



КОД
безопасности

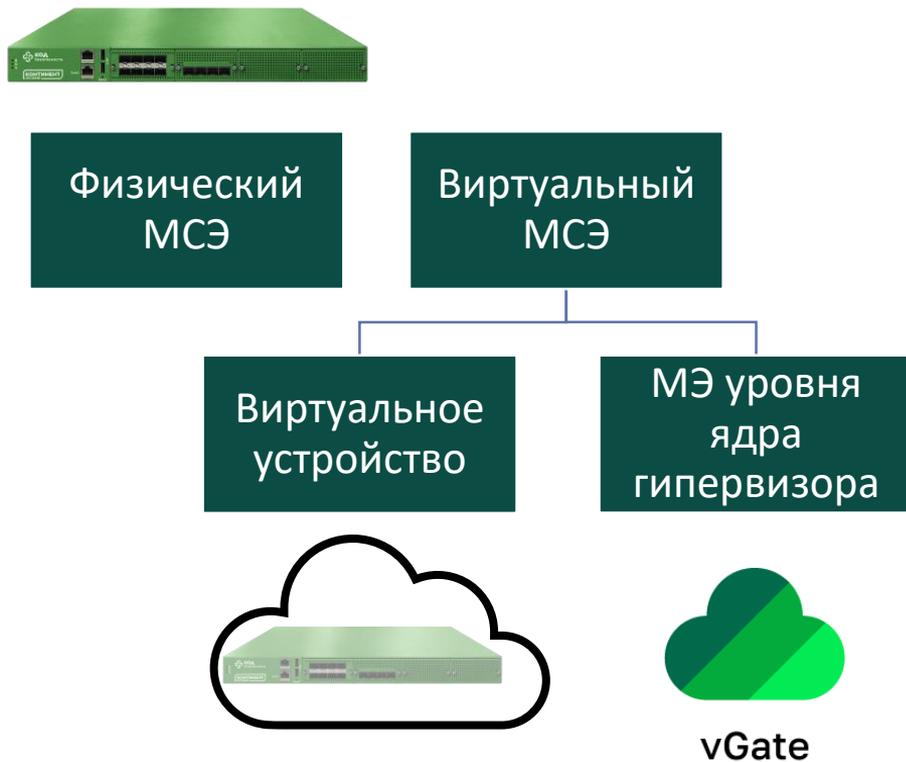


Микро сегментация сети. Защита отечественных сред виртуализации.



*....и еще кое что для выполнения
требований регуляторов*





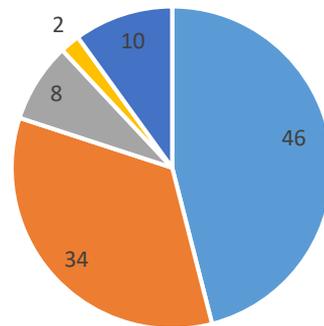
Выделяют три варианта использования МСЭ/NGFW в ЦОД

1. Физический межсетевой экран
2. Виртуальный межсетевой экран уровня сети
3. Виртуальный межсетевой экран уровня гипервизора

Преимущества

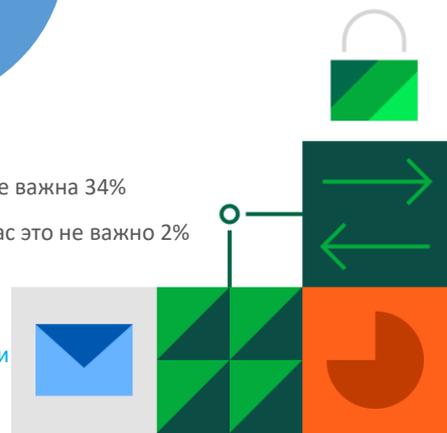
- Встроен в гипервизор
- Распределенная scale-out архитектура без ограничений по производительности
- Гиперконвергентность
- Правила привязаны к виртуальной машине, т.е. они мобильны и всегда актуальны
- Виртуальная машина может быть добавлена в сегмент в момент создания
- Политика сетевой безопасности накладывается в момент создания виртуальной машины

Насколько для вашей компании важна микро сегментация сети в виртуальной инфраструктуре?



