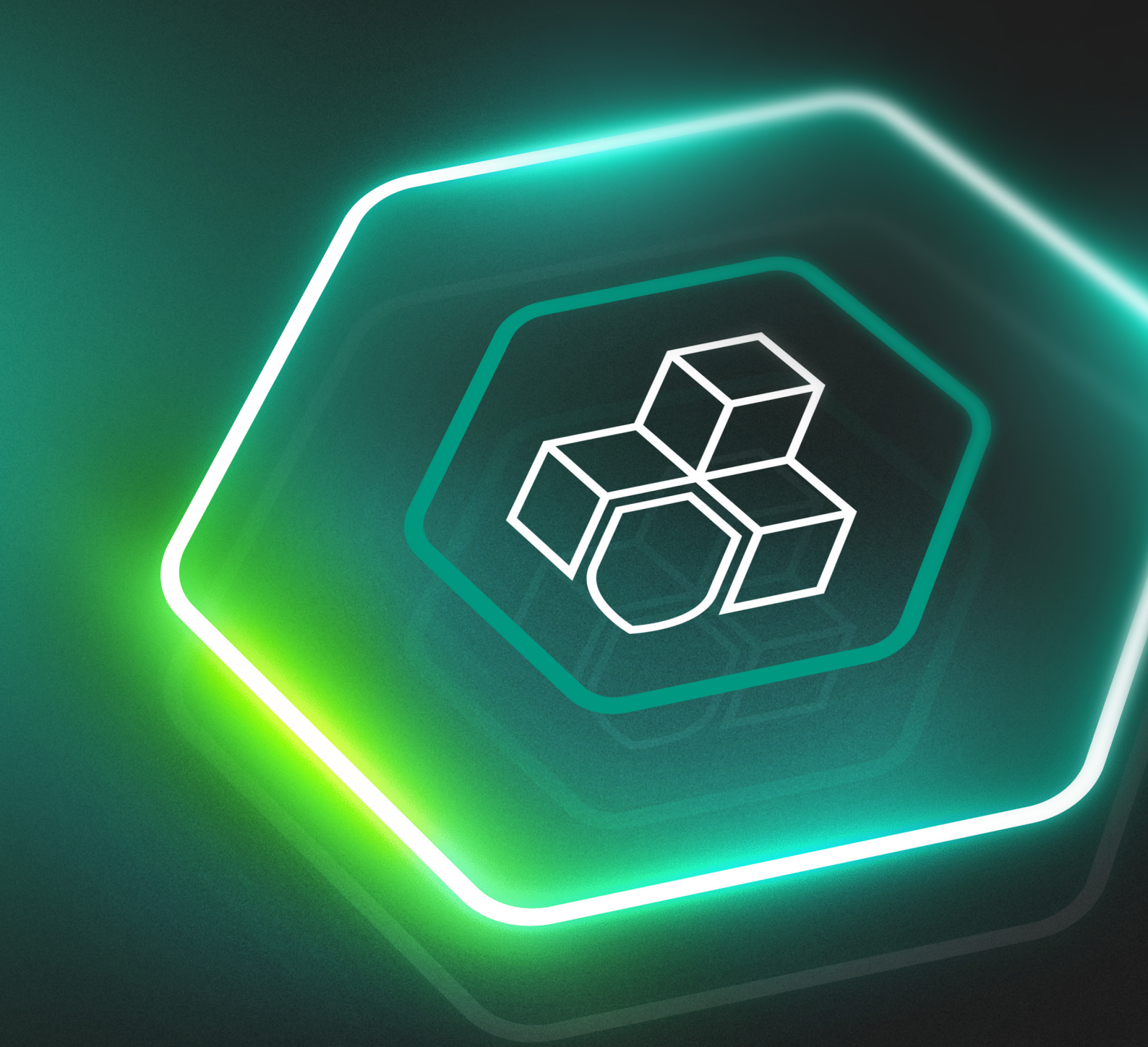

Feature list

Kaspersky Container Security

kaspersky BRING ON THE FUTURE

October 23

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

- CIS benchmarks audits
- Transparent reporting system

Introduction

Kaspersky Container Security (KCS) 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 specifically for containerized environments, ensuring protection at different levels from container image to host OS.

Licensing levels

Two protection levels:

Kaspersky Container Security

Standard

Provides container image protection, integration with image registries, orchestrators, CI/CD platforms, and tracks container status

Advanced

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

Features and licensing levels

Features	Standard	Advanced
Integration with container image registries Integrates with Docker Hub, JFrog, Sonatype Nexus OSS, GitLab Registry, Harbor	●	●
Orchestration environment support Supports Kubernetes and OpenShift	●	●
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 Automated image assessment based on criticality levels	●	●
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	●	●
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		●

Container integrity monitoring Monitoring consistency between scanned image and image from which container is running	●
Behavioral analytics of containers (based on templates) Monitoring containers based on the preset profile	●
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	●
Container platform component configuration analysis for best practice and regulatory compliance Infrastructure analysis for compliance with CIS standards to improve environment security level	●
Visualization of resources in a cluster View key information about the state of a cluster and its components	●

Kaspersky Container Security

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture