TEST REPORT
Tolly.

#211101
Февраль 2011
По поручению Trend Micro, Inc.

Сравнение решения Trend Micro Deep Security 7.5 с продуктами McAfee и Symantec

Производительность антивируса в виртуальных средах VMware ESX

Общая информация

Виртуализация серверов и настольных компьютеров является неотъемлемой частью любой ИТ-стратегии, ориентированной на снижение капитальных и эксплуатационных затрат. В погоне за внедрением технологий виртуализации многие организации попросту развертывают то же самое антивирусное решение, которое использовалось на физическом сервере и в настольных системах. Поскольку традиционные антивирусные решения не предназначены для работы в виртуальных средах, они могут вызвать значительные проблемы при эксплуатации (например, «антивирусные штормы», потеря ресурсов и административные накладные расходы) и свести на нет усилия по достижению максимальной плотности размещения виртуальных машин в организациях.

Компания Trend Micro, Inc. поручила независимой тестовой лаборатории Tolly оценить производительность решения Trend Micro Deep Security в виртуальных средах и сравнить ее с производительностью программ McAfee Total Protection for Endpoint и Symantec Endpoint Protection 11.0. Особое внимание уделялось воздействию каждого из решений на ресурсы системы хоста (физического сервера) при увеличении плотности гостевых машин до 100 виртуальных машин (ВМ), одновременно запущенных в среде VMware ESX 4.1.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

Решение Trend Micro Deep Security:

1. Продемонстрировало более низкий уровень нагрузки на хост, оперативную память и подсистему дискового ввода-вывода по сравнению с традиционными решениями на основе агента, даже во время пиковых нагрузок
2. Успешно справилось с проблемой «антивирусных штормов» во время сканирования по расписанию и обновления сигнатур, в отличие от конкурентных решений, которые не способны работать с нагрузкой, превышающей 25 виртуальных машин
3. Обеспечило повышение уровня плотности виртуальной среды в диапазоне от 29% до 275% по сравнению с McAfee и Symantec с учетом тестовых рабочих нагрузок

Тестирование показало, что решение Trend Micro Deep Security, специально разработанное для защиты виртуальных сред и не требующее установки агента, потребляет меньше ресурсов процессора, оперативной памяти и подсистемы дискового ввода-вывода, чем традиционные решения, в рамках которых работа антивирусных агентов и вычисления осуществлялись на каждой ВМ под управлением Windows 7.

Традиционные антивирусные решения использовали в 1,7-8,5 раза больше ресурсов по сравнению с решением Trend Micro при тестировании в режиме обычной нагрузки на систему. Кроме того, они не справились с проблемой «антивирусных штормов» во время пиковых нагрузок (т. е. выполнения сканирования по требованию и обновления сигнатур), когда одновременно запускались операции на 25 ВМ. Традиционные решения не учитывали особенностей виртуальной среды, поэтому при попытке восстановить ВМ, опирающиеся на одни и те же аппаратные ресурсы, происходил всплеск потребности в ресурсах хоста (например, ЦП и памяти). В частности, запрос на сканирование или обновление файлов сигнатур на 25 виртуальных машинах приводил к тому, что все без исключения виртуальные машины начинали выполнять эту задачу одновременно.

Экономия потребляемых ресурсов при использовании Trend Micro Deep Security позволяет организациям увеличить плотность размещения виртуальных машин (т. е. количество ВМ, которые можно запустить на хосте). Это обеспечивает снижение капитальных и эксплуатационных расходов. Повышение плотности ВМ возможно благодаря тому, что, по сравнению с продуктами McAfee и Symantec, решение Trend Micro потребляет меньше ресурсов, а также исключает вероятность возникновения эффекта «антивирусного шторма» в тестах со специализированной рабочей нагрузкой, которая варьируется от 29% (нагрузка, не вызывающая напряженной работы антивируса) до 275% (во время «антивирусных штормов»).

Инженеры Tolly оценили потребление ресурсов системой защиты, применив различные рабочие нагрузки с одновременным включением до 100 виртуальных машин. Базовый уровень был установлен с помощью рабочей нагрузки, моделирующей различные действия конечного пользователя в системах, где не установлено решение по защите конечных точек, и измерения потребления ресурсов.

Тестирование включало в себя оценку потребления ресурсов при выполнении конкретных задач антивируса (сканирование по требованию и обновление сигнатур), а также в условиях обычной пользовательской нагрузки при наличии антивирусной защиты на каждой виртуальной машине.

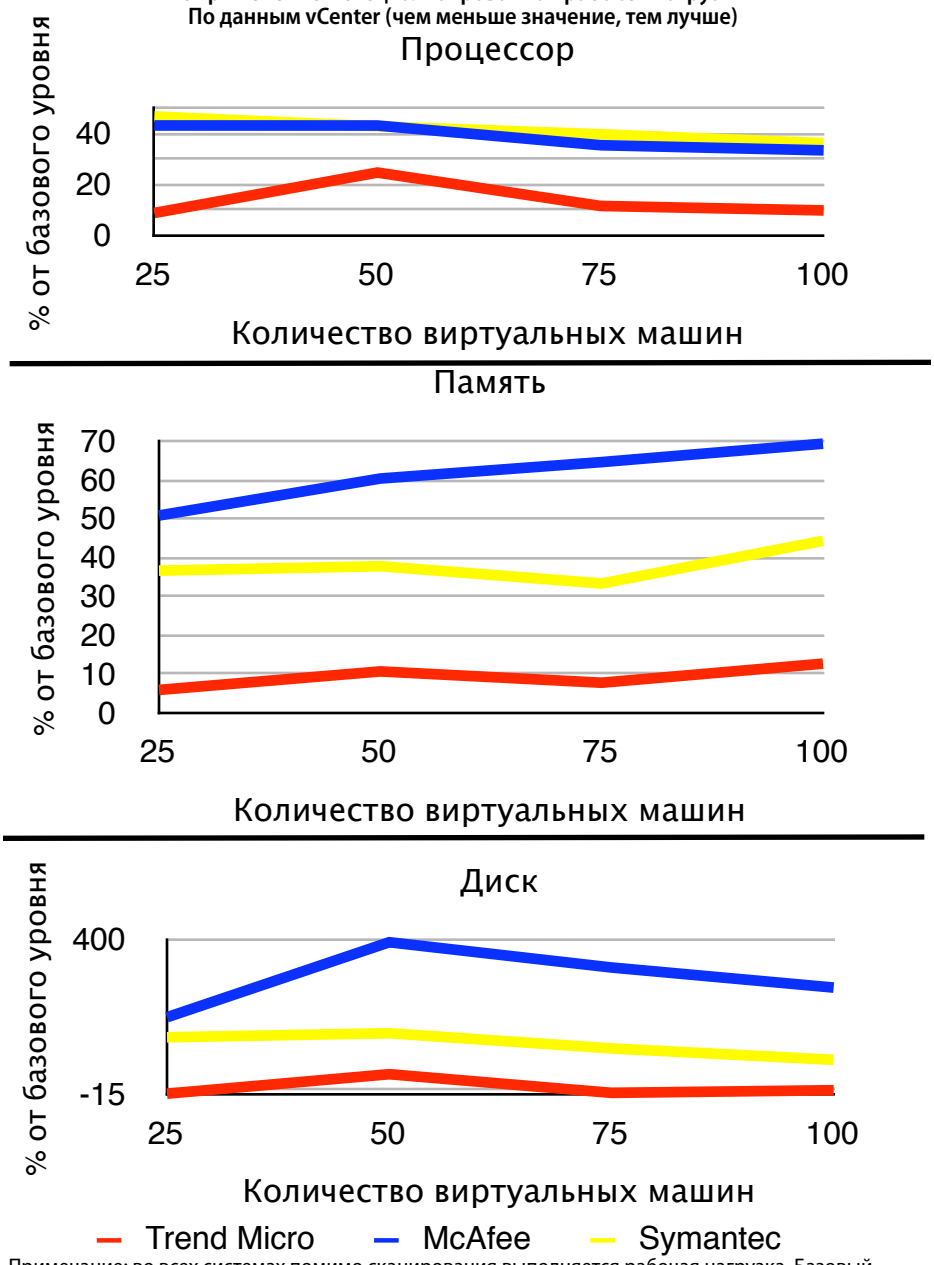
Использование ресурсов антивирусом с моделированием рабочей нагрузки (25–100 виртуальных машин)

На рисунке 1 показаны средние уровни потребления ключевых системных ресурсов на сервере VMware ESX при применении основной тестовой нагрузки и одновременной работе максимум 100 виртуальных машин. Отдельные частные значения см. в таблице 4.

Эти цифры включают как ресурсы, использованные виртуальными машинами, так и ресурсы, задействованные виртуальным устройством Deep Security. Подробные сведения о рабочих нагрузках и среде см. в разделе «Методология тестирования и настройка испытательного стенда».

Решения McAfee и Symantec требовали выполнения отдельного экземпляра антивирусного агента на каждой виртуальной машине. Для Trend Micro Deep Security необходим один экземпляр виртуального устройства на каждом хосте. На рисунке показано, как используется центральный процессор, память и диск на всех уровнях плотности ВМ и в отношении всех трех ресурсов. Продукты Symantec и McAfee потребляли в 1,7-8,5 раз больше ресурсов, чем решение Trend Micro.[1]

Потребление ресурсов хоста антивирусом VMware ESX 4.1 в сравнении с базовым уровнем
При наличии максимум 100 виртуальных машин под управлением Microsoft Windows 7 с применением специализированной рабочей нагрузки
По данным vCenter (чем меньше значение, тем лучше)



