AccuKnox

Case Studies

The Best CNAPP Solution Across Industries

TRUSTED BY GLOBAL INNOVATION LEADERS

xcitium · buck.ai · DeepOrigin · tible · Cashinvoice · AIDASH · IDT · PRUDENT THE FUTURE OF INSURANCE

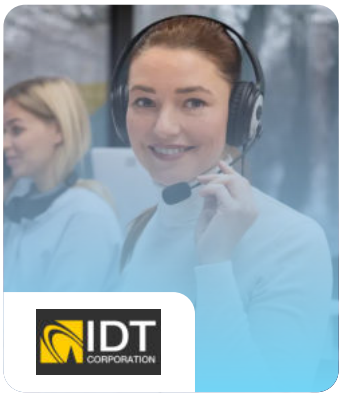


Table of Contents

Prudent Insurance

IDT Telecom

US DoD

Support Logic

Aviation

Tible

Sonesta

Humata Health

Alice Blue

Dovetail

UAE Islamic Bank

Yoma Fleet

AccuKnox

CASE STUDY - INSURANCE

PRUDENT
THE FUTURE OF INSURANCE

India's fastest growing Insurance firm with 200+ branches

Achieves 2x Operational Efficiency with AccuKnox

Supported Clouds

Compliance Frameworks

Security Tools

SIEM, EDR, WAF

PRUDENT
THE FUTURE OF INSURANCE

"At Prudent, we advocate for a comprehensive end-to-end methodology in application and cloud security. AccuKnox excelled in all areas in our in depth evaluation."

Manoj Kern
CIO

Challenges

- **Securing applications** and **cloud infrastructure with SAST, DAST, and IaC** security across 200+ branches
- **Ensuring compliance** with stringent insurance regulations, **avoiding penalties and data breaches**
- Gaining **real-time security insights** through **custom reporting** and **consolidated dashboards**

Solutions

- Deployed **automated vulnerability scanning** to detect and **mitigate threats pre-deployment**
- Enabled deep runtime visibility, reducing **incident response time by 60%**
- **Integrated Nessus** for host security
- Automated compliance checks, ensuring continuous adherence to **IRDAI, GDPR, and SOC 2**
- Provided a **centralized, agent-based security posture management** tool, streamlining cross-team collaboration

Outcomes

- Reduced **security misconfigurations by 75%** with **33+ compliances monitoring**
- Improved **regulatory adherence** with **automated reporting** and audit-ready assessments
- Enabled **secure DevOps integration** across various CI/CD security tooling
- Enhanced data protection, **securing sensitive customer information** against unauthorized access
- **Reduced security alert noise by 85%,** enabling **faster threat prioritization** and response

AccuKnox

AccuKnox

CASE STUDY - TELECOMMUNICATIONS

IDT CORPORATION

A Global Leader in Wholesale Telecommunications

Secures Point of Sale Devices, Reduced Service Interruptions by 80%

Supported Clouds

Virtualization

Security Tools

SIEM, NDR, Firewall, WAF

IDT CORPORATION

"Choosing AccuKnox was driven by opensource KubeArmor's novel use of eBPF and LSM technologies, delivering runtime security"

Golan Ben-Oni

Chief Information Officer

Challenges

- Securing 50,000+ devices across 30+ countries leading to dramatic increase in security incident response times
- A 25% higher risk of unauthorized access and a 30% increase in network attacks threatened critical payment systems
- Intermittent connectivity (20% offline) reduced security tool effectiveness by 50%, creating critical vulnerability gaps

Solutions

- Network security monitoring and threat detection
- Application workload protection across distributed environments
- Compliance management for end devices
- Traffic analysis for IoT/edge with mitigation of attack vectors

Outcomes

- **30,000 devices** onboarded within a week, resulting in inline defence against an attack attempted during the evaluation
- **Cost Effective:** As least as $0.06/device per month
- **Performance:** We improved workloads **efficiency by 25%**
- **88% Alerts reduced, 30% Time Reclaimed:** Accuknox delivered focused intelligence, maximizing analyst impact
- **Prevented installation of unauthorized software** by insiders
- **Prevented installation of unauthorized software**
- Low footprint of software achieved for **minimal constraints** – 1/50th of vCPU and 100MB RAM

AccuKnox

CASE STUDY - PUBLIC SECTOR

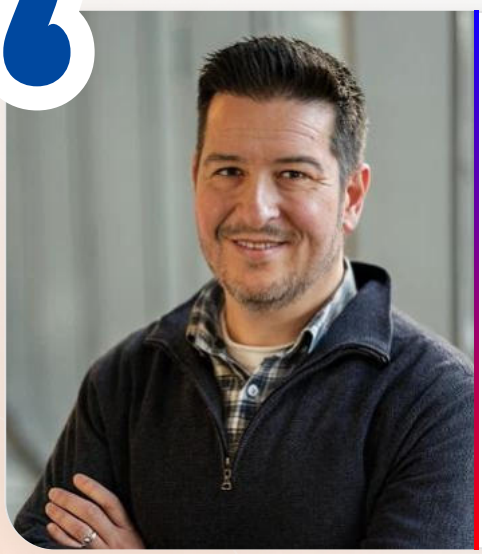
$1.5M Awarded for Cutting-Edge Security

Securing the Nation's Future with AccuKnox's Innovation in 5G Security

On-Prem Infrastructure

Applications

Integrations



5G OPEN INNOVATION LAB

"As 5G starts getting broad industry adoption, security is a very critical challenge. It is delightful to see an amazing innovator like SRI work with AccuKnox to deliver critical innovations"

Jim Brisimitzis

General Partner

Challenges

- Securing a Highly Distributed and Dynamic Environment
- Preventing Advanced Threats and Insider Threats
- Managing Alert Fatigue and Prioritizing Threat Response
- DoD has strict security regulations and compliance requirements (e.g., NIST standards)
- Ensuring Comprehensive Audit Trails and Reporting Capabilities

Solutions

- Accuknox's solution achieved a cost of less than **$0.05/node per month**, resulting in a projected 20% reduction in overall security operational expenses compared to traditional security approaches
- Provided real-time visibility into **100% of the network traffic** between 5G network functions
- Met stringent security requirements for sensitive military communications, achieving a **99.9% availability for critical 5G applications**

Outcomes

- **Onboarded 95%** of targeted 5G edge devices within the initial week, minimizing initial security gaps
- Improved **5G/ORAN** workload **efficiency by 85%**, ensuring minimal impact on network performance and latency
- Maintained optimal performance in resource-constrained 5G edge environments, operating within minimal vCPU and RAM requirements **(1/60th vCPU, 80MB RAM)**
- Demonstrated **no degradation of 5G network** performance during live traffic analysis and threat mitigation

AccuKnox

CASE STUDY - SOFTWARE TECHNOLOGY

SupportLogic

Securing Google Cloud Infrastructure with AccuKnox

Achieved 85% noise reduction, secured 18,000+ assets and mitigated 3.5M+ vulnerabilities.

Supported Clouds

Virtualization

Container Platform

SupportLogic

"As we were considering migrating from our current Cloud Security platform, we conducted an extensive evaluation of best-in-class vendors in the industry. We selected AccuKnox based on their comprehensive features, ease of deployment, automated alert suppression, etc. Their strong roadmap offerings in API Security and AI/LLM Security made AccuKnox the best choice for an integrated AppSec/CloudSec platform."

Tyler Pinckard

Head of Security and Data Privacy Officer (DPO)

Challenges

- Lack of unified cloud security across different providers
- Disconnected security workflows and manual tracking and ticketing
- Blind spots in runtime security across VMs and Kubernetes
- Difficulty complying with cloud best practices and identity governance

Solutions

- Automated vulnerability management with daily scans and CVSS scoring
- Enhanced identity and access governance with automated detection
- Unified security platform for cloud, VM, and Kubernetes security
- Continuous compliance and best practices enforcement
- Integrated vulnerability scanning for secure deployments

Outcomes

- **Modernized security infrastructure:** Successfully replaced a billion-dollar legacy CNAPP with a modern, cost-effective, and unified security platform.
- **Proactive vulnerability remediation:** Identified and prioritized fixes for over 3.5 million vulnerabilities across container images, leveraging CVSS-based scoring and package-level insights for efficient remediation.
- **Reduced security noise:** Smart correlation of vulnerabilities and misconfigurations drastically cut through the noise, reducing false positives by an impressive 85%.
- **Centralized visibility and control:** Achieved a unified view for Kubernetes, VMs, and GCP security posture, enabling comprehensive visibility and enforcement from a single pane of glass.
- **Enhanced compliance and audit readiness:** Ensured regulatory adherence and audit readiness across 18,000+ assets through continuous monitoring and automated checks.

AccuKnox

AccuKnox

CASE STUDY - AVIATION

Global Aviation Leader: Secures AI Workflows Against Supply Chain Attacks

Enterprise-Grade AI Security Across a Multi-Cloud Agent Estate with AccuKnox

Supported Clouds

Deployment

SaaS | On-Prem | aws

"AccuKnox gives us the protection we need for our cloud AI infrastructure, while ensuring our agents and models remain secure against emerging threats."

Global Airline

Head of Cloud & AI Security

Challenges

Uncontrolled AI Agent Sprawl Across Three Clouds
40+ AI agents running across AWS Bedrock, Azure AI Foundry, and Copilot Studio with no unified visibility, behaviour discovery, or runtime controls.

Production LLMs Exposed to Adversarial Attacks
SOC, SRE, FinOps, and DevOps agents running in production had zero guardrails against prompt injection, hallucination, abuse, and evolving threat tactics.

Multi-Cloud AI Misconfiguration
ML workspace governance gaps, public notebook exposure, and critical CVEs in AKS clusters (CVE-2023-24301) with no single platform to correlate risks.

No Compliance Posture for AI Regulations
Zero systematic tracking against OWASP LLM Top 10, NIST AI RMF, ISO 42001, or EU AI Act across sensitive aviation data flows.

Solutions

- **AI Asset Inventory:** Auto-discovered 40 shadow Copilot agents and 1,500+ ML models, eliminating shadow AI overnight.
- **Prompt Firewall:** Real-time LLM-as-a-judge inspection via Azure APIM and AWS API Gateway with session context.
- **Automated Red Teaming:** Continuous scanning of AI workloads across injection, toxicity, and model extraction.
- **Agent Behaviour Sandboxing:** eBPF-based runtime controls on AKS blocking unsafe tool usage and unauthorised outbound traffic.
- **AI Detection & Response (AI-DR):** Automated remediation workflows for public notebook exposure and unauthorised model changes.
- **AI Compliance Posture:** Mapping across 25+ frameworks, including ISO 27001, NIST AI RMF, and the EU AI Act.

Outcomes

- Achieved full-stack AI security, **reducing runtime security risks by 90%** across the entire estate.
- Eliminated blind spots — **achieving live inventory of 1,500+ models** across three clouds within days.
- **Minimised data leakage risk by 85%** through Prompt Firewall guardrails and DSPM controls.
- **Reduced cloud security incidents by 70%** and achieved **95% fewer false positives.**
- Continuous posture tracking across SOC 2, GDPR, and **30+ AI-specific frameworks.**

AccuKnox

CASE STUDY - IT SERVICE

tible

Global Waste Infrastructure Startup Unifies Security Across On-Prem and Runtime

Secures VM and Docker Workloads with Unified Application and Runtime Visibility Across Critical National Infrastructure

Environment

On-Prem | vm | Docker

Deployment

On-Prem | Hybrid

tible

"As we expand critical waste management infrastructure across the Netherlands, we required unified visibility across application and runtime layers. AccuKnox enables us to maintain strong security and governance across our VM and Docker environments."

Merijn Boom
Managing Director

Challenges

Fragmented Security Across VM and Docker
Application security and runtime protection operated in silos, creating blind spots between build-time vulnerabilities and production behaviour.

No Unified Threat Analytics
Time-series operational data lacked integrated threat correlation, making anomaly detection slow and reactive.

Limited Runtime Controls
Docker and VM environments had no granular behavioural enforcement to prevent lateral movement or privilege misuse.

On-Prem Governance Complexity
Operating fully on-prem required enterprise-grade visibility without cloud-native monitoring dependencies.

Solutions

Unified Application Security Posture
Continuous visibility across code, container images, and deployed workloads — consolidating findings into a single operational dashboard.

Runtime VM and Docker Behaviour Monitoring
Kernel-level runtime controls to detect abnormal process activity, privilege escalation, and unauthorised network connections.

Integrated Threat Analytics
Time-series behavioural analysis to surface attack patterns and correlate signals across infrastructure layers.

Centralised Security Governance
Single-pane visibility across application risk and runtime exposure for faster executive reporting and response workflows.

