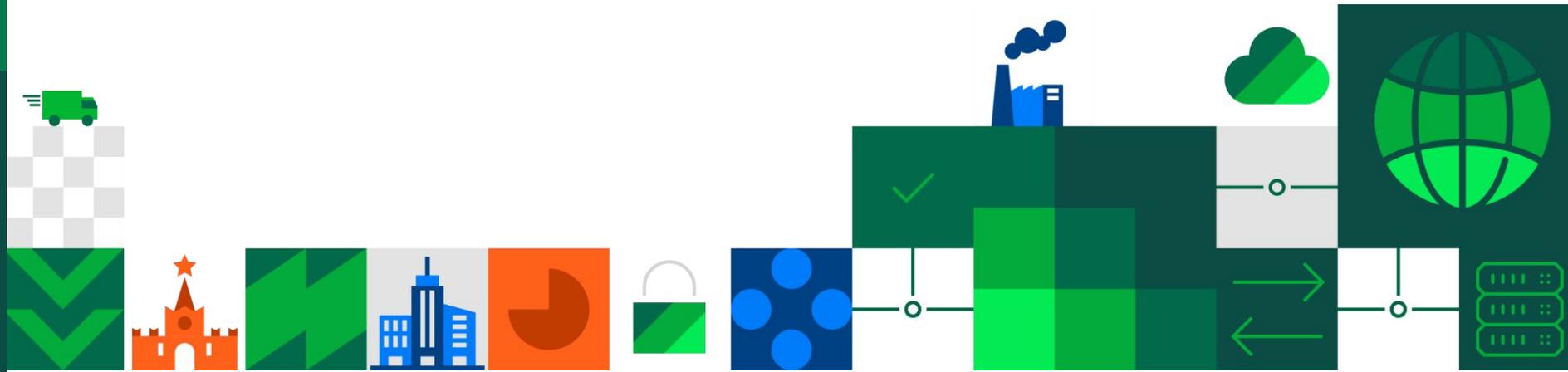


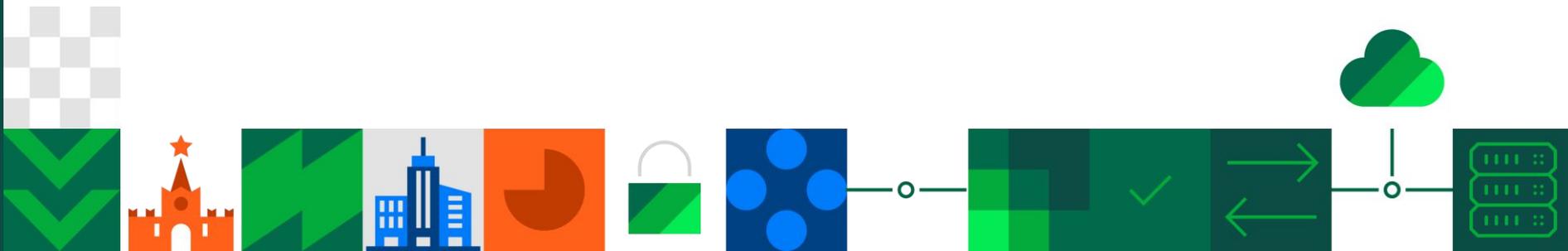


vGate 4.9





Специфика защиты виртуализации



VMware заявила о своем уходе
из России

Переход на другие платформы
будет постепенным

Одновременное использование VMware и других средств
виртуализации



Повышенные риски ИБ:

Несо согласованность настроек безопасности
Отсутствие централизованного мониторинга и
аудита различных гипервизоров



Использование единых настроек для любого типа виртуализации

Единый мониторинг

Общий аудит



Угрозы виртуальной инфраструктуры



Несанкционированный доступ к данным на виртуальных машинах

- Со стороны администратора
- Со стороны других виртуальных машин



Простой приложений при нештатной ситуации в виртуальной среде



Риски невыполнения требований ИБ в виртуальной среде



Сложности защиты виртуальной инфраструктуры



Средства защиты «облаков» концентрируются на защите только виртуальных машин



Средства защиты не обладают необходимой гибкостью настроек



Часть задач по защите решается дополнительной нагрузкой на администратора безопасности



К чему это приводит?



Четверть компаний не используют виртуализацию для аттестованных информационных систем



Две трети компаний опасаются ущерба, нанесенного действиями администратора инфраструктуры



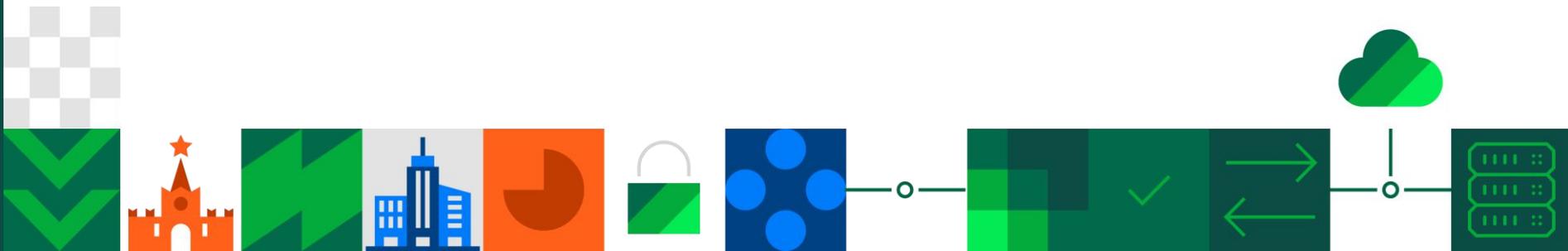
Треть компаний жалуется на неэффективную систему защиты по следующим причинам:

- влияние средств защиты на работу виртуальной инфраструктуры
- сложности настройки и администрирования механизмов защиты
- необходимость переконфигурирования инфраструктуры для эффективной защиты





О продукте vGate



- Реализована поддержка технологии VxLAN с возможностью конфигурирования параметров создаваемых программно-определяемых сетей (SDN – Software-Defined Network).
- Добавлена возможность аутентификации пользователей с использованием домена ALD Pro
- Реализовано управление параметрами межсетевого экранирования в мультиарендном режиме
- Расширен список доступных функциональных возможностей В веб-интерфейсе vGate.



О продукте



vGate

Защита платформ виртуализации на базе VMware vSphere, СКАЛА-Р, KVM и oVirt **new**

Предназначен для решения следующих задач:

- Защита виртуальных машин от несанкционированного копирования, клонирования, уничтожения
- Защита от специфических угроз, характерных для виртуальных сред
- Контроль привилегированных пользователей
- Микросегментация инфраструктуры
- Мониторинг событий безопасности и расследование инцидентов ИБ
- Автоматизация compliance и best practice





Планы по сертификации vGate 4.9 (ФСТЭК России):

- 5 класс защищенности (СВТ5)
- 4 уровень доверия
- МЭ типа Б 4-го класса

Будет сертифицирован для защиты:

- Защита ГИС до К1 включительно
- Защита ИСПДн до УЗ1 включительно
- Защита АС до класса 1Г включительно
- Защита АСУ ТП до К1 включительно
- ЗОКИИ до 1 категории включительно

Поддерживаемые сертифицированные версии: 4.4-4.8





Развертывание виртуальных машин

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



Эксплуатация

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



Уничтожение

- Гарантированное уничтожение данных виртуальной машины



Микросегментация



Мониторинг

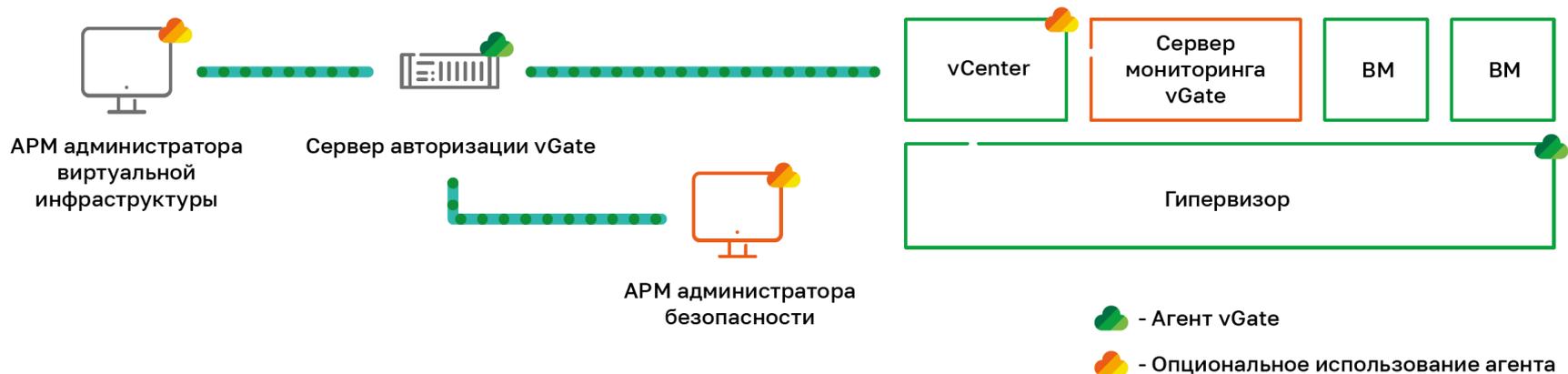


Отчетность



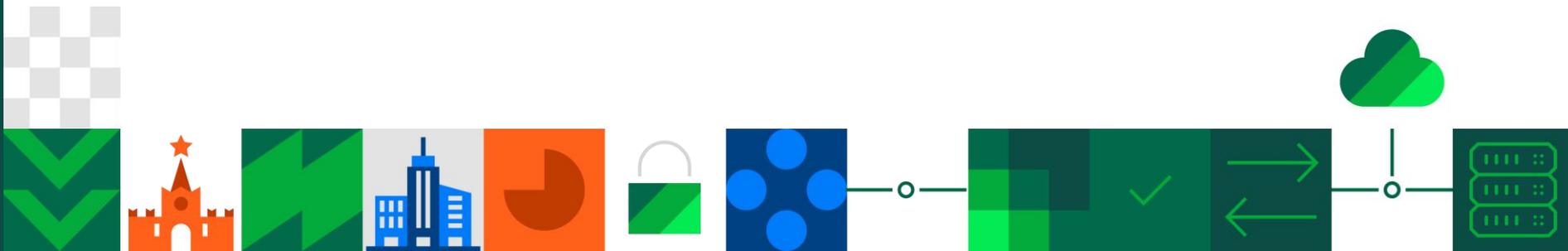
Автоматизация

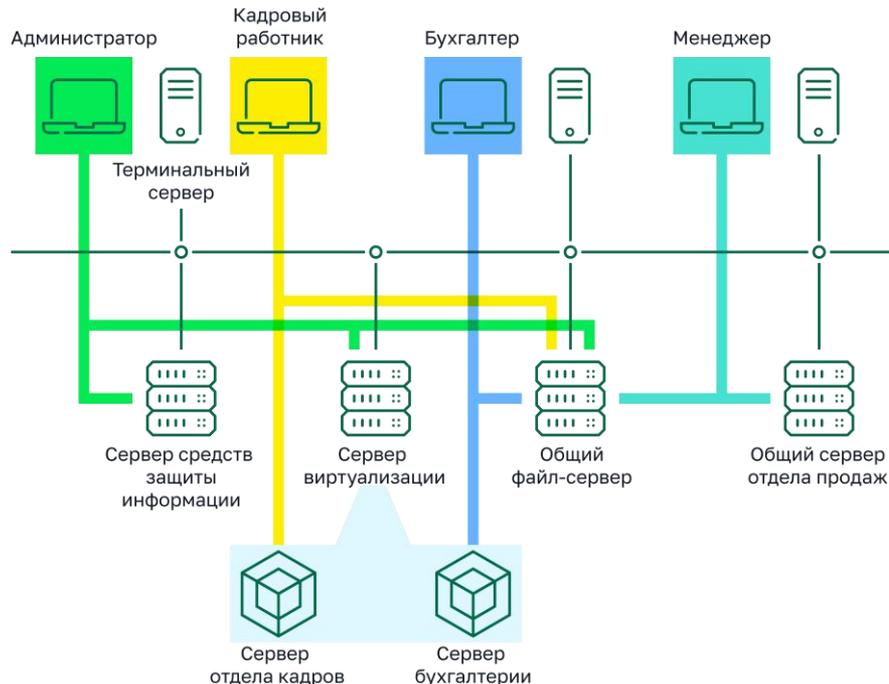
Архитектура vGate





Варианты применения





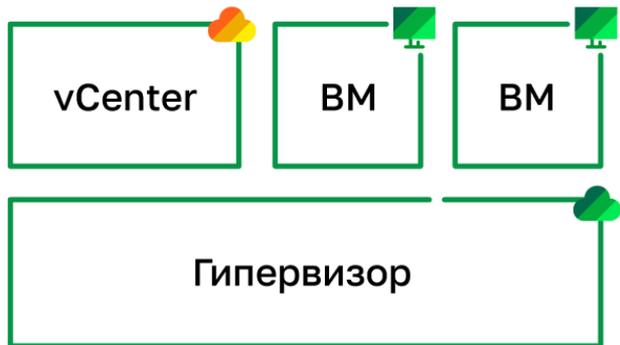
Сценарии использования:

