ACCUKNOX

AI-Powered CNAPP

AccuKnox Releases Gen-AI LLM based Cloud Security Interface

Ask Ada

Not just another chatbot. Bridge visibility gaps, eliminate alert fatigue, and fix vulnerability triages.
Ask Ada to help enable interactive hardening.

Contents

Why AI-Powered CNAPP?

Ask Ada Walkthrough

About AccuKnox

Summary

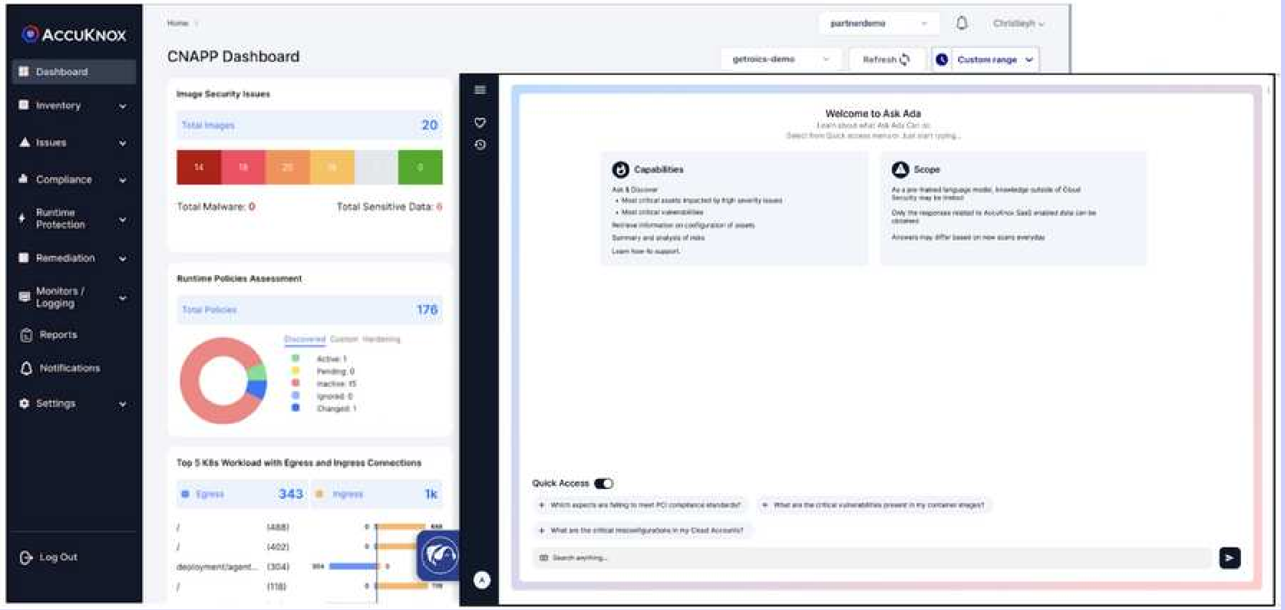
Start Your Free Trial →

Why AI-Powered CNAPP?

Explore how generative AI capabilities allow CNAPP platforms to deliver unified visibility, accelerated detection, and tailored recommendations across complex cloud environments.

Ask Ada Walkthrough

See Ask Ada in action with demo screens highlighting conversational interfaces, personalized insights, and automated security assistance for modern security teams.



Total Malware: 0

Total Sensitive Data: 6

Welcome to Ask Ada

Learn about what Ask Ada Can do

Select from Quick access menu or Just start typing...

Capabilities

Ask & Discover
- Most critical assets impacted by high severity issues
- Most critical vulnerabilities

Retrieve information on configuration of assets

Summary and analysis of risks

Learn how to support.

Scope

As a pre-trained language model, knowledge outside of Cloud Security may be limited

Only the responses related to AccuKnox SaaS enabled data can be obtained

Answers may differ based on new scans everyday

+ Which aspects are failing to meet PCI compliance standards?

+ What are the critical vulnerabilities present in my container images?

+ What are the critical misconfigurations in my Cloud Accounts?

One-Chat Solution

Incident Response Assistance

Proactive Vulnerability Detection

Platform Specific Guidance

Insights Into Data Security

Instant CNAPP Metrics

Get Response from Image

CNAPP – Cloud Native Application Protection Platform

Gartner®

Market Guide for Cloud-Native Application Protection Platforms

Gartner

Market Guide for Cloud-Native Application Protection Platforms

Published 14 March 2023 · ID G00785751 · 28 min read

By Neil MacDonald, Charlie Winckless, Dale Koeppen

Initiatives: Security of Applications and Data; Infrastructure Security

CNAPPs address the full life cycle protection requirements of cloud-native applications from development to production. Security and risk management leaders responsible for cloud security strategies should use this research to analyze and evaluate emerging CNAPP offerings.

- ✓ **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

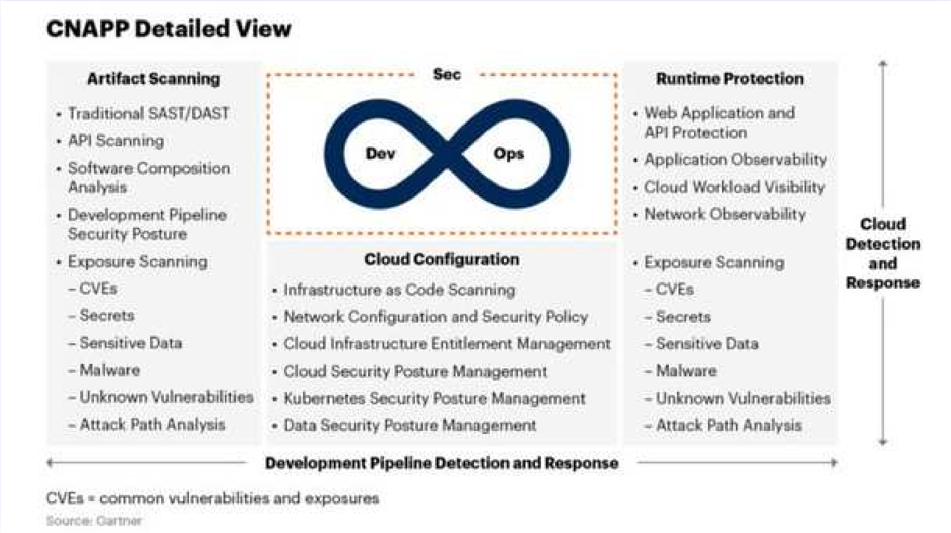
AccuKnox Enterprise CNAPP Suite

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).



CNAPP Detailed View

Artifact Scanning
- Traditional SAST/DAST
- API Scanning
- Software Composition Analysis
- Development Pipeline Security Posture
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Sec — Dev — Ops

Cloud Configuration
- Infrastructure as Code Scanning
- Network Configuration and Security Policy
- Cloud Infrastructure Entitlement Management
- Cloud Security Posture Management
- Kubernetes Security Posture Management
- Data Security Posture Management

Runtime Protection
- Web Application and API Protection
- Application Observability
- Cloud Workload Visibility
- Network Observability
- Exposure Scanning
  - CVEs
  - Secrets
  - Sensitive Data
  - Malware
  - Unknown Vulnerabilities
  - Attack Path Analysis

Cloud Detection and Response

Development Pipeline Detection and Response

CVEs = common vulnerabilities and exposures

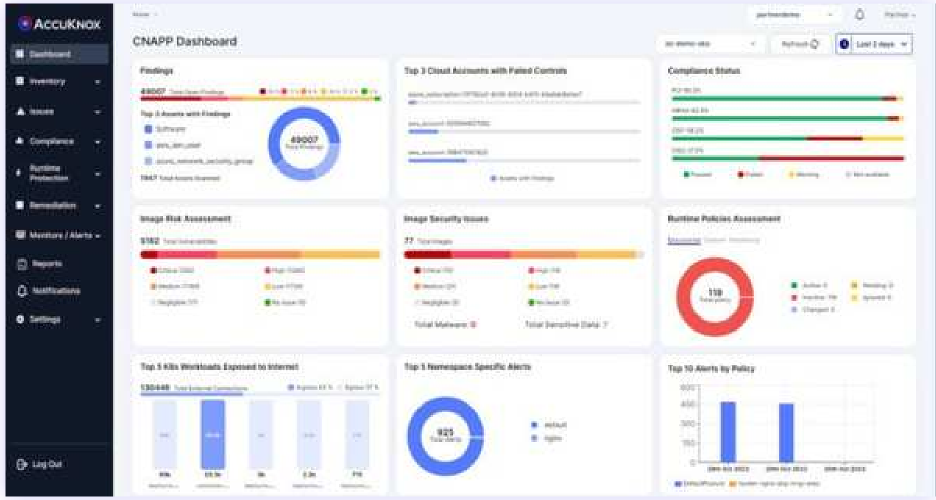
Source: Gartner

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.

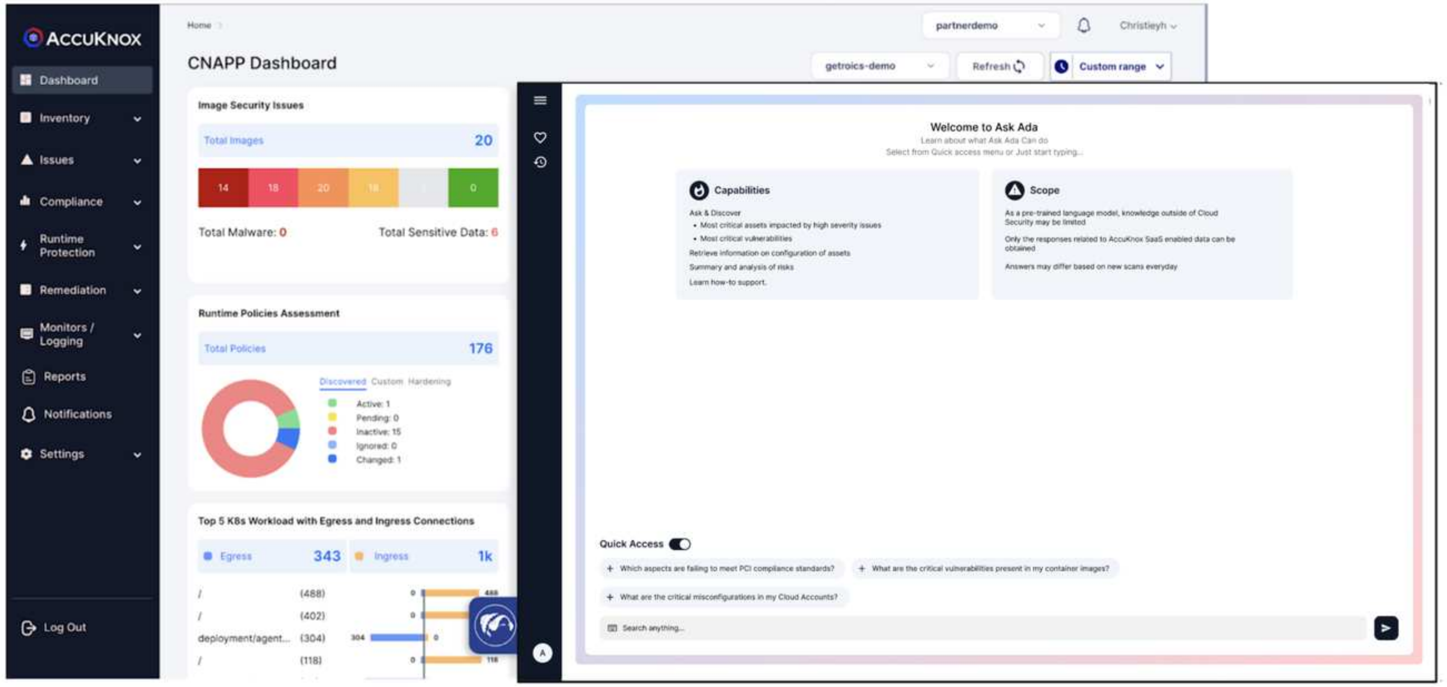
Revolutionizing Security Posture with AI Insights Automate the mundane, Empower the expert

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 DevSecOps and CISO Personas.
Security should provide Assistive Remediation to every security personas

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



Welcome to Ask Ada
Learn about what Ask Ada Can do
Select from Quick access menu or Just start typing...

