AccuKnox Newsletter | November 2025

Hot Off The Press!

Our Latest Partnerships, Blogs and News That Made the Headlines

Alice Blue - Top Brokerage Firm Selects AccuKnox

- Alice Blue partners with AccuKnox, setting a new standard in clarity, control, and ironclad compliance for its trading ecosystem.
- Powered by AccuKnox CNAPP, the firm's infrastructure is continuously protected and ready to meet the high-stakes demands of modern finance.

Read Press Release

Zero Trust Partnership in Latin America

- ShieldForce's standout Zero Trust CNAPP session at a major Mexican cybersecurity conference underscored how urgently the region is seeking stronger, modern defenses.
- AccuKnox brings a faster and more grounded approach to securing Latin America's cloud, AI, and enterprise environments.

Read Press Release

API Security - What's Coming Down the Pike?

A complete platform for API discovery, runtime protection, and Zero Trust enforcement across cloud and Kubernetes environments. Join the rollout and see how modern API security is meant to work.

Ask us for an API Security deep dive

Blogs & Resources

Latest blogs, product highlights, expert comparisons, and practical security tips.

MCP Security, Simplified

AI talking to your systems is powerful but risky. AccuKnox keeps every AI action verified, controlled, and safe so innovation never compromises security.

Read Full Blog

Top Microsegmentation Tools for 2025

This blog breaks down the 7 best microsegmentation tools. Learn how each tool isolates workloads, automates policies, and uses AI-driven insights to keep your environment secure.

Read Full Blog

How Attackers Escalate Privileges in OpenShift AI — and How AccuKnox Stops Them

A deep dive into how attackers exploit over-permissive RBAC roles in OpenShift AI and how AccuKnox runtime policies enforce Zero Trust to protect secrets, workloads, and clusters.

Read Full Blog

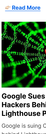
Inside Sysdig: Strengths & Gaps

Our latest blog breaks down what Sysdig offers and where it falls short. From limited runtime protection to visibility trade-offs, we analyze it all. See why AccuKnox outperforms as the more complete CNAPP.

Read Full Blog

CVE Defences

Read about recent cyber attacks and how to mitigate them.



CVE-2023-38408: Critical RCE Vulnerability in OpenSSH

A critical RCE flaw in OpenSSH's ssh-agent can let attackers run arbitrary code via SSH agent forwarding. AccuKnox mitigates the risks it poses to your systems with patching, configuration hardening, and runtime security.

Read Full Blog

CVE-2022-31160: jQuery UI XSS Vulnerability Explained

Understand where the vulnerability sits, who's most exposed, and why sectors like finance, e-commerce, and healthcare are still at risk. AccuKnox hardens production environments with runtime XSS detection, CSP enforcement, and CI/CD dependency scanning.

Read Full Blog

Product Tours

Experience our AI-powered CNAPP interactive product tours!

Breaking Down Log4j Attack: AccuKnox's Defense Mechanism

See how AccuKnox mitigates critical Log4j vulnerabilities with automated detection and runtime remediation.

Watch Now

LLM Prompt Firewalls

Step By Step Guide on How to Set Up Firewalls for Request and Response Level Prompts for better AI Security

Watch Now

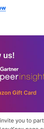
Industry News

Cyberworld headlines, stay informed

New Cyber Rules Hit the Defense Supply Chain

The U.S. DoD has formally activated CMMC. The rule introduces a phased certification model starting with self-assessments and progressing to mandatory third-party audits.

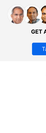
Read More



'Whisper Leak': Encrypted AI Chats Aren't Really Private

Microsoft discovered Whisper Leak, a side-channel attack that lets someone on the same network infer your AI chat topics by analyzing encrypted traffic patterns.

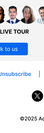
Read More



Google Sues China-Based Hackers Behind $1B Lighthouse Phishing Empire

Google is suing China-based hackers behind Lighthouse, a $1B Phishing-as-a-Service platform targeting M+ users across 120 countries.

Read More



Microsoft Patches 63 Vulnerabilities...

On Nov 12, 2025, Microsoft patched 63 flaws, including a Windows Kernel zero-day and a Kerberos delegation bug. Key issues: privilege escalation and remote code execution.

Read More

Google Unveils Private AI Compute for Secure Cloud AI Processing

Google launched Private AI Compute, a secure cloud platform that processes AI queries while keeping user data private, even from Google.

Read More

Amazon Exposes Advanced Attacks Exploiting Cisco ISE and Citrix NetScaler

Amazon's threat team discovered an advanced actor exploiting zero-day in Cisco ISE and Citrix NetScaler ADC to deploy custom malware.

Read More

Collaterals

Resources packed with long form and short form security information

AI Security One-Pager

Understand how AccuKnox AI-SPM protects against AI-driven threats.

Download Now

How AccuKnox Transformed Security for a Leading UAE Bank

AccuKnox replaced Prisma Cloud for a leading UAE bank, cutting CPU/RAM usage, alert noise, and SOC triage time while improving multi-cloud security coverage.

Download Now

We're excited to invite you to participate in our **Gartner review incentive program!** Simply visit the AccuKnox page on Gartner and share your honest feedback. Everyone who submits a review will be entereted to win a **$5 Gift Card** or exclusive **AccuKnox swag**.

1. **Submit Review : https://gtnr.io/XmiDjBLJV**
2. **Collect a Swag: accuknox.com/swag**