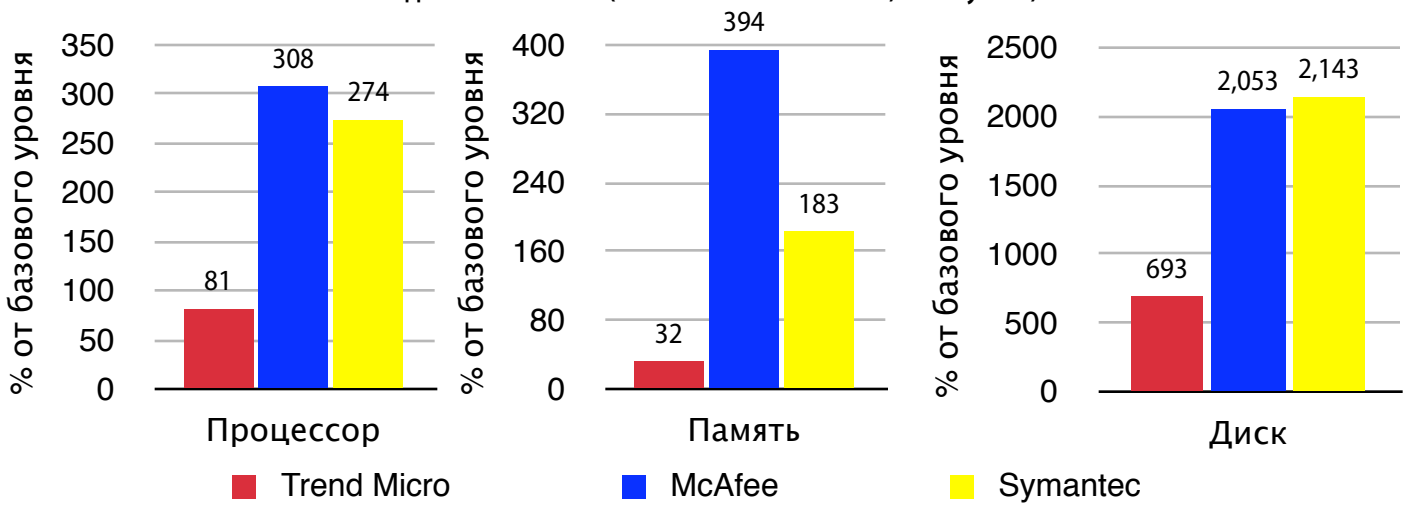
Примечание: во всех системах помимо сканирования выполняется рабочая нагрузка. Базовый уровень – специализированная рабочая нагрузка без установленного решения по защите конечных точек. Базовые значения и подробные результаты см. в тексте отчета. Использование ресурсов, превышающее базовый уровень, рассчитывается путем вычитания из результата значения базового уровня, деления на величину базового уровня и умножения на 100. Поскольку продукт McAfee не смог пройти тестирование на 100 ВМ, показатели для 100 машин были экстраполированы исходя из результатов тестов на 25, 50 и 75 ВМ. Вычисляются средние значения за 30 минут работы. Показатели использования ресурсов диска варьируются в пределах 30% и приведены только в качестве справочной информации.

Источник: Tolly, октябрь 2010 г.

Рисунок 1

[1] Решение McAfee не смогло пройти тест на 100 ВМ, несмотря на многочисленные попытки и повторные запуски. Инженеры компании Tolly экстраполировали показатели этого продукта для 100 ВМ на основании результатов тестирования на 25, 50 и 75 ВМ.

Потребление ресурсов хоста антивирусом VMware ESX4.1 в сравнении с базовым уровнем
Запрос о сканировании по требованию 25 виртуальных машин под управлением Microsoft Windows 7
По данным vCenter (чем меньше значение, тем лучше)



Примечание: во всех системах помимо сканирования выполняется рабочая нагрузка. Базовый уровень – специализированная рабочая нагрузка без установленного решения по защите конечных точек. Значения базового уровня: средняя частота ЦП = 4109,76 МГц, средний объем ОЗУ = 7893,28 МБ, средняя скорость работы с диском = 1741,23 КБ/с. Решение Trend Micro автоматически выполняет только одно сканирование за раз. Продукты других поставщиков запускали 25 процессов сканирования одновременно. Каждый поставщик рекомендует различные методы (например, рандомизацию для выравнивания нагрузки при сканировании по требованию). Подробные сведения см. в тексте отчета. Использование ресурсов, превышающее базовый уровень, рассчитывается путем вычитания из результата значения базового уровня, деления на величину базового уровня и умножения на 100. Вычисляются средние значения за 30 минут работы.

Источник: Tolly, октябрь 2010 г.

Рисунок 2

Тестирование антивируса при сканировании по требованию (25 ВМ)

Инженеры оценили реакцию каждого продукта на запрос системы управления безопасностью о полном сканировании 25 виртуальных машин. Одновременное сканирование является ресурсоемкой задачей и может негативно отразиться на работе пользователей.

