

Почему заказчики
выбирают VDI?!



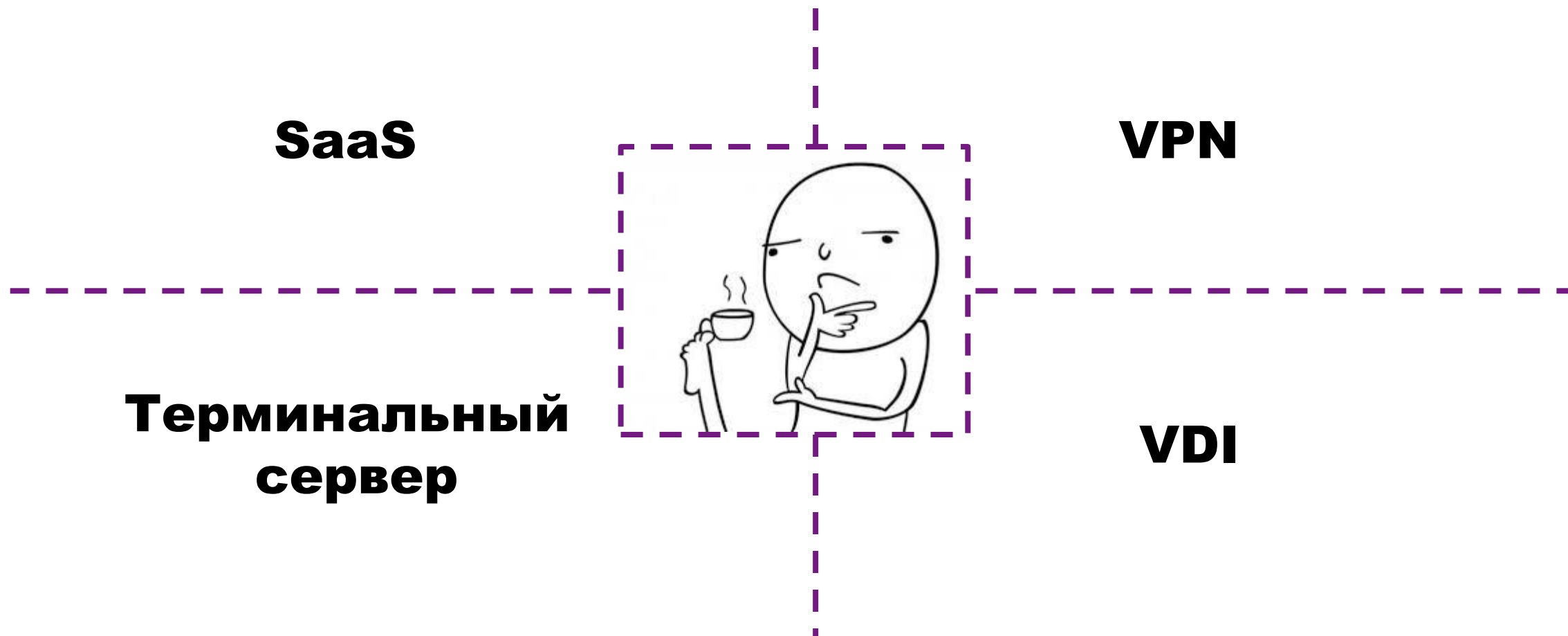
Погоржельский Станислав Игоревич

Какие задачи решаем?



- **Как пользователю получить доступ к рабочему месту**
- **Как обеспечить сохранность корпоративных данных**
- **Как гарантировать доступность корпоративных систем**
- **Инструментарий**

Какой вариант использования для удаленного доступа?



Какой вариант использования для удаленного доступа?

SaaS

Имеет ограниченный функционал
Данные находятся у провайдера услуги
Имеет оптимальную стоимость
Вопросы ИБ – на стороне провайдера

Функционал определяет Заказчик
Данные контролируются Заказчиком
Относительно дешёво в организации
Вопросы ИБ на стороне ИТ Заказчика

