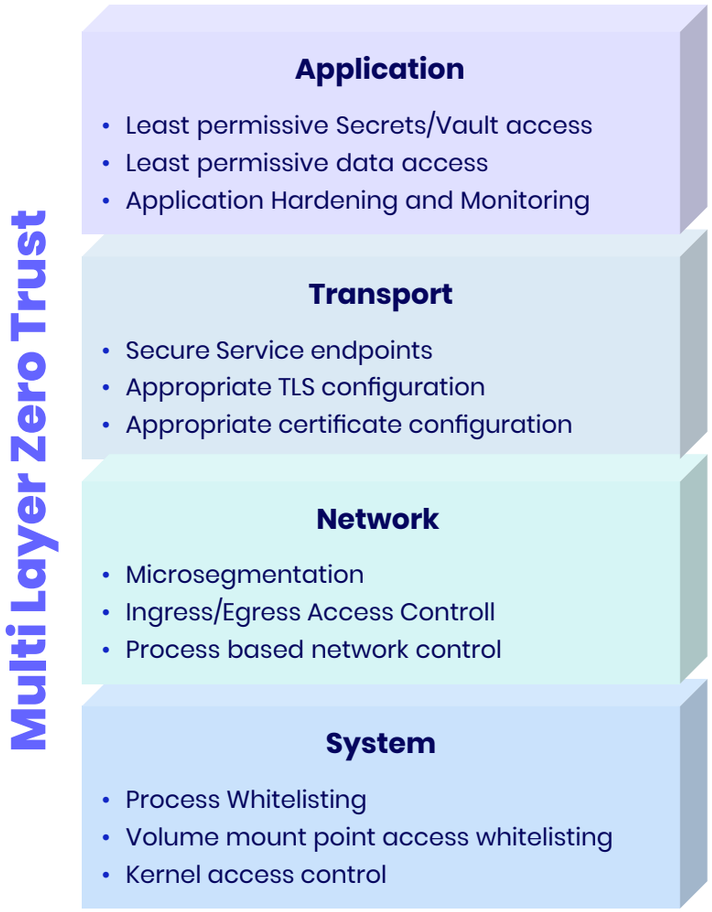
- Use of secure endpoints
- Ensure proper TLS and cert configuration

Network

- Micro-segmentation and Ingress/Egress control
- Process based Network access whitelisting

Systems

- Process Whitelisting
- Volume mount point access whitelisting
- Kernel security sensitive access primitives whitelisting



Focus

There were 70% more data breaches in 2022's Q3 than in Q2. Embrace Multi-Layer Zero Trust for robust security. From least permissive access at the application level to kernel-level whitelisting, fortify each layer to ensure comprehensive protection against evolving threats.

Zero Trust Synergy – Delivering Solutions At Every Stage

Elements of Zero Trust	AccuKnox Solution
Application Monitoring and Observability	KubeArmor: eBPF based monitoring
Application Hardening (NIST, MITRE, CIS, ENISA, FiGHT)	KubeArmor: eBPF + BPFLSM based enforcement
Network Microsegmentation	Discovery Engine + KubeArmor
Least permissive policies	Discovery Engine + KubeArmor
Process Whitelisting/Control	Discovery Engine + KubeArmor
Secure Endpoints	K8TLS
Service Mesh	K8tls + Existing Service Mesh [Roadmap]
CI/CD DevSecOps	GH Actions + KubeArmor + Discovery Engine
CIEM/KIEM (Identities and Entitlements)	AccuKnox Enterprise [coming soon]

Key Takeaway

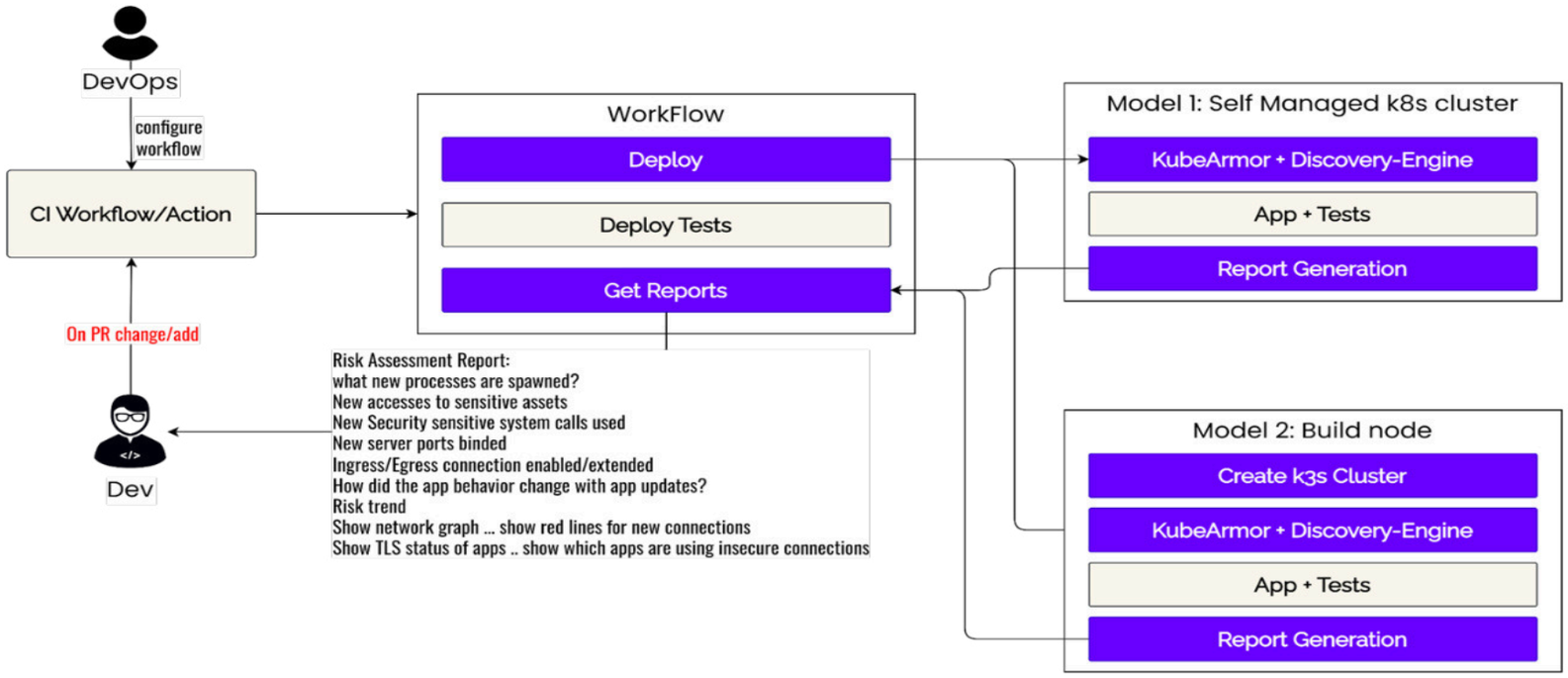
AccuKnox uses a Zero Trust framework with KubeArmor, NIST, MITRE, CIS, ENISA, FiGHT-compliant Application Hardening, and Network Microsegmentation for enhanced security in development lifecycle.

Zero Trust Assurance and Simplified DevOps Workflow

Challenges with maintaining Zero Trust Security Posture

- Applications change over time
- Application Dependencies change over time
- Cloud configuration changes over time

AccuKnox tooling helps identify deviations in Zero Trust Posture early in dev lifecycle.



Key Takeaway

Our Zero Trust CNAPP integrates with DevOps workflows, providing continuous verification across applications and cloud configurations. Get dynamic security and a commitment to Zero Trust principles.

GRC – Governance Compliance and Risk

Empowering Secure Cloud Governance, Risk, Compliance

SLOW paced, **PROCESS** driven, **POINT** in time

Real-Time Adaptive Monitoring

MANUAL process of Compliance

Continuous and Automated Compliance

SILOED and **FRAGMENTED** approach to GRC

Integrated, Correlated and Connected

TRIAGE of Alerts dilute the focus into high severity issues

Proactive Remediation and Zero False Positives

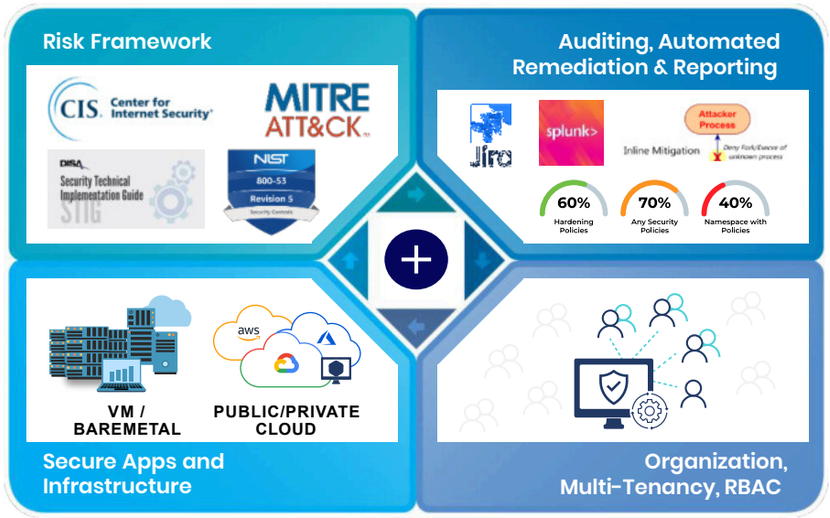
COMPLEX environment having MultiTenant, Multi-Cloud and RBAC control

Multi-Cloud, Hybrid-Cloud and On-Prem

Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

AccuKnox GRC Approach



Comprehensive and Automated GRC Platform

- Enforce Risk Framework conformance
- Visibility across entire infra or app
- Manage Organization multi-tenancy, RBAC
- Real-time Monitoring and Auditing
- Proactive and Automated Remediation
- Comprehensive Reporting

GRC ROADMAP

- Onboarding
- Auto-Discover Posture
- Baseline
- Continuous Observability
- Mode of Enforcement
- Reporting, Analytics and Auditing

1 GOVERNANCE

- Multi-Tenancy, RBAC controls, Separation of Duties
- Dashboard for definitions and runtime monitoring
- Continuous Logging, Monitoring, Alert and Audit
- Integrates into existing SOCs

2 RISK

- Auto-detect Security Posture for specific applications
- Automated generation of baseline and policy control
- Risk / compliance- based prioritization of the issues
- Workflow automation, monitoring , alerting, blocking on violation,
- Automated audit logs

3 COMPLIANCE

- System and application compliance with CIS1, CIS2, HIPAA, PCI-DSS, MITRE, NIST
- On demand Compliance Report
- Continuous, Periodic and On-demand scan
- Audit / Block based Remediation for violation
- Forensics, Audit Trail and RCA

Integrations

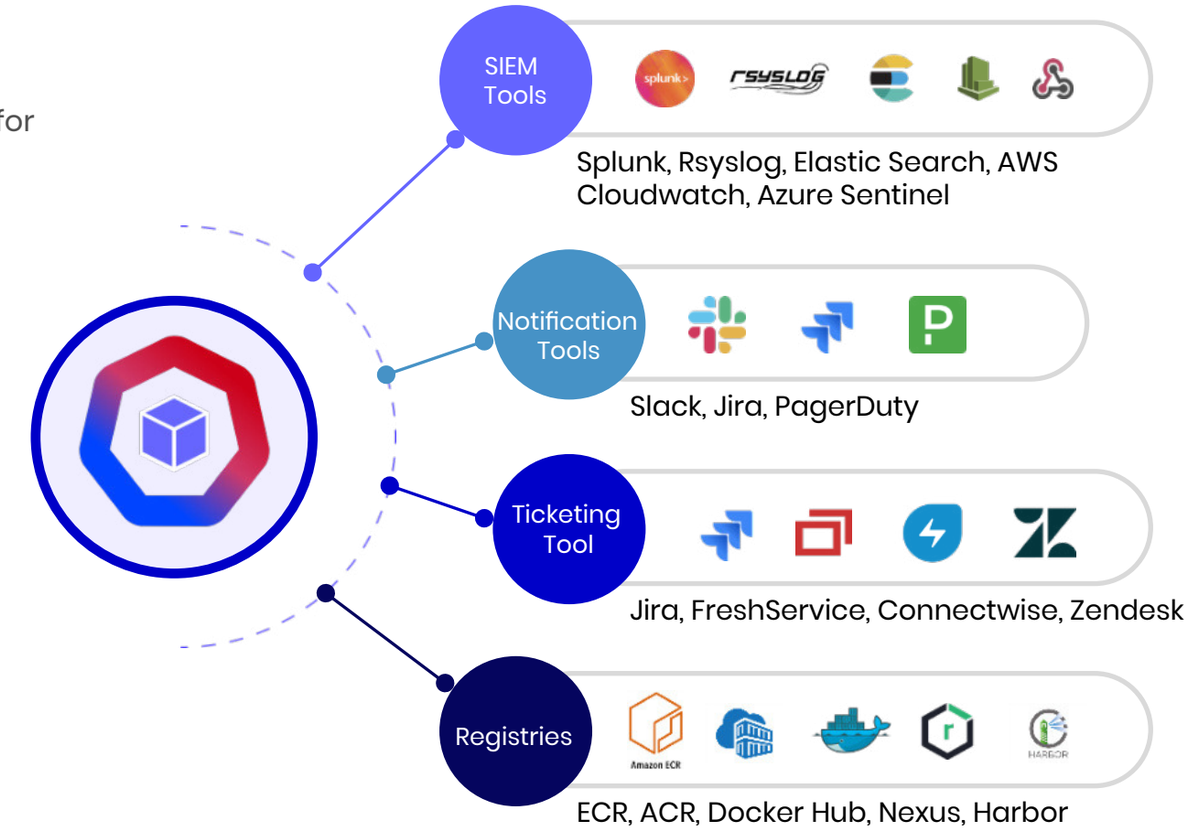
- Our lightweight agent and agentless provides us deep telemetry for workload and resources respectively.
- It can seamlessly integrate with existing security and IT-tool

✓ Monitors
✓ Logging
✓ eBPF based Telemetry

Troubleshooting

Accelerate troubleshooting with a single source of truth

- VM/Baremetal, Container or K8s context
- eBPF backed telemetry
- Logs Aggregation

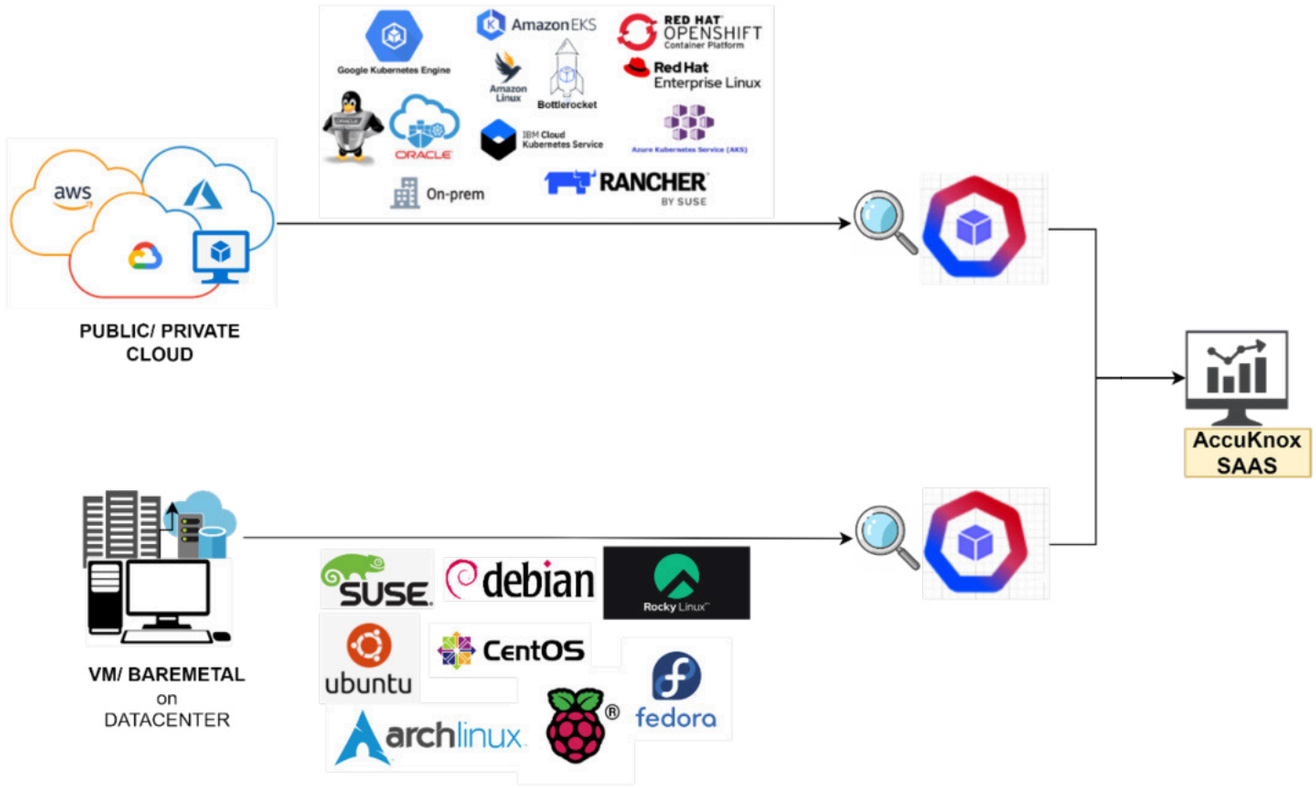


Key Takeaway

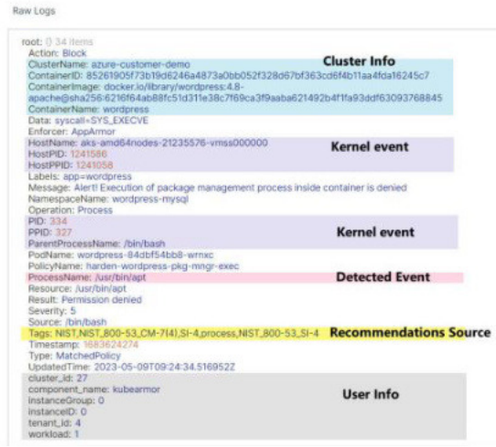
AccuKnox provides AccuKnox can integrate multiple Cloud Account, Registries, SIEM platform, Ticketing or Notifications Tools and the list is ever growing.

1. **Security Events/SIEM :** Splunk, Rsyslog, AWS CloudWatch, Elastic Search, Webhooks
2. **Notification Tools:** Slack, Jira, PagerDuty, Emails
3. **Ticketing Tools:** Jira, FreshService, Connectwise, Zendesk,
4. **Registries:** Nexus, ECR, GCR, DockerHub

Forensics



- eBPF powered rich **Telemetry**
  - **File** Accessed Logs
  - **Network** Connections Logs
  - **Process** Executed Logs
- **Audit** based Alerts
- **Block** based Alerts
- **Drift Detection** and Alerts



Key Takeaway

1. AccuKnox delivers a complete package of forensics services (process information, file access information, network activity, security-sensitive system calls, and in-depth audits of sensitive asset accesses).
2. These features cover virtual machines (VMs), public and private clouds, and onpremises installations.
3. Get end-to-end insights for reliable security analysis, guaranteeing visibility and traceability across various computing environments.

SIEM Integration

Key Takeaway

AccuKnox integrates with popular SIEMs like Splunk, Elastic, Grafana, etc. to deliver telemetry and insights so that the SIEM can be used for Analysis, Forensics, Incident Response, Reporting, etc.

AccuKnox DevSecOps Techstack

- Harness potential of multiple open source tools and optionally commercial security scanner tools to provide early detection and remediation of vulnerabilities in a shift-left approach.
- Aggregate and normalize results from different sources as a SOAR platform

Relevant for – CI/CD Security, Infrastructure Misconfiguration, Compliance, Drift Detection and Benchmarking

CI/CD Pipeline

Commit To Repo	Build	Deploy
IDE Plugins	SAST	DAST
	SCA	IAST
		Container Vulnerabilities
		Registry/Image Scan
		API Sec
		Infrastructure as Code