- Очень важна 46%
- Скорее важна 34%
- Скорее не важна 8%
- Для нас это не важно 2%
- Затрудняюсь ответить 10%

Опрос проводился в ходе онлайн конференции vGate 03 июля 2024, присутствовало около 1200 слушателей



- Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» с 1 января 2025 г.
- Указ Президента РФ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» с 1 января 2025 г.

1 января 2025

О продукте

vGate

Защита платформ виртуализации



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



Снижение вероятности
инцидентов ИБ

Выполнение
требований
регуляторов

Снижение нагрузки на
администраторов
сети/средств защиты

Решение проблемы
недостаточной
производительности
межсетевых экранов
уровня ЦОД



Спасибо за внимание!

Евгений Тарелкин– Ведущий эксперт
e.tarelkin@securitycode.ru

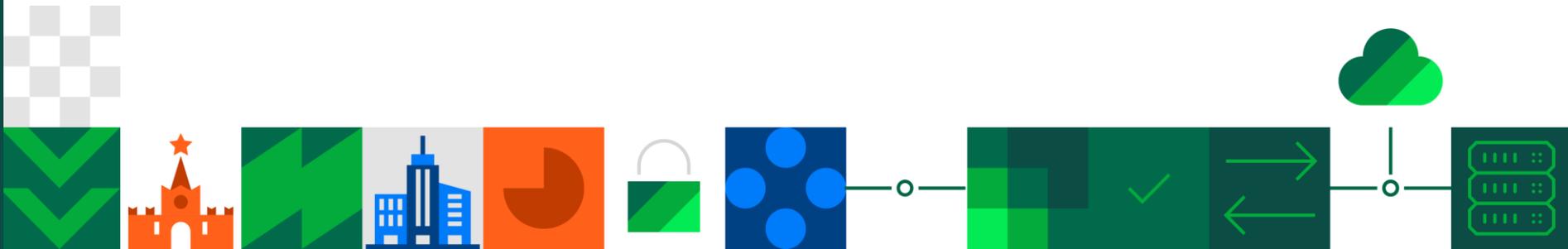
info@securitycode.ru

www.securitycode.ru





Истории успеха





- В своем составе **8 крупнейших ЦОД** (Москва, СПб, Новосибирск, Екатеринбург, Алматы, Минск, Нетания).
- По итогам 2023 года входит в **ТОП-3** провайдеров IaaS Enterprise 2023*



99,99%

SLA

150

инженеров

300

реализованных
проектов

Основные задачи :

- ✔ Соответствие строгим требованиям регуляторов (Защищенное облако 152-ФЗ)
- ✔ Искключение простоев предоставляемых сервисов
- ✔ Формирование образа надежного поставщика
- ✔ Сохранение конфиденциальности данных

- ✔ Крупная инсталляция ИТ инфраструктуры (более 800 физических серверов)
- ✔ Недоступность критических обновлений VMware

- ✔ Потребность в атомарной сегментации сети
- ✔ Прагматичный выбор заказчика, вынужденного использовать продукты ушедших компаний (Vmware)

VMware » Esxi : Security Vulnerabilities, CVEs

Published in: 2024 January February March April May June

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In: [CISA KEV Catalog](#)

Sort Results By: Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

10 vulnerabilities found

CVE ID	Max CVSS	EPSS Score	Published	Updated
CVE-2024-22273	8.1	0.00	2024-05-21	2024-05-22
CVE-2024-22255	7.5	0.00	2024-03-05	2024-03-05
CVE-2024-22254	7.0	0.00	2024-03-05	2024-03-05
CVE-2024-22253	8.3	0.00	2024-03-05	2024-03-05
CVE-2024-22252	8.3	0.00	2024-03-05	2024-03-05

Итоги внедрения:

КОНТРОЛЬ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ

АУДИТ ВИРТУАЛЬНЫХ МАШИН

МИКРОСЕГМЕНТАЦИЯ