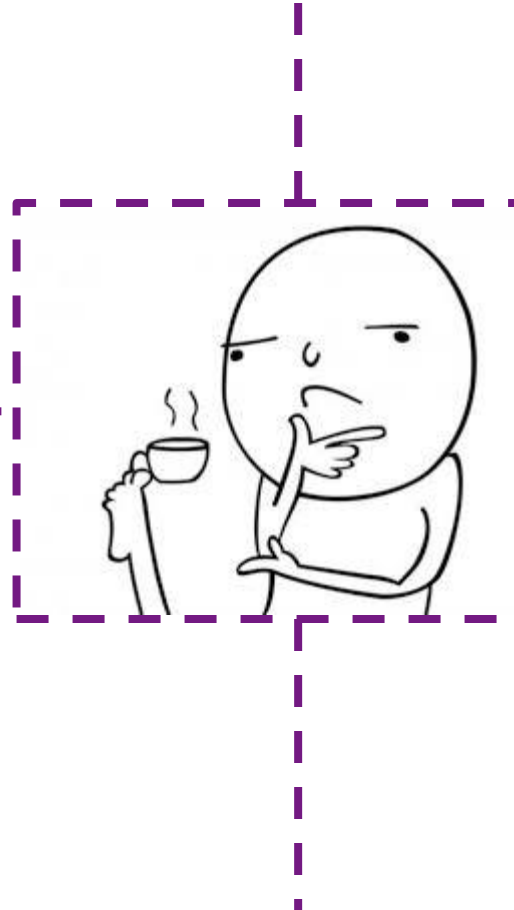
Терминальный сервер

VPN

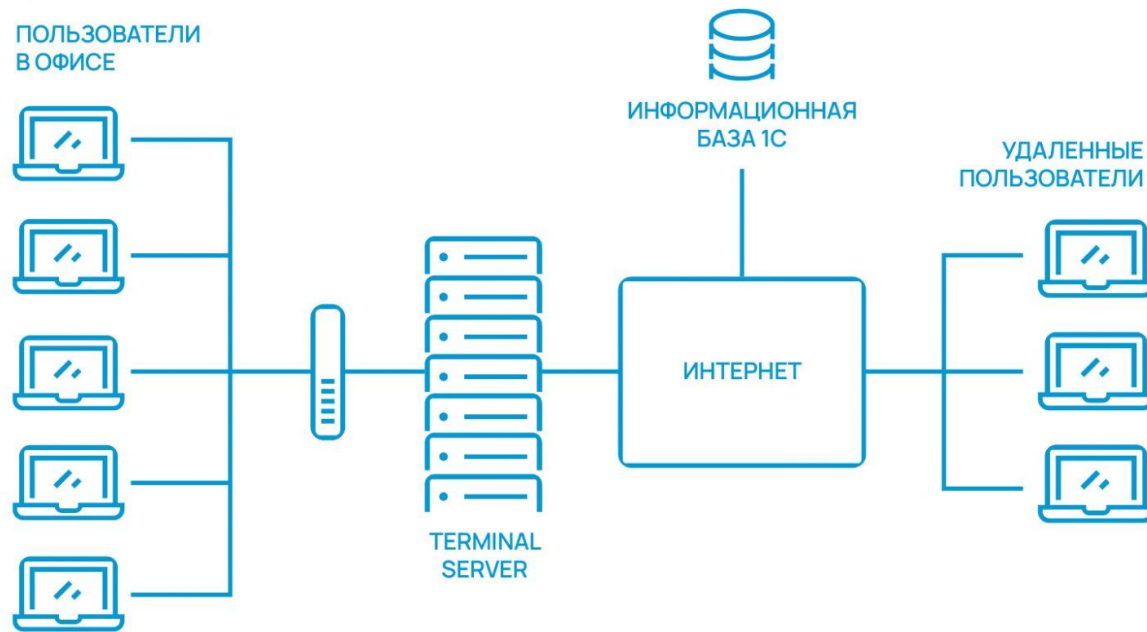
Данные контролируются Пользователем
Дешёво в организации
Вопросы ИБ на стороне ИТ Заказчика и пользователя

Функционал определяет Заказчик
Данные контролируются Заказчиком
Недешёво в организации
Вопросы ИБ на стороне ИТ Заказчика

VDI



Виртуализация рабочих столов приводит к инновационному изменению ИТ-инфраструктуры!



- **Рабочее место** может рассматриваться как услуга согласно концепции Desktop as a Service (DAAS) – рабочее место как сервис
- **Ориентация на потребителя** – возможность использования большого кол-ва клиентских устройств
- **Централизованное управление рабочими столами**, сокращение времени развертывания новых приложений и обновления старых

Обслуживание удалённых рабочих мест

Особенности удалённых АРМ:



- Централизация и унификация рабочих мест.
- Управление/изменение АРМ, только через специалиста ИТ
- Снижение требования к офисным ИТ специалистам
- Позволяет задействовать меньшее количество Системных администратор, на решения задач с АРМ
- Отсутствие географической привязки к АРМ и его обслуживания
- Резервирование данных. АРМ пользователя, легко резервировать, обеспечить бекап данных
- Нагрузочные профили АРМ
- Можно применить решения программно определяемых дата центров

Сервер терминальных подключений

Терминальный сервер

Плюсы

- Привычный для пользователей интерфейс
- Централизованная установка и администрирование ПО
- Экономия на покупке и содержании пользовательских устройств
- Ресурсы и кол-во рабочих столов можно оперативно масштабировать.
- VPN для безопасного подключения



Windows Server®

Минусы

- Ограничения по производительности
- Ресурсы разделены между пользователями
- Не получится развернуть рабочие места для дизайнеров, проектировщиков и пр.
- Не все ПО работает через терминальный сервер.

Протокол для терминального сервера?