Findings

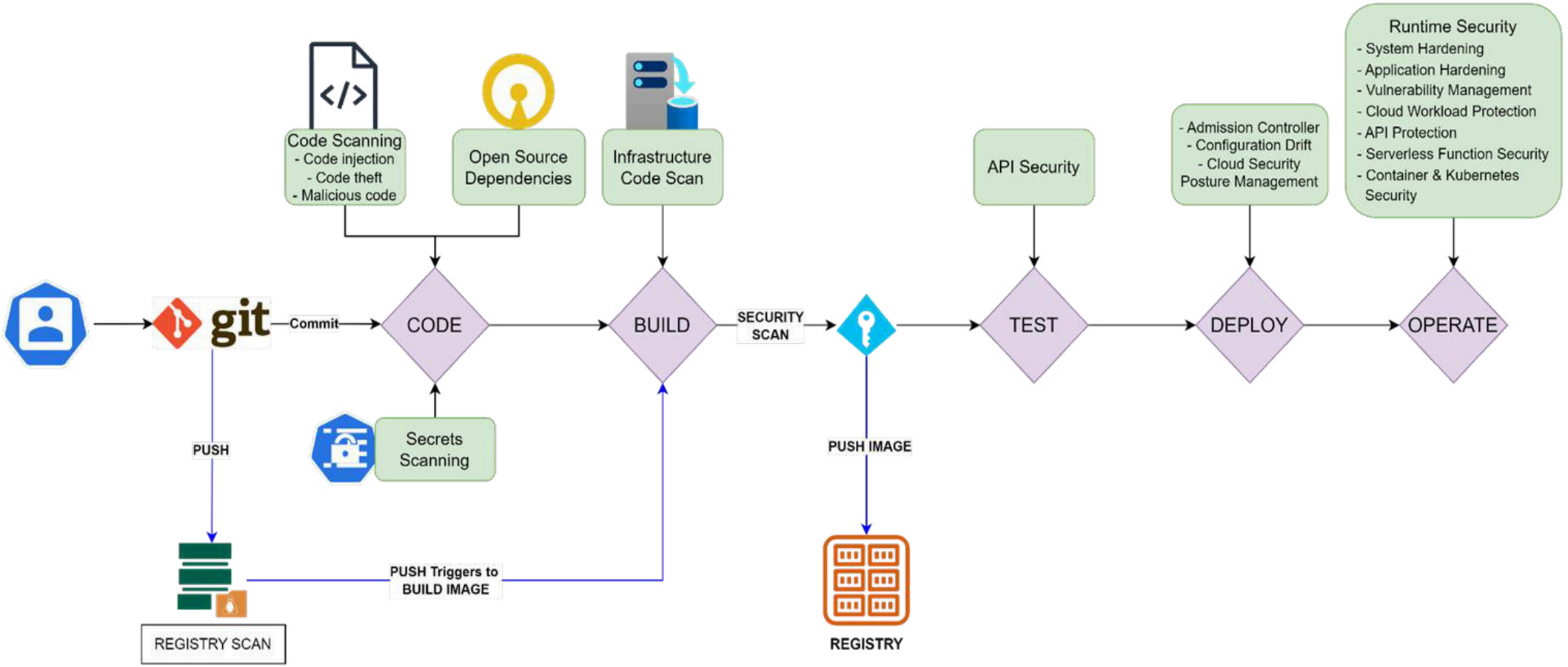
Server port status

Status	Name	Address	Status	Version	Ciphersuite	Hash	Signat
🚨	firewall	localhost:49180	NO_TLS				
🚨	verifier	localhost:49181	NO_TLS				
🚨	app_server	localhost:49182	NO_TLS				
🟢	Google	google.com:443	TLS	TLSv1.3	TLS_AES_256_GCM_SHA384	SHA256	ECDSA
🟢	AccuKnox	app.accuknox.com:443	TLS	TLSv1.3	TLS_AES_256_GCM_SHA384	SHA256	ECDSA
🚨	BadSSL	self-signed.badssl.com:443	TLS	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	SHA512	RSA
🚨	BadSSL	expired.badssl.com:443	TLS	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256	SHA512	RSA

Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

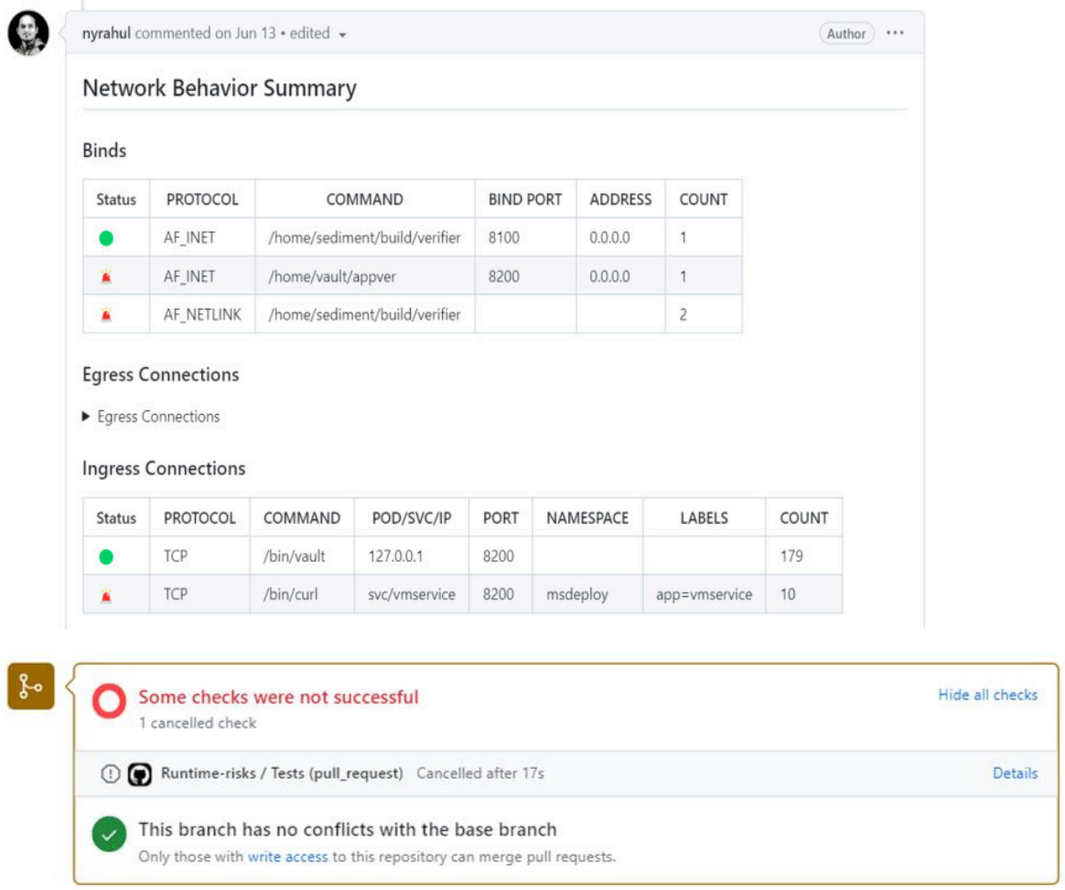
Orchestrating Secure DevOps Life Cycles with AccuKnox



Key Takeaway

Our tooling blends CI/CD pipelines, automates policy recommendations, and conducts container vulnerability screening, ensuring a secure DevOps journey with GitOps, robust identity verification, and runtime security solutions.

AccuKnox DevSecOps – IaC



nyrahul commented on Jun 13 • edited — Author

Network Behavior Summary

Binds

Status	PROTOCOL	COMMAND	BIND PORT	ADDRESS	COUNT
●	AF_INET	/home/sediment/build/verifier	8100	0.0.0.0	1
▲	AF_INET	/home/vault/appver	8200	0.0.0.0	1
▲	AF_NETLINK	/home/sediment/build/verifier			2

Egress Connections

▶ Egress Connections

Ingress Connections

Status	PROTOCOL	COMMAND	POD/SVC/IP	PORT	NAMESPACE	LABELS	COUNT
●	TCP	/bin/vault	127.0.0.1	8200			179
▲	TCP	/bin/curl	svc/vmservice	8200	msdeploy	app=vmservice	10

