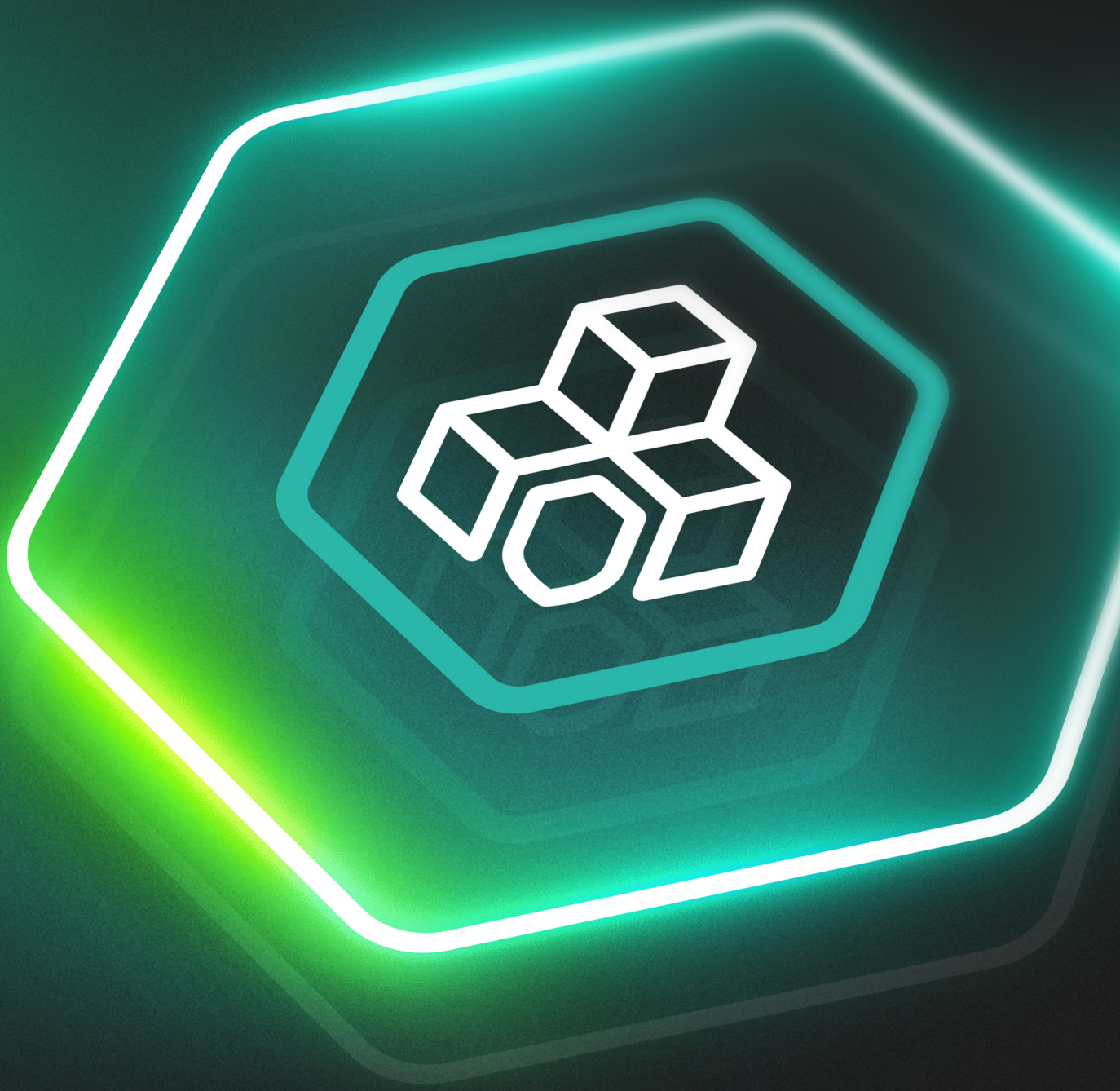


Scan. Secure. Speed up.

February '26

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 enables acceleration of 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-premises and cloud container environments, ensuring multi-level protection, from container images to the host OS.