- Фильтрация сетевого трафика
- Микросегментация сети без изменения ее топологии
- Назначение правил фильтрации трафика при создании VM

Продукты:

- vGate (редакция Enterprise Plus)





 - Агент vGate

 - Защита SNS и SN LSP

 - Опциональное использование агента

Сценарии использования:

- Защита настроек и виртуальных машин
- Контроль целостности конфигурации виртуальных машин и доверенная загрузка
- Контроль доступа администраторов ВИ к файлам виртуальных машин
- Контроль целостности объектов внутри VM
- Защита данных внутри VM

Продукты:

- vGate (все редакции)
- Secret Net Studio
- Secret Net LSP



Автоматизация соответствия требованиям безопасности



Сценарии использования:

- Автоматизированный аудит виртуальной инфраструктуры на соответствие требованиям и рекомендациям
- Контроль соответствия требованиям регуляторов

Продукты:

- vGate (все редакции)



Контроль действий администраторов



Сценарии использования:

- Эксплуатация виртуальных машин разного уровня критичности в единой инфраструктуре
- «Внешнее» разграничение прав доступа администраторов
- Подтверждение критичных действий над виртуальными машинами
- Независимый аудит действий администраторов

Продукты:

- vGate (все редакции)





Сценарии использования:

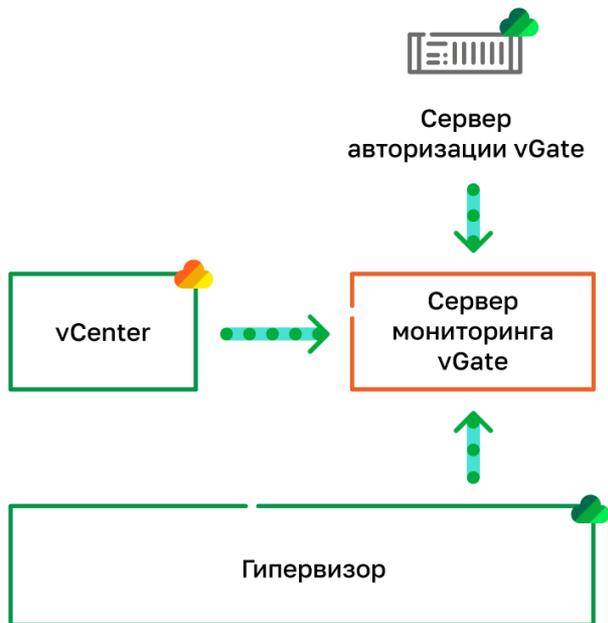
- Безопасная настройка гипервизора
- Контроль подключения к гипервизору внешних устройств
- Контроль соответствия настроек гипервизора стандартам и рекомендациям

Продукты:

- vGate (все редакции)



Мониторинг виртуальной инфраструктуры



 - Опциональное использование агента

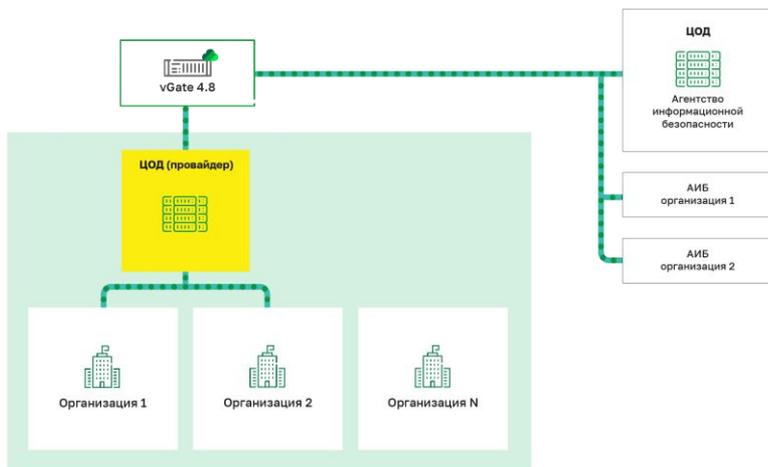
Сценарии использования:

- Мониторинг безопасности виртуальной инфраструктуры
- Отслеживание попыток обхода vGate
- Корреляция событий ВИ
- Отправка инцидентов во внешние системы
- Дашборды состояния безопасности

Продукты:

- vGate (редакция Enterprise Plus)





Сценарии использования:

- Разделение полномочий администратора безопасности ЦОД и администраторов безопасности обслуживаемых организаций
- Защищаемые объекты защищаемых организаций видны только соответствующим администраторам безопасности
- Администратор безопасности ЦОД не имеет доступа к объектам организаций

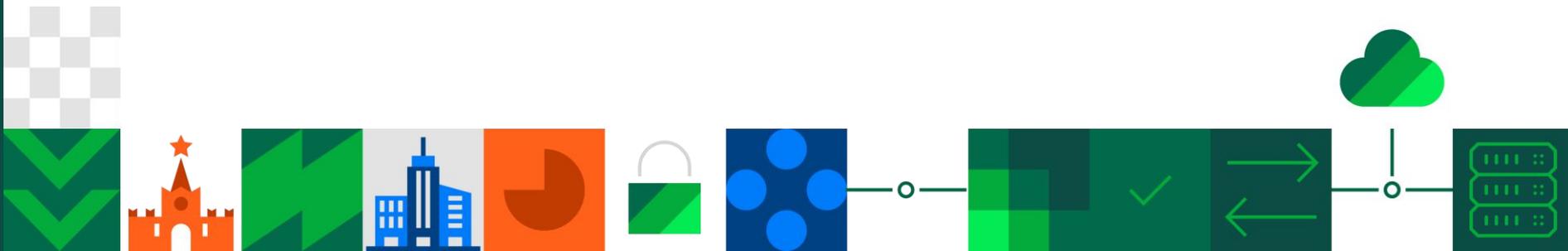
Продукты:

