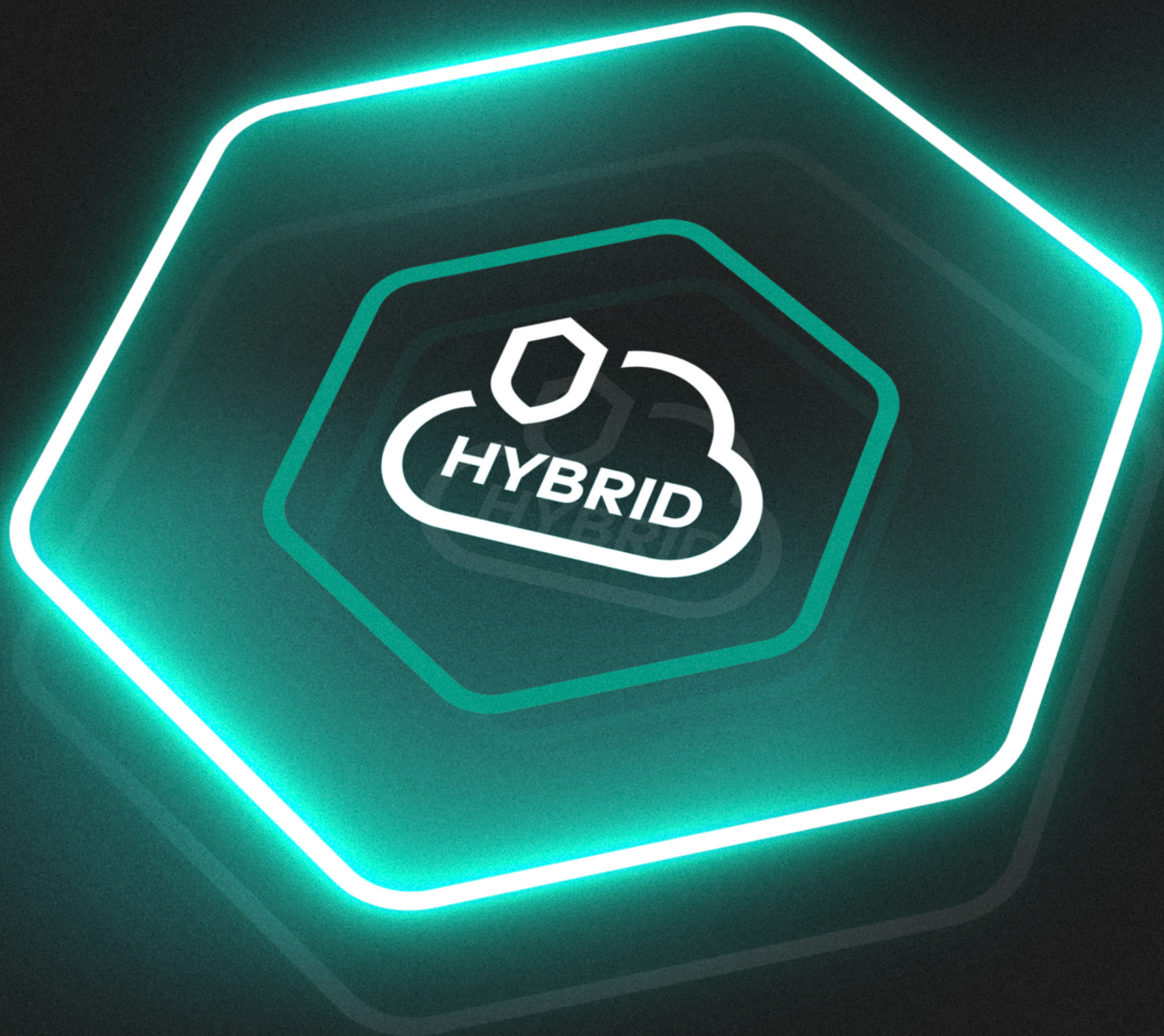


Kaspersky Hybrid Cloud Security



Licensing Guide
May '24

kaspersky bring on
the future

Part of



Kaspersky
Cloud Workload
Security

Kaspersky Hybrid Cloud Security makes cloud adoption, digital transformation, and doing business in general safer and more efficient. The product doesn't just mitigate security risk — it also saves labor hours, infrastructure resources, and money. In terms of cost-efficiency, we offer a flexible licensing model so you can choose only the capabilities you need. You have a choice of two tiers and different licensing objects such as desktops, servers, or CPUs. You can also combine different license types. Here is a brief summary to help you identify the best licensing option for you to get the most value from your security budget.

