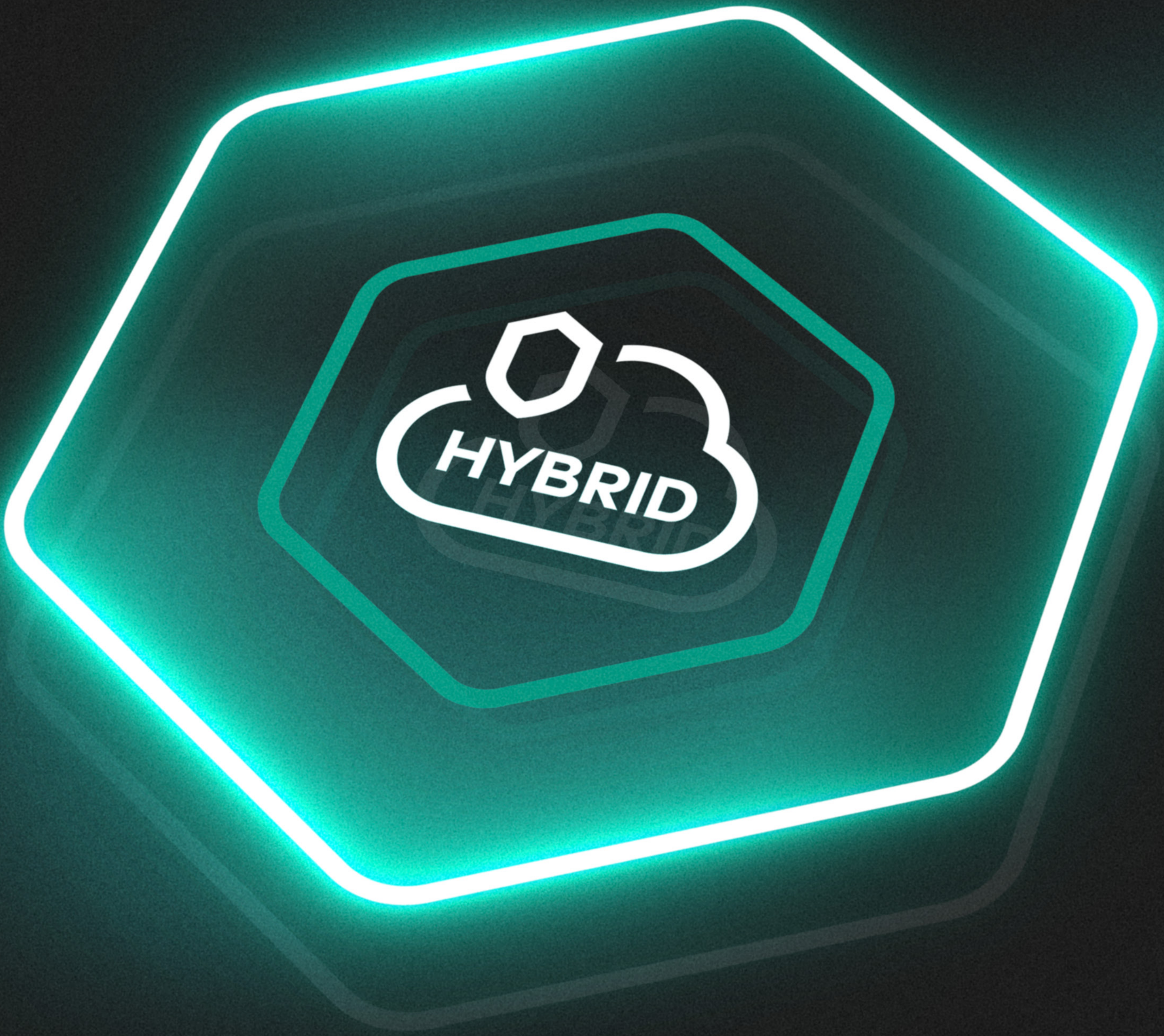
Kaspersky Hybrid Cloud Security



Licensing Guide
February '25

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
Desktop The maximum number of virtual desktops that might be created and used, both persistent and non-persistent		●	
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	●		●
CPU The total number of physical CPUs installed inside each host running protected virtual machines	●	●	●

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

Kaspersky Premium Technical Support is a set of maintenance services agreements (certificates) related to extended technical support services. It delivers a superior user experience, and provides high-priority maintenance and certain SLAs.

Premium Support for Kaspersky Hybrid Could Security offers several options depending on regional specifics:

1. Kaspersky MSA Start, Kaspersky MSA Plus, Kaspersky MSA Business, Kaspersky MSA Enterprise

2. Kaspersky Enhanced Support and Kaspersky Enhanced Support with TAM certificates (can be offered only in addition to Plus-licenses for Kaspersky Hybrid Security)*

See below Premium Support benefits and conditions table.

* Where the bundled MSA model is available

	MSA Start	MSA Plus	MSA Business / Enhanced Support	MSA Enterprise / Enhanced with TAM
Request receiving availability	Criticality level 1-4 — standard office hours of the Kaspersky Local Office	Criticality level 1-4 — standard office hours of the Kaspersky Local Office	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 — 6 business hours	Criticality level 1 — 4 business hours	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
Contacts	1 — the possible number of contacts people from the customer's side	2 — the possible number of contacts people from the customer's side	4 — the possible number of contacts people from the customer's side	8 — the possible number of contacts people from the customer's side • Dedicated Technical Account manager (TAM) • Quality monitoring and reporting • Review calls and Heath Check service • Private patch provisioning

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

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

Related solutions

Kaspersky Cloud Workload Security

Specialized solution for comprehensive cloud workload protection

Kaspersky Container Security

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

Kaspersky Next EDR Optimum

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

Kaspersky Unified Monitoring and Analysis Platform

Leave routine yet critical security tasks to the experts

Kaspersky Managed Detection and Response

Continuously hunts, detects and responds to threats targeting your business

Kaspersky Professional Services

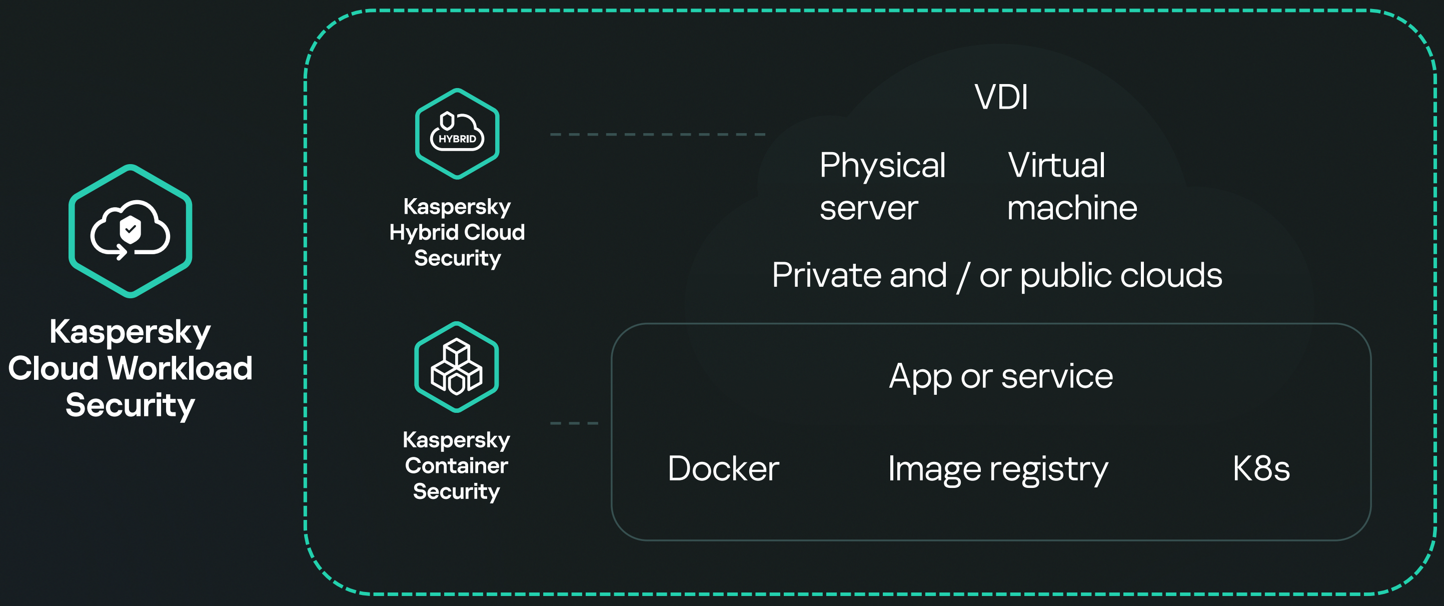
A SIEM system that improves infrastructure transparency and strengthens the effectiveness of protection

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 Hybrid Cloud Security in combination with Kaspersky Container 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.


Kaspersky Cloud Workload Security
HYBRID
Kaspersky Hybrid Cloud Security
Kaspersky Container Security
VDI
Physical server
Virtual machine
Private and / or public clouds
App or service
Docker
Image registry
K8s

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 Hybrid Cloud Security

Learn more

www.kaspersky.com

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

#kaspersky
#bringonthefuture