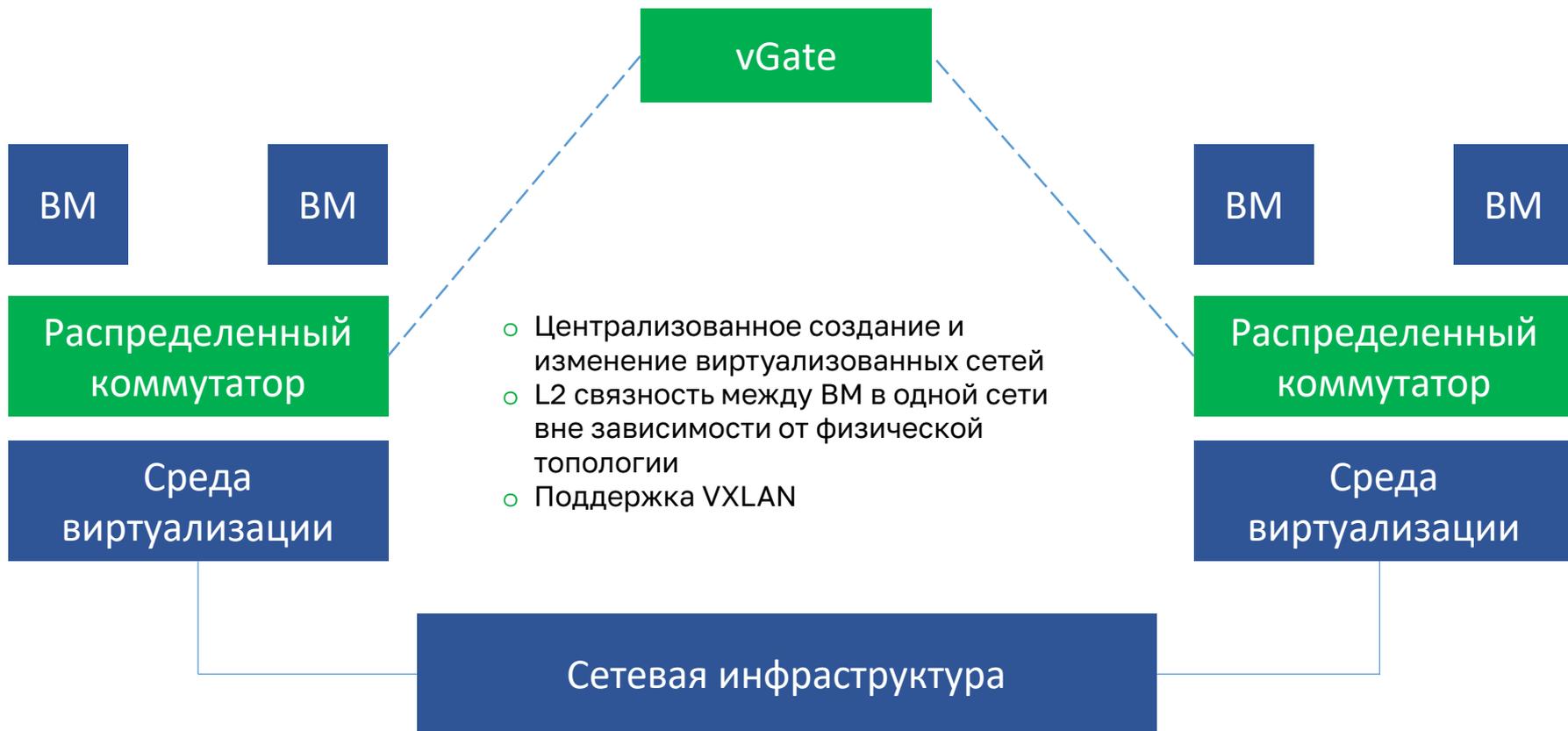
- vGate (редакция Enterprise Plus)





Возможности продукта vGate





Поддержка платформ виртуализации и их компонентов

Vmware:

- vSphere 7.0
- vSphere 6.7
- vSphere 6.5
- VMware Tanzu
- vCenter HA и Linked Mode
- VMware vSAN

KVM:

- Ubuntu 18.04.6 LTS
- Ubuntu 20.04.3 LTS
- Astra Linux Common Edition "Орел" 2.12.22
- Альт Сервер Виртуализации 10
- Альт Сервер 8 СП
- Платформа Р-виртуализация 7.0.13



- ✓ Контроль запуска виртуальных машин
- ✓ Доверенная загрузка виртуальных машин
- ✓ Затиранье остаточной информации после удаления виртуальных машин
- ✓ Разграничение доступа администраторов к гипервизорам



Средства управления KVM-виртуализацией:

- Proxmox 7.0, 8.0
- Proxmox 7.2 и OpenNebula 5.10.5 в составе Альт
Сервер Виртуализации 10
- OpenNebula 6.4.0.1 **new** в составе Ubuntu 20.04.5 LTS
- Utinet Glovirt 2.1.1 **new**
- SpaceVM **new** 6.2.0, 6.2.1

Скала-Р Управление

- 1.80, 1.90, 1.93, 1.98

Средства управления на базе oVirt **new** :

- РЕД Виртуализация 7.3
- ROSA Virtualization 2.1
- zVirt 3.0
- zVirt 4.0
- HOSTVM 4.4.8

Средства управления VMware:

