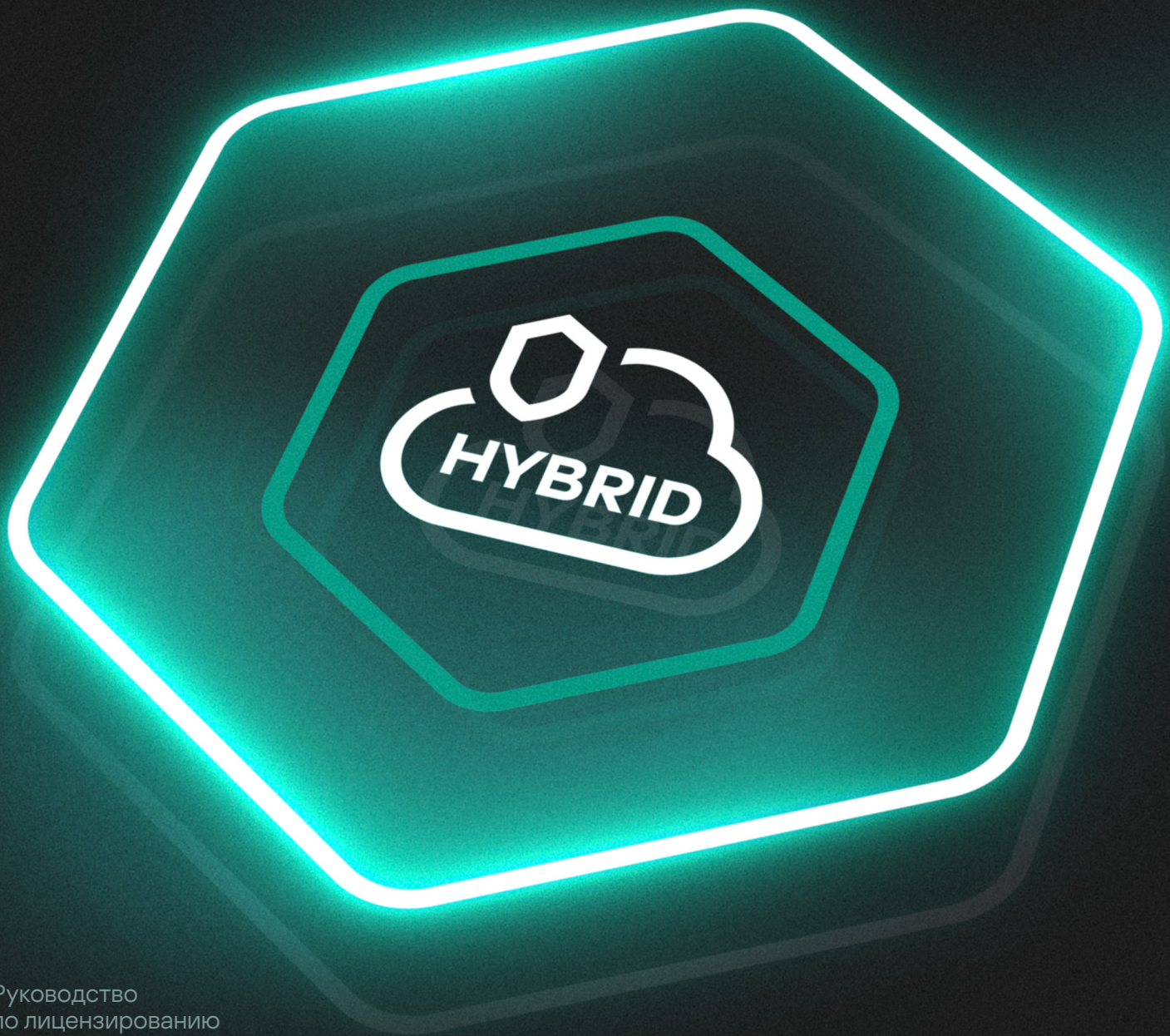
Kaspersky Security для виртуальных и облачных сред



Руководство
по лицензированию

Февраль '25

Входит в

Kaspersky
Cloud Workload
Security

kaspersky активируй будущее

Kaspersky Security для виртуальных и облачных сред повышает безопасность и эффективность перехода в облако, цифровой трансформации и бизнес-процессов в целом. Продукт не просто снижает риски безопасности — он экономит ваше время, вычислительные ресурсы и бюджет.
Мы предлагаем гибкую модель лицензирования, чтобы вы могли выбрать только необходимые функции защиты. Доступны два уровня защиты и разные объекты лицензирования — компьютеры, серверы и процессоры. Типы лицензий можно комбинировать. Таблица ниже поможет вам подобрать наиболее подходящую модель лицензирования и избежать лишних трат.

Уровни Kaspersky Security для виртуальных и облачных сред

Kaspersky Security для виртуальных и облачных сред доступен в двух вариантах: Standard и Enterprise.