Kaspersky Contiher Security is 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 more than one 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
- Protects cluster nodes as well as an orchestrator
- Monitoring processes and events in the cluster

Regulatory compliance audit

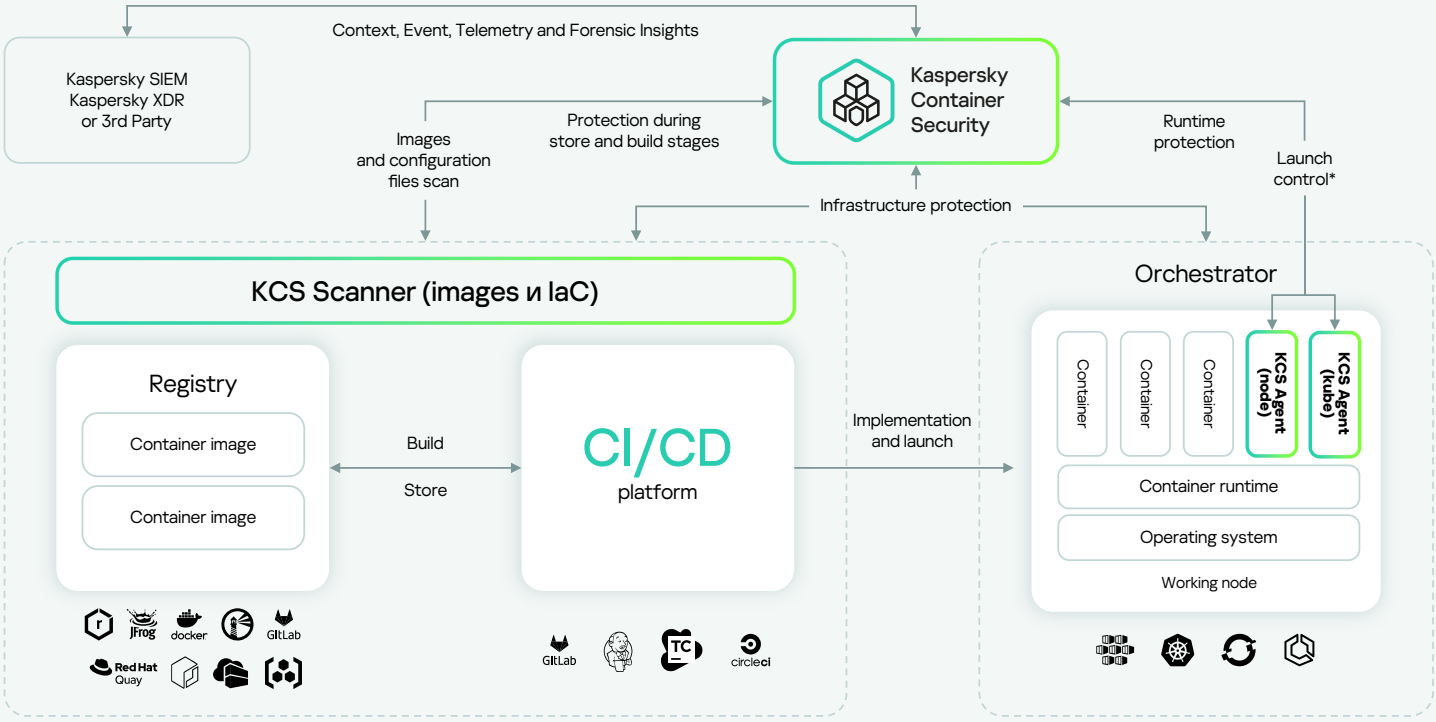
- Vulnerability analysis based on NIST's, Kaspersky's and customers' databases
- Best practice audits based on the most widely used security benchmarks, as well as customer-defined ones

Visualization and inventory of cluster resources

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

* Kaspersky. Managing Geo-Distributed Businesses, (Kaspersky, 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 four components: KCS Scanner, 2 KCS Agents and KCS Control Server.

KCS scanner

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 Node Agent

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

KCS Kube Agent

Detects vulnerabilities and file threats at orchestrator level ensuring host OS security. Installs into the cluster as a standalone container.

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.

MITRE ATT&CK Containers Matrix coverage

Kaspersky continuously improves its security practices and actively contributes to global security initiatives. One of these is the MITRE ATT&CK knowledge base of adversary tactics and techniques based on real-world observations.

Explore how Kaspersky Container Security covers key malicious techniques targeting container infrastructure and containerized applications

Learn more

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.

Customers' threat databases usage.

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.

Kaspersky Container Security
Advanced Pro

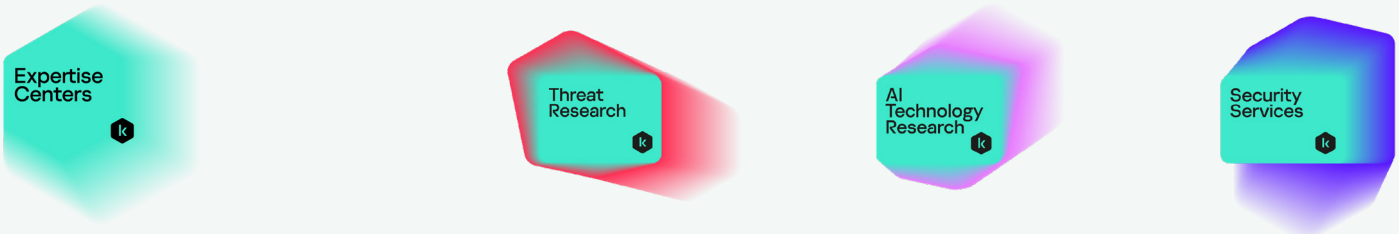
Improves product usability and agility with AI-based descriptions of scanned container images and customized security benchmarks.

1 license = 1 node with containers*

1 license = 1 node
with containers and
5100 tokens per node per day

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

Technology leadership based on world-class expertise

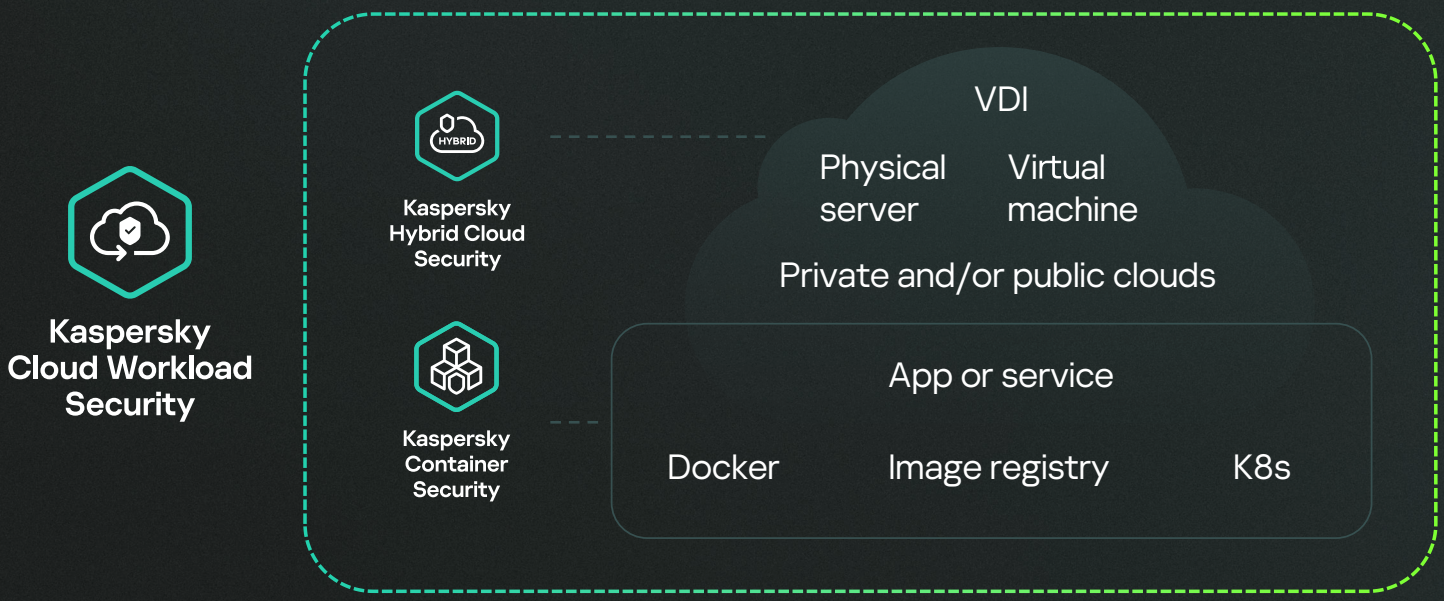


Kaspersky Container Security leverages the combined knowledge, technologies and refined skills of three of our five Centers of Expertise (Threat Research, AI Technology Research, Security Services).

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

Part of Kaspersky Cloud Workload Security

Kaspersky Container Security in combination with Kaspersky Hybrid Cloud Security forms 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.



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 · Azure Kubernetes Service

Image registries

dockerhub · Red Hat Quay · GitLab · Amazon ECR · JFrog · HARBOR · nexus repository

CI/CD platforms

Jenkins · TeamCity · GitLab · circleci

Kaspersky Container Security

Learn more

www.kaspersky.com

© 2025 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#bringonthefuture