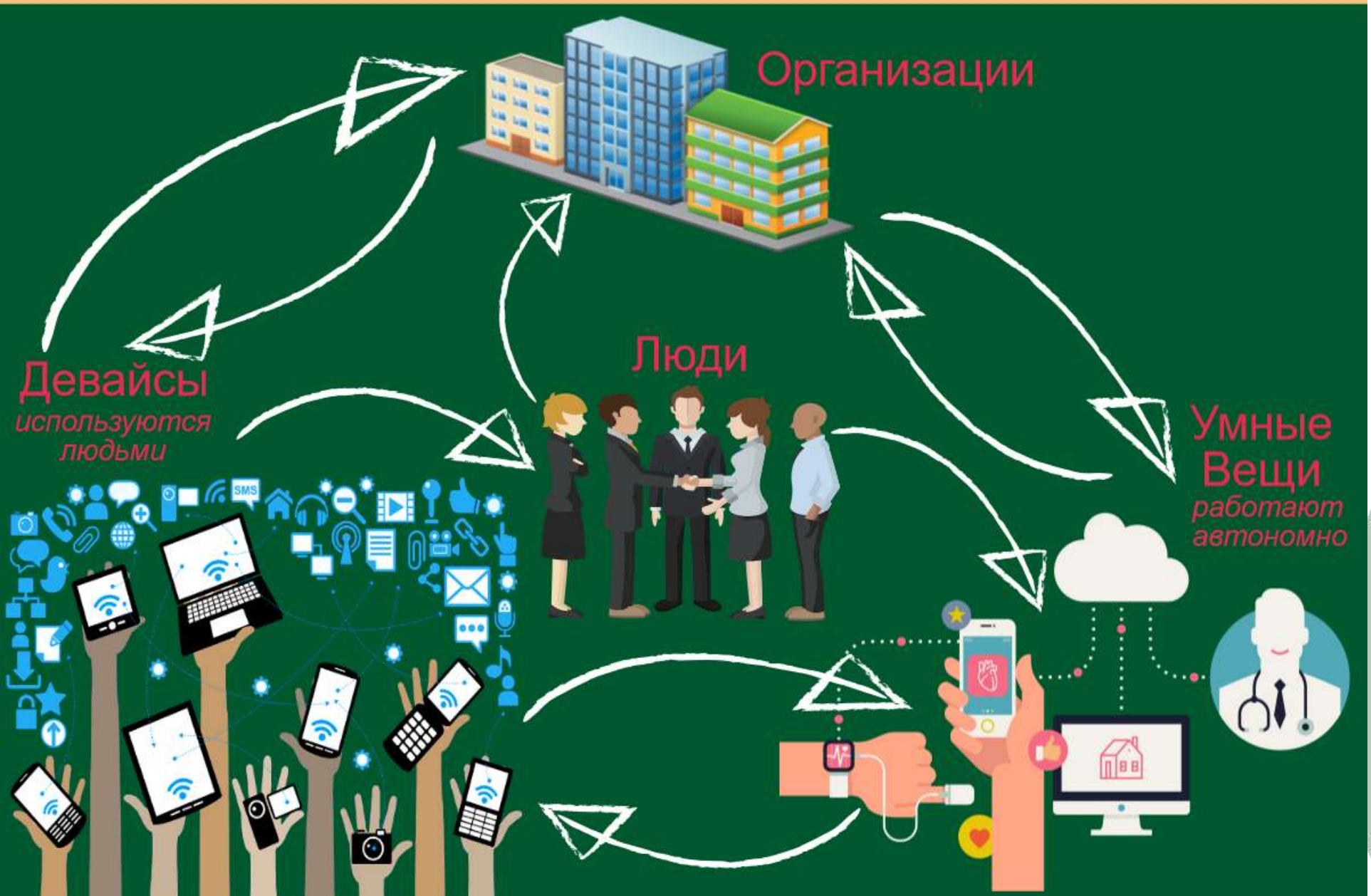
ПОЧЕМУ ХАКЕРЫ БЕРУТ КОНТРОЛЬ НАД ВАШЕЙ ИНФРАСТРУКТУРОЙ? ИЛИ ЗАБЫТЫЕ КЛЮЧИ ОТ КОРОЛЕВСТВА

Ресурсы организаций распределяются очень быстро



ПРИВОДИТ К РИСКАМ

IT ТЕРЯЕТ УПРАВЛЕНИЕ И КОНТРОЛЬ НАД КОРПОРАТИВНЫМИ ДАННЫМИ

Использование облачных приложений не предоставляемых IT-департаментом

Распространение чувствительной информации через частные аккаунты или социальные сети

Использования личных устройств (BYOD)

