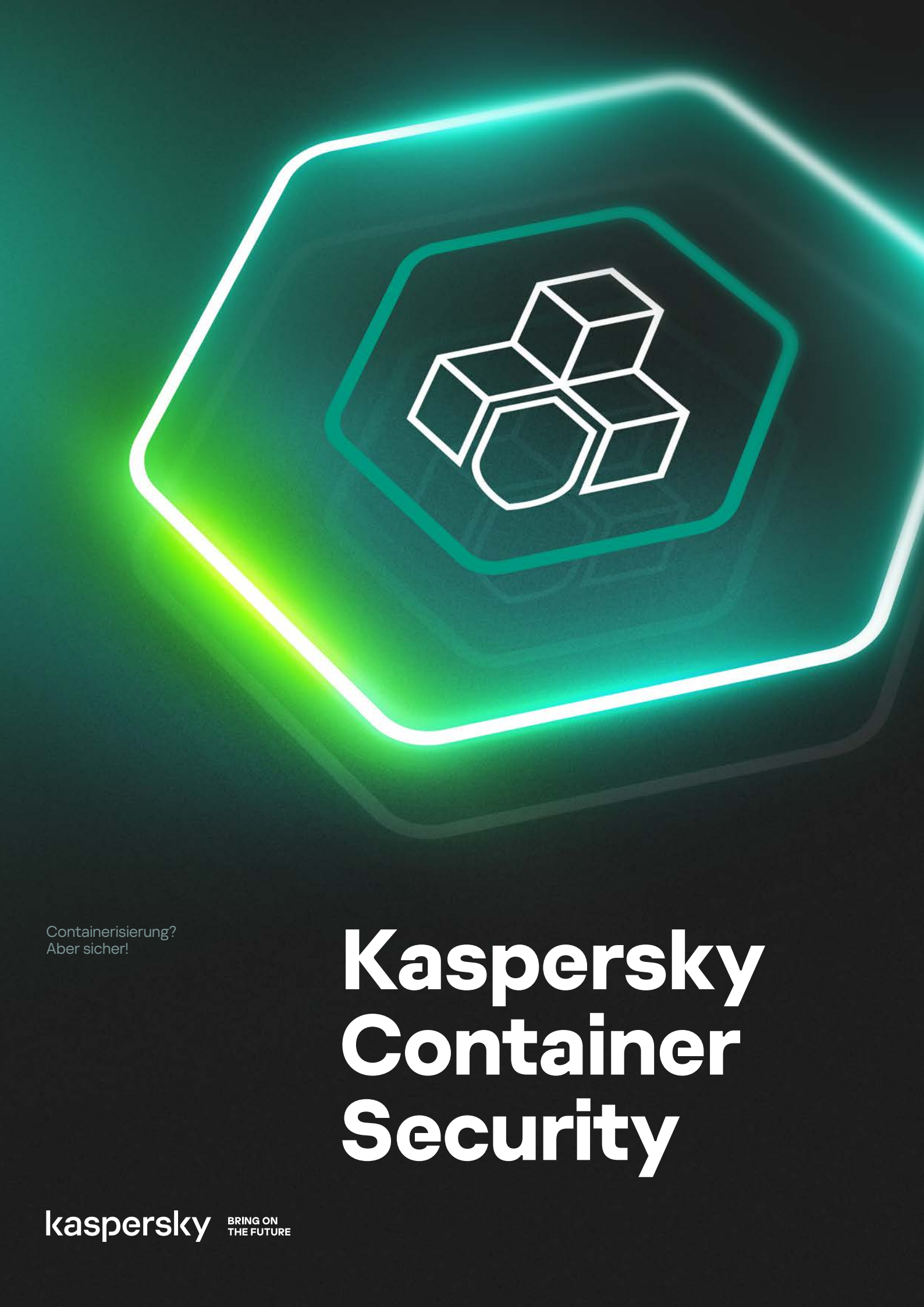


Containerisierung?
Aber sicher!

Kaspersky Container Security

kaspersky BRING ON THE FUTURE

Containerisierung

Die Containerisierung ist einer der wichtigsten globalen Trends in der Softwareentwicklung. Die Technologie ermöglicht es, den Prozess der Entwicklung und Bereitstellung von Apps zu beschleunigen. Herkömmliche Sicherheitslösungen sind jedoch nicht für die architektonischen Merkmale von Container-Umgebungen geeignet.

93%

der Unternehmen hatten in den letzten 12 Monaten mehr als einen Vorfall mit Kubernetes*.

55%

der Unternehmen haben ihre App-Veröffentlichungen aufgrund von Container-Sicherheitsproblemen verschoben*

31%

der Unternehmen haben in den letzten 12 Monaten aufgrund von Problemen mit der Container-Sicherheit Kunden und/oder Einnahmen verloren*

Schützt containerisierte Umgebungen zuverlässig und optimiert die Sicherheit der hybriden Infrastruktur Ihres Unternehmens

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 -vorschriften und unterstützt die Implementierung des DevSecOps-Ansatzes.

Kaspersky Container Security bietet umfassenden Schutz vor den neuesten 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.

