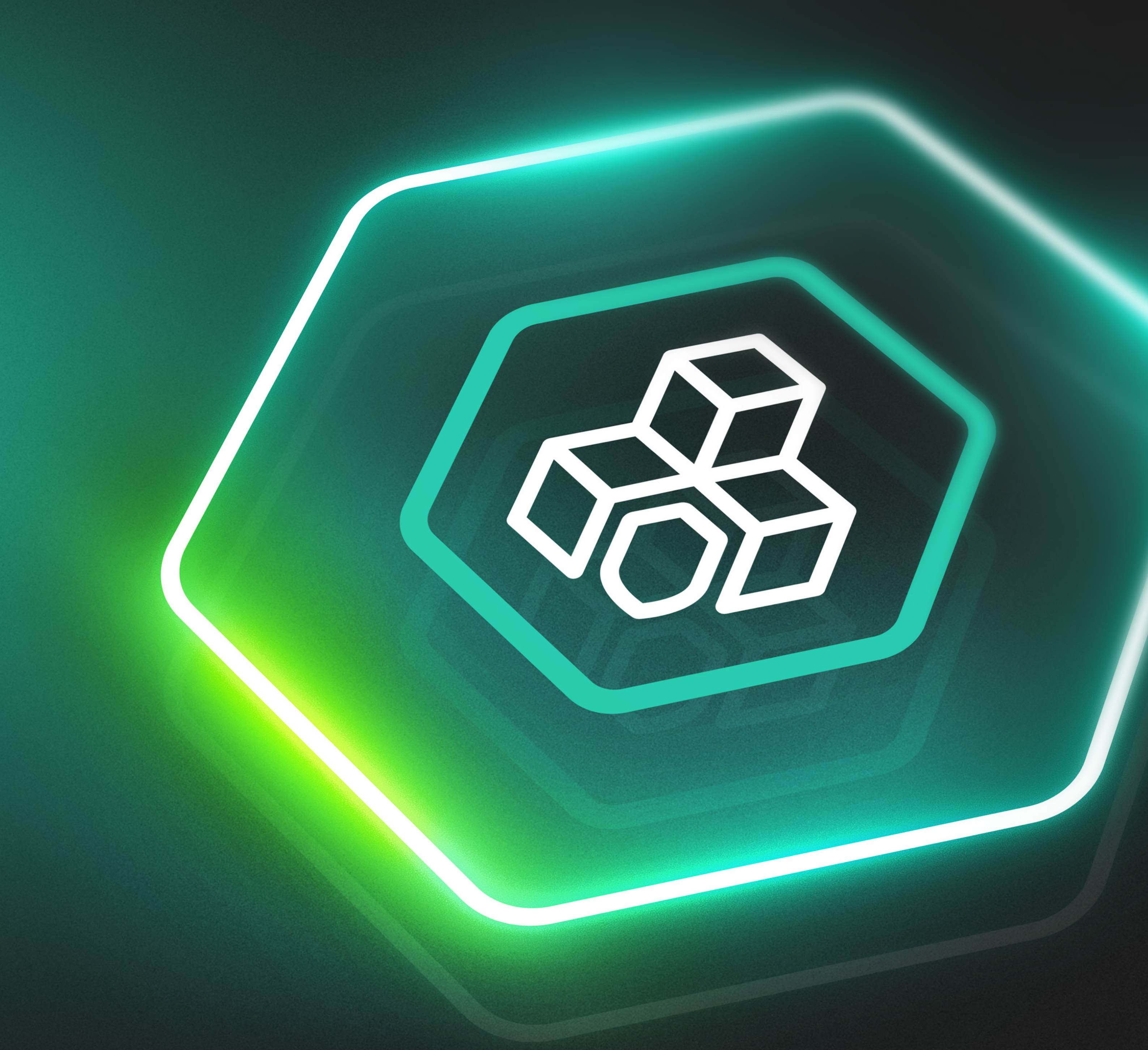


Scan. Secure. Speed up.

February '25

Kaspersky Container Security

Part of

Kaspersky Cloud Workload Security

kaspersky bring on the future

Containerization

Containerization is one of the primary global software development trends. The technology allows to accelerate the app design and delivery process. However, traditional security solutions aren't suitable for the architectural features of containerized environments.

Protecting containerized environments and enhancing your organization's hybrid infrastructure security

Kaspersky Container Security is a security solution that covers every stage of a containerized app's lifecycle, from development to operation. It protects your organization's business processes in line with security standards and regulations, and supports implementation of the DevSecOps approach.

Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats, and automates your compliance audits, freeing up the resources of your information security team to focus on other tasks, and shortening time to market.

Kaspersky Container Security has been developed both for on-premise and cloud container environments, ensuring multi-level protection, from container images to the host OS.

Kaspersky Continer Security is a part of the Kaspersky Cloud Workload Security offering. It provides comprehensive protection from attacks and reduces threat detection and response times in cloud environments.

85%

of companies suffered >1 incident in Kubernetes within the last 12 months*

39%

of companies reported a leak of confidential data due to container security issues*

38%

of companies lost revenue within the last 12 months due to container security issues*

Key capabilities

Integration into the development process

- Integration with image registries and CI/CD platforms
- Integration with security and notification systems

Orchestrator protection

- Enforces runtime container security
- Integration with orchestration platforms
- Monitoring processes and events in the cluster

Regulatory compliance audit

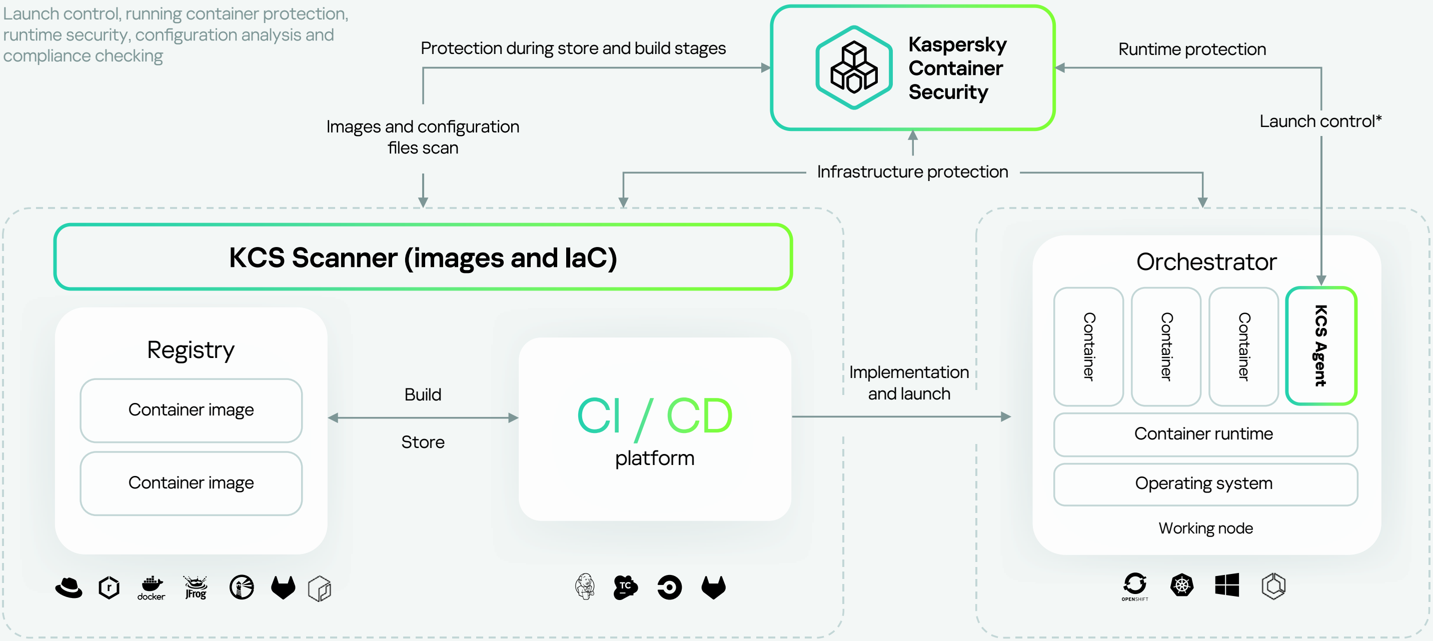
- Vulnerability analysis based on NIST and Kaspersky databases
- Best practices audits

Visualization and inventory of cluster resources

- Fully customized widgets to reveal cross-section data
- Transparent inventory of resources

* Source: Kaspersky. Managing Geo-Distributed businesses, 2024

Kaspersky Container Security architecture



* Launch control, running container protection, runtime security, configuration analysis and compliance checking

Kaspersky Container Security (KCS) enables protection at every stage of app design and operation. It consists of three components: KCS Agent, KCS Scanner and KCS Control Server.

KCS Agent

Detects vulnerabilities at container, cluster, and orchestrator levels, ensuring runtime security. Installs into the cluster as a stand-alone container on each node. The Agent can transmit cluster event logs directly into SIEM systems.

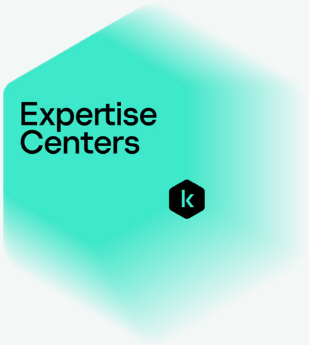
KCS Scanner of images and infrastructure

Checks the image registry for relevance and security. The scanner also checks images as part of the CI process, thus reducing the build stage risks. Installs into the cluster with the orchestrator's server components.

KCS Control Server

Responsible for monitoring the status of the solution components and interaction between them, as well as aggregation of information on detected events. Installs into the cluster with the orchestrator's server components.

Technology leadership based on world-class expertise



Kaspersky Container Security leverages the combined knowledge, technologies and refined skills of three of our five Centers of Expertise (GREAT, Threat Research, AI Technology Research, Security Services and ICS CERT).

These centers contribute considerably to the product through SSDLC & Secure-by-Design methodologies, vulnerability protection with a low false rate, and assistance for SOC-teams.

