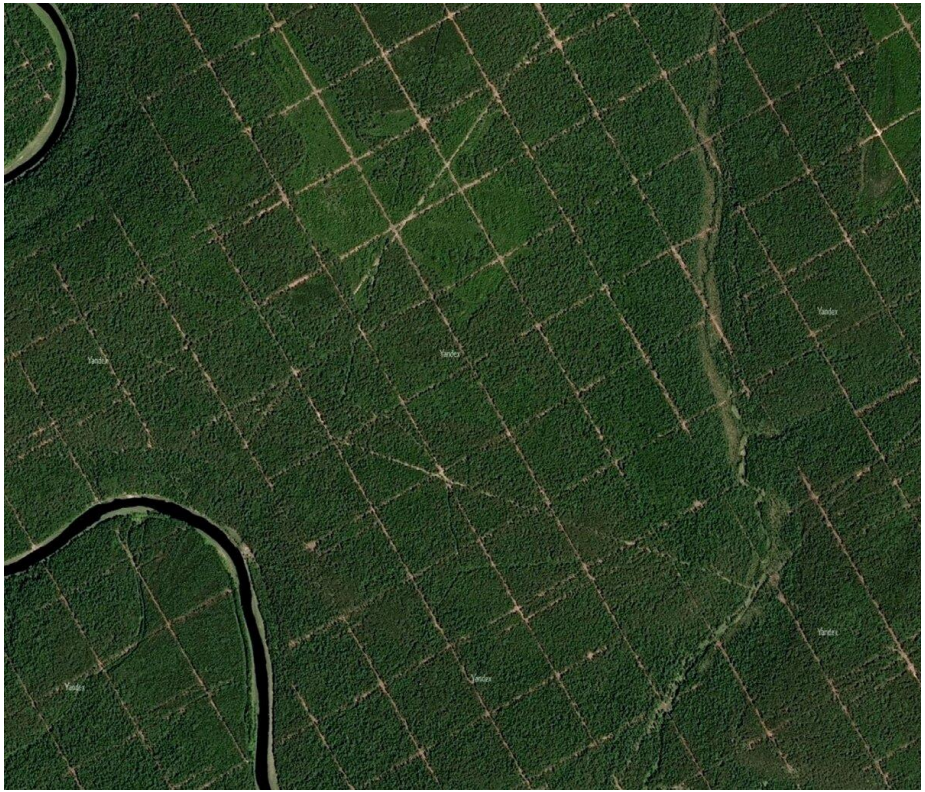
КОД безопасности

Микросегментация виртуальной среды

….и еще кое что для выполнения требований регуляторов

КОД безопасности

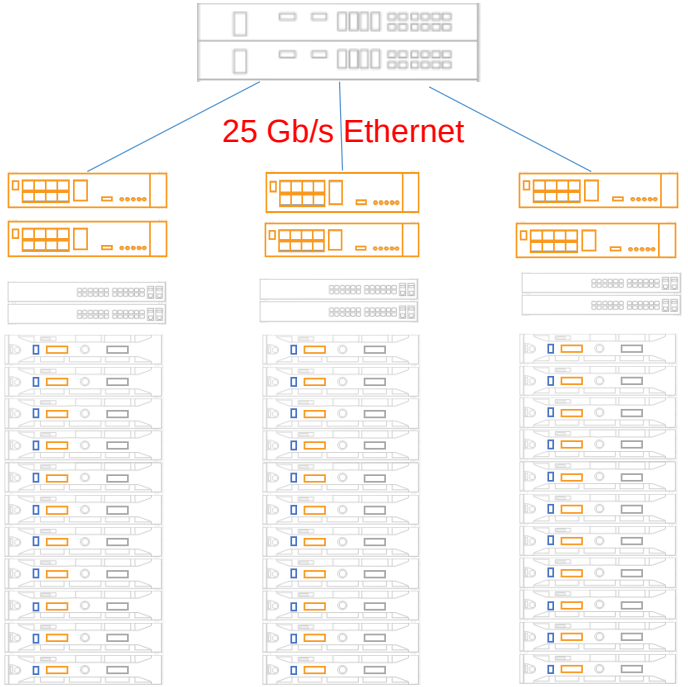
Пример изоляции пожаров



КОД безопасности

Трафик в ЦОДе

- 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)



КОД безопасности

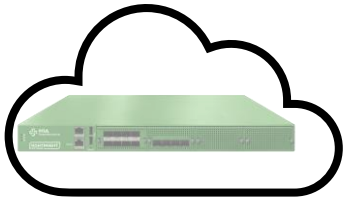
Различные варианты межсетевых экранов для задачи

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

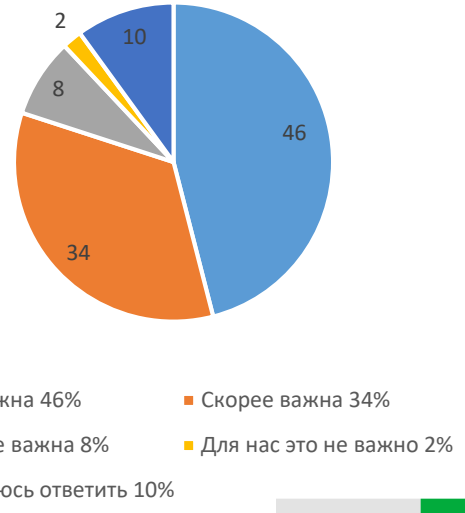
3.Виртуальный межсетевой экран уровня гипервизора

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?