Kaspersky Hybrid Cloud Security tiers

Kaspersky Hybrid Cloud Security is available in two tiers — Standard and Enterprise.

Features	Standard	Enterprise
Cloud API integration with public clouds (including AWS, MS Azure and Google Cloud)	●	●
File, process and memory protection	●	●
Host IPS/IDS, Firewall Management	●	●
Web AV, Mail AV, Anti-spam, Anti-phishing	●	●
Device and Web Security Controls	●	●
Application Control for Desktop OS	●	●
Behavioral Detection and Exploit Prevention	●	●
Anti-Cryptor for Shared Folders	●	●
Vulnerability Assessment & Patch Management		●
SIEM Connectors		●
Application Control for Server OS		●
File Integrity Monitor (FIM)		●
Log Inspection		●
NextGen IDS/IPS for VMware NSX (suspicious network activity detection)		●

Enterprise tier benefits



Additional use case enablement



Regulatory compliance support



Enhanced security capabilities




Licensing objects and scenarios

Each tier can be licensed on a per-object basis, for multiple scenarios.

You can combine license types if each model is deployed in a separate infrastructure — for example, activating CPU licenses on virtualization platforms and servers/desktops on physical or cloud workloads.

Licensing objects

Scenarios

	Virtualization	VDI	Public clouds
<div></div> <div>Desktop The maximum number of virtual desktops that might be created and used, both persistent and non-persistent</div>		●	
<div></div> <div>Server The total number of physical servers together with the maximum number of virtual servers that might be created and used, both persistent and non-persistent</div>	●		●
<div></div> <div>CPU The total number of physical CPUs installed inside each host running protected virtual machines</div>	●	●	●

Additional licensing options for public clouds



Bring Your Own License

Licensing that supports your digital transformation

Kaspersky Hybrid Cloud Security licensing is designed to support you during complex infrastructure change projects, such as server virtualization or migration from physical desktops to VDI. Both Server and Desktop licenses allow activation of Kaspersky Endpoint Security for Business applications. This way you can switch to Kaspersky Hybrid Cloud Security and take your time to gradually migrate to virtual workloads.

Premium technical support



Premium

Incident request receiving format

Criticality level 1 — on 24x7,
the rest — from 10 a. m. to 6:30 p. m
(Moscow time)

Incident 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

Contacts

4 — the possible number of contact people from
the customer's side



Premium Plus

Incident request receiving format

Criticality level 1 — on 24x7,
the rest — from 10 a. m. to 6:30 p. m
(Moscow time)

Incident 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

Contacts

8 — the possible number of contact people from
the customer's side



Personal technical manager

**Provides reports to the customer
on open incidents**

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

Related solutions



Kaspersky Cloud Workload Security

Optimum

Specialized ecosystem for comprehensive cloud workload protection



Kaspersky Container Security

Specialized containerization protection solution that protects every stage of the app lifecycle



Kaspersky Endpoint Detection and Response

Optimum

Build true defense-in-depth and boost your security efficiency with automated response and simple root cause analysis



Kaspersky Security for Storage

Protects file operations and sensitive data, including against crypto-malware



Kaspersky Professional Services

A SIEM system that improves infrastructure transparency and strengthens the effectiveness of protection



Kaspersky Managed Detection and Response

Continuously hunts, detects and responds to threats targeting your business

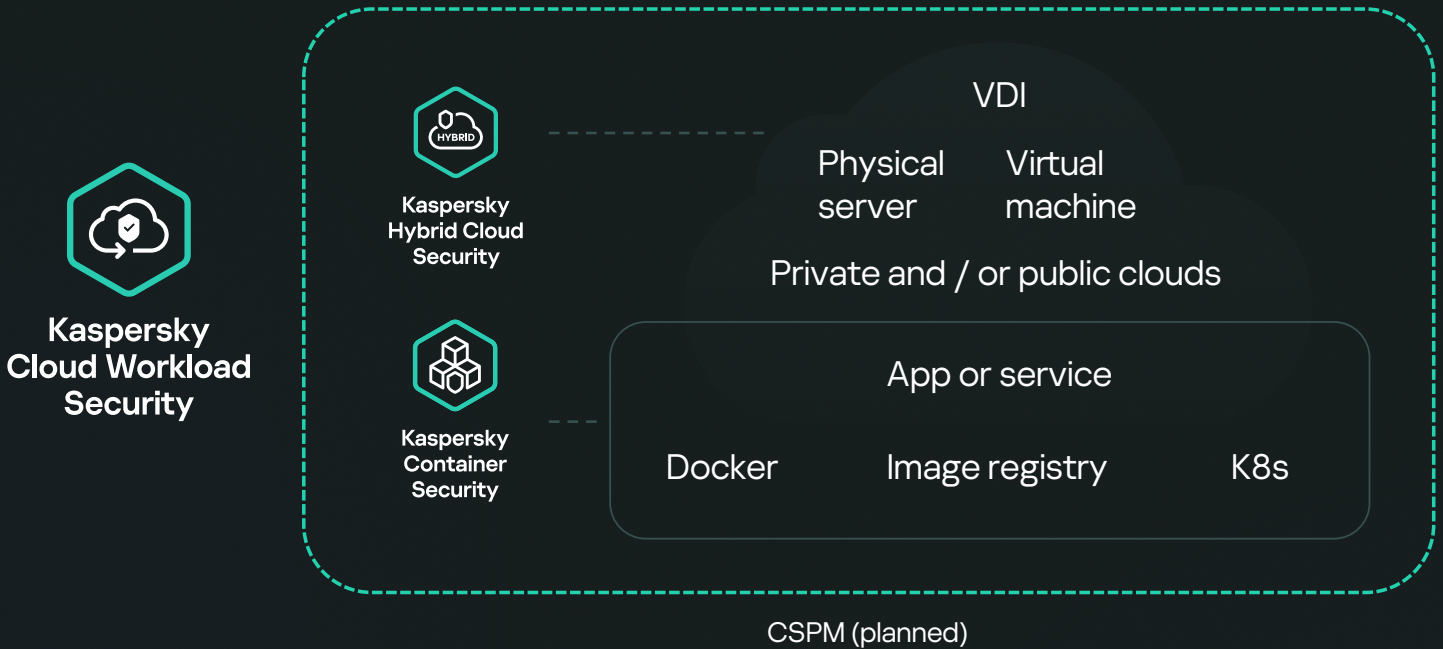


Kaspersky Unified Monitoring and Analysis Platform

Leave routine yet critical security tasks to the experts

Part of Kaspersky Cloud Workload Security

Kaspersky Hybrid Cloud Security in combination with Kaspersky Container Security forms a cloud workload security ecosystem for reliable, world-class protection from attacks together with shorter threat detection and response times in cloud environments. The Kaspersky Cloud Workload Security ecosystem ensures comprehensive protection of your hybrid and cloud infrastructures: virtual machines/container clusters.



Supported solutions



Public clouds

Google Cloud

Microsoft Azure

aws

Orchestrators

kubernetes

OPENSIFT

Private clouds

vmware

Red Hat Enterprise Linux

KVM

Image registries

dockerhub

HARBOR

JFrog

nexus repository

VDI platforms

vmware

TERMIDESK

citrix

CI / CD platforms

Jenkins

TeamCity

GitLab

circleci



Kaspersky Hybrid Cloud Security

[Learn more](#)

www.kaspersky.com

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

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