AccuKnox Zero Trust CNAPP
Compliance with Gartner Recommendations

Prevent Zero Day Attacks

as featured in:
aws, ORACLE, Gartner, NEPHIO, IBM, LF EDGE
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 documents¹.

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.

**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).
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.
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
Mapping to Gartner CNAPP Guidelines
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:

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.

Gartner CNAPP Recommendations and AccuKnox Compliance Fulfillment

Get a Demo

Overview AccuKnox Zero Trust CNAPP combines Mapping to Gartner CNAPP Guidelines Summary of Gartner’s viewpoints Gartner Recommendations for CNAPP Proving Effectiveness against Zero Day Attacks Summary About
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure</td>
<td>Major Cloud Providers</td>
<td>AccuKnox provides multi-cloud security with coverage to all major cloud providers such as AWS, AZURE &amp; GCP. We also additionally support GCP, Oracle Cloud and Private Cloud platforms like VMWare, OpenStack etc. Visit help to know more.</td>
</tr>
<tr>
<td>Application Security</td>
<td>Application layer observability/monitoring</td>
<td>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</td>
</tr>
<tr>
<td>Category</td>
<td>Support for VMware-based infrastructure (on-premises and public-cloud-based)</td>
<td>AccuKnox provides security for on-prem infrastructure such as VMware, private cloud such as IBM Private Cloud, Openshift and public cloud infrastructure.</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Support for other cloud and container environments such as Red Hat OpenShift and SUSE’s Rancher</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Traditional static analysis of custom code for unknown vulnerabilities</td>
<td>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</td>
<td></td>
</tr>
</tbody>
</table>

AccuKnox provides Software Development Life Cycle through below process:

- **CODE**
  - Static Code Analysis
  - Software Composition Analysis
  - Secret Scanning
- **IMAGE**
  - Vulnerability Scanning
  - Risk Prioritization
  - Sensitive Assets
  - Container Compliance
- **CLOUD**
  - Cloud Account/Asset Configuration Assessment
  - CIS Benchmarking
- **RUNTIME**
  - App behavior analysis
  - Workload hardening
  - FIM, Compliance
  - Zero Trust Policy
  - Network Micro segmentation
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td>API scanning for unknown</td>
<td>AccuKnox can detect application attack scenarios at running app to find</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vulnerabilities</td>
<td>vulnerabilities of application post-deployment based on OWASP Top10 for</td>
<td>finding common CVE and security best practices</td>
<td></td>
</tr>
<tr>
<td>Development pipeline/</td>
<td>AccuKnox can help to detect 3rd party dependencies/lib in open source which</td>
<td></td>
<td></td>
</tr>
<tr>
<td>software supply chain security</td>
<td>are used during dev, test or production to identify vulnerable 3rd party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>beyond SCA (see Note 4)</td>
<td>software and identify open-source component risks. Protecting against supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>chain attacks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development pipeline</td>
<td>AccuKnox can help to detect vulnerability early in the CI pipeline using its</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hardening</td>
<td>static code analysis, software composition analysis and secret scanning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>AccuKnox can detect hard coded secrets in repositories and can fail a build</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>in the CI pipeline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitive data in structured</td>
<td>AccuKnox can detect hard coded secrets in repositories and can fail a build</td>
<td></td>
<td></td>
</tr>
<tr>
<td>data repositories</td>
<td>in the CI pipeline</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Get a Demo
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Security Policy for All</td>
<td>All Artifacts</td>
<td>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.</td>
<td>Block access to /vault/</td>
</tr>
<tr>
<td>Runtime Security</td>
<td>Extended Berkeley Packet Filter (eBPF) support.</td>
<td>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</td>
<td>Allow access to /vault/ from /bin/vault only</td>
</tr>
</tbody>
</table>
## 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.
## 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.

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.

## Summary of Gartner’s viewpoints

- **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.

**KubeArmor**
- Runtime security engine
- not just observation/monitoring
- Deployment Modes
  - K8s as daemonset
  - Pure Containerized mode
  - Systemd mode

**Mentions LD_PRELOAD:**

- **Linux System Call Interception**

---

### Gartner CNAPP Recommendations and AccuKnox Compliance Fulfillment

Get a Demo
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Recommends use of DaemonSets for securing application</td>
<td>AccuKnox deploys KubeArmor as a DaemonSet on nodes. Full security monitoring and policy enforcement across the Kubernetes cluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network connectivity mapping and real-time workload visibility for critical VMs and containers.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Category: Scanning of containers and container registries for risk assessment

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.

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 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.

Overview AccuKnox Zero Trust CNAPP combines Mapping to Gartner CNAPP Guidelines Summary of Gartner’s viewpoints Gartner Recommendations for CNAPP Proving Effectiveness against Zero Day Attacks Summary About

Gartner CNAPP Recommendations and AccuKnox Compliance Fulfillment Get a Demo

24
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
</table>
| 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 |                                                                                       |                                                                                       |
<p>| 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. |                                                                                       |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Predefined Compliance Templates</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ease of Use</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

Gartner CNAPP Recommendations and AccuKnox Compliance Fulfillment

Get a Demo
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pricing and Licensing</strong></td>
<td>Usage Pricing</td>
<td>AccuKnox offers a very simple pricing model as depicted here</td>
<td></td>
</tr>
<tr>
<td><strong>Integration with Tools &amp; Workflows</strong></td>
<td>Integration and Support for Key Tools</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Advanced Analytics</strong></td>
<td>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</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Category
### Sub category
#### AccuKnox Compliance

<table>
<thead>
<tr>
<th>Cloud Control Plane API-based Integration</th>
<th>Integration into CI/CD Development Toolsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccuKnox supports API-based integration with cloud control planes. This allows inspection of cloud account findings, vulnerability scanning, asset inventory etc.</td>
<td>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.</td>
</tr>
</tbody>
</table>

---

### Screen Shot, Table, Architecture Diagram

**Diagram:**
- **DEVELOP**: Details on security policy, post-mortem analysis, and integration with DevOps tools.
- **AUDIT**: Focuses on compliance monitoring, policy enforcement, and integration with DevSecOps tools.
- **DEPLOY**: Highlights security policy enforcement, compliance monitoring, and integration with DevOps tools.
- **RUN**: Emphasizes runtime security, policy enforcement, and integration with DevSecOps tools.

**Table:**
- **DEVELOP**
  - Policy enforcement
  - Continuous monitoring
  - DevOps integration
- **AUDIT**
  - Compliance tracking
  - Post-mortem analysis
  - DevOps integration
- **DEPLOY**
  - Security policy enforcement
  - Compliance monitoring
  - DevOps integration
- **RUN**
  - Runtime security monitoring
  - Policy enforcement
  - DevOps integration
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub category</th>
<th>AccuKnox Compliance</th>
<th>Screen Shot, Table, Architecture Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance and Governance</td>
<td>Scanning of Containers and Container Registries for Risk</td>
<td>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.</td>
<td><img src="image" alt="Screen Shot, Table, Architecture Diagram" /></td>
</tr>
<tr>
<td></td>
<td>Snapshots of Running Workloads</td>
<td>Get snapshot-based analysis with our AccuKnox. Real-time visibility into containerized applications and threat detection and response.</td>
<td><img src="image" alt="Screen Shot, Table, Architecture Diagram" /></td>
</tr>
<tr>
<td></td>
<td>Ready To Use Compliance Templates</td>
<td>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.</td>
<td><img src="image" alt="Screen Shot, Table, Architecture Diagram" /></td>
</tr>
</tbody>
</table>
Proving Effectiveness against Zero Day Attacks
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
These are a few more examples that have been covered in greater detail in AccuKnox blogs:

### Summary

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

<table>
<thead>
<tr>
<th>CSPM</th>
<th>CWPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Static Application Security Testing (SAST)</td>
<td>1. Runtime Kubernetes Security</td>
</tr>
<tr>
<td>2. Software Composition Analysis (SCA)</td>
<td>2. Runtime On-Prem Security</td>
</tr>
<tr>
<td>3. Network security</td>
<td>3. Zero Trust workload hardening policies</td>
</tr>
<tr>
<td>4. API Security</td>
<td>4. Inline Remediation</td>
</tr>
</tbody>
</table>

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
AccuKnox provides a Zero Trust Cloud Native Application Security (CNAPP) platform. AccuK Knox 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.”

ONA

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 our 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
# AccuKnox Enterprise vs KubeArmor OpenSource

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

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