КОД безопасности

vGate 4.9

Средство защиты жизненного цикла виртуальных машин и микросегментации сетей

- Безагентный межсетевой экран уровня гипервизора
- Мониторинг событий безопасности виртуальной инфраструктуры
- Контроль действий администраторов виртуальной инфраструктуры
- Автоматическое приведение инфраструктуры в соответствие с отраслевыми стандартами и требованиями безопасности
- Поддержка KVM

Возможности

Поддержка распределенных инфраструктур

- Поддержка контейнеров VMware Tanzu.
- Горячее резервирование серверов vGate.
- Поддержка vCenter HA и Linked Mode.
- Поддержка гетерогенных инфраструктур.
- Отсутствие агентов на ВМ.
- Поддержка VMware Cloud Director.
- Поддержка операций VMware vSAN.
- Поддержка компонента SDN. new

Централизованное управление и контроль

В веб-консоли управления vGate R2 реализованы возможности:

- Возможность управления vGate в случае, если он находится на стороне сервис-провайдера;
- Управление учетными записями пользователей и правами доступа к защищаемым объектам;
- Развертывание и настройка компонентов защиты ESXi-/vCenter-серверов;
- Управление параметрами виртуальных машин;
- Автоматизация назначения меток на создаваемую виртуальную машину на основании имени ВМ;
- Просмотр журнала событий;
- Горячее резервирование и работа в режиме кластера;
- Интеграция с SIEM-системами;
- Автоматизация любых задач администратора;
- Контроль целостности образов контейнеров во встроенном реестре Harbor;
- Контроль доступа к vSphere Pods.

Межсетевой экран уровня гипервизора

- Безагентная фильтрация трафика между ВМ.
- Сохранение сетевых правил при миграции ВМ.
- Отслеживание трафика на Netflow- дашбордах.
- Контроль активных сессий в реальном времени.
- Совместимость с VMware NSX.
- Отслеживание состояния соединений.
- Разрешающие правила фильтрации для однонаправленной передачи трафика.
- Поддержка VMware и KVM-платформ.

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;
- Соответствие требованиям CIS for ESXi 7.0.

Разграничение доступа к управлению виртуальной инфраструктурой

- Усиленная аутентификация, в том числе двухфакторная (JaCarta, Rutoken).
- Ролевая модель управления.
- Контроль изменений в инфраструктуре администратором безопасности.
- Интеграция с Active Directory.
- Автоматизация настроек и политик безопасности.
- Система отчетов безопасности.
- Установка пользовательских уровней конфиденциальности.
- Ограничение числа одновременных сеансов администратора виртуальной инфраструктуры.
- Отдельная привилегия администратора для редактирования параметров межсетевого экрана vGate.
- Аутентификация пользователей с использованием домена ALD Pro. new

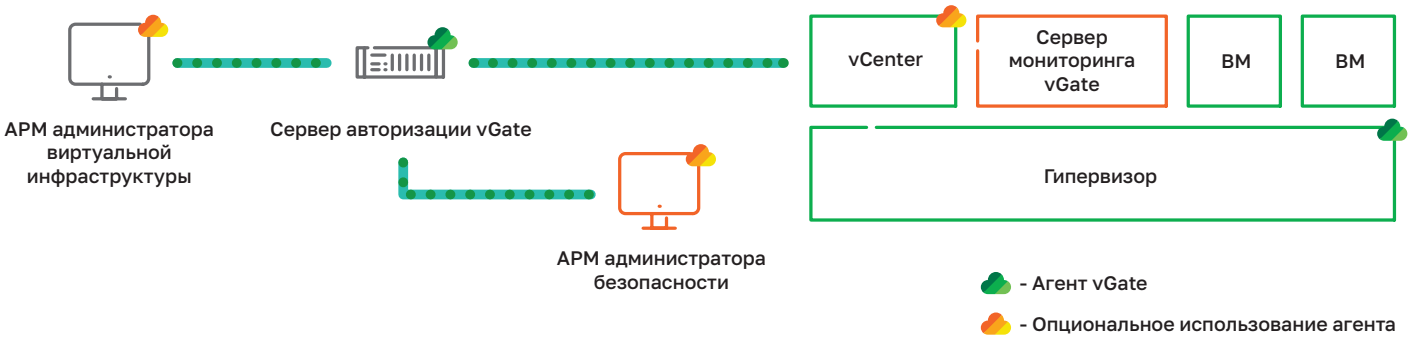
Мониторинг виртуальной инфраструктуры

- Корреляция событий и генерация инцидентов.
- Шаблоны правил корреляции специально разработанные для виртуальных сред.
- Контроль действий в инфраструктуре в обход средства защиты.
- Панель дашбордов в реальном времени.
- Интеграция по syslog с SIEM-решениями.
- Тепловая карта событий аудита.

Поддерживаемые среды виртуализации

- VMware vSphere 6.5, 6.7, 7.0;
- Альт Сервер Виртуализации 10.1 (OpenNebula 5.10.5, Proxmox 7.2);
- Р - Виртуализация 7.0.13 (Скала - Р Управление 1.98);
- zVirt Node 3.3, 4.0;
- РЕД Виртуализация 7.3;
- ROSA Virtualization 2.1;
- SpaceVM 6.2.0, 6.2.1;
- HostVM 4.4.8 в составе oVirt Node 4.4.8;
- Utinet Glovirt 2.1.1;
- OpenNebula 6.4.0.1 в составе Ubuntu 20.04.5 LTS;
- Proxmox 7.4.1, 8.0.2.

Архитектура



Комплексный подход к защите виртуализации

vGate

Развертывание виртуальных машин

- Доверенная загрузка ВМ
- Контроль развертывания из шаблонов ВМ
- Управление контурами безопасности

Эксплуатация

- Управление доступом
- Встроенные шаблоны политик безопасности
- Контроль целостности компонентов и настроек

Уничтожение

- Гарантированное уничтожение данных виртуальной машины

Микросегментация | **Мониторинг** | **Отчетность** | **Автоматизация**

Сертификаты

ФСТЭК России

vGate R2

- МЭ Б4, СВТ5, УД4, для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно, ГИС до К1 включительно и АСУ ТП до К1 включительно, ЗОКИИ до 1 категории 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.

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**