KubeArmor -- AccuKnox Open Source project now available in AWS Marketplace

KubeArmor -- an Open Source project by AccuKnox with +500k downloads -- now available in AWS Marketplace

KubeArmor

AccuKnox

CUPERTINO, CALIFORNIA, UNITED STATES, June 20, 2023 /EINPresswire.com/ -- AccuKnoxTM, 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).

> "By making KubeArmor available in AWS, we are taking steps towards achieving our goal of making Zero Trust Kubernetes Security project KubeArmor available to the AWS community," said Rahul Jadhav"
>
> *Rahul Jadhav*

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 is a cloud native runtime security engine that provides observability and inline mitigation of threats. KubeArmor uses eBPF and Linux Security Modules (LSM) -- a technology to run sandboxed programs in a privileged context and a framework. This allows for security extensions to be plugged into the operating system kernel respectively -- to provide a policy-based system to restrict any unwanted, malicious behavior of cloud-native workloads at runtime. KubeArmor helps to secure pods and containers on

Bottlerocket and Amazon Linux 2 – Linux-based operating systems purpose-built by AWS to run containers. KubeArmor offers the following features and benefits:

- Restrict the behavior of containers and other workloads: KubeArmor provides the ability to restrict specific behavior of process executions, file accesses, and networking operations, inside of your workload.
- Enforce security policies at runtime: KubeArmor directly enforces security policies using Linux Security Modules (LSMs) for each workload based on the identities (e.g., labels) of given containers or workloads.
- Enable Zero Trust Security: KubeArmor provides a way to enforce Zero Trust security posture by applying an allow-based policy which permits specific application behavior and denies/audits everything else.
- Generate logs when policy violations occur: KubeArmor produces alert logs for policy violations by monitoring the operations of containers' processes using its eBPF-based monitor.
- Simplify Zero Trust policy definitions: KubeArmor manages internal complexities associated with LSMs and provides easy semantics for policy definitions.
- Kubernetes-native security enforcement engine: KubeArmor allows operators to define security policies based on Kubernetes metadata and simply apply them into Kubernetes.

According to John McNeice, S&P Global, a Leading Cybersecurity Market Research Analyst, “AccuKnox is a Core Contributor to the highly popular Kubernetes Run-Time Security CNCF Project, which has achieved 500,000+ downloads." Golan Ben-Oni, CIO, IDT Telecom, adds “AccuKnox and its companion OpenSource offering, KubeArmor, have very powerful capabilities in the areas of in-line mitigation of run-time attacks, and very strong capabilities in the areas of Network Security. These are critical to thwarting advanced Zero Day Attacks. Every few years, a disruptive technology emerges which has the potential to uplift the industry in a way that exceeds the incremental advances made by traditional security providers. KubeArmor has exceeded these expectations. We are very pleased to partner with them in their quest to turn their innovation into product and market leadership.”

Availability in AWS Marketplace comes after news of AccuKnox raising a $6M funding round to fuel its growth.

To learn more about KuberArmor:

- Download and install KuberArmor (AWS Marketplace)
- Review KubeArmor Runtime protection for Kubernetes & other cloud Workloads
- Watch the motivations behind KubeArmor - video [11 mins]
- Read about secure Bottlerocket deployments on Amazon Elastic Kubernetes Service (Amazon EKS) with KubeArmor - AWS Blog
- Watch the KubeArmor Demo on Bottlerocket

About AccuKnox

AccuKnoxTM provides a Zero Trust Cloud Native Application Security (CNAPP) platform. AccuKnox is the core contributor to Kubernetes run-time security solution, KubeArmorTM, a very popular CNCF (Cloud Native Computing Foundation) project. AccuKnox was developed in strategic partnership with SRI and is anchored on seminal inventions in the areas of Application Security, Network Security, Anomaly Detection, and Data Provenance. AccuKnox and its companion OpenSource project can be used to secure Cloud (Public and Private), IoT/Edge and 5G workloads. AccuKnox has been funded by prestigious Silicon Valley investors and Strategic Investors with deep expertise in CyberSecurity. www.accuknox.com

Contact:
Nat Natraj, co-founder, CEO
n@accuknox.com
@N_SiliconValley

Nat Natraj
AccuKnox
+1 510-579-8785
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube
