Безопасность систем виртуализации

Особенности, проблемы, преимущества

Виртуализация вычислительных мощностей — ключевая тенденция последних лет

В настоящее время нет ни одного проекта построения центра обработки данных, который не включал бы в себя виртуализацию. Даже небольшие компании, закупающие два-три сервера, чаще всего планируют разворачивать на них не операционные системы общего назначения (Windows, Linux и т.д.), а гипервизор одной из платформ виртуализации, ведь переход в виртуализацию несет в себе такие преимущества как:

- Снижение расходов на оборудование и энергопотребление
- Консолидацию серверов и рабочих станций
- Более эффективное использование ресурсов
- Гибкость и масштабируемость ИТ-инфраструктуры

Виртуализация и защита информации

До сих пор многие специалисты считают что среда виртуализации, являясь, по сути, аналогом физической локальной сети, не требует какого-то специального подхода к защите информации, что позволяет обойтись «традиционными» средствами. Так, для защиты виртуальных серверов и VDI часто применяют обычные корпоративные антивирусы, аппаратные межсетевые экраны и системы предотвращения вторжений.

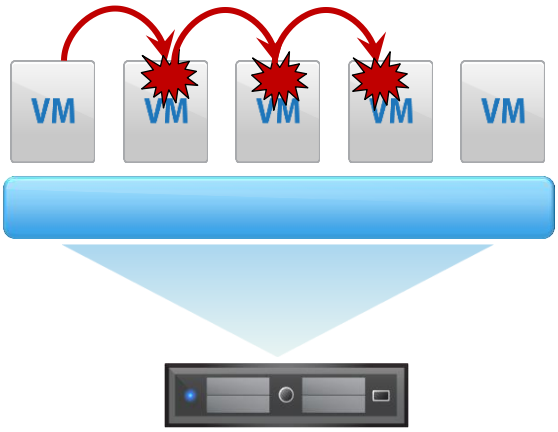
На самом же деле, при использовании виртуальных вычислительных ресурсов вопрос защиты информации встаёт еще более остро. Использование виртуализации не просто не отменяет все угрозы, присущие физической инфраструктуре локальных сетей, а еще и добавляет новые возможности для атак злоумышленников, которые теперь могут использовать особенности и уязвимости самой платформы виртуализации.

Если большинство администраторов ИТ и ИБ, в компаниях которых виртуализация успешно внедрена и используется, осознают возрастающие риски подобных технологий, то им часто не хватает информации о специальных средствах защиты.

Несмотря на то, что рынок виртуализации и средств защиты виртуальных сред активно развивается и все больше производителей средств защиты стараются предложить свои решения для защиты виртуализации, большинство этих решений не самодостаточны. Таким образом, для полноценной защиты виртуальных машин, работающих на ESX/ESXi-серверах, приходится применять несколько различных решений — антивирус, межсетевой экран, систему предотвращения вторжений, программное обеспечение для контроля доступа к объектам виртуальной инфраструктуры. Очевидными минусами такого подхода являются: сложность внедрения и обслуживания, множество консолей управления, высокая совокупная стоимость владения, трудности с аудиторской отчетностью и выполнением требований регуляторов и Российского законодательства.

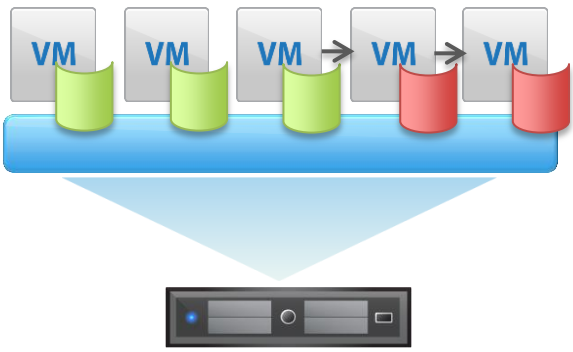
3 Проблемы безопасности, не решаемые стандартными средствами

- Сетевой трафик между виртуальными машинами – нет видимости.



