



# Trend Micro

## Система безопасности предприятий

Непосредственная защита. Легко.



Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

*Информационный документ Trend Micro*



## Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

### I ВВЕДЕНИЕ

После запуска первых экспериментальных приложений в 1960 и 1970-х годах виртуализация получила серьезное развитие как способ контроля основных и эксплуатационных расходов в сфере информационных технологий за счет консолидации серверов. Затем в 2005 г., когда «Intel» и AMD представили чипсеты для поддержки виртуального аппаратного обеспечения, виртуальная среда стала все больше и больше проникать в работу коммерческих приложений, где она продолжает поддерживать экономическую эффективность затрат в области информационных технологий за счет консолидации ресурсов. Сокращение стоимости использования информационных технологий сегодня для руководителей заключается в трех основных вопросах, и в соответствии с оценкой аналитической компании «Gartner» виртуализация – это основной ключ к снижению технологических затрат [1].

При широком использовании виртуализации для экономии затрат основное внимание было уделено качеству услуг в виртуализации, договорам о предоставлении услуг (SLA), скорости и стабильности. Но по мере того, как все больше и больше предприятий стали пользоваться преимуществами виртуализации, они столкнулись с необходимостью обеспечения безопасности своей виртуальной среды.

В настоящем документе рассматриваются вопросы безопасности конечных точек в виртуализованных средах, включая риски, присущие динамическим виртуальным машинам и ресурсоемкость программного обеспечения систем безопасности, например антивирусных сканеров в многочисленных гостевых виртуальных машинах (VM) на одном физическом хост-компьютере [2]. Для решения этих вопросов представлен новый стандарт безопасности виртуальных ЦОД, который объединяет технологию защиты от угроз и инновационную архитектуру антивирусной защиты в виртуализованных средах.

*“ Виртуализация почти 90% операционной среды позволила значительно сократить наши затраты и существенно расширить возможности по восстановлению работоспособности после аварий. ”*

**Гэри Уотли, директор по информационным технологиям; из интервью с компанией «Gartner», январь 2009 г.**

### II ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ВИРТУАЛЬНОМ ЦЕНТРЕ ОБРАБОТКИ ДАННЫХ.

Обеспечение безопасности виртуализации осложняется двумя факторами: (1) рисками, присутствующими в физическом центре данных и (2) рисками, которые присущи виртуализованным средам.

Лидеры виртуализации и обеспечения безопасности предприятий – компании VMware и Trend Micro – объединили свои усилия для формулирования задач и сотрудничества в специфических областях, чтобы помочь заказчикам решить эти вопросы.

Такой традиционный подход опирается в три основных вопроса для виртуализованных сред:

- Бреши в защите в момент включения VM
- Конфликт ресурсов
- Соответствие нормативам/ нехватка аудиторской отчетности

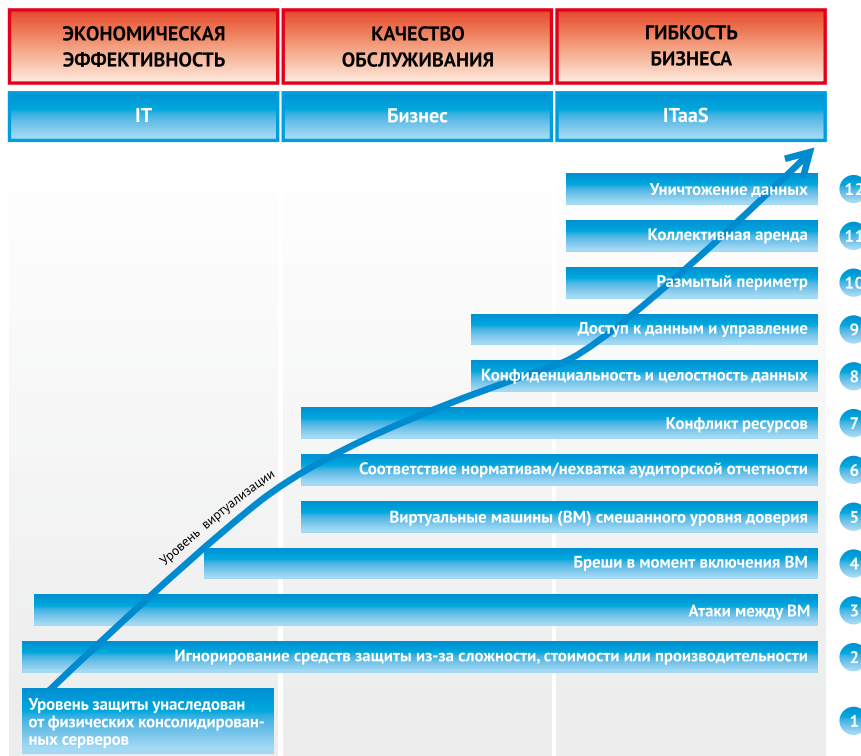


Рис. 1 Вопросы безопасности и виртуализации

## Традиционный подход в виртуальном центре обработки данных

По мере того, как предприятия переходят на стадию виртуализации, возникают проблемы, связанные с безопасностью. На практике, идея объединения физических хост-компьютеров вызывает скорее панику, чем воодушевление. Для решения вопросов, связанных с рисками гостевых виртуальных машин, предприятия, озабоченные вопросами безопасности, стали использовать имеющиеся решения обеспечения безопасности конечных точек для всех гостевых виртуальных машин в виртуализованных средах. Это привело «де факто» к стандарту использования антивируса в виртуальном центре обработки данных.

- **«Физический» против «виртуального».** В первую очередь, необходимо учесть различия присущие физическим и виртуальным архитектурам. Например, каждое устройство операционной системы (ОС) в физической среде работает непосредственно на выделенной аппаратной платформе. В отличие от этого каждое устройство ОС в виртуальной среде работает внутри гостевой виртуальной машины и многочисленные виртуальные машины запущены на уровне гипервизора. Этот гипервизор представляет собой своего рода абстрактный слой между виртуальными машинами и аппаратным обеспечением, обеспечивая динамическое распределение ресурсов системы.
- **Трудоемкое управление антивирусом:**  
Администраторы виртуальной инфраструктуры (ВИ) могут повысить эффективность, используя шаблоны для более быстрого развертывания. А администраторы, обеспечивающие безопасность, могут использовать централизованное управление антивирусом. Но даже при определенном уровне автоматизации ввод в действие и последующее сопровождение антивируса для каждой гостевой виртуальной машины не масштабируется.

### *Традиционное управление антивирусом*

1. *Сконфигурировать агента при установке*
2. *Изменить конфигурацию агента со временем при необходимости*
3. *Обновить/модернизировать агента*
4. *Развернуть обновления антивирусных сигнатур*



## Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

### Бреши в защите в момент включения VM

Помимо объединения серверов предприятия используют динамическую природу виртуальных машин для ввода в действие и снятия с эксплуатации при тестировании операционной среды, запланированного технического обслуживания, восстановления после аварии, а также для поддержки тех сотрудников, которым требуются вычислительные ресурсы по запросу. В результате, частые циклы включения и выключения виртуальных машин приводят к тому, что становится практически невозможным мгновенно обеспечить и поддерживать их безопасность. Неактивные виртуальные машины могут настолько отличаться от прототипа, что даже их включение может привести к нарушению системы безопасности. А новые виртуальные машины даже при формировании по шаблону с предустановленным антивирусом не могут мгновенно защитить гостевую машину без изменения конфигурации агента и обновлений антивирусных сигнатур. Проще говоря, если гостевая виртуальная машина не находится в работе при развертывании или обновлении антивирусного программного обеспечения, то она будет находиться в нерабочем и незащищенном состоянии и окажется уязвимой при переходе в рабочее состояние.

### Конфликт ресурсов

Работы с интенсивным использованием ресурсов, например, антивирусное сканирование и обновление антивирусных сигнатур может быстро привести к большой нагрузке на систему. Когда антивирусное сканирование и обновление сигнатур начинают работать на виртуальных машинах одной физической системы, то в результате возникает «антивирусный шторм». Этот «шторм», как налет на банк, где «банком» является основообразующий ресурс памяти, хранилище и центральный процессор. Такое влияние на рабочие характеристики препятствует работе приложений сервера и виртуализованных сред компьютера.

Традиционная архитектура также приводит к линейному росту распределения памяти с увеличением числа виртуальных машин в физическом хост-компьютере. В физической среде антивирусное программное обеспечение устанавливается для каждой операционной системы. Использование такой архитектуры для виртуальных систем означает, что для каждой виртуальной машины требуется дополнительный существенный объем памяти – нежелательный расход ресурса при попытках консолидации серверов.

### Вопросы контроля информационных технологий

Промышленные нормативы и политики обеспечения безопасности предприятий должны соответствовать развитию технологий виртуализации, которые представляют собой уникальный набор задач по объединению усилий виртуализации. Прозрачность и управляемость в рамках всей системы и сетевой активности оказываются намного сложнее в виртуальных средах, поскольку традиционное ПО обеспечения безопасности системы на базе хост-компьютера и обычные аппаратные IDS/IPS не интегрированы на уровне самодиагностики. Наиболее эффективный способ решения вопроса получается при интегрировании антивирусной функции непосредственно в платформу виртуализации, используя самодиагностику гипервизора, что дает возможности мониторинга и контроля всего, что проходит через гипервизор. Для эффективного использования требуется сотрудничество с провайдерами платформы виртуализации.

*“ PCI DSS 2.0 расширяет определения системных компонентов для включения виртуальных компонентов ”*

**PCI DSS 2/0 и PA-DSS 2.0.-**

**Обзор изменений –**

**основные положения.**

август 2010 г.



### III ТРЕБУЕТСЯ НОВЫЙ ПОДХОД

Эффективное выявление вредоносных программ, которое возможно сегодня в физической среде, порождает массу проблем при внедрении такого решения в виртуальном мире из-за присущих этим средам различий. Ошибки адресации при традиционном подходе: Антивирусные операции, которые являются причиной большинства проблем в виртуализированной среде, должны быть идентифицированы, и необходимо разработать бесперебойное выполнение этих операций. Во избежание возникновения брешей в защите в момент включения ВМ, решение должно предусматривать работу и управление виртуальными машинами в полностью защищенном режиме так, чтобы обеспечить надежную безопасность гостевых виртуальных машин не зависимо от того, когда проводилось обновление сигнатур антивируса или запланированное сканирование. Для устранения конфликта ресурсов решение должно уравнивать пиковые моменты использования ресурсов, вызванные упомянутой ранее антивирусной активностью.

Обеспечение эффективности нового подхода: При этом новом подходе должны быть расширены имеющиеся инвестиции, не просто для достижения экономической эффективности, но и для обучения персонала. Этот метод не должен также «раскачивать лодку» в других сферах бизнеса: правила обеспечения безопасности, промышленные правила и требования о соответствии должны выполняться и выполняться прозрачно – с журналами аудита и другими ознакомительными отчетами.

### IV ПЛАТФОРМА VMWARE VSHIELD ENDPOINT

VMware является мировым лидером в области виртуализации и сетевой инфраструктуры, обеспечивая проверенными решениями более 190000 заказчиков, среди которых 97% компаний из Fortune 1000 и 94% из Global 500. Продолжая развитие инновационных технологий в рамках работы виртуальных ЦОД, VMware расширила возможности платформы, разрешив самодиагностику гипервизора, необходимую для оптимизации функций безопасности в виртуализированных средах, с помощью VMware vShield Endpoint.

