AccuKnox Security Information and Event Management (SIEM)

ACCUKNOX
Secure Code to Cognition™

AI-First SIEM: Cloud, Container & Endpoint Security

Native CNAPP integration with GenAI-powered threat detection for modern enterprise security operations

Architecture & Deployment

Ingestion@Scale Pipeline

1. Multi-tenant K8s cluster architecture
2. OpenSearch endpoint integration
3. Storage lake for massive retention
4. SOAR & incident management ready

Key Features

1. AI-powered detection
2. Multivector correlation engine
3. GenAI threat analysis
4. MITRE ATT&CK integration

Vision & Differentiation

1. AI-first architecture
2. SOC-optimized dark mode UI
3. Modern SOC ready
4. CNAPP integration

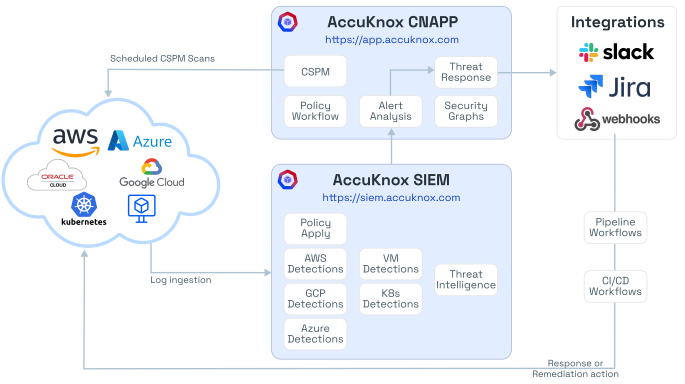
Business Impact Metrics

80%
Alert Noise Reduction
AI-powered correlation eliminates false positives

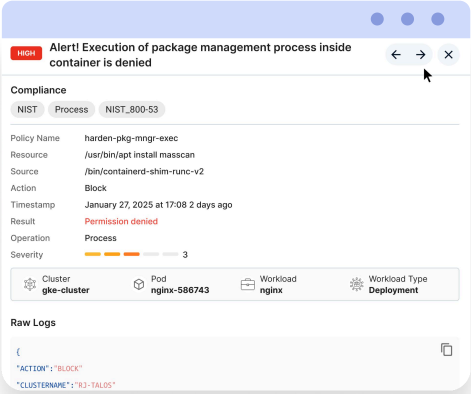
40-60%
Faster Incident Response
Automated threat hunting and analysis

50%
Reduced SOC Costs
GenAI automation reduces manual effort

Ingestion@Scale: Multi-Tenant Architecture



Integration: AccuKnox CNAPP



Alert! Execution of package management process inside container is denied

Compliance

NIST · Process · NIST_800-53

Policy Name	harden-pkg-mngr-exec
Resource	/usr/bin/apt install masscan
Source	/bin/containerd-shim-runc-v2
Action	Block
Timestamp	January 27, 2025 at 17:08 2 days ago
Result	Permission denied
Operation	Process
Severity	3

Cluster	Pod	Workload	Workload Type
gke-cluster	nginx-586743	nginx	Deployment

Raw Logs

```
{
"ACTION":"BLOCK"
"CLUSTERNAME":"RJ-TALOS"
```

Benefits for CNAPP Users

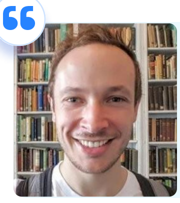
Unified Security Platform

1. Integrated SIEM + CNAPP security operations
2. Single pane of glass for all security events
3. Shared threat intelligence and context

Enhanced Detection

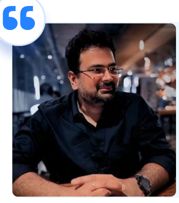
1. Custom KubeArmor-based detection rules
2. Container and cloud-native threat hunting
3. Automated compliance reporting

What Security Leaders Say



controlplane

> Kubernetes is the de facto Cloud Operating System, yet securing it efficiently and effectively presents a wide-ranging challenge. AccuKnox has been instrumental in bringing defense to unknown attacks at real-time.
>
> **Andrew Martin, CEO**



accelalpha
an IBM Company

> Security Integration - Provides runtime security and compliance - Zero-trust security for containers and Kubernetes. Benefit: Security and Compliance. I'm in charge with managing Security and Compliance for my organization. Difficult learning curve: One needs understanding of Kubernetes concepts too.
>
> **Pratik Shekhar, Senior Principal Consultant**

Ready for Next-Gen Security Operations?

AI-Powered SIEM
Compliance-ready detection

Unified Defense
Cloud, endpoint, container

Future-Ready
GenAI & CIEM enabled

Transform your SOC with AI-first SIEM technology

Contact AccuKnox today to see AccuLens in action and discover how AI-driven security operations can reduce costs while improving threat detection and response times.

About AccuKnox

AccuKnox is a Zero Trust CNAPP provider protecting multi-cloud environments, Kubernetes, VMs, and edge infrastructure.