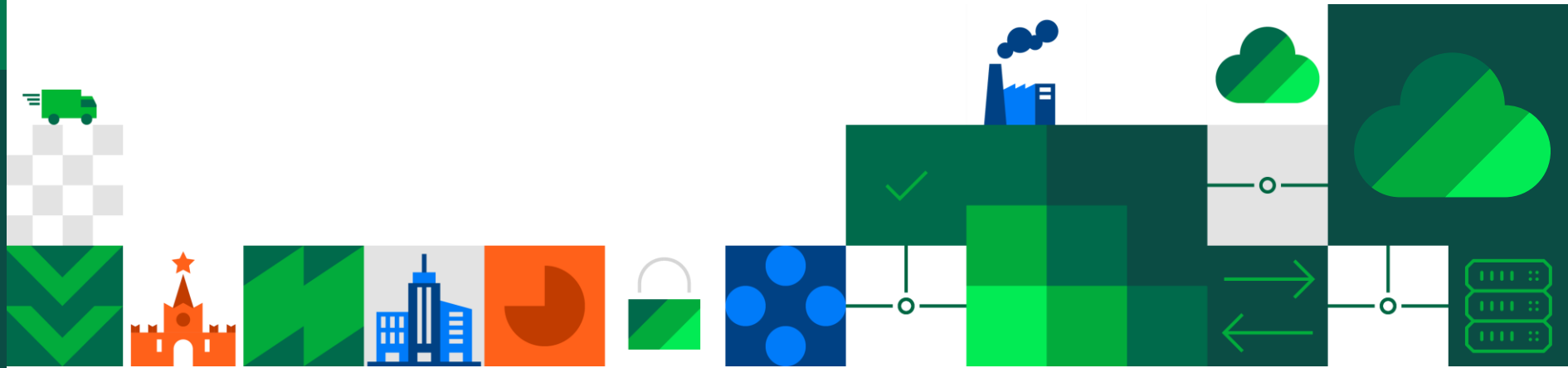
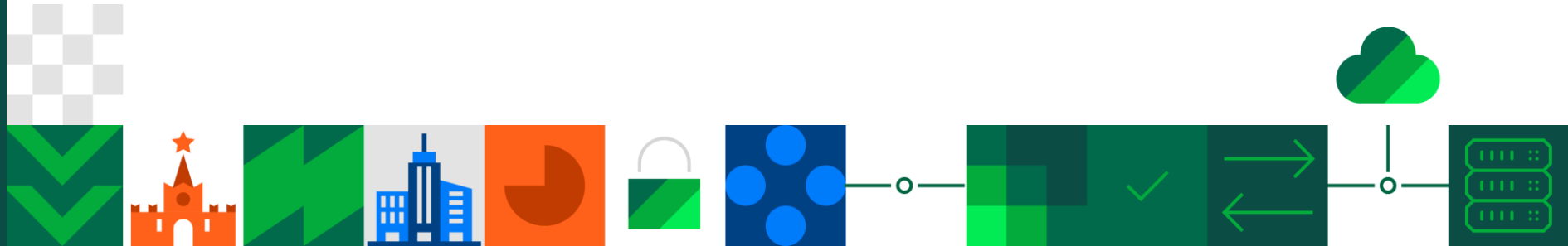
КОД безопасности

vGate 4.95



КОД безопасности

Специфика защиты виртуализации



КОД безопасности

Проблема

VMware заявила о своем уходе из России

Переход на другие платформы будет постепенным

Одновременное использование VMware и других средств виртуализации

Повышенные риски ИБ:

Несогласованность настроек безопасности

Отсутствие централизованного мониторинга и аудита различных гипервизоров

КОД безопасности

Решение

Использование единых настроек для любого типа виртуализации

Единый мониторинг

Общий аудит

КОД безопасности

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

КОД безопасности

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

КОД 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

КОД безопасности

О продукте vGate

КОД безопасности

Новый функционал vGate 4.95

- Возможность установки СЗИ vGate R2 на компьютеры под управлением операционных систем семейства Linux для VMware.
- Поддержка совместимости МСЭ vGate с Open vSwitch на KVM хостах.
- Поддержка новых средств управления KVM – виртуализацией.
- Поддержка совместимости МСЭ vGate с Open vSwitch на KVM хостах.
- Новая HTML-документация на продукт в vGate Web Console.
- Для Администраторов безопасности выделена отдельная привилегия «Администратор СЗИ» в стандартном режиме установки.
- Существенно увеличена производительность МСЭ для сценариев с большим количеством правил фильтрации на сегменты больших размеров.

КОД безопасности

О продукте

vGate

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

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

КОД безопасности

Сертификация

Сертификация vGate 4.95 (ФСТЭК России):

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

Подходит 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: 4.4-4.95

КОД безопасности

Концепция продукта

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

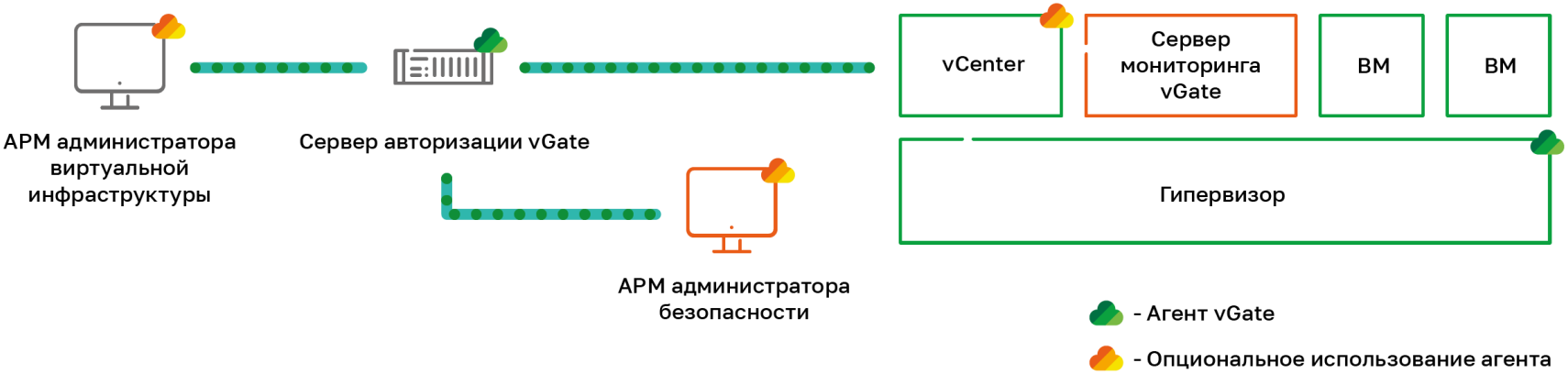
Уничтожение

- Гарантированное уничтожение данных виртуальной машины

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

КОД безопасности

Архитектура vGate

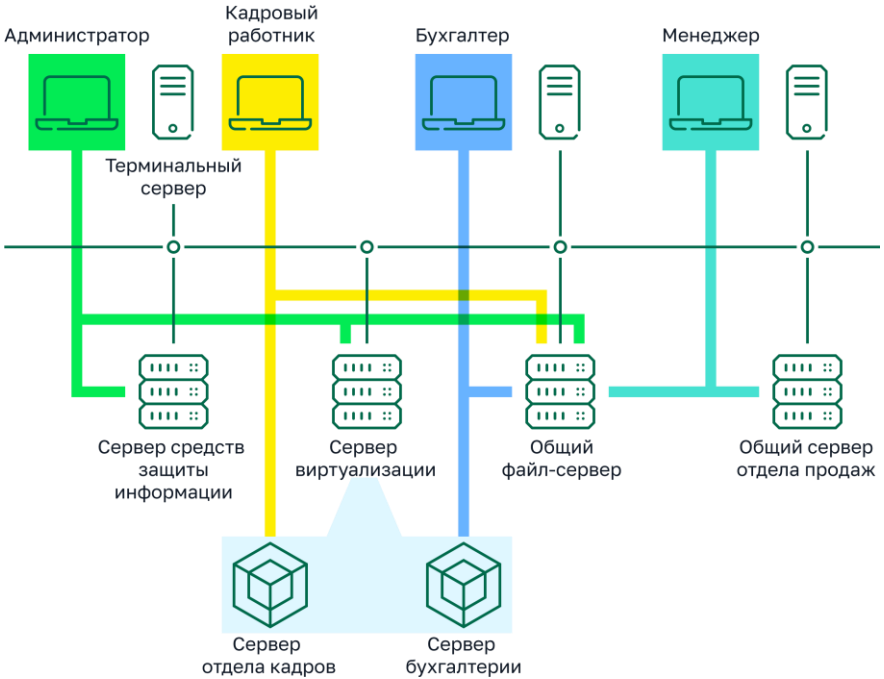


КОД безопасности

Варианты применения

КОД безопасности

Сегментация виртуальной сети



Сценарии использования:

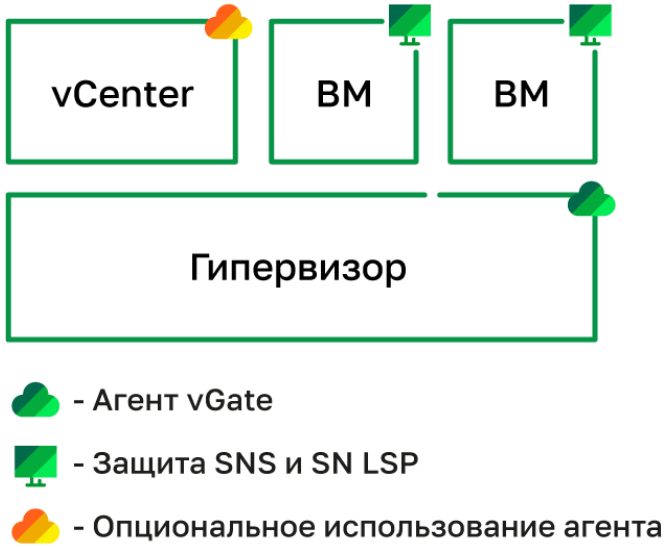
- Фильтрация сетевого трафика
- Микросегментация сети без изменения ее топологии
- Назначение правил фильтрации трафика при создании ВМ

Продукты:

- vGate (редакция Enterprise Plus)

КОД безопасности

Защита виртуальных машин



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 ВМ
- Защита данных внутри ВМ