VMware vShield Endpoint усиливает безопасность виртуальных машин и их хост-систем, на порядок улучшая при этом защиту конечных узлов. vShield Endpoint позволяет перенести нагрузку антивирусной обработки с конечной точки на специально выделенную виртуальную машину, разработанную Trend Micro. Она также позволяет значительно сократить объем потребляемой памяти, необходимой для обеспечения безопасности на виртуальных хост-компьютерах за счет удаления антивирусного ПО для гостевых виртуальных машин и использования этих функций в рамках выделенной виртуальной машины, обеспечивающей безопасность систем. Администраторы VI могут управлять VMware vShield Endpoint с консоли vShield Manager, которая интегрирована с VMware vCenter Server для управления платформой антивирусных решений Trend Micro.



## Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

### Как это работает

vShield Endpoint встроена непосредственно в платформу VMware vSphere, развернута на базе хост-машины и состоит из трех компонентов:

- Программное виртуальное устройство (поставляемое Trend Micro)
- Драйвер для виртуальных машин, обеспечивающий отслеживание операций ввода/вывода при работе с файлами на гостевых системах
- VMware Endpoint Security (EPSEC), модуль ESX для связи первых двух компонентов с гипервизором.

Драйвер vShield Endpoint включен на защищенной виртуальной машине, работающей на базе vSphere, и требует всего несколько мегабайт памяти для работы. [3] Драйвер контролирует обращения виртуальной машины к файлам и отправляет команду антивирусному движку, который сканирует и возвращает сведения о просканированных файлах. Кроме того, он поддерживает запланированное полное и частичное сканирование файлов, инициируемое антивирусной программой. В случае необходимости восстановительных процедур, администраторы могут задать действия, которые должны применяться, и VMware vShield Endpoint автоматически генерирует восстановительные действия для соответствующих виртуальных машин.

## V РЕШЕНИЕ – TREND MICRO DEEP SECURITY

Платформа VMware vShield Endpoint позволяет выполнить оптимизацию работы антивирусных решений в виртуализованных средах. Trend Micro как стратегический партнер VMware первой на рынке предоставила решение, учитывающее вышеупомянутые вопросы в обеспечении безопасности виртуализованных сред с помощью Trend Micro Deep Security.

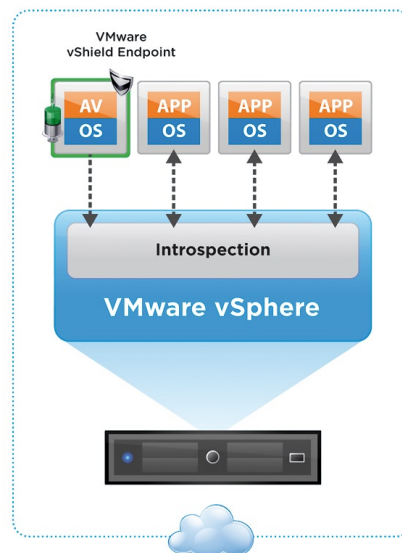


Рис. 2 VMware vShield Endpoint и Trend Micro Deep Security



Именно сочетание этих двух компонентов позволяет предприятиям эффективно решать вопросы обеспечения непрерывной защиты и конфликта ресурсов в виртуальном центре обработки данных. Такой инновационный подход меняет правила работы с антивирусом в виртуальном центре обработки данных.

В состав Trend Micro Deep Security входит виртуальная машина с встроенным антивирусным «движком», которая выполняет характерные для антивирусного ПО действия, такие как запланированное (или при обращении) сканирование файлов, обновление вирусных сигнатур, проверка типов файлов (вредоносная программа или нет) и инструкции по принудительным действиям (например, карантин, удаление). Фактически выполнение принудительного действия выполняется с помощью использования технологии VMware vShield Endpoint, которая позволяет контролировать и управлять гипервизором и файловой активностью гостевой виртуальной машины.

