VMware vShield Endpoint

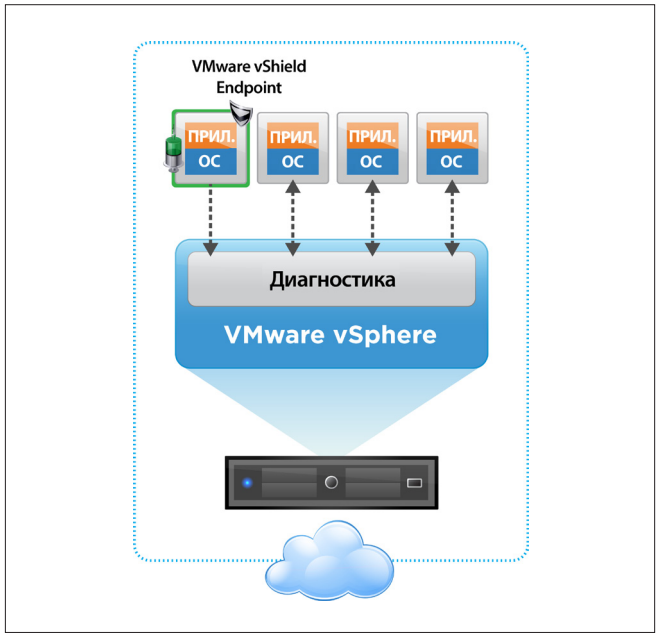
Повышение безопасности терминалов и производительности виртуальных ЦОД

КРАТКОЕ ОПИСАНИЕ

VMware vShield™ Endpoint укрепляет защиту виртуальных машин и многократно увеличивает производительность средств защиты терминалов. vShield Endpoint переносит операции защиты от вирусов и вредоносного ПО в выделенное виртуальное устройство безопасности, предоставляемое партнерами VMware. Решение разработано для эффективного использования имеющихся инвестиций и обеспечивает управление политиками защиты от вирусов и вредоносного ПО с помощью интерфейсов управления, которые уже применяются для обеспечения безопасности физических сред.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Улучшение коэффициентов консолидации и производительности благодаря удалению агентов защиты от вирусов из гостевых ВМ.
- Оптимизация развертывания и мониторинга средств защиты от вирусов и вредоносного ПО в средах VMware.
- Повышение безопасности за счет консолидации антивирусных агентов с целью уменьшения уязвимости.
- Выполнение нормативов и требований аудита благодаря журналам операций, создаваемым средствами защиты от вирусов и вредоносного ПО.



vShield Endpoint повышает производительность и коэффициенты консолидации для средств защиты от вирусов и вредоносного ПО.

Общие сведения о vShield Endpoint

vShield Endpoint совершает революцию в защите гостевых виртуальных машин от вирусов и вредоносного ПО. Это решение оптимизирует антивирусное ПО и другие средства защиты терминалов в средах VMware vSphere® и VMware View™.

vShield Endpoint повышает производительность путем переноса операций защиты от вирусов с каждой виртуальной машины в виртуальное устройство безопасности, включающее системы сканирования на наличие вирусов, а также сохраненные сигнатуры вирусов. Такая архитектура устраняет нагрузку программных агентов на гостевые виртуальные машины, освобождает системные ресурсы, улучшает производительность и исключает риск возникновения антивирусных «штормов» (перегрузки ресурсов во время плановых операций сканирования и обновления сигнатур). Поскольку виртуальное устройство безопасности не отключается, в отличие от гостевых виртуальных машин, оно может постоянно обновлять сигнатуры вирусов, обеспечивая непрерывную защиту виртуальных машин на узле. Кроме того, новые виртуальные машины (или существующие виртуальные машины, которые ранее были отключены) немедленно получают защиту благодаря актуальным сигнатурам.

vShield Endpoint повышает безопасность с помощью виртуального устройства безопасности, защищенного от несанкционированного вмешательства (предоставляется партнерами VMware). Эта виртуальная машина использует надежные и безопасные средства анализа гипервизоров vSphere, которые предотвращают несанкционированное вмешательство в работу самих служб защиты от вирусов и вредоносного ПО.

Кроме того, vShield Endpoint предоставляет партнерам VMware интерфейсы, которые обеспечивают не только сканирование файлов, но и сканирование памяти и процессов. Организации могут одновременно использовать несколько решений по обеспечению безопасности, например обнаружение конфиденциальных данных VMware vShield App with Data Security в одном виртуальной устройстве и средство защиты от вирусов в другом виртуальном устройстве.

Демонстрация соответствия нормативам и выполнение требований аудиторов обеспечивается подробными журналами операций, создаваемыми службами защиты от вирусов и вредоносного ПО.

Администраторы могут централизованно администрировать vShield Endpoint из консоли vShield Manager, входящей в основной комплект. Эта консоль поддерживает прозрачную интеграцию с VMware vCenter™ Server для унифицированного управления системой безопасности виртуальных ЦОД.