Возможности	Standard	Enterprise
Интеграция через API с публичными облачными службами (включая AWS, Microsoft Azure, Google Cloud, Yandex Cloud)	●	●
Защита данных, процессов и памяти	●	●
IDS (системы обнаружения вторжений) и IPS (системы предотвращения вторжений) на устройствах, Управление сетевым экраном	●	●
Веб-антивирус, Почтовый антивирус, Анти-спам, Анти-фишинг	●	●
Контроль защиты устройств и Веб-контроль	●	●
Контроль программ для ОС персональных компьютеров	●	●
Поведенческий анализ и защита от эксплойтов	●	●
Защита общих папок от шифрования	●	●
Оценка уязвимостей и управление установкой исправлений		●
Коннекторы SIEM		●
Контроль программ для серверных ОС		●
Мониторинг целостности файлов (FIM)		●
Анализ журналов		●
IDS/IPS нового поколения для VMware NSX (обнаружение подозрительной сетевой активности)		●

Преимущества уровня Enterprise

Дополнительные сценарии использования

Соответствие нормативным требованиям

Расширенная защита

Объекты и сценарии лицензирования

Лицензии обоих уровней могут выдаваться как отдельно для каждого объекта, так и для различных сценариев. Типы лицензий можно комбинировать, если они используются для разных инфраструктур. Например, вы можете активировать лицензии по процессорам на платформах виртуализации и лицензии по серверам и рабочим местам в физической или облачной среде.

Объекты лицензирования	Сценарии		
	Виртуализация	Инфраструктура виртуальных рабочих столов (VDI)	Публичные облачные платформы
ПК Максимально допустимое количество создаваемых и используемых виртуальных рабочих мест (временных и постоянных)		●	
Сервер Общее количество физических серверов и максимально допустимое количество создаваемых и используемых виртуальных серверов (временных и постоянных)	●		●
Физический процессор Общее количество физических процессоров установленных на каждом хосте, где запускаются защищенные виртуальные машины	●	●	●

Дополнительные возможности лицензирования для публичного облака

Использование собственных лицензий (BYOL)

Лицензирование для эффективной цифровой трансформации

Лицензии Kaspersky Security для виртуальных и облачных сред подходят для проектов комплексного преобразования инфраструктуры (например, виртуализации сервера или миграции из физической среды в виртуальную). Обе лицензии — для серверов и для ПК — позволяют активировать приложения Kaspersky Security для бизнеса. Так вы сможете переключиться на Kaspersky Security для виртуальных и облачных сред и постепенно перейти к работе в виртуальной среде.

Расширенная техническая поддержка

Premium

Формат получения сообщений об инцидентах

Уровень критичности 1 — круглосуточно, остальные — с 10:00 до 18:30 (МСК)

Время реагирования на инциденты

Уровень критичности 1 — 2 часа*
Уровень критичности 2 — 6 рабочих часов
Уровень критичности 3 — 8 рабочих часов
Уровень критичности 4 — 10 рабочих часов

Контакты

4 — возможное количество контактных лиц на стороне клиента

Premium Plus

Формат получения сообщений об инцидентах

Уровень критичности 1 — круглосуточно, остальные — с 10:00 до 18:30 (МСК)

Время реагирования на инциденты

Уровень критичности 1 — 2 часа*
Уровень критичности 2 — 6 рабочих часов
Уровень критичности 3 — 8 рабочих часов
Уровень критичности 4 — 10 рабочих часов

Контакты

8 — возможное количество контактных лиц на стороне клиента

Персональный менеджер по технической поддержке

Предоставляет клиенту отчеты об открытых инцидентах

* В нерабочее время необходим дополнительный контакт по телефону

Комплементарные продукты

Kaspersky Cloud Workload Security

Специализированное решение для всесторонней защиты облачных рабочих нагрузок

Kaspersky Container Security

Специализированное решение для защиты контейнеров, которое обеспечивает безопасность приложений на всех этапах их жизненного цикла

Kaspersky Endpoint Detection and Response Expert

Глубокая защита и высокая эффективность систем безопасности благодаря функциям анализа первопричин и автоматического реагирования

Kaspersky Security for Storage

Защита операций с файлами и конфиденциальных данных, в том числе от программ-шифровальщиков

Kaspersky Unified Monitoring and Analysis Platform

SIEM-система, повышающая прозрачность инфраструктуры и эффективность защиты

Kaspersky Managed Detection and Response

Непрерывный активный поиск, обнаружение и устранение угроз, направленных на ваш бизнес

Kaspersky Professional Services

Рутинные, но критически важные задачи — в руках наших экспертов

Компонент Kaspersky Cloud Workload Security

Kaspersky Security для виртуальных и облачных сред вместе с Kaspersky Container Security входят в состав решения для всеобъемлющей защиты облачных нагрузок Kaspersky Cloud Workload Security. Это комплексное решение обеспечивает безопасность всей гибридной и облачной инфраструктуры клиентов: хостов гипервизора, виртуальных машин, инстансов, контейнеров и Kubernetes.

Система управления состоянием безопасности облака (CSPM)
(в перспективе)

Совместимость

Kaspersky Security для виртуальных и облачных сред

Публичные облачные платформы

Google Cloud · Yandex Cloud · Microsoft Azure · aws

Платформы виртуализации

vmware · PROXMOX · Red Hat Enterprise Linux · AOS · HUAWEI · Microsoft Hyper-V · KVM

Инфраструктура виртуальных рабочих столов (VDI)

vmware · citrix · TERMIDESK

Kaspersky Container Security

Оркестраторы

kubernetes · Amazon ECS · OPENSHIFT · Deckhouse Kubernetes Platform

Реестры образов

dockerhub · Red Hat Quay · GitLab · Amazon ECR · HARBOR · nexus repository · JFrog

Платформы CI/CD

Jenkins · TeamCity · GitLab · circleci

Kaspersky Security для виртуальных и облачных сред

Подробнее

www.kaspersky.ru

© 2025 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее