Защита в виртуальном мире

Обзор функциональных возможностей решения SafeNet ProtectV™, позволяющего на корпоративном уровне обеспечивать защиту виртуальных инфраструктур от различных угроз ИБ (включая защиту от суперпользователя) при полном разделении управления компонентами безопасности между пользователями, администраторами и офицерами безопасности.

Рожнов Михаил – ведущий эксперт компании "Сертифицированные информационные системы".

Введение

Сегодня своя виртуальная инфраструктура есть практически в каждой компании. Это обусловлено тем, что содержать парк физических машин стало нецелесообразно. Плюсы очевидны – загруженность физических машин в своем максимуме достигает 15%. Консолидация парка физических машин на единую аппаратную платформу позволяет увеличить этот показатель до 70%, снизив при этом издержки на содержание станций до половины. Да и тот немалый функционал, который предоставляет среда, настолько вошел в ежедневный обиход, что отказаться от него уже невозможно. Помнится, как с опаской народ переходил в новую среду, как бурно обсуждались вопросы совместимости программного обеспечения при переносе его в «неродное окружение». Сегодня это уже в прошлом, и клиентов, мигрировавших в эту среду или завершающих этот процесс, с каждым днем все больше и больше.

Однако возникает интересный вопрос: насколько разумно держать среду виртуализации у себя в компании, а не брать ее у других в аренду? Решение такое, конечно, имеет право на существование, скорее всего, так и будет – снижение общей стоимости владения, снижение затрат ресурсов на администрирование. Но есть в компании одно подразделение, которое, скорее всего, скажет «нет». Это отдел информационной безопасности.

Угрозы для сред виртуализации

Рассмотрим, какие же угрозы актуальны на данный момент для сред виртуализации и существуют ли решения, которые позволят реализовать данную схему функционирования – «работа с виртуальной инфраструктурой, размещенной в неконтролируемом периметре». Для начала выберем претендента, который будет обеспечивать среду виртуализации. Основываясь на аналитическом отчете Gartner, выбираем решение VMware vSphere. Решение включает в себя следующие компоненты: гипервизор первого типа, VMware vCenter – приложение, являющееся средством централизованного управления виртуальной инфраструктурой, и VMware Tools – набор утилит, который повышает производительность гостевой операционной системы виртуальной машины и улучшает управление ею. Так как решение представляет собой набор программных компонентов, то все уязвимости, присущие обычному программному обеспечению, также справедливы и для среды виртуализации. В данной статье мы не будем углубляться в различные уязвимости решения VMware vSphere (если у читателя появится интерес к данной теме, он может обратиться к ресурсу *http://www.cvedetails.com/vulnerability-list/vendor_id-252/Vmware.html*), лишь отметим, что данные возможности позволяют повысить привилегии вплоть до административного уровня и получить доступ с высокими правами к данным и конфигурационным файлам среды. Правило одно – необходимо сохранять систему в актуальном состоянии, периодически проводя инсталляцию всех обновлений. Но бывает и так, что уязвимость еще не опубликована, а на «закрытых» ресурсах эксплойты уже лежат. В данной ситуации машины находятся под угрозой, что незамедлительно требует применения наложенных средств защиты во избежание утечки информации.

Второй тип угроз, который мы рассмотрим, – это ошибки при конфигурировании системы. Администраторы среды виртуализации, а в некоторых случаях и офицеры безопасности при конфигурации прав доступа могут допустить неточности, такие как установка наследования привилегий на все дочерние объекты узла. Это может привести к повышению привилегий с возможностью получения конфиденциальной информации.

Ну и третий тип угроз, который стал наиболее актуальным после раскрытия информации Эдвардом Сноуденом – это внутренний нарушитель. Внутренний нарушитель может совершать абсолютно любые действия, которые, с одной стороны, могут выглядеть безопасными и направленными на усиление функций защиты (например, использовать так называемый «promiscuousmode», который позволяет принимать все пакеты независимо от того, кому они адресованы, обычно используется для систем анализа трафика), а на самом деле – использовать в злонамеренных целях. Не исключен и самый простой вариант получения доступа к данным – копирование виртуального жесткого диска, монтирование его в аналогичной среде и анализ как «сырых данных». К сожалению, эти атаки актуальны и имеют практические реализации.

