



Kaspersky
Cloud Workload
Security

October' 24

Kaspersky Cloud Workload Security

kaspersky bring on
the future

Cloud migration overview

>90%

of organizations use some type of cloud*

84%

of organizations use containers in different environments**

72%

of respondents use hybrid clouds***



According to Frost & Sullivan, the CWS market will increase from \$3-billion in 2022 to \$9,8-billion in 2027, with a CAGR of 26,3%.



Speeds up processes



Reduces costs



Improves performance



Brings new risks

Cloud migration and the adoption of containerization technologies have become key components of success for businesses of every type, even those in highly regulated and closed industries. But the more workloads that are transferred to the cloud, the more complex and less controlled and transparent a cloud infrastructure becomes. This rapid transfer has brought new risks, as security doesn't always keep up with business transformation.

To provide better protection for business-critical services, enterprise-level companies tend to adopt a hybrid cloud approach with different mixes of on-premise and private / public cloud infrastructures.

But even in hybrid cloud environments, traditional security solutions, mostly based on endpoint protection, tend to become ineffective, due to the specifics of the cloud environment. These infrastructures need to work in combination with cloud workload security solutions to fully protect modern IT infrastructures.

Sail on through cloud obstacles

Kaspersky Cloud Workload Security (Kaspersky CWS) is a solution of comprehensive protection for hybrid cloud and DevOps infrastructures. It protects from the broadest range of cloud security risks, from malware and phishing to vulnerable containers in runtime.

Kaspersky CWS protects:

- hosts
- virtual machines
- other components of hybrid cloud and container environment
- containers
- orchestrators

The solution offers flexible licensing and easily integrates into your existing IT landscape. Kaspersky CWS is the ideal fit for companies with diverse and complex IT infrastructure.

* AAG. The Latest Cloud Computing Statistics, 2023

** CNCF. Annual Survey, 2024

*** Flexera. State of the Cloud Report, 2023

Kaspersky CWS benefits your entire organization



Business

- Saves on costs
- Reduces risks
- Speeds up business processes
- Boosts efficiency



IS department

- Secures cloud workloads and apps / services
- Enhances all-round visibility
- Risk management
- Supports regulatory compliance



IT department

- Optimizes hybrid cloud computing resources
- Improves infrastructure performance
- Provides visibility across your infrastructure
- Reduces IT incidents



Development department

- Enables faster time-to-market
- Provides transparent inventory of resources
- Saves time with automation
- Increases the reliability of apps and services

Key features



Protection you can rely on from a top-tier vendor

Kaspersky CWS provides the highest safety level standards and offers top quality “one-stop shop” technical support. It integrates with other Kaspersky solutions, so we could cover your cybersecurity risks the best way possible



Specifically designed to address cloud workload security risks

Multi-layered threat protection proactively fights the broadest range of cyber risks from malware and phishing to rogue containers in runtime



Smooth cloud migration with cost-efficient out-of-the-box security

Choose only the capabilities you need to protect all your workloads – physical, virtualized or containerized, regardless of where they’re deployed (private, public, or hybrid clouds)



A resource-saving cloud security solution for complex infrastructures

State-of-the-art technology saves up to 30% of virtualization hardware resources on protection in private clouds, and avoids degradation of cluster performance



Better, faster security checks

Kaspersky CWS helps to forecast time-to-market by automating information security compliance checks



Compliance-ready multi-environmental security

Kaspersky CWS supports ongoing regulatory compliance for cloud infrastructures, including best practices audits and self-scanning

Solution components

Kaspersky CWS consists of Kaspersky Hybrid Cloud Security and Kaspersky Container Security, with Cloud Security Posture Management (CSPM) functions to be added in the future.



**Kaspersky
Hybrid Cloud
Security**

Kaspersky Hybrid Cloud Security secures entire hybrid infrastructure fighting the broadest range of cyberattacks while going easy on your resources. Key capabilities:

- Multi-layered hybrid cloud threat protection
- System hardening that boosts resilience
- Extensive regulatory compliance toolbox
- Borderless visibility