Advantages for business

Globally renowned security

Kaspersky Container Security's features and capabilities are in line with global best practices for container security.

Internationally recognized and award-winning protection.

Regulatory compliance

Best practices audits.

Transparent reporting system.

Easy operation — reliable protection

Real-time visualization of threats.

Reduces the necessity of involving the information security team while improving the quality and speed of security checks.

Comprehensive protection for containerized environments

Protection at different levels of the containerized environment architecture.

App security for every stage of the lifecycle.

Licensing tiers and objects

Kaspersky Container Security

Standard

Provides container image protection, integration with image registries, orchestrators, CI/CD platforms, and SIEM solutions.

Kaspersky Container Security

Advanced

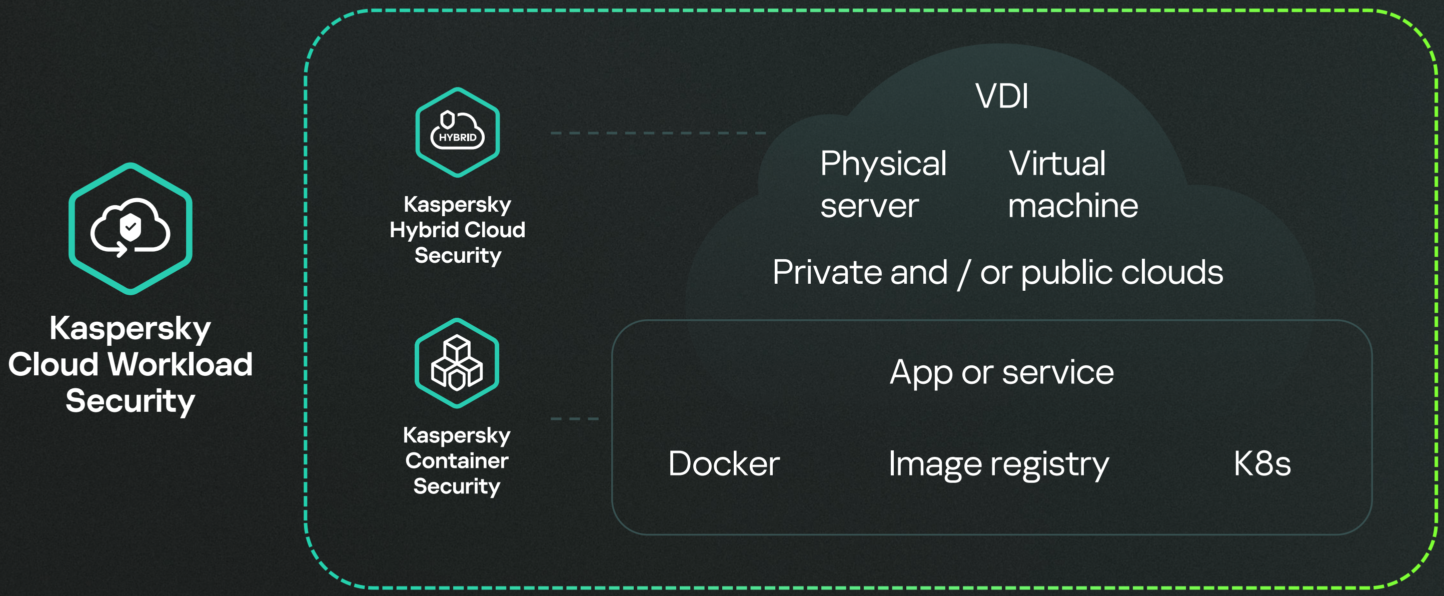
Ensures protection of containers in the runtime environment, provides enhanced monitoring capabilities and tools for compliance checks.

1 license = 1 node with containers*

* Quantity of nodes on which the KSC Agent is deployed are taken into account

Part of Kaspersky Cloud Workload Security

Kaspersky Container Security in combination with Kaspersky Hybrid Cloud Security forms a comprehensive cloud workload security offering for reliable, world-class protection from attacks together with shorter threat detection and response times in cloud environments. The Kaspersky Cloud Workload Security offering ensures comprehensive protection of your hybrid and cloud infrastructures: virtual machines / container clusters.


Kaspersky Cloud Workload Security
HYBRID
Kaspersky Hybrid Cloud Security
Kaspersky Container Security
VDI
Physical server
Virtual machine
Private and / or public clouds
App or service
Docker
Image registry
K8s

Cloud Security Posture Management (planned)

Supported solutions

Kaspersky Hybrid Cloud Security

Public clouds	Google Cloud aws Microsoft Azure
Private clouds	vmware AOS KVM Red Hat Enterprise Linux PROXMOX HUAWEI Microsoft Hyper-V
VDI platforms	vmware TERMIDESK citrix

Kaspersky Container Security

Orchestrators	kubernetes OPENSHIFT Amazon ECS
Image registries	dockerhub Red Hat Quay GitLab Amazon ECR HARBOR nexus repository JFrog
CI / CD platforms	Jenkins TeamCity GitLab circleci

Kaspersky Container Security

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture