Zestawienie danych

SUSE Security: bezpieczeństwo i kontrola zgodności środowisk Kubernetes

SUSE Security w skrócie

SUSE Security to zintegrowana platforma bezpieczeństwa i utrzymania zgodności, która upraszcza i automatyzuje procesy zabezpieczania, zapewniając zarazem wieloetapową ochronę aplikacji natywnych dla Kubernetesa - od ich tworzenia, aż po wdrożenie produkcyjne.

SUSE

Przegląd korzyści

- Segmentacja kontenerów „zero trust” oparta na zachowaniu
- Zautomatyzowane tworzenie polityk bezpieczeństwa i ich egzekwowanie
- Pełna widoczność sieci i kontenerów w warstwie 7
- Kompleksowa ocena zgodności i raportowanie
- Ograniczanie zagrożeń i zapobieganie atakom typu „zero day”.

W Reputation.com rozumiemy znaczenie reputacji firmy. Posiadanie bezpiecznej infrastruktury IT ma ogromne znaczenie dla naszej reputacji. SUSE NeuVector, koncentrując się na bezkompromisowym bezpieczeństwie środowiska uruchomieniowego i bezpieczeństwie sieci kontenerów na poziomie warstwy 7, daje nam wgląd w bezpieczeństwo ruchu w kontenerach, a także automatyzację, mechanizmy egzekwowania i ograniczania skutków naruszeń”.

Starszy dyrektor IT i bezpieczeństwa informacji w Reputation.com

Bezpieczeństwo kontenerów w całym cyklu ich życia

Przetwarzanie w chmurze i przejście na infrastrukturę kontenerową przyspiesza działalność biznesową, ale wprowadza również nowe problemy związane z bezpieczeństwem. Kubernetes, *de facto* standard orkiestracji kontenerów, dodaje warstwę złożoności do bezpieczeństwa przy jednocześnie niewielkiej wiedzy specjalistycznej przedsiębiorstw. Organizacje stają w obliczu nowych zagrożeń w tym rozproszonym środowisku obliczeniowym i nie mogą polegać na tradycyjnych środkach bezpieczeństwa w celu ochrony swoich sieci lub aplikacji.

SUSE Security umożliwia organizacjom nawet o zasięgu globalnym kompleksowe zabezpieczanie natywnych aplikacji Kubernetes bez negatywnego wpływu na szybkość działania biznesu. Zintegrowana platforma bezpieczeństwa i zgodności, jaką jest SUSE Security, upraszcza i automatyzuje zabezpieczenia, zapewniając bezpieczeństwo typu „zero trust” dla aplikacji natywnych dla środowiska Kubernetes od etapu projektowania po uruchomienie produkcyjne. SUSE Security zapewnia zespołom ds. bezpieczeństwa, DevOps i zarządzania infrastrukturą niezrównaną widoczność i ochronę sieci, usprawnioną automatyzację i egzekwowanie zgodności.

Najlepsze rozwiązanie do zabezpieczania nowoczesnych infrastruktur kontenerowych

Bezpieczeństwo kontenerów typu Zero Trust

- Kontrola dostępu dla każdego wdrożenia kontenera na poziomie sieci dla warstwy 7 i procesów obsługi polityk bezpieczeństwa automatycznie tworzonych na podstawie zachowania aplikacji.
- Eksportowanie i wdrażanie polityk bezpieczeństwa w klastrach (*Security as Code*) w celu replikacji segmentacji opartej na zerowym zaufaniu.
- Identyfikacja wszelkich anomalii w ruchu sieciowym lub procesach w kontenerach z opcją monitorowania (tylko alerty) lub ochrony (alerty i blokowanie).

Prostsza zgodność z przepisami

- Ocenianie zgodności i raportowanie dla wszystkich głównych standardów, w tym PCI, NIST, GDPR (RODO) i HIPAA
- Wdrożenie opatentowanej funkcji zapobiegania utracie danych w kontenerach (DLP) w celu zapewnienia zgodności z wymogami SOC2 w zakresie segmentacji kontenerów czy prywatności danych.

Ciągła ochrona sieci

- Uzyskanie widoczności sieci w warstwie 7 wewnątrz i pomiędzy podami Kubernetesa przy użyciu ruchu sieciowego jako źródła prawdziwej informacji
- Identyfikacja i weryfikacja protokołów aplikacji w celu zapobiegania tunelowaniu i atakom „zero day”
- Wykrywanie zagrożeń sieciowych za pomocą głębokiej, opatentowanej metody inspekcji pakietów
- Automatyczne blokowanie zarówno znanych, jak i nieznanych zagrożeń.

Automatyzacja przyjazna dla DevOps

- Wykorzystanie zautomatyzowanego uczenia się zachowań i tworzenia polityk w celu zapewnienia bardziej precyzyjnego dbania o bezpieczeństwo bez zwiększania nakładu pracy programistów
- Automatyzacja skanowania pipeline'ów CI/CD, a także środowiska uruchomieniowego i zabezpieczanie tego środowiska w celu ochrony aplikacji od etapu ich tworzenia po wdrożenia produkcyjne.

Przegląd zagadnień technicznych

SUSE Security jako platforma zapewniająca bezpieczeństwo i zgodność kontenerów ustanawia standardy nowoczesnej infrastruktury kontenerowej. Żadne inne rozwiązanie nie ma tak szerokiego i zaawansowanego wachlarza funkcjonalności - w tym obserwowalność, bezpieczeństwo i automatyzację na wszystkich większych platformach chmurowych i orkiestratorach klastrów Kubernetes. Nasza opatentowana technologia pozwala na głęboką inspekcję pakietów oraz uczenie się na podstawie obserwacji zachowań, pozwalając zidentyfikować poprawne zachowania.

Zespoły DevOps zyskują możliwość zarządzania podatnościami i zgodnością, w tym zautomatyzowane skanowanie CI/CD oraz kontrolę dostępu opartą na rolach. SUSE Security zapewnia kompletny zestaw funkcji do wykrywania i blokowania ataków w czasie rzeczywistym, aktywnie chroniąc produkcyjne środowiska uruchomieniowe. SUSE Security instaluje się jako kontener, co czyni go wysoce skalowalnym rozwiązaniem.

Więcej informacji można uzyskać na stronie www.suse.com lub kontaktując się z SUSE: tel. +48 22-537-5020, email: infolinia@suse.com