- vCenter
- VMware Cloud Director

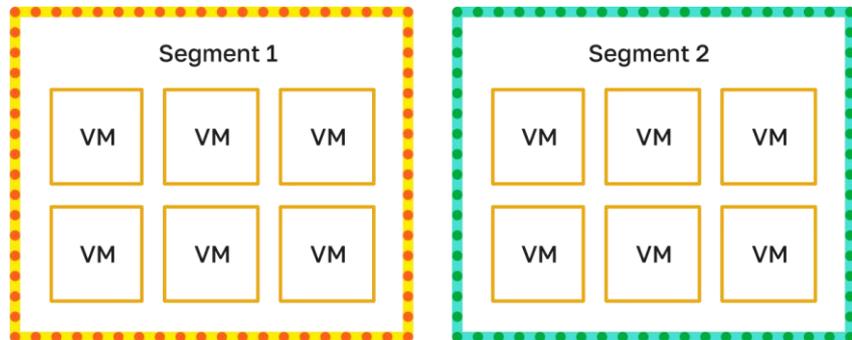


Фильтрация сетевого трафика с помощью vNETWORK



- Централизованное управление правилами фильтрации во всей виртуальной инфраструктуре
- Гранулярная настройка правил фильтрации
- Оперирование на уровне VM и групп VM и поддержка механизмов миграции VM
- Автодобавление виртуальных машин в сегменты
- Нет агента в гостевой ОС
- Не требуются дополнительные VM для обработки пакетов
- Отсутствие единой точки отказа
- Подробный аудит запрещенных/разрешенных пакетов
- Не требует наличие NSX
- Нет требований к редакциям платформ виртуализации

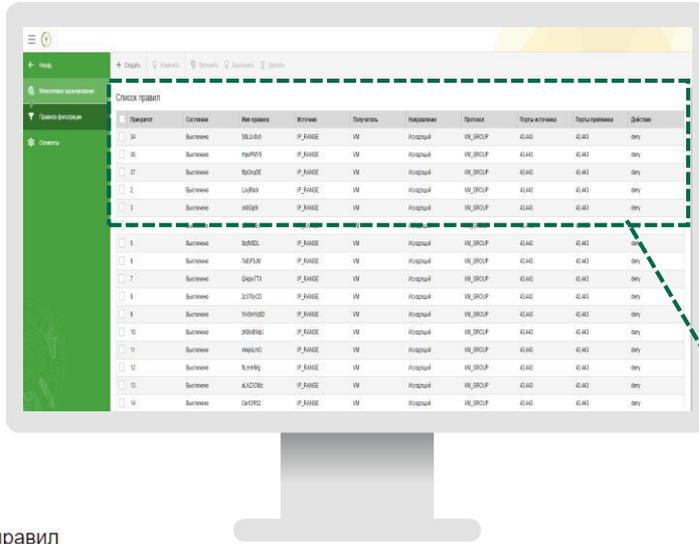
vNETWORK. Сегментация виртуальной инфраструктуры



- Возможность выделять группы VM (сегменты)
- Оперирование как на уровне VM, так и на уровне сегментов
- Автодобавление VM в сегменты
- Интеграция со средой виртуализации
- Фильтрация всего сетевого трафика сегмента по правилам
- Сохранение правил фильтрации при миграции VM
- Сегментирование как VMware, так и KVM ^{new}



vNETWORK. Правила фильтрации



Приоритет	Состояние	Имя правила	Источник	Получатель	Направление	Протокол	Порты источника	Порты приёмника	Действие
34	Выключено	S6LUx0x0	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
36	Выключено	hpoPMY9	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
37	Выключено	f8pOkqGE	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
2	Выключено	LJvjRbck	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
3	Выключено	ckl8Gp9i	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny

Правила фильтрации



Список правил

<input type="checkbox"/>	Приоритет	Состояние	Имя правила	Источник	Получатель	Направление	Протокол	Порты источника	Порты приёмника	Действие
<input type="checkbox"/>	34	Выключено	S6LUx0x0	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
<input type="checkbox"/>	36	Выключено	hpoPMY9	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
<input type="checkbox"/>	37	Выключено	f8pOkqGE	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
<input type="checkbox"/>	2	Выключено	LJvjRbck	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny
<input type="checkbox"/>	3	Выключено	ckl8Gp9i	IP_RANGE	VM	Исходящий	VM_GROUP	43,443	43,443	deny

Мониторинг виртуальной инфраструктуры



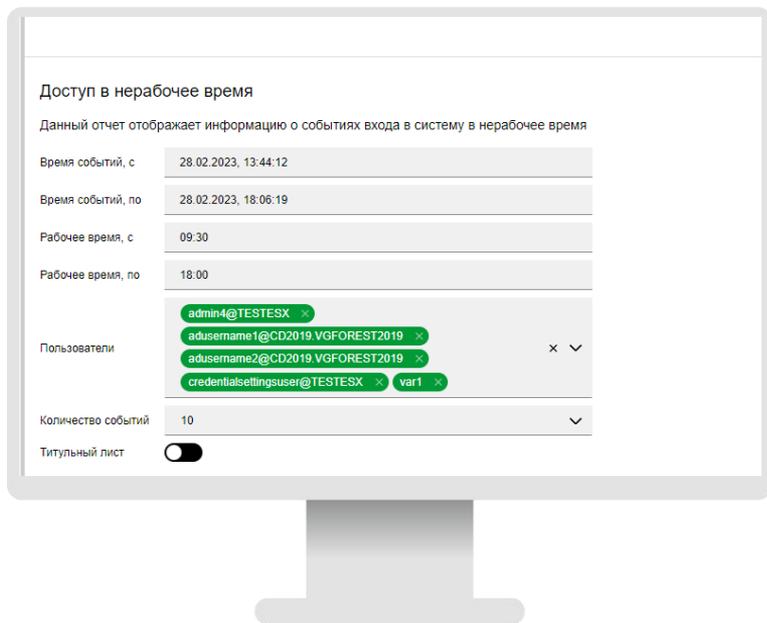
- Сбор, нормализация и фильтрация данных о событиях, происходящих в виртуальной инфраструктуре
- Корреляция событий, в том числе и с событиями самого vGate
- Отправка инцидентов безопасности во внешние системы по протоколу syslog и SMTP
- Встроенные шаблоны правил корреляции
- Контроль действий, осуществляемых в обход сервера авторизации vGate
- Работа в гетерогенных виртуальных инфраструктурах
- Возможность создания отчетов в новом веб-интерфейсе



Мониторинг событий в реальном времени

Панель мониторинга





28 типов отчетов, разделенных по группам:

- Топ-листы (статистика)
- Настройки
- Аудит
- Соответствие стандартам безопасности





Разграничение доступов администраторов безопасности^{new}

- Администратор безопасности ЦОД
- Администратор безопасности организации-арендатора

Встроенные роли администраторов

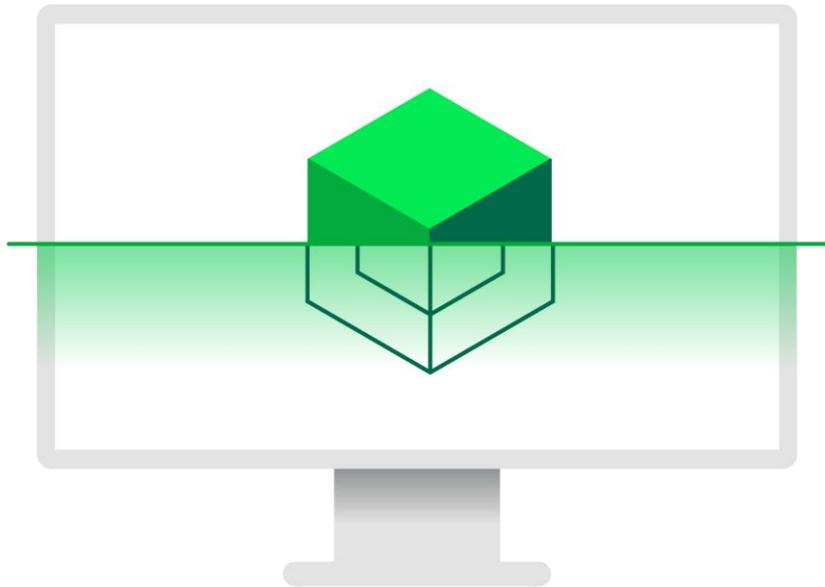
- Администратор ВМ
- Администратор сети
- Администратор СХД
- Пользователь ВМ
- Аудитор

Поддержка аутентификации с JaCarta, Рутокен

Возможность подключения с использованием браузера на любой ОС



Контроль целостности виртуальных машин



Проверка целостности компонентов ВМ:

- Процессор
- Объем ОЗУ
- Подключенные диски
- Сетевые интерфейсы
- И др.

Проверка целостности образов контейнеров в реестре Harbor

Принцип двух персон при изменении конфигурации ВМ

- Изменение не вступит в силу, пока не будет подтверждено администратором ИБ



Защита виртуальных машин



- Запрет создания снимков
- Запрет клонирования VM
- Гарантированное удаление информации из хранилища
- Контроль подключаемых устройств
- Контроль доступа к консоли VM
- Контроль скачивания файлов VM
- Контроль доступа к vSphere Pods

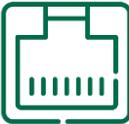
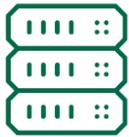




- Включение Lockdown Mode
- Запрет подключения USB-устройств к хосту
- Запрет SSH-подключения к хосту
- Настройка журналирования VM
- Контроль используемых на хосте приложений
- Контроль разделения управляющей и «боевой» сетей



Назначение меток и политик безопасности



Политики объединяются в шаблоны

- Встроенные
- Пользовательские

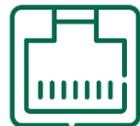
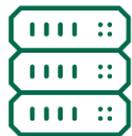
Шаблоны политик назначаются на:

- Сервер виртуализации
- Виртуальную машину
- Физический сетевой интерфейс
- Группу объектов



Назначение меток и политик безопасности

Метки и правила могут назначаться группам пользователей в соответствии со структурой Microsoft Active Directory



Метки могут применяться к:

- Серверу виртуализации
- Хранилищу
- Виртуальной машине
- Физическому сетевому интерфейсу
- Виртуальной сети
- Пользователю

Типы меток:

- Неиерархические (категории конфиденциальности)
- Иерархические (уровни конфиденциальности)
- Пользовательские уровни конфиденциальности





- Поддержка VMware vCenter SRM
- Поддержка vCSA HA
- Поддержка vCenter Linked Mode
- Кластеризация сервера авторизации vGate
- Поддержка VMware Auto Deploy



Интеграция с SIEM и другими системами



- Отправка событий безопасности во внешние системы по протоколу syslog
- Подробная настройка событий, которые отправляются на syslog-сервер
- Отправка информации о произошедших событиях на почту через SMTP

