AccuKnox | Migawka z 1 slajdem

AccuKnox

O nas

AccuKnox zapewnia platformę Zero Trust Cloud Native Application Security (CNAPP) i dostarcza kod do zabezpieczeń w czasie wykonywania. AccuKnox jest głównym współtwórcą rozwiązania zabezpieczającego Kubernetes Run-time, KubeArmor® i projektu CNCF (Cloud Native Computing Foundation), z którego pobrano ponad 700 000 plików. AccuKnox został opracowany we współpracy z SRI (Instytut Badawczy Stanforda) i opiera się na przełomowych wynalazkach w obszarach bezpieczeństwa kontenerów, wykrywania anomalii i pochodzenia danych. AccuKnox jest finansowany przez wiodących inwestorów CyberSecurity www.accuknox.com

Kluczowe fakty

 # Pracownicy: 65 **Zasięg sprzedaży:** Światowy **Podniesiony kapitał:** $11M

Produkt

Sterowniki biznesowe, techniczne

- Bezpieczeństwo zerowego zaufania
- Bezpieczeństwo Kubernetesa
- Multi-cloud – Chmura Publiczna Chmura Prywatna
- Bezpieczeństwo w czasie wykonywania
- Priorytetyzowanie luk w zabezpieczeniach, automatyzacja
- Wykrywanie i łagodzenie znoszenia

Produkt, rozwiązania

- CNAPP (platforma ochrony aplikacji natywnych w chmurze)
- CSPM – Zarządzanie stanem bezpieczeństwa w chmurze – Bezpieczeństwo statyczne
- ASPM – zarządzanie stanem bezpieczeństwa aplikacji. – DevSecOps
- CWPP – platforma ochrony obciążeń w chmurze – bezpieczeństwo w czasie wykonywania
- KIEM – Kubernetes Zarządzanie tożsamością i uprawnieniami
- AskADA – drugi pilot bezpieczeństwa oparty na GenAI

Przypadków użycia

- Zautomatyzowane podejście do bezpieczeństwa chmury o zerowym zaufaniu (publicznej, prywatnej, hybrydowej, bezprzewodowej).
- Zarządzanie lukami w zabezpieczeniach i ustalanie priorytetów
- Bezpieczeństwo w czasie wykonywania, mikrosegmentacja
- Zapora sieciowa aplikacji, hartowanie jądra
- Wykrywanie dryfu i ścieżka audytu
- Ciągła diagnostyka i łagodzenie skutków
- GRC – CIS, HIPAA, RODO, SOC2, STIG, MITRE, NIST
- Zabezpieczanie zadań o znaczeniu krytycznym, takich jak Vault
- Zabezpieczanie środowiska roboczego AI, takiego jak Jupyter Notebook

Kluczowe wyróżniki

- Bezpieczeństwo w linii (w przeciwieństwie do zabezpieczeń po ataku)
- Zabezpiecza nowoczesne obciążenia (K8) i tradycyjne obciążenia (maszyny wirtualne)
- Multi Cloud, prywatna, bezpieczna chmura z przerwami powietrznymi
- KIEM – Kubernetes Zarządzanie tożsamością i uprawnieniami
- CDR – wykrywanie i reagowanie w chmurze
- IAC – Infrastruktura jako skanowanie kodu
- ASPM – Możliwość przeprowadzania kontroli w potoku CI, takich jak DAST, SAST, SCA

Opinie klientów

Duży integrator z USA

"Przeprowadziliśmy obszerną analizę porównywalnych ofert branżowych i wybraliśmy AccuKnox ze względu na obsługę chmury publicznej i prywatnej oraz wysoce zróżnicowane możliwości w obszarach priorytetyzacji ryzyka, wykrywania dryfu i zaawansowanej zgodności. Co więcej, byliśmy pod wielkim wrażeniem integracji AccuKnox z wiodącymi platformami do zarządzania lukami, takimi jak Nessus."

Duży europejski klient

"Potężne połączenie CSPM i CWPP AccuKnox; Podstawy OpenSource; Wbudowane bezpieczeństwo Zero Trust; Wsparcie dla chmur publicznych i prywatnych; uczynił ich idealnym partnerem dla nas. Nasz klient, duża europejska agencja CyberSecurity, szukała rozwiązania bezpieczeństwa Zero Trust, które obsługuje platformy Private Cloud. Nasze zwycięstwo jest wyraźnym świadectwem wartości, jaką nasi klienci widzą w tym partnerstwie. Mamy nadzieję, że przed nami jeszcze wiele sukcesów."

Wzmacniacz

Chmura: aws, Azure, Google Cloud Platform, Red Hat, NUTANIX, MIRANTIS

Integratorzy Systemów: accenture, TCS TATA CONSULTANCY SERVICES, TATA ELXSI, HCL

OEM: xcitium

Sprzedawcy, dystrybutorzy: Kilka

MSSP: Kilka

Kluczowe kontakty

Handlowy: Emre Kulali Emre@accuknox.com

Federalny: Bill Kalogeros bk@accuknox.com

Związki partnerskie: Raj Panchapakesan raj@accuknox.com
Ron Victor ron@accuknox.com

Informacja: Siddiq siddiq@accuknox.com