Оценка Trend Micro Deep Security производилась в условиях среды, в которой ресурсы использовались всеми ВМ, а автоматически запланированные сканирования происходили последовательно (не более чем на одной машине за 1 раз). В результате система Deep Security успешно прошла тестирование на 25 и 50 ВМ. Исходя из потребления ресурсов во время этих тестов, компания Tolly прогнозирует, что решение Trend Micro может поддерживать работу более чем со 100 ВМ.

Другие решения (не учитывающие особенности виртуальной среды) по умолчанию пытались выполнить одновременное сканирование на всех 25 машинах. На рисунке 2 представлены средние значения использования ресурсов в этих тестах. Продукту McAfee потребовалось в 2,8 раза больше ресурсов ЦП и в 11 раз больше оперативной памяти, чем Trend Micro. Уровень использования ресурсов ЦП для решения Symantec в 2,4 раза превысил уровень Trend Micro (в 4,7 раза по объему оперативной памяти).

Кроме того, совокупность данных для продуктов Symantec и McAfee на 25 ВМ не дает полной картины в отношении надежности и удобства работы пользователей. Всплеск потребности в ресурсах у решений McAfee и Symantec часто замедлял работу пользовательских систем. В частности, ни Symantec, ни McAfee не удалось протестировать в среде, включающей более 25 ВМ. При тестировании продукта Symantec два агента потеряли соединение с управляющим сервером, а задержка при работе с диском (не указана на рисунках) в среднем составила 31 мс. При выполнении сценария сканирования по требованию с применением решения McAfee средняя задержка при работе с диском была равна 80 мс. В ходе проверки 14 из 25 пользователей не имели доступа к своим настольным компьютерам. Дополнительные комментарии см. в таблице 2.

Поставщики традиционных решений обычно рекомендуют два метода предотвращения конкуренции за ресурсы в виртуальной среде: рандомизацию и группировку. Ни один из этих подходов не учитывает особенностей виртуализации и, таким образом, оказывается за рамками данного тестирования.

Администратор может настроить период рандомизации так, чтобы конечные точки выполняли задачи, случайным образом выбирая время начала. Если задачи требуют много времени (например, полное сканирование), этот период должен быть очень большим (более дня или недели, в зависимости от плотности ВМ в хосте), чтобы увеличить

вероятность раздельного выполнения задач клиентом. В результате, столкнувшись с критической угрозой безопасности, администраторы предприятия могут не иметь возможности быстро восстановить свои системы. Задачи, запланированные случайным образом, могут также снизить удобство работы пользователей, если будут выполняться в условиях значительной нагрузки на систему.

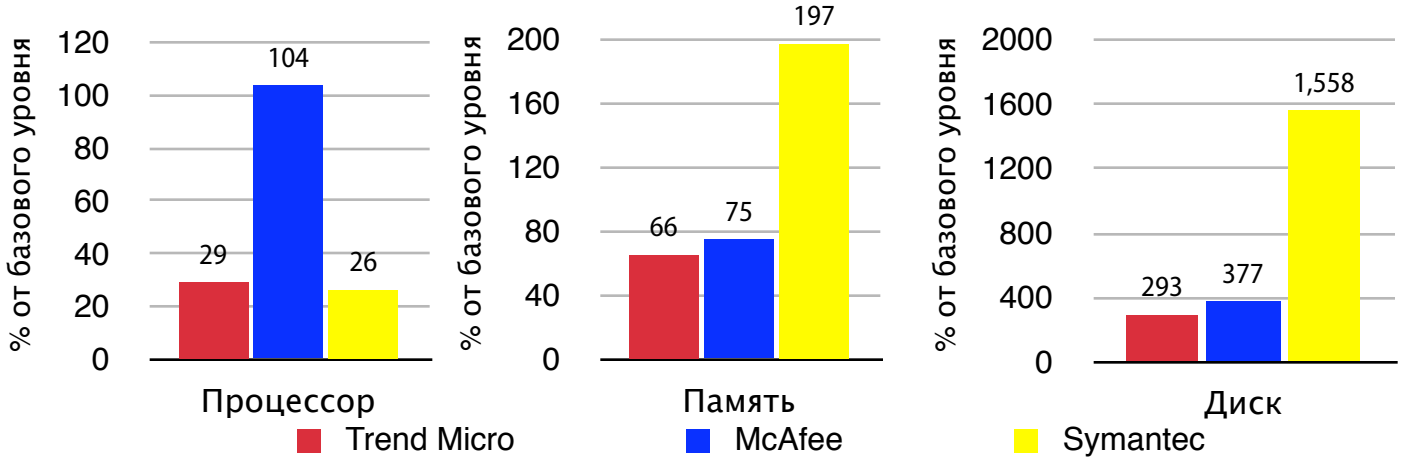
Масштабируемость антивирусного решения в среде VMware ESX 4.1
Сканирование по требованию ВМ под управлением Microsoft Windows 7

