Особенности национального управления уязвимостями

Vulns.io VM

Новые реалии – зарубежные VM-решения

Qualys
VMDR
Vulnerability Management, Detection and Response

tenable
Nessus
vulnerability scanner
tenable.io

RAPID7
metasploit
nexpose

TRIPWIRE
IP360

GFI LanGuard

Новые реалии – зарубежные VM-решения ушли из РФ

фродекс

Российскому IT – Российское VM

Переход на отечественные ОС

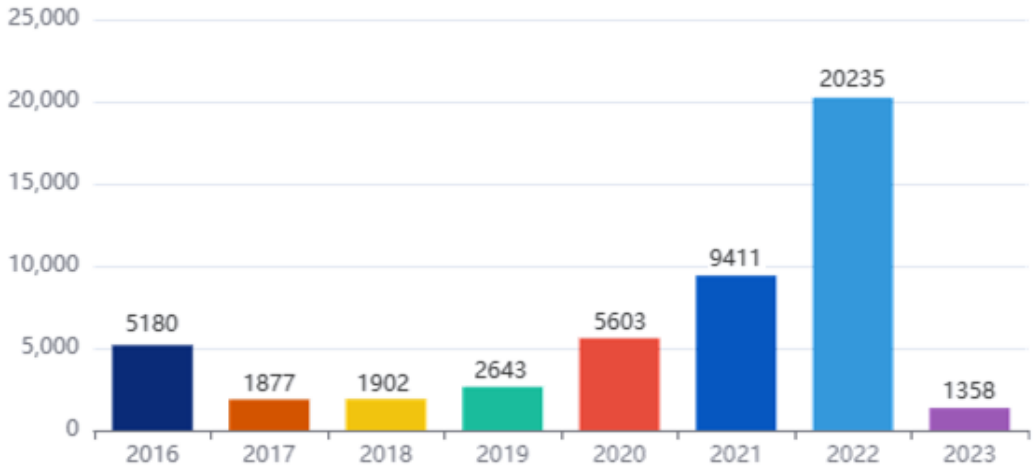
Развитие российского ПО

РЕЕСТР РОССИЙСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

16 201
Включено ПО в Реестр

5 485
Правообладателей

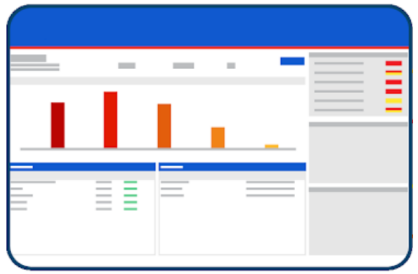
Статистика заявлений в РРПО за 2016-2023 гг.



фродекс

Приоритизация уязвимостей – какую выбрать?

Приоритизация уязвимостей – методика ФСТЭК



Результат аудита ИС

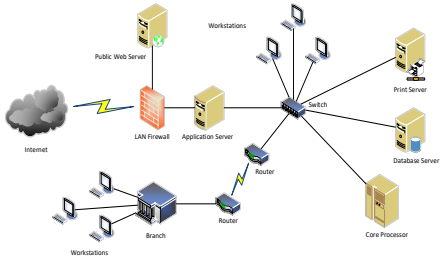
CVE

CVSS 3.1

- Базовые метрики
- Временные метрики
- Контекстные метрики

I_{cvss}

Сведения о составе и архитектуре ИС



Тип компонента

$k \cdot K$

Кол-во уязвимых компонент

$l \cdot L$

Влияние на защиту периметра

$p \cdot P$

I_{infr}

V

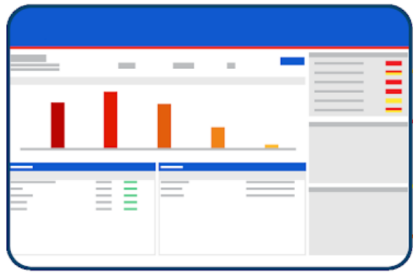
Время устранения

< 4м | < 4н | < 7д | < 24ч

0 | 1,5 | 4,5 | 7 | 10

фродекс

Приоритизация уязвимостей – методика ФСТЭК



Результат аудита ИС

CVE

CVSS 3.1

- Базовые метрики
- Временные метрики
- Контекстные метрики

I_{cvss}

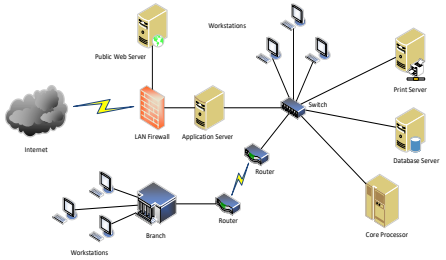
?

