CA Privileged Access Manager

(CA PAM, ex.Xceedium Xsuite)

Решение контроля
привилегированных пользователей

Структура презентации

- ✓ Портрет Заказчика
- ✓ Что такое CA PAM, из чего состоит?
- ✓ Ключевые потребности клиента
- ✓ Ключевые блоки функционала CA PAM
- ✓ Стратегия и тактика, преимущества
- ✓ Структура лицензирования решения
- ✓ Ценность для ИТ и ИБ

Портрет Заказчика

- Профиль деятельности не принципиален (стандартная TCP-сеть)
- Компания использует сторонние людские ресурсы
- Компания желает контролировать деятельность привилегированных пользователей (вн., внешн.). Видеть, контролировать, блокировать.
- Есть потребность управления паролями привилегированных пользователей (для них и конечных приложений).
- Желательно: пул ресурсов Заказчика – в едином управляемом пространстве (ЦОД, единая серверная и т.п.).

Где уже есть?

- Телекоммуникационная компания Top-5, Россия (РФ)
- Две крупные российские компании банковского сектора Top-20 (РФ)
- Представительство автомобильного производителя Top-10
- Одна из крупных международных экономических комиссий
- Энергетика (РФ)
- Производитель продуктов из списка Fortune 200
- Онлайн брокер из списка Top 3
- Фармацевтическая сеть из списка Top 3 (Food and Drug Retailer)