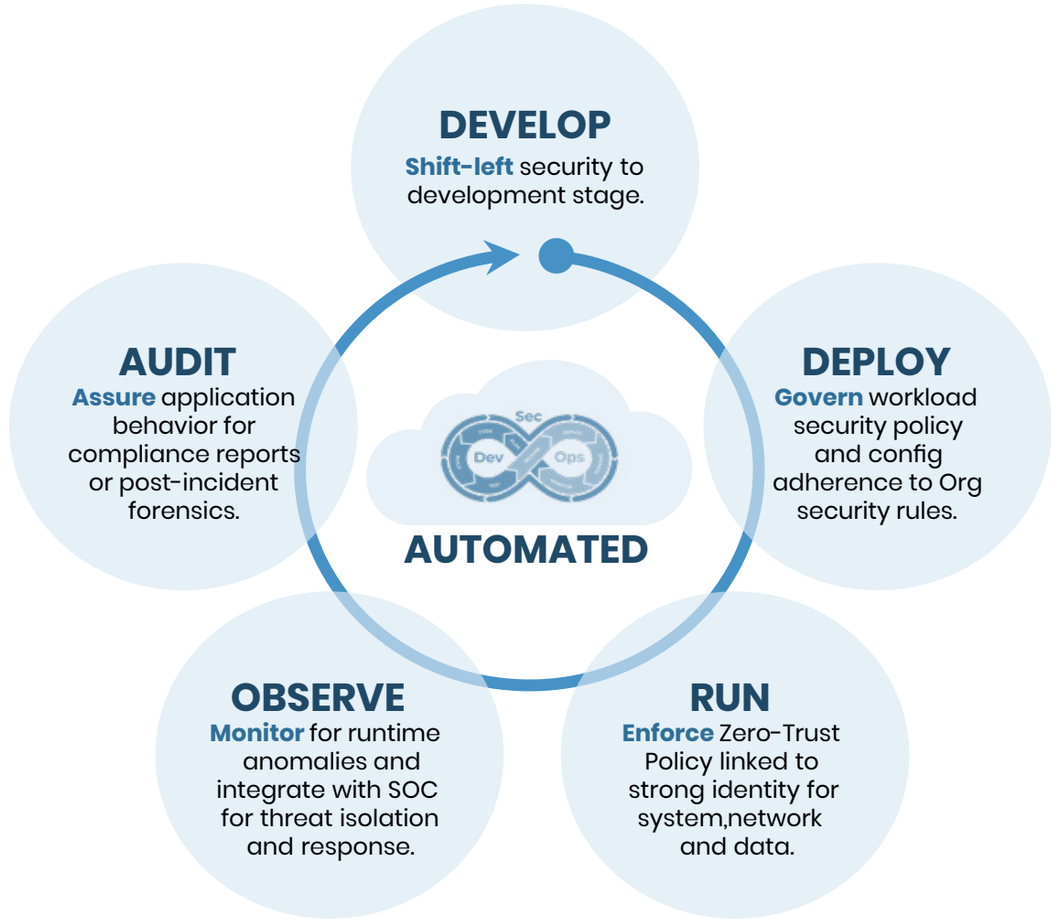
Some checks were not successful — Hide all checks

1 cancelled check

Runtime-risks / Tests (pull_request) Cancelled after 17s — Details

This branch has no conflicts with the base branch

Only those with write access to this repository can merge pull requests.



Beware

Template misconfigurations pose a significant security risk for IaC. It potentially allows skilled attackers to exploit system security or unintentionally undermine system security.

Deploy Securely Across Public and Private Clouds

We support SaaS model for public Cloud security with an option to host customer's data on S3 bucket owned by them

Modern Infrastructure

- Public Clouds
  - AWS
  - Azure
  - GCP

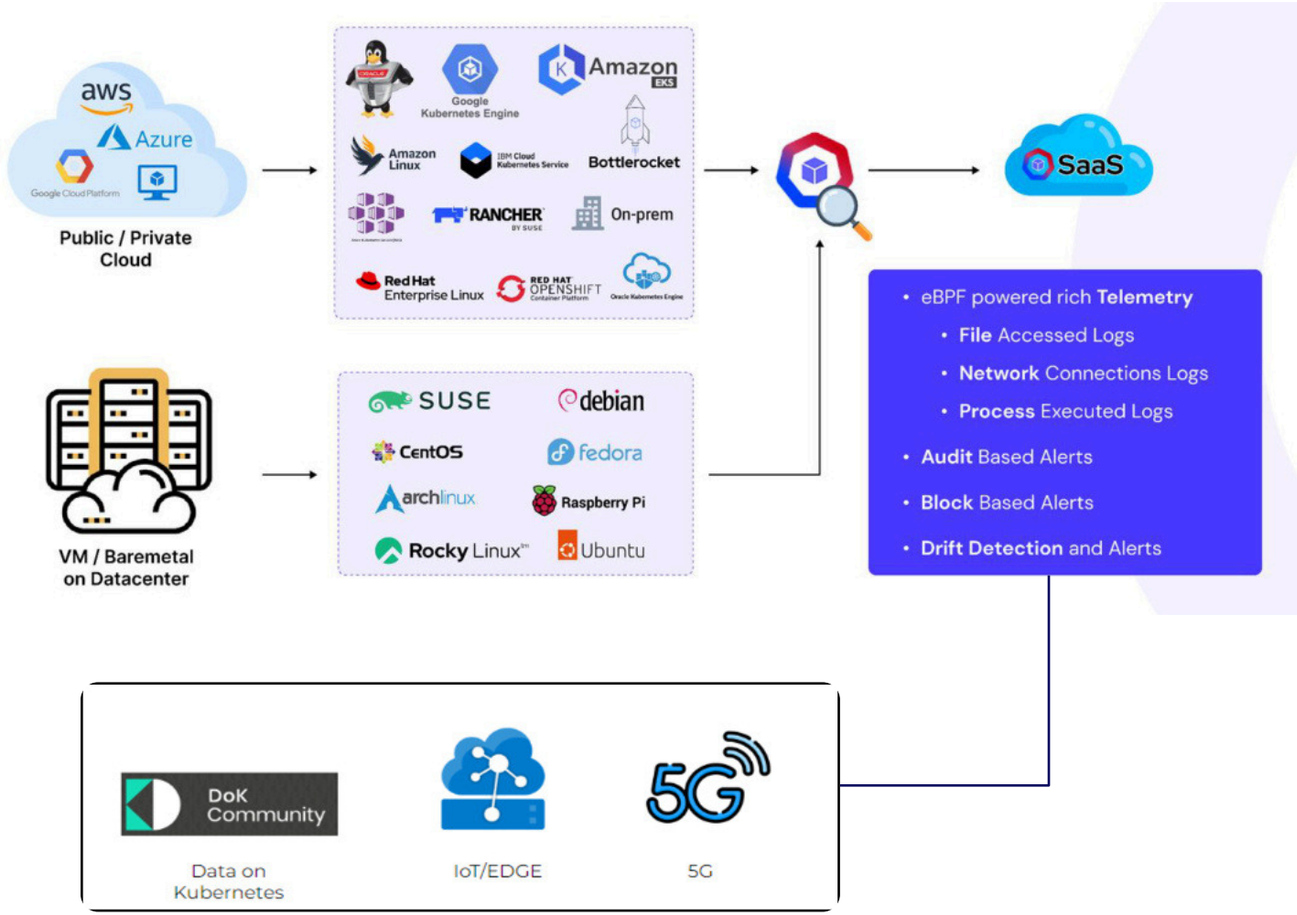
To support coverage for Digital Transformation Journey, we have controls and technical "knowhow" to secure the following:

Modern Workload

- Kubernetes
- Containers

Traditional Workload

- VM/Baremetal



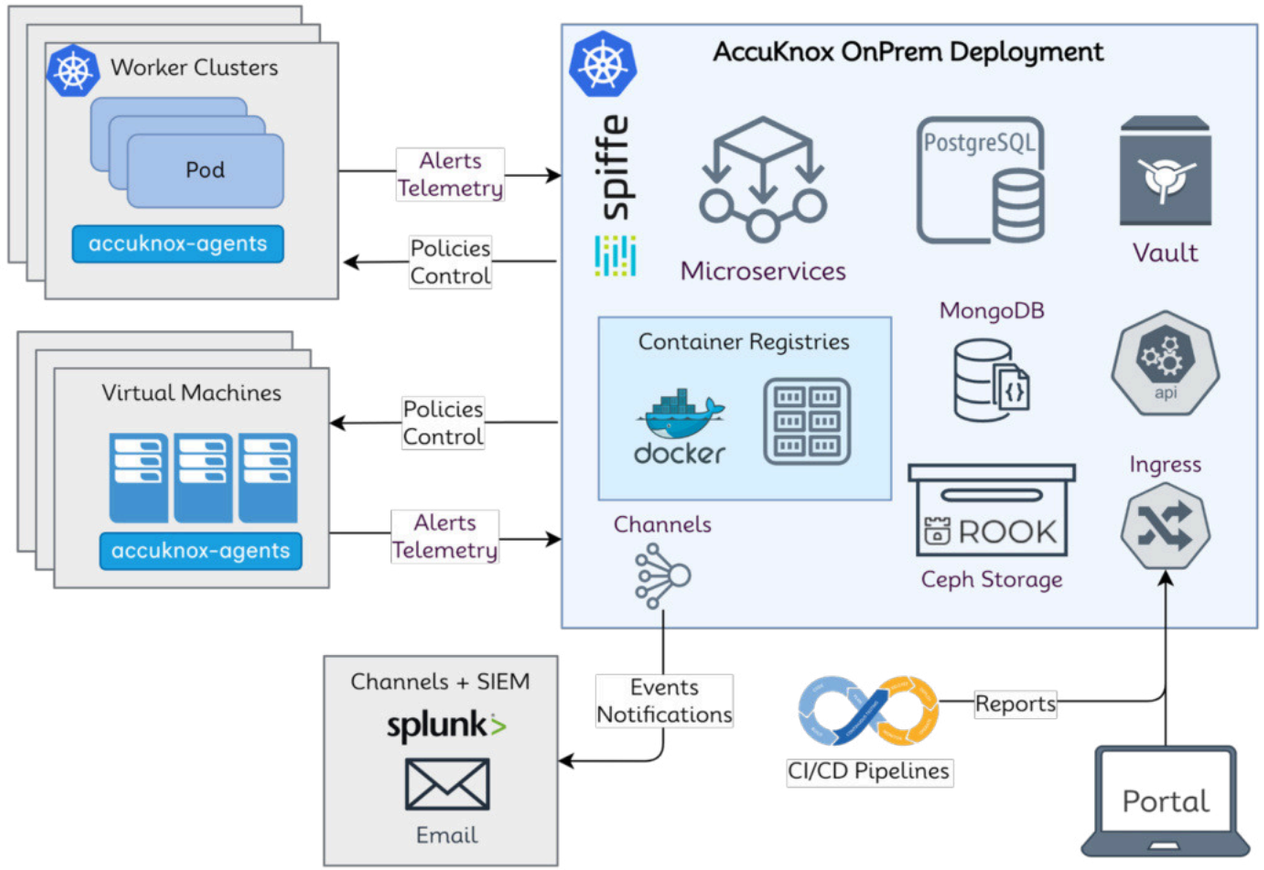
Technical Stuff

AccuKnox guarantees efficiency in public and private cloud deployments with end-toend visibility and support for cloud native resources and workloads across major platforms (AWS, Azure, and Google Cloud).

Air Gapped Environments

We support On-Prem airgapped deployment model to secure infrastructure and applications on restricted environments such as

We primarily require installation of Microservices, databases, secrets management, scaling, accuknox-agents. For more info, visit Help Documentation



Key Takeaway

AccuKnox uses strong governance, multi-tenancy, RBAC controls, duty separation, thorough risk assessment, automation, and compliance standards to provide a safe, legal, and auditable cloud infrastructure.

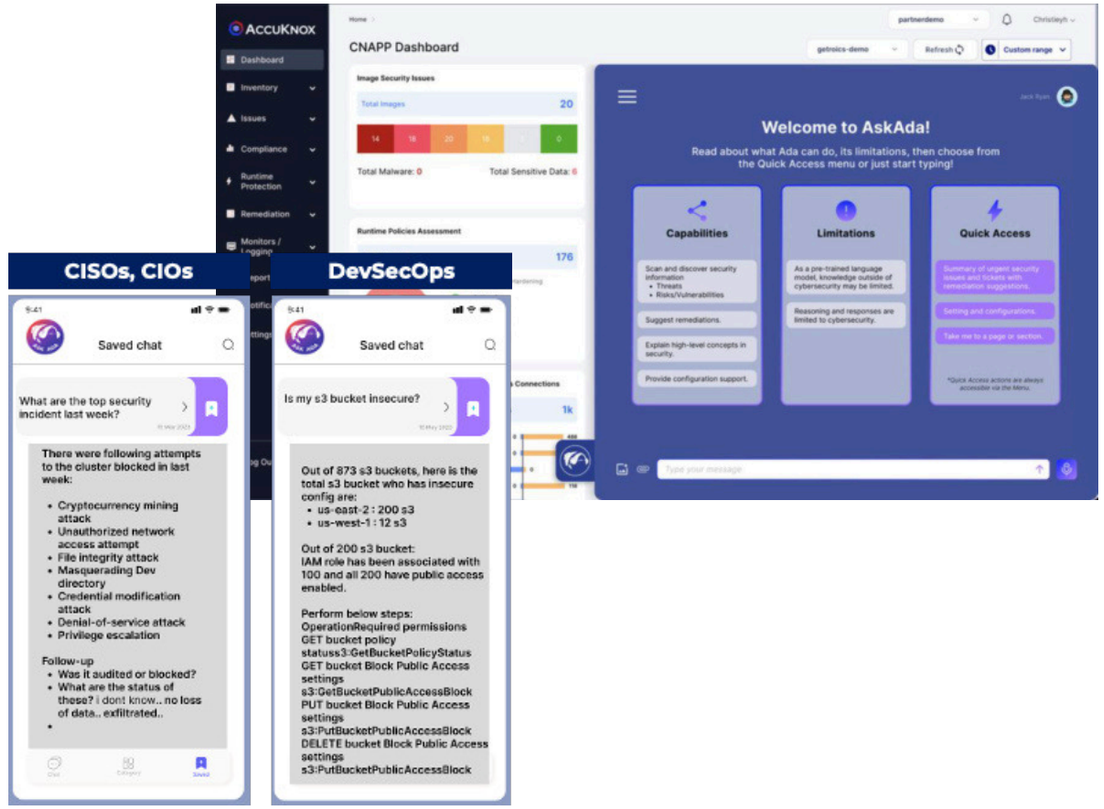
Revolutionizing Security Posture with AI Insights Automate the mundane, Empower the expert

Proactive action on drift or anomalies.
Security Posture should be easier to comprehend and propose Actionable insights

Know current security posture quickly.
Security should be reflecting current posture in a non-intrusive way (NLP)

Empower different personas towards Security.
Security should provide Assistive Remediation to every security personas

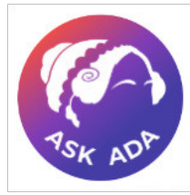
Translating customized request into security configuration.
Generating automatic configuration based on simple text



Key Takeaway

CyberAiDE (Ask-Ada) is a revolutionary security tool that offers proactive anomaly response, NLP-driven posture insights, and automatic configuration generation, empowering diverse security personas with actionable insights

