# Защита виртуальных рабочих станций. Устранение последнего препятствия на пути к повсеместному использованию

Саймон Кросби (Simon Crosby), главный технический директор подразделения Datacenter & Cloud, компания Citrix Systems, Inc.

В мае 2010 года компании Citrix и McAfee объявили о подписании соглашения о стратегическом партнерстве и сотрудничестве, целью которого является упрощение и расширение возможностей масштабирования систем безопасности виртуальных рабочих станций для крупных предприятий. Сотрудничество двух лидеров в сфере безопасности и виртуализации позволит заказчикам решения Citrix XenDesktop расширить управление безопасностью рабочих станций до виртуальных сред с помощью платформы McAfee® ePolicy Orchestrator®. Подписанное соглашение стало результатом растущего пользовательского спроса на интегрированные решения по управлению безопасностью в рамках крупных проектов по виртуализации рабочих станций.

Имея некоторый опыт разработки решений виртуализации, в том числе передовой продукт для виртуализации рабочих станций Citrix XenDesktop, компании Citrix, несомненно, есть что предложить в этой области. Однако мы отнюдь не являемся специалистами в области безопасности. Компания Citrix понимает, насколько важную роль играет безопасность для виртуальных рабочих станций и серверов. Поэтому мы считаем, что сотрудничество с партнерами, являющимися специалистами в данной сфере, является безусловно эффективнее попыток самостоятельно встроить функции безопасности в наши решения виртуализации. Партнерство компаний Citrix и McAfee выгодно прежде всего нашим клиентам, поскольку оно позволяет им оптимально использовать все преимущества визуализации.

Такое партнерство важно, поскольку, несмотря на очевидные преимущества, переход компаний на виртуальные решения осуществляется медленнее, чем предполагалось, это прежде всего касается виртуализации рабочих станций (или инфраструктуры виртуальных рабочих станций, VDI). Согласно имеющимся данным, инфраструктура виртуальных рабочих станций имеется сегодня лишь у 40 процентов от общего числа компаний, которые могли бы извлечь пользу из ее применения. Аналитические компании, такие как Gartner, полагают, что низкие темпы внедрения данной технологии прежде всего связаны с опасениями по поводу того, что обеспечение безопасности может отрицательно сказаться на производительности в виртуализированной среде. Такие опасения имели под собой веские основания. Но только до сих пор.

Вот некоторые из них. Не имея решений, оптимизированных для виртуальных сред, ИТ-службам приходилось обеспечивать безопасность виртуальных машин и рабочих станций таким же образом, как и безопасность конечных точек, иными словами, одна программа безопасности на одну конечную точку. Воспринимая каждую виртуальную машину (ВМ) как конечную точку, нуждающуюся в защите, ИТ-службы, как правило, развертывали одну программу-агент безопасности на каждой ВМ или виртуальной рабочей станции.

Такая модель хороша для традиционных конечных точек, однако влечет за собой большие проблемы в виртуализованной среде. Поскольку одна физическая машина может являться «вместилищем» для большого количества виртуальных машин или виртуальных рабочих станций, каждая из которых имеет собственную программу безопасности, физический сервер перегружается многочисленными копиями программ безопасности, файлами сигнатур, базами данных об угрозах и т. д. Такой подход приводит к нерациональному использованию ресурсов ЦП, памяти и дискового пространства.

Но главной проблемой является производительность. Если все эти системы защиты конечных точек начинают обновляться в одно и то же время, происходит то, что я называю «антивирусным штормом», который вызывает катастрофическое падение производительности. Такая модель может привести к быстрому и полному истощению всех ресурсов ЦП и памяти, замедлению работы сети и возникновению «узких мест» интерфейсов ввода-вывода. Например, если у вас на одном сервере параллельно работают 120 систем безопасности, то совсем неудивительно, что ИТ-администраторы серьезно озабочены вопросом производительности.

Для решения проблемы производительности при обеспечении безопасности решений виртуализации некоторые поставщики продуктов виртуализации предприняли попытки усилить функции безопасности. Их усилия бесспорно заслуживают похвалы, однако специалисты Citrix не считают этот путь правильным. Как уже упоминалось выше, мы считаем, что наибольшую пользу нашим клиентам принесет интегрированный подход с использованием передовых решений в данной области. Citrix открыто признает, что «выискивать злоумышленников» — это не наш конек. Для нас партнерство с McAfee представляет собой идеальное совмещение широчайшего спектра продуктов безопасности с исключительно большим выбором моделей предоставления сервисов.

С учетом этого Citrix и McAfee выработали совместный подход, который выводит функцию безопасности за пределы виртуальной машины, позволяя виртуальной инфраструктуре выполнять функции обеспечения безопасности гостевых виртуальных машин. Одним из преимуществ данного подхода является способность обеспечивать безопасность самой виртуальной инфраструктуры, которая также уязвима и нуждается в надлежащей защите. Но главное преимущество — это высокая производительность.

Платформа McAfee Management for Optimized Virtual Environments (McAfee MOVE), поддерживающая решение Citrix XenDesktop, обеспечивает функции управления безопасностью, специально разработанные для виртуализированных сред. Отказавшись от принципа установки программ безопасности конечных точек для каждой виртуальной машины, решение McAfee MOVE AntiVirus for Virtual Desktops представляет собой виртуальное устройство, объединяющее процессы сканирования и обновления сигнатур и обеспечивающее защиту всех виртуальных рабочих станций при существенном расширении возможностей масштабирования.

Посредством выноса функций безопасности за пределы виртуальной машины мы получили возможность использования интеллектуальных технологий сканирования, что позволяет ИТ-администраторам осуществлять плановое сканирование в наиболее удобное для этого время, исходя из загрузки гипервизора, или тогда, когда образы виртуальных машин находятся в автономной режиме. Этот подход позволят также централизовать ресурсоемкие процессы, снижая нагрузку на отдельные виртуальные машины. Кроме того, данное решение упрощает работу ИТ-служб, централизуя процесс управления безопасностью и позволяя без труда управлять поиском вирусов и обновлением файлов вирусных сигнатур с единой консоли, например McAfee ePolicy Orchestrator. В результате, снизив требования к ресурсам ЦП, памяти и дисковому пространству и упростив управление безопасностью, нам удалось повысить уровень безопасности и масштабирования виртуальных рабочих станций.

Результаты действительно феноменальны! По результатам тестов, выполненных McAfee и Citrix, решение McAfee MOVE AntiVirus for Virtual Desktops позволяет увеличить количество виртуальных машин в три раза по сравнению с решениями, предусматривающими установку средств защиты конечных точек для каждой виртуальной машины. Такая эффективность абсолютно необходима для компаний, желающих использовать виртуальные рабочие станции. Мы уверены в том, что это решение устраняет главную преграду на пути широкого внедрения технологий виртуализации.

Дополнительную информацию о том, как партнерство McAfee и Citrix может помочь вам реализовать преимущества безопасной виртуализации рабочих станций см. на сайте www.mcafee.com/ru/partners/global-alliances/citrix-systems.aspx или www.mcafee.com/ru/solutions/virtualization/virtualization.aspx.

---

**Саймон Кросби (Simon Crosby)** — главный технический директор подразделения Datacenter & Cloud компании Citrix. Он был основателем и техническим директором компании XenSource, которая позже была приобретена Citrix Systems. До основания XenSource работал ведущим инженером компании Intel. Кроме того, был основателем компании CPlane Inc., занимавшейся разработкой ПО для оптимизации сетей.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru


14103brf_virtualization_0910_fnl_ASD