Но существовать в виртуальном мире возможно, и главное – делать это безопасно. Компания SafeNet, являясь одним из крупнейших игроков на рынке разработчиков средств защиты информации, видит большие перспективы в части виртуализации и уже разработала специализированное решение для защиты виртуальных контейнеров (виртуальных машин) – SafeNet ProtectV™. Далее мы рассмотрим экосистему решения, а также отметим те преимущества, которые предлагает данный комплекс.

Решение SafeNet ProtectV™

Решение SafeNet ProtectV™ представляет собой программный (программно-аппаратный) комплекс, предназначенный для реализации следующих показателей защищенности:

1) доверенная загрузка виртуальных машин – администратор среды виртуализации имеет привилегии для старта виртуальной машины (контейнера), но загрузка гостевой операционной системы будет возможна только при условии, что субъект решения ProtectV (а этот субъект не пересекается с пользователями виртуальной инфраструктуры) разрешит выполнение данной операции;
2) прозрачное шифрование виртуальных жестких дисков, включая системные разделы и MBR-запись. Для выполнения данной операции ProtectV использует алгоритм шифрования AES-256. Поддержки ГОСТ пока нет, но оценивая рынок для данного решения, компания SafeNet планирует выполнить интеграцию российских криптоалгоритмов и пройти процедуру сертификации в обозримом будущем;
3) централизованное управление жизненным циклом ключей шифрования. Ключи шифрования всегда расположены в контролируемой зоне, поэтому кража зашифрованного контейнера никогда не приведет к утечке конфиденциальной информации;
4) ролевой принцип контроля доступа к объектам виртуальной инфраструктуры. Решение позволяет изолировать пользователей, отвечающих за безопасность, от пользователей среды виртуализации. Это гарантирует невозможность повышения привилегий, и как следствие, полное разделение обязанностей в части администрирования и безопасности;

Таблица 1. Поддерживаемые операционные системы.

Операционная система	VMware	AWS	Физическая среда
Microsoft Windows Server 2003 R2 (32-bit), SP2	Да	Да	Да
Microsoft Windows Server 2003 R2 (64-bit), SP2	Да	Да	Да
Microsoft Windows Server 2008 (32-bit), SP2	Да	Да	Да
Microsoft Windows Server 2008 (64-bit), SP2	Да	Да	Да
Microsoft Windows Server 2008 R2 (64-bit), SP1	Да	Да	Да
Microsoft Windows Server 2012 (64-bit)	Да	Да	Да
CentOS Linux 6.2 (64-bit)	Нет	Да	Нет
SUSE Linux Enterprise Server (SLES) 10 SP4, 64-bit	Да	Нет	Нет
SUSE Linux Enterprise Server (SLES) 11 SP1, 64-bit	Да	Нет	Нет
Red Hat Enterprise Linux (RHEL) 5.8, 64-bit	Да	Да	Нет
Red Hat Enterprise Linux (RHEL) 6.2, 64-bit	Да	Да	Нет
Red Hat Enterprise Linux (RHEL) 6.3, 64-bit	Да	Да	Нет

5) Аудит – решение позволяет выполнять регистрацию действий пользователей и при необходимости синхронизировать информацию с внешним syslog-сервером.

Актуальная версия комплекса поддерживает работу с гипервизорами от компании VMware – это VMware vSphere 4.1, 5.0, 5.1, 5.5, а также средой виртуализации (облачной инфраструктурой) от компании Amazon. Функционал продукта не зависит от среды виртуализации, однако, в силу меньшей популярности сервиса Amazon AWS (Amazon Web Services) в России, в данной статье мы будем рассматривать только гипервизор от VMware. Также необходимо отметить, что решение способно работать в гетерогенной среде, то есть в окружении, которое содержит физические машины. Функционал при этом незначительно изменяется. А именно: запуск машины возможен только при физическом доступе, процедура доверенной загрузки строится на механизме Challenge-Response (данный механизм будет раскрыт ниже).