Принципы работы vShield Endpoint

vShield Endpoint интегрируется с vSphere и состоит из трех компонентов.

- Виртуальные устройства безопасности (предоставляются партнерами VMware)
- Тонкий» агент для виртуальных машин, обеспечивающий перенос событий системы безопасности (входит в VMware Tools)
- Модуль гипервизора VMware Endpoint ESX® для обмена данными между первыми двумя компонентами на уровне гипервизора

Например, в случае антивирусного решения vShield Endpoint отслеживает события файлов виртуальных машин и уведомляет систему защиты от вирусов, которая выполняет сканирование и возвращает их расположение. Решение поддерживает сканирование файлов по требованию (по расписанию) и при обращении, которое инициируется антивирусной системой в виртуальном устройстве безопасности.

Если потребуется устранение проблем, администраторы смогут задать необходимые действия с помощью имеющихся средств защиты от вирусов и вредоносного ПО. При этом vShield Endpoint будет управлять действиями по устранению проблем на затронутых виртуальных машинах.

Использование vShield Endpoint

Консоль управления, предоставленная партнером VMware, используется для настройки и администрирования партнерского ПО, размещенного в виртуальном устройстве безопасности. Партнеры VMware предоставляют интерфейс, который делает управление (в том числе управление политиками) похожим на управление ПО, размещенным на выделенном физическом устройстве безопасности.

Нагрузка на администраторов виртуальной инфраструктуры существенно сокращается, поскольку на виртуальных машинах отсутствуют антивирусные агенты, которыми необходимо управлять. Вместо этого для управления виртуальным устройством безопасности используется партнерская консоль управления. Кроме того, такой подход помогает устранить необходимость в частом обновлении виртуальных машин. С точки зрения развертывания VMware Tools включает «тонкий» агент и модуль ESX, который обеспечивает диагностику гипервизора.

Администраторы виртуальной инфраструктуры получают удобный мониторинг сред, например для проверки правильности работы решения по защите от вирусов.

Основные возможности

Освобождение от операций защиты от вирусов и вредоносного ПО

- vShield Endpoint повышает производительность благодаря модулю vShield Endpoint для ESX, который переносит операции антивирусного сканирования в виртуальное устройство безопасности, выполняющее сканирование.
- Такие задачи, как сканирование файлов, памяти и процессов, переносятся с виртуальных машин в виртуальное устройство безопасности с помощью «тонкого» агента и партнерского модуля ESX.
- vShield Endpoint EPSEC обеспечивает управление подключениями между обычными виртуальными машинами и виртуальным устройствам безопасности с помощью средств диагностики на уровне гипервизора.
- Антивирусная система и файлы сигнатур обновляются только на виртуальном устройстве безопасности, однако политики могут применяться ко всем виртуальным машинам на узле vSphere.

Исправление

- Политики vShield Endpoint определяют, нужно ли удалить вредоносный файл, поместить его в карантин или обработать иным образом.
- Агент управляет операциями исправления файлов в пределах виртуальной машины.

Интеграция с партнерскими решениями

- API-интерфейс EPSEC дает партнерам VMware по антивирусным решениям возможность интегрировать свои продукты с vShield Endpoint, предоставляя анализ операций гипервизора с файлами. Этот API-интерфейс реализует важные возможности антивируса.

vShield Manager, управление на основе политик и автоматизация

- vShield Manager полностью поддерживает развертывание и настройку vShield Endpoint.
- API-интерфейсы REST обеспечивают настраиваемую автоматическую интеграцию возможностей vShield Endpoint с решениями.
- Предоставляются отчеты о мониторинге.
- vShield Manager можно использовать как подключаемый модуль vCenter.

Журналы и аудит

- Ведение журналов и аудит на основе стандартного формата syslog

Поддерживаемые версии

Сведения о поддерживаемых версиях сред vSphere, ESX и View см. по адресу http://vmware.com/products.

Связанные продукты

Семейство продуктов vShield для обеспечения безопасности включает также VMware vShield Edge для защиты периметра, vShield App with Data Security для защиты приложений от сетевых атак и обнаружения конфиденциальных данных, vShield Manager и пакет vShield Bundle, включающий все продукты.

Дополнительная информация

Для получения информации или приобретения продуктов VMware обращайтесь по телефону +7(495) 970-1746, посетите страницу www.vmware.com/ru/products или найдите уполномоченного торгового посредника на сайте VMware. Подробные технические характеристики и системные требования продукта можно найти в руководстве администратора VMware vShield по адресу http://www.vmware.com/pdf/vshield_41_admin.pdf.

Дополнительные сведения о продуктах vShield см. по адресу http://vmware.com/ru/products.

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Тел.: (877) 486-9273 Факс: (650) 427-5001 www.vmware.com
121099, Россия, Москва, Смоленская площадь, 3 Тел.: +7(495) 970-1746 Факс: +7(495) 970-1748 www.vmware.ru