Licensing Guide

Kaspersky Hybrid Cloud Security

kaspersky

kaspersky.com/hybrid

Kaspersky Hybrid Cloud Security Licensing guide

Here is a brief summary of the various licensing options available for Kaspersky Hybrid Cloud Security, offering you choice and flexibility. For complete and up-to-date information about Kaspersky Hybrid Cloud Security licensing please reach out to a Kaspersky partner.

Kaspersky Hybrid Cloud Editions

Kaspersky Hybrid Cloud is available in two editions — 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	✓	✓
Container Security and DevOps integrations		✓
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)		✓

While the Standard edition provides essential protection for physical, virtualized and cloud workloads, there are scenarios where a customer would benefit from the Enterprise version:

1. Organizations that employ hardening scenarios up to full-scale default deny implementations. Application Control in default deny mode combined with FIM provides a thorough security baseline.
2. Organizations that are looking to minimize their attack surface and optimize software management time by leveraging Vulnerability Assessment and Patch Management technology.
3. Organizations seeking to secure DevOps processes and integrate repository, image and container scanning into their CI/CD pipelines.
4. Organizations aiming to achieve stringent compliance requirements. Application Control, File Integrity Monitoring and loginspection can assist companies to comply with system and data security requirements, such as PCI DSS (V3.21 ref# 10.5, 11.5), ISO/IEC 27001 (A10.10.1, A10.10.3, A.12.4.2), FedRAMP (CM-7, RA-5, AU-2, AU-5, AU-6, AU-9), Common Criteria (CC 3.2-3.4, 4.2, 5.1, 5.2, 6.1, 7.2, 7.3) and others.
5. Organizations using the VMWare platform and shooting for maximum network security would benefit from NextGen IDS/IPS for VMware NSX.
6. Organizations that employ a SIEM system and intend to aggregate security events from virtualized and cloud endpoints.

Kaspersky Hybrid Cloud Security Licensing Modes

Kaspersky Hybrid Cloud Security can be licensed per workload (physical servers, virtual servers, and virtual desktops) and per CPU. Here are a few simple rules that can help you identify the best licensing option:

1. "Per CPU" licensing is only available for virtual machine protection when the customer controls the hypervisor layer
2. For physical machines or cloud workload protection the only available option is "per VM"
3. When choosing the right license for protection of virtual machines, it's necessary not only to consider the consolidation ratio but also to account for the organization's IT infrastructure evolution plans. CPU licensing makes changing the number and the type of protected VMs easy and if the number of VM changes often or is expected to grow, CPU licensing is the best option.

Licensing Objects

Virtual Workstation (for Kaspersky Hybrid Cloud Security, Desktop and for Kaspersky Hybrid Cloud Security Enterprise, Desktop)	**The maximum total number of virtual desktops that might be created and used, both persistent and non-persistent**
Server (for Kaspersky Hybrid Cloud Security, Server and Kaspersky Hybrid Cloud Security Enterprise, Server)	**The total number of physical servers together with the maximum total number of virtual servers that might be created and used, both persistent and non-persistent**
CPU (for Kaspersky Hybrid Cloud Security, CPU and Kaspersky Hybrid Cloud Security Enterprise, CPU)	**The total number of physical CPUs installed inside each host running protected virtual machines**

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

For containerization security and DevOps integration tasks, a host where Kaspersky Hybrid Cloud Security agent is installed must be licensed with an Enterprise tier license.

Making sense of Kaspersky Hybrid Cloud Security licensing during an infrastructure change project

Kaspersky Hybrid Cloud Security licensing is designed to accommodate 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. And if you ever need to take a step back, that is fine, too. A Kaspersky Hybrid Cloud Security license will let you to roll back, regroup and move forward with your digital transformation.

Kaspersky Hybrid Cloud Security: kaspersky.com/hybrid
Kaspersky Hybrid Cloud Security for AWS: kaspersky.com/aws
Kaspersky Hybrid Cloud Security for Microsoft Azure: kaspersky.com/azure
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

© 2020 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.