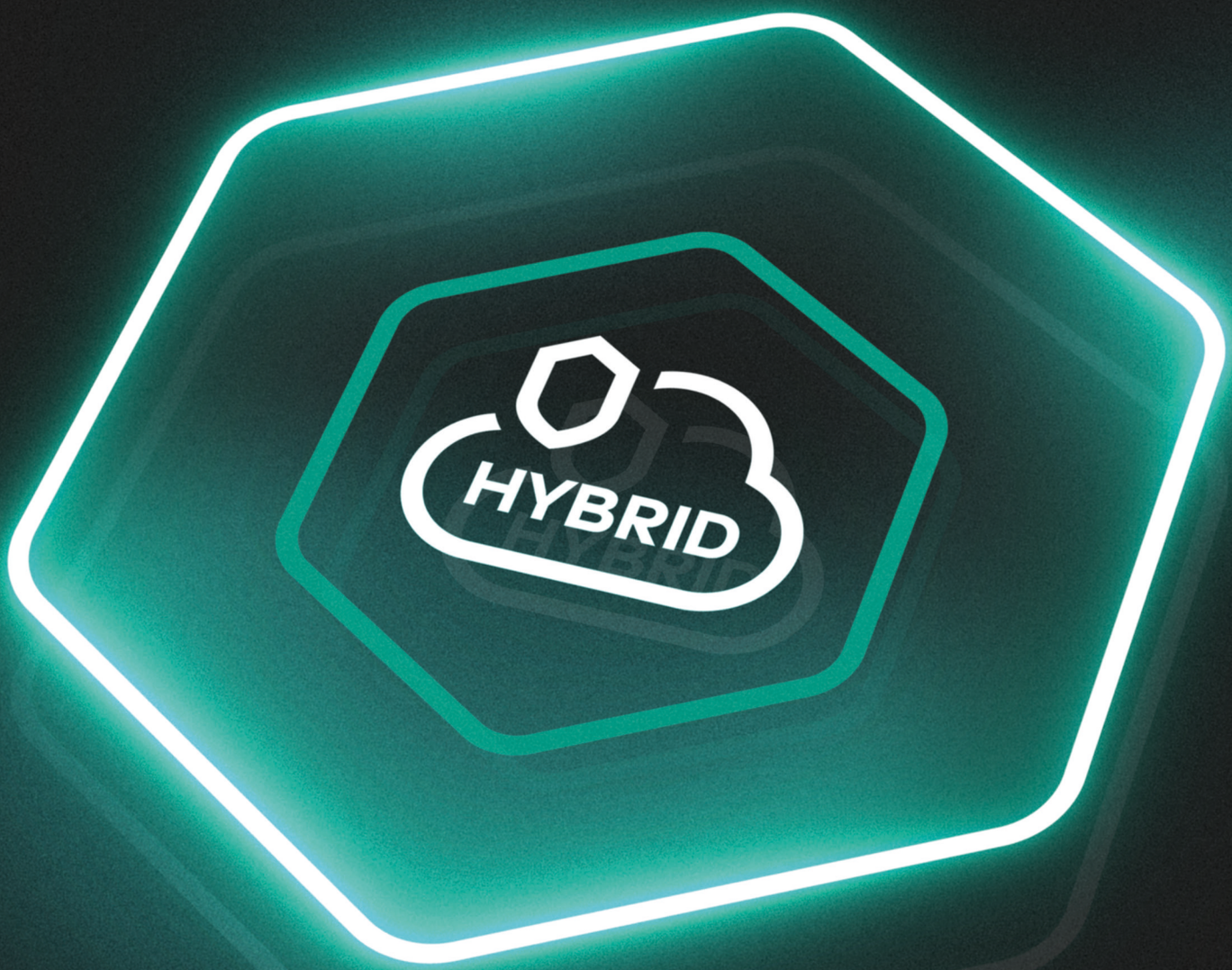
Kaspersky Hybrid Cloud Security



September '25

Part of

Kaspersky Cloud Workload Security

kaspersky bring on the future

Overview

>90%

of organizations use some type of cloud*

72%

of respondents use hybrid clouds*

79%

of respondents say security is a top challenge*

It used to be that an on-premise infrastructure with endpoints and physical servers was the only option. But those days are long gone, and today, cloud computing has become commonplace and most companies use hybrid cloud installations — a mix of on-premise and cloud (public or private) environments.

The cloud benefits companies in numerous ways, including greater agility and flexibility. But there are downsides, such as the sudden growth in infrastructure complexity, costs and performance inefficiency.

When it comes to cloud protection, traditional endpoint security solutions tend to become ineffective, as they don't address all the specifics of cloud and virtualized environments, e.g. the cloud's scalability by demand, deployment of multiple workloads from a single template (golden image), and others.

Kaspersky Hybrid Cloud Security addresses security and infrastructure inefficiency challenges.

Proven cloud-agnostic protection and the best performance for your hybrid environments

Kaspersky Hybrid Cloud Security makes cloud adoption, digital transformation, and doing business in general safer and more efficient.

- Secures hybrid infrastructures
- Mitigates risks
- Supports regulatory compliance
- Increases visibility
- Saves virtualization resources
- Saves labor hours
- Reduces costs
- Simplifies management

With Kaspersky Hybrid Cloud Security, cloud protection becomes one less thing to worry about — leaving you free to focus on other aspects of your digital transformation journey.

* Flexera. State of the Cloud Report, 2023

Product value

Best-of-breed protection designed to address hybrid environment security risks

Multi-layered threat protection proactively fights the broadest range of cyberattacks, including malware, phishing, and more.

Machine learning algorithms powered by human expertise deliver the highest detection levels with minimal false positives.

Real-time threat intelligence data helps defend against the latest exploits.

A cloud-agnostic approach for the best hybrid infrastructure security performance

The cybersecurity engine protects the entire hybrid infrastructure, whatever the workload — physical, virtualized, or based in private, public, and hybrid clouds.

Light agents optimized for each OS efficiently reduce consumption of virtualization resources by up to 40% in private clouds, freeing them up for use in other areas of the business.

Cost-efficiency and convenient management for a comfortable cloud journey

A flexible licensing model means you choose only the capabilities you need, and get maximum value from your security investment.

A unified console makes the security management of your cloud infrastructure (public, private, hybrid or multicloud) simpler, saving on valuable IT staff resources.

Straightforward cloud infrastructure inventory and automated security provisioning, regardless of the agents' location, contribute to maximum visibility.

Compliance-ready security for highly-regulated industries

Adaptive and multi-faceted, the product is designed to enable and continuously support regulatory compliance, through technologies ranging from system hardening and agent self-defense to vulnerability assessment and automated patch management.

Features

Multi-layered threat protection

- Global Threat Intelligence
- Machine Learning
- Web and Mail Threat Protection
- Log Inspection
- Behavior Analysis
- Remediation Engine
- Exploit Prevention
- Anti-Ransomware Functionality
- Network Threat Protection

System hardening that boosts resilience

- Application Control
- Device Control
- Vulnerability Assessment and Patch Management
- Host-based Intrusion Prevention System (HIPS)
- File Integrity Monitoring
- Web Control

Borderless visibility

- Unified Security Management
- Cloud API
- Flexible Management Options
- SIEM Integration

One product. One console. One license

Kaspersky Hybrid Cloud Security features a unique unified console — Kaspersky Security Center. It allows you to manage the entire infrastructure from one window. Don`t waste your valuable labor hours switching between screens.

Advantages for business

Reduced risks

- Platform-agnostic protection
- State-of-the-art security technologies

Cost efficient

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

Unified console

- 360° overview in multicloud
- Time and labor optimization

Compliance-ready security

- Continuous regulatory compliance support, even in highly-regulated industries
- A wide range of features

Customer reviews*

This solution helps to protect virtual and cloud environments, without affecting system performance or disrupting user experience.

