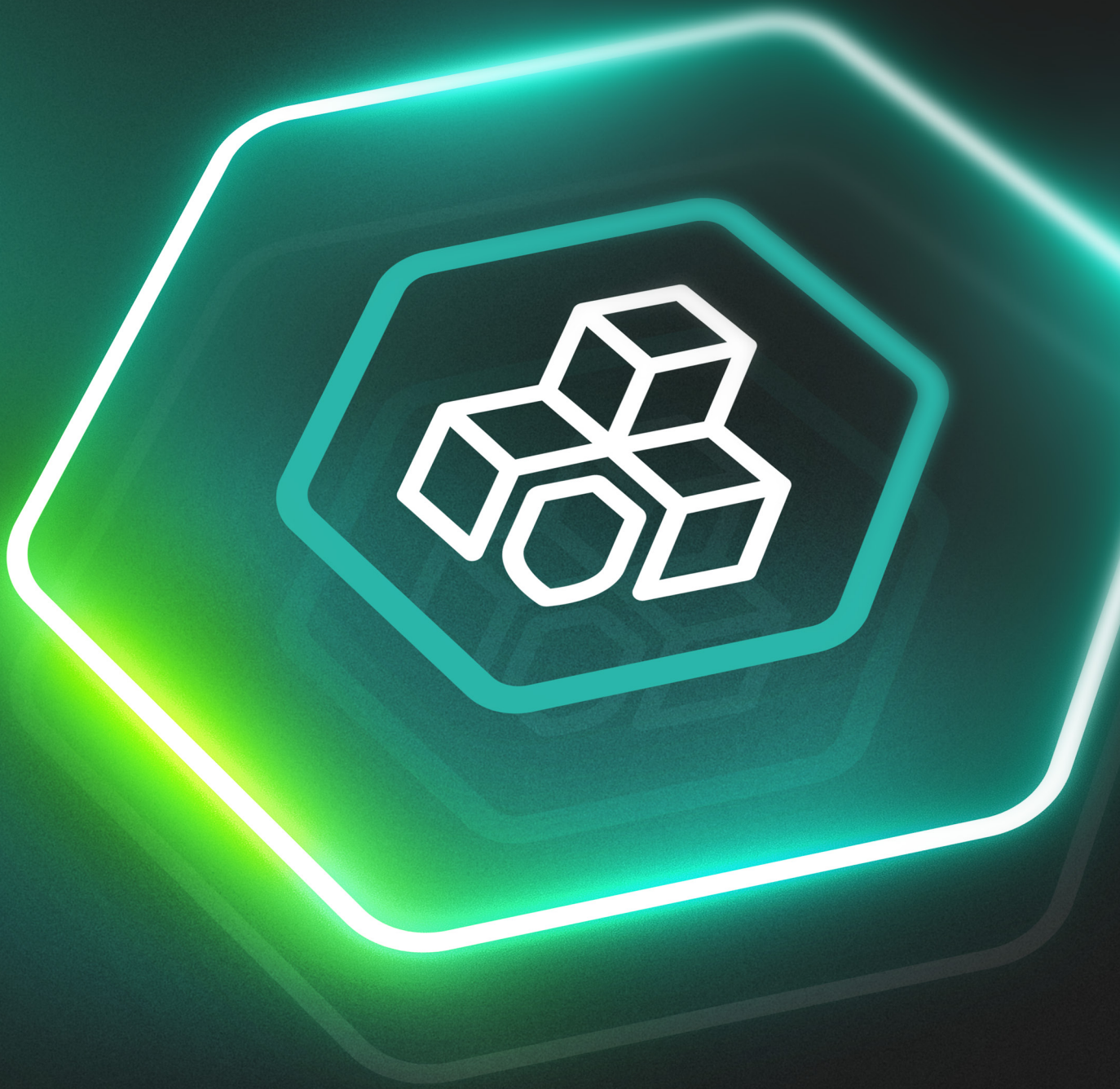


Licensing Guide
February '25

Kaspersky Container Security

kaspersky bring on the future

Part of

Kaspersky Cloud Workload Security

Containerization

is one of the primary global software development trends right now. Most companies globally use containers in their apps. The technology shortens time to market, enables more rational use of computer resources, and delivers robust and well-built apps to customers. However, the architectural features of containerized apps prevent traditional and open-source solutions designed for code analysis and endpoint protection from providing adequate information security.

Kaspersky Container Security

Kaspersky Container Security protects 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 DevSecOps.

Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats. It automates your compliance audits, freeing up your security team's resources so they can focus on other tasks, and shortens 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 Contiher 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.

Licensing levels

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

Features and licensing tiers

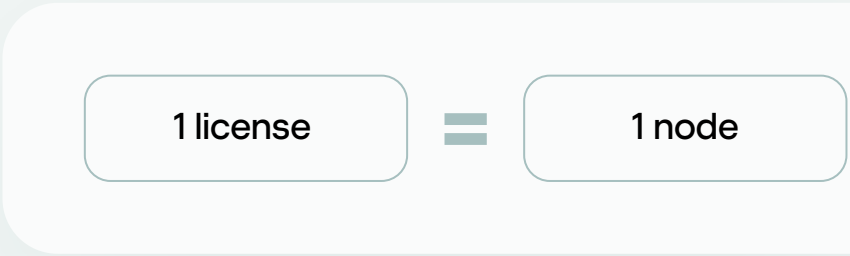
Features	Standard	Advanced
Integration with container image registries Integrates with Docker Hub, JFrog Artifactory, Sonatype Nexus OSS, GitLab Registry, VMWare Harbor, Red Hat Quay, Amazon ECR	●	●
Orchestration environment support Supports Kubernetes, Red Hat Openshift, Azure AKS, Amazon ECS	●	●
Integration with public clouds Supports AWS and Microsoft Azure	●	●
Scanning of images for malicious objects, vulnerabilities and secrets Scanning can be performed manually or automatically based on predefined parameters	●	●
Risk assessment for container images and configuration files (IaC) Automated image assessment based on criticality levels	●	●
Scanning of configuration files (IaC) Configuration error detection and best practice checks	●	●
Set of criteria in UI for creating custom policies and editing preset policies Enables creation of policies for image security scanning, response, and runtime analysis	●	●
Integration with CI/CD platforms and scanning of images and IaC at development stage Integrates with Jenkins, Team City and Circle CI to block images and containers when security threats are detected	●	●
Visualization tools Visualization of information about images, containers, and infrastructure elements	●	●
Reporting system Generation of reports and ability to download them from the log on demand	●	●
Integration with external security and notification systems Integration with SIEM (via syslog), LDAP, e-mail, Telegram	●	●
Open API for key product functionality (Swagger) Integration and installation convenience improvement	●	●
Analysis of the configuration of container platform components for compliance with best practices Infrastructure analysis for compliance with best protection practices to improve the environment's security level	●	●
Orchestrator vulnerability analysis Checks clusters for compliance with security policies and the cluster health as well as Kubernetes components	●	●

Container launch monitoring and control in accordance with security policies Product can prohibit launch of non-compliant images, unregistered images, and images with privileges, as well as mount specific datastores in containers.	●
Detecting and scanning images in a cluster Ability to scan images at runtime	●
Behavioral analytics of containers (based on templates) Monitoring containers based on the preset profile (automatically and manually)	●
Container integrity monitoring Monitoring consistency between scanned image and image from which container is running	●
File threat protection for running containers (eBPF and KESL -based) Preventing potential attacks on orchestrator via containers in runtime	●
Controls the launch of applications and services inside containers Detecting and blocking suspicious activity inside containers	●
Monitors the traffic of running containers Detecting and blocking suspicious activity between containers in cluster and between clusters	●
File operation monitoring (eBPF) Detects file changes (e.g. rights and owner changes, creation, modifications, save history, etc.)	●
Logs host syscalls Improves forensics on events that occurred in the system before and following a policy violation	●
Event log transmission directly from monitored clusters to SIEM systems Helps SOC teams when investigating complex incidents	●
Dedicated vulnerability page Facilitates focusing on specific vulnerabilities across the entire container environment	●
Container platform component configuration analysis for regulatory compliance Infrastructure analysis for compliance with internal and / or external security requirements	●
Visualization of resources in a cluster View key information about the state of a cluster and its components	●

Licensing objects

Nodes with containers

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



Premium technical support

Kaspersky Premium support is provided within Kaspersky Maintenance Service Agreement (MSA) and focused on superior user experience with high class priority maintenance. For Kaspersky Container Security you may choose out of two support options: MSA Business for KCS or MSA Enterprise for KCS.