Для каких задач:

- Для пользователей с однотипными задачами
- Пользователи которые работают с Word, Excel, Почта, бухгалтерское ПО

Основные возможности протокола:

- Шифрование
- Функции уменьшения полосы пропускания
- Использование буфера обмена
- Удаленное управление

VDI

Виртуальное рабочее место

Виртуализации рабочих мест (VDI)



Настольные персональные компьютеры пользователей размещаются в виртуальных машинах или виртуальных рабочих местах (ВРМ)

Организационную же часть решения – управление правами, соединениями пользователей, развертывание виртуальных машин и прочее – реализуют компоненты продукта VMware HORIZON или Citrix

Виртуальные рабочие места (VDI)

Плюсы

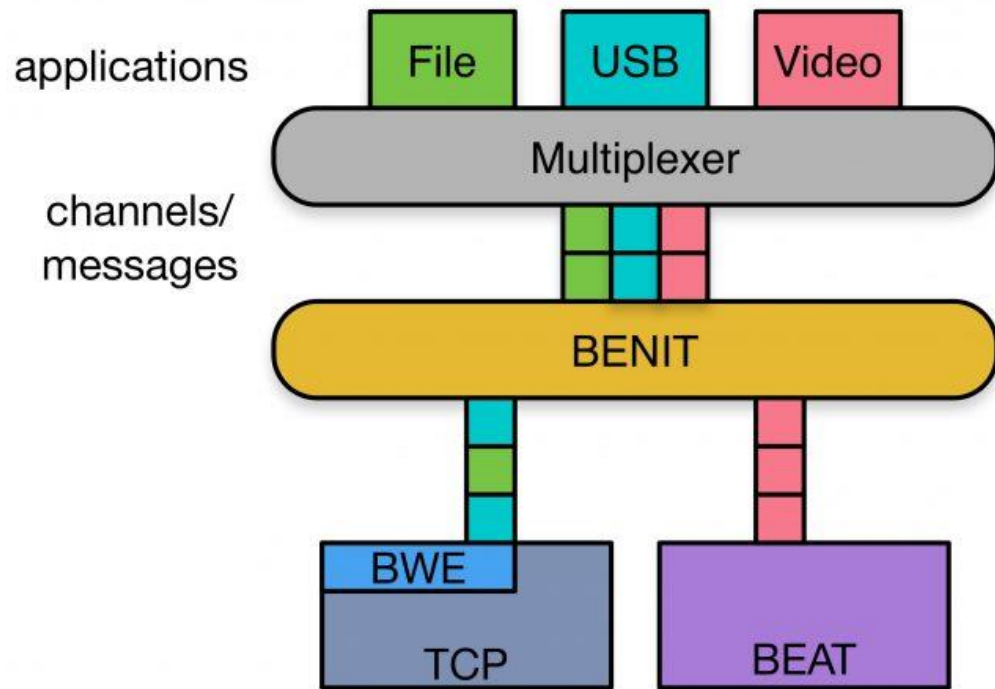
- Безопасность и удобный доступ к корпоративным данным
- Гарантированная производительность и выделенные ресурсы под каждого пользователя
- Возможность проброса пользовательских устройств
- Возможность использования GPU

Минусы

- Дороже чем терминальный сервер (нужно платить за ресурсы и за лицензии)

Протокол для VDI?

- Independent Computing Architecture (ICA)
- Blast Extreme Network Intelligent Transport (BENIT)



*Пример схема работы BLAST протокола

Основные возможности протокола:

- **Надежность** - гарантия последовательной доставки данных в условиях прерывания сетевого соединения / переключения сетевых адаптеров.
- **Переключение транспорта** для отдельного приложения на основе отклика приложения в сети.
- **Балансировка нагрузки** за счет одновременного использования обоих транспортов для различных приложений, а также за счет выбора конкретного транспорта для определенного класса трафика (например, File Copy).

Вопросы ИБ

Информационная безопасность



1. **Обмен данными**, только на уровне приложений. Защита от эксплоита RDS. Пример, CVE-2019-0708 (BlueKeep), связан с работой Remote Desktop Services (RDS) и RDP. Перехват прав администратора, если RDS
2. **Полный контроль** за действиями, конкретного пользователя
3. **Установка доп.ПО**, например, DLP
4. Всегда известно, какой пользователь, что делает и быстро определяется возможная точка взлома
5. Антивирус, не отъедает ресурсов самого АРМ

Выводы

Какие основные задачи решает удалённое рабочее место:

- Сокращение административных ИТ затрат
- Экономия на времени организации рабочего места
- Увеличение срока службы устаревших клиентских устройств
- Централизация данных и реализация средств ИБ

Сервер терминальных подключений

- Для однотипных задач
- Вычислительные ресурсы ОС делят все коллеги
- Экономически выгодно использовать
- Нет возможности использовать индивидуальные средства ИБ
- Через одного пользователя, можно нарушить работу всей компании
- Нельзя использовать GPU
- Только Windows Server



VDI (Виртуальное рабочее место)

- Для разных задач (профили ресурсов)
- Вычислительные ресурсы ОС у каждого пользователя свои
- Дороже в организации и ТП
- Можно использовать индивидуальные средства ИБ (DLP | MDM | НСД)
- Через одного пользователя, нельзя нарушить работу всей компании, а также можно выдать права администратора на ОС
- Можно использовать GPU и Windows 7/10



**Спасибо за
внимание!**

Погоржельский Станислав Игоревич
pogorzhelskij@gmail.com / +7(906)7190883