Oberig it

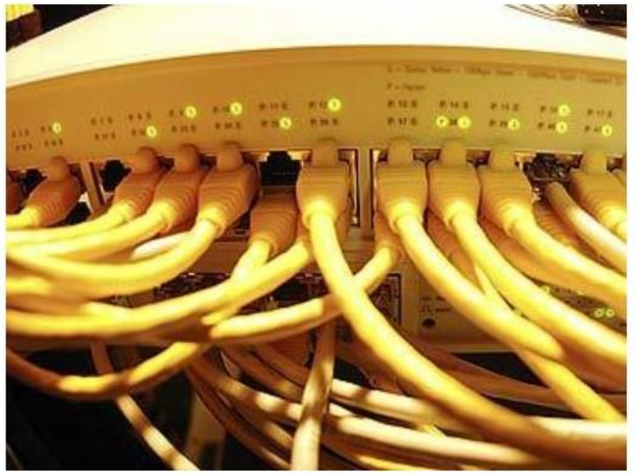
Distribution of Innovations

# Привилегированные пользователи: поиск истинных чувств и проверка их на прочность

# Проблематика. Инциденты и их последствия

## Американский сисадмин получил рекордный срок за компьютерный саботаж

Добавить в «Мою Ленту»



Американский системный администратор приговорен к 30 месяцам
умышленное нанесение ущерба серверам компании Medco, передае
самый большой срок в истории США за подобное преступление.

Юнг Сун Лин (Yung-Hsun Lin) признался, что изменил программы и
"логическую бомбу", которая должна была сработать в октябре 2003
уничтожить данные на серверах компании. Примерно в то же врем

## Обиженный на низкую зарплату админ уничтожил базу данных компании

Анатолий Ализар , 19.05.2008 16 сек на чтение 0 0 115

Уволенный сисадмин остановил производство ковбойских сапогов, существующее с 1883 г.

# КТО ТАКОЙ ПРИВИЛЕГИРОВАННЫЙ ПОЛЬЗОВАТЕЛЬ?

Все привилегированные пользователи имеют доступ к критически важным ресурсам компании!

- Администратор;
- Внутренний сотрудник;
- Внешний подрядчик.