Далее хотелось бы рассмотреть экосистему программного комплекса, выделить основные элементы и показать отличие

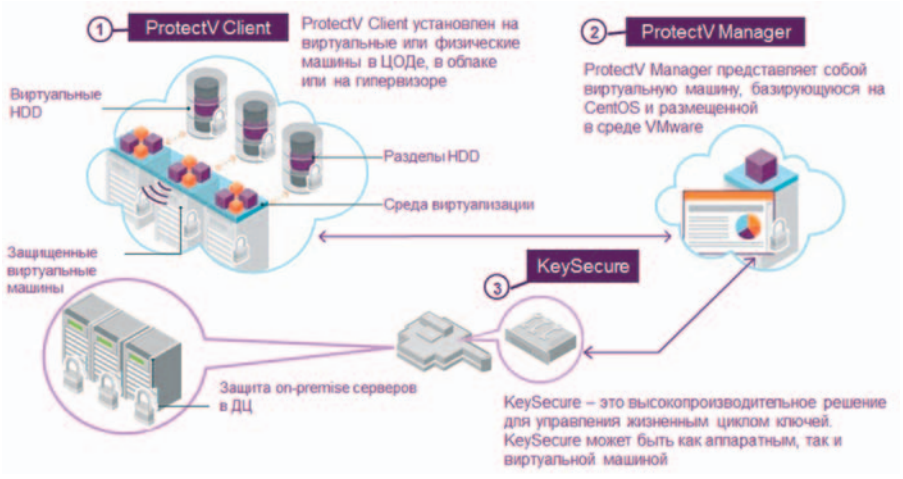

Рис. 1. Архитектура решения SafeNet ProtectV.

Рис. 2. «BoottoOS» – старт операционной системы.

Enterprise-решения от существующих аналогов для рабочих станций. Архитектура решения представлена на рис. 1.

Основными компонентами являются следующие элементы (архитектура полностью идентичная как для среды виртуализации VMware, так и для гибридной среды и среды Amazon AWS):

– *ProtectV Manager* – виртуальное устройство, разворачиваемое в среде виртуализации и предоставляющее web-консоль для администрирования. Компонент работает в режиме кластера, что обеспечивает его отказоустойчивость;

– *ProtectV Client* – программный агент, инсталлируемый в гостевую операционную систему, либо физическую среду. Поддерживаемые операционные системы текущей версией ProtectV представлены в табл. 1;

– *KeyManager* – аппаратная или программная (virtual appliance) реализация хранилища ключевой информации от компании SafeNet: SafeNet KeySecure или SafeNet DataSecure (отличие от KeySecure состоит в наличии криптопроцессора, который может использоваться для шифрования внутри устройства для других решений от компании SafeNet, например SafeNet ProtectDB). Устройство обеспечивает процедуру управления жизненным циклом ключей шифрования (генерация ключа, передача ключа до узла шифрования, безопасное резервное копирование, безвозвратное удаление ключа на устройстве и т.д.). Компонент работает в режиме кластера, что обеспечивает его отказоустойчивость.

Доверенная загрузка

Доверенная загрузка гостевой операционной системы становится доступной сразу после инсталляции агента и шифрования одного из разделов. Для пользователя это выглядит довольно просто: администратор ProtectV Manager создает специализированный пул виртуальных машин и назначает субъекта, ответственного за старт виртуальных машин и старт операционных систем. Механизм защиты состоит в том, что при условии старта виртуальной машины администратором датацентра, она будет находиться в состоянии ожидания запуска операционной системы до тех пор, пока не получит разрешение от субъекта на выполнение данного действия из консоли ProtectV Manager (операция «Boot-toOS», рис. 2).

Доверенная загрузка физического сервера строится на технологии Challenge-Response. Для пользователя это выглядит следующим образом: после физического старта машины система отображает окно, содержащее некоторую последовательность. Субъект, обладающий правами на запуск операционной системы, должен авторизоваться в web-интерфейсе ProtectV Manager, скопировать данную последовательность и получить от сервера на нее ответ (Response). Ответную последовательность необходимо ввести на физическом сервере и при условии, что ответ будет сформирован в соответствии с Challenge, операционная система будет успешно загружена (рис. 3).

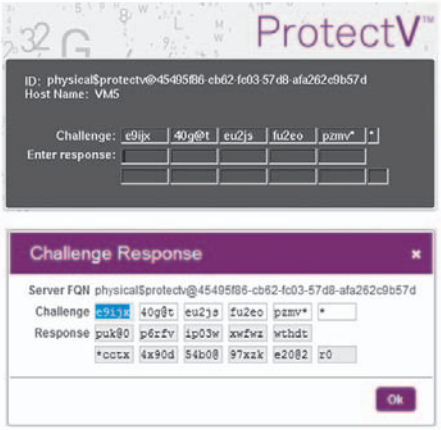

Рис. 3. «Challenge-Response» – старт ОС на физической машине.

Шифрование

Основное назначение изделия – выполнять прозрачное шифрование как виртуальных, так и физических жестких дисков. При этом, в отличие от других конкурентных решений, шифрованию подвержены как системные разделы (включая MBR), так и разделы с данными (включая файл подкачки). Прозрачность позволяет начать шифрование дискового пространства, не прерывая работы систе-

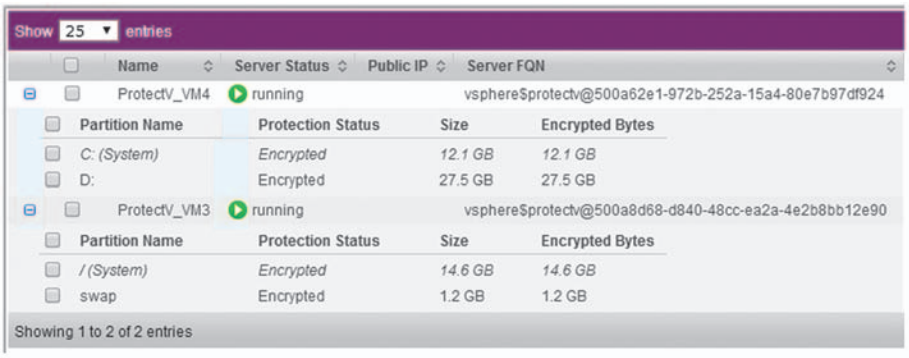

Рис. 4. Шифрование разделов средствами ProtectV.

мы. При этом ни для операционной системы, ни для приложений процедура шифрования абсолютно незаметна. Для пользователя эта процедура также тривиальна: после успешного прохождения процедуры аутентификации на web-консоли ProtectV Manager, пользователь видит все разделы машины (виртуальной или физической), выбрав один или несколько разделов при наличии привилегий на выполнение операции шифрования, пользователь может ее начать. При этом процедура генерации ключа шифрования, сопоставление ключа с объектом (машина, раздел дискового пространства), передача ключа в систему – все это решается за счет компонентов комплекса без требования вмешательства администратора (рис. 4). Следует также отметить, что при выполнении каких-либо административных операций с дисковыми объектами виртуальной инфраструктуры, они также остаются зашифрованными (например, при создании снимков виртуальных машин).

Заключение – для чего это нужно?

Когда речь заходит о вопросах безопасности, говорить о выгоде использования решения достаточно сложно: «Вы не получите выгоды от использования данного решения, но Вы будете уверены в отсутствии неудач». Виртуализация стала незаменима в повседневной жизни, в том числе в областях обработки критически важных объектов. Помимо преимуществ, появляются и новые угрозы, с которыми необходимо бороться. Сложность, конечно же, состоит в том, что защищать необходимо то, что находится в неконтролируемом периметре, «это что-то мое, но не в моих руках». Решение одно – использовать шифрование, при этом критически важным объектом является не компонент, отвечающий за шифрование, а централизованное хранилище ключей. Это, в первую очередь, отличает решение ProtectV от конкурентов не Enterprise-уровня. Когда парк виртуальных машин – один–два объекта, все достаточно просто, но как только парк разрастается, возрастает и сложность по администрированию средства защиты. Прозрачность реализации, простота развертывания и автоматизация действий позволяет использовать ProtectV для сегмента любого масштаба, при этом технологию защиты можно расширить и на физическую среду, что унифицирует его применение.

Рожнов Михаил,
компания "Сертифицированные информационные системы".

IBM: комплексная система безопасности для борьбы с киберугрозами

Май 2014 г. – IBM представила новые программные решения IBM Threat Protection System и Critical Data Protection Program, которые стали результатом обширных инвестиций IBM в системы безопасности на протяжении двух последних лет. В частности, корпорация приобрела такие компании как Q1 Labs, Trusteer, Guardium, Ounce Labs, Watchfire и Fiberlink / MaaS 360. С момента своего выхода на этот рынок в 2011 г. IBM успела стать одним из крупнейших игроков и показать значительный рост на протяжении шести кварталов. Согласно данным IDC ' s Software Tracker, за 2013 год компания продвинулась с 4-го места до 3-го среди поставщиков систем безопасности.

Новые решения призваны помочь организациям защитить важные данные от продвинутых угроз, атак нулевого дня и утечек, используя всеобъемлющую поведенческую аналитику и исследовательскую экспертизу. Согласно двум исследованиям, проведенным Ponemon Institute по заказу IBM, финансовые потери от утечки данных возросли на 15% по всему миру, в среднем составив $3,5 млн. Большинство опрошенных компаний отметили, что целевые атаки представляют наибольшую угрозу – ущерб от них составил в среднем $9,4 млн.

Решение IBM Threat Protection System объединяет систему безопасности и поведенческую аналитику в одном инструменте, который превосходит традиционные защитные системы и средства межсетевой безопасности и предотвращает атаки на всех уровнях – от взлома до выхода из системы.

Система IBM Threat Protection System включает комплексный портфель программного обеспечения для экспертного анализа данных, которое помогает организациям выявлять, предотвращать и реагировать на сложные кибератаки, а также устранять угрозы до того, как они успеют навредить предприятию. Среди ключевых возможностей:

– *предотвращение угроз.* IBM представила новое решение Trusteer Apex для блокирования вредоносных программных средств, усовершенствованные возможности оборудования IBM Network Protection для помещения подверженных угрозе участков системы в карантин, а также новые решения, интегрированные с сетевыми средами компаний-партнеров;
– *обнаружение.* IBM усовершенствовала платформу QRadar Security Intelligence благодаря новым функциональным возможностям, которые позволяют организациям своевременно выявлять угрозы и блокировать действия злоумышленников;
– *реагирование.* IBM представила решение IBM Security QRadar Incident Forensics, а также продолжает развивать глобальный портфель сервисов для управления реагированием на аварийные ситуации.

Заказчики, тестирующие IBM Threat Protection System, уже заметили положительные результаты. К примеру, благодаря решению IBM один поставщик медицинских услуг провел мониторинг тысяч устройств и выявил десятки вредоносных программ, с чем не справились бы традиционные системы безопасности. Найденные вредоносные программные средства могли быть использованы с целью получения несанкционированного удаленного доступа к устройствам компании и дальнейшей кражи данных, однако были полностью выведены из строя благодаря системе IBM. Таким же образом один из крупнейших европейских банков сумел избавиться от скрытых вредоносных программ, распространенных по всей организации.

IBM Threat Protection System поддерживается по всему миру благодаря центрам управления безопасностью (Security Operation Centers, SOC), которые осуществляют мониторинг функционирования систем, развернутых заказчиками. Специалисты IBM также могут оказывать услуги по развертыванию и интеграции систем заказчиков в центрах управления безопасностью.

«Эволюция продвинутых угроз оказала большое влияние на подход организаций к обеспечению безопасности данных, – прокомментировал Брендан Ханниган *(Brendan Hannigan)*, генеральный директор IBM Security Systems. – Сегодня защита от кибератак требует большего, чем просто наличие системы аутентификации по подписи и защиты периметра сети. Возможности аналитики данных и экспертного анализа киберугроз крайне важны для защиты конечных устройств, обеспечения безопасности периметра и предотвращения атак до того, как они нанесут вред организации».

Новое решение Critical Data Protection Program помогает защитить наиболее ценные данные организации. Как правило, на изменение дохода компании оказывают влияние не более чем 2% данных предприятия, от которых также зависит конкурентное преимущество организации, репутация бренда, рыночная стоимость и общий рост.

«Руководство большинства компаний считает защиту критически важных данных от кибератак своей приоритетной за-