Продукты:

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

КОД безопасности

Автоматизация соответствия требованиям безопасности

Сценарии использования:

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

Продукты:

- vGate (все редакции)

КОД безопасности

Контроль действий администраторов

Сценарии использования:

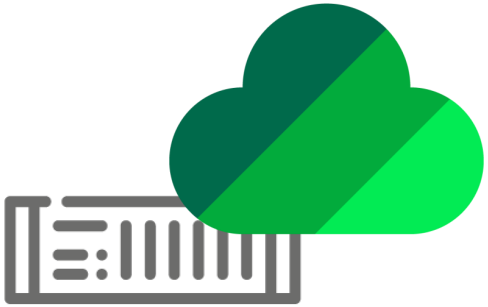
- Эксплуатация виртуальных машин разного уровня критичности в единой инфраструктуре
- «Внешнее» разграничение прав доступа администраторов
- Подтверждение критичных действий над виртуальными машинами
- Независимый аудит действий администраторов

Продукты:

- vGate (все редакции)

КОД безопасности

Защита гипервизора



Сценарии использования:

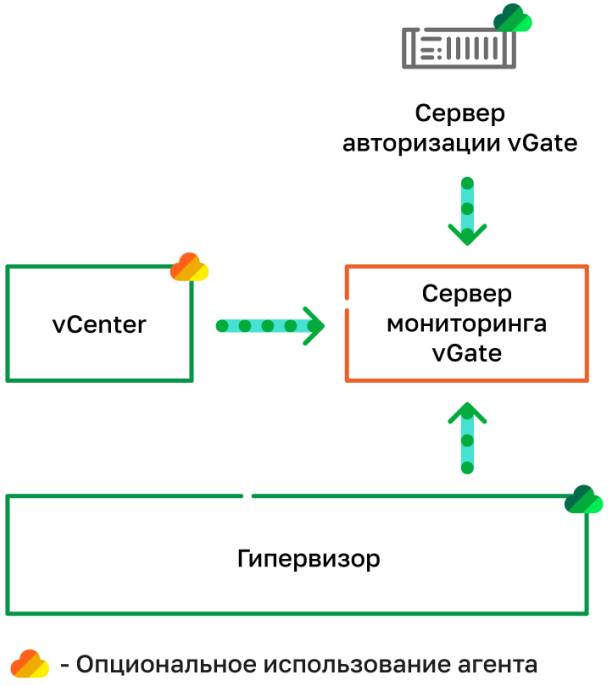
- Безопасная настройка гипервизора
- Контроль подключения к гипервизору внешних устройств
- Контроль соответствия настроек гипервизора стандартам и рекомендациям

Продукты:

- vGate (все редакции)

КОД безопасности

Мониторинг виртуальной инфраструктуры



Сценарии использования:

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

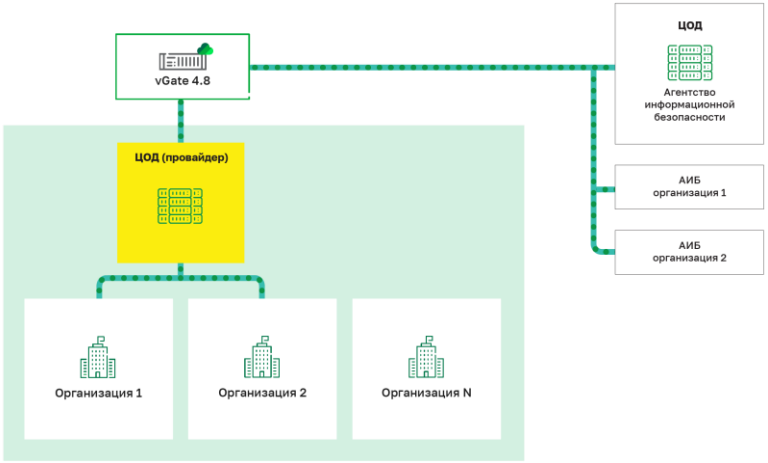
Продукты:

- vGate (редакция Enterprise Plus)

В настоящий момент доступно только для продуктов VMware

КОД безопасности

Мультиарендность



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)

КОД безопасности

Возможности продукта vGate

КОД безопасности

Создание программно-определяемых сетей (SDN) new

- Централизованное создание и изменение виртуализованных сетей
- L2 связность между ВМ в одной сети вне зависимости от физической топологии
- Поддержка VXLAN

КОД безопасности

Поддержка сред виртуализации

Поддерживаемые среды виртуализации	СЗИ	МСЭ
Vmware vSphere 6.5, 6.7, 7.0	+	+
Альт Сервер Виртуализации 10.1 (OpenNebula 5.10.5, Proxmox 7.2)/ 10.2 (OpenNebula 6.2.0, Proxmox 7.4-17) new	+	+
Р-Виртуализация 7.0.13 (Скала-Р Управление 1.98)	+	+
zVirt Node 3.3, 4.0 new, 4.1 new	+	+
РЕД Виртуализация 7.3 (РЕД ОС Муром 7.3.1) new	+	+
ROSA Virtualization 2.1 new	+	+
SpaceVM 6.2.0, 6.2.1, 6.3.1 new, 6.5.0 new	+	-
HostVM 4.4.8 в составе oVirt Node 4.4.8 new	+	+
Utinet Glovirt 2.1.1	+	+
OpenNebula 6.4.0.1 в составе Ubuntu 20.04.5 LTS	+	+
Proxmox 7.4-1, 8.0-2	+	+
ПК СВ «Брест» 3.3 в составе Astra Linux SE 1.7.4.11 релиз «Смоленск» new	+	+
ECP Veil 5.1.9 new	+	-