Outcomes

- **Reduced runtime attack** surface by **80%** across VM and Docker workloads.
- **Eliminated visibility gaps** between application vulnerabilities and production behaviour.
- **Accelerated incident investigation timelines by 60%** through correlated threat analytics.
- Established a unified **Zero Trust posture** across critical national waste infrastructure systems.

AccuKnox

CASE STUDY - HOSPITALITY

SONESTA INTERNATIONAL HOTELS

Global Hospitality Leader Standardizes Compliance Across 1,100+ Properties

Standardizes PCI, SOC 2, and FedRAMP Compliance Across Multi-Cloud and DevSecOps Environments

Supported Clouds

aws

Environment

Multi-Cloud | SaaS

Deployment

SaaS | Hybrid

SONESTA INTERNATIONAL HOTELS

"AccuKnox's roadmap in API and AI security, combined with strong DevSecOps and GRC mapping capabilities, made them the clear choice for securing our global hospitality operations."

David Billeter
Cybersecurity Leader

Challenges

Disparate Compliance Across 1,100+ Properties
Operating multiple brands across regions required consistent PCI, SOC 2, and FedRAMP governance without centralised enforcement.

Fragmented DevSecOps Security
Application development across Azure DevOps lacked standardised security validation integrated into the pipeline.

Multi-Cloud Visibility Gaps
AWS and Azure workloads operated without a unified security posture view, increasing misconfiguration and compliance drift risk.

Executive-Level Reporting Complexity
Security and GRC teams required consolidated dashboards aligned to regulatory controls for audit readiness.

Solutions

Centralized Multi-Cloud Governance
Unified visibility across AWS and Azure accounts with continuous compliance posture monitoring.

DevSecOps Security Integration
Embedded security controls directly into Azure DevOps workflows to prevent vulnerable deployments.

Compliance Mapping & Automation
Automated mapping to PCI DSS, SOC 2, FedRAMP, and additional regulatory frameworks for continuous audit readiness.

Consolidated Risk Dashboarding
Executive-level reporting aligning cloud, application, and compliance risks into a single operational view.

Outcomes

- Standardised compliance governance across **1,100+ global properties**.
- Reduced manual audit preparation effort by over **80%.**
- **Accelerated remediation** timelines across development and cloud infrastructure.
- Established **continuous compliance** posture tracking across major regulatory frameworks.

AccuKnox

CASE STUDY - HEALTHCARE

Humata Health

AI Healthcare Innovator Secures HIPAA Compliance Across GenAI Pipelines

Achieves Continuous HIPAA Compliance Across On-Prem GenAI Development Pipelines

Environment

On-Prem

Deployment

On-Prem

Humata Health

"Protecting sensitive healthcare data while accelerating AI innovation is non-negotiable. AccuKnox enables us to maintain continuous security visibility across our development and production environments."

Security Leadership Team

Humata Health

Challenges

HIPAA-Driven On-Prem Constraints
Operating in a strictly regulated healthcare environment required full on-prem deployment without cloud-native shortcuts.

Securing AI-Based Authorization Workflows
Generative AI automating prior authorisation introduced new attack surfaces across application layers.

Fragmented Security Across CI/CD
GitLab and Azure DevOps pipelines lacked unified application security posture visibility from code to deployment.

Limited Continuous Compliance Tracking
HIPAA controls require ongoing validation, not periodic assessment, across sensitive healthcare data flows.

Solutions

Continuous Application Security Visibility
Centralised insight from code repositories through deployment for complete risk traceability.

CI/CD-Integrated Security Controls
Security validation is embedded directly into GitLab and Azure DevOps pipelines to prevent vulnerable releases.

HIPAA-Focused Compliance Monitoring
Automated posture tracking aligned to healthcare regulatory requirements.

End-to-End Application Risk Correlation
Correlated findings across development and runtime environments to prioritize high-impact risks.

Outcomes

- Achieved continuous **HIPAA compliance** visibility across AI-driven healthcare workflows.
- **Eliminated security blind spots** between development and deployment environments.
- Reduced remediation time across pipelines by **60%**.
- Established enterprise-grade governance across **regulated AI healthcare** operations.

AccuKnox

CASE STUDY - FINANCIAL SERVICES

aliceblue
Growth inevitable

Premier Trading Platform Strengthens Application Security and CIS Compliance

Achieves Continuous CIS Configuration Governance Across Production Trading Environments

Environment

SaaS

Deployment

SaaS

aliceblue
Growth inevitable

"In a trading environment where uptime and integrity are critical, we needed continuous application and workload visibility aligned to CIS standards. AccuKnox helped us operationalise that across development and production."

Security Leadership
Alice Blue

Challenges

Securing High-Frequency Trading Applications
Trading platforms require strict application integrity, but vulnerability assessments were not consistently embedded into development workflows.

Lack of Continuous CIS Benchmark Validation
VM configurations drifted over time, creating compliance gaps against CIS standards.

Limited Visibility into Deployed SaaS Risk
Applications deployed in production lacked ongoing dynamic testing for runtime vulnerabilities.

Manual Vulnerability Testing
On-demand security validation required manual effort, slowing release cycles and increasing operational risk.

Solutions

GitHub-Integrated Application Security
Security validation embedded directly into GitHub pipelines to identify vulnerabilities before deployment.

Continuous Dynamic Testing of Deployed Applications
Automated and on-demand runtime vulnerability testing across live SaaS environments.

Periodic VM Configuration Assessment
Automated benchmarking against CIS standards to detect configuration drift and policy violations.

Centralized Risk Visibility
Unified dashboard correlating application vulnerabilities and workload configuration risks across environments.

Outcomes

- Achieved continuous **CIS compliance** visibility across VM infrastructure.
- Embedded **vulnerability detection** directly into the SDLC without slowing release velocity.
- **Reduced production security blind spots** across trading applications.
- **Improved operational confidence** across SaaS-based brokerage workloads.

AccuKnox

CASE STUDY - SOFTWARE DEVELOPMENT

Dovetail

API Infrastructure Specialist Operationalises Live Vulnerability Detection

Achieves Continuous API Security Monitoring Aligned to SOC 2 and ISO 27001 Requirements

Environment

SaaS | API

Deployment

SaaS

Dovetail

"Integrating dynamic security testing directly into our GitHub workflows was critical for securing our live APIs without impacting performance. AccuKnox enabled continuous visibility across development and production."

Security Leadership
Dovetail India

Challenges

No Continuous Dynamic Testing of Live APIs
APIs serving capital market operations required runtime vulnerability detection, but scanning was periodic and manual.

Security Not Embedded in GitHub Actions
Static and dynamic testing were not fully integrated into CI/CD workflows, creating delayed feedback loops.

Compliance Requirements (SOC 2, ISO 27001)
Audit readiness required traceable evidence of continuous testing and vulnerability management.

Fragmented Visibility Across Environments
Findings from development and production environments were siloed, limiting centralised risk prioritisation.

Solutions

Collectors-Based Continuous DAST
Deployed lightweight collectors to perform live dynamic scans on production applications and APIs without impacting performance.

GitHub Actions Security Integration
Automated triggering of static analysis directly within GitHub workflows to prevent vulnerable code merges.

Continuous API Monitoring
Ongoing scanning for OWASP Top 10 and API-specific vulnerabilities in live environments.

Centralized Vulnerability Correlation
Unified visibility into static and dynamic findings across development and production environments.

Outcomes

- Operationalized continuous API security across GitHub-driven development.
- **Reduced detection time** for runtime vulnerabilities by **70%.**
- Achieved audit-aligned evidence tracking for **SOC 2 and ISO 27001.**
- Eliminated security blind spots between **CI/CD and production APIs.**

AccuKnox

CASE STUDY - UAE BANK

UAE Islamic Bank Achieves Continuous Cloud Compliance on Azure

Achieves 300+ Vulnerabilities Detected Across 6 Azure Subscriptions

Supported Clouds

Registry

Deployment

On-Prem

"AccuKnox gave us continuous visibility across our entire Azure footprint — from cloud configuration to container images to runtime workloads. We now meet CIS, PCI, and SOC 2 requirements without stitching together multiple tools."

Security Leadership

Cloud Security Team

AccuKnox delivers a CNAPP purpose-built for regulated financial institutions. This UAE-based Islamic bank needed continuous compliance across Azure CIS, PCI, and SOC 2 Type II — without disrupting Sharia-compliant banking operations running on AKS.

Challenges

- No unified visibility across 6 Azure subscriptions to continuously validate posture against Azure CIS, PCI, and SOC 2 Type II.
- AKS production workloads ran without a runtime security layer, leaving the bank exposed to in-cluster threats without detection.
- Container images in ACR were not scanned, allowing vulnerable images into production without any CVE assessment.
- No agentless assessment capability to inspect Azure resources without disrupting live regulated banking operations.

