Код безопасности

vGATE

Сертифицированное средство защиты платформ виртуализации на базе VMware vSphere или Microsoft Hyper-V

ПРЕИМУЩЕСТВА

- ПОДДЕРЖКА САМЫХ РАСПРОСТРАНЕННЫХ ПЛАТФОРМ ВИРТУАЛИЗАЦИИ – VMWARE VSPHERE И MICROSOFT HYPER-V
- КОНТРОЛЬ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ
- АВТОМАТИЧЕСКАЯ ПРОВЕРКА И ШАБЛОНЫ НАСТРОЕК НА СООТВЕТСТВИЕ СТАНДАРТАМ И ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ
- ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ ПО ЗАЩИТЕ СИСТЕМ ВИРТУАЛИЗАЦИИ

ВОЗМОЖНОСТИ

ПОДДЕРЖКА РАСПРЕДЕЛЕННЫХ ИНФРАСТРУКТУР

- Горячее резервирование серверов vGate.
- Поддержка работы с несколькими серверами vCenter, объединенными с помощью режима VMware vCenter Linked Mode.
- Подключение агента аутентификации к нескольким серверам авторизации vGate R2.
- Построение леса серверов авторизации vGate R2.
- Контроль управления Microsoft Hyper-V через System Center Virtual Machine Manager и Failover Cluster Manager.

РАЗГРАНИЧЕНИЕ ДОСТУПА К УПРАВЛЕНИЮ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРОЙ

- Усиленная аутентификация администраторов виртуальной инфраструктуры, в том числе двухфакторная, с использованием ключей iButton, eToken, JaCarta.
- Разделение ролей администраторов информационной безопасности и виртуальной инфраструктуры в целях исключения суперпользователя.
- Согласование изменений настроек виртуализации у администратора информационной безопасности.
- Мандатное управление доступом на основе категорий и уровней конфиденциальности.
- Контроль доступа администраторов виртуальной инфраструктуры к данным, обрабатываемым виртуальными машинами.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ И КОНТРОЛЬ

Консоль управления vGate R2 позволяет:

- Управлять учетными записями пользователей и правами доступа к защищаемым объектам.
- Развертывать и настраивать компоненты защиты ESX(i)-/vCenter-серверов и серверов Hyper-V.
- Управлять параметрами виртуальных машин.
- Просматривать журнал событий.
- Осуществлять горячее резервирование и работать в режиме кластера.
- Интегрировать продукт с SIEM-системами.

ЗАЩИТА ОТ СПЕЦИФИЧЕСКИХ УГРОЗ, ХАРАКТЕРНЫХ ДЛЯ ВИРТУАЛЬНЫХ СРЕД

- Контроль виртуальных устройств.
- Контроль изменений в системе на основе заданных политик безопасности.
- Контроль целостности и доверенная загрузка ESX(i)-серверов и виртуальных машин.

РЕГИСТРАЦИЯ И АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ

- Расширенная регистрация событий, связанных с информационной безопасностью.
- Создание структурированных отчетов о текущем состоянии системы и произошедших изменениях.
- Эффективный инструмент расследования инцидентов.

СЦЕНАРИИ ПРИМЕНЕНИЯ

ЗАЩИТА ВИРТУАЛЬНЫХ МАШИН

Результат:

- Минимизированы финансовые и репутационные риски, связанные с несанкционированным копированием, клонированием, переносом и уничтожением виртуальных машин.

ЗАЩИТА СРЕДСТВ УПРАВЛЕНИЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРОЙ

Результат:

- Средства управления виртуальной инфраструктурой размещены внутри защищаемого периметра и защищены от НСД.
- Минимизированы риски несанкционированного доступа к управлению системой виртуализации.

КОНТРОЛЬ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Результат:

- Разграничен доступ к управлению виртуальной инфраструктурой.
- Снижены риски простоя из-за повреждения администраторами виртуальной инфраструктуры и обрабатываемой в ней информации.
- Снижены риски финансовых потерь из-за утечек информации, связанных с недобросовестной работой администраторов виртуальной инфраструктуры.

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

Результат:

- Виртуальная инфраструктура приведена в соответствие требованиям нормативных документов:
  - Защита банковской тайны и платежных систем СТО БР ИББС (в том числе РС БР ИББС-2.8-2015), PCI DSS;
  - Требования ФСТЭК России: приказы №21 (ПДн), №17 (ГИС) и №31 (АСУ ТП), РД АС до класса 1Б.
  - Защита медицинской и других видов тайн.
- Минимизированы финансовые, репутационные и юридические риски, связанные с невыполнением требований регуляторов.

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ОТРАСЛЕВЫХ СТАНДАРТОВ

Результат:

- Снижено время внедрения и настройки средства защиты виртуальной инфраструктуры.
- Минимизированы финансовые и репутационные риски за счет приведения защиты среды виртуализации в соответствие с рекомендациями отраслевых стандартов и лучших международных практик.

СЕРТИФИКАТЫ

ФСТЭК России.

- vGate R2: СВТ5/НДВ4, для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до К1 включительно и АСУ ТП до К1 включительно.
- vGate-S R2: ТУ/НДВ2, для защиты АС до класса 1Б включительно (гостайна с грифом «совершенно секретно»), ИСПДн до УЗ1 включительно, ГИС до К1 включительно и АСУ ТП до К1 включительно.

ЛИЦЕНЗИРОВАНИЕ

ФУНКЦИОНАЛ	STANDARD[1]	ENTERPRISE
Идентификация и аутентификация субъектов и объектов доступа (в т.ч. двухфакторная)	●	●
Управление доступом в виртуальной инфраструктуре	●	●
Регистрация событий (аудит)	●	●
Управление потоками информации между компонентами виртуальной машины и по периметру виртуальной машины	●	●
Доверенная загрузка виртуальных машин	●	●
Управление перемещением виртуальных машин и обрабатываемых на них данных	●	●
Контроль целостности виртуальной инфраструктуры и ее конфигураций	●	●
Разбиение виртуальной инфраструктуры на сегменты	●	●
Создание и выгрузка резервной копии конфигурации vGate R2	●	●
Горячее резервирование и автопереключение сервера авторизации vGate R2		●
Подключение агента аутентификации к нескольким серверам авторизации vGate R2		●
Создание леса серверов авторизации (синхронизация настроек между серверами vGate R2)		●
Поддержка серверов управления vCenter Linked Mode		●
Контроль управления серверами Microsoft Hyper-V через System Center Virtual Machine Manager		●
Контроль управления через Failover Cluster Manager		●

[1] – vGate R2 версии 2.8 и более ранние версии приравниваются к редакции Standard.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка vGate может осуществляться как напрямую, силами специалистов «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера – партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов – обращается в службу технической поддержки вендора.

Существует несколько пакетов технической поддержки: Базовый, Стандартный, Расширенный, VIP

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) info@securitycode.ru www.securitycode.ru