Нарушение конфиденциальности данных

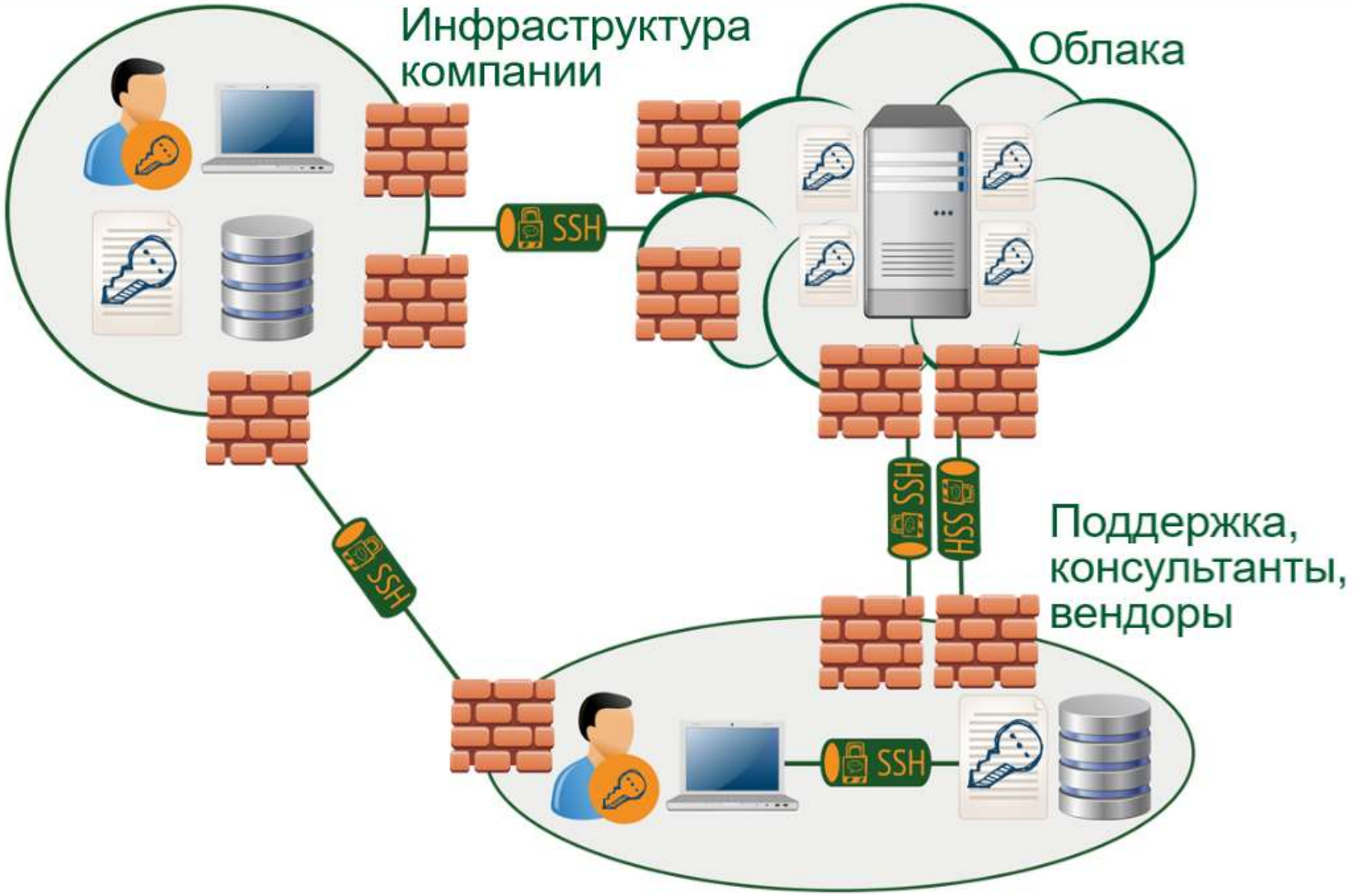
Конфликты конфиденциальности, приватности и соответствия требованиям (compliance)

100% крупных организаций подвержены рискам

- Неконтролируемый обход IAM систем
- Отсутствие жизненного цикла по управлению аккаунтами и их идентификацией
- Возможность получения злоумышленниками доступа к внутренним ресурсам
- Потенциальные нарушения
- Возможность получения злоумышленниками доступа к внутренним ресурсам

ВЕЗДЕ!

Где бывает привилегированный доступ?



ХАКЕРЫ

Как они используют Вашу инфраструктуру?

Поиск жертвы среди партнеров компании

Фишинговая атака. Цель - захват системы с доступом в сеть компании

Получение доступа с украденной учетной записи

Повышение привилегий. Доступ к другим системам

Получение привилегий в других системах. Подключение к C&C

Передача украденных данных. Деструктивные действия.

Виновники инцидентов: производственные компании

источник: PWC - The Global State of Information Security Survey 2016,

Сотрудники + Бывшие сотрудники = до 62 процентов всех виновников !

