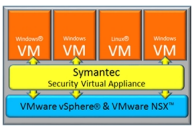
Автор:
30.12.14 22:00 -

Мы начинаем рассказ о группе продуктов компании Symantec, входящей в семейство Data Center Security, как следует из названия -предназначенных для защиты центров обработки данных.

В этой статье пойдет речь о продукте Data Center Security: Server 6.0 который является безагентским антивирусом для сред VMware и использующий для управления платформу VMware NSX.

С точки зрения архитектуры все довольно традиционно: используется виртуальный аплайнс,содержащий в себе антивирусный движок, на каждом из хостов гипервизора и, используя VMware vShield Endpoint аплайнс получает доступ к файловой системе защищаемых виртуальных машин для их проверки, не используя агентов.



Естественно, продукту присущи все ограничения vShield Endpoint, такие как: поддерживаемые типы операционных систем (на данный момент только семейства Microsoft Windows), необходимость установки VMware Tools, невозможность защиты помяти в безагентском режиме и т.д. Так же новая версия vShield Endpoint, позволяет использовать использовать репутационные технологии при проверке файлов, что значительно снижает нагрузку на системы хранения.

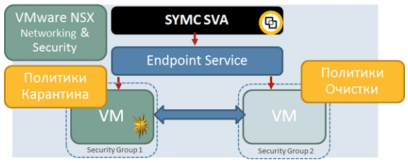
Первое ключевое отличие от большинства безагентских решений в том, что развертывание виртуальных аплайнсов и назначение политик безопасности на группы производится через консоль VMware NSX. В консоли управления самого продукта политика только создается и, затем, публикуется на VMware NSX.

После регистрации продукта во вкладе Services вы получаете дополнительный сервис безопасности, который вы можете установить для определенных групп кластеров и

датацентров, устаналивая виртуальные аплайнсы только для тех групп ипервизоров, которые вы указали.

VMware NSX предоставляет механизм создания групп безопасности, в которые могут быть включены виртуальные машины по определенным критериям. При этом группы могут быть статическими, где виртуальные машины в них добавляются вручную, так и динамические, когда в группы включаются виртуальные машины, соответствующие определенным криетериям, например тип операционных системи т.д. Самое интересное - это возможность изменять членство виртуальных машин в группах динамически, на основании тегов.

Один из примеров использования тэгов – перемещение виртуальных машин, на которых было обнаружено вредоносное ПО, в специальную карантинную группу. На группу карантина может быть назначена, например, отдельная политика межсетевого экрана (встроенного от VMware или стороннего), предотвращая распространение вредоносного ПО по сети до момента ее удаления. После удаления вредоносного ПО виртуальная машина будет возвращена в стандартную группу и продолжит функционирование.



Разумеется, теги на виртуальных машинах могут быть изменены, помимо вышеописанного решения, и с помощью продуктов сторонних компаний, например IPS систем от PaloAlto Networks, систем управления уязвимостями от Rapid7 и т.д. Таким образом можно не только назначать различные политики на группы виртуальных машин, но и интегрировать между собой различные решения от разных производителей.

Автор:
30.12.14 22:00 -

В скором времени ожидается выход новой версии продукта DCS: Server 6.5, в котором будет добавлен функционал сетевого IPS.

Получить тестовую версию продукта вы можете по ссылке http://www.symantec.com/data-center-security/trialware/

Read more http://feedproxy.google.com/~r/Vmguru-tech/~3/sFbMPOMKfdM/syamntec-data-center-security