КОД безопасности

Функционал, доступный для KVM

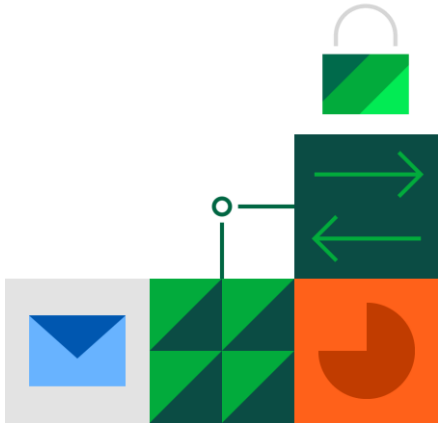
- Контроль запуска виртуальных машин
- Доверенная загрузка виртуальных машин
- Затирание остаточной информации после удаления виртуальных машин
- Разграничение доступа администраторов к гипервизорам

КОД безопасности

vGate на базе Linux new

Доступный функционал:

- vGate Web UI и REST API.
- Поддержка VMware VCSA 7.0.
- Безагентный мандатный контроль для vSphere HTML5 Web Client.
- Политики безопасности для VMware ESXi.
- Контроль целостности ВМ и затирание остаточных данных при удалении ВМ на ESXi хостах.
- Новый механизм резервирования в кластере.
- Дискреционные правила доступа к защищаемым серверам.
- Установка из OVA в виде виртуальной машины.
- Установка на Альт СП релиз 10 и Astra Linux 1.7.5 Смоленск.



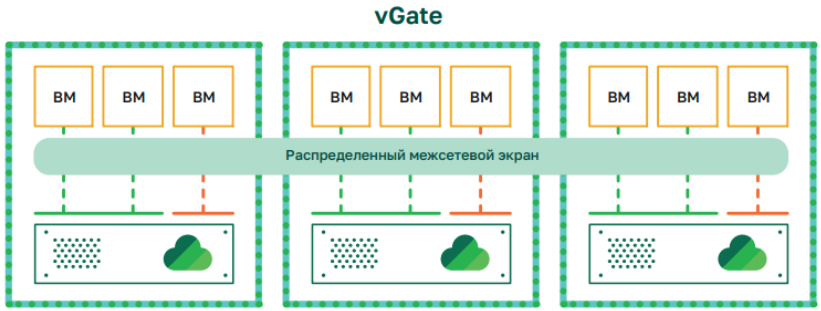
КОД безопасности

Фильтрация сетевого трафика с помощью межсетевого экрана

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

КОД безопасности

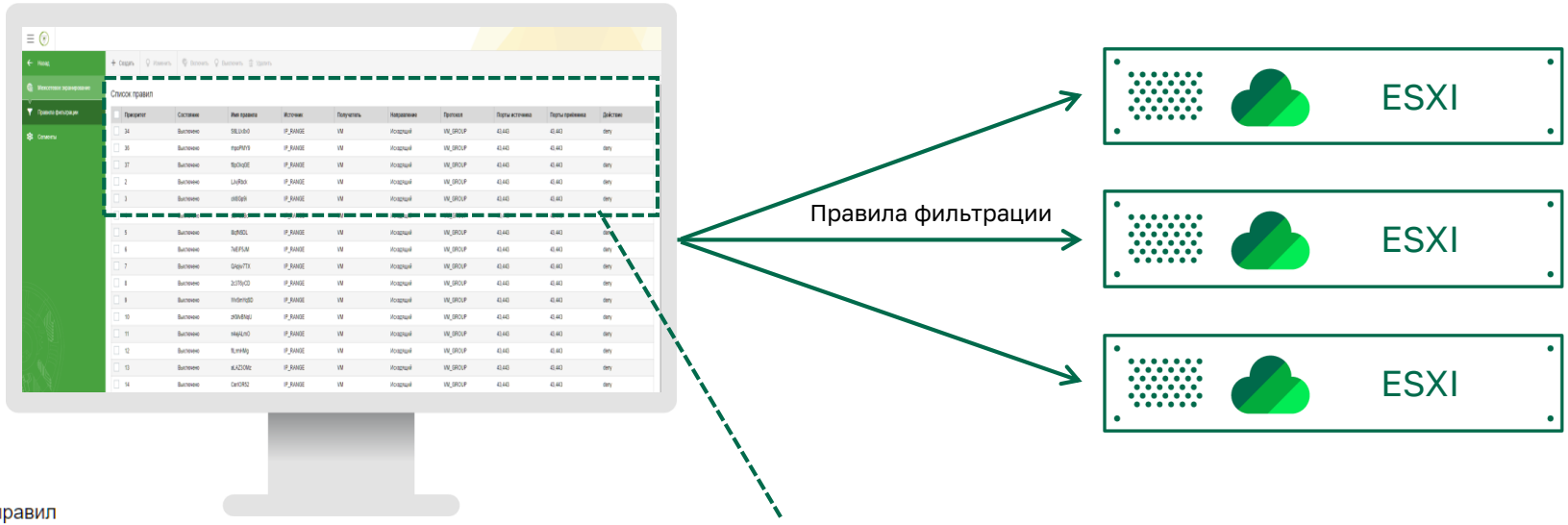
Сегментация виртуальной инфраструктуры с помощью МЭ