Capabilities
Ask & Discover
- Most critical assets impacted by high severity issues
- Most critical vulnerabilities

Retrieve information on configuration of assets
Summary and analysis of risks
Learn how-to support.

Scope
As a pre-trained language model, knowledge outside of Cloud Security may be limited
Only the responses related to AccuKnox SaaS enabled data can be obtained
Answers may differ based on new scans everyday

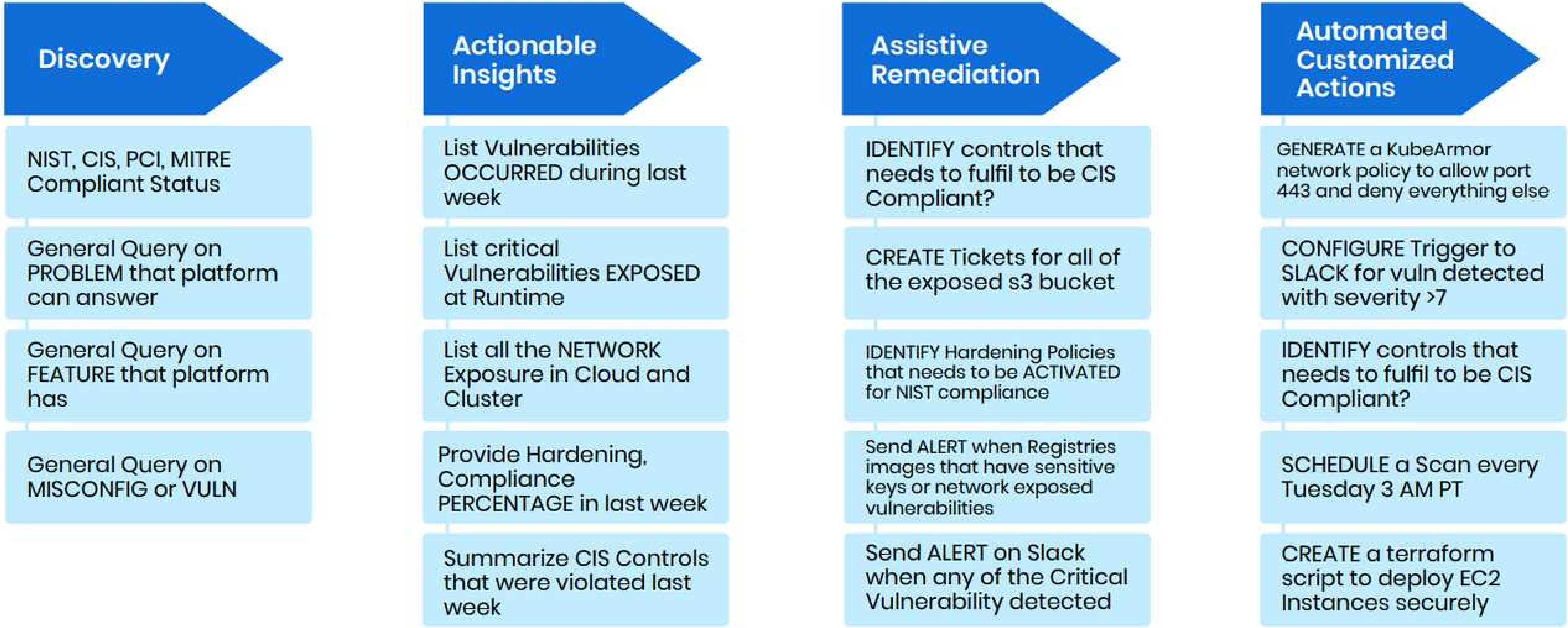
Quick Access
+ Which aspects are failing to meet PCI compliance standards?
+ What are the critical vulnerabilities present in my container images?
+ What are the critical misconfigurations in my Cloud Accounts?

Search anything...

Key Takeaway

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

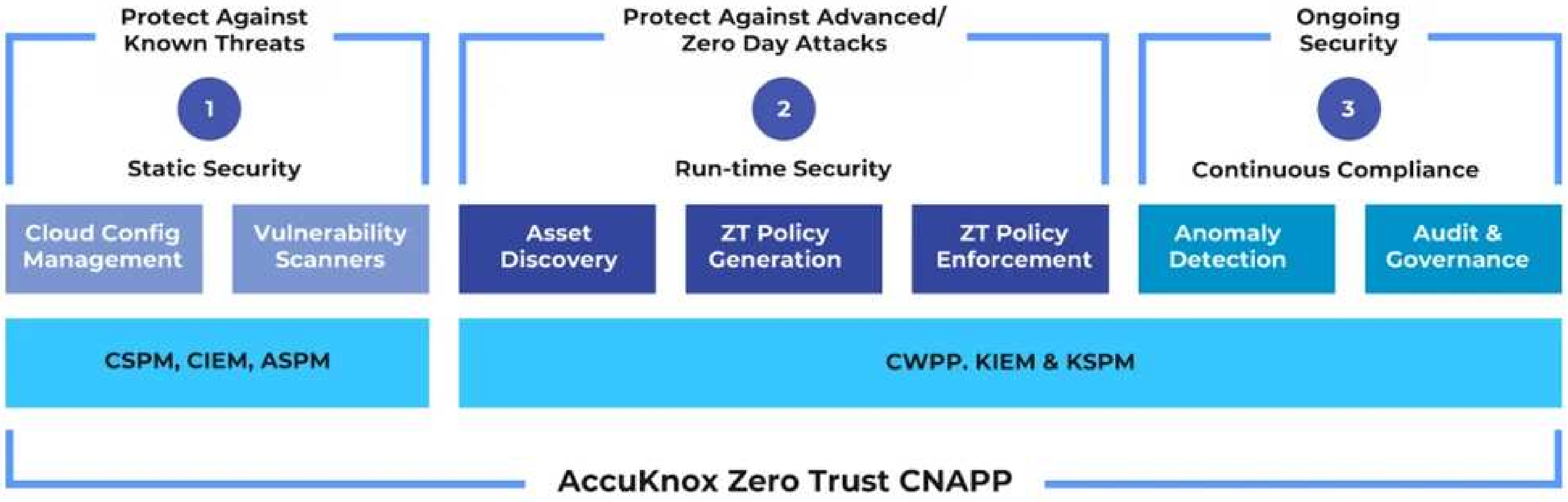
Key Takeaway

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

The Issue with Traditional CNAPPs

Why Gen-AI Interface Is the Need of the Hour

Accelerate detection and response by leveraging AI to surface relevant threats from the noise.



- Cloud environments have **exploded in complexity**, creating **visibility gaps** that allow threats to hide.
- Traditional tools fail to keep up, flooding teams with fragmented alerts lacking context. This slows response times and allows critical risks to slip through the cracks. There is an urgent need for automation and AI to help overwhelmed teams regain control.
- **Ask Ada** by AccuKnox brings the power of **generative AI** to simplify cloud-native security. It acts as an intuitive assistant allowing users to ask questions in plain language and receive detailed summaries, recommendations, and workflows in response. Key capabilities include **automated data correlation, crown jewels tracking, contextual vulnerability insights, compliance drift detection, and proactive guidance.**

Newsflash

Over 93% of organizations now operate multi-cloud or hybrid environments, but only 40% feel confident in visibility.

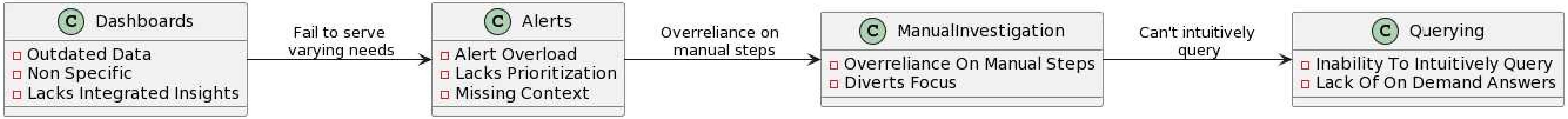
Challenges Faced By DevSecOps Teams

And How Ask Ada Combats Information Deluge for for Overwhelmed DevSecOps Teams

Accelerating cloud-native adoption strains DevSecOps teams struggling to secure complex new environments. Pain points include:

- **Data Mapping Overload** - 93% operate multi-cloud but only 33% can correlate insights. This hides threats.
- **Lack of Critical Data Focus** - Identifying crown jewels across environments to prioritize protection is extremely difficult.
- **Alert Fatigue** - Floods of low-level alerts lacking context lead to ignoring warnings.
- **No Preventative Guidance** - Getting clear steps tailored to user skill level for hardening or achieving compliance is sorely lacking.

Ask Ada helps enterprises overcome these roadblocks to easily build zero trust cloud environments. It leverages automation and reasoning to provide guardrails allowing innovation without compromising resilience.



C Dashboards
- □ Outdated Data
- □ Non Specific
- □ Lacks Integrated Insights

Fail to serve varying needs →

C Alerts
- □ Alert Overload
- □ Lacks Prioritization
- □ Missing Context

Overreliance on manual steps →

C ManualInvestigation
- □ Overreliance On Manual Steps
- □ Diverts Focus

Can't intuitively query →

C Querying
- □ Inability To Intuitively Query
- □ Lack Of On Demand Answers

Key Takeaway

DevSecOps teams face challenges securing multi-cloud environments due to visibility gaps and tool integration issues with traditional CNAPP platforms.

Maximize DevSecOps Productivity

- AccuKnox's Ask Ada is purpose-built to serve user personas. It offers personalized security experiences for different personas, enhancing infrastructure visibility and productivity.
- CISOs can access compliance reports and risk assessments easily, and Security Engineers get granular details with low-level info.
- Ask Ada improves collaboration and alignment among teams by tailoring responses to individual needs.
- It bridges the gap between top-down risk visibility and bottom-up hardening.