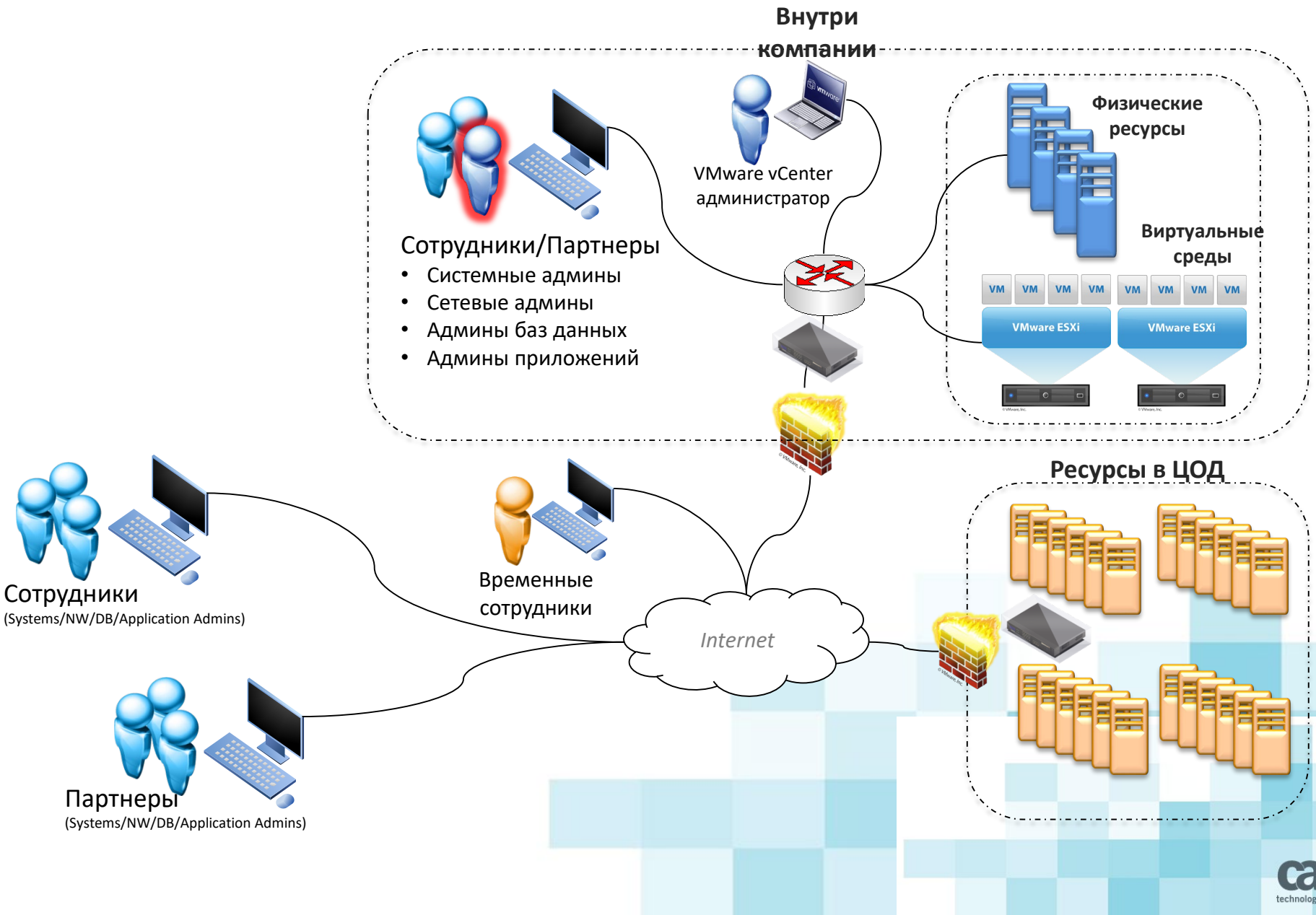
Операторы сотовой связи

Компании на IT-аутсорсинге

Финансовый сектор

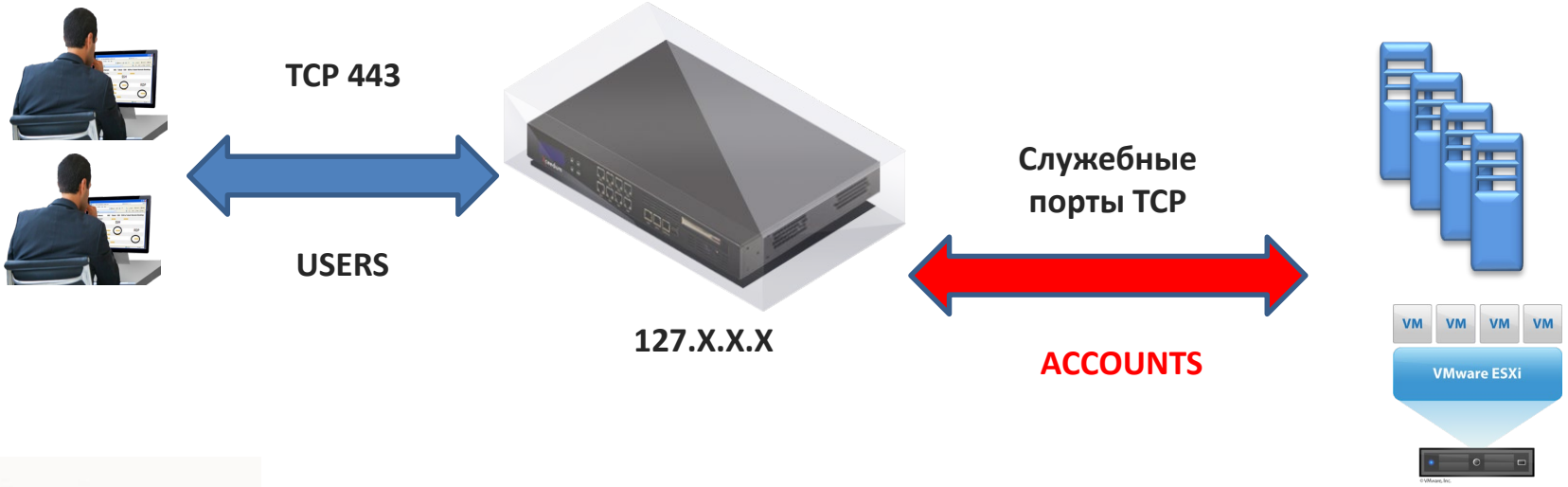
Автомобилестроение

Что такое CA PAM (Xceedium)?



Что такое CA PAM (Xceedium)?

- Учетные записи пользователей в системе (локальные, AD LDAP(s), Open LDAP, RADIUS, TACACS+, LDAP) – ПОЛЬЗОВАТЕЛИ (ПП)
- Учетные записи для подключения к конечным устройствам – УЧЕТНЫЕ ДАННЫЕ
- Отношение МНОГИЕ К НЕСКОЛЬКИМ, МНОГИЕ К ОДНОМУ



Из чего состоит решение?

Модуль контроля доступа (Access Control)

- Запись сессий (графика, текст)
- Контроль вводимых команд (фильтры ввода)
- Контроль переходов за пределы назначенных устройств (leapfrogging)
- Действия в связи с нарушениями (оповещения, блокировки)

Модуль управления паролями (Password Management)

- Хранение, обновление и генерация новых паролей для служебных УЗ (те, которые в конечной системе)
- Политики работы с паролями служебных УЗ (просмотр, разрешения, подтверждения)
- Важное преимущество – в системе CA PAM это уже встроено

Модуль управления паролями в приложениях (Application to Application)

- Удаление логинов паролей из файлов «самописных» приложений
- Хранение и обновление УЗ через CA PAM

Ключевые блоки функционала (Password Management)

Типовые задачи

- ПП не должны знать учетные данные на конечные системы:
- Надежное хранение учетных данных (логинов, паролей, ключей, сертификатов) в системе;
- Защита шифрованием (математическим преобразованием);
- Применение учетных данных системой «прозрачно» для ПП.

- Заказчик должен управлять ЖЦ паролей учетных данных (везде):
- Политики составления паролей – синхронизация с конечными системами;
- Смена паролей из PAM на конечных системах;
- Управление ПРОСМОТРОМ паролей (сложная логика)

Ключевые потребности клиента (актуальные проблемы)

- **Права в конечных системах изначально зачастую шире, чем нужно по процедуре самому Заказчику**
- **Привилегированные пользователи есть локальные и удаленные – разные ограничения**
- **Информационные системы сопряжены между собой множеством связей (других систем, учетными данными, коннекторами), что порождает смежные права**
- **Простой пример – учетная запись в Microsoft Active Directory**
- **Образуется излишек учетных данных (в каждой конечной системе)**
- **Доверяем, но проверяем…**

Структура лицензирования CA PAM

- Модуль Access Control – по числу серверов (устройств), к которым обращаются ПП
- Начальное число – 30 или более

- Модуль Password Management – по числу серверов (устройств), к которым обращаются ПП

- Модуль Application to Application – по числу серверов, на которых работают приложения

Спасибо Вам!