ГОССОПКА

НКЦКИ

V

Сведения о составе и архитектуре ИС



Тип компонента

$k \cdot K$

Кол-во уязвимых компонент

$l \cdot L$

Влияние на защиту периметра

$p \cdot P$

I_{infr}

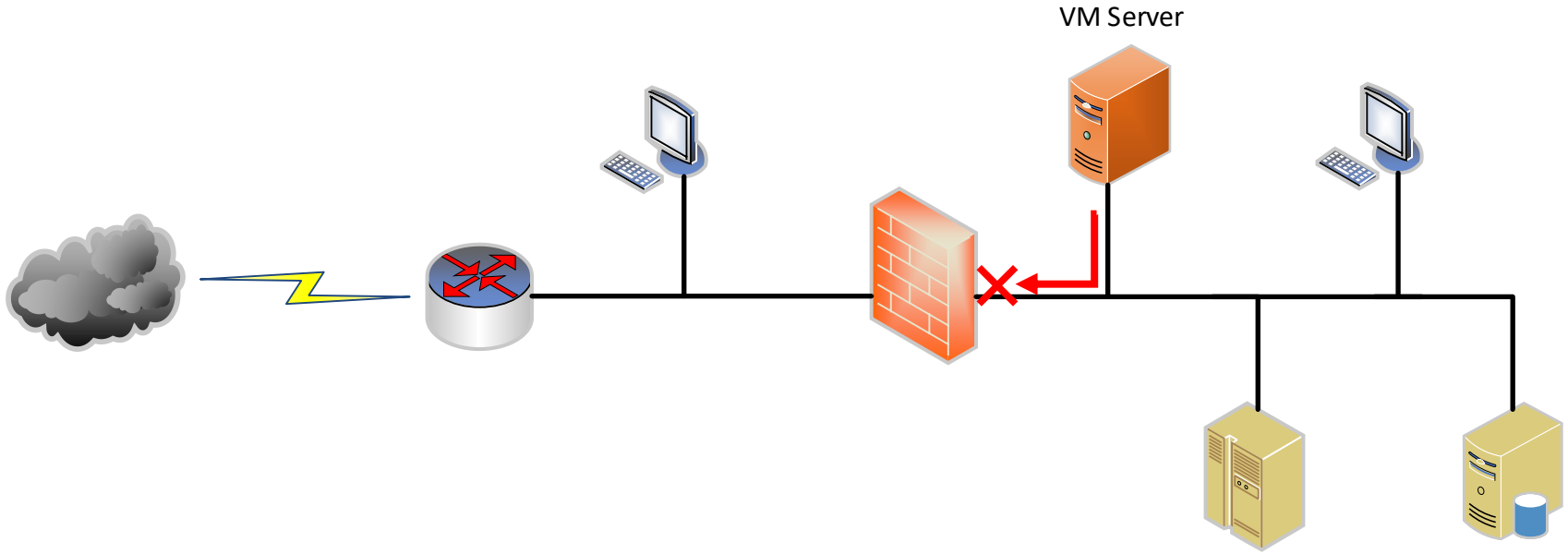
Время устранения

< 4м < 4н < 7д < 24ч

0 1,5 4,5 7 10

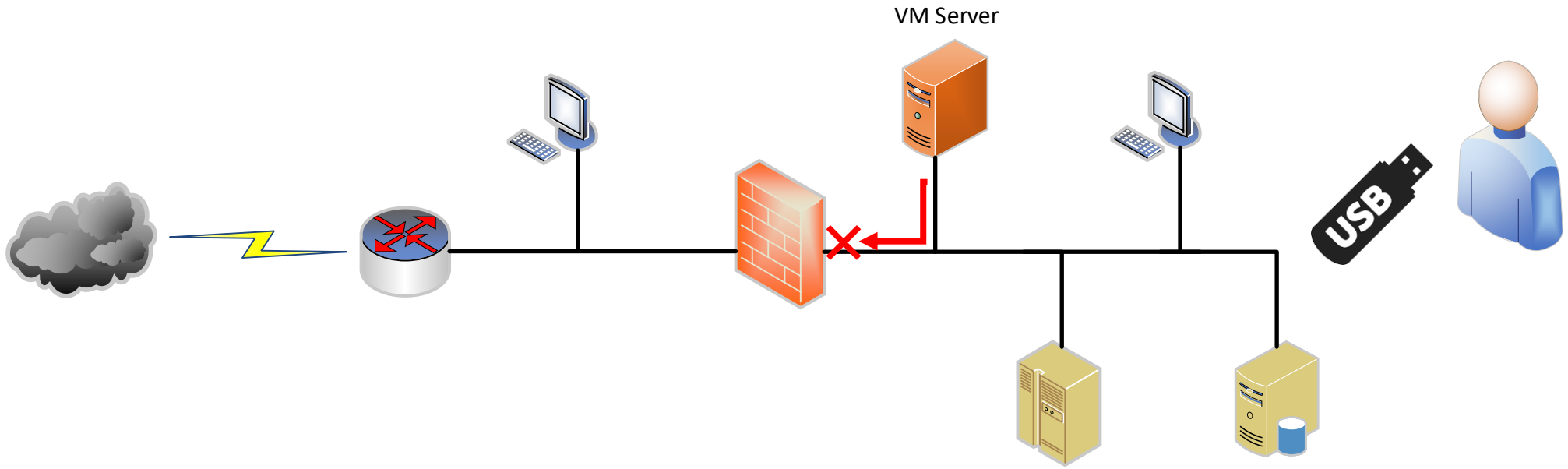
фродекс

«Оффлайн» режим – обновления в изолированной ИС



Как обновлять VM-систему?