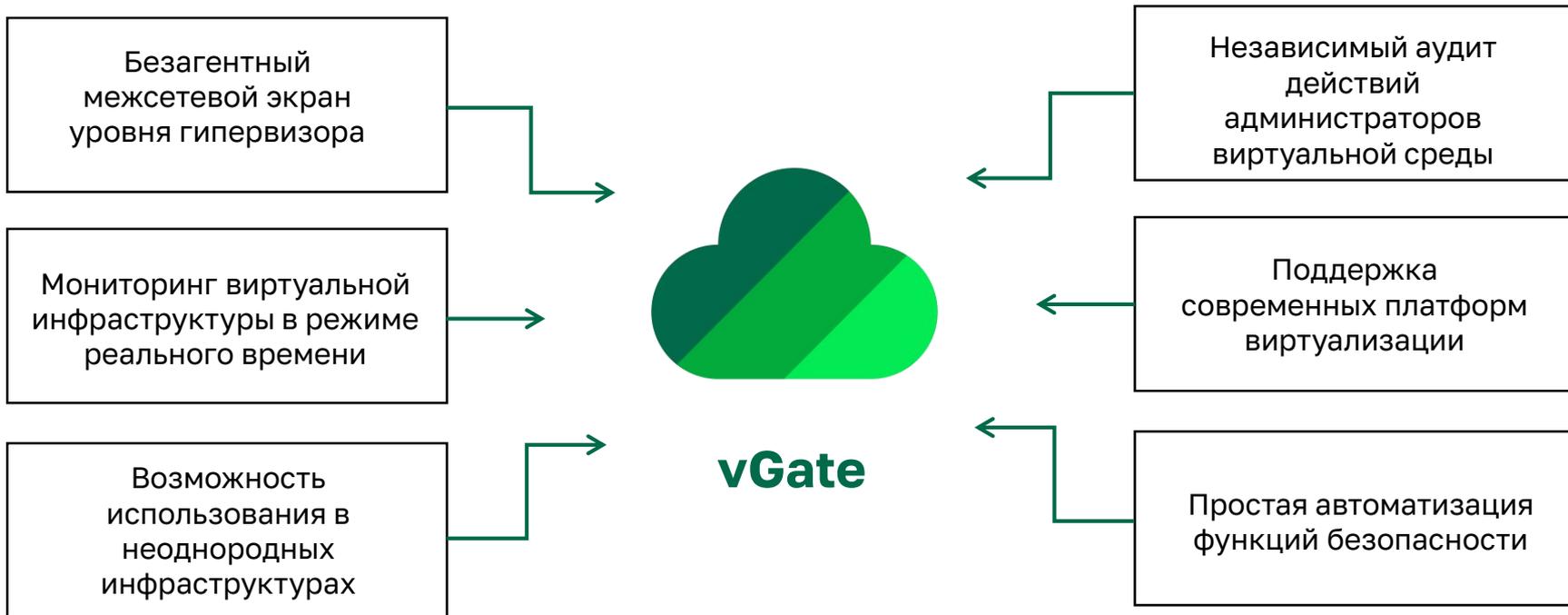




- VMware vSphere Security Configuration Guide
- ГОСТ 57580.1-2017 Защита информации финансовых организаций.
- Обеспечение безопасности значимых объектов КИИ (Приказ №239)
- Приказ №21 (ИСПДн)
- Приказ №17 (ГИС)
- ГОСТ Р 56938-2016
- РД АС
- СТО БР ИББС
- PCI DSS
- CIS Benchmarks
- VMware vSphere Security Configuration Guide 7
- CIS for ESXi 7.0

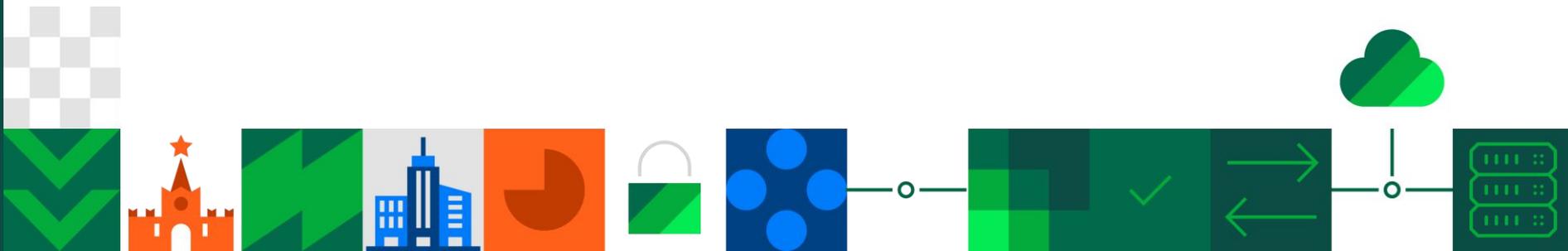


Преимущества vGate





Лицензирование



Принципы лицензирования vGate



- vGate лицензируется по количеству сокетов (физических процессоров)
- Сервер авторизации vGate включен в стоимость лицензии
- Лицензия включает в себя защиту как VMware, так и других поддерживаемых гипервизоров



vGate: редакция Standard



Редакция предназначена для защиты простой виртуальной инфраструктуры



Базовый набор функциональных возможностей



В состав лицензии входит один экземпляр сервера авторизации





Редакция предназначена для защиты крупной виртуальной инфраструктуры с высокими требованиями к обеспечению отказоустойчивости



Количество серверов авторизации, входящих в лицензию, не ограничено



Имеется возможность резервирования





Редакция предназначена для защиты крупной виртуальной инфраструктуры с высокими требованиями к обеспечению отказоустойчивости



Количество серверов авторизации, входящих в лицензию, не ограничено



Имеется возможность резервирования



Безагентный виртуальный межсетевой экран



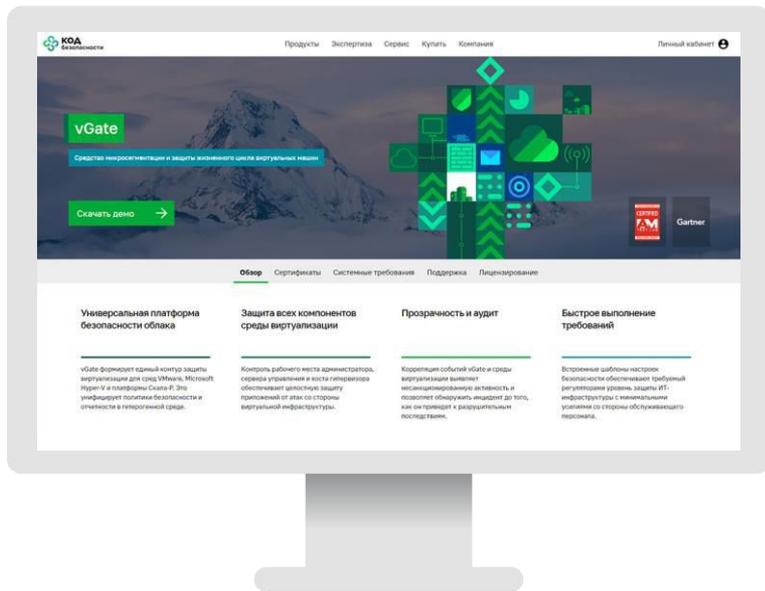
Расширенные возможности мониторинга виртуальной инфраструктуры



Поддержка мультиарендного режима



Модуль отчетов vReporter



<https://www.securitycode.ru/products/vgate/>

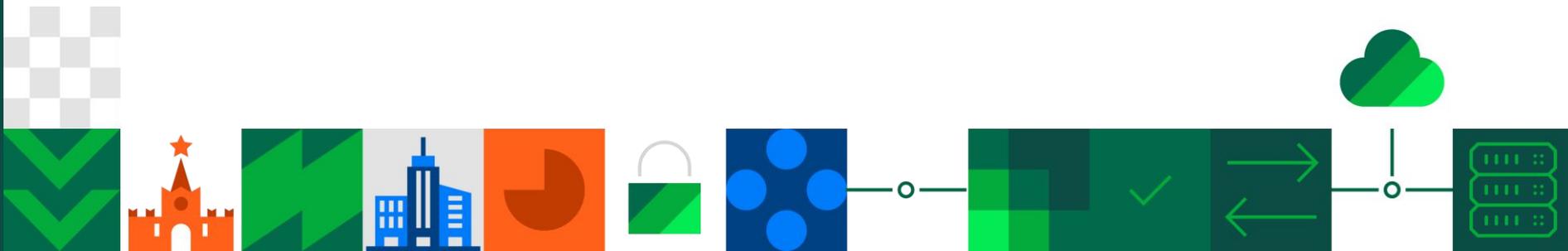
- Подробное описание продукта
- Техническая документация
- Листовки, презентации
- Сертификаты соответствия
- Онлайн-калькулятор для расчета стоимости
- Демоверсия