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

КОД безопасности

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

КОД безопасности

Защита отечественной виртуализации

- Разграничение доступа
- Контроль старта ВМ
- Затирание дисков при удалении ВМ
- Контроль целостности ВМ

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

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

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

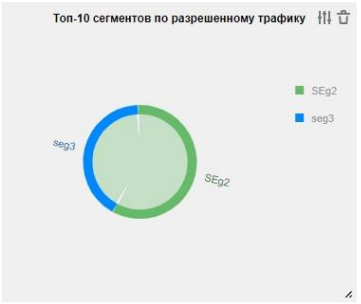
Планируете ли вы мигрировать на отечественные системы виртуализации?

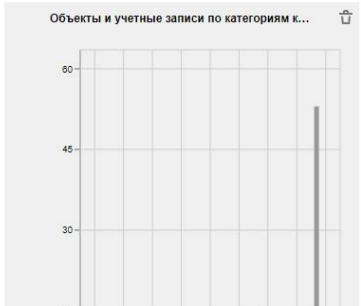
Опрос проводился в ходе онлайн конференции vGate 03 июля 2024, присутствовало около 1200 слушателей

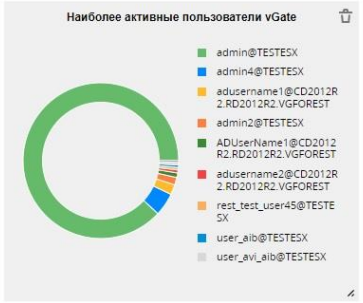
КОД безопасности

Мониторинг событий в реальном времени

Панель мониторинга







КОД безопасности

Эффект от внедрения

Снижение вероятности инцидентов ИБ

Выполнение требований регуляторов

Снижение нагрузки на администраторов сети/средств защиты

Решение проблемы недостаточной производительности межсетевых экранов уровня ЦОД

КОД безопасности

Социальные сети

КОД безопасности

Спасибо за внимание!

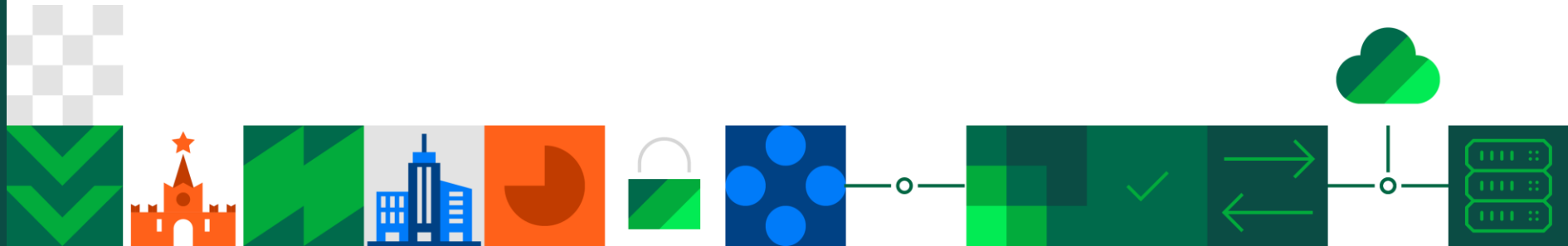
Евгений Тарелкин– Ведущий эксперт
e.tarelkin@securitycode.ru

info@securitycode.ru

www.securitycode.ru

КОД безопасности

Истории успеха



КОД безопасности

Softline Cloud Provider

- 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 :

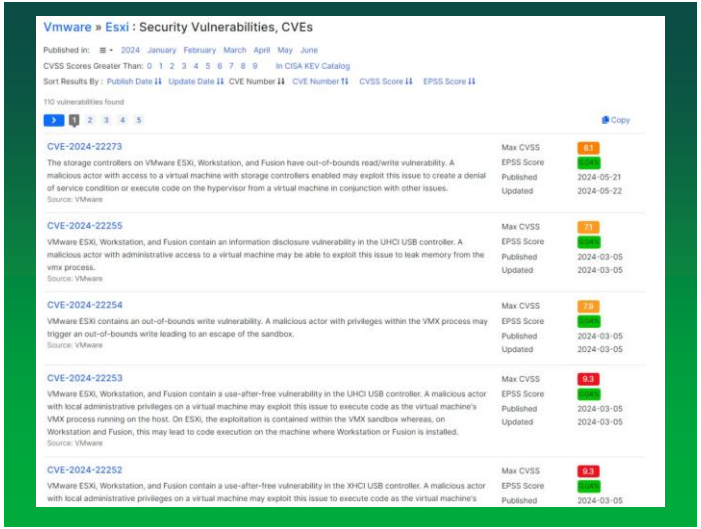
- Соответствие строгим требованиям регуляторов (Защищенное облако 152-ФЗ)
- Исключение простоев предоставляемых сервисов
- Формирование образа надежного поставщика
- Сохранение конфиденциальности данных

* Source https://www.cnews.ru/reviews/iaas_enterprise_2023

КОД безопасности

Крупнейший заказчик из Энергетического сектора

- 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)



Итоги внедрения:

КОНТРОЛЬ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ

АУДИТ ВИРТУАЛЬНЫХ МАШИН

МИКРОСЕГМЕНТАЦИЯ