	MSA Business for KCS	MSA Enterprise for KCS
Request receiving availability	Criticality level 1 — on 24×7, the rest — standard office hours of the Kaspersky Local Office	Criticality level 1 and 2 — on 24×7, the rest — standard office hours of the Kaspersky Local Office
Response time	Criticality level 1 — 2 hours* Criticality level 2 — 6 business hours Criticality level 3 — 8 business hours Criticality level 4 — 10 business hours	Criticality level 1 — 30 minutes* Criticality level 2 — 4 hours* Criticality level 3 — 6 business hours Criticality level 4 — 8 business hours
Contact persons	4 — the possible number of contact persons from the customer's side	8 — the possible number of contact persons from the customer's side Dedicated Technical Account Manager (TAM) Provides reports to the customer on open incidents

Note: Please check availability of MSA contracts and all terms and conditions in your country with your account manager

* Outside of business hours, additional contact by phone is required

License calculation examples

Scenario A	Scenario B
The customer needs to secure container images ONLY	The customer needs to secure not only container images, but also runtime apps, and they also want to check their compliance
For example, in both cases the customer has a total of 810 nodes deployed in infrastructure. On 500 nodes from total amount deployment of containers is planned. Despite the customer purposes described in scenarios A and B we should consider only nodes on which containers are deployed where 1 node count as a 1 license. 500 nodes = 500 licenses	
500 licenses Kaspersky Container Security Standard	500 licenses Kaspersky Container Security Advanced

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

Comprehensive protection for containerized environments

- Protection at different levels of the containerized environment architecture
- App security for every stage of the lifecycle

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

Regulatory compliance

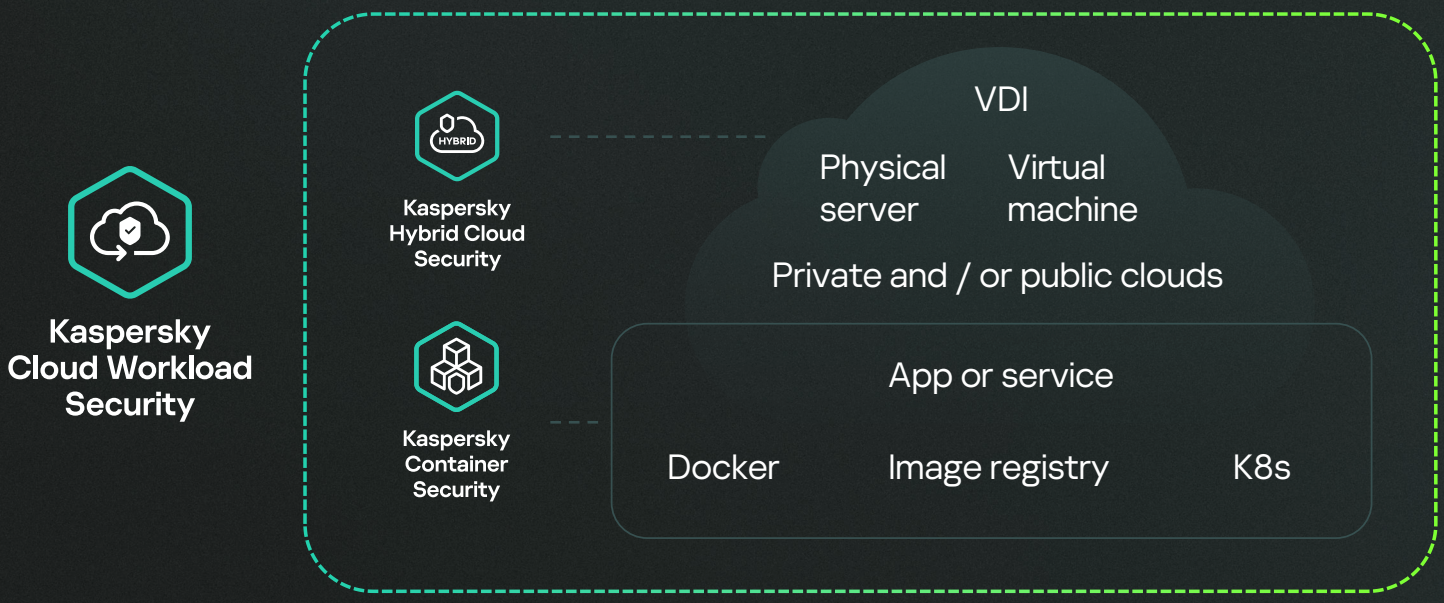
- Best practices audits
- Transparent reporting system

Technology leadership based on world-class expertise

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



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