



Код безопасности
ГК «Информзащита»

vGate

Сертифицированная защита виртуальной инфраструктуры

vGate решает все возложенные на него функции защиты. Даже если злоумышленник попал в ЦОД, то, в худшем случае, самое серьезное, что он сможет совершить – это удалить незащищенные файлы виртуальных машин.

Руслан Чиняков,
Директор Департамента СХД и инфраструктурного ПО



О компании

Компания OCS образована в 1994 г. Занимается дистрибуцией компьютерной техники, телекоммуникационного, периферийного, сетевого оборудования, компонентов, СХД, ПО

(в том числе инфраструктурного), расходных материалов. Имеет самую широкую региональную сеть офисов со складами – в 23 городах России.

OCS фокусируется на проектной и вольюмной дистрибуции: работе с системными интеграторами, поставщиками корпоративного рынка, розничными сетями, представителями российской сборки, разработчиками ПО, универсальными реселлерами и др. Партнерская база OCS не имеет аналогов по региональному присутствию и объему – более 6500 компаний России. Продуктовый портфель насчитывает более 70 линеек от ведущих мировых вендоров.

OCS входит в состав «Национальной компьютерной корпорации» (НКК), крупнейшего многопрофильного холдинга на российском ИТ-рынке (рейтинг Forbes, «Эксперт», «Финанс.», и др.).

Весной 2010 года, в рамках программы тестирования аппаратного и программного обеспечения, применяемого при построении инфраструктуры ЦОД, в демо-центре компании OCS был установлен новый программный продукт Security Code vGate for VMware Infrastructure от отечественного производителя «Код Безопасности». В этом центре партнерам и их заказчикам показываются продукты Brocade, EMC, Riverbed, Symantec и VMware. Оборудование и ПО позволяют построить модель ЦОД практически любой сложности, в том числе с полным резервированием и катастрофоустойчивостью. Кроме демонстраций, центр служит для пилот-проектов, проведения тестов на функциональность и производительность, а также для регулярно проводимых тренингов для партнеров и их заказчиков.

ПО vGate служит для обеспечения сертифицированной защиты виртуальной инфраструктуры. Собственные средства VMware способны обеспечивать безопасность на основе механизма ролевого доступа с интегрированной поддержкой Active Directory или стандартной схеме авторизации Windows (при использовании vCenter) или Linux (при использовании изолированных ESX-хостов). Однако, согласно требованиям регулирующих органов, использование встроенных средств защиты недостаточно.

Совместное использование продуктов VMware с программным обеспечением vGate, прошедшим сертификацию ФСТЭК по уровню СВТ 5 и НДВ 4, дает возможность получить преимущества от виртуализации государственным организациям и компаниям, работающим с персональными данными.

Продукт обеспечивает следующий функционал:

- Контроль доступа к хостам ESX, виртуальным машинами vCenter
- Доверенная загрузка виртуальных машин
- Аудит событий безопасности



О продукте

Security Code vGate for VMware Infrastructure – средство защиты информации, предназначенное для обеспечения безопасности виртуальной инфраструктуры на базе систем VMware Infrastructure 3 и VMware vSphere 4.

Применение vGate дает возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих данные ограниченного доступа и помогает провести аттестацию.

Сертификаты ФСТЭК России позволяют использовать vGate для защиты от несанкционированного доступа (НСД) конфиденциальной информации и персональных данных.

Программа состоит из нескольких компонентов – Сервера авторизации, Агента аутентификации и Модулей защиты ESX-сервера. Сервер авторизации и Агент аутентификации устанавливаются на Windows-платформу, а Модули защиты на ESX-сервера. Установка программы не вызывает осложнений у опытного администратора ESX. После установки требуется провести конфигурирование сервера - процесс настройки детально описан в документации.

После настройки продукта получение доступа к управлению серверами ESX и vCenter возможно только после авторизации на Сервере авторизации vGate. Запустить виртуальную машину на хосте ESX с установленными Модулями защиты vGate без авторизации не получится даже в случае доступа с другой машины, расположенной в управляющей подсети VMware.

Таким образом, продукт решает все возложенные на него функции защиты. Даже если злоумышленник попал в ЦОД, то, в худшем случае, самое серьезное, что он сможет совершить – это удалить незащищенные файлы виртуальных машин (которые могут быть восстановлены из резервной копии, если специализированными средствами регулярно проводится резервное копирование и тестирование восстановления). Сами виртуальные машины предлагается защищать традиционными для гостевых ОС средствами типа Secret Net.

К сожалению, в настоящей версии не поддерживается защита ESXi-серверов. Однако, в будущих версиях разработчик обещал исправить эту ситуацию.

Руслан Чиняков,

Директор Департамента СХД и инфраструктурного ПО

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетних наработок в области создания средств защиты информации для государственных и коммерческих заказчиков.



Код безопасности
ГК «Информзащита»

Тел.: +7 (495) 980-2345,
E-mail: info@securitycode.ru
www.securitycode.ru