Поставщик	Продукт	Количество виртуальных машин, выбранных для сканирования по требованию			
		25	50	75	100
Trend Micro	Deep Security 7.5	Да, полностью стабилен	Да, полностью стабилен	Да (прогноз, не тестировался)	Да (прогноз, не тестировался)
McAfee	Total Protection for Endpoint	Да, но были проблемы со стабильностью	Из-за нестабильности при выполнении 25 одновременных процессов сканирования инженеры Tolly не пытались увеличить количество ВМ. В клиенте ПО McAfee можно включить функцию рандомизации, которая способна обеспечить распределение нагрузки для запланированных и запущенных вручную задач.		
Symantec	Endpoint Protection 11.0	Да, но были проблемы со стабильностью	Из-за нестабильности при выполнении 25 одновременных процессов сканирования инженеры Tolly не пытались увеличить количество ВМ. Symantec рекомендует настраивать плановые задачи в произвольном порядке. Это приведет к распределению запросов сканирования по требованию по 100 виртуальным машинам, что занимает, по умолчанию, 160 часов. Время начала выполнения задач, запускаемых вручную, не может быть задано произвольно.		

Примечание: решение Trend Micro – единственное из числа протестированных, которое учитывает особенности виртуальной среды и автоматически распределяет задачи сканирования по требованию так, чтобы они выполнялись последовательно.
Источник: Tolly, октябрь 2010 г.

Таблица 1

Потребление ресурсов хоста антивирусным решением VMware ESX 4.1 в сравнении с базовым уровнем
Запрос обновления сигнатур 50 виртуальных машин под управлением Microsoft Windows 7
По данным vCenter (чем меньше значение, тем лучше)



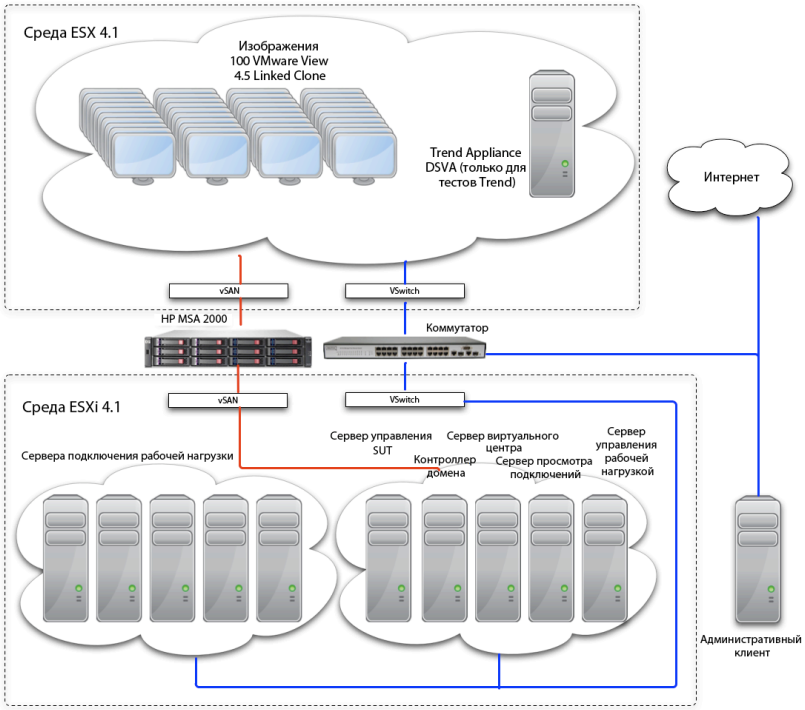
Примечание: во всех системах помимо тестовой задачи выполнялась рабочая нагрузка. Базовый уровень – рабочая нагрузка без установленного решения по защите конечных точек. Значения базового уровня: средняя частота ЦП = 8434,91 МГц, средний объем оперативной памяти = 14119,62 МБ, средняя скорость работы с диском = 2341,41 КБ/с. Решению Trend Micro необходимо лишь загрузить файл сигнатуры на одно виртуальное устройство защиты. Продукты других поставщиков запускали 25 процессов обновления одновременно. Каждый поставщик рекомендует различные методы для выравнивания нагрузки при обновлении. Подробные сведения см. в тексте отчета. Использование ресурсов, превышающих базовый уровень, рассчитывается путем вычитания из результата значения базового уровня, деления на величину базового уровня и умножения на 100. Вычисляются средние значения за 15 минут работы.

Источник: Tolly, октябрь 2010 г.

Рисунок 3

С помощью системы классификации администратор может создавать различные группы ВМ и планировать задачи клиента для этих групп. Этот подход требует усилий со стороны администратора и усложняет управление ИТ-инфраструктурой предприятия. Новые ВМ необходимо распределять по группам вручную. Если ВМ переносятся с одного хоста на другой в целях сбалансированного распределения нагрузки или по другой причине, администраторам придется изменить назначение группы.

Виртуализированная среда тестирования антивируса



Источник: Tolly, октябрь 2010 г.

Рисунок 4

Тестируемые системы

Поставщик	Продукт	Компоненты	Учет особенности виртуальной среды	Реализация
Trend Micro	Deep Security 7.5	Trend Micro Deep Security Manager версии 7.5.1378; Trend Micro Deep Security Virtual Appliance 7.5.0.1600; драйвер фильтра 7.0.0.894; конфигурация по умолчанию. Присвоен заранее настроенный профиль безопасности для защиты Windows от вредоносных программ.	Да	Автоматическая, одно виртуальное устройство. Клиент без агента связывается через VMware vShield API
McAfee	Total Protection for Endpoint	McAfee ePolicy Orchestrator 4.5; McAfee Agent для Windows 4.5.0 дополнительный номер версии 1270; McAfee VirusScan (R) Enterprise 8.7.0 дополнительный номер версии 570 с исправлением Hot Fix 2; McAfee AntiSpyware Enterprise 8.7 дополнительный номер версии 129; McAfee Host Intrusion Prevention 7.0.0 дополнительный номер версии 1070; McAfee SiteAdvisor (R) Enterprise Plus 3.0.0 дополнительный номер версии 476; везде выбраны политики по умолчанию. Отменены клиентские задачи полного сканирования и обновления.	Нет	Традиционный клиент на конечной точке
Symantec	Endpoint Protection 11.0	Версия 11.0.6100.645	Нет	Традиционный клиент на конечной точке

Источник: Tolly, октябрь 2010 г.

Таблица 2

Тест с обновлением сигнатур антивируса (50 ВМ)

Инженеры оценили реакцию каждого решения на запрос об обновлении сигнатур системного антивируса. Хотя эти процессы менее требовательны к ресурсам, чем полное сканирование, они все же снижают производительность и затрудняют эксплуатацию (особенно при выполнении в обычные рабочие часы).

Инженеры запустили сценарий обновления сигнатур на 50 виртуальных машинах. Традиционные решения требовали обновлять файлы сигнатур на каждой виртуальной машине, а система Trend Micro требовала наличия только одной копии файла сигнатуры, которая находилась на виртуальном устройстве Trend Micro Deep Security и применялась для всех ВМ, находящихся под защитой Trend Micro. Таким образом, в то время как традиционные продукты потребляли значительно больше ресурсов процессора или памяти, потребление ресурсов при применении решения Trend Micro было существенно ниже. См. рисунок 3.

Инженеры также отметили, что менеджерам по сетевой безопасности, внедряющим решение Trend Micro, при обновлении сигнатур не нужно беспокоиться о виртуальных машинах, находящихся в режиме оффлайн. Традиционные системы подразумевают, что виртуальные машины для получения обновлений должны находиться в режиме онлайн.

Как и в тесте на синхронное сканирование по требованию, у решений McAfee и Symantec необходимость обработки обновлений на всех 50 виртуальных машинах одновременно вызвала увеличение потребления ресурсов и падение производительности на системном уровне.

В случае Symantec большинство ВМ отправило на станцию управления vCenter VMware уведомления о проблемах с памятью, так как задача обновления сигнатур Symantec полностью задействовала 1 ГБ оперативной памяти, выделенный каждой из машин. 10 из 50 пользователей настольных компьютеров с VMware View были отключены от сети во время тестирования.

Решение McAfee содержало задачу по ежедневному обновлению файлов сигнатур для простаивающих ВМ. Несмотря на то, что инженеры отменили эту задачу, она продолжала автоматически запускаться. Данный факт не учитывался в тесте.

Как и в случае с Symantec, ресурсы, потребляемые при синхронном обновлении 50 ВМ, могут оказаться значительными. Во время некоторых запусков теста использование ресурсов процессора решением VMware ESX оставалось на уровне 100% в течение более чем 10 минут, а производительность виртуализированной системы в целом значительно снизилась.

Сравнение плотности (консолидации) ВМ

В большинстве проектов по виртуализации при расчете масштаба учитываются преимущественно основные рабочие нагрузки ВМ. При этом не принимается во внимание рабочая нагрузка традиционного антивируса, снижающая производительность. В рамках данного теста специалисты Tolly попытались также оценить влияние эффективности антивируса на плотность ВМ. Повышение консолидации можно вычислять в различных условиях: (а) когда антивирус простаивает; и (б) когда антивирусные решения выполняют непосредственные клиентские задачи, такие как сканирование по требованию и обновления сигнатур.

Номинальная плотность ВМ (с простаивающим антивирусом)

Здесь внимание, в основном, уделялось расходу ресурсов на простаивающее антивирусное решение: применялась основная рабочая нагрузка, но конкретная задача антивируса не запускалась. Увеличение плотности ВМ при использовании решения Trend Micro по сравнению с продуктом Symantec составило 34,5% и 29% для ресурсов процессора и памяти, соответственно. Повышение плотности ВМ по сравнению с решением McAfee – 31,4% и 42,4% для ресурсов процессора и памяти. См. таблицу 5.

Trend Micro, Inc.

Deep Security 7.5

Производительность антивируса в среде VMware

Тестирование проведено в октябре 2010 г.