FUDO SECURITY

Oberig it

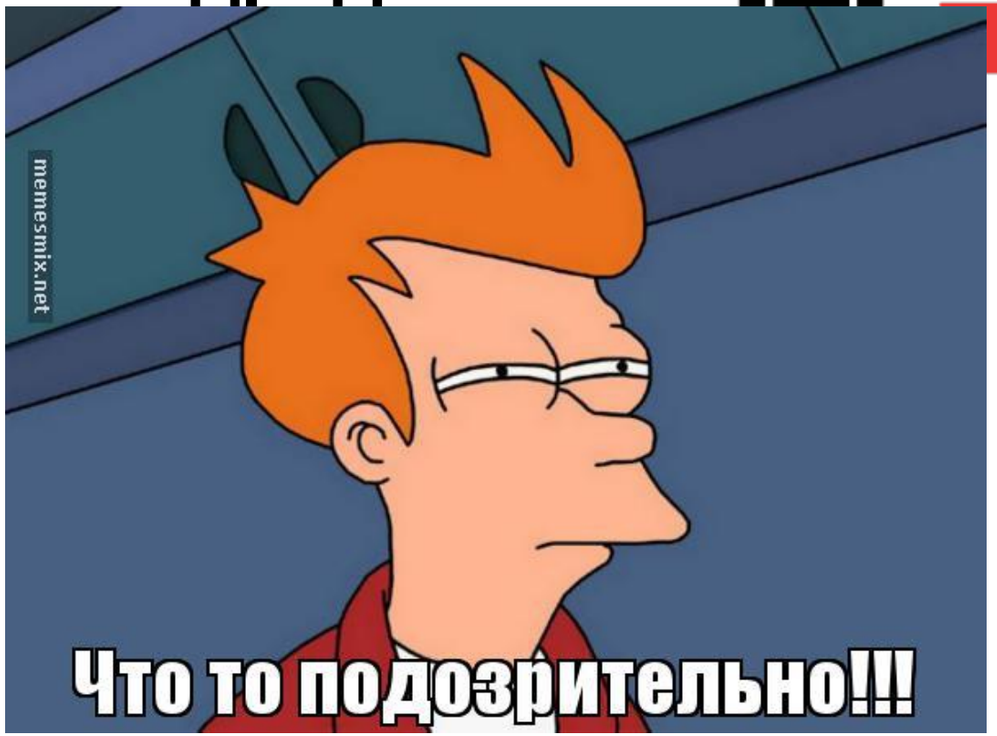
# ОН НЕ БЫЛ ХАКЕРОМ

FUDO SECURITY

Oberig it

# Проблематика

## 1. Ошибки в работе удаленных администраторов, тех. поддержки, аудиторов, внешних подрядчиков

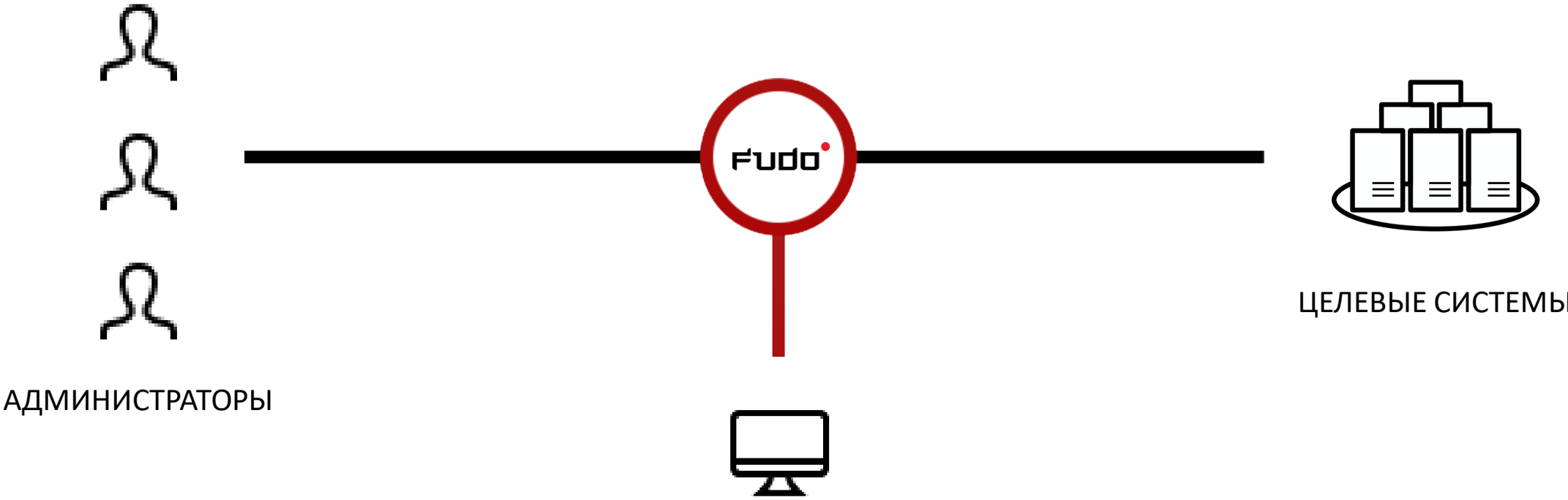



**Невозможность доказать вину конкретного пользователя из-за недостаточности улик.**

**Логи не дадут полной картины действий пользователя и не всегда могут быть использованы как улика**

**Решение** – система записывает все действия пользователя (включая ввод/вывод команд и переданные файлы)

# РЕШЕНИЕ - как это работает с FUDO PAM




АДМИНИСТРАТОРЫ

ЦЕЛЕВЫЕ СИСТЕМЫ

SECURITY MANAGER

(управление привилегированной архитектурой,
в том числе пользователями, учетными записями и удаленными сессиями)

FUDO SECURITY

Oberig it

# Fudo PAM
## поддержка протоколов и соответствие стандартам

## ПРОТОКОЛЫ:

- SSH
- Telnet
- TN 3270
- RDP
- VNC
- X11
- RemoteApp
- Oracle
- MySQL
- TDS for MS SQL
- Modbus Scada
- HTTP/HTTPS

## COMPLAINCE

- PCI DSS v3.2 (since April 2017) – MFA for all CDE
- NIS Directive (2016-2018)
- GDPR Directive (2016-2018)
- ISO 27000

FUDO SECURITY

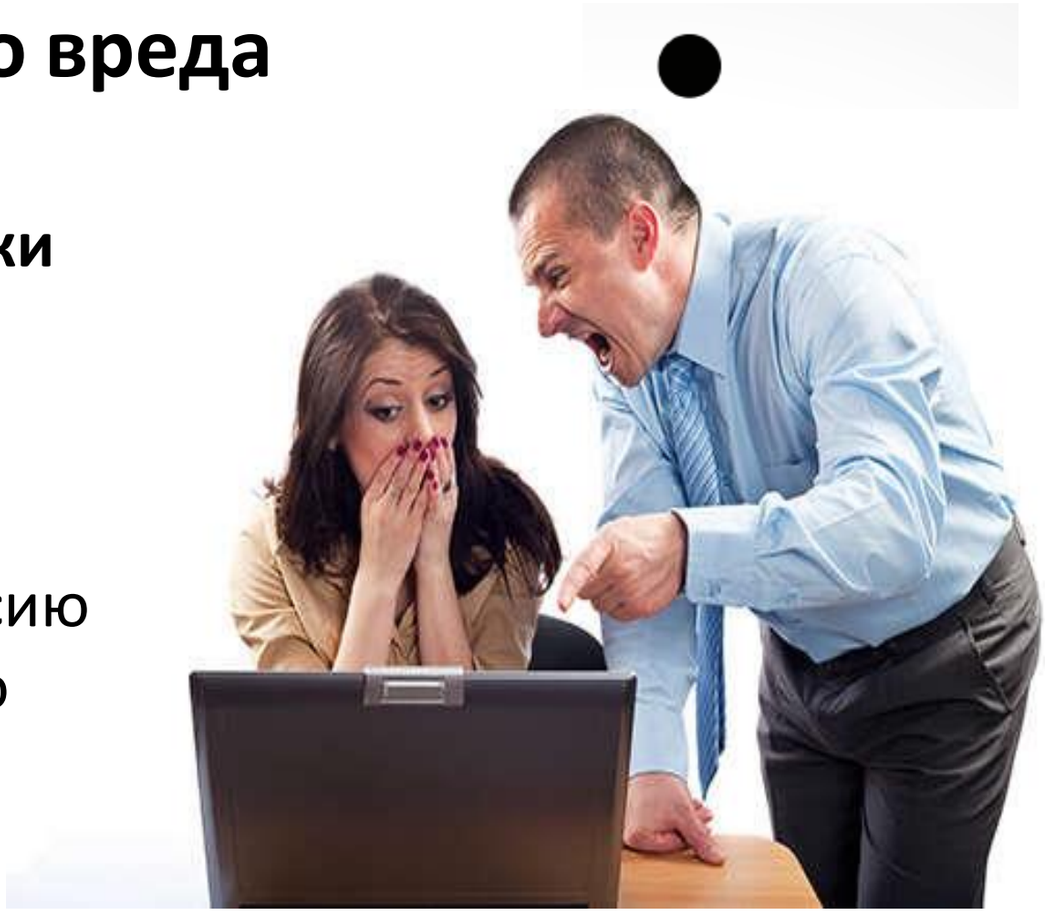
Oberig it

# 2. Контроль непредумышленного вреда

**Нет возможности ПРЕДОТВРАТИТЬ ошибки**

**Время на выявление ошибок со стороны внешних администраторов.**

**Решение** – система может прерывать сессию и/или блокировать пользователя согласно политике.
Дает возможность не только смотреть на удаленную сессию, но и использовать режим совместной работы.



# PRIVILEGED SESSION MANAGER

## Управление сессиями и мониторинг


FUDO SECURITY

Oberig it

# Проблематика

## 3. Совместное использование «обезличенных /системных» учетных записей.


**Невозможность определить кто вносил изменения.**

**Сложность в управлении доступом к удаленным ресурсам.**

**Возможность случайной блокировки доступа для всех пользователей.**

**Решение** – Каждый пользователь использует свой логин и пароль для входа.
Возможность подставлять необходимые учетные данные для входа на контролируемое устройство.
Детальный отчет по каждому соединению.

# ВОЗМОЖНОСТИ АУТЕНТИФИКАЦИИ


## ВХОД С ОРИГИНАЛЬНЫМИ ДАННЫМ

- Логин и пароль пользователя такие же, как и на конечную систему


## ПОДМЕНА ВСЕХ РЕКВИЗИТОВ

- Пользователь входит с учетными данными FUDO, при этом учетные данные задаются политиками системы


## ПОДМЕНА ПАРОЛЯ

- Транслируется логин, пароль – уникальный, политика смены пароля задается политиками

FUDO SECURITY

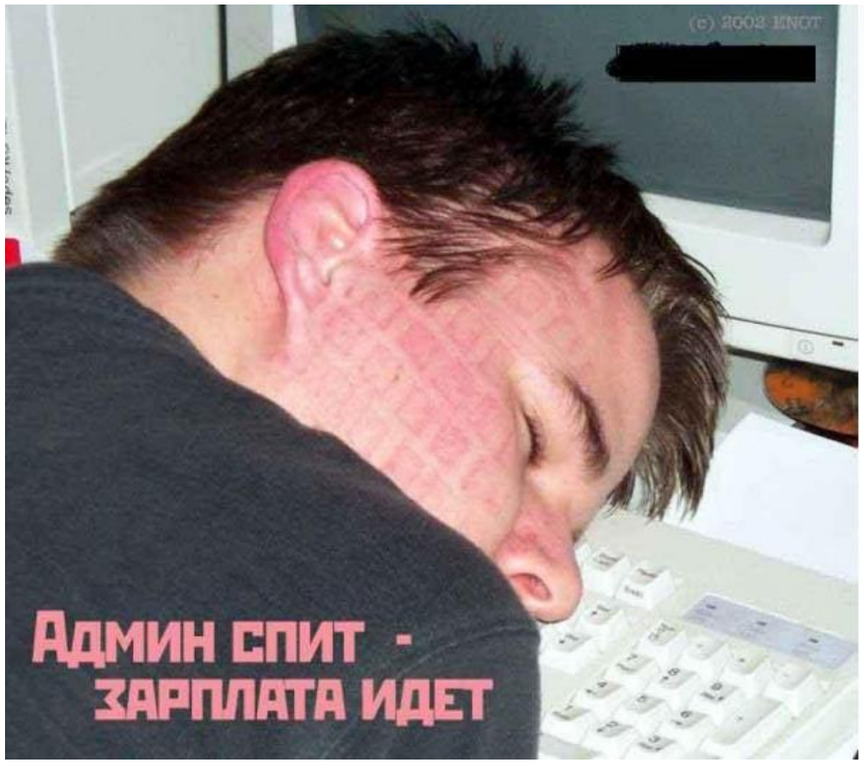
Oberig it

# Проблематика

## 4. Контроль выполнения SLA.

**Отсутствие возможности проверить время реально потраченное на оказание услуги.**

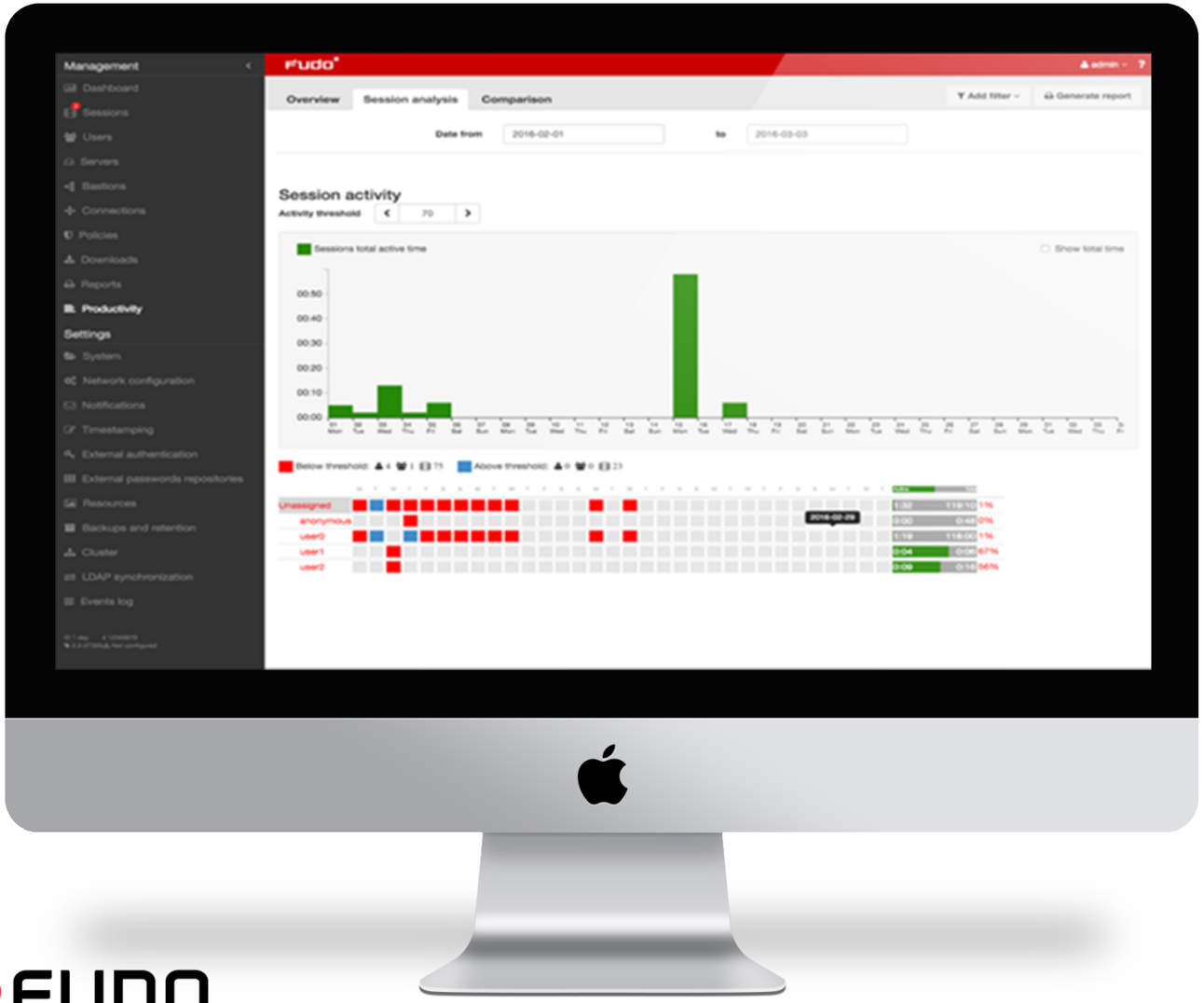
**Дороговизна и не обязательная эффективность оказываемых услуг.**




**Решение** – система записывает все действия пользователя с возможностью дальнейшего воспроизведения видео.
Позволяет подтвердить конечное время затраченное на работу.

# EFFICIENCY ANALYZER

## Анализ продуктивности




- Видимость активности пользователей
- Видимость активности организации
- Сравнение продуктивности пользователей
- Построение удобных отчетов