Streamlining Cloud Security with LLM Automate the Mundane, Empower the Expert



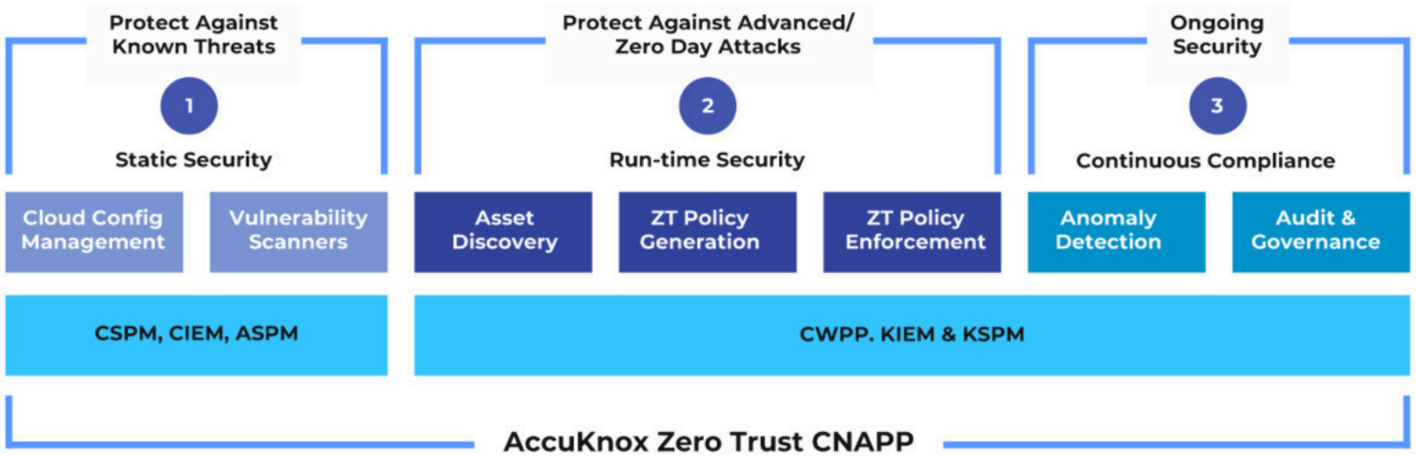
Discovery	Actionable Insights	Assistive Remediation	Automated Customized Actions
NIST, CIS, PCI, MITRE Compliant Status	List Vulnerabilities OCCURRED during last week	IDENTIFY controls that needs to fulfil to be CIS Compliant?	GENERATE a KubeArmor network policy to allow port 443 and deny everything else
General Query on PROBLEM that platform can answer	List critical Vulnerabilities EXPOSED at Runtime	CREATE Tickets for all of the exposed s3 bucket	CONFIGURE Trigger to SLACK for vuln detected with severity >7
General Query on FEATURE that platform has	List all the NETWORK Exposure in Cloud and Cluster	IDENTIFY Hardening Policies that needs to be ACTIVATED for NIST compliance	IDENTIFY controls that needs to fulfil to be CIS Compliant?
General Query on MISCONFIG or VULN	Provide Hardening, Compliance PERCENTAGE in last week	Send ALERT when Registries images that have sensitive keys or network exposed vulnerabilities	SCHEDULE a Scan every Tuesday 3 AM PT
	Summarize CIS Controls that were violated last week	Send ALERT on Slack when any of the Critical Vulnerability detected	CREATE a terraform script to deploy EC2 Instances securely

Key Takeaway

AccuKnox's CyberAiDE (Ask-Ada) is an LLM powered Cloud Security Solution that aims to Automate the Mundane Empower the Expert

ZERO-TRUST CNAPP (Cloud Native Application Protection Platform)

Cloud Security at Scale with Runtime Protection



Key Takeaway

Zero Trust is a journey not a destination. As they say it is hard to get to Zero Trust, it is even harder to stay there. AccuKnox CNAPP platform allows you to get to Zero Trust in a systematic way.

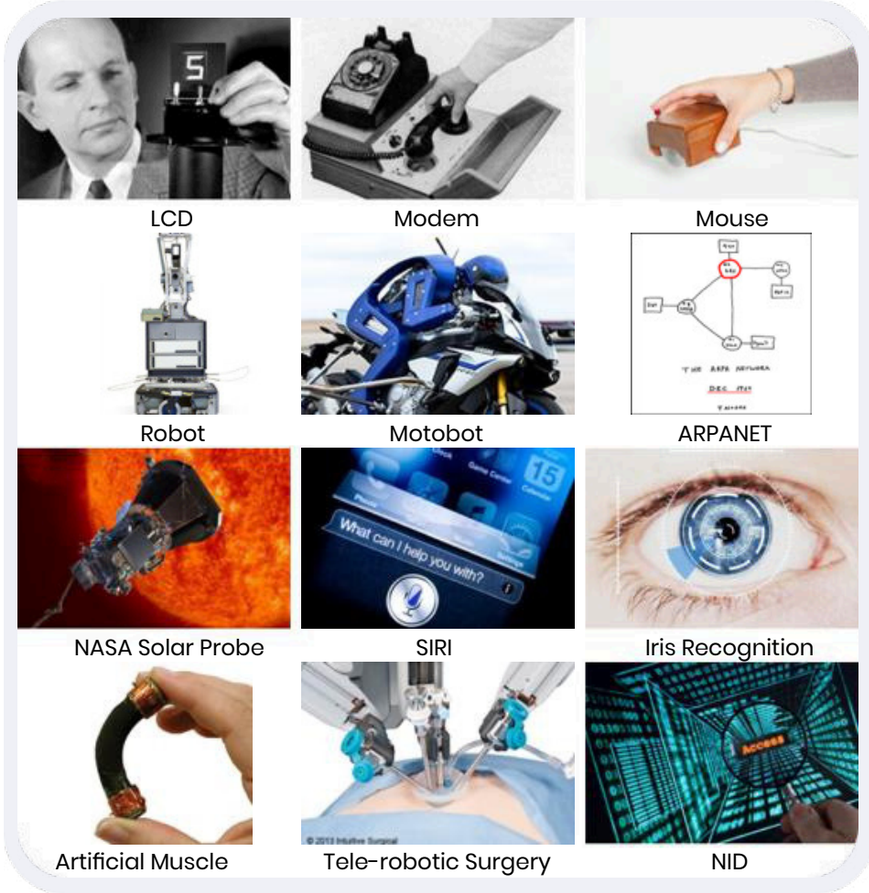
About AccuKnox

- Deep Tech, Innovation Roots
- Customer Accolades
- Innovation Patents
- Analyst praise
- Power of partnerships
- Differentiation

Deep Tech, Innovation Roots

AccuKnox was co-created in partnership with Stanford Research Institute
(SRI International) CyberSecurity Computer Science Labs
SRI is an investor and R&D Partner

75 YEARS OF INNOVATION SRI International



Key Takeaway

SRI International, founded in 1946, has been a pioneer in creating innovative products like the mouse, modem, MICR ink, SIRI voice recognition, and robotic surgery. In the field of cybersecurity, SRI has developed anomaly detection, intrusion prevention, and intrusion detection. The company is also an R&D partner and investor in AccuKnox, contributing to the advancements in modern living.