### Непрерывное обеспечение безопасности для решения проблем в виртуальной среде

Для сред, которые защищены с помощью Trend Micro Deep Security и vShield Endpoint, виртуальные машины защищены в течение всего их срока службы с гарантией того, что любой доступ к файлу сканируется на наличие всех известных угроз. Виртуальная машина Trend Micro Deep Security развернута таким образом, чтобы обеспечить необходимый уровень защиты, обеспечивающий гарантированную доступность антивирусного «движка», способного выполнять связанные с ним задачи.

### Снятие нагрузки, связанной с работой антивируса, позволяет решить вопросы конфликта ресурсов

С помощью этой инновационной технологии организации могут улучшить производительность системы и повысить уровень консолидации благодаря переносу нагрузки, связанной с антивирусным сканированием, выполняемым на каждой виртуальной машине в отдельности, на одну виртуальную машину Trend Micro для каждого защищенного хоста vSphere.

- **Восстановление памяти для поддержания консолидационных отношений.** Сокращение распределения памяти на одну гостевую виртуальную машину позволяет администраторам существенно увеличить консолидационные отношения сервера. Вместо того, чтобы тратить сотни мегабайт под антивирусное программное обеспечение для каждой гостевой виртуальной машины на физическом устройстве, организации могут теперь использовать один антивирусный движок в рамках виртуального устройства и использовать в каждой виртуальной машине один драйвер, занимающий очень небольшой объем памяти, для выполнения необходимых операций. Эти преимущества особенно очевидны в среде VDI (VMware View), где часто встречаются отношения консолидации 200 : 1 [5]. При таком сильном снижении распределения памяти можно добиться сокращения издержек, и предприятия смогут расширить возможности использования физических серверов и достигнуть еще больших отношений консолидации.
- **Централизованное сканирование и обновление для предотвращения «антивирусного шторма».** Новая архитектура Deep Security позволяет рационально использовать ЦП и выполнять операции ввода/вывода в процессе интенсивного сканирования файлов и обновления сигнатур, оставляя больше ресурсов гостевым виртуальным машинам для выполнения важных рабочих функций. Такое решение предотвращает «антивирусный шторм» и «узкие места», связанные с одновременным сканированием и обновлением, за счет последовательного выполнения операций на виртуальных машинах данного хост-компьютера.



## Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

### Прозрачность и контроль для упрощения процедуры прохождения аудита

Кроме обеспечения безопасности платформа Trend Micro Deep Security позволяет решить ряд вопросов, связанных с обеспечением уровня соответствия стандартам.

- **Одна функция на сервер.** Последнее обновление PCI DSS 2.0 предполагает, что технология виртуализации будет допустимой даже при необходимости выполнения требования 2.2.1 – «одна основная функция на сервер». А виртуальное программное устройство для обеспечения безопасности представляет собой виртуальную машину для выполнения одной единственной задачи – защиты вирусов и ничего больше.
- **Прозрачность за счет самодиагностики.** Для решения используются эффективные и надежные средства самодиагностики гипервизора с помощью vShield Endpoint, обеспечивая полную прозрачность активности файлов при антивирусном сканировании. Большинство промышленных нормативов и правил обеспечения безопасности данных на предприятиях требуют контроля активности системы на наличие вредоносных программ и Trend Micro успешно выполняет подобное сканирование в виртуальных системах.
- **Учет активности vSphere и Trend Micro.** Предусмотрен подробный учет соответствующих операций по обеспечению безопасности с помощью Trend Micro и VMware, что позволяет выполнять требования регуляторов и политики компаний, когда могут потребоваться данные для расследования.
- **Разделение обязанностей.** Такая архитектура позволяет администраторам, обеспечивающим безопасность, внедрять и управлять антивирусными программами в виртуальной среде с помощью Deep Security Manager – и тот же интерфейс можно использовать для обеспечения безопасности физической среды. Аналогичным образом администратор VI может использовать vCenter для развертывания vShield Endpoint наряду с виртуальным программным устройством Trend Micro. Никто не может управлять с их помощью другой инфраструктурой. Упомянутое разделение обязанностей между администратором VI и администратором по обеспечению безопасности плюс подробный учет активности помогает предприятиям обеспечить соответствие и выполнять требования аудиторов.

## VI ДОПОЛНИТЕЛЬНЫЕ ПРЕИМУЩЕСТВА

Trend Micro обеспечивает эффективное решение вопросов, связанных с конфликтом ресурсов и нарушением целостности защиты в момент включения VM за счет тесной интеграции на уровне гипервизора, что приводит к повышению эффективности в управлении информационными технологиями и ресурсами без ухудшения работоспособности.

### Упрощенное управление

- Первоначальное развертывание и последующее сопровождение антивирусной защиты является достаточно трудоемким процессом в физическом ЦОД.

Модернизированное антивирусное управление – С помощью VMware vShield Endpoint и Trend Micro Deep Security администраторам нужно развернуть только антивирусный движок и обновления сигнатур на виртуальном программном устройстве Deep Security Virtual Appliances. Фактически отпадает необходимость в выполнении трудоемких задач, связанных с традиционным подходом:

1. НЕ требуется настройка агента при установке
2. НЕ требуется повторная настройка агента в дальнейшем
3. НЕ требуется обновление/ переустановка агента
4. НЕ требуется распространение сигнатур



- **Не требуется переобучение администраторов** – Ролевая модель управления доступом через VMware vCenter, интегрированная с консолями управления Trend Micro, позволяет сотрудникам выполнять ежедневные операции с минимальным перерывом. Администраторы могут настроить ролевой доступ через vCenter, что позволит развернуть виртуальное программное устройство Trend Micro на виртуальные хосты только авторизованным администраторам. Консоль Trend Micro может быть также сконфигурирована для ограничения доступа к правилам Deep Security и операциям по обеспечению безопасности для составления оптимального расписания обновления, чтобы избежать конфликта ресурсов.

## Улучшенная безопасность

Платформа Trend Micro Deep Security обеспечивает улучшенную степень безопасности поскольку в нее заложен подход к безопасности, который эффективен для среды виртуальных ЦОД. За последние двадцать лет в этой индустрии использовался стандартный антивирус – это само по себе является приглашением для вирусной атаки.

- **Устранение цели атаки** – в Deep Security отсутствует агент, поскольку никакое антивирусное ПО не устанавливается на гостевой виртуальной машине. Как уже было сказано выше, антивирусная технология используется в виртуальном программном устройстве. Более того драйвер VMware vShield Endpoint в каждой гостевой виртуальной машине допускает только определенную связь с Deep Security Virtual Appliance. Большинство атак против антивирусной продукции предполагают встречу с клиентской антивирусной установкой на гостевой виртуальной машине, но эти атаки абсолютно бесплодны при таком подходе.
- **Устранение уязвимостей при общих атаках:** Deep Security Virtual Appliance, в котором работает антивирусный движок, защищен от общих вирусных атак, например, от червя Conficker. При взаимодействии между виртуальным устройством и гостевыми виртуальными машинами допускаются только специальные действия, связанные с защитой от вредоносных программ. Поскольку устройство всегда включено защита постоянно контролирует виртуальные машины, благодаря чему достигается необходимый уровень безопасности даже выключенных VM.

### *Типовые способы атак:*

1. Удаление антивирусной программы.
2. Остановка антивирусной программы.
3. Изменение ключей регистрации, необходимых для антивирусной программы.

## VII ПОЧЕМУ TREND MICRO

Занимающаяся обеспечением безопасности контента, начиная со своего основания 20 лет, назад Trend Micro постоянно демонстрирует свою компетенцию и опыт в обеспечении безопасности контента. Trend Micro постоянно внедряет новые разработки с помощью Trend Micro Smart Protection Network, в режиме реального времени коррелируя данные в соответствии с появлением новых и неизвестных угроз и обеспечивая постоянно обновляемую защиту, которая идеально подходит для физической и виртуальной среды. Инфраструктура Smart Protection Network обеспечивает расширенную защиту «из облака», блокируя угрозы в реальном времени до того, как они достигнут корпоративной сети. Обеспечивая уникальную архитектуру «сеть-клиент», она использует интеллектуальные датчики угроз, электронную почту, интернет, и сведения о репутации файлов на конечных точках, что все вместе существенно снижает распространение заражения.



## Изменение принципов работы антивирусной защиты в условиях виртуального центра обработки данных

Технологические возможности, входящие в Smart Protection Network, являются частью антивирусной технологии Deep Security, позволяя использовать сигнатуры небольшого размера. Deep Security Virtual Appliance представляет собой совершенно новое готовое решение, готовое к работе в виртуальной среде, помогающее предприятиям сократить эксплуатационные затраты за счет централизованного управления антивирусом как для физической, так и для виртуальной среды.

Ежегодный доход более миллиона долларов, больше 1000 исследователей возможных рисков, более 4000 сотрудников по всему миру. Trend Micro обладает уникальной технологической инфраструктурой, необходимой для обеспечения безопасности предприятий в нынешних условиях.

### VIII ВЫВОД

Совершенно естественно, что предприятия пытаются разрешить вопросы безопасности в виртуальном центре обработки данных известными методами, но различия между физической и виртуальной инфраструктурой не дают желаемый результат при традиционном решении. Trend Micro в сотрудничестве с VMware предлагает инновационный подход для антивирусной защиты виртуальных центров обработки данных с помощью платформы Trend Micro Deep Security. Этот беспрецедентный подход нацелен на разрешение основных вопросов, связанных с традиционным подходом при одновременном упрощении управлений согласовании информационных технологий и улучшении общей безопасности проекта.

Вопросы безопасности в виртуализованной среде	Преимущества решения
Бреши в безопасности, возникающие в момент включения VM	<ul style="list-style-type: none"> <li>• Автоматическая защита до установки антивируса</li> </ul>
Конфликт ресурсов	<ul style="list-style-type: none"> <li>• Всегда имеется антивирусная программа за счет централизованного использования в виртуальном устройстве</li> <li>• Поддерживаются отношения консолидации за счет высвобождения памяти</li> </ul>
Вопросы соответствия стандартам в области информационных технологий	<ul style="list-style-type: none"> <li>• Предупреждение «антивирусного шторма» за счет централизованного сканирования</li> <li>• Одна функция на сервер для выполнения требований PCI DSS и других регуляторов</li> <li>• Прозрачность за счет самодиагностики</li> </ul>
Сложность управления	<ul style="list-style-type: none"> <li>• Отчет по операциям vSphere, Deep Security</li> <li>• Разделение обязанностей</li> <li>• Упрощенное антивирусное управление</li> </ul>
Риски обеспечения безопасности при традиционном антивирусе	<ul style="list-style-type: none"> <li>• Не требуется переобучение администраторов</li> <li>• Устраняется цель атаки</li> <li>• Устраняются уязвимости в случаях типовых атак</li> </ul>



Более подробные сведения о Trend Micro Deep Security можно получить по адресу:

**<http://www.trendmicro.com>**

Более подробные сведения о VMware vShield Endpoint можно получить по адресу:

**<http://www.vmware.com/products/vshield-endpoint/>**

## IX ЛИТЕРАТУРА

[1] “Meeting the Challenge: The 2009 CIO Agenda”, January 2009, pages 32 and 45

[2] Программное обеспечение, определяющее вирусы, шпионские программы, троянов и другие вредоносные программы, называемое также антивирусной или антивредоносной программой. В настоящей статье мы называем ее «антивирус».

[3] Исходно этот драйвер должен быть развернут с помощью существующих методов управления виртуальной инфраструктурой, например шаблонов. VMware рассматривает его как дополнительный драйвер для VM Tools. Источник: VMware

[4] Источник VMware ROI TCO Calculator <http://roitco.vmware.com/vmw/>

vmware®