Ask Ada Metrics

1k+ VULNERABILITY REMEDIATIONS

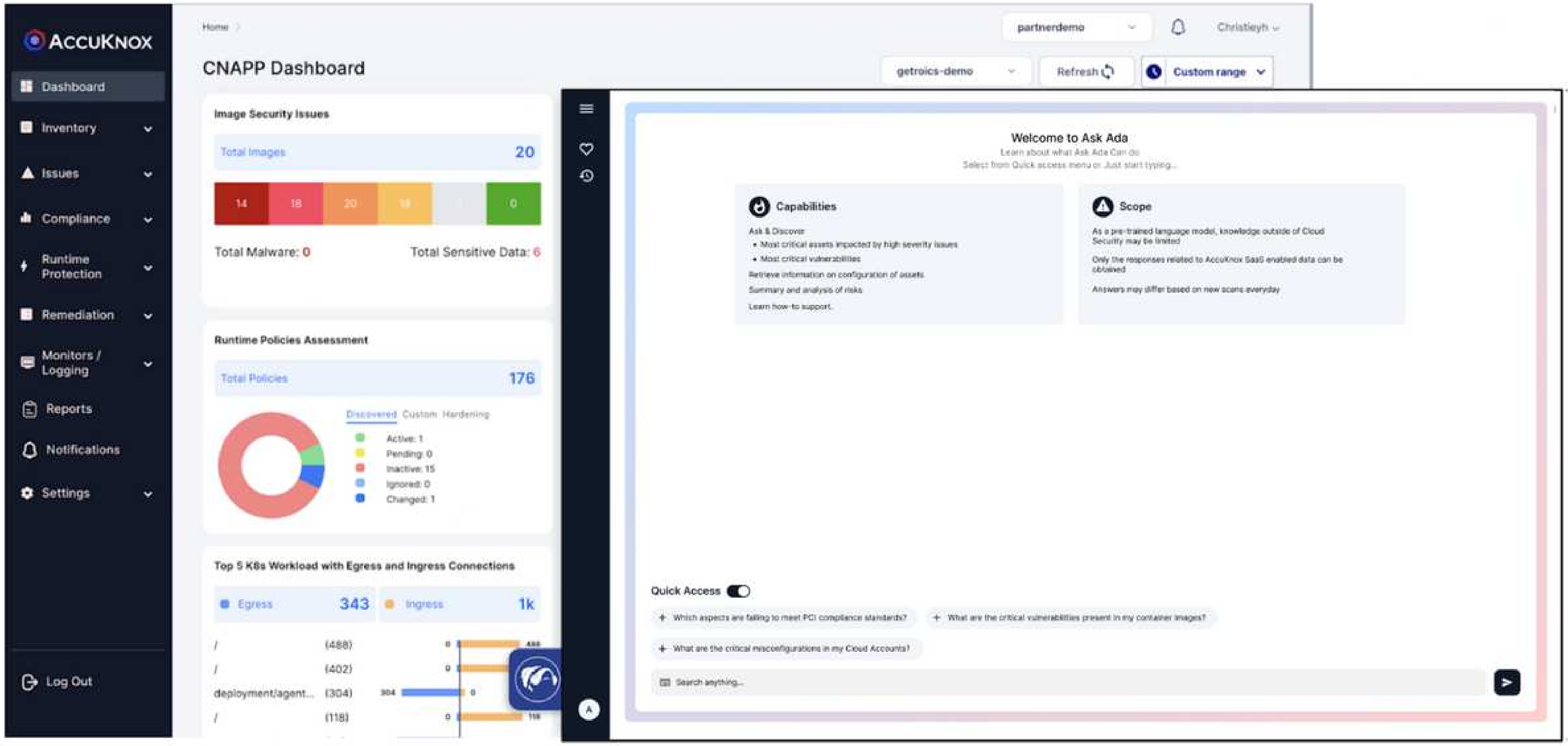
3x PRODUCTIVITY

7+ COMPLIANCES

9k+ MISCONFIGURATION DETECTIONS

Newsflash Simplifying cloud security so enterprises can innovate fearlessly without sacrificing resilience.

Introducing Ask Ada



Welcome to Ask Ada

Learn about what Ask Ada Can do

Select from Quick access menu or Just start typing...

Capabilities

Ask & Discover

- Most critical assets impacted by high severity issues
- Most critical vulnerabilities

Retrieve information on configuration of assets

Summary and analysis of risks

Learn how-to support.

Scope

As a pre-trained language model, knowledge outside of Cloud Security may be limited

Only the responses related to AccuKnox SaaS enabled data can be obtained

Answers may differ based on new scans everyday

Quick Access

+ Which aspects are failing to meet PCI compliance standards?

+ What are the critical vulnerabilities present in my container images?

+ What are the critical misconfigurations in my Cloud Accounts?

Search anything...

Ask Ada applies the power of generative AI to act as an intuitive assistant that boosts productivity for DevSecOps, cloud security, and GRC teams.

Ask questions conversationally in plain language and receive detailed summaries, recommendations, and workflows in response.

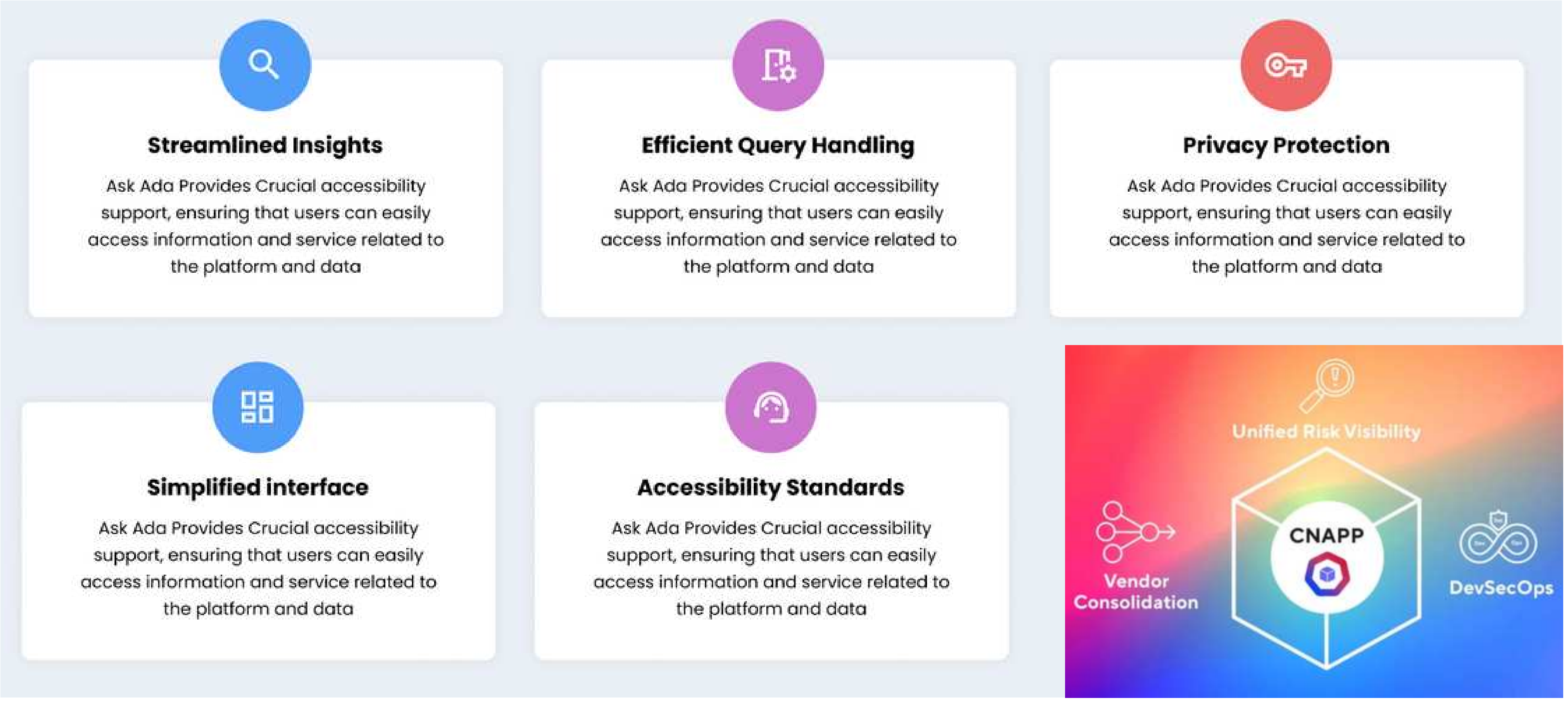
Key Takeaway

Apply the power of generative AI as an assistant to simplify cloud-native security. With a simple chat interface get aggregated view of all your cloud assets

The Future of Cloud Security

Achieve Agility With AccuKnox's Gen-AI Powered CNAPP - Ask Ada

By delivering unified insights and control planes, generative AI solutions like Ask Ada allow enterprises to achieve resilient security at the pace of cloud innovation versus struggling with fragmented tools.
The future offers hope of confidently securing dynamic environments while increasing productivity - finally aligning business demands with operational realities.



Streamlined Insights

Ask Ada Provides Crucial accessibility support, ensuring that users can easily access information and service related to the platform and data

Efficient Query Handling

Ask Ada Provides Crucial accessibility support, ensuring that users can easily access information and service related to the platform and data

Privacy Protection

Ask Ada Provides Crucial accessibility support, ensuring that users can easily access information and service related to the platform and data

Simplified interface

Ask Ada Provides Crucial accessibility support, ensuring that users can easily access information and service related to the platform and data

Accessibility Standards

Ask Ada Provides Crucial accessibility support, ensuring that users can easily access information and service related to the platform and data

"Generative AI is transforming what's possible in cybersecurity by applying the power of natural language and automation."

Newsflash

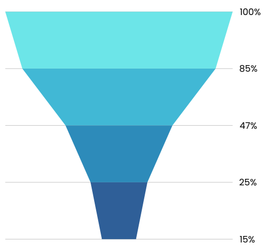
Apply generative AI to provide unified control planes delivering security at the speed of cloud.

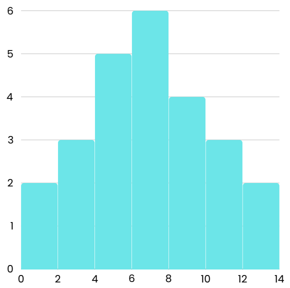
Key Capabilities

Maximizing Control Across Complex Cloud Environments

Ask Ada streamlines cloud security via 5 key capabilities:

1. **Automated Data Correlation** - Ingests and synthesizes insights across infrastructure
2. **Crown Jewels Tracking** - Discovers sensitive data and classifies risk
3. **Contextual Vulnerability Insights** - Analyzes exploitability based on hosting critical data
4. **Compliance Drift Detection** - Continuously audits environments
5. **Proactive Guidance** - Provides clear remediation workflows based on risk and configurations





Applying generative AI to accelerate correlation, validation, and control allows understaffed teams to keep pace with dynamic cloud environments.

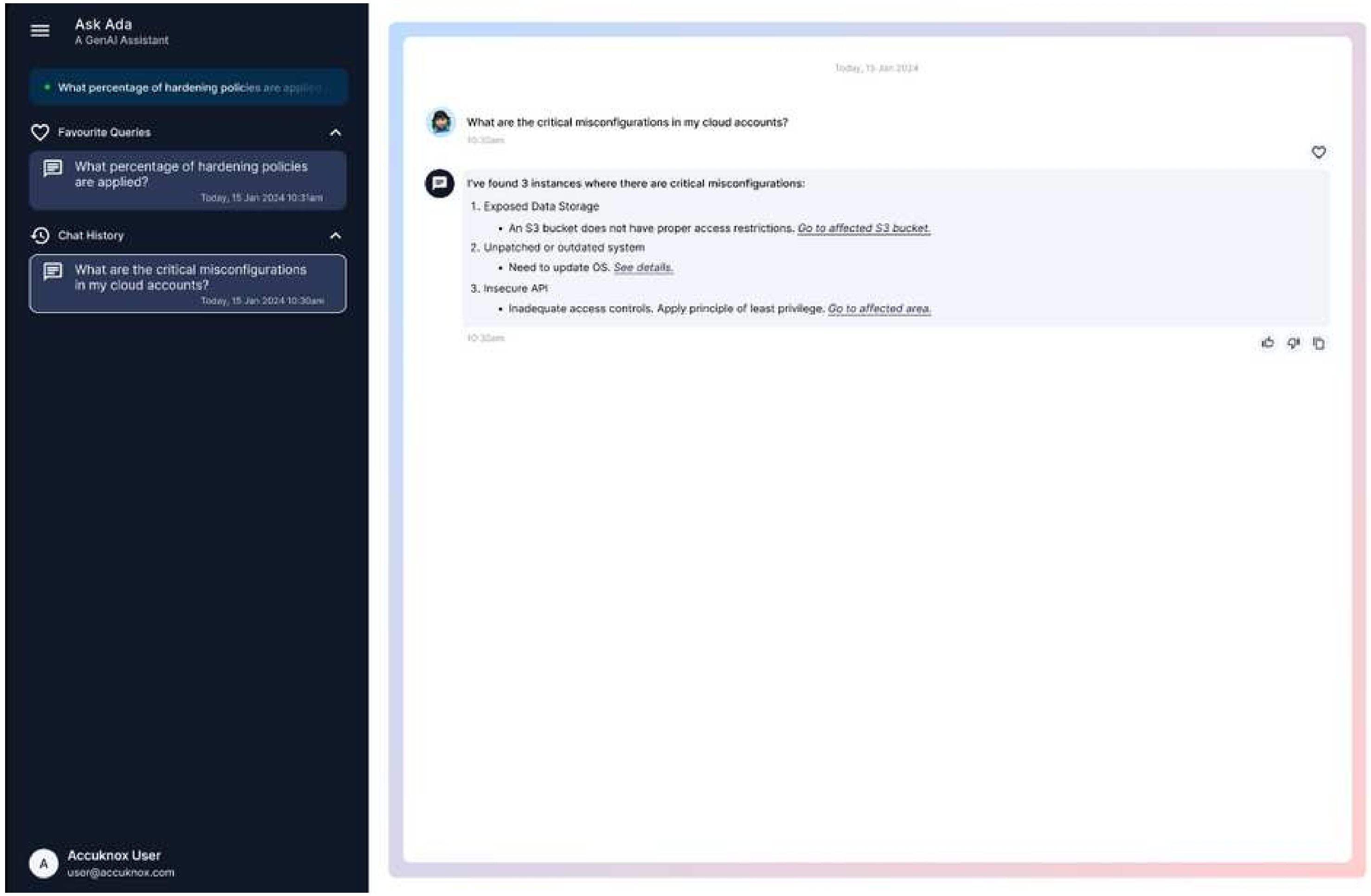
Key Takeaway

Automate tedious data correlation tasks to eliminate visibility gaps and accelerate detection.

Getting Started with Ask Ada

Conversational Cloud Security On Demand

- Ask Ada offers an intuitive conversational interface accessible directly within AccuKnox workflows to boost productivity.
- New users are guided in platform configuration via a side-bar chatbot. Once onboarded, Ask Ada provides just-in-time insights on dashboards and during investigations. It highlights risks and recommends resolution steps personalized to the user's environment and persona.
- With Ask Ada, cloud security teams regain visibility, focus efforts, and enable resilience via natural language - no matter their skill level.



Ask Ada
A GenAI Assistant

What percentage of hardening policies are applied

Favourite Queries

What percentage of hardening policies are applied?
Today, 15 Jan 2024 10:31am

Chat History

What are the critical misconfigurations in my cloud accounts?
Today, 15 Jan 2024 10:30am

Accuknox User
user@accuknox.com

Today, 15 Jan 2024

What are the critical misconfigurations in my cloud accounts?
10:30am

I've found 3 instances where there are critical misconfigurations:

1. Exposed Data Storage
   - An S3 bucket does not have proper access restrictions. *Go to affected S3 bucket.*
2. Unpatched or outdated system
   - Need to update OS. *See details.*
3. Insecure API
   - Inadequate access controls. Apply principle of least privilege. *Go to affected area.*

10:30am

Key Takeaway Enable conversational accessibility to security insights directly within existing workflows.

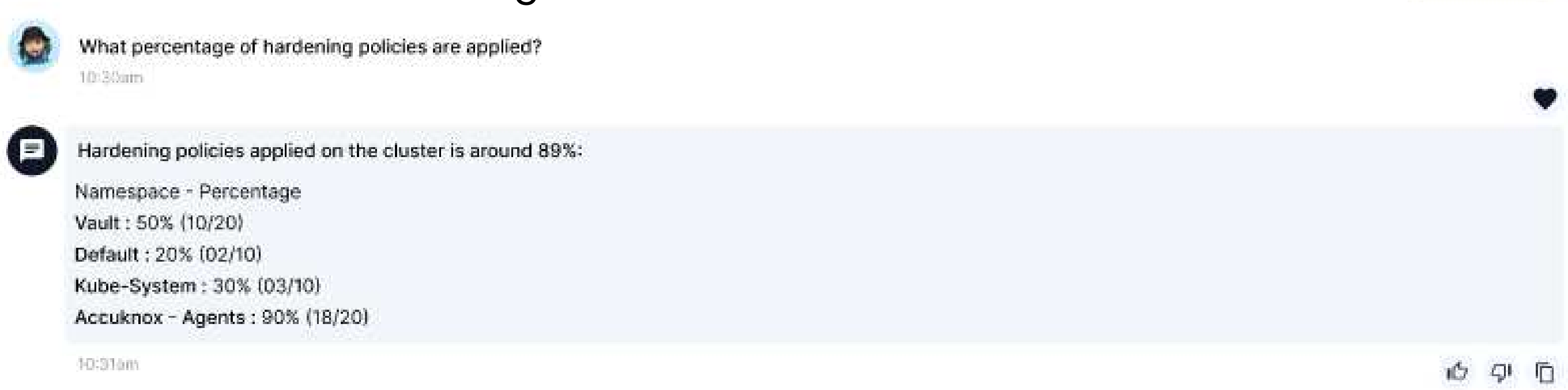
Use Cases - Asset Security Posture

Elevated Security Posture with Unified Visibility and Query Capabilities

Ask Ada allows intuitive queries to understand security posture, integrations, policies and more.

Example Queries:

1. What are all the HARDENING Policies & DISCOVERED Policies
2. Explain about BASELINES and how to CONFIGURE CIS Baseline
3. How to be COMPLIANT to PCI-DSS benchmark?
4. EXPLAIN process of integration into 3rd party ticketing tool like ServiceNow?
5. What are the SIEM tools supported and integration guide link?
6. What are different applications ENVIRONMENT this tool can SUPPORT?
7. "What controls are failing for this workload?"



What percentage of hardening policies are applied?

10:30am

Hardening policies applied on the cluster is around 89%:

Namespace - Percentage
Vault : 50% (10/20)
Default : 20% (02/10)
Kube-System : 30% (03/10)
Accuknox - Agents : 90% (18/20)

10:31am

Gain unified visibility by querying details on configurations, controls, and risks across clouds in plain language.

Key Takeaway

Query details on security posture, policy configuration and more in plain language.

Use Cases - Log Analysis

Contextual Intelligence For Precise Risk Analysis

Ask Ada automatically synthesizes and prioritizes threats versus traditional alert overload.

Get Insights Easily from Ask-Ada -

1. Clusters with exposed ports to internet
2. Exploitable container image vulnerabilities exposed to web
3. Summary of application security posture from last week
4. *Runtime actions* blocked
5. Exceptions for *CIS Hardened Kubernetes Clusters*
6. *S3 Buckets* exposed to the internet
7. Riskiest assets and associated vulnerabilities
8. Most critical vulnerabilities in Production Cluster
9. *CVEs › 7 CVSS Score a*cross Platform with Root Cause

Ingested Data

- *Audit logs, telemetry*
- *Vulnerability scans*
- *Web app scans*
- *CI/CD notifications*

Accelerate detection and response by leveraging AI to surface relevant threats from the noise.

Key Takeaway Automatically prioritize threats by criticality and risk rather than just volume.

Use Cases - Remediation Guidance

Conversational Remediation Assistance Tailored For Teams

Example Queries

1. Can you generate security policies to stop access to any /vault directory
2. Do I have a NETWORK PORT EXPOSED at runtime in any of the clusters?
3. How many percentages of hardening policies are applied?
4. Tell me how CVE-2016-20013 got introduced in the product
5. Tell me the top 5 critical issues in SCA, SAST, DAST or registry scan
6. Generate a *KubeArmor* network policy to allow port 443 and deny everything else
7. Configure triggers to *Slack* for vulnerabilities detected with severity >7

Resolution Components

- Knowledge base articles
- Playbook workflows
- Policy templates

Save analysts hours by answering questions on securing infrastructure, resolving alerts, achieving compliance and more.

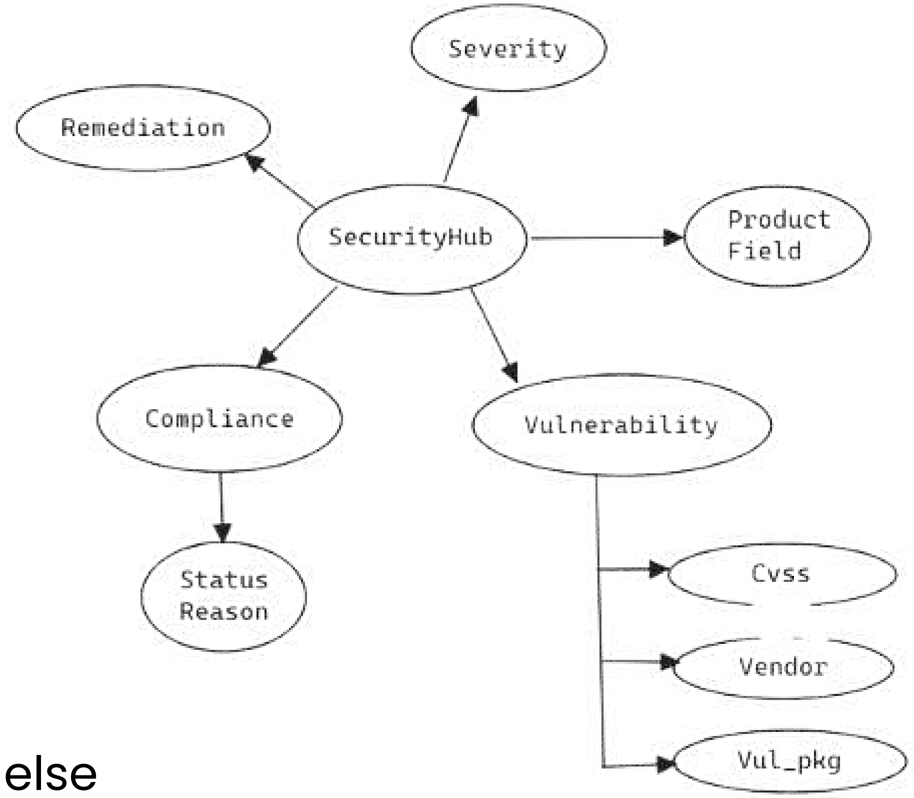
Key Takeaway

Boost team efficiency by providing clear and tailored resolution steps tuned to environment and skill level.

Use Cases - Security Automation

Simplify Cloud Administration with Ask Ada's Automation

Get auto-generated customized actions on policy creation, handle ticketing, create notifications or schedule scans



Simply command Ask-Ada to do all of this and more:

1. Restrict assets with severity 9+ vulnerabilities
2. Alert on signs of crypto mining in VPCs
3. Schedule scans on ecommerce subnet nightly
4. Generate a KubeArmor policy to allow 443 port and block everything else
5. Create a CIS compliance baseline
6. Configure a trigger to slack for all of the CVSS score above 8
7. Schedule a scan every Tuesday at 3 AM PT
8. Create a terraform script to deploy an EC2 instance

Automated Workflows

- Quarantine/Kill chain
- Notification routing
- Scan scheduling
- Control deployment

Key Takeaway Enable natural language policy and action creation to simplify administration.

Give Your Security Teams A Chance To Level Up!

Democratize Security by Empowering Every Role with Ask Ada

Ask Ada democratizes security by enhancing visibility, productivity, and controls for every persona - from analysts to CISOs.

Key Persona Benefits:

1. **CISOs** - Automated risk summaries and compliance reporting
2. **Security Engineers** - Detailed asset hardening and investigation
3. **Cloud Architects** - Intuitive policy and configuration guidance
4. **Analysts** - Alert prioritization and guided remediation

By leveraging flexible experiences tuned to context, Ask Ada connects top-down leadership with bottom-up operations.

Focus

Democratize security by enhancing visibility, productivity and controls for every role - from analyst to the CISO.

KubeArmor Integration

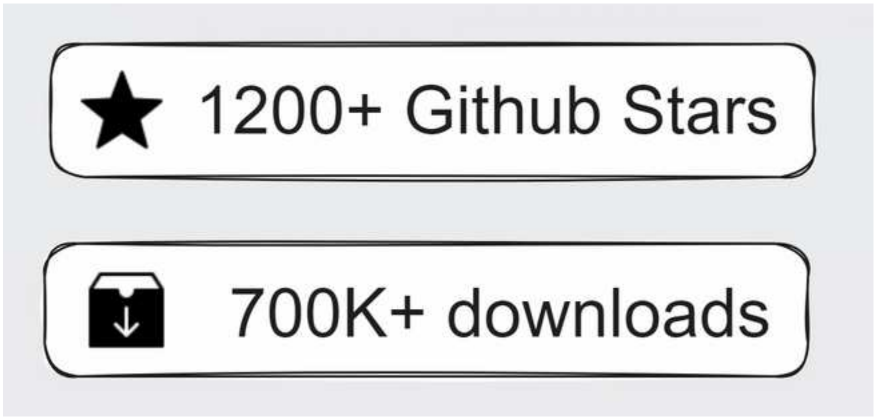
Simplified Kubernetes Security with Low Overhead

Ask Ada integrates hardened runtime application self-protection for Kubernetes via KubeArmor policy enforcement.

Enhanced Detections:

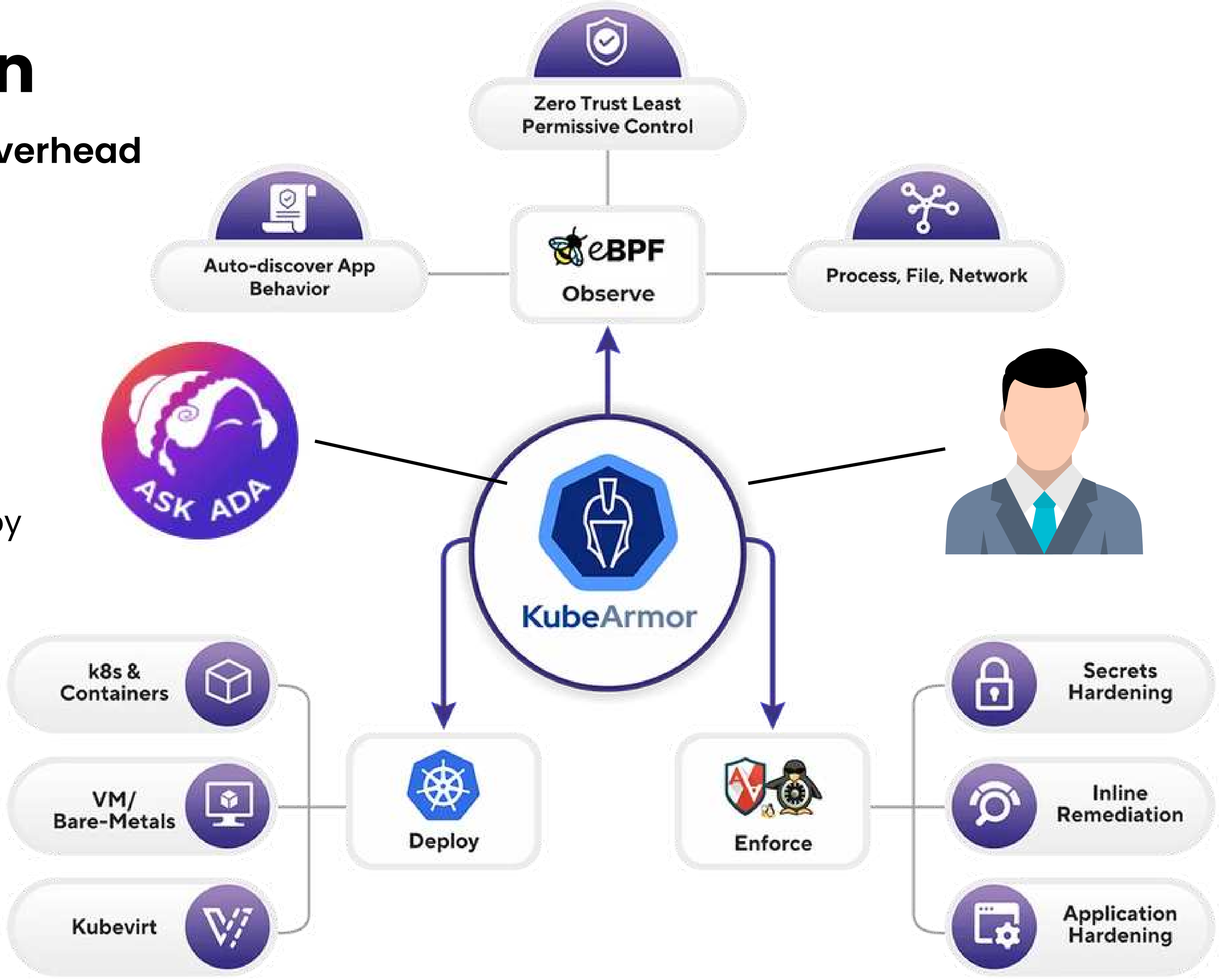
- Identify malicious inbound traffic
- Detect abnormal container escapes
- Recognize cryptojacking activities

Teams can now leverage KubeArmor capabilities at scale by using Ask Ada's conversational interface to apply policies, customize alerts, check statuses, and more.



★ 1200+ Github Stars

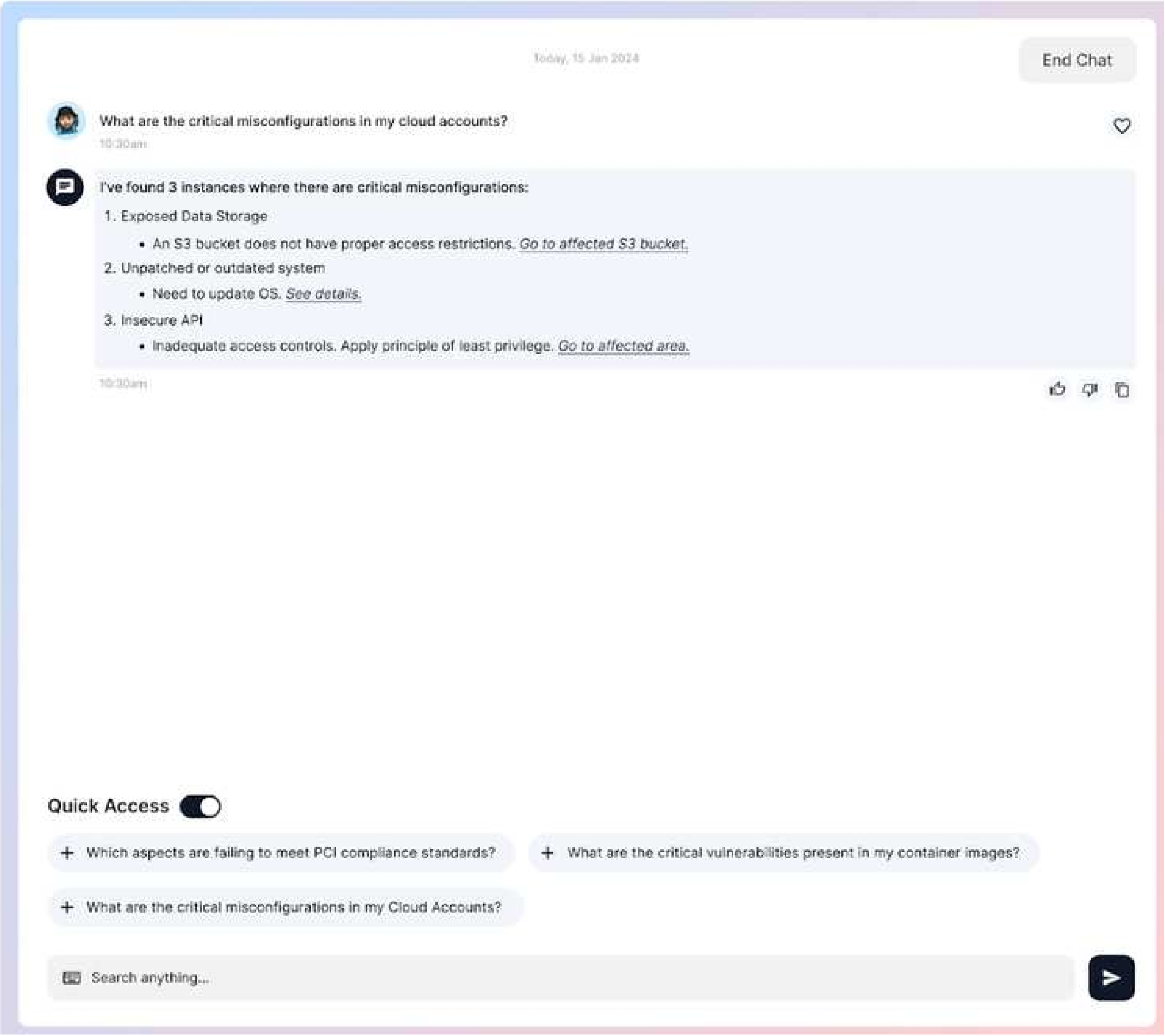
700K+ downloads



Key Takeaway

Hardened runtime application self-protection controls now simplified via conversational interface.

Empower overwhelmed teams struggling with limited visibility across complex cloud environments.



What are the critical misconfigurations in my cloud accounts?
10:30am

I've found 3 instances where there are critical misconfigurations:

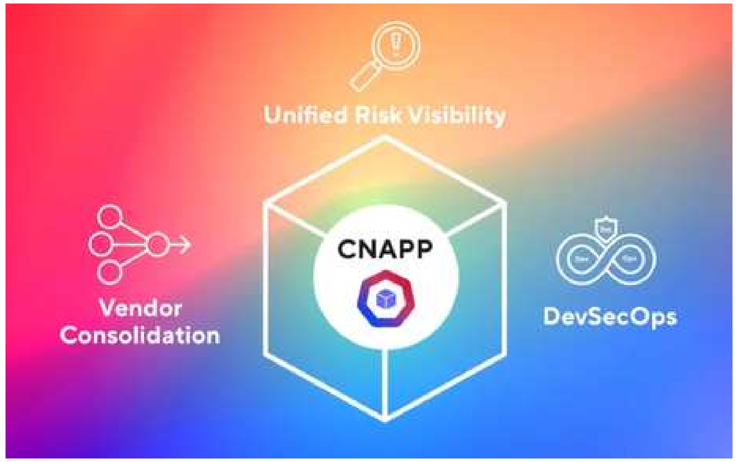
1. Exposed Data Storage
   - An S3 bucket does not have proper access restrictions. *Go to affected S3 bucket.*
2. Unpatched or outdated system
   - Need to update OS. *See details.*
3. Insecure API
   - Inadequate access controls. Apply principle of least privilege. *Go to affected area.*

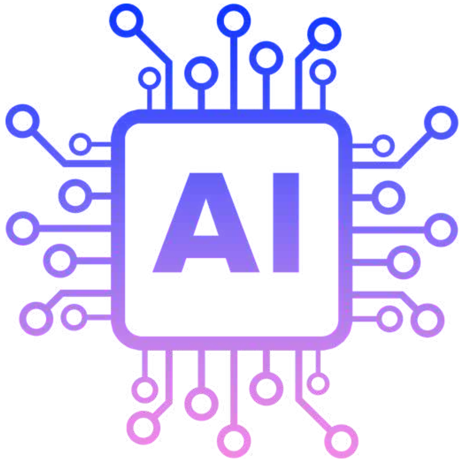
10:30am

Quick Access
+ Which aspects are failing to meet PCI compliance standards?
+ What are the critical vulnerabilities present in my container images?
+ What are the critical misconfigurations in my Cloud Accounts?
Search anything...

Supported Tools:

1. Cloud platforms - AWS, Azure, GCP
2. CI/CD - GitHub, GitLab, Jenkins
3. Ticketing - Jira, ServiceNow
4. ChatOps - Slack, MS Teams





Ask questions to get straight to the point answers:

1. "What vulnerabilities should I prioritize based on risk?"
2. "Summarize posture of production workloads."
3. "How can I achieve HIPAA compliance for this database?"

Key Takeaway

True cloud-native security requires correlating insights across infrastructure, applications, identities and data.

- √ Monitoring
- √ Logging
- √ eBPF based Telemetry

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

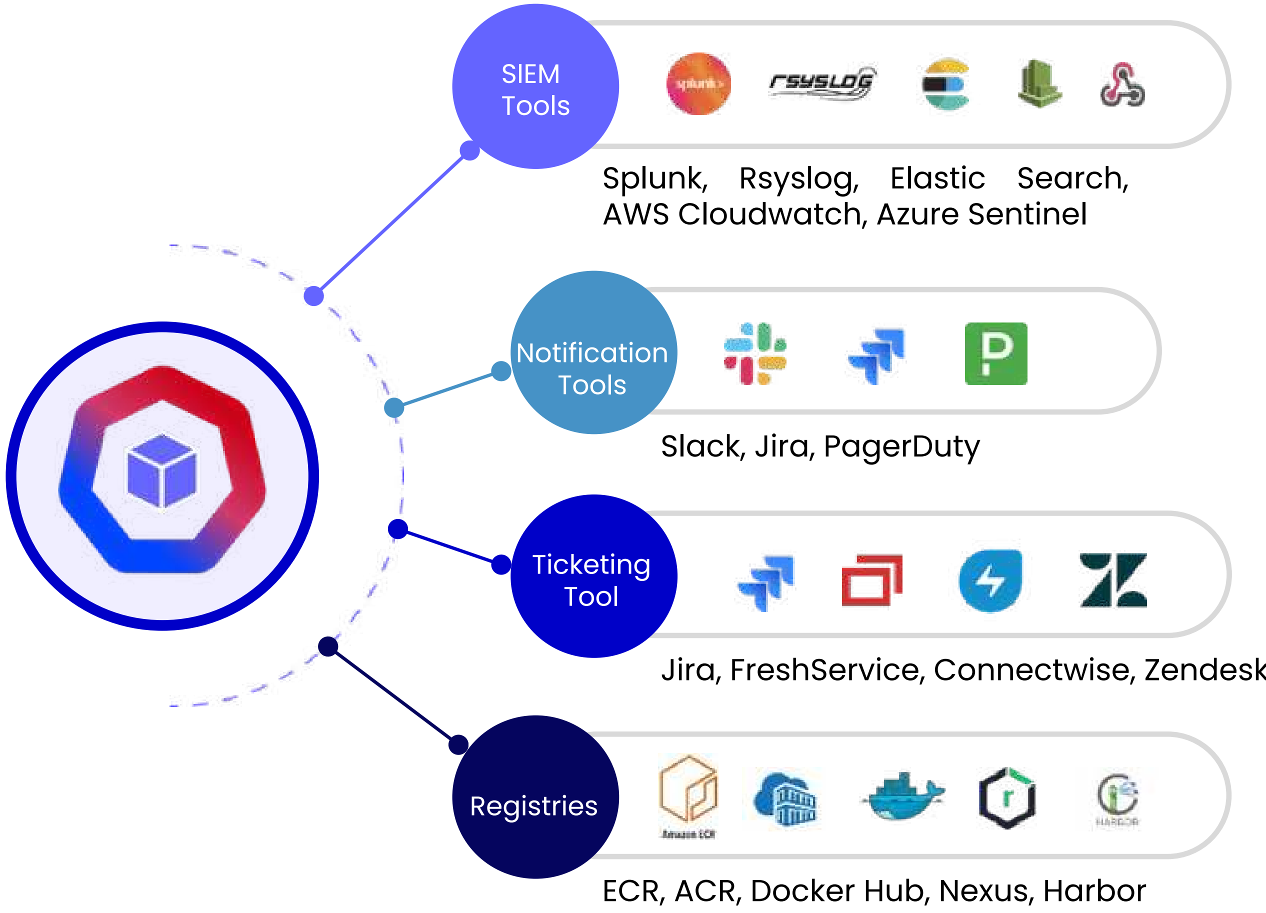
Troubleshooting

Accelerate troubleshooting with a single source of truth

VM/Baremetal, Container or K8s context

eBPF backed telemetry

Logs Aggregation



SIEM Tools

Splunk, Rsyslog, Elastic Search, AWS Cloudwatch, Azure Sentinel

Notification Tools

Slack, Jira, PagerDuty

Ticketing Tool

Jira, FreshService, Connectwise, Zendesk

Registries

ECR, ACR, Docker Hub, Nexus, Harbor

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

Architectural Overview

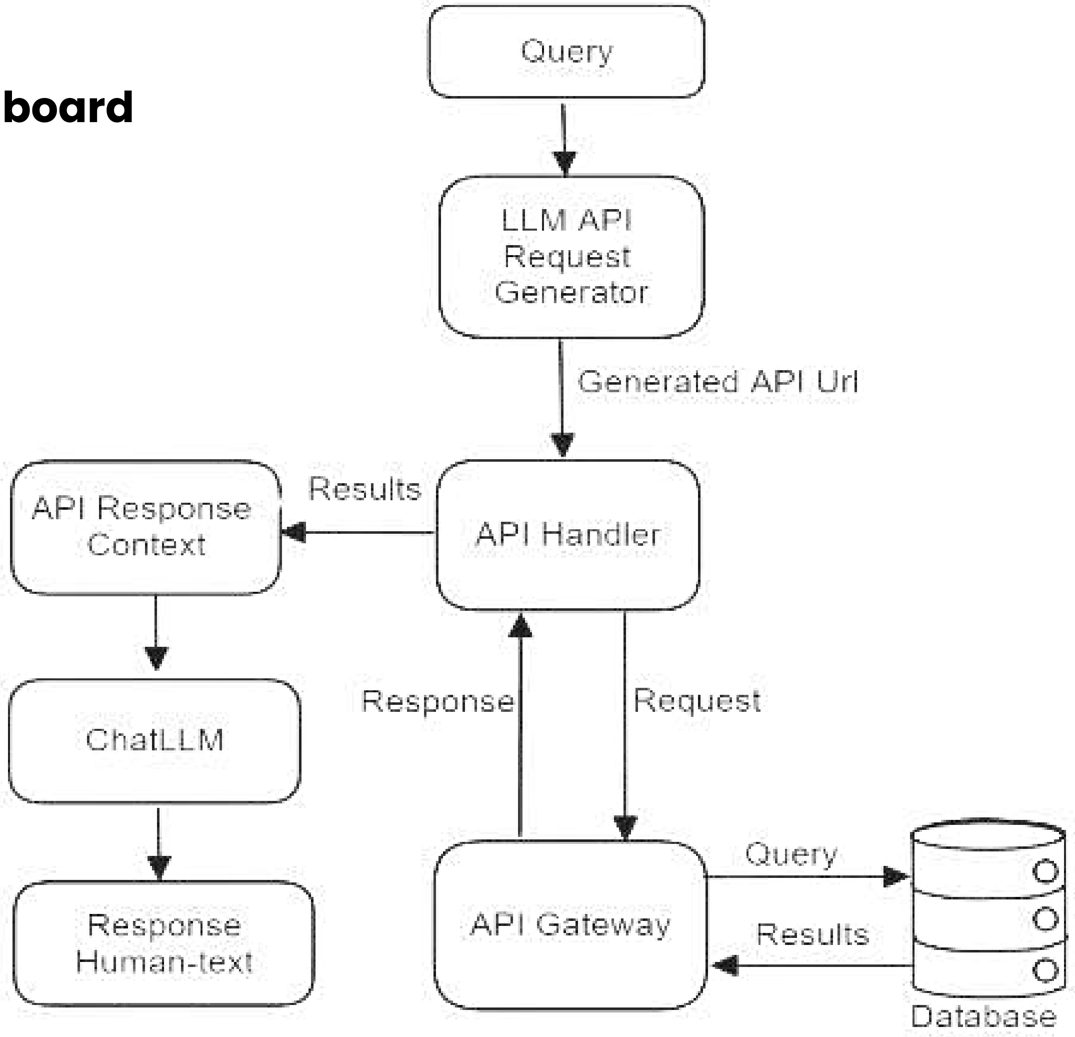
Correlate Insights Across Entire AccuKnox CNAPP Dashboard

Ask Ada correlates insights across infrastructure, identities, applications and data to deliver unified cloud-native security.

Key Data Sources

- Cloud audit logs and APIs
- Kubernetes telemetry
- CI/CD notifications
- Vulnerability scans
- Web application scans

By synthesizing signals from disjointed tools. Ask Ada offers a complete view of dynamic environments, which helps teams to ensure security.



Key Takeaway

True cloud-native security requires correlating insights across infrastructure, applications, identities and data.