Customer testimonials

Large US Government Contractor

"We performed an extensive analysis of comparable industry offerings and selected AccuKnox due to its support for public and private cloud and highly differentiated capabilities in the areas of Risk Prioritization, Drift Detection, and Advanced Compliance. Furthermore, we were very impressed with AccuKnox's integration with leading Vulnerability Management platforms like Nessus."

Large Cyber Insurance Provider

"Their comprehensive and integrated offering; flexible deployment options; ongoing R&D commitment; Open Source foundations; and their track record of successful partnerships made them a clear winner."

Large Digital Health Provider

"Zero Trust security is a Clint Health imperative and commitment we have to our customers. AccuKnox's leading product combined with their successful track record of partnering with their customers forms the foundation for this objective."

European Cyber Service Provider

"AccuKnox's powerful combination of CSPM and CWPP; OpenSource foundations; In-line Zero Trust Security; Support for Public and Private Clouds; made them the ideal partner for us. Our client, a Large European CyberSecurity agency, was looking for a Zero Trust Security Solution that supports Private Cloud platforms. Our win is a clear testament to the value our clients see in this partnership. We look forward to many more successes ahead."

Key Takeaway

Because of its sophisticated skills in Risk Prioritization, Drift Detection, and Compliance, AccuKnox is a reliable option for a wide range of sectors. It provides comprehensive, adaptable, Zero Trust security solutions and is recognized by government contractors, cybersecurity vendors, and innovators in digital health.

Pioneering Security Solutions with Patents

10+ Patents


Patented

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


Patented

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


Patented

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


Patented

Container Function Virtualization: high-performance L7 protocol analysis


Patented

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


Patented

System and method for predefined policy specification for containerized workloads


Patented

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


Patented

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


Patented

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

Focus

With more than ten patents to its name, AccuKnox is a proud innovator in the fields of deep learning for ultra-scale container forensics, federated peer-based anomaly detection, and live eBPF-based data flow tracing across dynamic container clusters. Get a free demo of our stateof-the-art products on the **AWS Marketplace** right now

Security Experts Laud AccuKnox Innovations

"Zero Trust run-time Cloud Security has become an organizational imperative for Companies and Governments. Accuknox' highly differentiated approach, their eBPF foundations and their seminal innovations developed in partnership with Stanford Research Institute (SRI) positions them very well to deliver a highly efficient Zero Trust Cloud Security platform."

Frank Dickson
Vice President
Security and Trust, IDC

"Run-time Cloud Security is extremely important to detect Zero Day attacks, Bitcoin Miners, DDOS attacks, etc. Accuknox delivers a critical component of the CWPP (Cloud Workload Protection Platform). Their ability to deliver Network, Application and Data Security makes Accuknox a unique and differentiated offering."

Chris Depuy
Technology Analyst
650 Group Analyst

"Accuknox' foundational capabilities are innovative in the areas specific to Kubernetes security. By combining technologies like un-supervised Machine Learning and Data Provenance, Accuknox is positioned to deliver a comprehensive and robust cloud native Zero-Trust security platform to their customers."

Chase Cunningham
Renowned Cyber Security Analyst and Zero-Trust Expert

Key Takeaway

AccuKnox, a pioneer in cloud-native security, is renowned for its innovative Zero Trust runtime security, Cloud Workload Protection, and Kubernetes-specific capabilities, backed by a groundbreaking partnership with Stanford Research Institute.

Power of Partnerships

IBM

LF EDGE

AccuKnox joins mimik Technologies, IBM as Open Horizon project partner

Optimized for Intel® Smart Edge

Zero Trust Cloud Native Application Protection

ACCUKNOX intel

KubeArmor

Overview of KubeArmor

KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operations) of containers and nodes (VMs) at the system level. KubeArmor leverages Linux security modules (LSMs) such as AppArmor, SELinux, or BPF-LSM) to enforce the

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

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

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

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

KubeArmor support for Oracle Container Engine for Kubernetes (OKE)

KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)

5G OPEN INNOVATION LAB

September 13, 2022

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

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

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

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

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

aws

Secure Bottlerocket deployments on Amazon EKS with KubeArmor

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

vmware troduction

August 1, 2022

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

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

News Flash

AccuKnox, brings together a range of industry partnerships (Software Vendors, Hyperscalers, Systems Integrators, MSSP, Resellers, etc.) to deliver customers with the most optimal solution, quick implementation approach and best ROI (Return on Investment)

Differentiation – Our Unique Offerings

Features	AccuKnox	Prisma	Wiz	Orca Security	Sysdig
Comprehensive CNAPP Coverage	✓ ✓ ✓	✓	✗	✓	✗
CNCF OpenSource Led	✓ ✓	✗	✗	✗	✓ ✓ ✓
Continuous Detection and Response	✓	✓	✓	✓	✓
Continuous Detection and In-line Mitigation	✓ ✓ ✓	✓ ✓	✗	✗	✗
Support for on-premises air-gapped env.	✓ ✓ ✓	✓	✗	✗	✗
ASPM	✓ ✓ ✓	✓ ✓	✓	✗	✗

Differentiation – Our Unique Offerings

Features	AccuKnox	Prisma	Wiz	Orca Security	Sysdig
Drift Detection and Custom Baseline	✓ ✓ ✓	✓	✓	✗	✓ ✓
Auto-Discovery of App Behavior	✓ ✓ ✓	✓	✗	✗	✓
Network Micro-segmentation	✓ ✓ ✓	✓	✗	✗	✓
Network Topology and Continuous Monitoring	✓ ✓ ✓	✓	✓	✗	✓
Container exec and drift prevention	✓ ✓ ✓	✓ ✓	✗	✗	✓
5G, Edge & IoT Security	✓ ✓ ✓	✓ ✓	✗	✗	✗

Summary

Summary

Zero Trust is an imperative in current times.

ZT is a journey not a destination.

ZT requires a comprehensive CNAPP solution.

AccuKnox is your partner in your ZT journey.

About AccuKnox

AccuKnox provides a Zero Trust Cloud Native Application Protection Platform (CNAPP). AccuKnox is the core contributor to Kubernetes Run-time security solution, KubeArmor®, a very popular CNCF (Cloud Native Computing Foundation) project. AccuKnox was developed in partnership with SRI (Stanford Research Institute) and is anchored on seminal inventions in the areas of Container Security, Anomaly Detection, and Data Provenance. AccuKnox can be deployed in Public, Private and Hybrid Cloud environments. AccuKnox is funded by leading CyberSecurity Investors like National Grid Partners, MDSV, Avanta Venture Partners, Dolby Family Ventures, DreamIT Ventures, 5G Open Innovation Lab and Seedop.

www.accuknox.com contact@accuknox.com

as featured in:

Leadership

Nat Natraj
CEO, Co-founder,Business
LinkedIn

Phil Porras
Co-founder, Innovations
LinkedIn

Rahul Jadhav
Co-founder, VP of Engg
LinkedIn

Brian Burgess
Product
LinkedIn

Raj Panchapakesan
Global Head- Business Development& Partner Ecosystem
LinkedIn

Jen Wilson
Director, Operations& Customer Success
LinkedIn

20+
TOOLS INTEGRATION

10+
PATENTS

30+
TRUSTED PARTNERS

10+
COMPLIANCE FRAMEWORKS

You cannot secure what you cannot see.

Your most sensitive information is stored on cloud and on premise infrastructure. Protect what is most important from cyber attacks. Real-time autonomous protection for your network's edges.

Ready to get started? Get Free Trial →