Защита центров обработки данных

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД ЗАЩИТА БЕЗ АГЕНТА

Новые возможности и полная интеграция с VMWare NSX

Сегодня все больше компаний используют преимущества новых технологий и внедряют программно-определяемые центры обработки данных (ЦОД), которые нуждаются в надежной защите без ущерба для производительности.

В новой версии Kaspersky Security для виртуальных сред | Защита без агента значительно усовершенствовано взаимодействие программно-определяемого центра обработки данных на базе VMware NSX с защитным решением – теперь они расширяют возможности друг друга, при этом защита становится еще более интеллектуальной, быстрой и эффективной.

Новые возможности и технологии защиты:

Интеграция с VMware NSX ***НОВИНКА***

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО БЕЗ УСТАНОВКИ АГЕНТА

Каждая виртуальная машина под управлением VMware NSX мгновенно обеспечивается надежной защитой от вредоносного ПО. При этом не требуется устанавливать агента на каждую машину.

ЗАЩИТА ОТ СЕТЕВЫХ АТАК

Возможности обнаружения и предотвращения вторжений (IDS/IPS) также распространяются на виртуальные хосты под управлением платформы VMware NSX. Благодаря им виртуализированная инфраструктура надежно защищена от самых сложных сетевых угроз и уязвимостей нулевого дня.

АВТОМАТИЧЕСКОЕ РАЗВЕРТЫВАНИЕ

Тесная интеграция с VMware NSX позволяет полностью автоматизировать процесс развертывания компонентов решения. Виртуальные машины защиты и блокировщики сетевых атак в автоматическом режиме запускаются на гипервизоре в соответствии с политиками безопасности каждой виртуальной машины.

ПОЛИТИКИ БЕЗОПАСНОСТИ

Тесная интеграция с VMware NSX означает, что у каждой виртуальной машины появляются индивидуальные, точно настроенные средства и методы защиты. Эта функция способствует созданию и масштабированию хорошо сбалансированных программно-определяемых ЦОД.

ТЕГИ БЕЗОПАСНОСТИ

Kaspersky Security для виртуальных сред и платформа VMware NSX теперь обмениваются тегами безопасности, которые могут изменяться по специальным правилам (например, при обнаружении вредоносного ПО в виртуальной машине). Постоянное взаимодействие между инфраструктурой и средством ее защиты означает, что программно-определяемый центр обработки данных может реагировать в режиме реального времени на любой инцидент безопасности. При необходимости ЦОД может автоматически запустить изменение конфигурации всей виртуальной инфраструктуры.

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY NETWORKING AND SECURITY

CITRIX READY

Полная проверка инфраструктуры в режиме Защита без агента ***НОВИНКА***

Традиционные решения не могут провести проверку на наличие вредоносного ПО, даже если агент установлен на виртуальную машину, но сама машина выключена или остановлена. В новой версии Kaspersky Security для виртуальных сред | Защита без агента появился расширенный набор функций. С его помощью можно проверять как включенные, так и выключенные виртуальные машины. В результате проверка по требованию становится эффективнее и лучше, а вся инфраструктура – безопаснее.

Режимы Full и Server Core

Решение Kaspersky Security для виртуальных сред | Защита без агента поддерживает операционные системы Windows Server, работающие в режимах Full и Server Core. Это особенно важно сейчас, когда компании разворачивают все больше серверов с критически важной инфраструктурой без пользовательского интерфейса в режиме Server Core (например, контроллеры домена, DHCP, DNS).

Серверы интеграции для крупных инфраструктур

Выделенный сервер интеграции в решении Kaspersky Security для виртуальных сред может быть подключен сразу к нескольким серверам VMware vCenter, чтобы получать больше данных от вашей виртуальной инфраструктуры на базе VMware.

Расширенный SNMP-мониторинг

В решение Kaspersky Security для виртуальных сред теперь встроен SNMP-агент. Он отслеживает и передает исчерпывающую информацию о состоянии виртуальных устройств безопасности корпоративным системам мониторинга, например Zabbix или Nagios. SNMP-счетчики включают общие метрики виртуальных машин защиты (данные о процессоре, оперативной памяти и т. д.), а также конкретные метрики.

Поддержка vShield Endpoint

Большое количество компаний переходят или планируют переходить на платформу VMware NSX. Однако есть те, кто все еще используют предыдущую технологию – vShield Endpoint. Решение Kaspersky Security для виртуальных сред | Защита без агента версии 4.0 интегрируется с платформой NSX, но в нашем решении мы оставляем поддержку vShield Endpoint. Мы обязуемся и дальше поддерживать эту технологию, пока она необходима нашим клиентам. Мы обеспечиваем защиту всего корпоративного программно-определяемого ЦОД, вне зависимости от того, как меняется ваша стратегия ИТ.

Kaspersky Security для виртуальных сред | Защита без агента – еще быстрее, еще эффективнее, еще надежнее.

РЕШЕНИЯ ДЛЯ ЗАЩИТЫ КРУПНОГО БИЗНЕСА:
kaspersky.ru/enterprise

KASPERSKY lab