ENTERPRISE SECURITY

WWW.ENTERPRISESECURITYMAG.COM

ZERO TRUST SECURITY EDITION

TOP
ZERO TRUST SECURITY
Solution Provider
2021

$15

AccuKnox

Zero-Trust Identity-Driven Security for Virtual Application Management

Kubernetes has established itself as a clear winning Cloud micro-services orchestration platform. However, the ephemeral and transient nature of Kubernetes creates considerable security challenges. There are several instances where some of the world's biggest tech companies have been victims of a cyber attack because their Kubernetes cluster was vulnerable, and hackers were able to take control and find the credentials of their cloud environments. Even the traditional approaches to Linux, VM security like IPTables are not effective and are not scalable/ cost-effective for securing large-scale container workloads.

This is where the value proposition of AccuKnox comes in.

Partnering with Stanford Research Institute's (www.sri.com SRI International) innovations in the areas of container security, anomaly detection, data provenance/data security, AccuKnox has made Zero-Trust runtime security deployable and usable by mainstream enterprises. Leveraging an identity-driven security approach, AccuKnox runtime Zero Trust Kubernetes security solution protects networks, applications, data, APIs, Edge/IoT, and 5G.

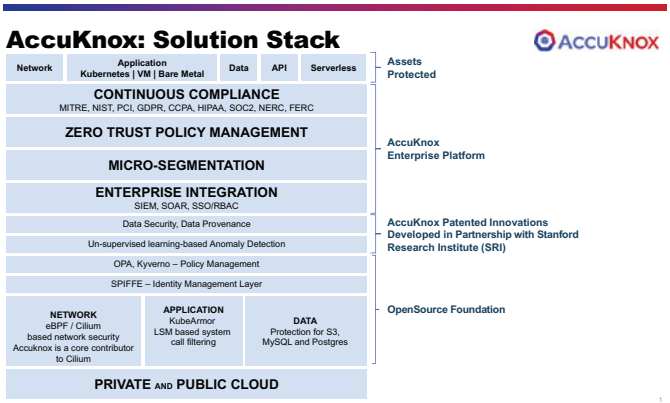
The AccuKnox platform is based on a rock-solid open-source foundation of Extended Berkeley Packet Filter (eBPF), one of the high performance kernel tracing technologies. AccuKnox has contributed KubeArmor (www.kubearmor) a container-aware runtime security enforcement system to the OpenSource community. AccuKnox uses SPIFFE [https://spiffe.io/ - Secure Production Identity Framework For Everyone] to generate cryptographically unique user and service identities that serve as the perimeter to enforce an identity-driven security model.

On top of this, AccuKnox provides a very comprehensive Policy Management Lifecycle engine for different stakeholders (developers, security, compliance) to author policies, create policy tiers, execution sequences, etc. This further allows organizations to implement micro-segmentation.

Accuknox employs unsupervised learning-based AI-engine to detect anomalies and instabilities in large scale Kubernetes environments, thereby detecting early indications of potential compromise. In addition, AccuKnox delivers comprehensive Data Security through the use a Data Provenance engine for tracking and tracing data access, modification, exfiltration, etc.

Furthermore, AccuKnox provides a Continuous Compliance engine providing a real time dashboard of compliance with major governance standards (PCI, GDPR, CCPA, HIPAA, etc.)

The platform also provides comprehensive integration with 3rd party security platforms pertaining to SIEM, SOAR, and SSO/ RBAC for enterprises.



Such comprehensive and holistic features of the Accuknox platform have helped it gain huge client traction. To expand a bigger footprint in the market, the company will continue on its road to innovation and research and access the R&D facility of SRI. Backed by the expert minds of scientists from the US department of defense, such as Phil Porras, Accuknox will be focusing on enhancing its platform, building new products, IoT, and 5G technology. "The technical and business benefits of Kubernetes have been well established. ZeroTrust security is an imperative for all organizations and governments. ZeroTrust is far easy to preach than practice. AccuKnox aims to allow organizations to deploy ZeroTrust Kubernetes Security and Continuous Compliance for Public and Private clouds with remarkable ease and cost-effectively," concludes Nat Natraj, CEO of Accuknox. ES