SSH

Используется везде

ПЛАТФОРМЫ

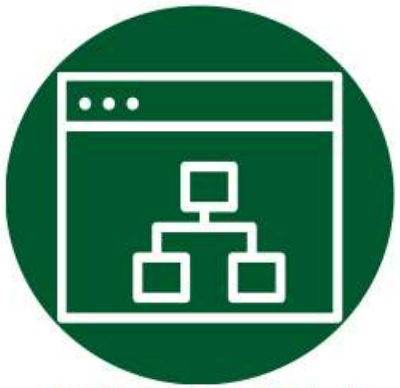
- Unix/Linux/MacOS
- Windows
- Mainframes
- Smartphones
- Network devices
- IoT “things”

АДМИН-НИЕ

- Remote shell
- Remote command
- Automation

ШИФРОВАНИЕ ТРАФИКА

- Secure file transfer
- Backup and sync
- Remote storage
- Tunneling/VPN
- Cloud computing



АККАУНТЫ

- Привилегированные аккаунты
- Совместно используемые аккаунты
- Аккаунты в приложениях
- Стандатные пользователи
- Потерянные, Забытые , Мошеннические

This image cannot currently be displayed.

SSH

Контрольные вопросы

Вы можете определить все доверительные связи между серверами?

У Вас централизованы процедуры
по созданию ключей и управлению доступом?

Они контролируются?

Вы удаляете ключи?

Вы меняете ключи?

Вы можете показать отчет по соответствию требованиям регуляторов?

Почему хакеры захватывают Вашу инфраструктуру?

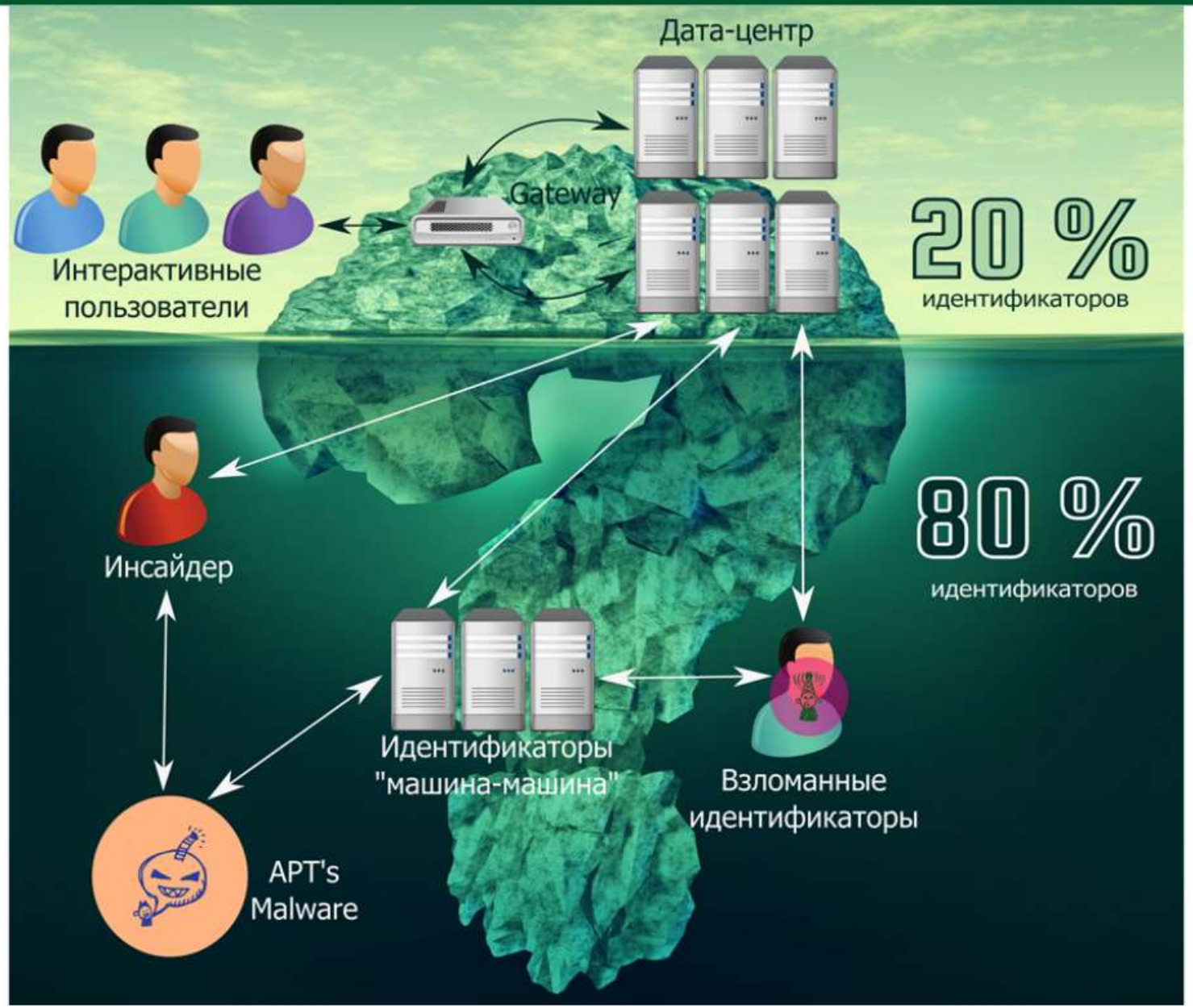
- 20 лет неуправляемых SSH ключей

- Не прописываются ограничения в ключи:
  - Можно где угодно копировать (устанавливать) приватные ключи
  - Ключи не выводятся из действия