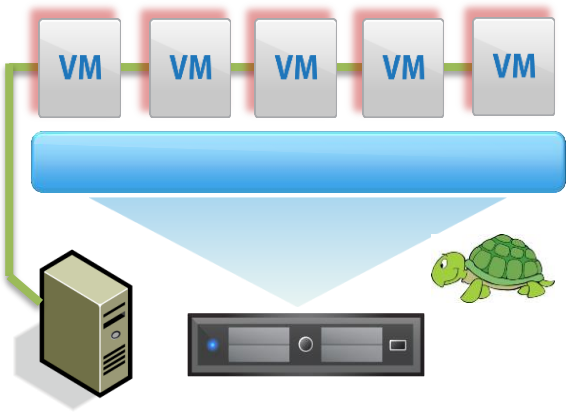
Если в физических локальных сетях передача любого трафика между рабочими станциями возможна лишь через специальные узлы сети (маршрутизаторы, хабы, свитчи, коммутаторы), то в виртуальной среде присутствует трафик которым рабочие станции и сервера обмениваются напрямую между собой. Внешние сетевые системы безопасности не применимы для защиты систем виртуализации, так как они «не видят» сетевого трафика, передаваемого между виртуальными машинами внутри платформы виртуализации.

- Бреши в защите в момент включения виртуальных машин.



Виртуальные сервера и рабочие станции гораздо чаще физических вводятся и выводятся из эксплуатации, часто хранятся выключенными в виде файлов, не редко доступ к ним предоставляется по требованию. Разумеется, что внутри выключенных виртуальных машин не устанавливаются обновления прикладного ПО и сигнатур антивируса, т.к. выключенных виртуальных машин для «традиционных» средств защиты, например антивируса - просто не существует.

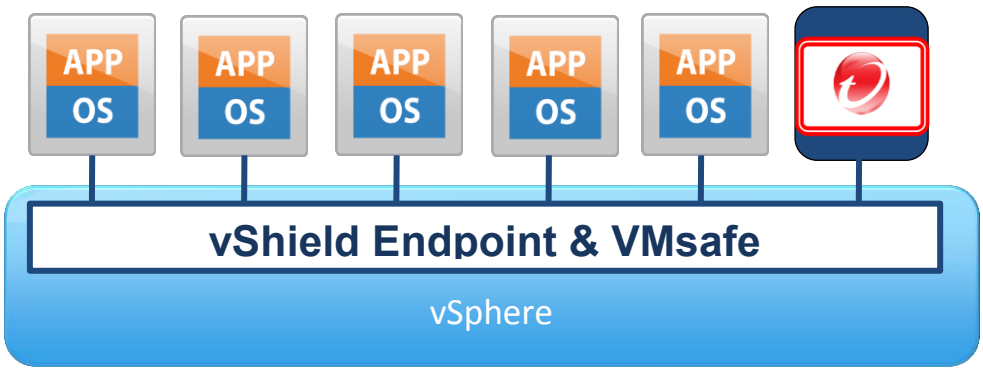
- Конфликт ресурсов, «антивирусный шторм»



В наши дни антивирус на каждом сервере и рабочей станции уже практически не снижает производительности самой системы. В среде виртуализации ситуация несколько иная, т.к. на одной аппаратной платформе может быть развернуто множество виртуальных серверов и рабочих станций. При одновременном сканировании хотя бы части виртуальных ресурсов производительность платформы значительно снижается. Традиционный антивирус хранит экземпляр антивирусной базы в каждой виртуальной машине и не учитывает, что защищаемые узлы размещены на одной аппаратной платформе (физическом сервере).

Решение

Сегодня на рынке средств виртуализации действует несколько серьёзных компаний, среди которых Microsoft, Citrix, Red Hat и другие. Но пока лишь компания VMware для своей линейки продуктов VMware vSphere предложила интерфейсы VMware vShield Endpoint и VMsafe. Эти интерфейсы позволяют сторонним производителям защитных программ организовать защиту виртуальных систем на уровне гипервизора VMware ESX/ESXi, без необходимости установки на каждую виртуальную систему, работающую на ESX/ESXi-хосте полноценного агента защиты. А интеграция с системой управления vCenter позволяет системе защиты обладать всей информацией о виртуальной инфраструктуре, в том числе и о неактивных виртуальных машинах. Все эти преимущества приводят к созданию всё большего количества проектов с применением виртуализации, функционирующих на базе VMware vSphere.



На прочих платформах виртуализации полноценный безагентский подход к защите, на сегодняшний день не возможен, т.к. разработчики этих платформ не предоставляют интерфейсов аналогичных vShield и VMsafe для разработчиков средств защиты, которые вынуждены использовать другие методы решения вышеописанных проблем.

Подход Trend Micro. DeepSecurity – комплексная защита виртуальных сред

Trend Micro Deep Security это решение для всесторонней защиты физических серверов и виртуальных машин, в состав которого входят следующие модули:

- Anti-malware & Web Reputation — Антивирусная защита и репутационный анализ веб-ресурсов;
- Intrusion Prevention & Firewall — Система предотвращения вторжений и Межсетевой экран; глубокий анализ пакетов, виртуальный патчинг (блокировка уязвимостей еще до выпуска соответствующих исправлений);
- Integrity Monitoring — Контроль над важными файлами операционных систем и приложений, например каталогами, разделами и параметрами реестра, для выявления вредоносных и незапланированных изменений в режиме реального времени. Контроль целостности гипервизора;
- Log Inspection — Сбор данных и анализ журналов операционной системы и приложений с целью обнаружить подозрительную активность, события в системе безопасности и действия администратора в масштабах всего центра обработки данных.

Дополнительно доступны расширения:

- Deep Security Manager Multi-tenancy mode, предназначен для поставщиков услуг, предлагающих в аренду виртуальные вычислительные мощности;
- Secure Cloud, предназначен для шифрования всей виртуальной машины при размещении ее в не доверенной среде, например в «публичном» облаке.

DeepSecurity позволяет:

- Выполнить требования регуляторов, федеральных законов и отраслевых стандартов, таких как PCI DSS для банков и 152-ФЗ для компаний, обрабатывающих персональные данные
- Отражать атаки злоумышленников и блокировать активность известных и неизвестных вредоносных программ, используя нейтрализацию уязвимостей в программном обеспечении еще до выхода официальных «заплаток» от производителя
- Выявлять скрытые атаки и активность необнаруженных вирусов, благодаря контролю целостности, блокировке сетевого трафика неавторизованных приложений а также выявлению подозрительной сетевой активности
- Транслировать информацию о найденных угрозах на остальные решения Trend Micro благодаря интеграции с глобальной сетью Smart Protection Network
- Предельно упростить управление безопасностью всего серверного парка, благодаря централизованному управлению защитой физических и виртуальных серверов, функцией автоматической настройки правил безопасности, а также тесной интеграцией с платформой VMware, что позволяет автоматически обеспечивать защитой все появляющиеся виртуальные машины
- Минимизировать влияние защиты на производительность платформы виртуализации и высвободить дополнительные ресурсы, благодаря глубокой интеграции с гипервизором VMware

Ключевые преимущества

- Сертификация ФСТЭК позволяет использовать продукт для защиты персональных данных любого типа, конфиденциальной информации, а также промышленных систем
- Высокая производительность решения в среде VMware, благодаря тесной интеграции с платформой, а также таким технологиям, как дедупликация сканирования, позволяющая избежать повторной проверки одного и того же файла в разных виртуальных машинах, дающая более чем десятикратный прирост скорости при проверке
- Виртуальный патчинг, позволяющий защититься от самого широкого спектра угроз, проникающих в сеть через уязвимости в прикладном программном обеспечении
- Сканер на рекомендации, позволяющий в автоматическом режиме оптимально настроить защиту каждого сервера, по результатам его анализа
- Сквозная защита всего серверного парка, включая традиционные и виртуальные сервера, а также системы VDI; Обеспечивается защитой не только платформа Windows, но и Linux, и другие разновидности UNIX
- Модульная архитектура, позволяющая выбрать защиту от традиционных атак, неизвестных и новых атак «нулевого дня», а также специфичных угроз, характерных для виртуальных и облачных сред

Deep Security поставляется на рынок более 7 лет и за это время, решение Trend Micro, стало признанным лидером средств обеспечения безопасности традиционных и виртуализованных центров обработки данных, а также облачных систем. Среди заказчиков есть как небольшие организации, так и крупнейшие предприятия, среди которых ГК Норильский Никель, ФНС России, ЦБ РФ и многие другие. Даже сама компания VMware использует Deep Security для защиты своих внутренних ресурсов.

Подробнее о решении: http://www.trendmicro.com.ru/products/deep-security/index.html