FUDO SECURITY

Oberig it

# FUDO PAM КОМПОНЕНТЫ

**SECRET MANAGER**

**PRIVILEGED SESSION MANAGER**

**EFFICIENCY ANALYZER**

**APPLICATION TO APPLICATION PASSWORD MANAGER**

Xen Project

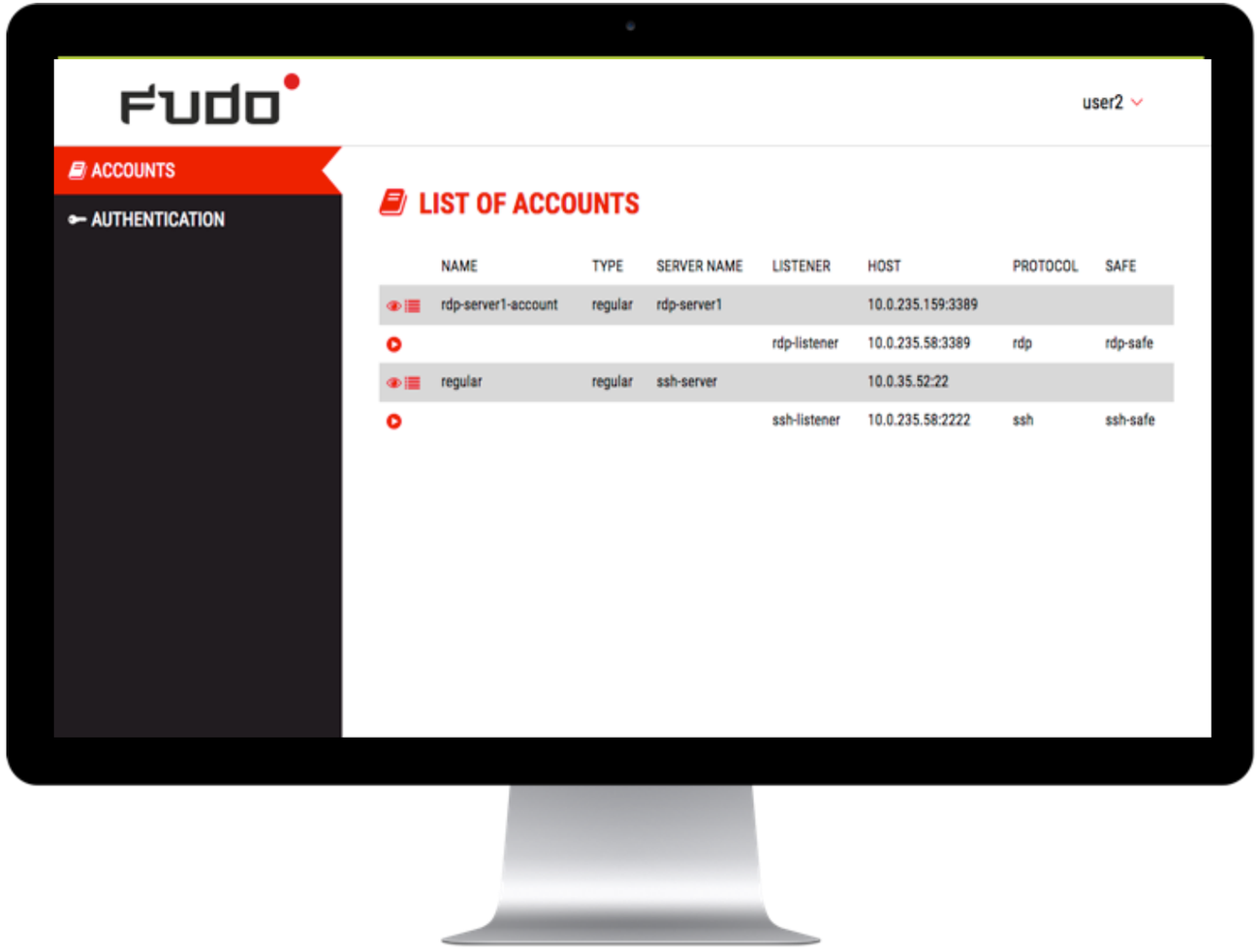
vmware

VirtualBox

FUDO SECURITY

Oberig it

# USER PORTAL – веб-портал для привилегированного пользователя

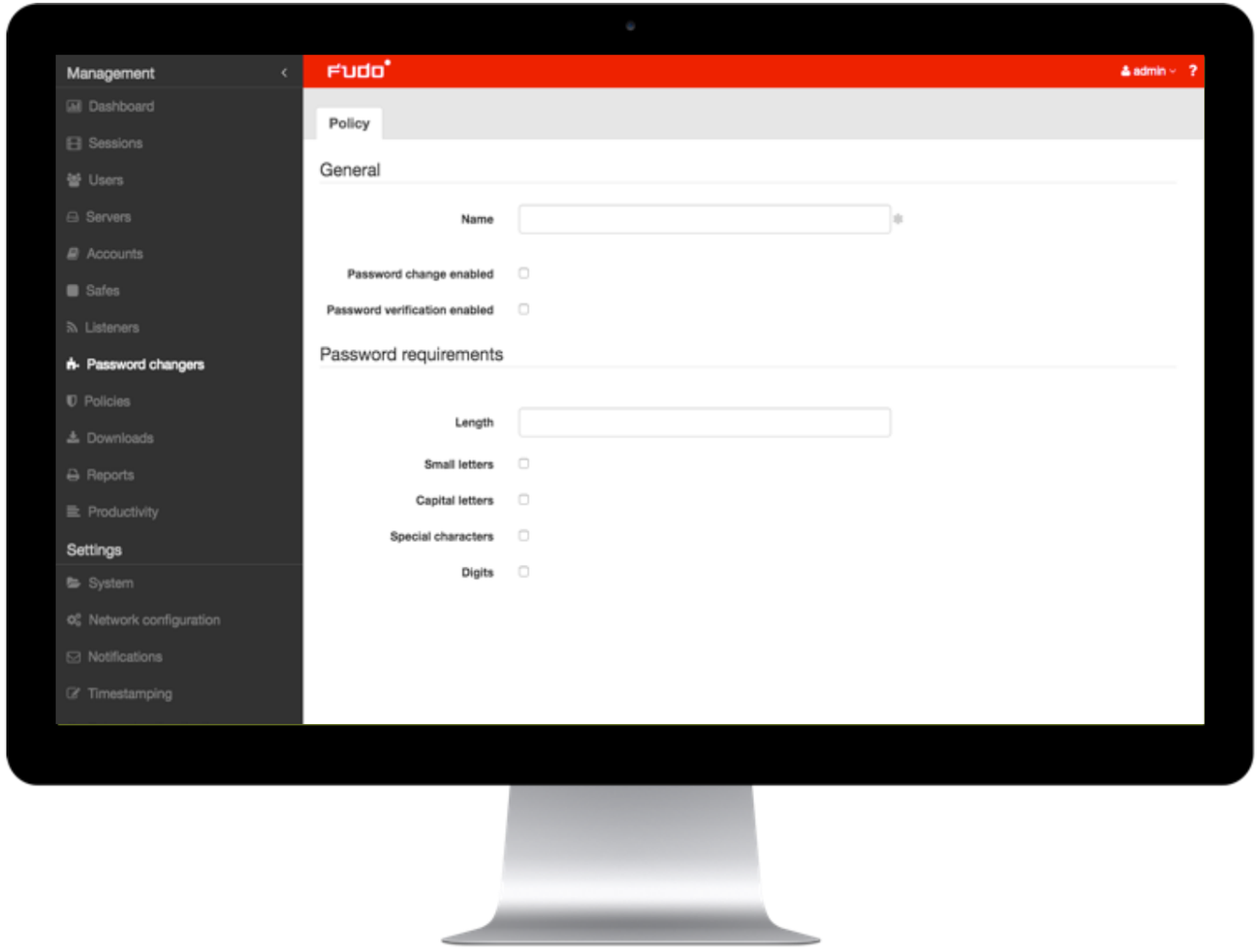



- Список доступных учетных записей для пользователя
- Подключение к серверу нажатием одной кнопки
- Просмотр текущего пароля и историю паролей

FUDO SECURITY

Oberig it

# Политики смены паролей на целевых системах




- Частота смены паролей
- Требования к надежности пароля
- История паролей позволяет восстановить пароль в случае стихийного бедствия или в целях восстановления
- Поддержка платформ: Unix, Windows, MySQL, CISCO
- Пользовательские смены паролей для нестандартных систем

FUDO SECURITY

Oberig it

# РАЗЛИЧНЫЕ РЕЖИМЫ РАБОТЫ с целевыми системами

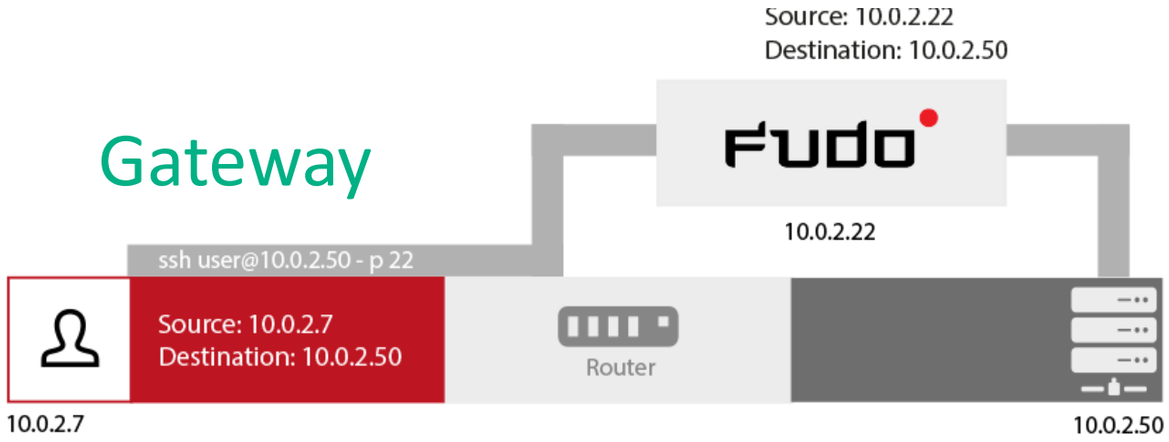
## Transparent


## Proxy

| Servers |
| --- |
| 10.0.2.20:50 > 10.0.2.50:22 |
| 10.0.2.20.51 > 10.0.2.51:22 |


| Allow |
| --- |
| 10.0.2.20 |
| Deny |
| all_other |

## Gateway

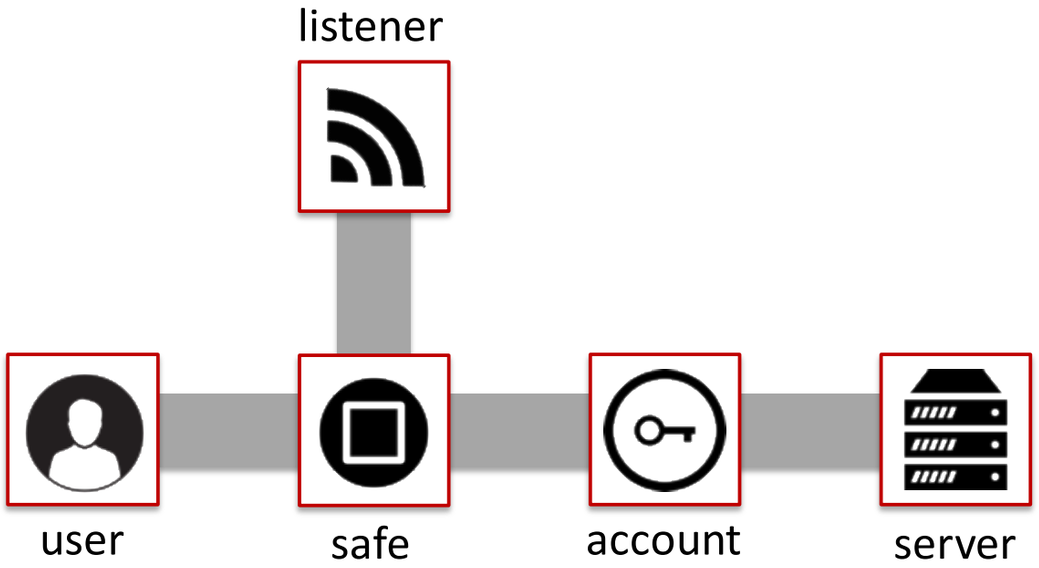



## Bastion


FUDO SECURITY

Oberig it

# ТИПЫ БАЗОВЫХ ОБЪЕКТОВ




- **USER** – субъект, которому можно подключаться к целевым серверам. Субъекту задаются основные параметры подключения (логин, пароль и его политики, реквизиты, роль)
- **SERVER** – целевой объект (сервер), к которому подключается привилегированные пользователи (IP,  порт, протокол).

