КОД безопасности

vGATE

Сертифицированное средство защиты платформ виртуализации, обеспечивающее контроль инфраструктуры, действий администраторов и фильтрацию сетевого трафика на уровне гипервизора

ПРЕИМУЩЕСТВА

- БЕЗАГЕНТНЫЙ МЕЖСЕТЕВОЙ ЭКРАН УРОВНЯ ГИПЕРВИЗОРА
- МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ
- КОНТРОЛЬ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ
- ПОДДЕРЖКА ЗАРУБЕЖНЫХ И РОССИЙСКИХ ПЛАТФОРМ ВИРТУАЛИЗАЦИИ – VMWARE VSPHERE, MICROSOFT HYPER-V, СКАЛА-Р
- АВТОМАТИЧЕСКОЕ ПРИВЕДЕНИЕ ИНФРАСТРУКТУРЫ В СООТВЕТСТВИЕ С ОТРАСЛЕВЫМИ СТАНДАРТАМИ И ТРЕБОВАНИЯМИ БЕЗОПАСНОСТИ
- ПОДДЕРЖКА РАСПРЕДЕЛЕННЫХ ИНФРАСТРУКТУР

ВОЗМОЖНОСТИ

ПОДДЕРЖКА РАСПРЕДЕЛЕННЫХ ИНФРАСТРУКТУР

- Поддержка VMware vSphere 6.0, 6.5, 6.7, Microsoft Windows Server 2008 R2, 2012 R2 и 2016
- Горячее резервирование серверов vGate
- Поддержка работы с несколькими серверами vCenter, объединенными с помощью режима VMware vCenter Linked Mode
- Поддержка vCenter Server Appliance
- Поддержка vCenter High Availability
- Подключение агента аутентификации к нескольким серверам авторизации vGate R2
- Возможность установки агента аутентификации на ОС АЛЬТ 8 СП
- Построение леса серверов авторизации vGate R2
- Контроль управления Microsoft Hyper-V через System Center Virtual Machine Manager и Failover Cluster Manager
- Поддержка гетерогенных инфраструктур
- Исключение необходимости установки агента на каждую виртуальную машину

РАЗГРАНИЧЕНИЕ ДОСТУПА К УПРАВЛЕНИЮ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРОЙ

- Усиленная аутентификация администраторов виртуальной инфраструктуры, в том числе двухфакторная, с использованием ключей iButton, JaCarta, Рутокен
- 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
- Назначение меток и правил доступа группам пользователей в соответствии со структурой Microsoft Active Directory

МОНИТОРИНГ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

- Сбор событий безопасности напрямую с объектов виртуальной инфраструктуры
- Корреляция событий и генерация инцидентов
- Шаблоны правил корреляции, специфичные для виртуальной среды
- Полный контроль действий в виртуальной инфраструктуре в обход средства защиты, в том числе аутентификации пользователей в vSphere
- Удобная панель мониторинга инцидентов в реальном времени
- Направление инцидентов в другие системы по протоколу syslog и на e-mail сервера

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ И КОНТРОЛЬ

Консоль управления vGate R2 позволяет:

- Управлять учетными записями пользователей и правами доступа к защищаемым объектам
- Развертывать и настраивать компоненты защиты ESXi-/vCenter-серверов и серверов Hyper-V
- Управлять параметрами виртуальных машин
- Автоматизировать назначение меток на создаваемую виртуальную машину на основании имени ВМ
- Просматривать журнал событий
- Осуществлять горячее резервирование и работать в режиме кластера
- Обеспечить интеграцию с SIEM-системами
- Автоматизировать любые задачи администратора

ПРИМЕНЕНИЕ ШАБЛОНОВ ПРИ НАСТРОЙКЕ ПОЛИТИК БЕЗОПАСНОСТИ

Использование шаблонов для различных категорий:

- Защита государственных информационных систем
- Защита информационных систем персональных данных
- Защита объектов КИИ
- Соответствие РД АС
- Соответствие СТО БР ИББС
- Соответствие ГОСТ Р 56938-2016
- Соответствие ГОСТ Р 57580.1-2017
- Стандарт безопасности данных индустрии платежных карт PCI DSS
- Соответствие требованиям VMware по повышению уровня безопасности (VMware vSphere Security Configuration Guide)
- Соответствие требованиям CIS Benchmarks

МЕЖСЕТЕВОЙ ЭКРАН УРОВНЯ ГИПЕРВИЗОРА

- Фильтрация сетевого трафика
- Централизованное управление правилами фильтрации
- Создание правил фильтрации на уровне виртуальных машин и групп виртуальных машин
- Автодобавление виртуальных машин в сегменты
- Поддержка механизмов миграции виртуальных машин
- Поддержка любой инфраструктуры VMware
- Поддержка любой редакции vSphere