Hauptfunktionen

Integration in den Entwicklungsprozess

- Integration mit Image Registries und CI/CD-Plattformen
- Integration mit Sicherheits- und Benachrichtigungssystemen

Orchestrator-Schutz

- Erzwingt zur Laufzeit die Sicherheit von Containern
- Integration mit Orchestrierungsplattformen
- Überwachung von Prozessen und Ereignissen im Cluster

Prüfung der Einhaltung von Rechtsvorschriften

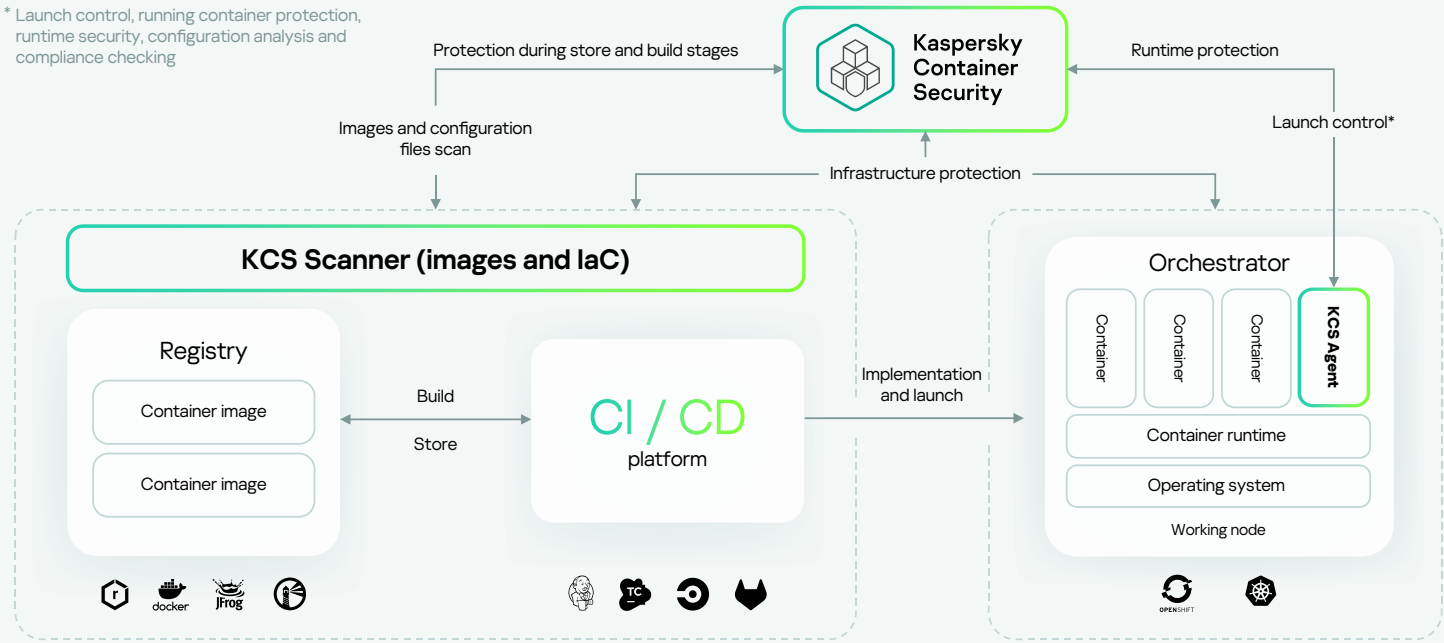
- Schwachstellenanalyse auf der Grundlage der NIST-Datenbank
- CIS-Benchmarks-Audit

Virtualisierung und Inventarisierung von Cluster-Ressourcen

- Vollständig angepasste Widgets zur Anzeige von Querschnittsdaten
- Transparente Inventarisierung der Ressourcen

*Quelle: RedHat 2022

Kaspersky Container Security: Architektur



Kaspersky Container Security (KCS) bietet Schutz in jeder Phase der Entwicklung und des Betriebs von Anwendungen. Die Lösung besteht aus drei Komponenten: KCS Agent, KCS Scanner und KCS Control Server.

KCS Agent

Erkennt Schwachstellen auf Container-, Cluster- und Orchestrator-Ebene und gewährleistet so die Laufzeit-Sicherheit. Wird als eigenständiger Container in den Cluster installiert.

KCS-Scanner für Images und Infrastruktur

Überprüft die Image Registry auf Relevanz und Sicherheit. Der Scanner prüft auch Images als Teil des CI-Prozesses und reduziert so die Risiken der Build-Phase. Wird zusammen mit den Serverkomponenten des Orchestrators im Cluster installiert.

KCS Control Server

Verantwortlich für die Überwachung des Status der Lösungskomponenten und der Interaktion zwischen ihnen sowie für die Zusammenstellung von Informationen über erkannte Ereignisse. Wird zusammen mit den Serverkomponenten des Orchestrators im Cluster installiert.

Integration in den Entwicklungsprozess

Registry und Versionskontrollsystem

Recherche

- Scannt IaC und Dockerfile auf Konfigurationsfehler und Plaintext-Informationen
- Überprüft Registry Images

CI-Werkzeuge

Entwurfs- und Testphase

- Scannt Images auf Schwachstellen, Malware und Plaintext-Informationen

Orchestrator

Ausführung

- Überwachung und Kontrolle des Starts von Containern in Übereinstimmung mit den Sicherheitsrichtlinien
- Verhaltensanalyse von Containern

CD-Werkzeuge

Lieferung und Bereitstellung

- Die Image-Lieferung wird kontrolliert und Sicherheitsrichtlinien werden eingehalten

Vorteile für Unternehmen

Weltweit anerkannte Sicherheit

Die Funktionen und Möglichkeiten von Kaspersky Container Security stehen im Einklang mit 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

Kaspersky Container Security

Weitere Informationen

www.kaspersky.de

#kaspersky
#bringonthefuture