«Оффлайн» режим – обновления в изолированной ИС

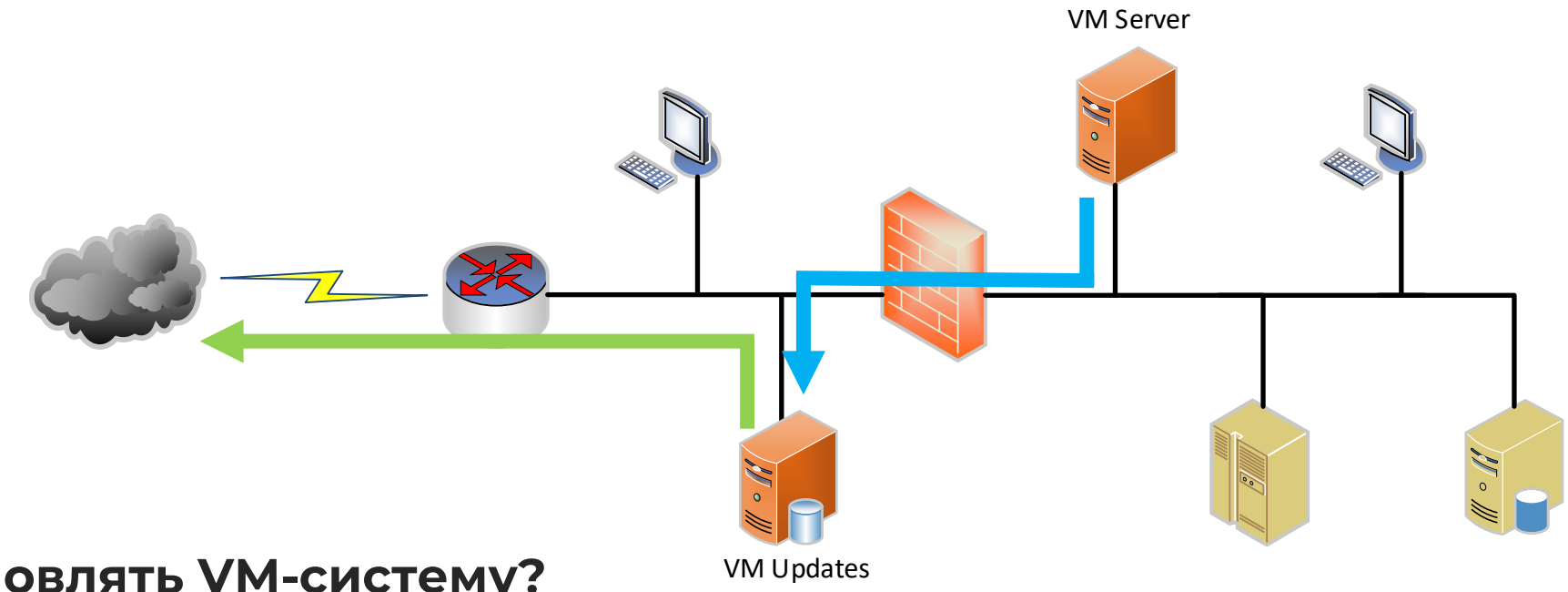


Как обновлять VM-систему?

1) Вручную

- Нужен регламент обновления
- Снижается оперативность обновления

«Оффлайн» режим – обновления в изолированной ИС



Как обновлять VM-систему?

