Kaspersky Security
для виртуальных
и облачных сред

Надежная защита с унифицированным управлением безопасностью гибридного облака

kaspersky

Kaspersky Security для виртуальных и облачных сред

К виртуализации приходят почти все компании, которые не хотят упускать прибыль и стремятся вовремя адаптироваться к изменениям на рынке. Логичным следующим шагом становятся облачные вычисления. Переход в облако позволяет избавиться от переусложненной инфраструктуры и добиться высокой эффективности. Однако такой переход имеет свои подводные камни. Некоторые из них новые, а другие достались по наследству от физической инфраструктуры.

Kaspersky Security для виртуальных и облачных сред – это универсальная защита компании на всех этапах перехода в облако по любому сценарию. Решение подходит как для систем, переносимых в облако, так и для тех, которые развертываются в облаке изначально. Оно защищает физические и виртуализированные рабочие нагрузки независимо от того, где они выполняются – локально, в центре обработки данных или в общедоступном облаке. Поскольку все компоненты решения были разработаны с учетом особенностей виртуальных сред и серверных систем и идеально сбалансированы, оно защищает даже от самых продвинутых известных и неизвестных угроз, не снижая производительности инфраструктуры.

Главные сложности перехода в облако:

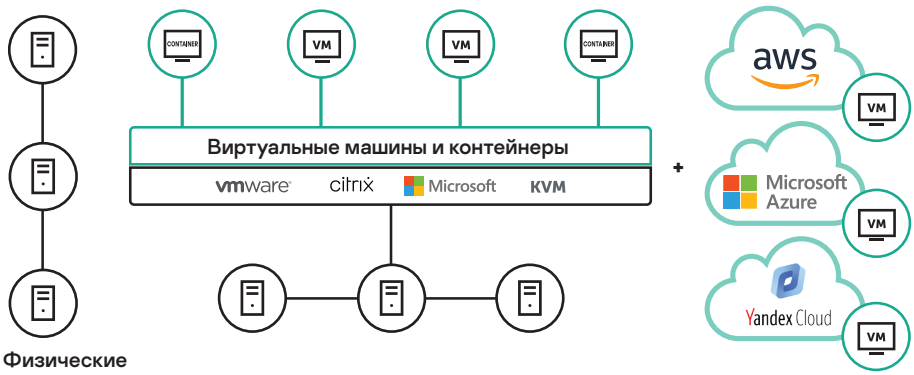
- Растущая сложность инфраструктуры может снизить прозрачность операций.
- Несмотря на то что многоуровневый подход – основа надежной защиты, он редко реализуется в одном продукте.
- Традиционные тяжеловесные защитные продукты тратят много системных ресурсов.
- Разрозненные средства защиты с несовместимыми средствами управления усложняют администрирование.
- Шифровальщики и другие вредоносные программы атакуют как физические, так и виртуальные рабочие места.
- Отсутствие адекватных мер кибербезопасности для защиты персональных данных может повлечь за собой юридические проблемы.

Почему Kaspersky Security для виртуальных и облачных сред?

- Оптимизация для физических, виртуальных и облачных рабочих нагрузок
- Интегрированная многоуровневая система защиты для всех типов рабочих нагрузок
- Гармоничная интеграция гибких автоматизированных средств безопасности с публичными облачными средами Яндекса, Amazon, Microsoft и Google
- Полный набор инструментов для соблюдения требований общей ответственности
- Централизованное управление безопасностью всей гибридной облачной среды
- Надежность защиты подтверждена многочисленными наградами и результатами независимых тестирований[1]

1 В тестах испытывался широкий диапазон продуктов «Лаборатории Касперского» на основе технологий, используемых и в Kaspersky Security для виртуальных и облачных сред. Подробнее см. на сайте kaspersky.com/top3