Компоненты тестового стенда для оценки производительности хоста VMware

Компонент	Версия/сборка
VMware ESX	4.1.0
VMware vCenter Server	4.1.0 сборка 258902
VMware View Composer Server	2.1 сборка 277387
VMware View Connection Server	4.5.0
VMware vShield Manager	4.1 build 310451
Аппаратное обеспечение сервера	2x Xeon x5680 (Hexacore) с частотой 3,33 ГГц и 192 Гб ОЗУ DDR 3 (всего 24 логических ядра)
Сеть хранения данных	Система хранения HP StorageWorks MSA, подключенная по оптоволоконному каналу (4 Гб)
Ресурсы гостевой ВМ	1 ГБ ОЗУ и 1 виртуальный процессор (vCPU)
Гостевая операционная система	Microsoft Windows 7 Enterprise

Источник: Tolly, октябрь 2010 г. Таблица 3

Истинная плотность ВМ (полное сканирование)

Использование номинальных значений плотности для простаивающего антивируса не учитывает действия антивируса при пиковой нагрузке. По этой причине при использовании виртуализированной инфраструктуры все чаще происходят «антивирусные штормы», истощающие хост ESX и рабочие нагрузки на ВМ. Во время тестирования выяснилось, что сканирования и обновления антивируса требовательны к ресурсам всех трех видов (процессор, память и диск). От системы и рабочей нагрузки зависит, какой из ресурсов станет слабым звеном.

Увеличение плотности ВМ при использовании решения Trend Micro по сравнению с продуктом Symantec составило 106% и 114% для ресурсов процессора и памяти, соответственно. Повышение плотности ВМ по сравнению с решением McAfee – 124,9% и 273,5% для ресурсов процессора и памяти, соответственно.

Trend Micro Deep Security

Компания Trend Micro разработала решение Deep Security 7.5, предусматривающее возможность «учета виртуальных машин». В отличие от традиционных решений на базе агентов Deep Security нацелено, в первую очередь, на предотвращение проблем с эксплуатацией (таких как «антивирусные штормы», потеря ресурсов и расходы на администрирование). В Deep Security реализован безагентский подход к антивирусной защите, оптимизированный для виртуализации, который обеспечивает более быструю обработку, повышенную консолидацию ВМ, упрощенное управление и сокращение «времени, затрачиваемого на защиту» виртуализированных активов.

Источник: Trend Micro, октябрь 2010 г.

Потребление ресурсов хоста антивирусом VMware ESX 4.1 в сравнении с базовым уровнем

При наличии максимум 100 виртуальных машин под управлением Microsoft Windows 7 с применением специализированной рабочей нагрузки

По данным vCenter (чем ниже значение, тем лучше)

Количество виртуальных машин	Антивирусное решение		Базовый уровень использования ресурсов хоста ESX / % Увеличение относительно базового уровня		
			Процессор (ГГц)/%	Память (Гб)/%	Диск (Кб/с)/%
25	Базовый уровень		4.113 GHz	6.306 GB	1.705 KBps
	Trend Micro	% увеличения относительно базового уровня	8.86%	5.94%	-13.26%
	McAfee		43.04%	50.83%	191.82%
	Symantec		46.58%	36.63%	138.05%
50	Базовый уровень		8.467 GHz	11.908 GB	2.592 KBps
	Trend Micro	% увеличения относительно базового уровня	24.65%	10.7%	38.98%
	McAfee		43.02%	60.34%	393.09%
	Symantec		42.73%	37.78%	148.91%
75	Базовый уровень		12.645 GHz	17.325 GB	3.381 KBps
	Trend Micro	% увеличения относительно базового уровня	11.61%	7.79%	-11.03%
	McAfee		35.33%	64.57%	325.32%
	Symantec		39.61%	33.33%	108.22%
100	Базовый уровень		17.197 GHz	22.468 GB	5.417 KBps
	Trend Micro	% увеличения относительно базового уровня	9.86%	12.7%	-4%
	McAfee		33.33%	69.31%	271.43%
	Symantec		36.14%	44.31%	77.61%

Примечание: значения базового уровня получены в результате 30 минутных прогонов теста с применением рабочей нагрузки без установленного антивирусного решения или решения для защиты конечных точек. Чем ниже процент увеличения потребления ресурсов, тем лучше. Во многих случаях прогоны тестов были не завершены в связи с истечением срока открытия тестового окна. Решение McAfee не смогло пройти тест на 100 ВМ, несмотря на многочисленные попытки и повторные запуски. Инженеры компании Tolly экстраполировали показатели этого продукта на 100 ВМ на основании результатов тестирования на 25, 50 и 75 ВМ. Показатели использования диска варьируются в пределах 30% и приведены только в качестве справочной информации.

Источник: Tolly, октябрь 2010 г. Таблица 4

Trend Micro Deep Security

Все тесты проводились с использованием одной и той же инфраструктуры аппаратного обеспечения. Они выполнялись последовательно для каждой системы. В таблице 2 приведены подробные сведения о тестируемых решениях и гостевых системах виртуальных машин, а в таблице 3 представлена информация о среде хоста виртуальной машины для производственного хоста.

