Funktionsliste

Kaspersky Container Security

kaspersky BRING ON THE FUTURE

Vorteile für Unternehmen

Weltweit anerkannte Sicherheit

- Die Funktionen und Möglichkeiten von Kaspersky Container Security entsprechen den weltweiten Best Practices für Container-Sicherheit.
- Vielfach getesteter und ausgezeichneter Schutz

Umfassender Schutz für containerisierte Umgebungen

- Schutz auf verschiedenen Ebenen der Architektur der Container-Umgebung
- App-Sicherheit für jede Phase des Lebenszyklus

Einfache Bedienung – zuverlässiger Schutz

- Visualisierung von Bedrohungen in Echtzeit
- Mit der Lösung werden Informationssicherheitsteams entlastet. Gleichzeitig wird die Qualität und Geschwindigkeit der Sicherheitsprüfungen verbessert.

Einhaltung gesetzlicher Vorschriften

- CIS-Benchmark-Audits
- Transparentes Reporting-System

Einleitung

Kaspersky Container Security (KCS) ist eine Sicherheitslösung, die jede Phase des Lebenszyklus einer containerisierten Anwendung abdeckt, von der Entwicklung bis zum Betrieb. Die Lösung schützt die Geschäftsprozesse Ihres Unternehmens in Übereinstimmung mit industriellen Sicherheitsstandards und -regulatorien und unterstützt die Implementierung des DevSecOps-Ansatzes.

Kaspersky Container Security bietet umfassenden Schutz vor selbst den komplexesten Cyberbedrohungen und automatisiert Ihre Compliance-Audits. Dadurch werden die Ressourcen Ihres Informationssicherheitsteams für andere Aufgaben freigesetzt und die Time-to-Market verkürzt.

Kaspersky Container Security wurde speziell für containerisierte Umgebungen entwickelt und bietet Schutz auf verschiedenen Ebenen, vom Container Image bis zum Host-Betriebssystem.

Lizenzierungsstufen

Zwei Schutzstufen:

Kaspersky Container Security

Standard

Bietet Schutz für Container Images, Integration mit Image Registries, Orchestratoren und CI/CD-Plattformen und verfolgt den Container-Status

Advanced

Sorgt für den Schutz von Containern in der Laufzeitumgebung, bietet erweiterte Überwachungsfunktionen und Tools für die Konformitätsprüfung

Funktionen und Lizenzierungsstufen

Funktionen	Standard	Advanced
Integration mit Container Image Registries Integriert mit Docker Hub, JFrog, Sonatype Nexus OSS, GitLab Registry, Harbor	●	●
Unterstützung der Orchestrierungsumgebung Unterstützt Kubernetes und OpenShift	●	●
Scannen von Images auf bösartige Objekte, Schwachstellen und Plaintext-Informationen Das Scannen kann manuell oder automatisch auf der Grundlage vordefinierter Parameter durchgeführt werden.	●	●
Risikobewertung für Container Images und Konfigurationsdateien (IaC) Automatisierte Image-Beurteilung auf der Grundlage von Kritikalitätsstufen	●	●
Scannen von Konfigurationsdateien (IaC) Erkennung von Konfigurationsfehlern und Überprüfung bewährter Verfahren	●	●
Kriteriensatz in der Benutzeroberfläche für die Erstellung benutzerdefinierter Richtlinien und die Bearbeitung voreingestellter Richtlinien Automatisierte Image-Beurteilung auf der Grundlage von Kritikalitätsstufen	●	●
Integration mit CI/CD-Plattformen und Scannen von Images und IaC im Entwicklungsstadium Integration mit Jenkins, Team City und Circle CI, um Images und Container zu blockieren, wenn Sicherheitsbedrohungen erkannt werden	●	●
Werkzeuge zur Visualisierung Visualisierung von Informationen über Images, Container und Infrastrukturelemente	●	●
Reporting-System Erstellung von Berichten und die Möglichkeit, diese bei Bedarf aus dem Protokoll herunterzuladen	●	●
Integration mit externen Sicherheits- und Reportingsystemen Integration mit SIEM (über Syslog), LDAP, E-Mail, Telegramm	●	●
Überwachung und Kontrolle des Starts von Containern in Übereinstimmung mit den Sicherheitsrichtlinien Das Produkt kann das Starten von nicht konformen Images, nicht registrierten Images und Images mit Privilegien verbieten sowie bestimmte Datenspeicher in Container einbinden.		●
Erkennen und Scannen von Container Images in einem Cluster Möglichkeit, Images zur Laufzeit zu scannen		●
Überwachung der Container-Integrität Überwachung der Konsistenz zwischen dem gescannten Image und dem Image, von dem der Container ausgeführt wird		●
Schutz vor Dateibedrohungen für laufende Container Prävention potenzieller Angriffe auf den Orchestrator über Container zur Laufzeit		●
Verhaltensanalyse von Containern (auf der Grundlage von Vorlagen) Überwachung von Containern auf der Grundlage des voreingestellten Profils		●
Kontrolliert den Start von Anwendungen und Diensten in Containern Erkennung und Blockierung verdächtiger Aktivitäten in Containern		●

Überwacht den Verkehr der laufenden Container

Erkennung und Blockierung verdächtiger Aktivitäten zwischen Containern innerhalb eines Clusters und zwischen Clustern

●

Analyse der Konfiguration von Komponenten der Container-Plattform für Best Practice-Verfahren und Richtlinienkonformität

Analyse der Infrastruktur im Hinblick auf die Einhaltung der CIS-Standards zur Verbesserung des Sicherheitsniveaus der Umgebung

●

Visualisierung von Ressourcen in einem Cluster

Anzeige wichtiger Informationen über den Status eines Clusters und seiner Komponenten

●

Kaspersky Container Security

Weitere Informationen

www.kaspersky.de

#kaspersky
#bringonthefuture