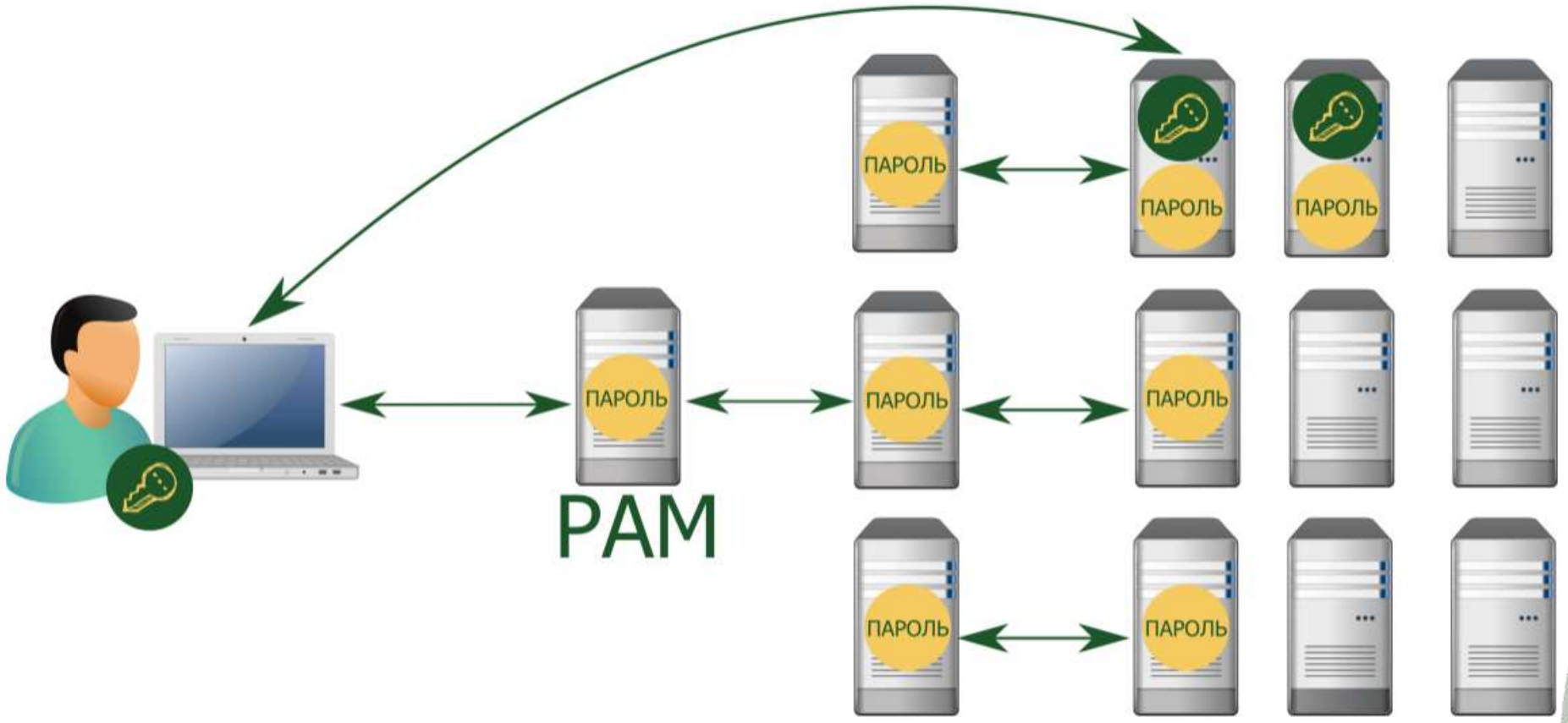
- Нет абсолютного соответствия между приватным ключом и аккаунтом

- Что такое управление? – Создание ключей, контроль над ними, и удаление; контроль разрешений прописанных в ключах , контроль где устанавливаются ключи и как используются.