Solutions

- Deployed CSPM across all 6 Azure subscriptions for continuous benchmarking against Azure CIS, PCI, and SOC 2 Type II controls.
- Implemented KSPM and CWPP on AKS to harden cluster configuration and detect runtime threats in active workloads.
- Integrated container image scanning with ACR to catch vulnerabilities before images reach production.
- Ran agentless risk assessment across all subscriptions — surfacing 300+ unique vulnerabilities with zero operational disruption.

Outcomes

- Detected **300+ unique vulnerabilities** across 6 Azure subscriptions — zero disruption to banking operations.
- Achieved **continuous CIS, PCI, and SOC 2 Type II compliance** via automated CSPM monitoring.
- Closed the **AKS runtime security gap** with live threat detection across production workloads.
- Eliminated **ACR image blind spots** by scanning containers before production deployment.
- Consolidated cloud, container, and runtime security into a **single AccuKnox Managed OnPrem deployment** — reducing toolchain complexity across a regulated environment.

AccuKnox

CASE STUDY - FLEET & LEASING

YOMA FLEET

Fleet & Leasing Leader Achieves $1B+ in Secured Operations on AWS

Secures AWS Infrastructure, Replaces Wazuh, & Consolidates Multi-Tool Findings with AccuKnox SIEM & CSPM

Supported Cloud

aws

Integrations

Deployment

SaaS

YOMA FLEET

"AccuKnox SIEM gives us the end-to-end visibility and control to protect our fleet management systems, customer data, and operational infrastructure. Easy to deploy, with analytics that made the decision straightforward. We're confident this partnership strengthens our security posture as we grow."

Spokesperson

Yoma Fleet

We deliver a Cloud Native Application Protection Platform (CNAPP) that secures critical infrastructure. Yoma Fleet, part of Singapore-listed Yoma Strategic Holdings, runs its fleet and logistics operations on AWS. Their previous SIEM, Wazuh, couldn't meet the governance demands of a listed parent group. AccuKnox replaced it, providing unified AWS event management, continuous CIS compliance, and consolidated insights from Snyk and GitHub in a single pane of glass.

Challenges

- Ensuring regulatory compliance across AWS environments and reducing the risk of non-compliance penalties from Yoma Strategic Holdings' governance framework.
- Achieving comprehensive security coverage across AWS with findings fragmented across Wazuh, Snyk, and GitHub — requiring manual correlation with no unified view.
- No continuous CIS benchmark enforcement for AWS, exposing the organization to compliance drift between infrequent manual audits.
- Limited security automation and executive reporting capability — insufficient for the governance standards required by an SGX-listed parent group.

Solutions

- Deployed AccuKnox SIEM to ingest AWS CloudTrail, VPC Flow Logs, and GuardDuty events, replacing Wazuh with real-time AWS-native incident detection and automated response workflows.
- Implemented unified findings aggregation across Snyk and GitHub pipeline scans, consolidating multi-tool alerts into a single prioritized view and eliminating manual correlation.
- Activated AccuKnox CSPM for continuous CIS benchmark assessments across the AWS environment, generating audit-ready compliance reports on demand.

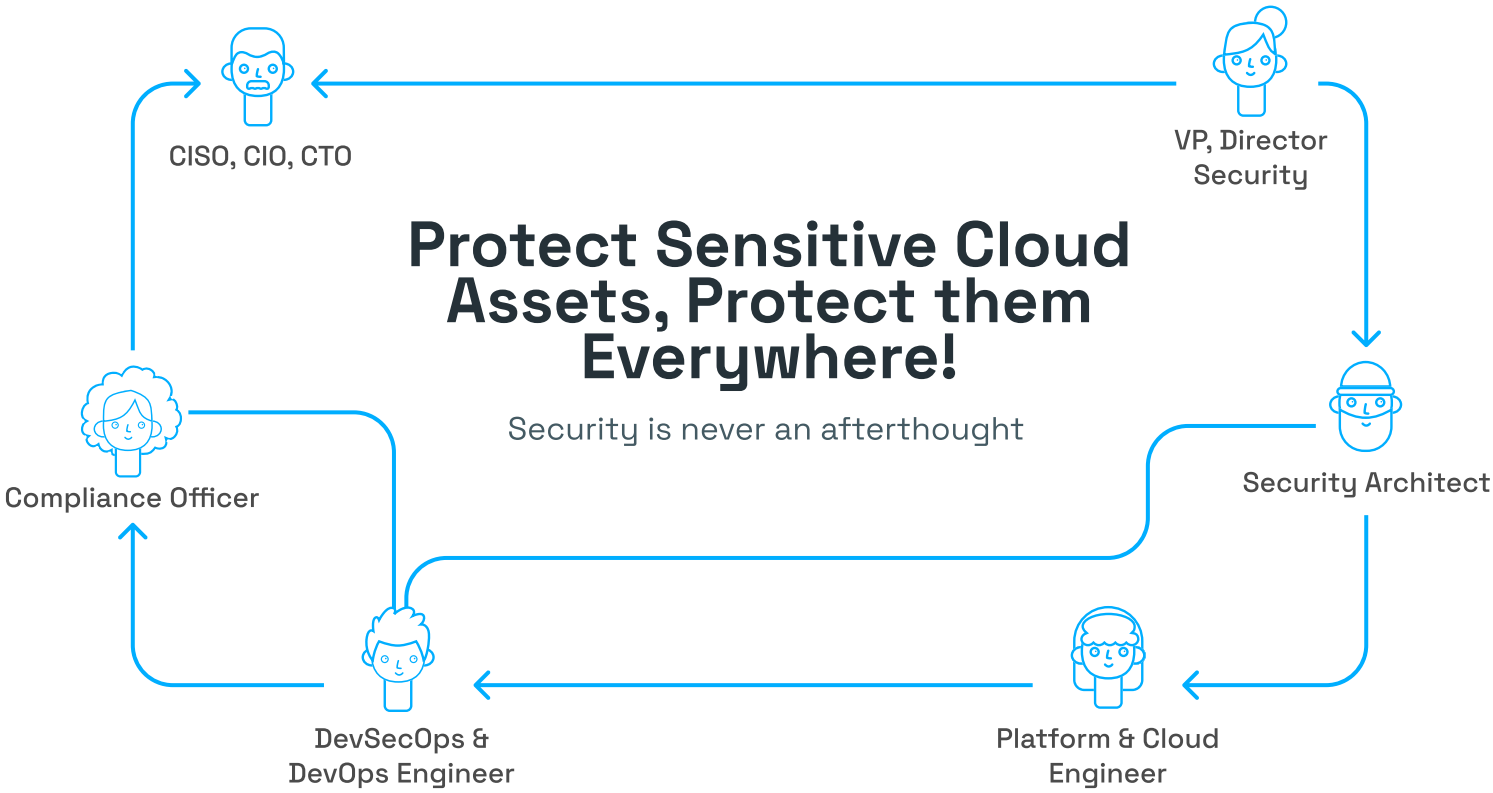
- Configured automated insights and governance-grade reporting dashboards aligned to the standards of Yoma Strategic Holdings' corporate leadership.
- Secured applications pre-deployment through policy-driven guardrails in the GitHub CI/CD pipeline, reducing the attack surface before workloads reach AWS.

Outcomes

- Wazuh fully replaced within the POC window — **AccuKnox SIEM became the primary security operations** platform for all AWS event logging and incident management.
- **CIS compliance for AWS** shifted from periodic manual checks to continuous automated assessment, with audit-ready reports available on demand.
- **Enabled proactive compliance management**, helping Yoma Fleet meet and maintain CIS and AWS security standards required by their SGX-listed parent group.
- AccuKnox purchased directly via the AWS Marketplace, enabling **rapid deployment** without extended procurement cycles.
- Phase 2 expansion covering **ASPM and Runtime Security** is already planned, extending AccuKnox into full-stack security coverage across Yoma Fleet's cloud operations.

Featured by

aws ORACLE Gartner NEPHIO IBM Cloud LF EDGE



Extra 30 Days Free Trial

aws

*No strings attached, limited period offer!

Scan for Demo

About AccuKnox

AccuKnox is a Zero Trust Cloud Security Platform that protects Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.

kubernetes CERTIFIED SERVICE PROVIDER

AICPA SOC 2 Formerly SAS 70 Reports

CLOUD NATIVE COMPUTING FOUNDATION SILVER MEMBER

NEPHIO

aws PARTNER Containers Software Competency

ACCUKNOX®

linkedin.com/accuknox

@AccuKnox