Reasoning Capabilities

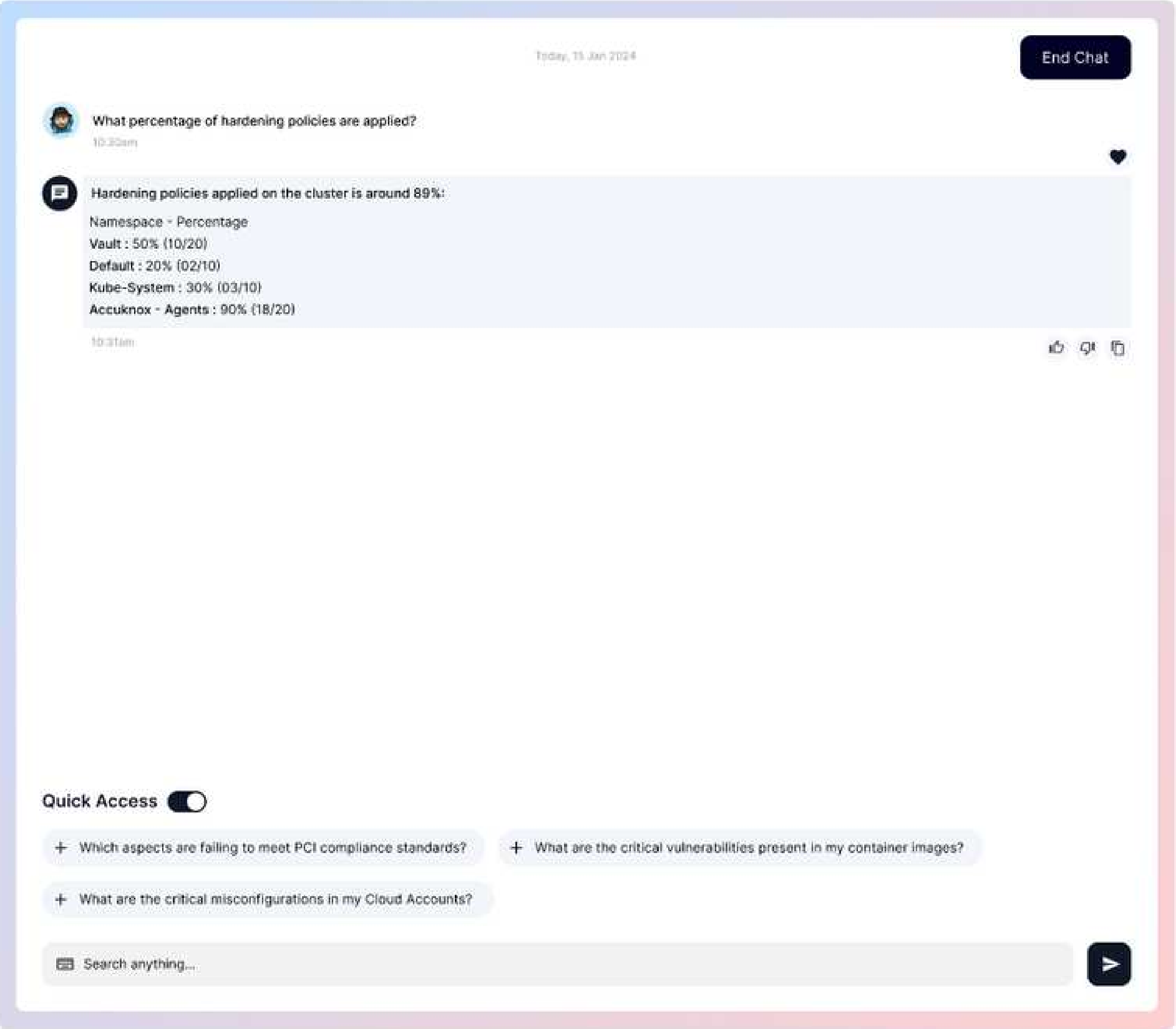
Threat Detection Through Advanced Reasoning

Ask Ada reasons across data, tools, and time to accelerate detection and response.

Analytical Capabilities

- Causality analysis
- Pattern detection
- Anomaly identification
- Risk extrapolation

By mimicking human understanding, Ask Ada can connect disparate alerts into higher fidelity incidents, predict attack trajectories, and guide optimal remediation.



Today, 15 Jan 2024

End Chat

What percentage of hardening policies are applied?
10:30am

Hardening policies applied on the cluster is around 89%:

Namespace - Percentage
Vault : 50% (10/20)
Default : 20% (02/10)
Kube-System : 30% (03/10)
Accuknox - Agents : 90% (18/20)

10:31am

Quick Access

+ Which aspects are failing to meet PCI compliance standards?
+ What are the critical vulnerabilities present in my container images?
+ What are the critical misconfigurations in my Cloud Accounts?

Search anything...

Key Takeaway

True cloud-native security requires correlating insights across infrastructure, applications, identities and data.

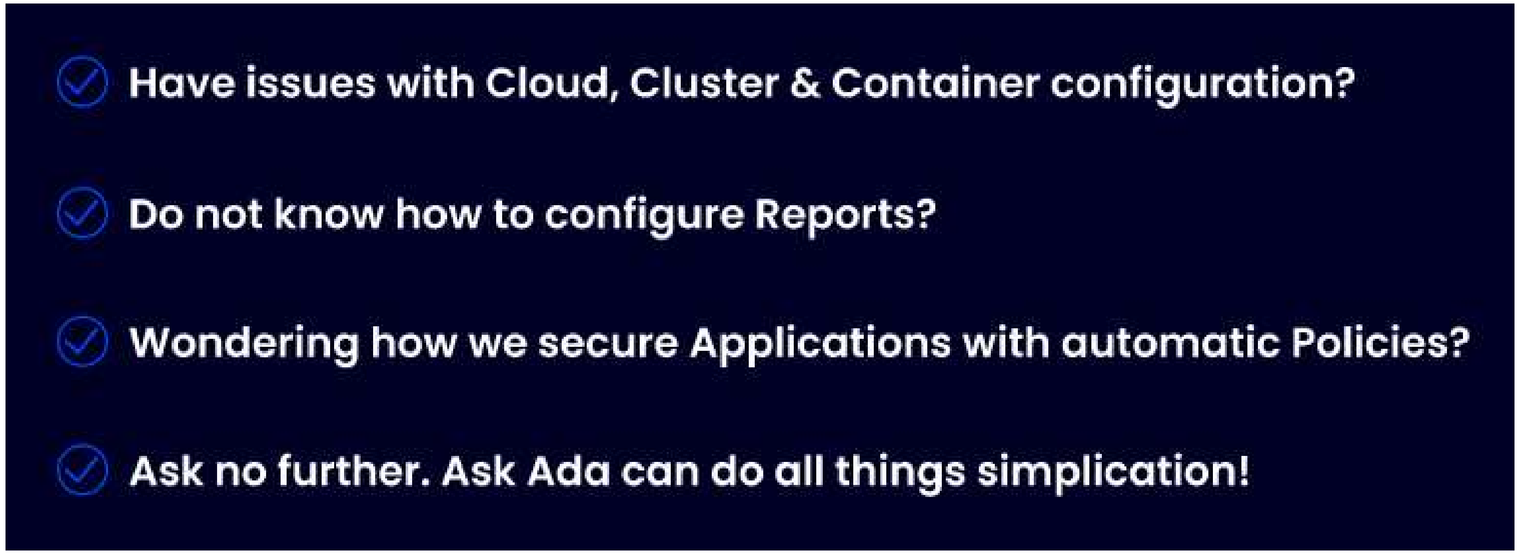
Assistive Workflows

Tailored Guidance for Efficient Workflows

Ask Ada handles redundant questions and offers guidance to user skill level to boost productivity.

Sample Workflows

- Personalized Onboaring
- Remediation plan tuning
- Contextual policy recommendations
- Access permissions assistance
- Compliance evidence gathering



✓ Have issues with Cloud, Cluster & Container configuration?

✓ Do not know how to configure Reports?

✓ Wondering how we secure Applications with automatic Policies?

✓ Ask no further. Ask Ada can do all things simplication!

With continuous assistance for security teams, Ask Ada overcomes key challenges around skill gaps, tribal knowledge, alert overload, constantly changing environments, and limited resources.

Key Takeaway Increase productivity by handling redundant questions and tailoring guidance to skill level.

Try Ask Ada Today

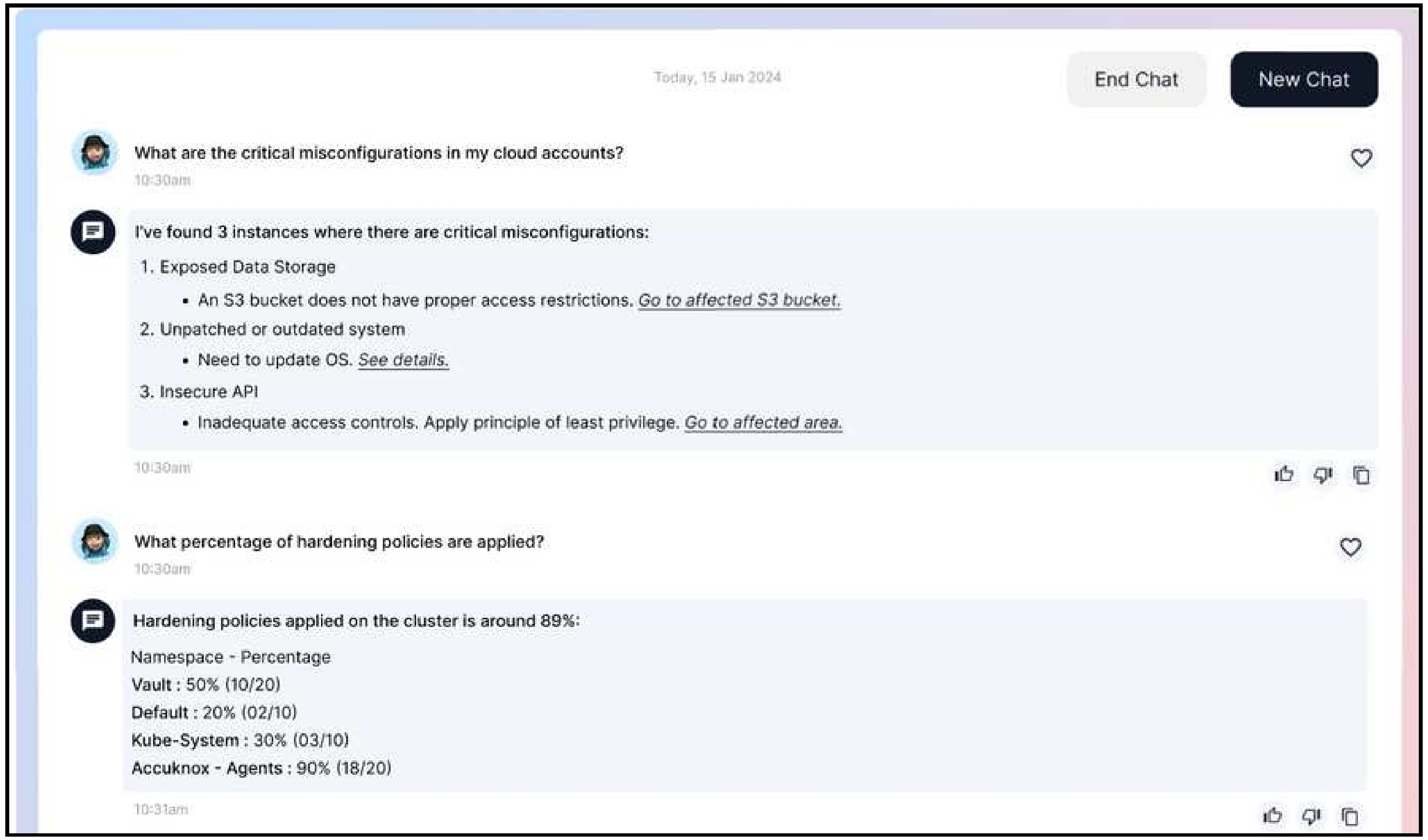
Bridge visibility gaps, eliminate alert fatigue, enable proactive hardening and much more!

Ask Ada will be available for customers with industry-leading data privacy/security controls plus anti-hallucination guardrails.

Get Started:

- Sign up via accuknox.com to get early beta access
- Schedule a customized demo of critical use cases
- Visit our interactive forums to provide inputs

Empower your team by leveraging Ask Ada's advanced generative capabilities today!



What are the critical misconfigurations in my cloud accounts?
10:30am

I've found 3 instances where there are critical misconfigurations:

1. Exposed Data Storage
   - An S3 bucket does not have proper access restrictions. Go to affected S3 bucket.
2. Unpatched or outdated system
   - Need to update OS. See details.
3. Insecure API
   - Inadequate access controls. Apply principle of least privilege. Go to affected area.

10:30am

What percentage of hardening policies are applied?
10:30am

Hardening policies applied on the cluster is around 89%:

Namespace - Percentage
Vault : 50% (10/20)
Default : 20% (02/10)
Kube-System : 30% (03/10)
Accuknox - Agents : 90% (18/20)

10:31am

Newsflash

Ask Ada provides valid and accurate information without the "hallucination" seen in other Gen-AI tools. It ensures industry-leading data privacy/security and includes anti-hallucination guardrails.

Takeaway

AccuKnox Ask Ada: One of the first Gen-AI Based Cloud Security Assistant

One-chat solution for :

Misconfigurations, Vulnerabilities, Attack Remediations, Zero Trust Policies, Inline Prevention

JOIN WAITLIST

- ✓ Have issues with Cloud, Cluster & Container configuration?
- ✓ Do not know how to configure Reports?
- ✓ Wondering how we secure Applications with automatic Policies?
- ✓ Ask no further. Ask Ada can do all things simplication!

Leverage Ask Ada's blend of knowledge, reasoning, and automation on top of AccuKnox's CNAPP for fearless innovation without compromising resilience or compliance.

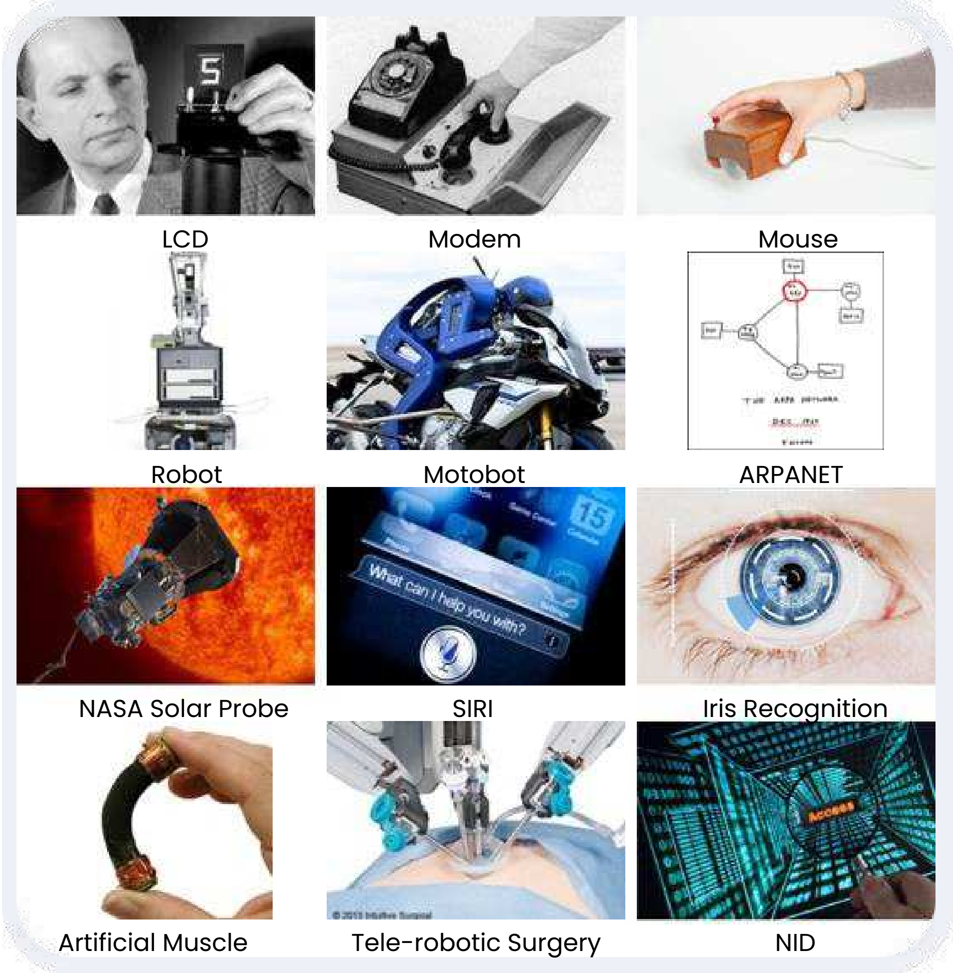
About AccuKnox

- 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


LCD
Modem
Mouse
Robot
Motobot
ARPANET
NASA Solar Probe
SIRI
Iris Recognition
Artificial Muscle
Tele-robotic Surgery
NID

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."

LIVANTA™

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."

ONDA

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."

clint™

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."

IXEL-INTERNATIONAL

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."

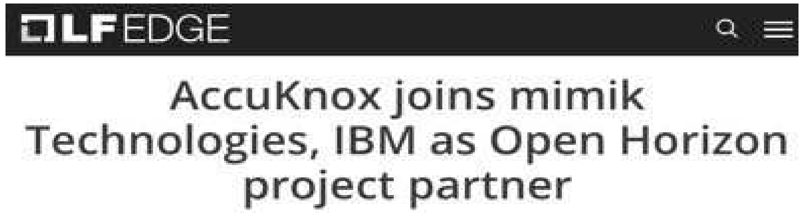
Chase Cunningham
Renowned Cyber Security Analyst and Zero-Trust Expert

Key Takeaway

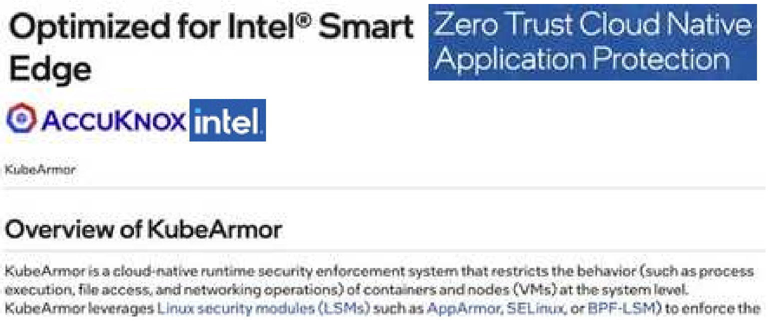
AccuKnox, a pioneer in cloud-native security, is renowned for its innovative Zero Trust runtime security, Cloud Workload Protection, and Kubernetes-specific capabilities, backed by a groundbreaking partnership with Stanford Research Institute.

Power of Partnerships

IBM



AccuKnox joins mimik Technologies, IBM as Open Horizon project partner



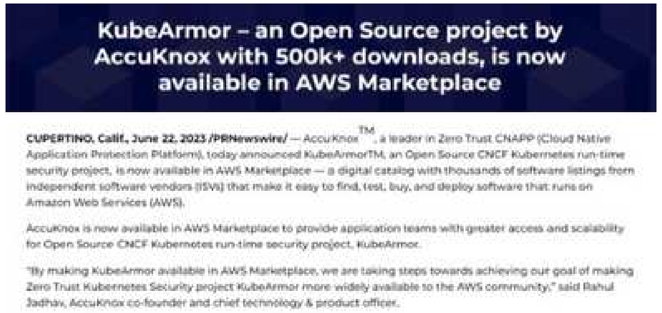
Optimized for Intel® Smart Edge

Zero Trust Cloud Native Application Protection

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

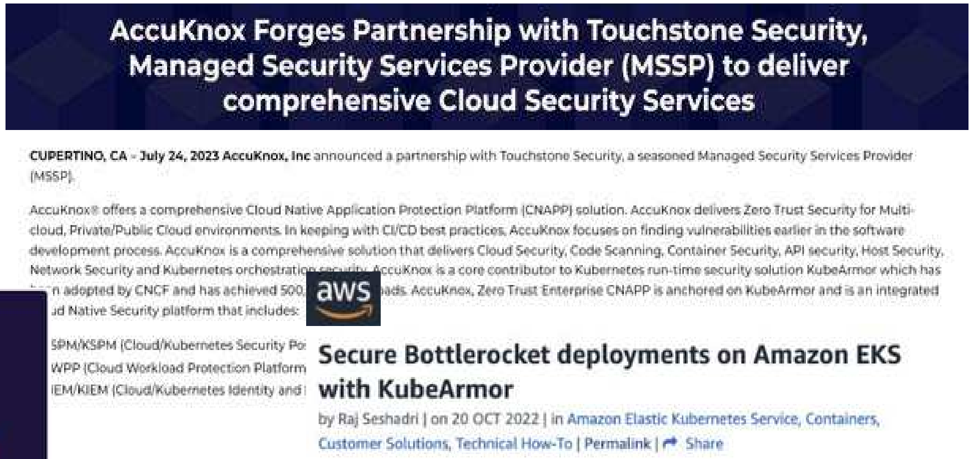
CUPERTINO, Calif., June 22, 2023 /PRNewswire/ — AccuKnox™, a leader in Zero Trust CNAPP (Cloud Native Application Protection Platform), today announced KubeArmorTM, an Open Source CNCF Kubernetes run-time security project, is now available in AWS Marketplace — a digital catalog with thousands of software 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)
ORACLE Cloud

KubeArmor Support for Oracle Container Engine for Kubernetes (OKE)



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, ads. AccuKnox, Zero Trust Enterprise CNAPP is anchored on KubeArmor and is an integrated ud Native Security platform that includes:

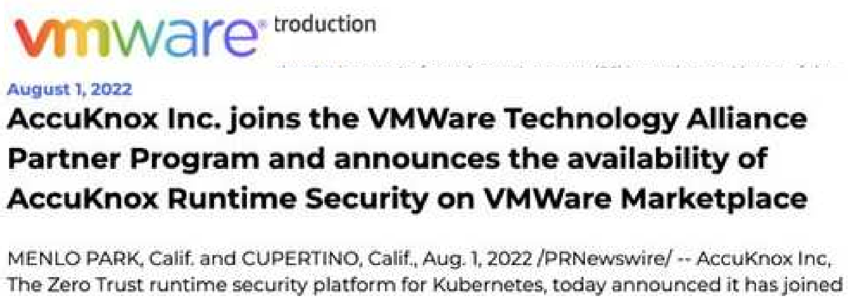
SPM/KSPM (Cloud/Kubernetes Security Po

WPP (Cloud Workload Protection Platform

IEM/KIEM (Cloud/Kubernetes Identity and

Secure Bottlerocket deployments on Amazon EKS with KubeArmor

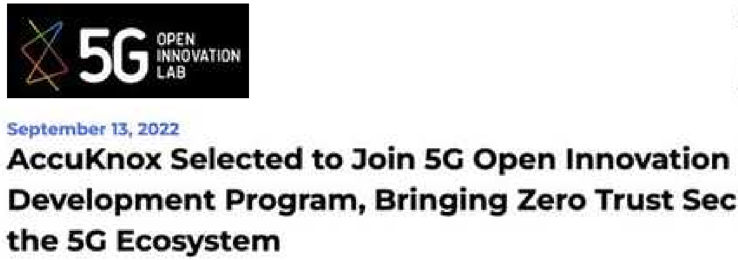
by Raj Seshadri | on 20 OCT 2022 | in Amazon Elastic Kubernetes Service, Containers, Customer Solutions, Technical How-To | Permalink | Share



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



September 13, 2022

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

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

AccuKnox

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:

aws ORACLE Gartner NEPHIO IBM LF EDGE

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+	10+	30+	10+
TOOLS INTEGRATION	PATENTS	TRUSTED PARTNERS	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** →