kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Security для виртуальных и обачных сред

Kaspersky Security для виртуальных сред и VMware NSX

Создано специально для VMware NSX

- Признанные технологии мирового уровня распознают и блокируют известные, неизвестные и сложные угрозы, включая угрозы нулевого дня.
- Автоматизация развертывания для VMware NSX позволяет виртуальному устройству безопасности (SVM) автоматически учитывать требования каждой защищаемой на этом хосте виртуальной машины.
- Интеграция с политиками безопасности означает, что каждая ВМ обеспечивается необходимым уровнем защиты на основе корпоративных политик безопасности и роли ВМ.
- Интеграция с метками безопасности NSX позволяет программно-определяемому центру данных реагировать в течение реального времени на инциденты безопасности, и, если необходимо, заново конфигурировать всю инфраструктуру.
- Проактивная защита от сложных угроз — благодаря интеграции с облачной сетью безопасности Kaspersky Security Network.
- Одновременная поддержка NSX и vShield Endpoint позволяет защитному решению оптимально вписываться в любую страгегию развития ЦОД.

Оптимальный баланс защиты и производительности

- Эффективность защиты повышается благодаря тому, что проверка файлов осуществляется не на ВМ, а на вирту-альных устройствах безопасности (SVM).
- Виртуализированная система обнаружения и предотвращения вторжений (IDS/IPS) защищает от угроз на уровне сети.
- Технология Shared Cache снижает нагрузку на ВМ, так как проверке подвергается только один экземпляр файла, размещенного на разных виртуальных машинах.

Эффективная защита программно-определяемых ЦОД

Для любого бизнеса самым ценным ресурсом являются данные. И, разумеется, инфраструктура, в которой эти данные хранятся, обрабатываются и передаются, — очень важный инструмент для достижения конкурентных преимуществ.

В то же время существующие в современных центрах обработки данных (ЦОД) решения по организации сетевой связности и средства обеспечения безопасности являются недостаточно гибкими и иногда чрезмерно сложными. Это создает дорогостоящие препятствия на пути к достижению полной адаптивности современного ЦОД к быстроменяющимся требованиям бизнеса.

Компании VMware® и «Лаборатория Касперского» вместе решают эту проблему, предлагая не только современные решения и технологии виртуализации инфраструктуры, но и передовые методы обеспечения ее защиты от внешних и внутренних угроз.

Встроенные в VMware NSX сервисы	
Распределенный сетевой экран	Виртуальные сети (VXLAN)
Мониторинг активности ВМ	VPN (IPSec, SSL, L2VPN)
Kaspersky Security для виртуальных сред	
Защита от вредоносного ПО	Система предотвращения вторжений (IPS)
Интеграция с метками безопасности	Интеграция с политиками безопасности
Автоматизация развертывания	Проверка даже выключенных виртуальных машин

Решение Kaspersky Security для виртуальных сред | Защита без агента специально создано, чтобы защитить программно-определяемых центры обработки данных на базе VMware vSphere с технологиями NSX®. Защитное решение сочетает передовые возможности защиты с минимальным влиянием на производительность платформы и сохранением высокой степени консолидации виртуальных машин (ВМ).

Безопасность и мониторинг

- Решение осуществляет проверку всей инфраструктуры и защищает все, даже выключенные, виртуальные машины.
- Операции проверки ВМ могут быть заранее запланированы — это позволяет учитывать потребности любой организации.
- Самозащита и SNMP-мониторинг гарантируют, что виртуальные устройства безопасности постоянно запущены, а также обеспечивают передачу информации сторонним средствам мониторинга для дополнительного контроля.
- Защита виртуальной среды никогда не прерывается, даже при переносе ВМ на другой хост —решение полностью поддерживает VMware vMotion и Disaster Recovery.
- Полная интеграция с VMware vCenter Server и NSX Manager означает, что уровень безопасности готов к любым изменения инфраструктуры.

