Kaspersky® Security для виртуальных сред

Надежная, гибкая и эффективная защита виртуальных серверов и рабочих станций

Все большее число компаний использует преимущества программно-определяемых центров обработки данных (ЦОД). Всем им необходим высочайший уровень защиты от киберугроз без снижения производительности.

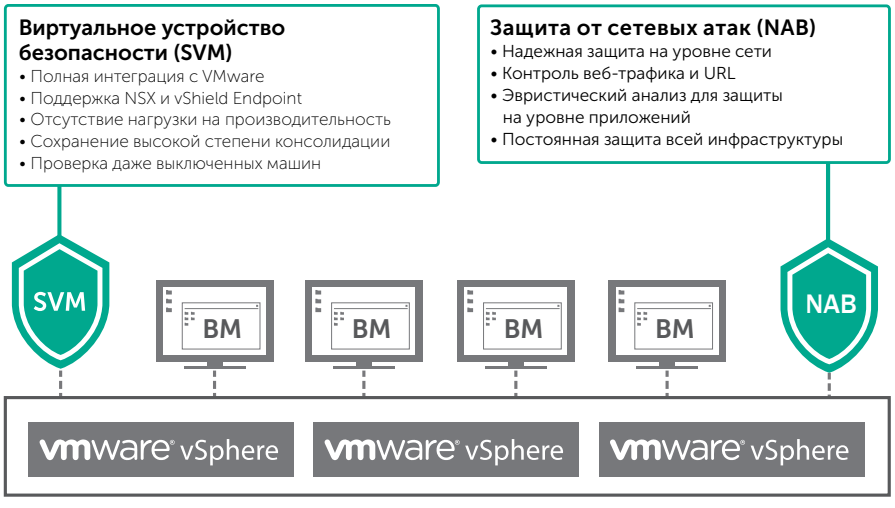
Решение Kaspersky Security для виртуальных сред обеспечивает надежную, многоуровневую и гибко настраиваемую защиту инфраструктуры VDI и виртуальных серверов. Технологии «Лаборатории Касперского» интегрированы с ведущими платформами и технологиями виртуализации, такими как VMware® vSphere® с NSX®, Microsoft® Hyper-V®, Citrix® XenServer® и KVM, а также VMware Horizon® и Citrix XenDesktop®.

Решение Kaspersky Security для виртуальных сред без агента или с Легким агентом позволяет вывести взаимодействие защитного решения и программно-определяемого центра обработки данных на новый уровень и способствует их слаженной, быстрой и эффективной работе.

- **Проверенная многолетним опытом и сотнями тестов технология защиты от вредоносного ПО**, усиленная системой обнаружения вторжений (IDS/IPS), распознает и блокирует известные и неизвестные угрозы, включая атаки нулевого дня.
- **Автоматизация развертывания специальных виртуализированных устройств безопасности** на основе политик NSX, действующих применительно к каждой ВМ на хосте гипервизора.
- **Интеграция с политиками безопасности NSX** позволяет максимально полно использовать возможности защиты и при этом менять и расширять инфраструктуру корпоративного ЦОД без каких-либо ограничений.
- **Интеграция с метками безопасности NSX** позволяет программно-определяемым ЦОД реагировать на угрозы в режиме реального времени и в случае необходимости автоматически перенастраивать всю виртуальную инфраструктуру.
- **Проактивная защита** от известных и новых угроз, в том числе угроз нулевого дня, с помощью интеграции с облачной репутационной сетью Kaspersky Security Network.

Полная интеграция с VMware NSX

Полная интеграция между платформой виртуализации VMware NSX и Kaspersky Security для виртуальных сред Защита без агента позволяет реагировать на инциденты безопасности максимально оперативно.