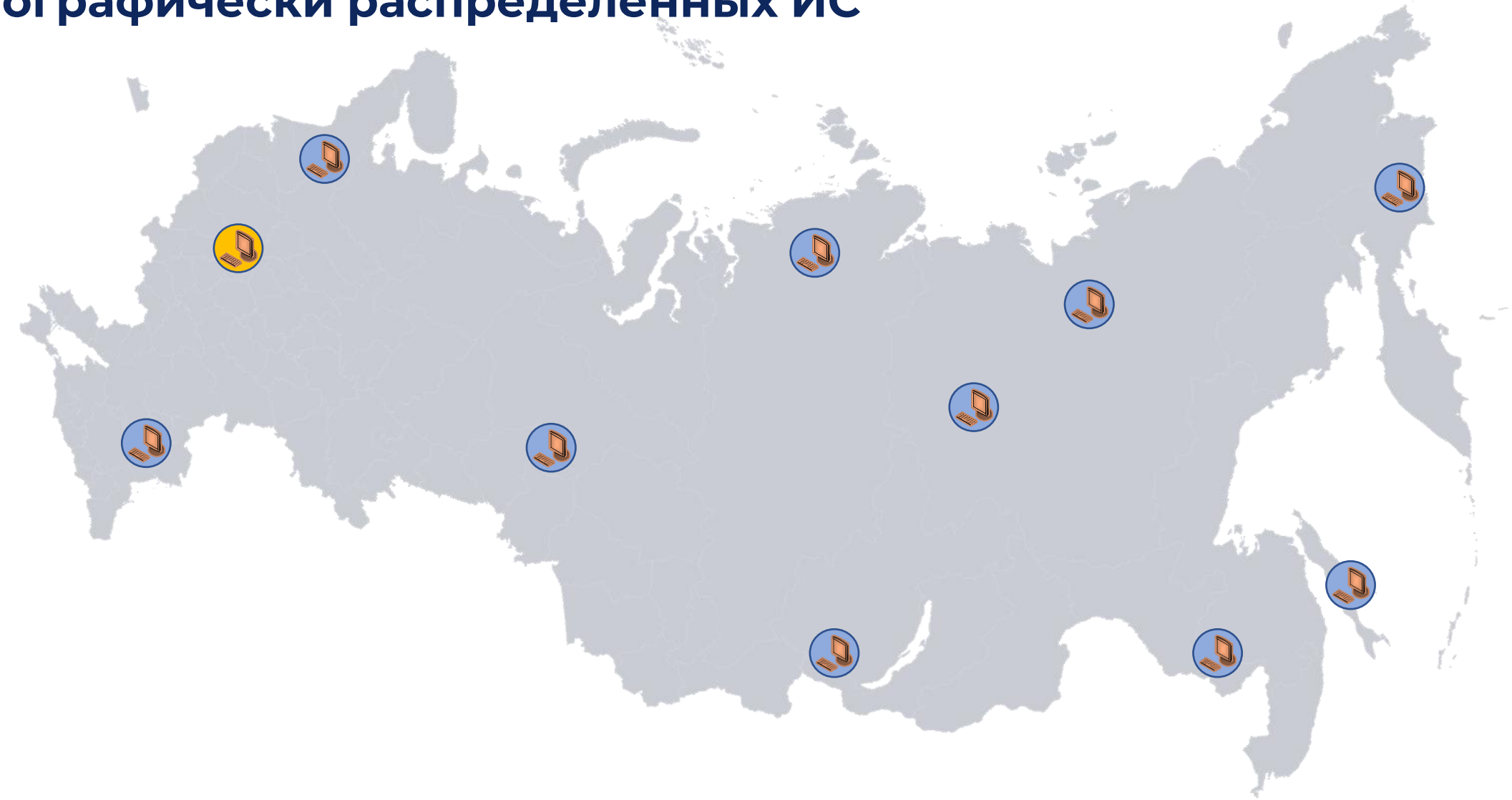
1) Вручную

- ✗ Нужен регламент обновления
- ✗ Снижается оперативность обновления

2) Автоматически

- ✓ Локальный сервер обновлений – всегда актуальные данные
- ✓ Схема попеременного доступа – сегмент остается изолированным