Centralized cloud solution for data protection. All in one place.

Protection applies instantly to all VMs, because you don't need to download new updates at all.

Great way to combine all the security solutions in one license.

No need to install additional anti-virus software and other agents.

The optimal solution that does not require long administrator training.

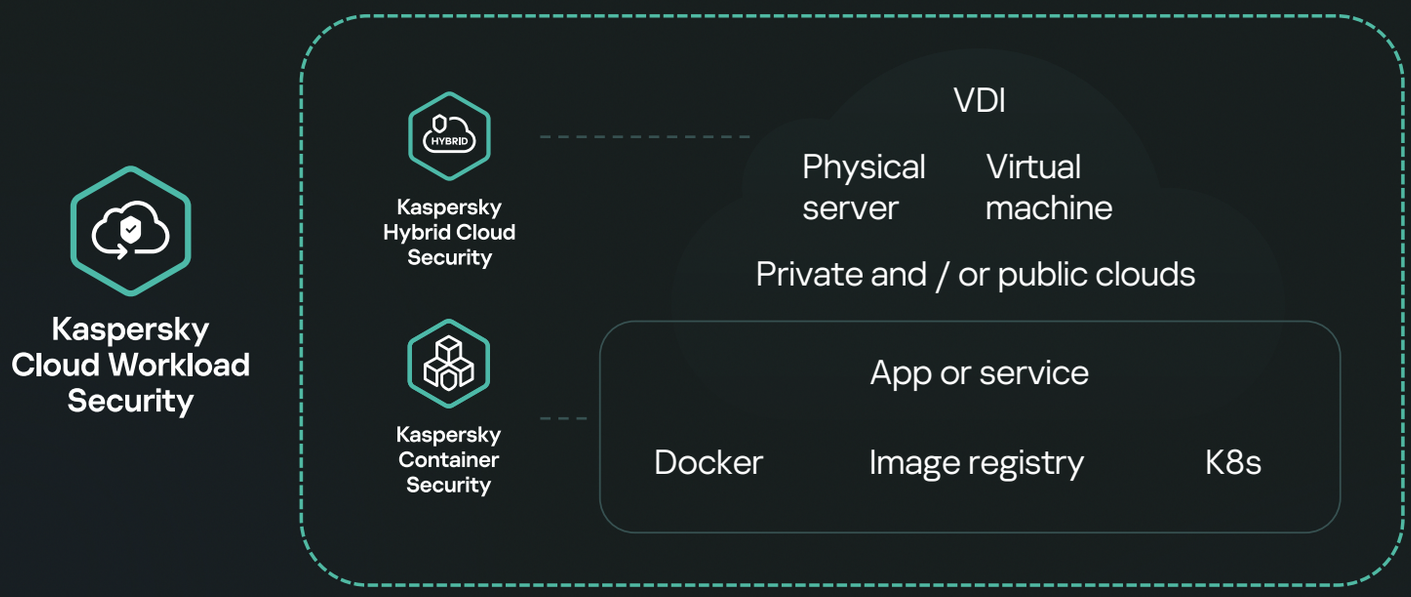
Technology leadership based on world-class expertise

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.

* Taken from public sources

Part of Kaspersky Cloud Workload Security

Kaspersky Hybrid Cloud Security in combination with Kaspersky Container Security forms a 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, Red Hat Enterprise Linux, PROXMOX, HUAWEI, Microsoft Hyper-V, KVM

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, HARBOR, nexus repository, JFrog, Azure Registry, Google Container Registry

CI / CD platforms

Jenkins, TeamCity, GitLab, circleci

Kaspersky Hybrid Cloud Security

www.kaspersky.com

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

#kaspersky
#bringonthefuture