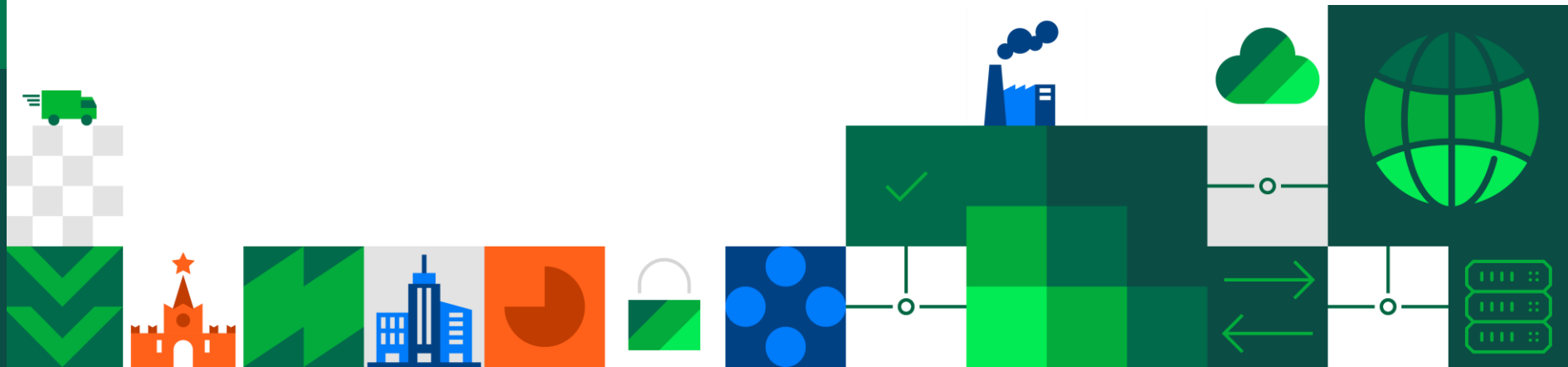
КОД безопасности

vGate. Защита виртуальных инфраструктур



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


За безопасность необходимо платить, а за её отсутствие — расплачиваться.
Уинстон Черчилль

КОД безопасности

Последствия:
Вот как отразилась хакерская атака на СДЭКе

Инцидент обездвижел компанию на 3 дня

Ущерб от простоя. Эксперты оценивают его от 300 миллионов до 1 миллиарда рублей.

Чистая прибыль СДЭК-Глобал в 2023 г. выросла на 43.17% до 1.49 млрд руб

Лицензия на продукт может стоить порядка 3 миллионов рублей. Лицензия на автоматизированную систему для слежения за внешней поверхностью атак — 800 тысяч рублей.

КОД безопасности

Соответствие требованиям регуляторов

- 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

Преимущества использования накладных средств СЗИ

- Сертифицированные версии требуют время на сертификацию(около 12 месяцев) за это время функционал их устаревает

- Лучший продукт(стабильный и доказавший масштабирование) в области защиты виртуализации мы внедряем лучшее решение и реализуем

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

КОД безопасности

Сертификация

ФСТЭК России

ФСТЭК России:

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

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

Сертификация по требования приказа ФСТЭК №187 от 27.10.2022 (Требования безопасности к средам виртуализации) не планируется

КОД безопасности

Основные направления развития средств защиты виртуализации

Контроль жизненного цикла ВМ

- Контроль потенциально фатальных действий админа
- Аудит
- Контроль целостности ВМ

Виртуализация сети

- Микросегментация
- Обеспечение сетевой связности

КОД безопасности

О продукте

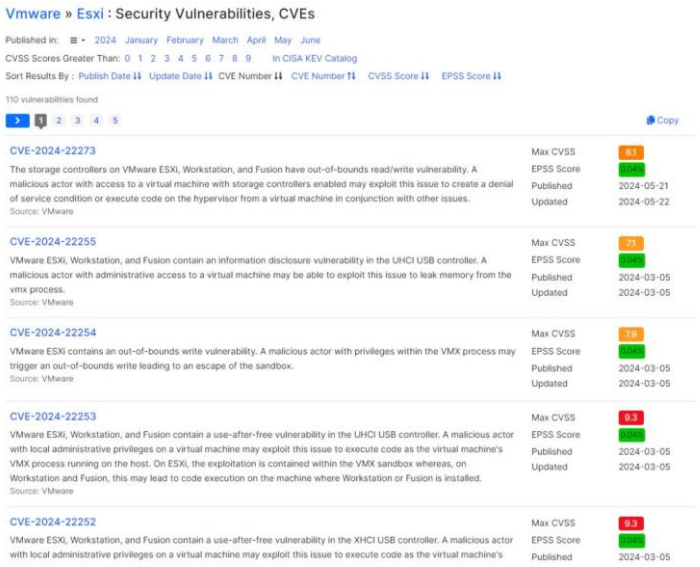
vGate

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

Обзор уязвимостей VMware



Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	0	0	0	8	1
2015	3	1	1	8	0
2016	6	3	3	9	3
2017	20	2	5	12	5
2018	12	2	6	7	8
2019	4	1	3	11	9
2020	14	4	12	15	5
2021	10	6	11	10	16
2022	21	7	17	11	15
2023	10	0	9	12	6
2024	8	2	5	7	7
Total	108	28	72	110	75

Например 20 июня 2024 года найдена была уязвимость с рейтингом 9.8

https://www.cvedetails.com/cve/CVE-2024-37080/

Сервер vCenter Server содержит уязвимость, связанную с переполнением очереди при реализации протокола DCERPC. Те злоумышленник, имеющий сетевой доступ к серверу vCenter Server, может активировать эту уязвимость, отправив специально созданный сетевой пакет, который может привести к удаленному выполнению любого (в том числе вредоносного) кода на данной инфраструктуре

2022 год – 15 CVE

2023год- 25 CVE

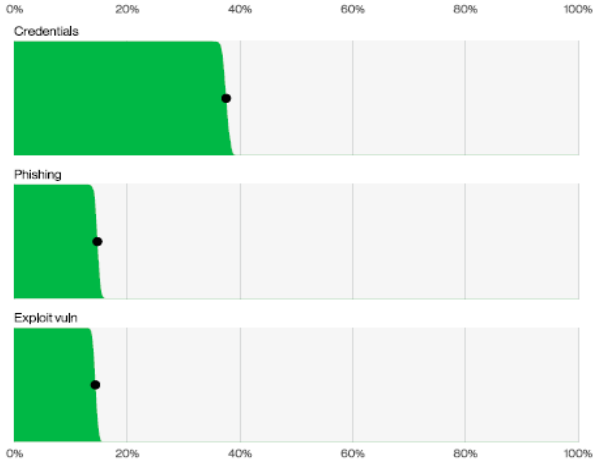
За текущий 2024 -уже 6 CVE

Всего – более 400 уязвимостей было найдено

Так же в апреле 2025 года end of general support VMware vSphere 7.0, которой сейчас пользуется большая часть рынка. Это произойдет 2 апреля 2025 год. После этой даты для пользователей больше не будет доступных обновлений и патчей продукта, в том числе по информационной безопасности, а поддержка прекратится, когда подойдет к концу срок действия сертификата на нее

КОД безопасности

Значительный рост атак



of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error

Щелчок Таноса для оператора связи

Анализ показывает значительный рост атак, связанных с использованием уязвимостей в качестве критического пути для инициирования взлома - почти в три раза по сравнению с прошлым годом.

В первую очередь использующими веб-приложения в качестве начальных точек входа.

Source: 2024 DBIR Summary Report

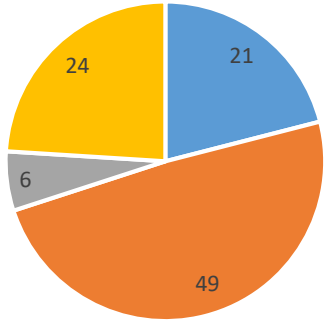
КОД безопасности

Доли российских игроков на рынке решений для виртуализации растут после утраты доминирующих позиций Vmware и Microsoft

Активно импортозамещение виртуализации идет в следующих секторах

- Государственном
- Финансовый (банках, страховых компаниях)
- ИТ телеком

Планируете ли вы мигрировать на отечественные системы виртуализации?

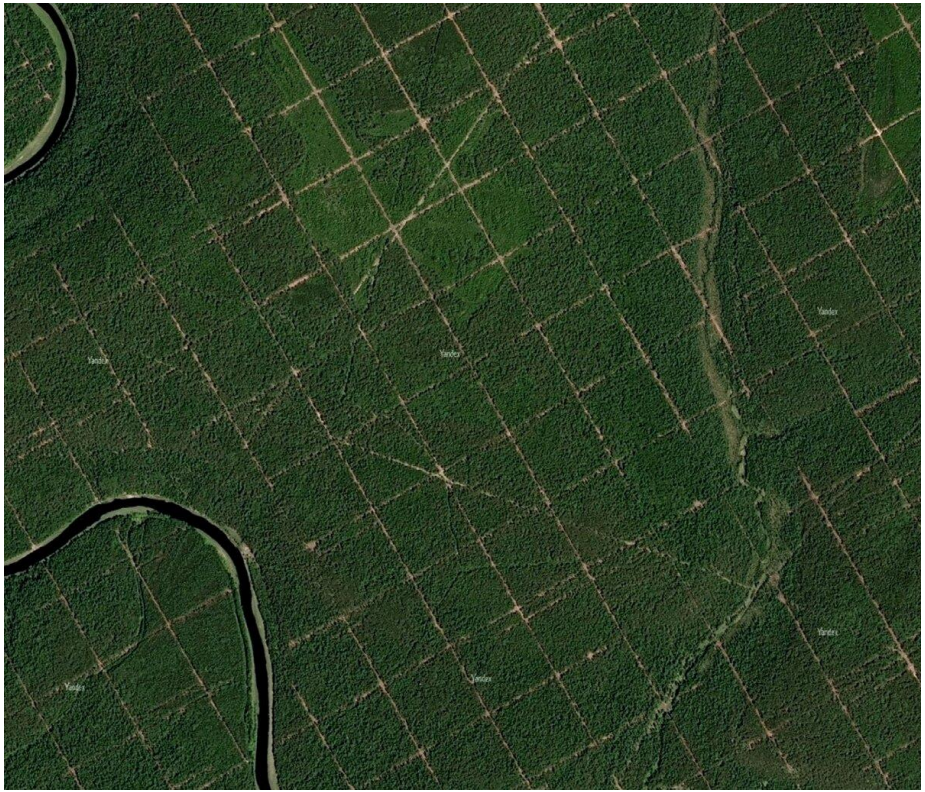


- Да, уже мигрируем на российские системы 21%
- Да, но пока смотрим и тестируем 49%
- Нет, точно останемся на импорте 6%
- Нет, пока ждем и наблюдаем 24%

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

КОД безопасности

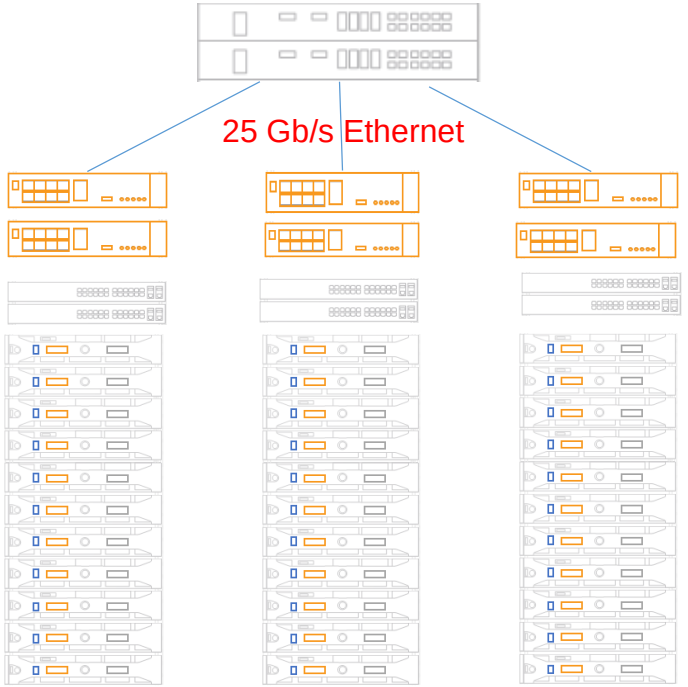
Пример изоляции пожаров



КОД безопасности

Нюансы защиты сети ЦОД

- В ЦОД обрабатываются большие объемы трафика и нужна соответствующая пропускная способность МСЭ/NGFW.
- К тому же необходимо фильтровать трафик как для выхода виртуальных машин в Интернет (паттерн север-юг), так и трафик между виртуальными машинами (паттерн запад-восток)
- Высокие требования производительности и отказоустойчивости под нагрузкой
- Поддержка VXLAN и других сетевых технологий
- Переход на отечественную виртуализацию



КОД безопасности

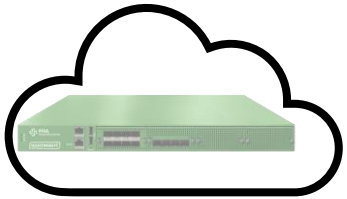
Различные варианты межсетевых экранов для задачи

Физический МСЭ

Виртуальный МСЭ

Виртуальное устройство

МЭ уровня ядра гипервизора



vGate

Выделяют три варианта использования МСЭ/NGFW в ЦОД

1.Физический межсетевой экран

2.Виртуальный межсетевой экран уровня сети

3.Виртуальный межсетевой экран уровня гипервизора

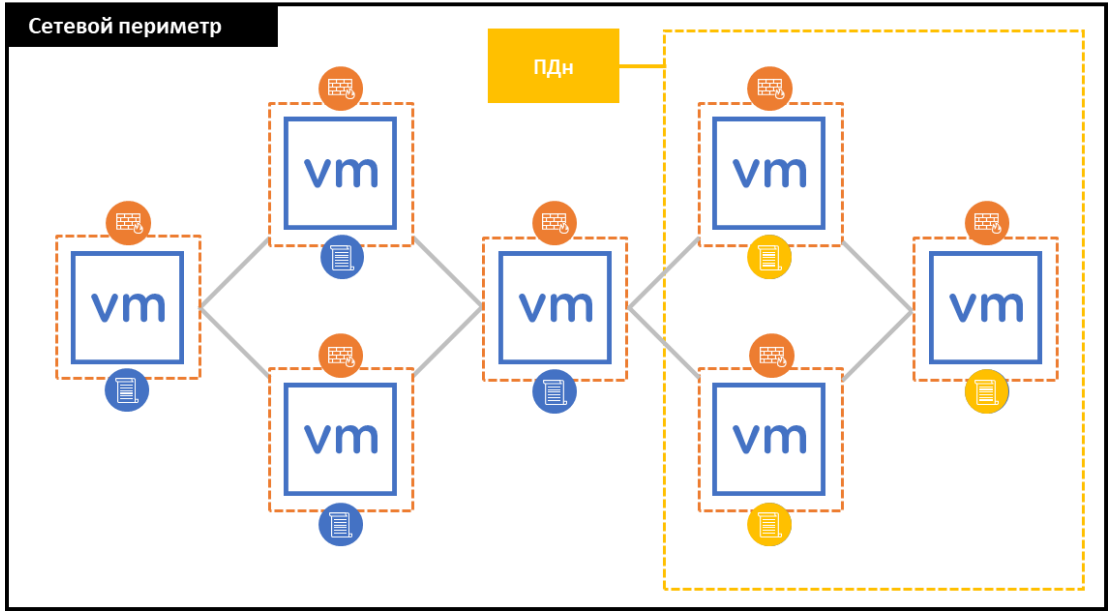
КОД безопасности

Аппаратное решение уровня ЦОД

- Модульность
  - 12 вычислительных лезвий
  - 2 коммутатора-балансировщика
- Интерфейсы
  - 24x QSFP 100G
- Производительность (Real-world mix)
  - Межсетевой экран: 600 Гбит/с
  - Режим COB: 200 Гбит/с
  - Режим NGFW: 100 Гбит/с

КОД безопасности

Межсетевой экран уровня гипервизора



Для каждой виртуальной машины:

- Индивидуальный межсетевой экран
- Индивидуальные политики безопасности

Политики на основе разных критериев

- Атрибуты ВМ
- Сетевые атрибуты

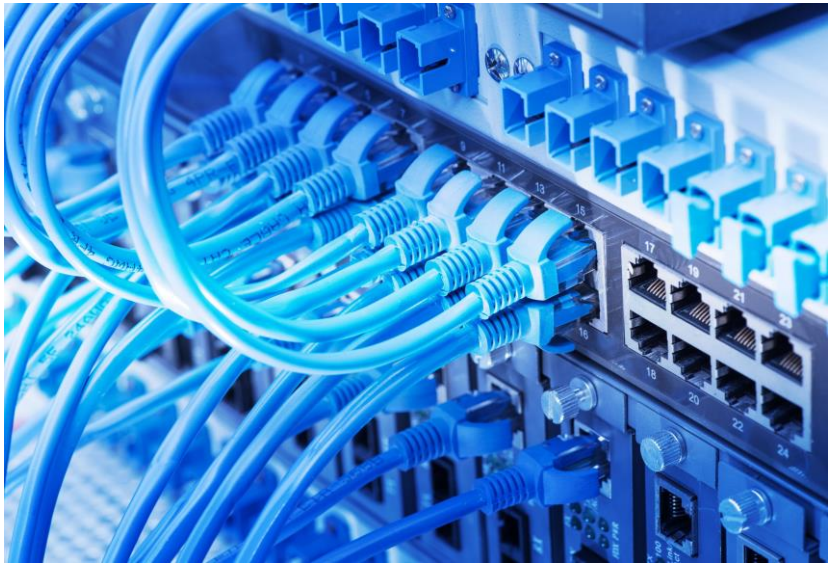
Сравнение стоимости с физическим МСЭ

Вариант №1 интерконект выполнен на 10 ГБ\с интерфейсе

Расчет стоимости фильтрации трафика – NGFW
100 Серверов с 10Гб\с сетью 2х1000 Гб\с
20 х IPC-R5000 по 100 Гб\с
ориентировочный прайс – 5 млн штука
Итого 100 млн руб
Расчет стоимости фильтрации трафика – vGate
100 серверов = 200 лицензий vGate
Итого 30 млн руб

Вариант №2 интерконект выполнен на 25 ГБ\с интерфейсе

Расчет стоимости фильтрации трафика – NGFW
300 Серверов с 25Гб\с сетью 2х7500 Гб\с
150 х IPC-R5000 по 100 Гб\с
ориентировочный прайс – 5 млн штука
Итого 750 млн руб
Расчет стоимости фильтрации трафика – vGate
300 серверов = 600 лицензий vGate
Итого 90 млн руб



КОД безопасности

Социальные сети

КОД безопасности

Спасибо за внимание!

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

info@securitycode.ru

www.securitycode.ru