Высочайшая надежность и управляемость

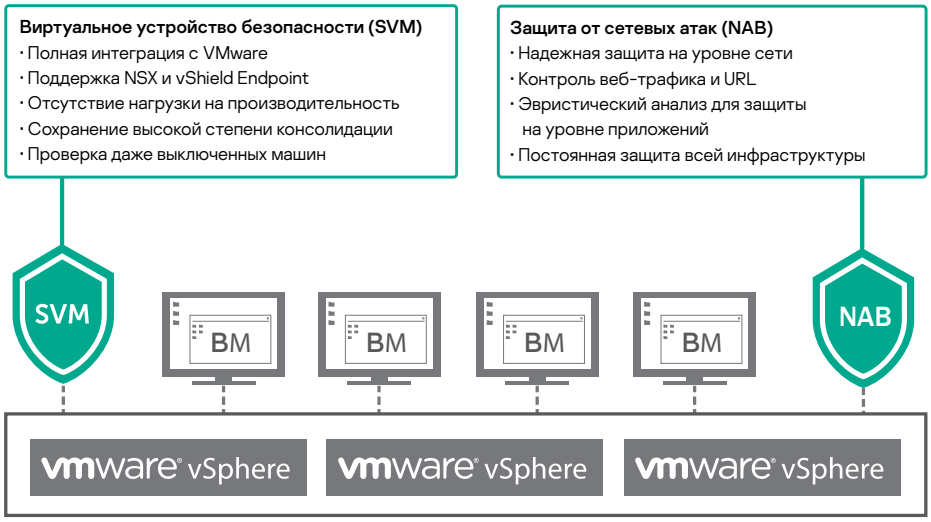
- Единая консоль — для управления физическими, виртуальными и мобильными устройствами. Благодаря этому на всех типах устройств действуют одинаковые политики безопасности.
- Быстрое развертывание решения — нет необходимости перезагружать ВМ или переводить хост-сервер в режим обслуживания.
- Интеллектуальная система распределения задач устраняет пики в потреблении ресурсов гипервизором и увеличивает общую эффективность платформы.
- Широкие возможности монитинга и отчетности упрощают управление и контроль системы безопасности во всей инфраструктуре.

Результат — гибко настраиваемая виртуальная среда корпоративного уровня, которая сочетает высокую эффективность с надежной защитой.

Интеграция Kaspersky Security для виртуальных сред с платформой VMware NSX

Платформа VMware NSX воспроизводит модель сети на программном уровне, обеспечивая возможность за несколько секунд создать или переконфигурировать любую сетевую топологию — от самой простой до многоуровневой, а также внедрить стратегию безопасности ЦОД, основанную на модели «нулевого доверия».

Благодаря тесной интеграции с VMware NSX решение Kaspersky Security для виртуальных сред | Защита без агента обеспечивает автоматическую защиту каждой ВМ и виртуализированной сети от самых сложных угроз. Решение устраняет необходимость установки агента безопасности на каждую ВМ, поэтому влияние на ресурсы и производительность платформы является минимальным.



Полная интеграция между платформой виртуализации и защитным решением позволяет программно-определяемому ЦОД реагировать на любой инцидент безопасности в режиме реального времени.

Оптимальная защита для программно-определяемого ЦОД

Виртуальные и физически среды сталкиваются с одинаковыми угрозами безопасности — киберпреступники не делают между ними различий. Поэтому виртуальные среды должны быть защищены так же надежно, как и физические.

Защита от киберугроз

Kaspersky Security для виртуальных сред базируется на технологиях защиты от вредоносного ПО, которые неоднократно удостаивались высших оценок в независимых тестах, однако эти технологии были адаптированы для защиты виртуальных сред. Благодаря этому решение защищает всю виртуальную инфраструктуру от самых сложных угроз и уязвимостей, а также учитывает технологические особенности платформы виртуализации. Надежная защита сочетается с высокой скоростью и минимальным потреблением ресурсов.

vmware PARTNER TECHNOLOGY ALLIANCE
vmware READY NETWORKING AND SECURITY
NUTANIX READY
VBLOCK READY
VCE VALIDATION READY

Полная оптимизация для VMware NSX

Полная интеграция решения с платформой VMware NSX означает, что платформа виртуализации становится еще более эффективной. Инфраструктура VMware NSX и решение Kaspersky Security для виртуальных сред | Защита без агента работают сообща, что открывает новые возможности для автоматизации и применения единых политик безопасности во всей инфраструктуре. Интеграция с политиками и метками безопасности делает взаимодействие быстрым, удобным и гибким.

Простота управления

Единая консоль позволяет IT-отделу централизованно управлять защитой всех ВМ, так же как защитой физических устройств. Это упрощает управление в гибридных средах, которые объединяют виртуальные, физические и мобильные платформы. Кроме того, это упрощает стратегическое развитие виртуальной платформы, снижает количество ошибок и уменьшает нагрузку на IT-ресурсы.

Kaspersky Security для виртуальных сред — это самые современные возможности защиты для гибридных корпоративных сред, построенных на базе VMware NSX. Решение увеличивает эффективность платформы и практически не влияет на ее производительность. Интеграция с платформой виртуализации позволяет развивать виртуальную инфраструктуру без каких-либо ограничений и получать дополнительные возможности защиты.

www.kaspersky.ru