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

КОД безопасности

Межсетевой экран
Правила фильтрации



Список правил

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	rhpoPMY9	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

КОД безопасности

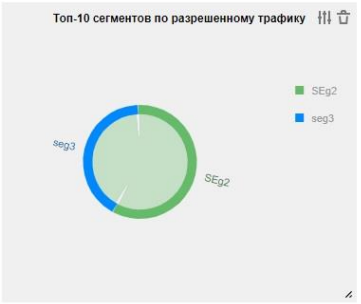
Мониторинг виртуальной инфраструктуры

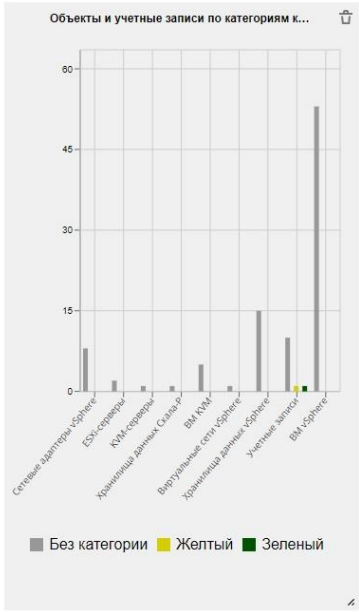
- Сбор, нормализация и фильтрация данных о событиях, происходящих в виртуальной инфраструктуре
- Корреляция событий, в том числе и с событиями самого vGate
- Отправка инцидентов безопасности во внешние системы по протоколу syslog и SMTP
- Встроенные шаблоны правил корреляции
- Контроль действий, осуществляемых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

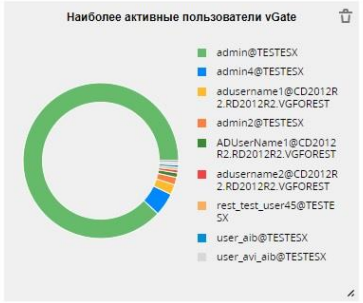
КОД безопасности

Мониторинг событий в реальном времени

Панель мониторинга

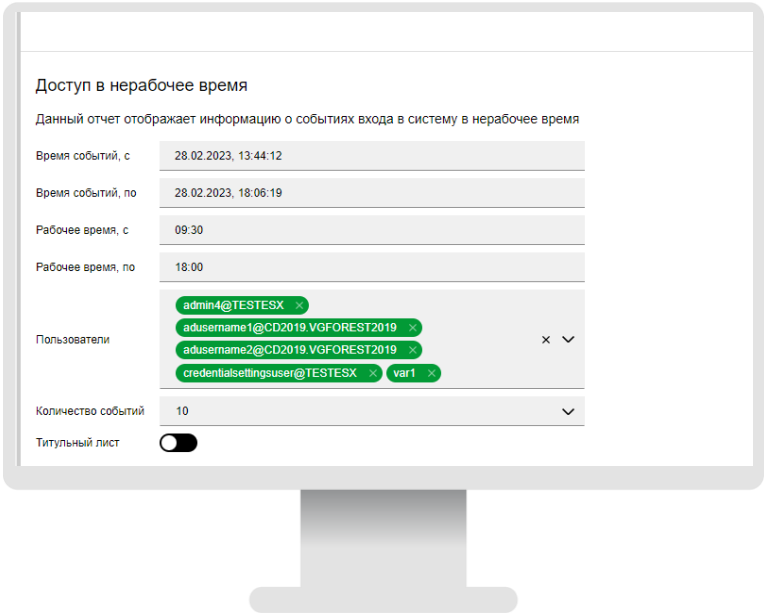






КОД безопасности

Отчетность



28 типов отчетов, разделенных по группам:

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

КОД безопасности

Администрирование

Разграничение доступов администраторов безопасности[new]

- Администратор безопасности ЦОД
- Администратор безопасности организации-арендатора

Встроенные роли администраторов

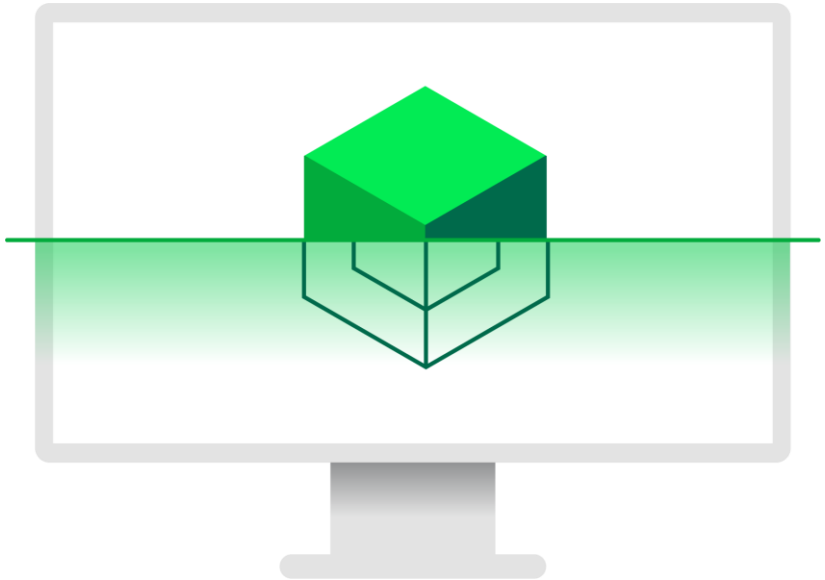
- Администратор ВМ
- Администратор сети
- Администратор СХД
- Пользователь ВМ
- Аудитор

Поддержка аутентификации с JaCarta, Рутокен

Возможность подключения с использованием браузера на любой ОС

КОД безопасности

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

КОД безопасности

Защита виртуальных машин

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

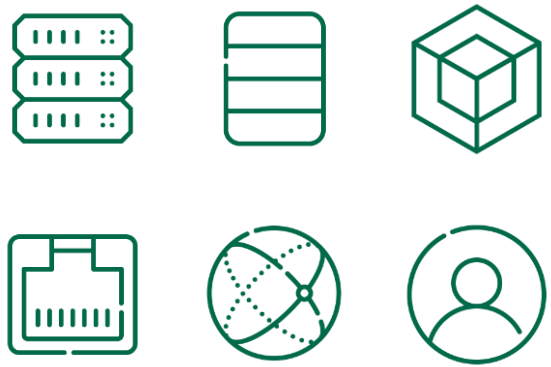
КОД безопасности

Защита гипервизора

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

КОД безопасности

Назначение меток и политик безопасности



Политики объединяются в шаблоны

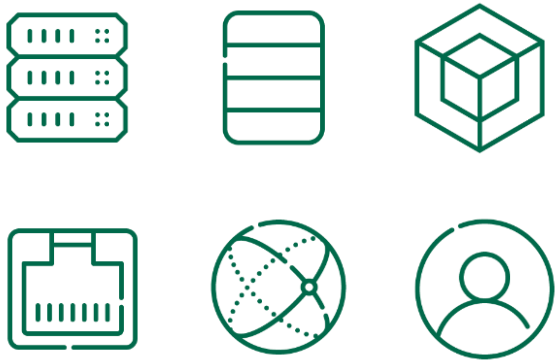
- Встроенные
- Пользовательские

Шаблоны политик назначаются на:

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

КОД безопасности

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

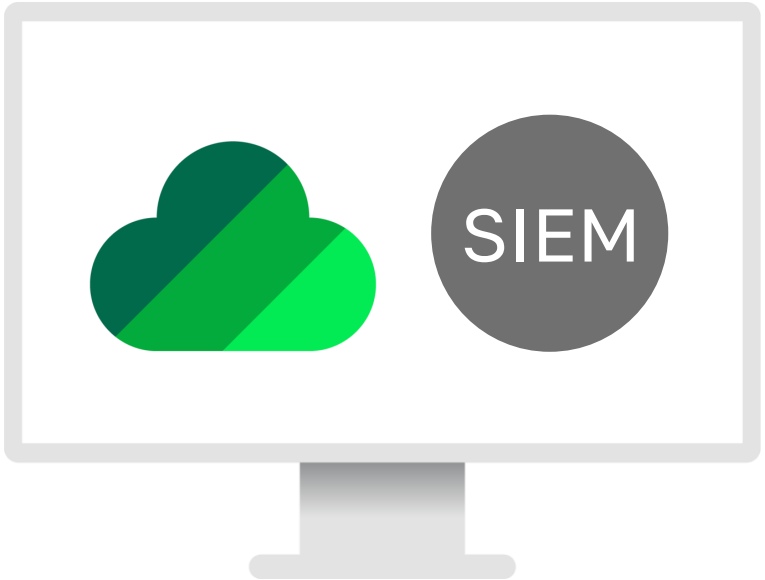
КОД безопасности

Отказоустойчивость

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

КОД безопасности

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

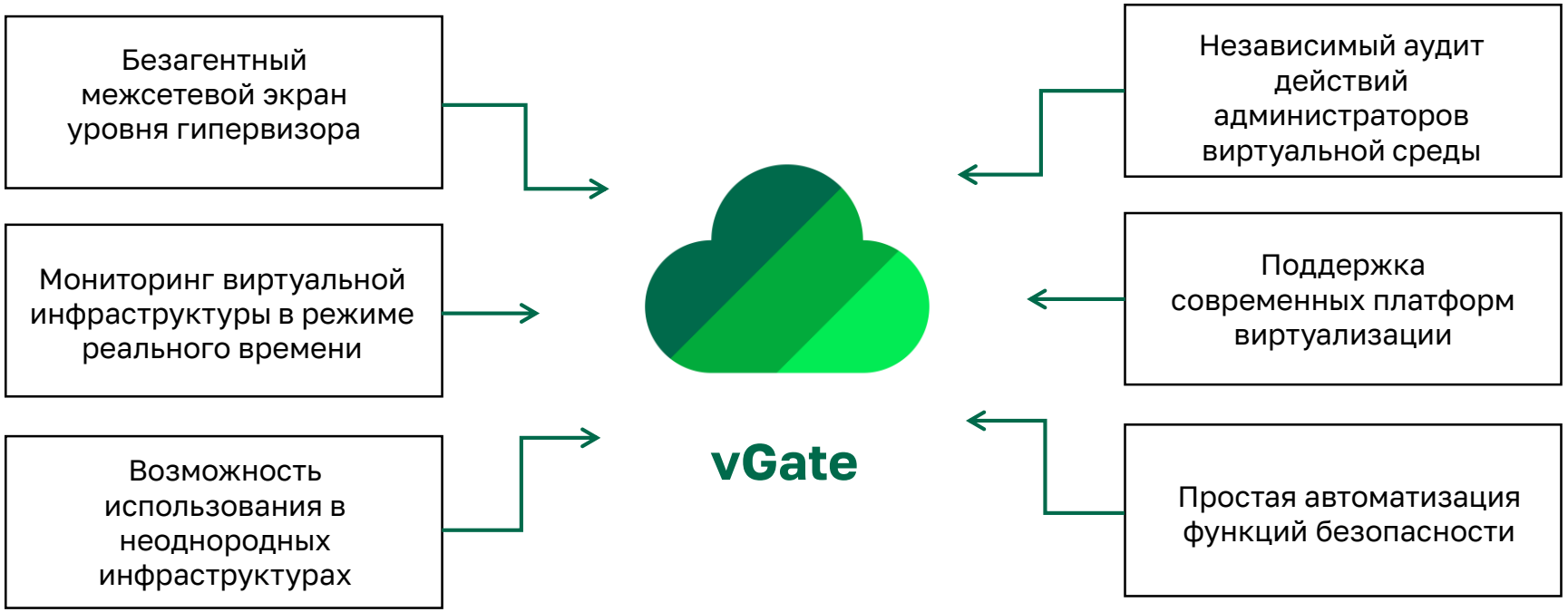
КОД безопасности

Шаблоны политик безопасности

- 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

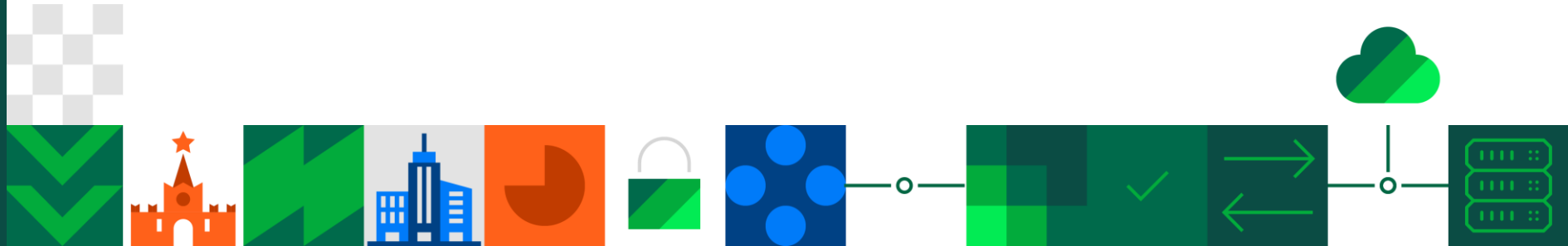
КОД безопасности

Преимущества vGate



КОД безопасности

Лицензирование



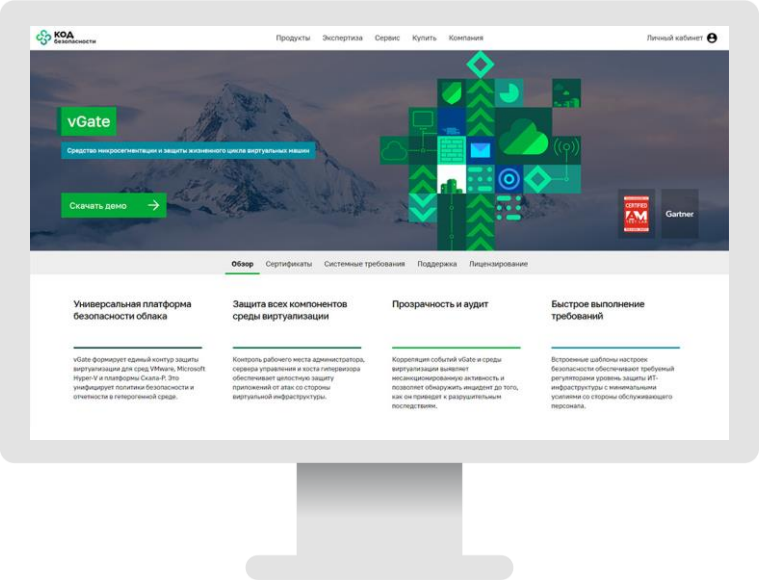
КОД безопасности

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

КОД безопасности

Узнать подробнее



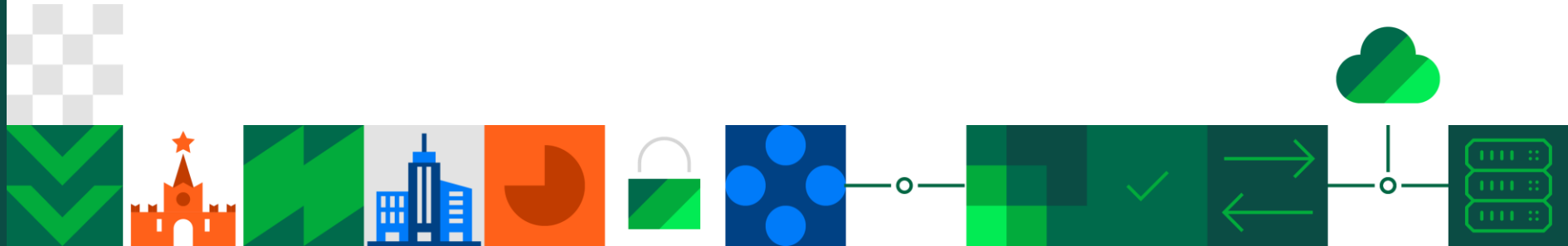
https://www.securitycode.ru/products/vgate/

- 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

КОД безопасности

О компании



КОД безопасности

Факты о компании

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

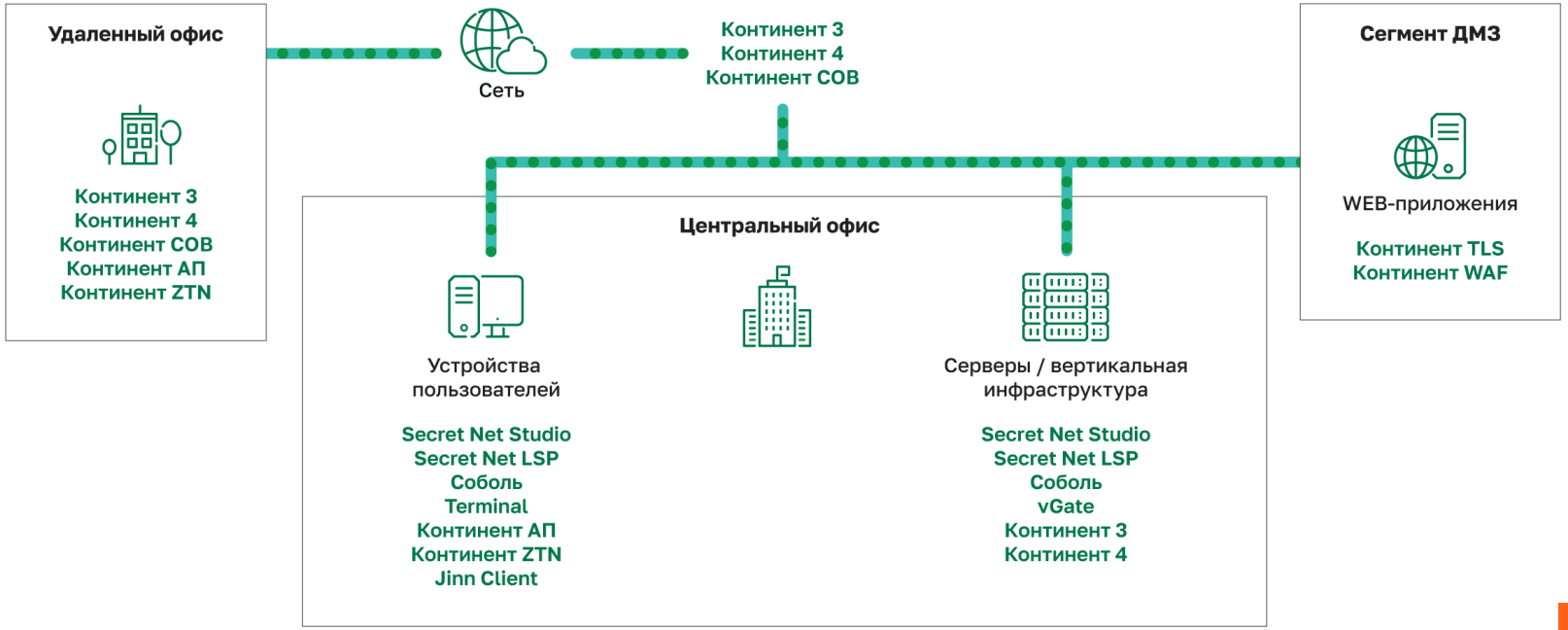
- **Более 30 лет** на страже безопасности крупнейших предприятий России. Ведет свою деятельность на основании **9 лицензий ФСТЭК, ФСБ и Минобороны России.**
- Технологии защиты обеспечивают безопасность **3 000 000** компьютеров в **50 000 организаций.**
- **3 центра разработки:** Москва, Санкт-Петербург, 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).

КОД безопасности

Комплексный подход к защите инфраструктуры



КОД безопасности

Нам доверяют

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

Силовые структуры:

- 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»

Предприятия ТЭК:

- ГК «Росатом»
- ПАО «Газпром»
- ПАО «АК «Транснефть»
- ПАО «НК «Роснефть»»
- ПАО «Россети»

КОД безопасности

Спасибо за внимание!

По вопросам стоимости и покупки продуктов:
buy@securitycode.ru
Служба технической поддержки: support@securitycode.ru

info@securitycode.ru
www.securitycode.ru