Ключевые преимущества



Физические серверы

Облачные рабочие нагрузки

Безопасный переход в облако с защитой на всех уровнях

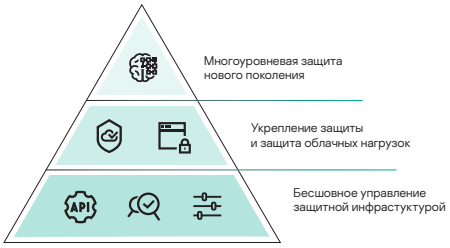
- Передовые технологии обеспечивают безопасность любых рабочих нагрузок – физических, виртуальных и облачных.
- Многоуровневая защита в режиме реального времени на основе машинного обучения защищает ваши данные, процессы и приложения даже от новых и еще не известных угроз.
- Комплексный подход позволяет снизить юридические и репутационные риски, связанные с соблюдением нормативов по защите данных.

Максимальная отдача от ваших ресурсов и инвестиций

- Защита без агента и Легкий агент позволяют обезопасить виртуализированные активы как в обычных, так и в программно определяемых облачных сетях без ущерба для производительности.
- Интеграция со встроенной системой безопасности общедоступных и управляемых облачных сред помогает защищать приложения, ОС, потоки данных и рабочие места пользователей с минимальным расходом ресурсов.
- Объединенное управление физическими и виртуальными ресурсами экономит человеко-часы как на стадии освоения системы, так и при дальнейшей эксплуатации.

Возможности

Возможности	Описание
Многоуровневая защита от угроз Предлагаемая «Лабораторией Касперского» защита нового поколения включает проактивные компоненты, блокирующие широкий спектр кибератак на критически важные рабочие нагрузки.	
Глобальная аналитика угроз	Данные о состоянии ландшафта киберугроз, доступные в режиме реального времени, поддерживают постоянную актуальность защиты.
Машинное обучение	Большие данные, на основе которых анализируются глобальные угрозы, обрабатываются алгоритмами машинного обучения и нашими экспертами. Таким образом достигается высокий уровень обнаружения угроз с малым числом ложноположительных срабатываний.
Защита от почтовых и веб-угроз	Защита от проникновения через почту и веб-приложения обеспечивает безопасную работу виртуальных и удаленных рабочих столов.
Анализ журналов	Сканирование файлов внутренних журналов позволяет проверять безопасность операций.
Поведенческий анализ	Контроль приложений и процессов защищает системы от продвинутых угроз, включая бесфайловые и скриптовые вредоносные программы.
Откат вредоносных действий	Откат любых несанкционированных изменений рабочих нагрузок в случае необходимости.
Защита от эксплойтов	Эффективное противостояние продвинутым атакам и полная совместимость с защищаемыми приложениями без ущерба их производительности.
Защита от программ-вымогателей	Безопасность виртуализированных рабочих нагрузок и предотвращение любых посягательств на коммерчески важные данные. При попытке удаленного шифрования все поврежденные файлы откатываются к предыдущему состоянию, а само шифрование блокируется.
Защита от сетевых угроз	Обнаружение и предотвращение сетевых вторжений в облачные активы.
Защита контейнеров	Защита от заражения гибридной IT-инфраструктуры вирусами через скомпрометированные контейнеры Docker или Windows.
Повышение надежности системы	
Контроль программ	Возможность перевести все рабочие нагрузки в гибридном облаке в режим «запрет по умолчанию»: выполняться смогут только проверенные и доверенные компоненты.
Контроль устройств	Определение того, какие виртуализированные устройства могут обращаться к отдельным рабочим нагрузкам в облаке.
Веб-Контроль	Контроль использования веб-ресурсов виртуальными и удаленными рабочими станциями для снижения рисков и повышения производительности.
Хост-система предотвращения вторжений (HIPS)	Ограничение доступа запущенных программ к критически важным ресурсам в зависимости от присвоенных им категорий доверия.
Мониторинг целостности файлов	Отслеживание целостности ключевых компонентов системы.
Оценка уязвимостей и управление установкой исправлений	Централизация и автоматизация таких ключевых задач безопасности, конфигурации системы и управления, как мониторинг уязвимостей, распространение исправлений и обновлений, учет и развертывание приложений.
Полная прозрачность	
Унифицированное управление защитой	Управление всеми средствами защиты из Kaspersky Security Center, включая рабочие места и серверы – в офисе, ЦОД и облаке.
Облачные API	Полная интеграция с общедоступными средами AWS, Azure, Yandex Cloud и Google Cloud позволяет обнаруживать инфраструктуру, автоматически развертывать агенты безопасности и управлять системами с помощью политик, а также упрощает инвентаризацию и развертывание средств безопасности.
Гибкие возможности управления	Поддержка нескольких клиентов и контроль учетных записей на основе разрешений, а также все преимущества унифицированного администрирования из единой консоли.
Интеграция с SIEM-системами	В зрелых IT-инфраструктурах средства управления данными и событиями в системе безопасности (SIEM) служат для обзора различных аспектов корпоративной кибербезопасности во всей гибридной сети.



Унифицированная защита для любых облачных систем

Публичные облака
- Amazon Web Services (AWS)
- Microsoft Azure
- Платформа Google Cloud
- Yandex.Cloud

Платформы виртуализации
- VMware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox
- Huawei FusionSphere
- Скала-Р

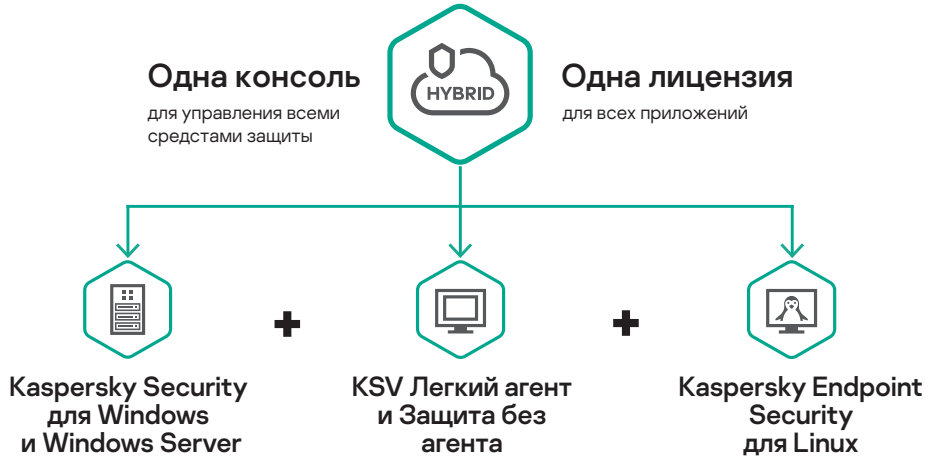
Среды VDI
- VMware Horizon
- Citrix Virtual Apps and Desktops

Физические серверы
- Windows
- Linux

Физические рабочие места
- Windows
- Linux

Согласованное отслеживание и контроль гибридной инфраструктуры при любой ее конфигурации

- Простое развертывание средств безопасности и защита на основе политик доступны для всей гибридной облачной среды.
- Гибкость лицензирования позволяет переходить с физических рабочих мест к виртуальной инфраструктуре поэтапно и в удобном темпе, а также откатывать изменения в случае необходимости.
- Средства управления безопасностью работают сразу в нескольких облаках.
- Полная видимость, управляемость и комплексная защита от продвинутых угроз доступны для каждой рабочей нагрузки, независимо от ее местоположения.



Решение Kaspersky Security для виртуальных и облачных сред использует полный набор передовых технологий защиты. Оно упростит и ускорит трансформацию IT-среды, позволив безопасно перейти с физической инфраструктуры на виртуальную или облачную.

www.kaspersky.ru