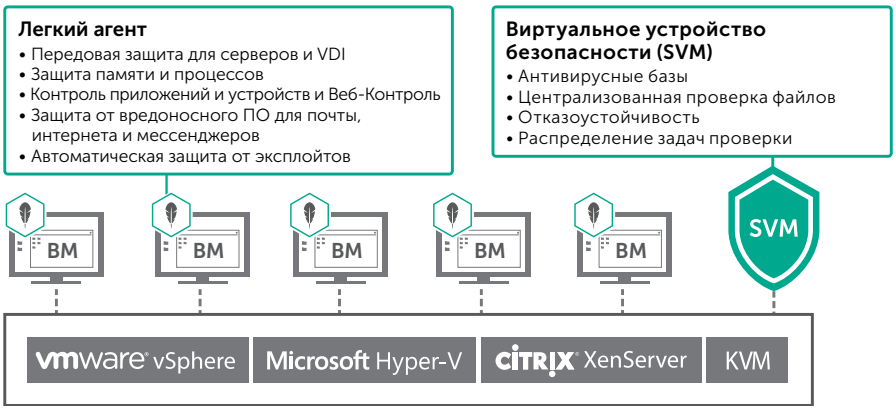


- Технология **Мониторинг Системы** контролирует поведение программ, исполняющихся на ВМ, своевременно производит откат вредоносных действий и защищает от программ-шифровальщиков.
- Технология **защиты от сетевых атак (NAB) и система предотвращения вторжений (HIPS)** защищают виртуальную инфраструктуру от самых сложных сетевых угроз.
- **Контроль внешних URL** позволяет оградить каждую ВМ и ее пользователей от интернет-ресурсов, которые не соответствуют принятым политикам безопасности или несут высокий риск компрометации безопасности компании, ее данных и пользователей.
- **Контроль запуска программ и их привилегий, в том числе режим «Запрет по умолчанию»,** контролируют активность пользователей, благодаря чему на ВМ могут быть запущены только доверенные приложения.
- **Система защиты почтового и веб-трафика** обеспечивает безопасность обмена данных и коммуникаций корпоративных пользователей с внешним миром.
- **Контроль устройств** обеспечивает надежную защиту каждого виртуального рабочего стола при подключении к нему виртуализированных USB-устройств и сетевых принтеров.

Kaspersky Security для виртуальных сред Легкий агент

Защита без агента подходит для инфраструктур VMware, которые нуждаются в защите на уровне файловой системы и корпоративной сети. Тем не менее для надежной защиты критически важных для бизнеса виртуальных серверов и рабочих столов (VDI) требуется решение, обеспечивающее многоуровневую защиту.

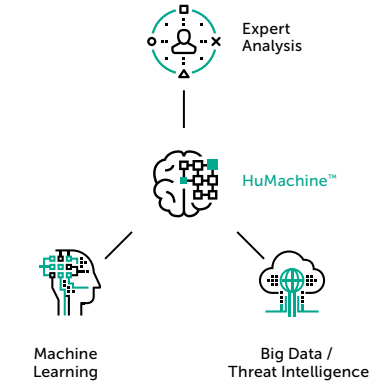
Kaspersky Security для виртуальных сред Легкий агент – это единое защитное решение, которое обеспечивает безопасность виртуальных серверов и VDI. Благодаря поддержке всех популярных платформ виртуализации — VMware vSphere, Citrix XenServer, Microsoft Hyper-V and KVM — это решение идеально подходит для гибридных программно-определяемых ЦОД. Легкий, но мощный агент поддерживает ведущие платформы VDI Citrix XenDesktop и VMware Horizon, значительно усиливая их защиту и практически не влияя на производительность каждой ВМ.



Виртуальное устройство безопасности (SVM) «Лаборатории Касперского» осуществляет централизованную проверку всех виртуальных машин, размещенных на хост-сервере. Легкий агент устанавливается на каждой виртуальной машине, и его развертывание позволяет активировать расширенные функции безопасности, в том числе Контроль программ, Контроль устройств и Веб-Контроль, а также эвристические модули и антивирусную защиту для служб мгновенных сообщений, электронной почты и интернета. Пики в потреблении ресурсов снижаются с помощью интеллектуальной системы распределения задач, которая автоматически группирует и приоритизирует задачи проверки ВМ.

Вы можете выбрать удобный для себя вариант установки — с легким агентом или без. Два подхода в одном решении обеспечивают мощную защиту, которая сочетается с высокой производительностью, что особо важно для виртуальных сред.

Решение Kaspersky Security для виртуальных сред (без агента и с Легким агентом) сертифицировано ФСТЭК России и внесено в Единый реестр российских программ Минкомсвязи РФ.



www.kaspersky.ru

#ИстиннаяБезопасность