Возможности, которые Вы не видите

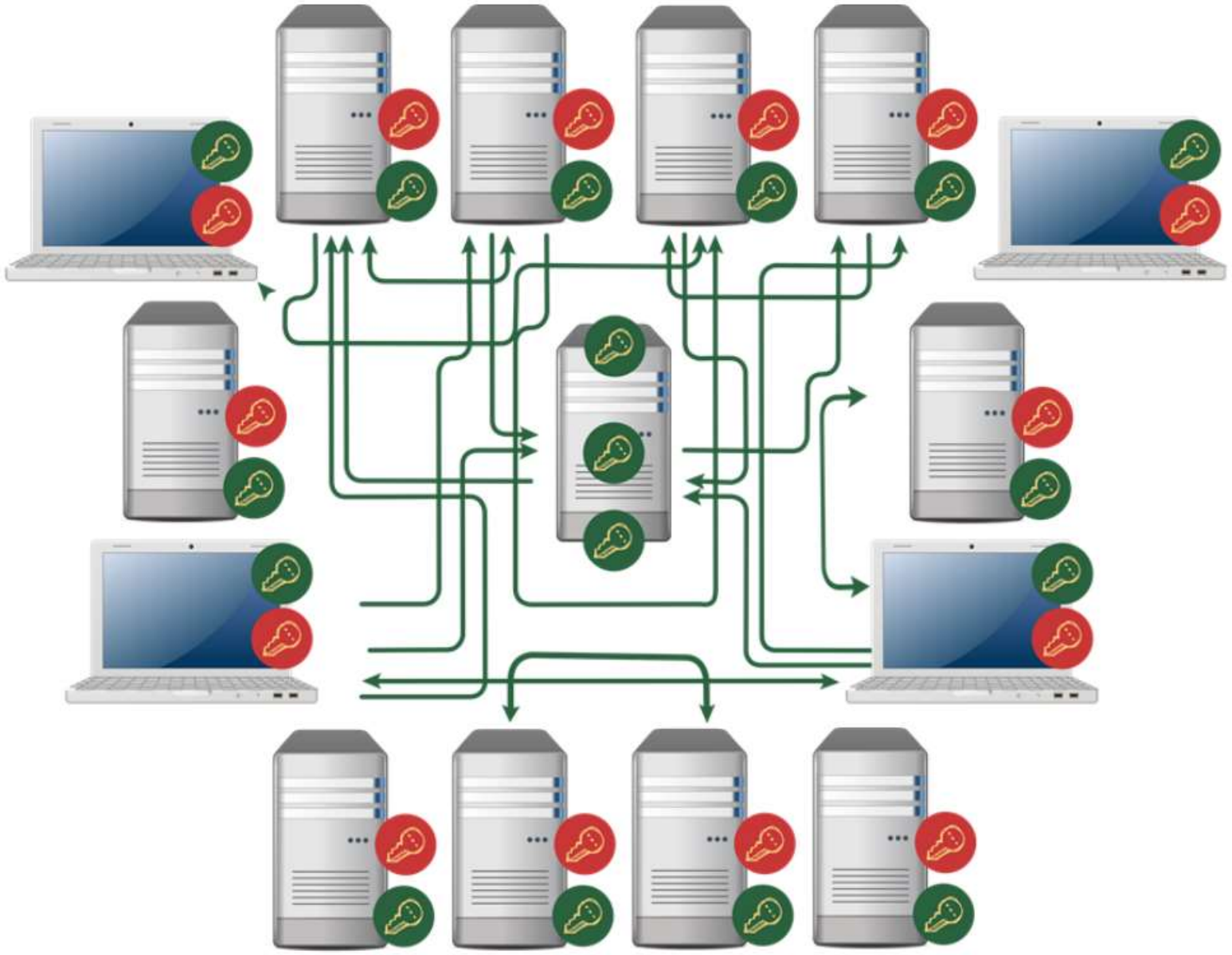


Не очевидный обход систем контроля

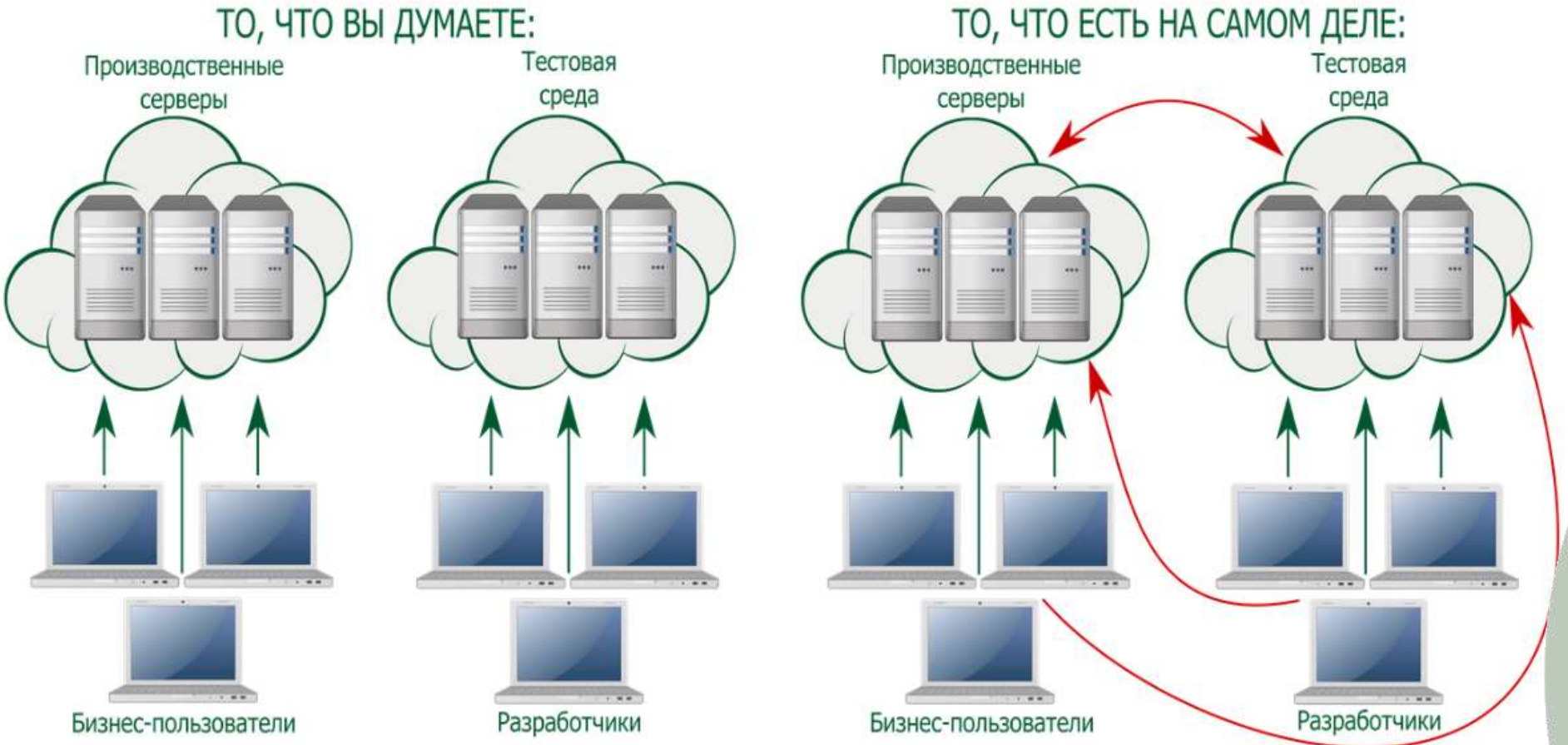


Типичный сценарий: У нас все хорошо, никаких ключей, унификация, мы всех авторизуем по паролю и пароли хранятся в AD (центральный репозиторий и др.)

Неуправляемое множество доверенных связей



Из среды разработчиков - в производственную среду

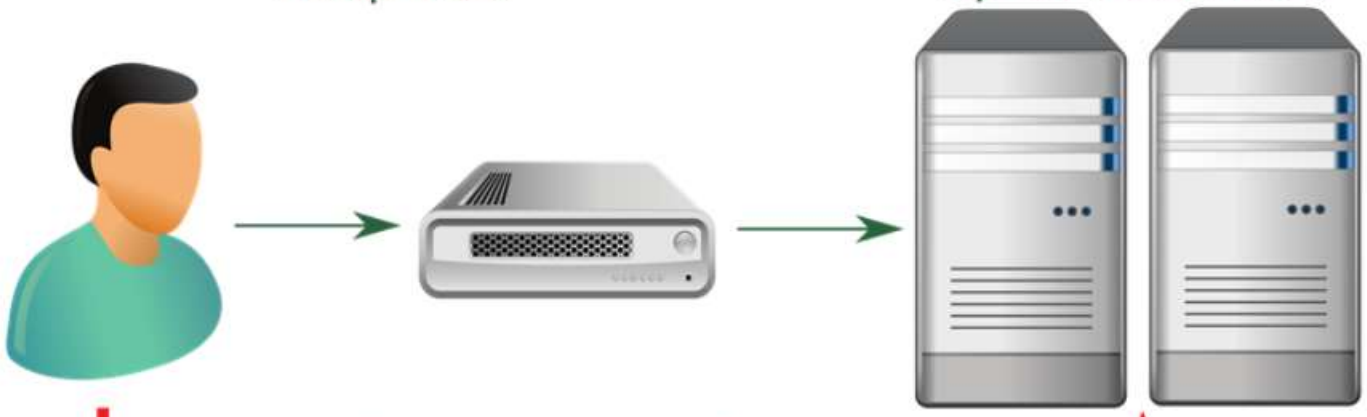


Обход систем безопасности

Первая авторизация

Пользователь авторизуется на сервере через Jump Host

Пользователь получает доступ и загружает публичный ключ



Последующие авторизации

Пользователь обходит Jump Host и внутренние проверки безопасности, используя SSH-ключ

Нежелательное доверие

ПРИМЕР №1

ГЛОБАЛЬНЫЙ БАНК

- Более 10,000 серверов в их сети

-1,5 миллиона Secure Shell ключей

- 10% или 150,000 пользовательских ключей были неизвестны

ОНИ ИМЕЛИ ROOT ДОСТУП

- Нет возможности мониторить или управлять доступом по SSH

- Не прошли SOX и MAS аудит

Что мы предлагаем

Уникальные знания и предметная экспертиза;

Снижение рисков;

- Обеспечение внутреннего и внешнего комплайнса,
- Снижение рисков получения не авторизованного доступа,
- Улучшение устойчивости бизнес-процессов.