Для авторизованных партнеров компании «Код Безопасности» доступен закрытый раздел с дополнительными материалами





О компании



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

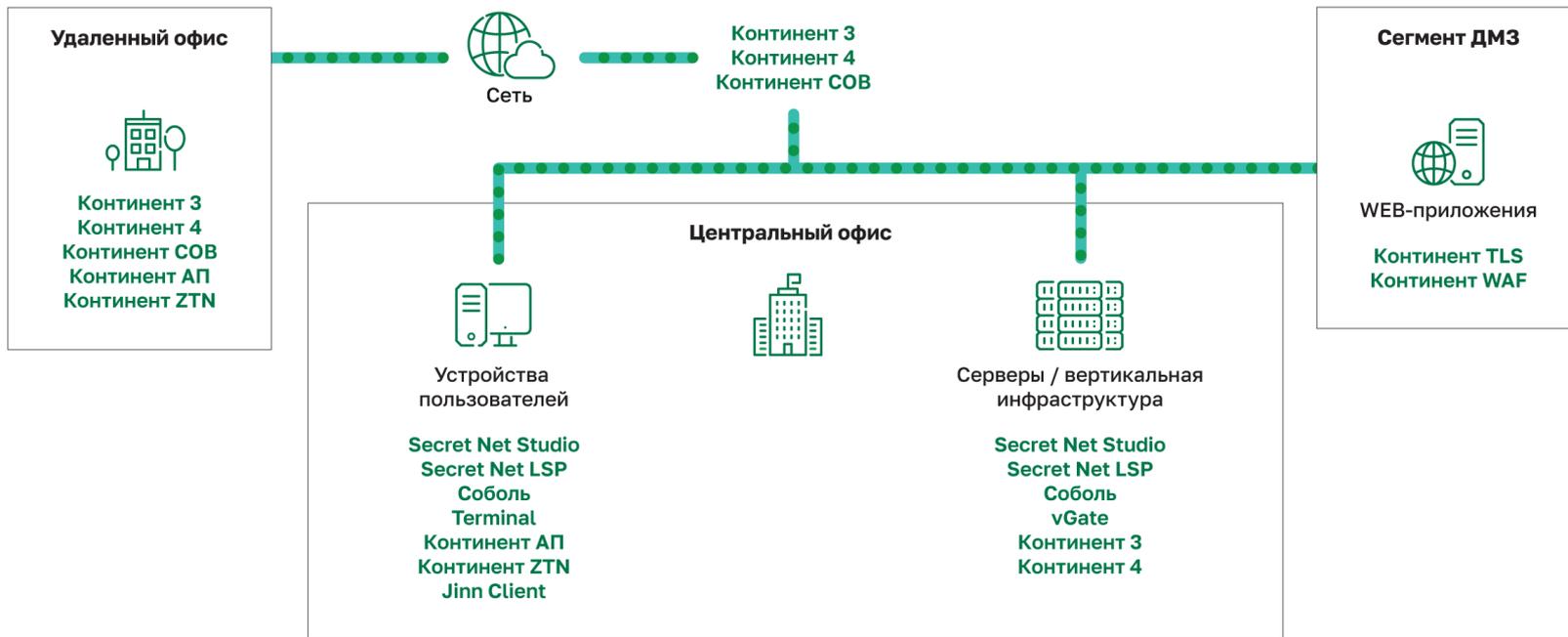
- **Более 30 лет** на страже безопасности крупнейших предприятий России. Ведет свою деятельность на основании **9 лицензий ФСТЭК, ФСБ и Минобороны России**.
- Технологии защиты обеспечивают безопасность **3 000 000 компьютеров** в **50 000 организаций**.
3 центра разработки: Москва, Санкт-Петербург, Пенза.
- Более **800 квалифицированных специалистов R&D**, имеющих уникальные компетенции.
- Более **50 разработанных СЗИ и СКЗИ**.
- Более **60 действующих сертификатов** соответствия подтверждают высокое качество продуктов.
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров**.

Компетентность «Кода Безопасности» подтверждена независимыми аналитиками:

- «Крупнейшие производители высокотехнологичного оборудования»: №1 («Эксперт РА»), №3 («Коммерсант»).
- «Крупнейшие разработчики программного обеспечения»: №7 («Эксперт РА»), №9 («Коммерсант»).
- «Крупнейшие ИТ-компании России»: №30 («Коммерсант»), №47 (TAdviser).



Комплексный подход к защите инфраструктуры



Государственные организации:



Федеральное казначейство России



Федеральная налоговая служба России



Федеральная таможенная служба России



Федеральный Фонд обязательного медицинского страхования



Центральная избирательная комиссия Российской Федерации



Министерство юстиции Российской Федерации



Министерство внутренних дел Российской Федерации



Министерство обороны Российской Федерации



Федеральная служба безопасности Российской Федерации



Федеральная служба охраны Российской Федерации

Телекоммуникационные компании:



ПАО «Ростелеком»



ПАО «МГТС»



ГК «АКАДО Телеком»



АО «Воентелеком»

Финансовые организации:



ПАО «Сбербанк»



Центральный банк Российской Федерации



ГК «Внешэкономбанк»



АО «Газпромбанк»



ПАО «Промсвязьбанк»



Банк ВТБ (ПАО)



ПАО «Московский кредитный банк»



АО «АЛЬФА-БАНК»

Промышленные предприятия:



ГК «Ростех»



АО «Российские космические системы»



ПАО «ГМК «Норильский никель»



ГК «Росатом»



ПАО «Газпром»



ПАО «АК «Транснефть»



ПАО «НК «Роснефть»»



ПАО «Россети»

Предприятия ТЭК:



Спасибо за внимание!

По вопросам стоимости и покупки продуктов:

buy@securitycode.ru

Служба технической поддержки: support@securitycode.ru

info@securitycode.ru

www.securitycode.ru