VM для географически распределенных ИС



фродекс

VM для географически распределенных ИС

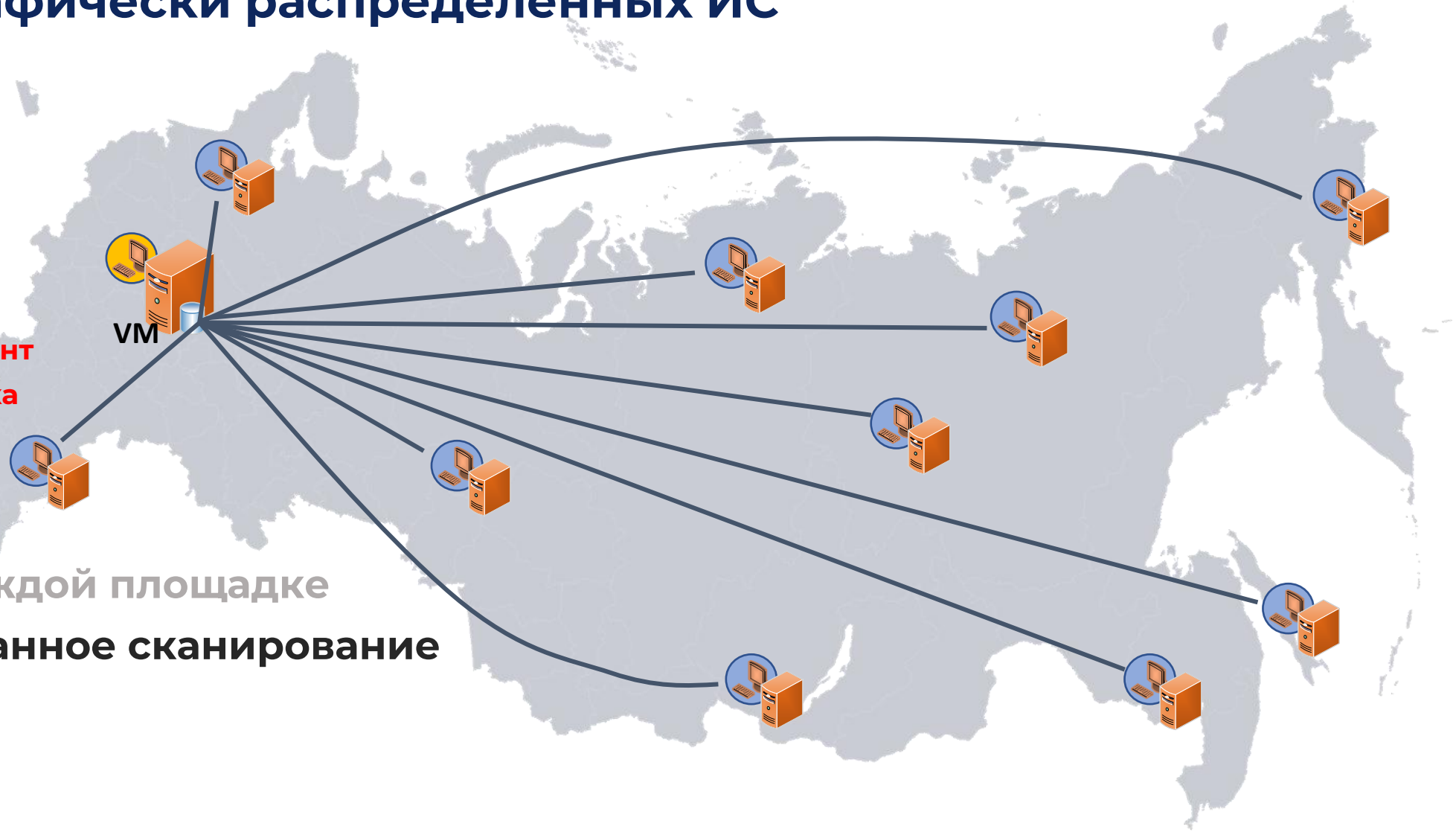
- × Дорого
- × Нет общей картины

1) VM-решение каждой площадке

фродекс

VM для географически распределенных ИС

- × Обслуживание компонент
- × Большой расход трафика



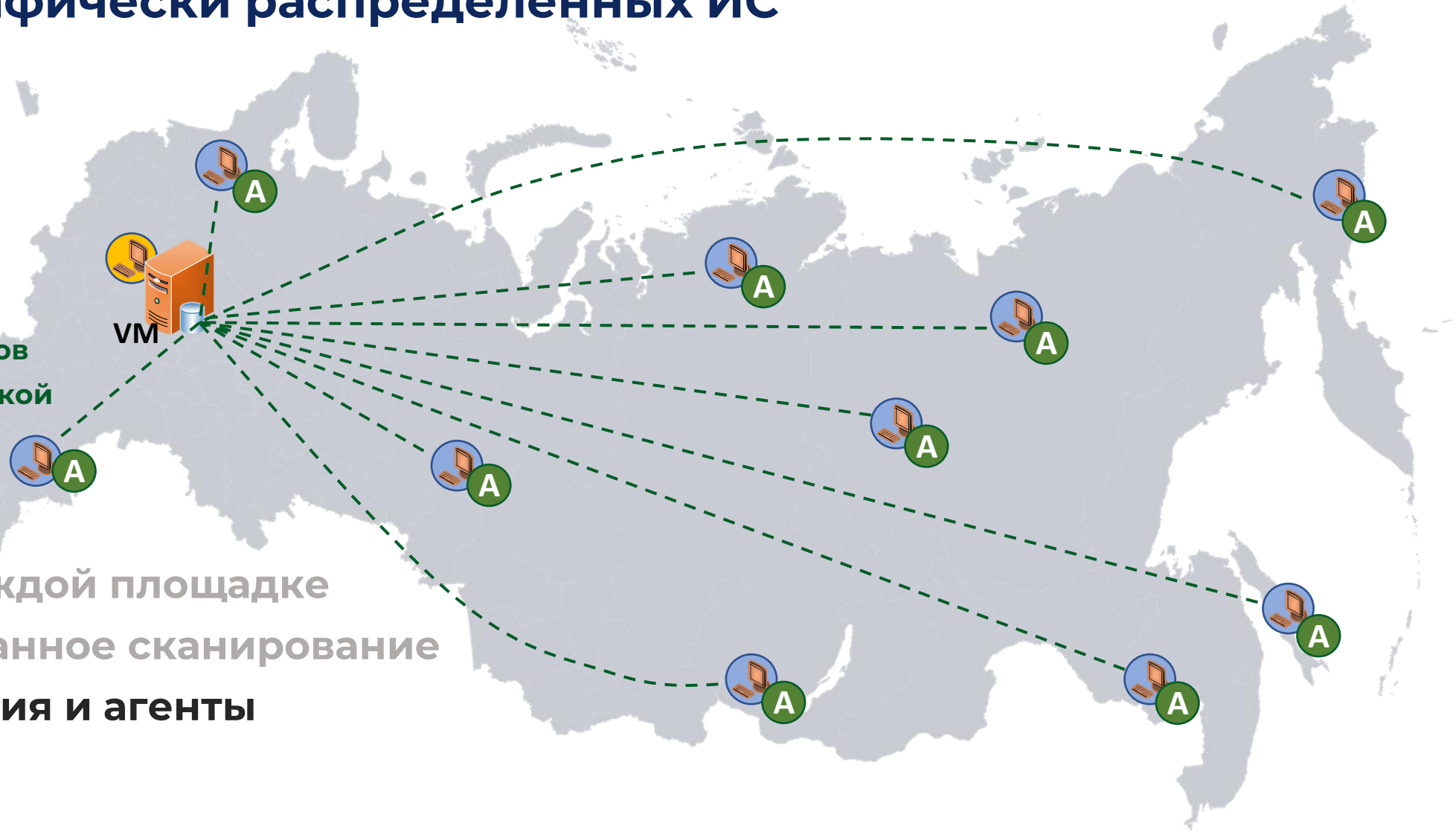
1) VM-решение каждой площадке

2) Децентрализованное сканирование

фродекс

VM для географически распределенных ИС

- ✓ Единая точка результатов
- ✓ Нет проблем с поддержкой
- ✓ Экономия трафика



1) VM-решение каждой площадке

2) Децентрализованное сканирование

3) Центр управления и агенты

фродекс

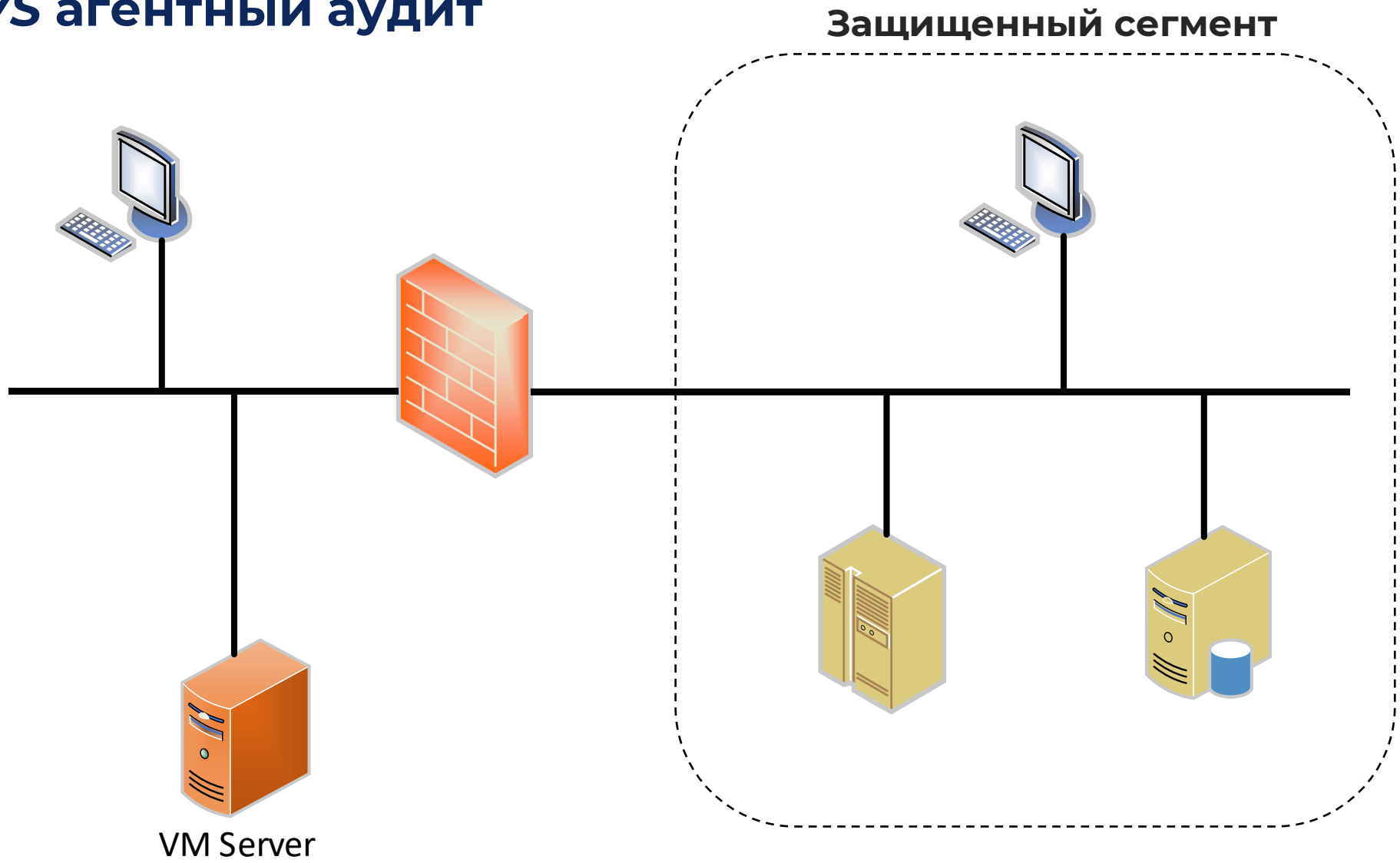
VM для географически распределенных ИС

- ✓ Создано для распределенных ИС
- ✓ Оптимизация затрат (OpEx)
- ✓ Всегда обновлено
- × Доверие к облаку
- × SLA < 100%
- × Не развито в РФ

1) VM-решение каждой площадке
2) Децентрализованное сканирование
3) Центр управления и агенты
4) **Облачное решение (VMaaS)**

фродекс

Безагентный *VS* агентный аудит

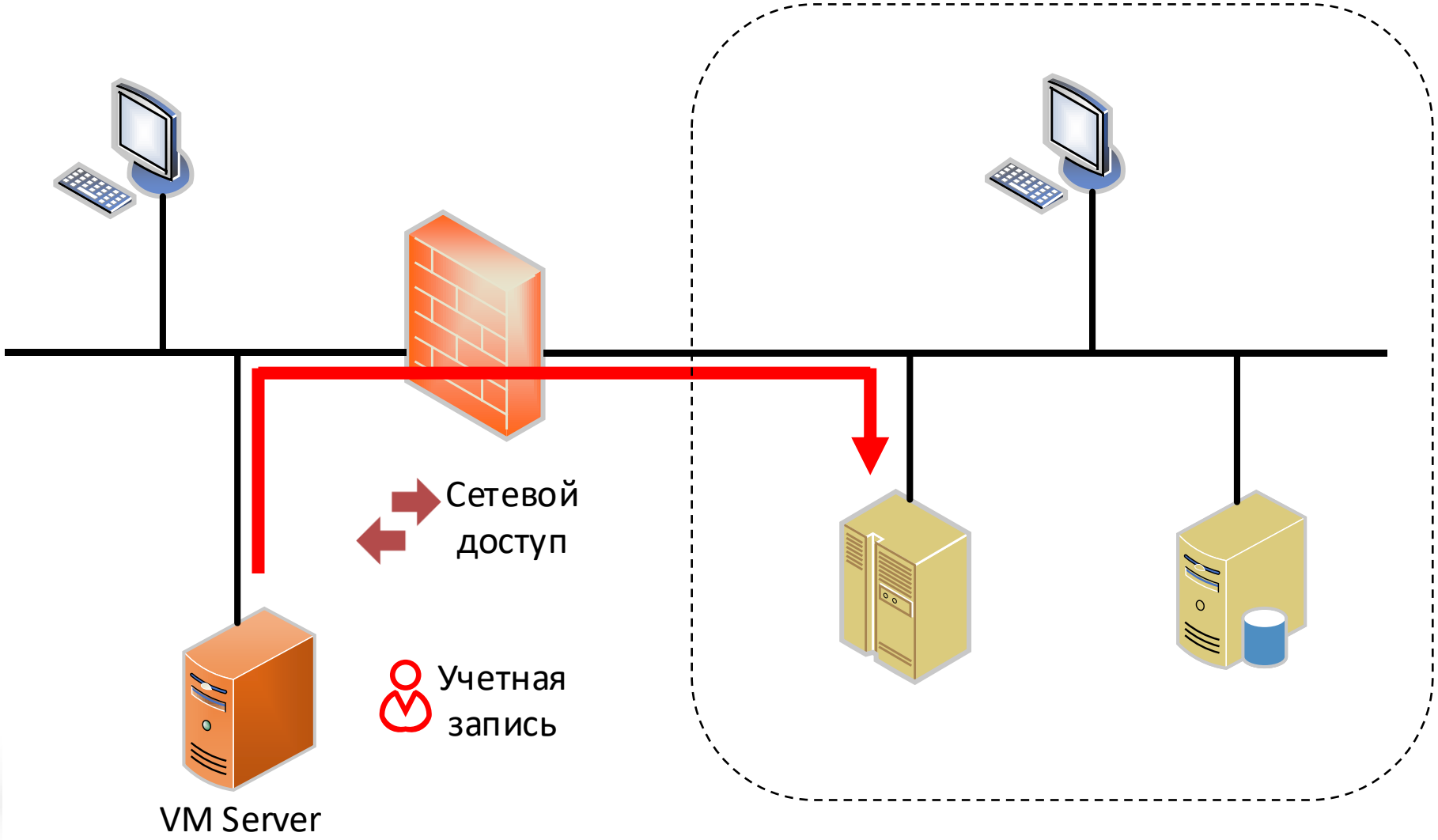


фродекс

Безагентный *VS* агентный аудит

ТЕПЕРЬ НЕЗащищенный сегмент

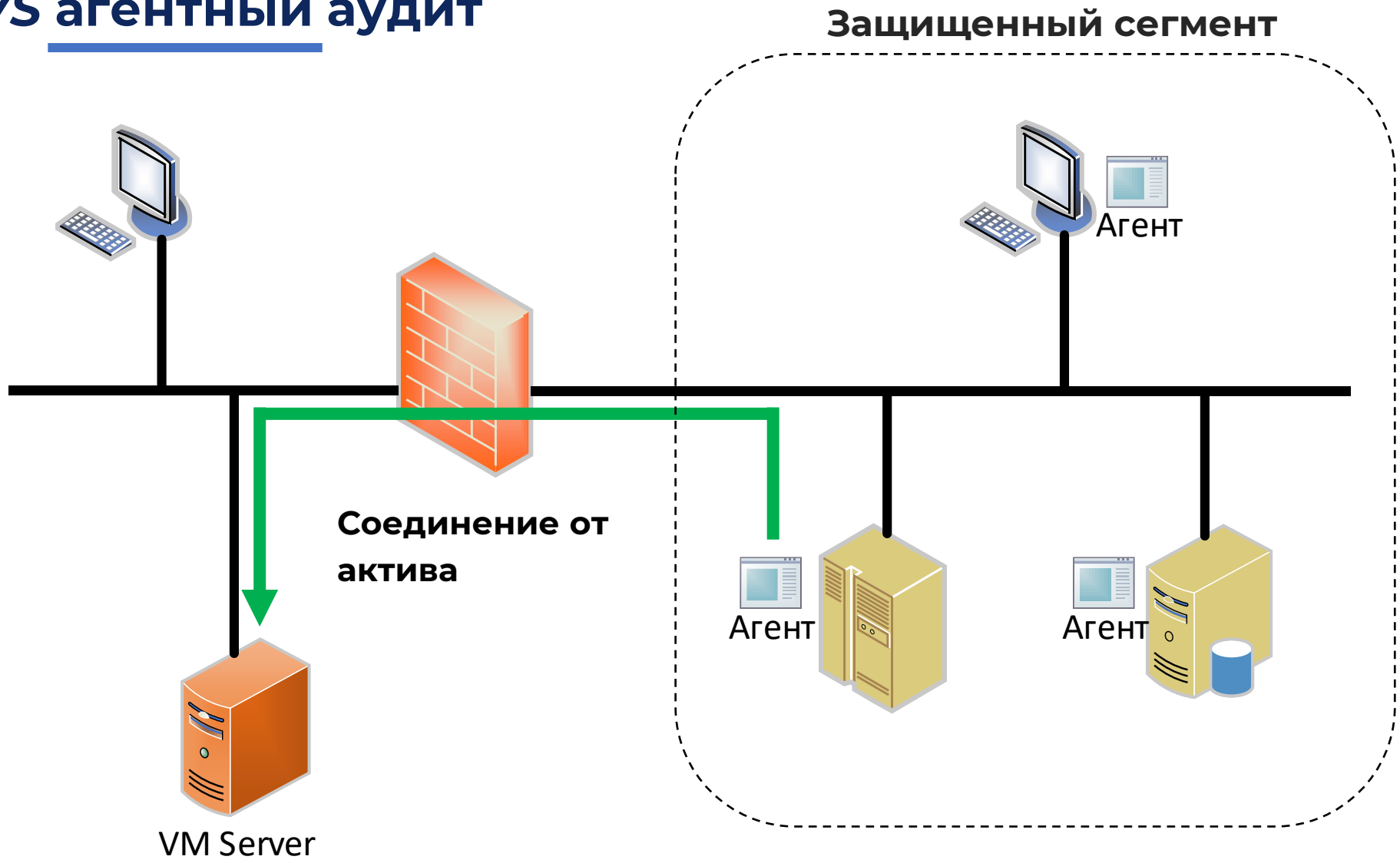
Сегмент все еще защищен?



фродекс

Безагентный *VS* агентный аудит

Сегмент все еще защищен



фродекс

Особенности национального VM

- **Импортозамещение – надеемся только на себя**
  Переход на российское ПО требует использования российских VM систем

- **Данные об уязвимостях – усиливаем связь с вендорами**
  Необходимо развитие процесса публикации данных об уязвимостях российского ПО

- **Приоритизация – используем национальную методику**
  Методика приоритизации должна учитывать статистику атак на российский IT-сегмент

- **Изолированные ИС – обновляемся без доступа к Интернету**
  Важно обеспечить процесс обновления VM-системы даже для изолированной ИС

- **Географически распределенные ИС – развиваем облачные VM-сервисы**
  VM-решения должны учитывать особенности работы распределенных ИС

Андрей Никонов

Старший инженер-программист

a.nikonov@frodex.ru

+7(495) 967 65 19

frodex.ru

Техническая поддержка:
support@frodex.ru

офис
г.Уфа, ул. Пархоменко, 133/1, 2 этаж