Снижение расходов и увеличение эффективности;

- Самые простые и быстрые по внедрению решения,
- Наименьшее влияние на инфраструктуру,
- Низкие расходы на управление и обслуживание,
- Автоматизация процессов.

Увеличение эффективности бизнеса;

- Полноценная работа с облаками с полноценным контролем,
- Динамический доступ к управлению инфраструктурой,
- Выявление и реагирование. От форенсикса к проактивности.

SafeServer

РЕШЕНИЕ ПОСТАВЛЕННЫХ ВОПРОСОВ В СРЕДЕ SSH

Риски не авторизованного использования

НЕИСПОЛЬЗУЕМЫЕ (НЕИЗВЕСТНЫЕ) КЛЮЧИ, ДОВЕРИТЕЛЬНЫЕ СВЯЗИ

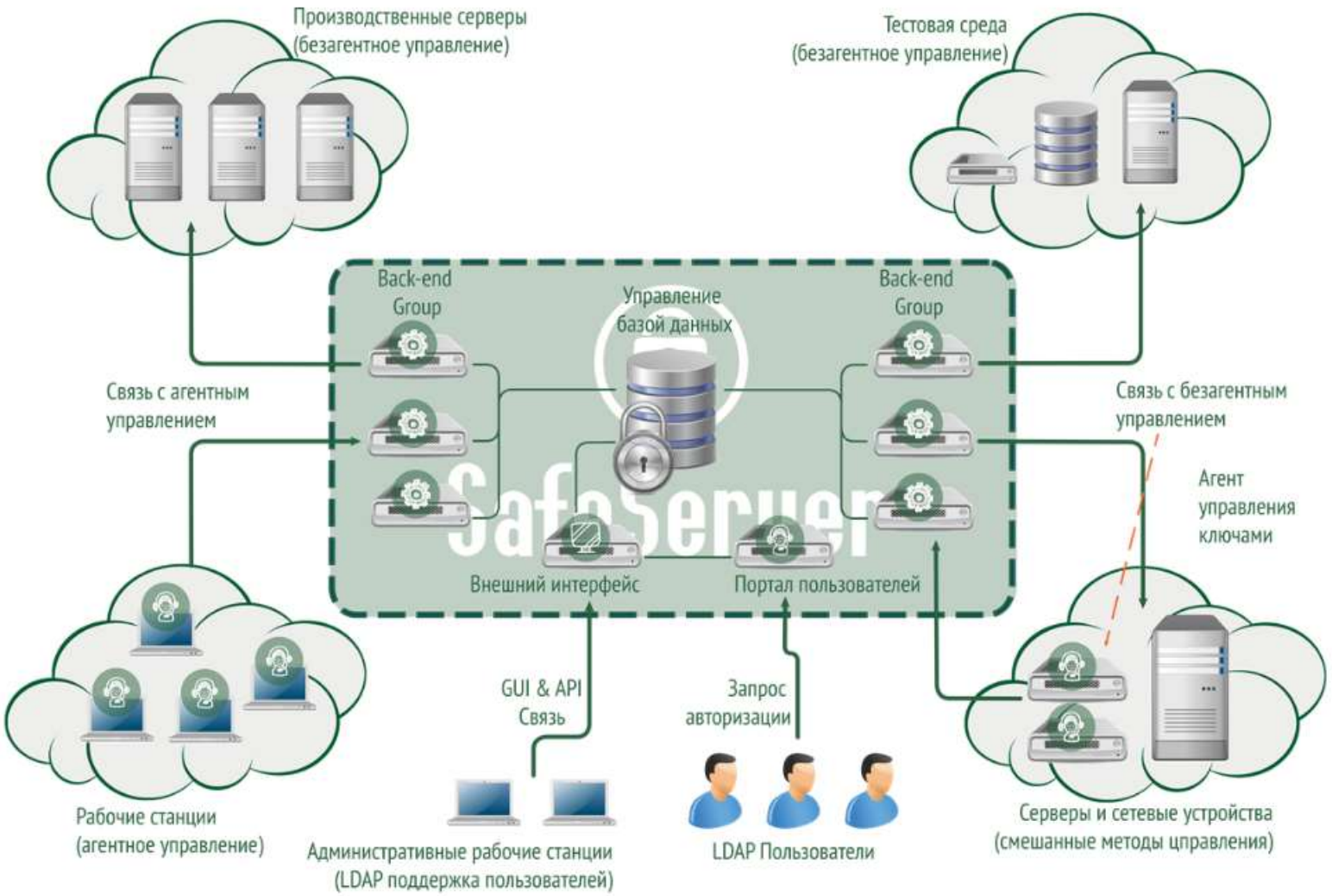
- Несанкционированный доступ к привилегированным аккаунтам (root, oracle, admin)
- Ключи для обхода jump серверов/PAM решений
- Удаленные/восстановленные аккаунты и ключи
- Не выведенные из действия ключи приложений и связи
- Поврежденные файлы ключей
- Транзитивные доверительные связи/ SSH hopping

- Неизвестные доверительные связи
- Неавторизованные доступы через неавторизованные приложения и системные аккаунты
- Совместно используемые ключи
- DR/HA ключи и связи
- Старые ключи
- SSH 1 ключи и связи
- Слабые ключи

ВЫЯВЛЕНИЕ, АНАЛИЗ	1. Хосты, 2. Пользователи, 3. SSH ключи, 4. Доверительные связи
МОНИТОРИНГ	1. Логины и использование ключей 2. Неавторизованные операции
ЗАЩИТА	1. Перемещение ключей в безопасные места
ПРОВЕРКА	1. Удаление неизвестных ключей
УПРАВЛЕНИЕ	1. Автоматизация жизненных циклов, 2. Управление SSH, 3. Управление инфраструктурой SSH.