**Kaspersky
Container
Security**

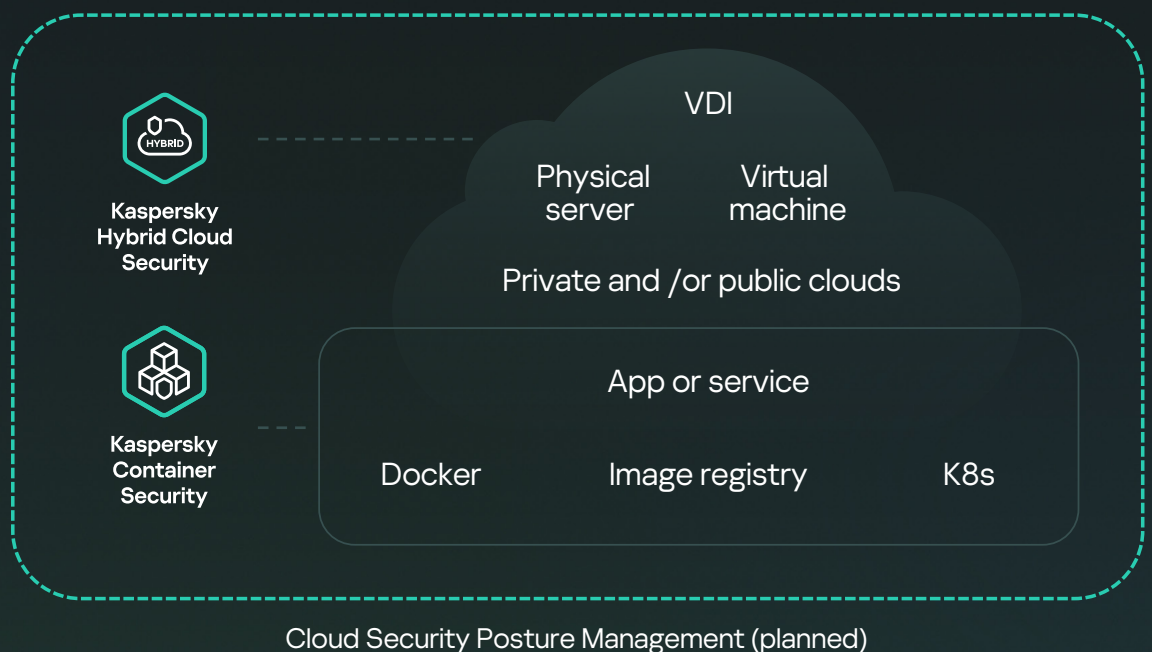
Kaspersky Container Security detects security issues at every stage of the containerized app lifecycle, from development to operation. Key capabilities:

- Integration into the development process
- Orchestrator protection
- Regulatory compliance audit
- Visualization and inventory of cluster resources

How it works



**Kaspersky
Cloud Workload
Security**



Supported solutions



**Kaspersky
Hybrid Cloud
Security**



**Kaspersky
Container
Security**

Public clouds

AWS, Microsoft Azure, Google Cloud with the ability to integrate with smaller local public clouds and / or MSP providers



Google Cloud



**Microsoft
Azure**



aws

Orchestrators

Kubernetes, OpenShift



kubernetes



OPENSIFT

Private clouds

Based on VMware, KVM, RHEL and others



vmware



**Red Hat
Enterprise Linux**

KVM

Image registries

Docker hub, Harbor, jFrog, Nexus



dockerhub



HARBOR



JFrog



**nexus
repository**

VDI platforms

VMware Horizon, Termidesk VDI, Citrix Virtual Apps and Desktops



vmware



TERMIDESK

citrix

CI / CD platforms

Jenkins, TeamCity, GitLab, CircleCI

Jenkins



TeamCity



GitLab



circleci

Licensing

The Kaspersky Cloud Workload Security solution combines two products with separate licenses. This offers unique flexibility and allows you to adjust the solution to yourspecific tasks.



Kaspersky Hybrid Cloud Security

Standard

Fundamental hybrid cloud security



Kaspersky Hybrid Cloud Security

Enterprise

Standard + Comprehensive hybrid cloud security with regulatory compliance support



Kaspersky Container Security

Standard

Container image security



Kaspersky Container Security

Advanced

Standard + Runtime security and regulatory compliance

Example

		 Kaspersky Hybrid Cloud Security		 Kaspersky Container Security	
Use cases		Standard	Enterprise	Standard	Advanced
Option 1	Basic VM security	•	•		
	Container image security			•	•
Option 2	Basic VM security	•	•		
	Container runtime security				•
Option 3	Advanced VM security		•		
	Container image security			•	•
Option 4	Advanced VM security		•		
	Container runtime security				•

Advantages for business



Cost saving

- Choose only the capabilities you need
- Resource-saving features and technologies



Reduced risks

- Rich protection functionality for multicloud and container infrastructures
- Regulatory compliance for cloud and DevOps



Faster business processes

- Automation of security checks
- Predictable time-to-market



Improved efficiency

- Shift-left approach
- 360° overview in hybrid cloud and Kubernetes

Why Kaspersky:



Top-tier vendor



Proven technology efficiency



Transparency and compliance with standards



World-class experience and expertise



Most tested, most awarded vendor



>25 years of excellence



Kaspersky Cloud Workload Security

[Learn more](#)

www.kaspersky.com

© 2024 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

[#kaspersky](#)
[#bringonthefuture](#)