Визитка

АНДРЕЙ БИРЮКОВ, специалист по информационной безопасности. Работает в крупном системном интеграторе. Занимается внедрением решений по защите корпоративных ресурсов

Защищаем виртуальную среду
Часть 1: Trend Micro Deep Security

Виртуальные серверы нуждаются в обеспечении безопасности не меньше физических. Сегодня существует ряд решений по безопасности виртуальных сред. В этой статье мы начнем их обсуждение

В последние годы средства виртуализации получили широкое распространение. Сейчас во многих крупных организациях имеются десятки, а то и сотни виртуальных серверов, обеспечивающих различные промышленные задачи. У этих решений есть множество преимуществ перед аппаратными.

Во-первых, возможность снизить требования к системе электропитания. Во многих офисных центрах в крупных городах существуют проблемы при подаче энергетических мощностей, организации зачастую не могут разместить на арендуемой площади желаемое число серверов для своих приложений.

Во-вторых, экономия места в серверной, так как на нескольких мощных физических машинах можно разместить несколько десятков виртуальных.

В-третьих, большое значение имеет потребление процессорных ресурсов, которое при использовании виртуализации можно существенно оптимизировать.

Проблемы с безопасностью

Однако в связи с массовым распространением виртуальных сред появились и новые проблемы с безопасностью. Но прежде поговорим о различиях между ИТ-средами, использующими физические и виртуальные серверы.

Физические серверы для обмена трафиком всегда используют сетевую инфраструктуру, то есть пакет, переданный с одного сервера на другой, обязательно пройдет через коммутатор, где, как правило, имеются средства межсетевого экранирования, предотвращения вторжений и другие элементы сетевой безопасности. Для виртуальных серверов это совершенно необязательно.

В случае вирусной эпидемии, вредоносному коду необходимо для заражения других машин перемещаться по сети. В виртуальной среде зачастую для заражения десятков серверов не нужно передавать по внешней сети ни одного пакета.

И наконец, для виртуальных машин более вероятна ситуация, когда долгое время отключенный сервер после включения какое-то время работает с устаревшими средствами защиты. Такая ситуация часто бывает после восстановления виртуальной машины из резервной копии.

Виртуальные машины, находящиеся в отключенном состоянии, не обновляют антивирусные базы и другие компоненты защиты. В результате при включении данные машины некоторое время (до нескольких часов) могут находиться в недостаточно защищенном состоянии, что может привести к заражению их вредоносным кодом. Сходная проблема существует и с обновлениями операционной системы виртуальных машин.

Также важная проблема с безопасностью виртуальных машин – возможность доступа к их памяти извне. Так как оперативная память виртуальной машины представляет собой набор файлов, то реальна ситуация, когда злоумышленник сможет получить доступ к содержимому оперативной памяти всех виртуальных машин, находящихся на данном сервере. Или, к примеру, вирус сможет заразить все виртуальные машины на сервере, просто скопировав себя в их оперативную память.

На первый взгляд это кажется почти невозможным. Ведь речь идет не только о раздельных виртуальных машинах и системе гипервизора. Зачастую с помощью виртуализации создаются абсолютно разнородные среды, например, UNIX-система (VMware ESX, Citrix XenServer) в качестве виртуальной среды (гипервизора) и гостевые системы под Windows. Или, наоборот, используется майкрософтовский Hyper-V и нескольких гостевых виртуалок под Linux.

А, как известно, у Windows и UNIX-систем очень много различий, как в архитектуре, так и в адресации памяти и других элементах. Однако не стоит забывать, что в различных реализациях VMware для обмена между виртуальной средой и гипервизором применяются программные средства. Не стоит рассчитывать на то, что злоумышленники никогда не смогут разработать вредоносное ПО, которое будет проникать из виртуальной среды или из физических серверов и других источников в гипервизор и оттуда заражать другие виртуальные машины.

Конечно, некоторые из этих проблем можно решать традиционными средствами, например, поставив антивирусное

ПО на каждую из виртуальных машин. Но сейчас уже имеется ряд решений, предназначенных для обеспечения безопасности виртуальной среды. Об этих решениях мы и поговорим в данной и последующих статьях.

Поскольку сегодня весьма популярным решением является использование гипервизоров на базе VMware ESX, мы будем рассматривать описанные проблемы применительно именно к этому гипервизору.

Новый подход в концепции защиты

Описанные в предыдущем разделе вопросы безопасности виртуальной среды были озвучены на VMware Virtualization Forum, который прошел 26 ноября 2010 года в Москве. Специалисты VMware и представители компаний-партнеров выступали с докладами, посвященными решениям по безопасности. Подробнее узнать об этом можно на сайте [2].

На форуме были представлены системы для решения данных задач информационной безопасности. В качестве средства защиты от вредоносного кода был продемонстрирован продукт Trend Micro Deep Security.

Также было представлено решение vGate от компании «Код Безопасности», которое обеспечивает управление доступом, контроль параметров безопасности и позволяет автоматизировать работу администраторов по конфигурированию и эксплуатации системы безопасности виртуальной среды. Для повышения безопасности виртуализированных сред разработан продукт VMware vShield Edge.

В комплексе все эти средства позволяют защитить виртуальные машины от вредоносного кода, ограничить доступ виртуальной среде и обеспечить более высокую безопасность инфраструктуры VMware.

Типовая виртуальная среда

Прежде чем обсуждать, как мы хотим защищать нашу виртуальную среду, необходимо определиться, безопасность чего именно мы хотим обеспечивать.

Типовая инфраструктура VMware представлена на рис 1.

Как видно из схемы, виртуальная среда тесно связана с реальными физическими серверами. Пользователи, размещающиеся в корпоративной сети, обращаются к бизнес-приложениям, которые находятся на виртуальных машинах. Машины размещаются в корпоративных хранилищах. Но для самих пользователей все это выглядит совершенно прозрачно. Группа виртуальных машин находится под управлением гипервизора ESX. При этом возникает упоминавшаяся выше ситуация, когда виртуальные машины обмениваются трафиком не только с корпоративными серверами, но и между собой. В таком случае трафик не попадает в корпоративную сеть.

Конечно, возможны различные изменения в архитектуре построения виртуальной среды, но в целом типовая инфраструктура выглядит подобным образом.

Защита от вредоносного кода

В этой статье я начну с описания Trend Micro Deep Security.

Изначально данный продукт разрабатывался компанией Third Brigade. Однако некоторое время назад антивирусный гигант Trend Micro приобрел эту компанию вместе с ее разработками по защите виртуальной среды.

В продукте используется новейший API VMware vShield Endpoint, который компания VMware предоставляет разработчикам для взаимодействия с виртуальной средой.

С помощью VMware vShield Endpoint производится обмен данными между физическим сервером гипервизора и виртуальными машинами. Благодаря использованию специализированного интерфейса для разработчиков (API), входящего в состав VMware vShield Endpoint, она отличается более высокой производительностью, при этом обеспечивая повышенный уровень защиты от вредоносного кода.

Также Deep Security содержит модуль защиты от вредоносного кода. Этот модуль не требует установки агента и дополняет уже имеющиеся возможности средств защиты предыдущих версий продукта с тем же названием (7.0), включая механизмы обнаружения и предотвращения вторжений, средства защиты и контроля целостности приложений, брандмауэр с отслеживанием состояния соединений, средства мониторинга целостности и анализа событий в журналах. Как видно из этого описания, с помощью Trend Micro Deep Security вполне можно решить описанные ранее проблемы вредоносного кода и распространения трафика по сети между виртуальными машинами.

Но обо всем по порядку, начнем с описания архитектуры данного продукта.

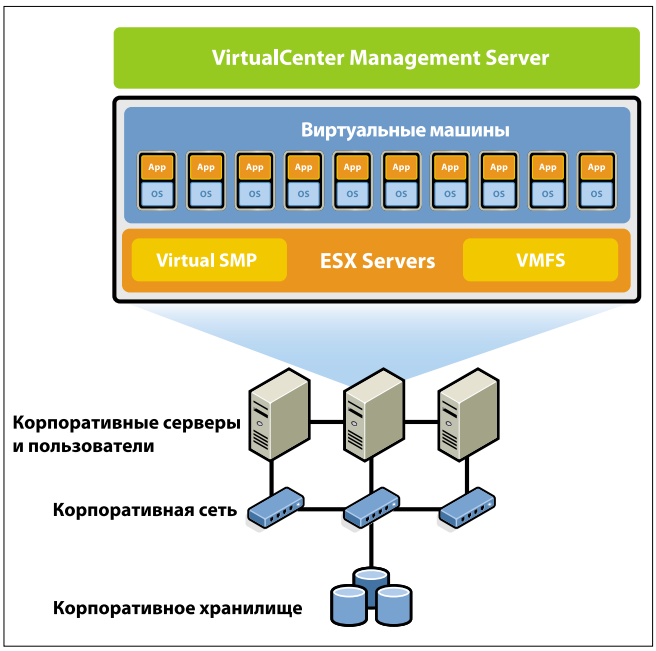
Архитектура Trend Micro Deep Security

Данное решение состоит из следующих четырех модулей:

- Deep Security Manager;
- Deep Security Agent;
- Security Center;
- Deep Security Virtual Appliance.

Первый модуль Deep Security Manager осуществляет централизованное управление всей системой защиты виртуальной инфраструктуры. Диспетчер Deep Security Manager – система управления, с помощью которой адми-

Рисунок 1. Типовая инфраструктура VMware



нистраторы могут создавать профили безопасности и применять их к серверам. Она оснащена централизованной консолью для отслеживания предупреждений и выполнения предупреждающих действий в ответ на обнаружение угроз. Deep Security Manager может в автоматическом режиме или по запросу рассылать обновления безопасности серверам. С помощью данного продукта можно создавать отчеты в целях контроля его действий и обеспечения соответствия требованиям законодательства.

Также добавлена новая функция назначения тегов для событий, которая оптимизирует работу с большим количеством угроз и позволяет задавать процедуры реагирования на них.

Deep Security Agent – это небольшой программный компонент, устанавливаемый на защищаемый сервер или виртуальную машину и обеспечивающий применение политики безопасности. Он поддерживает систему обнаружения и предотвращения атак (Intrusion Detection and Prevention, или IDS/IPS), выполняет функции защиты веб-приложений, управления приложениями, брандмауэра, контроля целостности и проверки журналов. Установка агентов не является обязательной, однако она позволяет обеспечить соответствие политике безопасности.

Центр управления безопасностью Security Center – это команда специалистов Trend Micro в области безопасности, которые разрабатывают и предоставляют обновления для исправления только что обнаруженных уязвимостей. Security Center имеет клиентский портал, используемый для доступа к этим обновлениям и последней информации. Обновления безопасности могут доставляться диспетчеру Deep Security Manager автоматически или по запросу с последующей установкой на тысячах серверов за считанные минуты.

Deep Security Virtual Appliance – специализированная виртуальная машина, защищающая остальные виртуальные машины в рамках одного ESX-сервера путем анализа трафика с использованием технологии VMsafe. Виртуальное устройство Deep Security Virtual Appliance содержит ядро системы сканирования вредоносного кода.

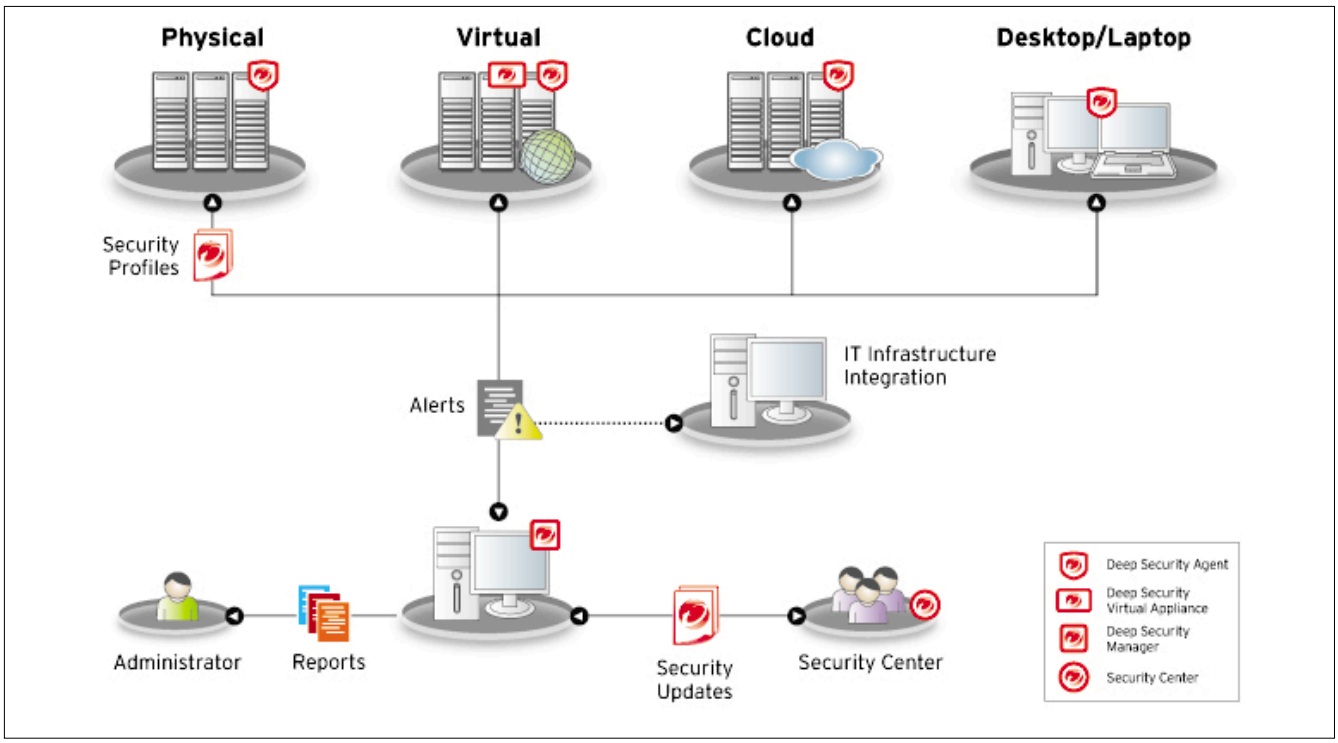
VMsafe – технология, позволяющая сторонним разработчикам получить доступ к гипервизору VMware и фактически представляющая собой набор API-интерфейсов [4].

При взаимодействии виртуальных устройств и гостевых виртуальных машин допускаются только специальные действия, связанные с защитой от вредоносных программ. Поскольку устройство всегда включено, система безопасности постоянно контролирует виртуальные машины, благодаря чему достигается необходимый уровень безопасности даже в выключенных системах, так как обновления антивирусных баз будут скачиваться виртуальным устройством, которое также может сканировать не запущенные на данный момент машины.

Однако здесь стоит отметить наличие угрозы безопасности, которая существует для выключенных гостевых виртуальных машин. Когда guest-система включается после долгого простоя, антивирусные базы, а также обновления операционной системы на ней некоторое время являются не актуальными. Время, в течение которого защита системы будет ослаблена, зависит от настроек антивирусной системы, установленной на виртуальной машине, а также от пропускной способности канала связи между сервером обновлений и данной виртуалкой. Это широко распространенная проблема.

Для борьбы с ней Trend Micro Deep Security производит сканирование памяти виртуальной машины без участия

Рисунок 2. Схема защиты Deep Security



программы агента, и, как только в ней появляется какая-либо вредоносная активность, антивирусная система тут же предпринимает установленные политиками действия по защите.

А для случаев, когда еще не установлены обновления операционной системы, Deep Security предлагает защиту от атак «нулевого дня», речь о которых пойдет чуть позже.

Одним из способов заражения физических машин вредоносными программами является отключение антивирусного ПО в процессе проникновения в систему. При использовании виртуального устройства вредоносный код не сможет отключить агента антивируса, потому что его нет на виртуальной машине.

Немаловажным обстоятельством для организаций, чья деятельность регулируется государственными нормативными актами, является то, что Deep Security также помогает обеспечить соблюдение нормативных требований и стандартов, например, PCI DSS и других.

Payment Card Industry Data Security Standard (PCI DSS) – стандарт защиты информации в индустрии платежных карт, разработанный международными платежными системами Visa и MasterCard. Объединяет в себе требования ряда программ по защите информации [5].

На рис. 2 представлена схема защиты, обеспечиваемая с помощью описанных модулей.

В продукте Trend Micro Deep Security антивирусный функционал реализован как основная часть системы, дополненная другими модулями безопасности, такими как виртуальное управление установкой обновлений и межсетевой экран, разработанный с учетом особенностей защиты виртуальной среды. В частности, в данном функционале предусмотрена защита уязвимых мест от известных атак и атак типа «нулевого дня».

Атакой «нулевого дня» (или «нулевого часа») называется компьютерная атака, использующая уязвимости, не известные разработчикам средств защиты, либо уязвимости, для которых отсутствуют заплатки. В контексте антивирусной защиты атаками нулевого дня являются вирусы, которые не определяет антивирусное ПО.

Интеллектуальные правила защиты от атак типа «нулевого дня», которые позволяют предотвратить угрозы, направленные на неизвестные уязвимые места, обнаруживают необычные данные протоколов, содержащие вредоносный код. В случае если найдены новые угрозы, производится автоматическое обеспечение защиты недавно обнаруженных уязвимых мест в течение нескольких часов и развертывание защитных правил на тысячах серверов за считанные минуты без перезагрузки системы.

Вообще в Deep Security предусмотрена работа в режиме поиска угроз или профилактики. В первом случае осуществляется реактивная защита, во втором проактивная. Реактивной считается защита, которая реагирует на угрозу, проактивная пытается предотвратить ее появление. Проактивный механизм защиты позволяет предотвратить заражение уязвимых мест операционных систем и приложений предприятия. Говоря об известных уязвимостях, следует отметить, что в Deep Security имеются встроенные функции защиты уязвимых мест более чем 100 приложений, включая базы данных, веб-серверы, а также почтовые и FTP-серверы.

Тщательная проверка пакетов

В Deep Security имеется набор средств для обеспечения сетевой безопасности. В первую очередь это двунаправленный потоковый брандмауэр, обеспечивающий контроль обмена трафиком как с внешней сетью, так и между виртуальными машинами. Также в межсетевом экране имеется детальная фильтрация (IP- и MAC-адреса, порты). Есть возможность разработки политик для отдельных сетевых интерфейсов и получения сведений об их расположении. Управление политиками серверного брандмауэра, включая шаблоны для использования на серверах распространенных типов, осуществляется централизованно.

Дополнительно межсетевой экран Deep Security обладает функционалом для защиты от атак на уровне приложений, а также от внедрения кода в базы данных (SQL-инъекции) и межсайтового выполнения сценариев (Cross Site Scripting).

Атаки типа «отказ в обслуживании» получили широкое распространение в последние годы из-за сравнительной простоты их реализации. Deep Security обладает механизмом для предотвращения данных атак, а также обнаружения «разведывательного» сканирования, которое взломщики часто используют перед началом атаки. Также межсетевой экран поддерживает все IP-протоколы (TCP, UDP, ICMP и т.д.) и типы фреймов (IP, ARP и т.д.).

Защита веб-приложений

Виртуальные машины очень часто используют в качестве веб-серверов. Поэтому в Trend Micro Deep Security предусмотрены специальные средства защиты. В частности, имеются:

- Средства по контролю за уязвимостями, имеющимися в веб-приложениях, и защита уязвимых мест до выпуска соответствующих исправлений.
- Защита от внедрения кода SQL, межсайтового выполнения сценариев и других атак, направленных на веб-приложения.
- Обеспечение соответствия требованиям различных стандартов в целях защиты веб-приложений и обрабатываемых ими данных.

Управление приложениями

Администратору виртуальной среды всегда необходимо знать, какие именно приложения имеют доступ во внешнюю сеть для обеспечения более полного контроля над ними.

В Deep Security предусмотрено предоставление более подробной информации о таких приложениях и использование правил управления ими для обнаружения вредоносных программ, проникающих в сеть.

Анализ событий и инцидентов

Помимо средств защиты, в Deep Security также предусмотрены инструменты для анализа событий информационной безопасности, происходящих на виртуальных машинах. В частности, производится сбор и анализ журналов операционной системы и приложений в целях обнаружения событий в системе безопасности. В целом механизм обеспечивает обнаружение подозрительной деятельности, сбор сведений о событиях, относящихся к системе безопасности, и действиях администратора в центре обработки данных,

а также создание усовершенствованных правил с помощью синтаксиса анализатора журналов событий OSSEC.

Помимо этого, в Deep Security имеется механизм обнаружения и предотвращения проникновений. Данный механизм анализирует события и предоставляет аналитическую информацию, содержащую сведения о времени атаки, IP-адрес источника и уязвимости, которой он попытался воспользоваться. Также производится автоматическое оповещение администратора об атаке по электронной почте.

Здесь также обеспечивается соответствие требованиям международных стандартов для оптимизации поиска важных событий в журналах системы безопасности.

Помимо самостоятельного анализа угроз, Deep Security может также уведомлять систему управления событиями безопасности (например, ArcSight) об инцидентах для сопоставления моделей угроз, формирования отчетов и архивации.

Контроль целостности

Механизм контроля целостности в виртуальных машинах является важным элементом функционала защиты Trend Micro Deep Security. Система осуществляет наблюдение за важными элементами операционных систем и приложений, например, каталогами, разделами реестра и значениями, в целях поиска вредоносных и незапланированных изменений.

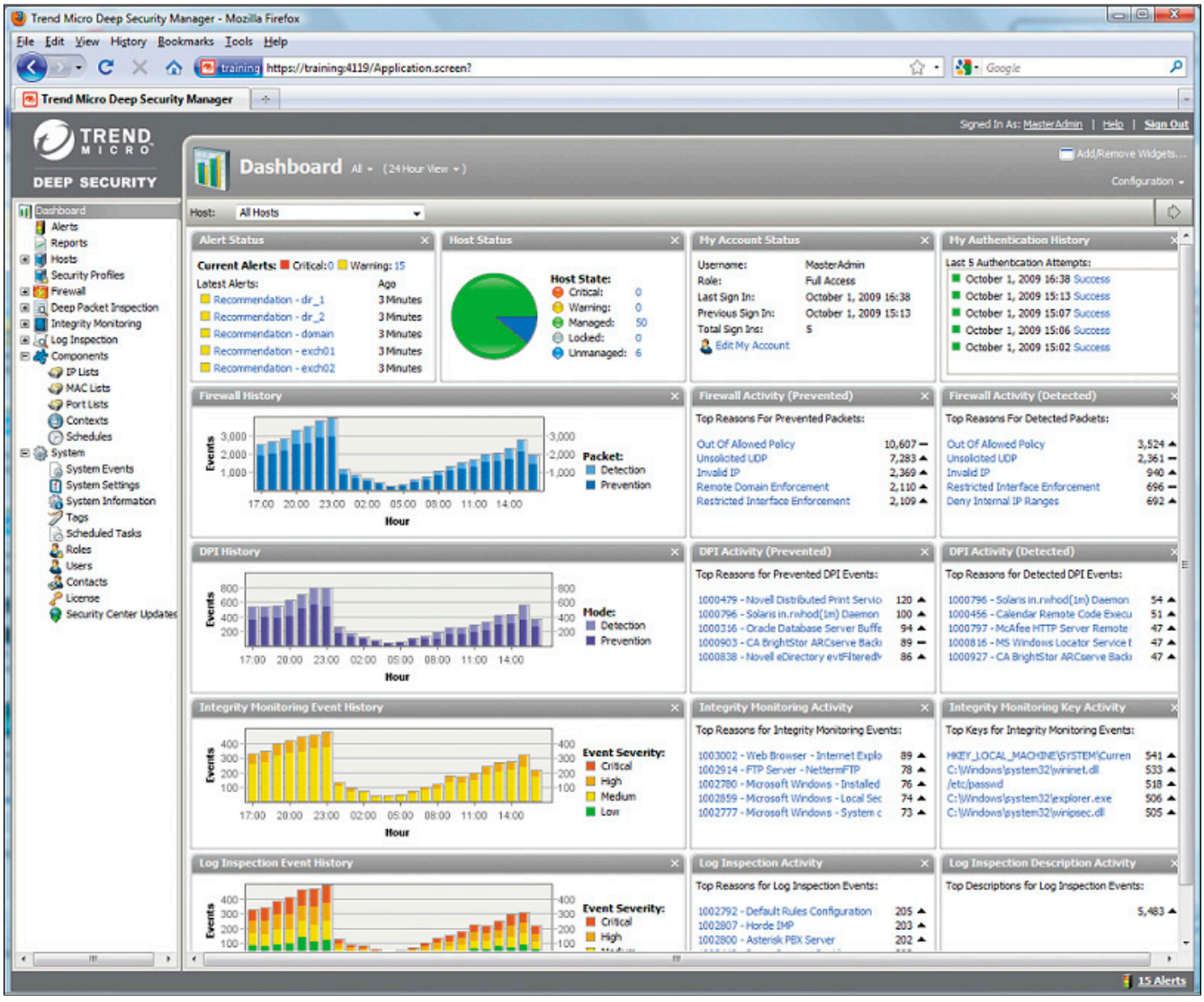
Deep Security производит поиск изменений в существующих файловых системах, а также анализ создаваемых файлов и оповещение о них в реальном времени.

Сканирование на наличие изменений может производиться по требованию, по расписанию или в реальном времени. Также имеется возможность проверки свойств файлов в соответствии со стандартами и наблюдение за отдельными каталогами.

Имеются средства гибкого мониторинга с возможностью указания исключений и доступные для проверки отчеты (см. рис. 3).

И хотя ряд функций, таких как контроль целостности файлов, требует установки агента, большая часть имеющихся в решении инструментов доступна без установки данного программного обеспечения. Однако его использование поз-

Рисунок 3. Отчеты Deep Security



воляет заметно снизить нагрузку на вычислительные мощности виртуальной машины.

Снижение нагрузки при сканировании

Вопрос об экономии мощностей в виртуальной среде нужно рассмотреть особо. Когда мы защищаем группу физических машин от вредоносного кода, нам необходимо на каждую из них поставить антивирусную систему. Когда мы защищаем группу виртуальных машин, мы также можем поставить агентов антивирусной системы на каждую из машин.

Но если нам необходимо произвести сканирование всех виртуальных машин, да еще и одновременно, то нагрузка на аппаратные серверы, содержащие эти машины, возрастет кратно их количеству. Для того чтобы снизить эту нагрузку, Trend Micro Deep Security содержит ядро системы защиты от вредоносного кода на физической машине, и при сканировании запускается лишь один процесс, который проверяет все виртуальные машины. Это существенно экономит ресурсы и снижает нагрузку аппаратного обеспечения host-серверов.

Данное обстоятельство является еще одним преимуществом использования Trend Micro Deep Security перед «традиционными» средствами антивирусной защиты.

***

До недавнего времени защита виртуальных машин осуществлялась теми же средствами, что и защита физических серверов и рабочих станций. То есть использовались те же антивирусы, межсетевые экраны и другие инструменты для обеспечения безопасности. Однако с развитием корпоративных средств виртуализации выявились недостатки такого подхода.

Вполне очевидно, что для виртуальной среды требуются специализированные средства защиты, одно из которых – Trend Micro Deep Security. Данный продукт сегодня обладает наиболее развитым функционалом по обеспечению антивирусной защиты, предотвращению вторжений и анализу трафика для гостевых систем, являясь надежным средством обеспечения безопасности данной среды от вредоносного кода.

В следующих статьях я расскажу подробнее о продуктах vGate и семействе продуктов vShield, также предназначенных для решения различных задач по обеспечению безопасности в виртуальной среде. EOF

1. Презентация Trend Micro Deep Security с конференции VMware – http://www.slideshare.net/bezkod/ss-6092854.
2. Программа конференции VMware – http://www.idc-cema.com/?showproduct=40396&content_lang=RU&action=Agenda.
3. Описание продукта VMware View – http://www.vmware.com/ru/products/view.
4. Описание vSphere, содержащее информацию о VMsafe – http://www.vmware.com/ru/products/oldvsphere/features.html.
5. Сайт, посвященный PCI DSS – http://www.pcidss.ru.

Рисунок 4. Консоль управления Deep Security