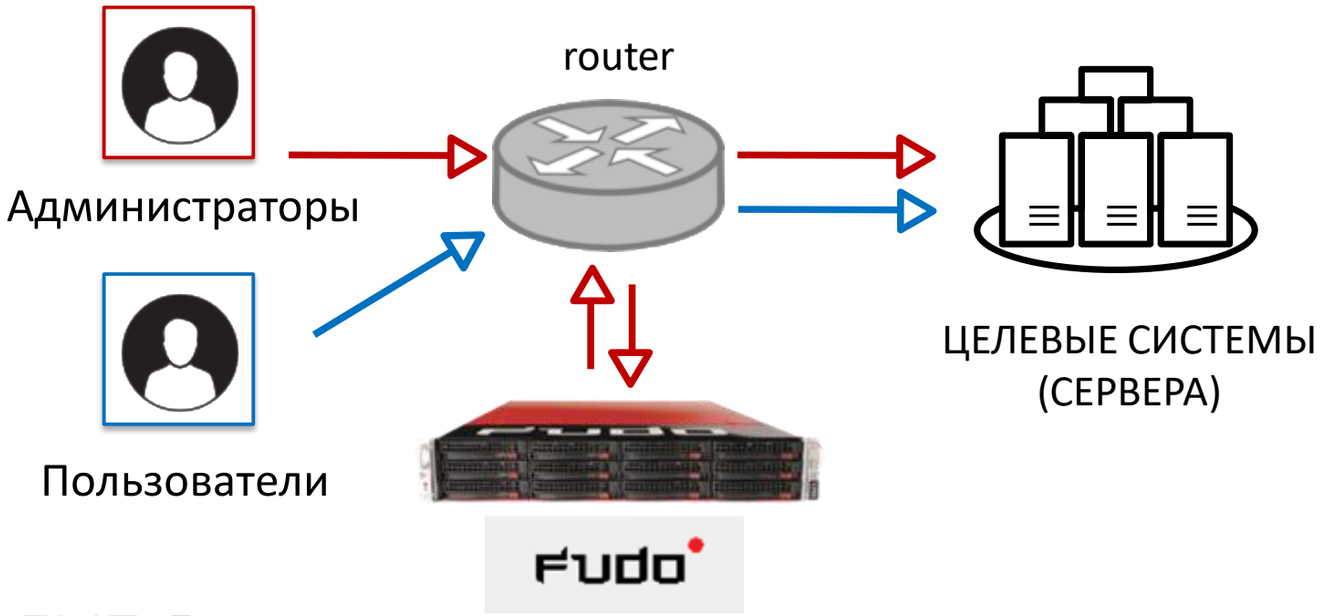
- **LISTENER** – данные компонент определяет режим подключения к серверу (прозрачный, шлюз, прокси, бастион) и другие особенности подключения.
- **ACCOUNT** – раздел, в котором задаются параметры доступа привилегированным пользователям к целевому серверу (учетные данные для входа, режим аутентификации и т.п.) и политика смены паролей к целевым системам.
- **SAFE** – раздел в FUDO, который определяет параметры доступа к серверам (какие протоколы, права, политики доступа и т.п.).

Oberig it

# ВАРИАНТЫ РАЗВЕРТЫВАНИЯ В СЕТИ


## BRIDGE

- Ставиться в разрыв сети
- Прозрачная IP-адресация
- Минимум 2 порта
- Не надо менять настройки сети в компании



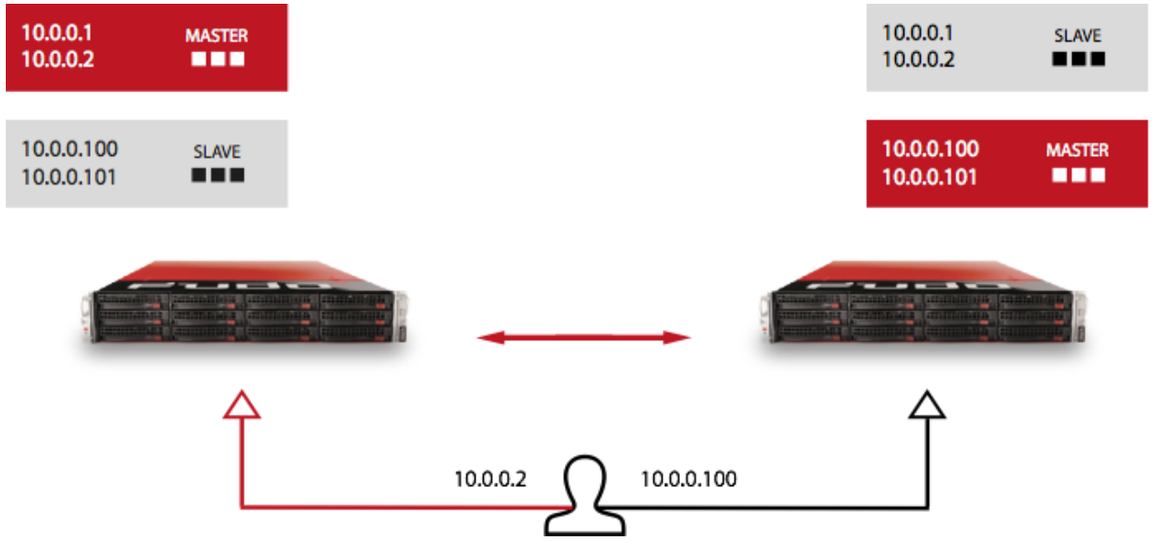

## ПРИНУДИТЕЛЬНАЯ МАРШРУТИЗАЦИЯ

- Требуется настройка на роутере (3 Layer)
- Разделение маршрутизации (привилегированные пользователи - на FUDO, обычные пользователи – напрямую)
- Не требуется изменений в топологии сети

FUDO SECURITY

Oberig it

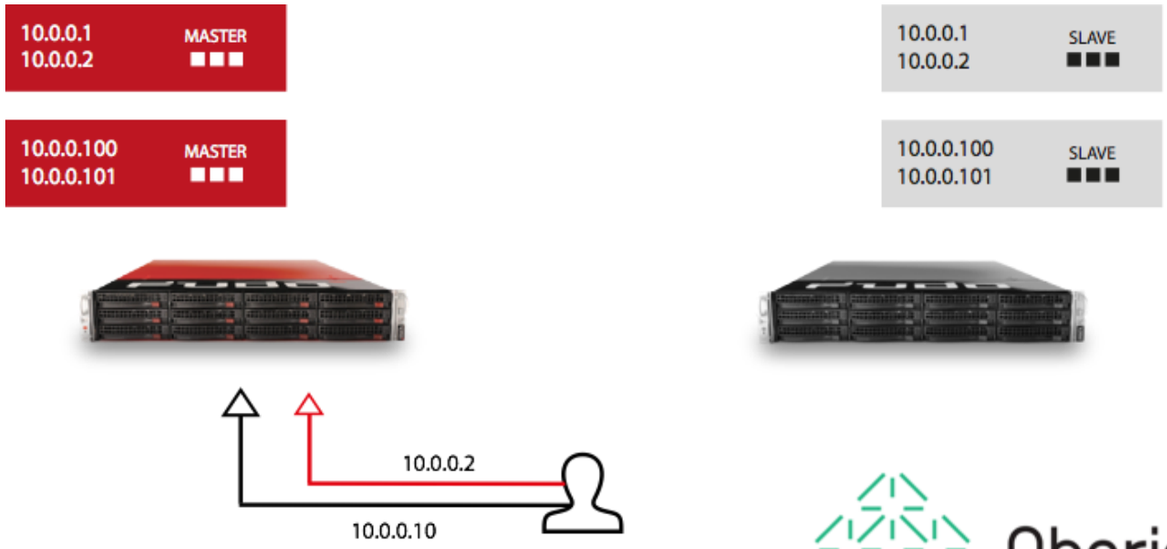
# ВАРИАНТЫ ОТКАЗОУСТОЙЧИВЫХ РЕШЕНИЙ




- Кластер может строиться между смешанными устройствами, например между Hardware и Virtual Appliance

## ОСОБЕННОСТИ

- Каждая нода может быть master или slave или одновременно master/slave
- Обеспечивается синхронизация данных между нодами по сети




FUDO SECURITY

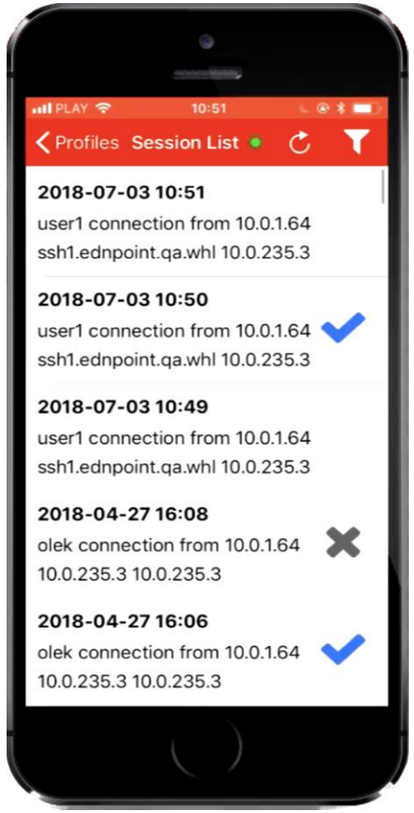
Oberig it

# FUDO PAM – постоянное развитие решения

servicenow™

KIR

PWPW




- Ticket  системы
- Сертификаты времени (time stamping)
- СХД и сервера РК
- FUDO Mobile (скоро...)
- Поведенческий анализ (реализовано с версии 4.0)

FUDO SECURITY

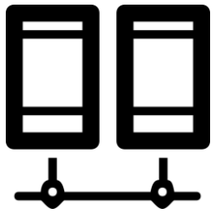
Oberig it

# FUDO PAM: ПРЕИМУЩЕСТВА

Уменьшение времени расследования инцидентов

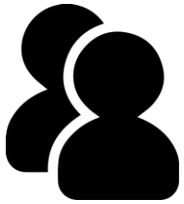
Экономия ресурсов на управлении паролями и эффективное использование политик изменения паролей

Быстрый возврат инвестиций за счет эффективного использования средств по договорам аутсорсинга и технического обслуживания



Работа с различными целевыми системами по различным протоколам и контроль/предотвращение действий

Простота внедрения, эксплуатации, а также - обучения при работе с целевыми системами (запись видео как «пример» для новых сотрудников)



Защита администраторов (доказательства того, что не допускали ошибок при работе)

FUDO SECURITY

Oberig it

# Спасибо за внимание

Станислав Похилько

Менеджер по развитию бизнеса

s.pokhilko@oberig-it.com

www.oberig-it.com

04050, г. Киев, ул. Николая Пимоненка 13,

корпус 1В, офис 1В/12