Процессор физического сервера состоял из 24 логических ядер. Это означает, что системы, сконфигурированные для 100 виртуальных машин, превысили потребность в ресурсах физического процессора в соотношении примерно 4:1. Во время тестирования недостатка в ресурсах процессора не наблюдалось.

Хост VMware ESXi применялся для другой инфраструктуры, использованной при оценке, включая различные управляющие серверы, необходимые тестируемым продуктам, а также системы, генерирующие нагрузку.

Решение Trend Micro реализовано в виде виртуального устройства. Для связи с гостевыми машинами оно использует интерфейс VMware API. Этот API обменивается данными через интерфейс виртуальной сети.

Другие решения не учитывали особенности виртуальных машин. Поэтому они были развернуты так, как если бы это было 100 физических машин под управлением Windows.

На момент завершения разработки тестовой среды продукт McAfee для защиты конечных точек в виртуальных средах, McAfee Management for Optimized Virtual Environments (MOVE), еще не был доступен для хостинговых сред VMware.

Во всех тестируемых продуктах применялись антивирусные политики по умолчанию. Заранее настроенные задачи полного сканирования и обновления были отменены.

Основная рабочая нагрузка

В основных тестах применялась рабочая нагрузка, разделенная на 3 уровня активности:

Высокий: на 55% гостевых машин выполнялись сценарии с использованием приложений Microsoft Outlook, Word, Excel, Powerpoint, Internet Explorer и Adobe Reader. Низкий: на 35% гостевых машин выполнялись сценарии с использованием приложений Microsoft Outlook, Word, Excel, Powerpoint, Internet Explorer и Adobe Reader. Во время простоя: на 10% гостевых машин была запущена ОС Windows, после чего они оставались в состоянии простоя.

Эта рабочая нагрузка использовалась во всех тестах и выполняла роль фоновой нагрузки при тестировании со сканированием по требованию и обновлением сигнатур. Брандмауэр Windows и Windows Defender были отключены на всех гостевых виртуальных машинах.

Во время тестов с основной рабочей нагрузкой автоматически выполнялся вход всех пользователей в клиенты VMware View и запуск сценариев этого приложения.

Сценарии включали в себя редактирование сообщения электронной почты и документов Microsoft Office, пролистывание документов Adobe PDF и просмотр веб-страниц. Рабочая нагрузка не содержала каких-либо задач копирования файлов или ввода-вывода. Продолжительность прогонов составляла 30 минут.

Тесты со сканированием по требованию и обновлением сигнатур

Основная рабочая нагрузка запускалась инженерами Tolly в качестве фоновой, а затем всем гостевым виртуальным машинам, участвовавшим в тесте, назначалась одна задача полного сканирования или обновления с управляющего сервера. Продолжительность прогонов составляла 15 минут.

Все показатели производительности записывались из VMware vCenter с интервалом в 20 секунд.

Увеличение плотности ВМ — специализированная рабочая нагрузка: решение Trend Micro в сравнении с конкурентным решением (номинальная плотность)

	Процессор	Память	Диск
McAfee	31.4%	42.4%	236%
Symantec	34.6%	29%	174%

Увеличение плотности ВМ — сканирование по требованию: решение Trend Micro в сравнении с конкурентным решением (истинная плотность)

	Процессор	Память	Диск
McAfee	124.9%	273.5%	171.6%
Symantec	106.0%	114.1%	183%

Примечание: цифры в таблице отражают потенциал масштабирования и повышения плотности для продукта Trend Micro в сравнении с каждым конкурентным решением, исходя из потребления ресурсов.
Номинальная плотность относится к системам, которые выполняют нагрузку, не приводящую к напряженной работе антивируса.

Источник: Tolly, октябрь 2010 г. Таблица 5

О компанииTolly

Группа компаний Tolly на протяжении более чем 20 лет предоставляет ИТ-услуги мирового класса. Tolly – ведущий мировой поставщик услуг по тестированию ИТ-продуктов, компонентов и служб для их производителей.

С компанией можно связаться по электронной почте (*sales@tolly.com*) или по телефону (1 561.391.5610)

Посетите веб-сайт Tolly:
http://www.tolly.com

Взаимодействие с конкурентами

Следуя нашей процедуре проведения сравнительных тестов, Tolly Group связалась с конкурирующими производителями, пригласив их ознакомиться с методологией и результатами тестирования перед публикацией. Компания McAfee не ответила. Компания Symantec откликнулась и выразила готовность к сотрудничеству с инженерами Tolly. Symantec порекомендовала воспользоваться функцией рандомизации для распределения требовательных к ресурсам рабочих нагрузок в длительном интервале времени.
Дополнительная информация об Уставе справедливого тестирования (Tolly Fair Testing Charter) доступна по адресу: http://www.tolly.com/FTC.aspx

Правила использования

211101-uv-3-kt - 04Feb2011VerP