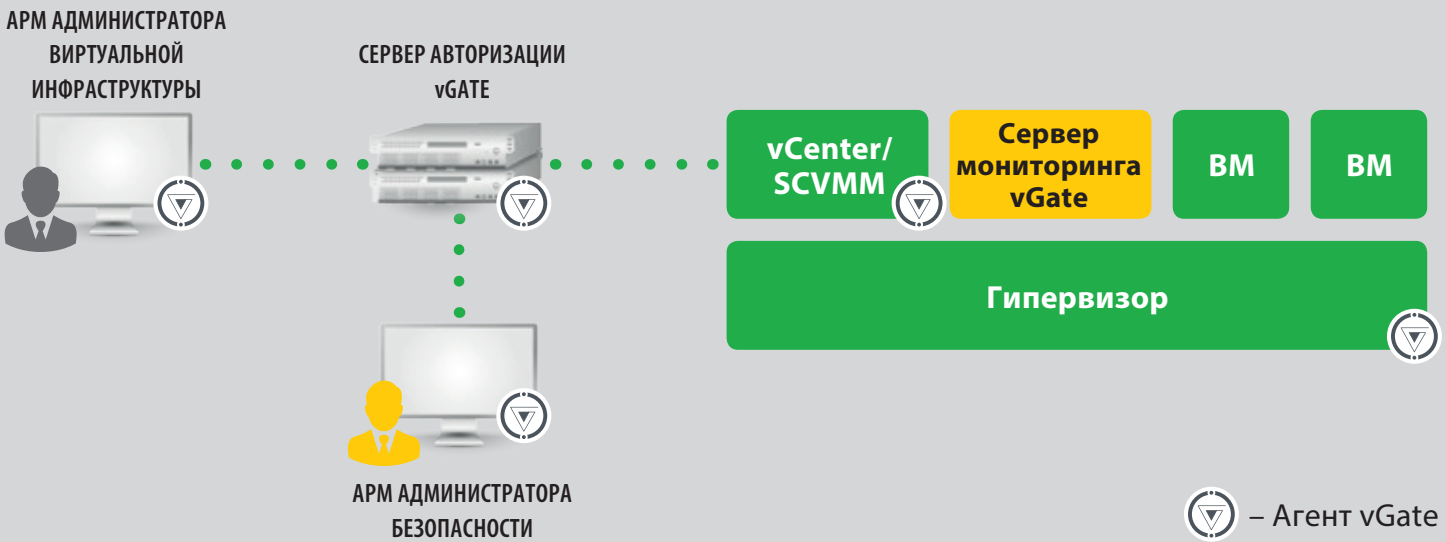
РЕГИСТРАЦИЯ И АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ

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

РЕШАЕМЫЕ ЗАДАЧИ

- Защита виртуальных машин от несанкционированного копирования, клонирования, переноса и уничтожения
- Защита средств управления виртуальной инфраструктурой от несанкционированного доступа
- Защита от специфических угроз, характерных для виртуальных сред
- Контроль действий привилегированных пользователей
- Контроль целостности виртуальных машин
- Мониторинг событий безопасности
- Приведение системы защиты виртуальной инфраструктуры в соответствие требованиям регуляторов
- Приведение системы защиты виртуальной инфраструктуры в соответствие требованиям отраслевых стандартов (защита банковской, медицинской и других видов тайн)
- Сегментация виртуализованной сети

АРХИТЕКТУРА



ЛИЦЕНЗИРОВАНИЕ

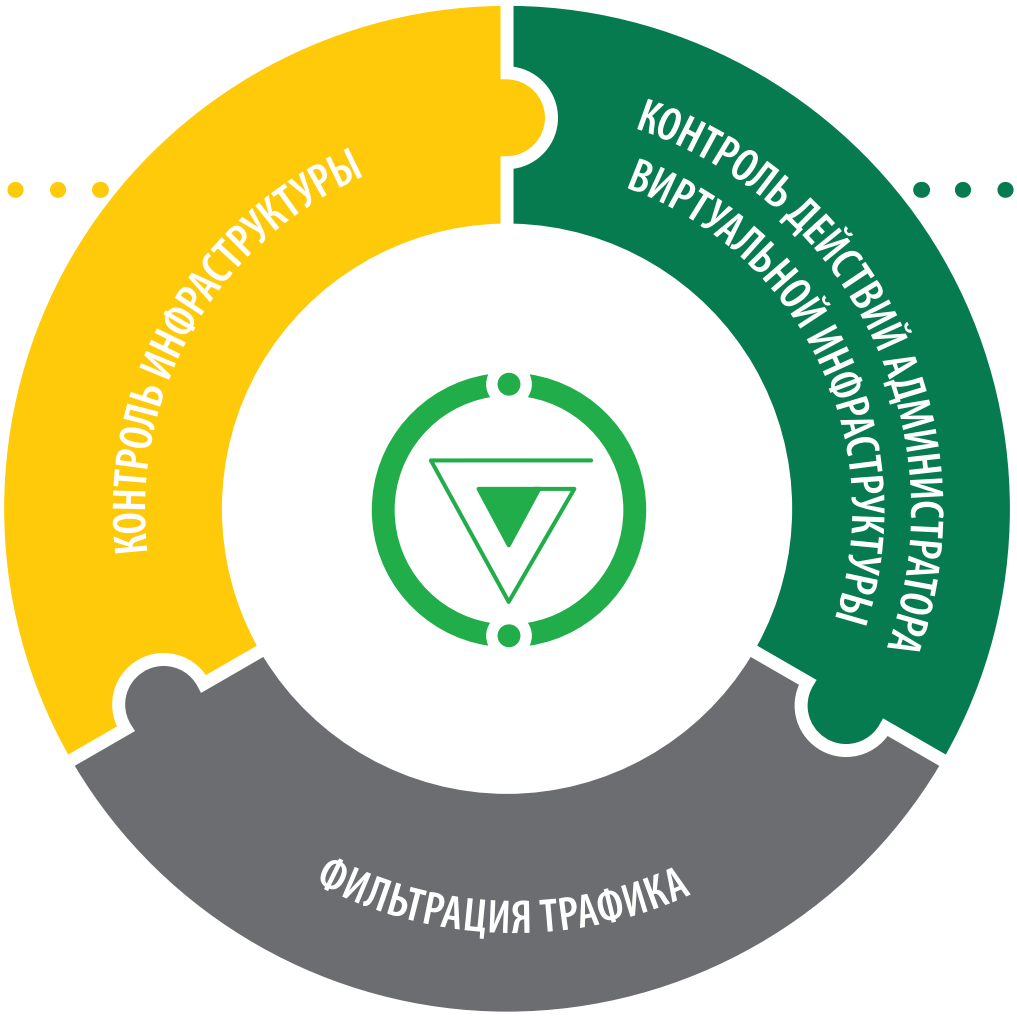
ФУНКЦИОНАЛЬНОСТЬ	STANDARD[1]	ENTERPRISE	ENTERPRISE PLUS
Количество серверов авторизации vGate	1	Не ограничено	Не ограничено
vAccess:			
Выделенные роли администраторов	●	●	●
Мандатное и дискреционное разграничение доступа	●	●	●
Разбиение виртуальной инфраструктуры на сегменты	●	●	●
Управление перемещением виртуальных машин и обрабатываемых на них данных	●	●	●
Контроль целостности и доверенная загрузка ВМ	●	●	●
Регистрация событий безопасности (аудит)	●	●	●
Автоматизация меток и политик, группировка объектов	●	●	●
vCompliance:			
Шаблон безопасности КИИ	●	●	●
Шаблон безопасности ГОСТ Р 57580.1-2017	●	●	●
Шаблон безопасности ГИС	●	●	●
Шаблон безопасности ИСПДн	●	●	●
Шаблон безопасности РД АС	●	●	●
Шаблон безопасности СТО БР ИББС	●	●	●
Шаблон безопасности PCI DSS	●	●	●
Шаблон безопасности VMware vSphere 6.7 Security Configuration Guide new	●	●	●
Шаблон безопасности CIS Benchmarks	●	●	●
Шаблон безопасности ГОСТ Р 56938-2016	●	●	●
vNetwork			
Межсетевое экранирование на уровне гипервизора	–	–	●
vMonitor			
Корреляция событий безопасности виртуализации	–	–	●
vReport			
Создание отчетов безопасности	–	–	●
Отказоустойчивость:			
Создание резервной копии конфигурации vGate (BackUp сервера авторизации)	●	●	●
Архивирование журналов аудита	●	●	●
Горячее резервирование серверов vGate (кластер)	–	●	●
Подключение агента авторизации к нескольким серверам авторизации vGate	–	●	●
Создание фермы серверов авторизации (синхронизация настроек между серверами vGate)	–	●	●
Совместимость с компонентами виртуализации:			
Совместимость с VMware vCenter SRM	●	●	●
Совместимость с VMware View (Horizon)	●	●	●
Совместимость с VMware vCloud Director	●	●	●
Поддержка серверов управления vCenter Linked Mode	–	●	●
Поддержка VMware Auto-Deploy	–	●	●
Поддержка vCenter High Availability	–	●	●
Контроль управления серверами 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

КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ВИРТУАЛИЗАЦИИ

- **Контроль безопасности настроек**
- **Мониторинг безопасности**
- **Автоматизация соответствия ИБ-стандартам с помощью шаблонов политик безопасности**

- **Контроль доступа к хранилищу данных виртуальных машин**
- **Контроль доступа к консоли виртуальной машины**
- **Независимый аудит действий администратора**



- **Отсутствие агентов на виртуальных машинах**
- **Автоматизация процесса настройки межсетевого экрана**
- **Поддержка миграции виртуальных машин**

СЕРТИФИКАТЫ

ФСТЭК России

- vGate R2: СВТ5/НДВ4, для защиты АС до класса 1Г включительно, ИСПДн до У31 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 У31 включительно, ГИС до К1 включительно и АСУ ТП до К1 включительно

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка vGate может осуществляться как напрямую, силами специалистов компании «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

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

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