SafeServer

АРХИТЕКТУРА

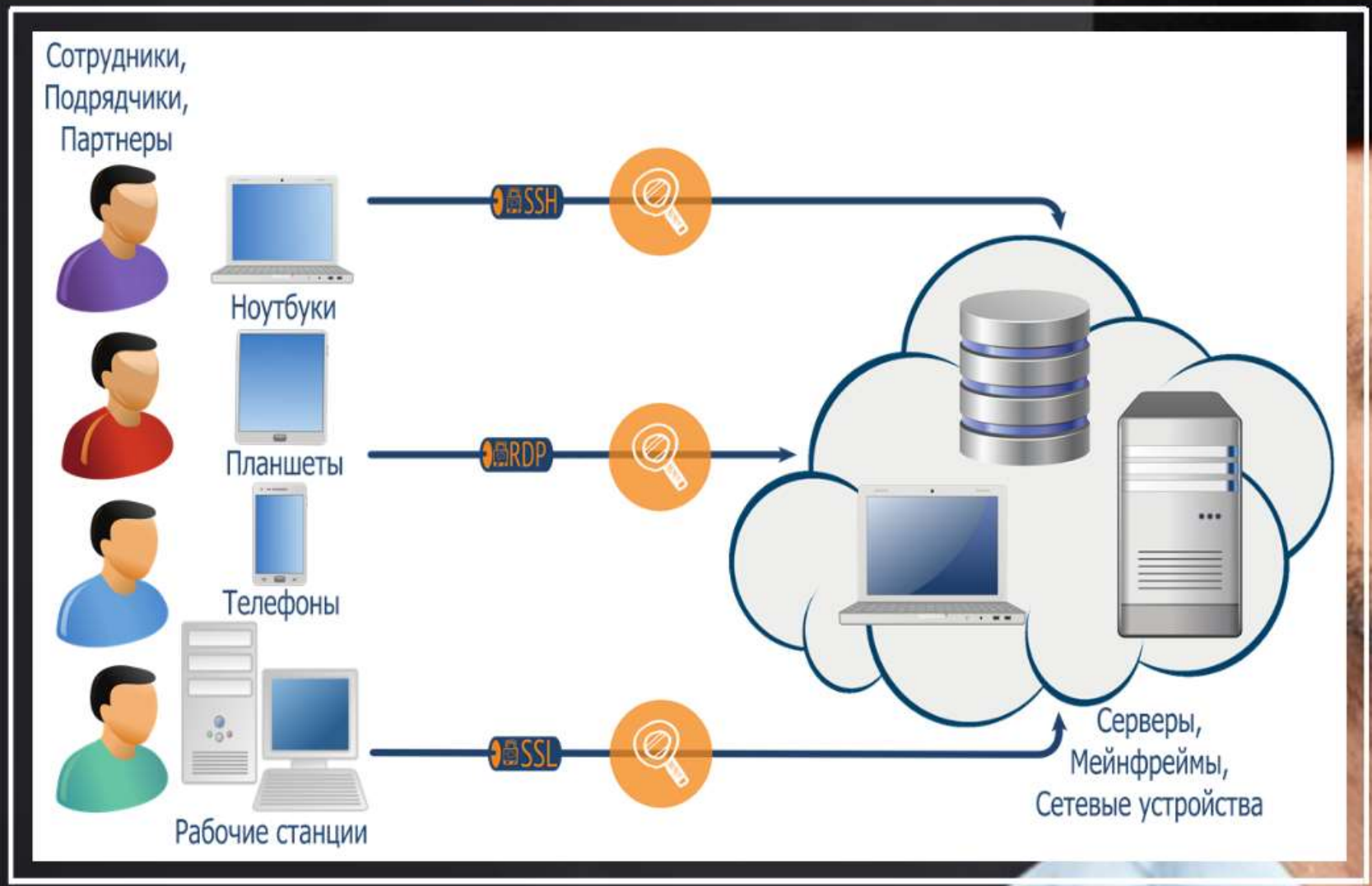


SafeInspect

КОНТРОЛЬ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

ПАРАДОКС

СЛЕПОТА ОТ ПРИМЕНЕНИЯ КРИПТОГРАФИИ!



Контрольные вопросы

У Вас есть решение для контроля привилегированных пользователей, соответствующее требованиям (например, PCI-DSS)?

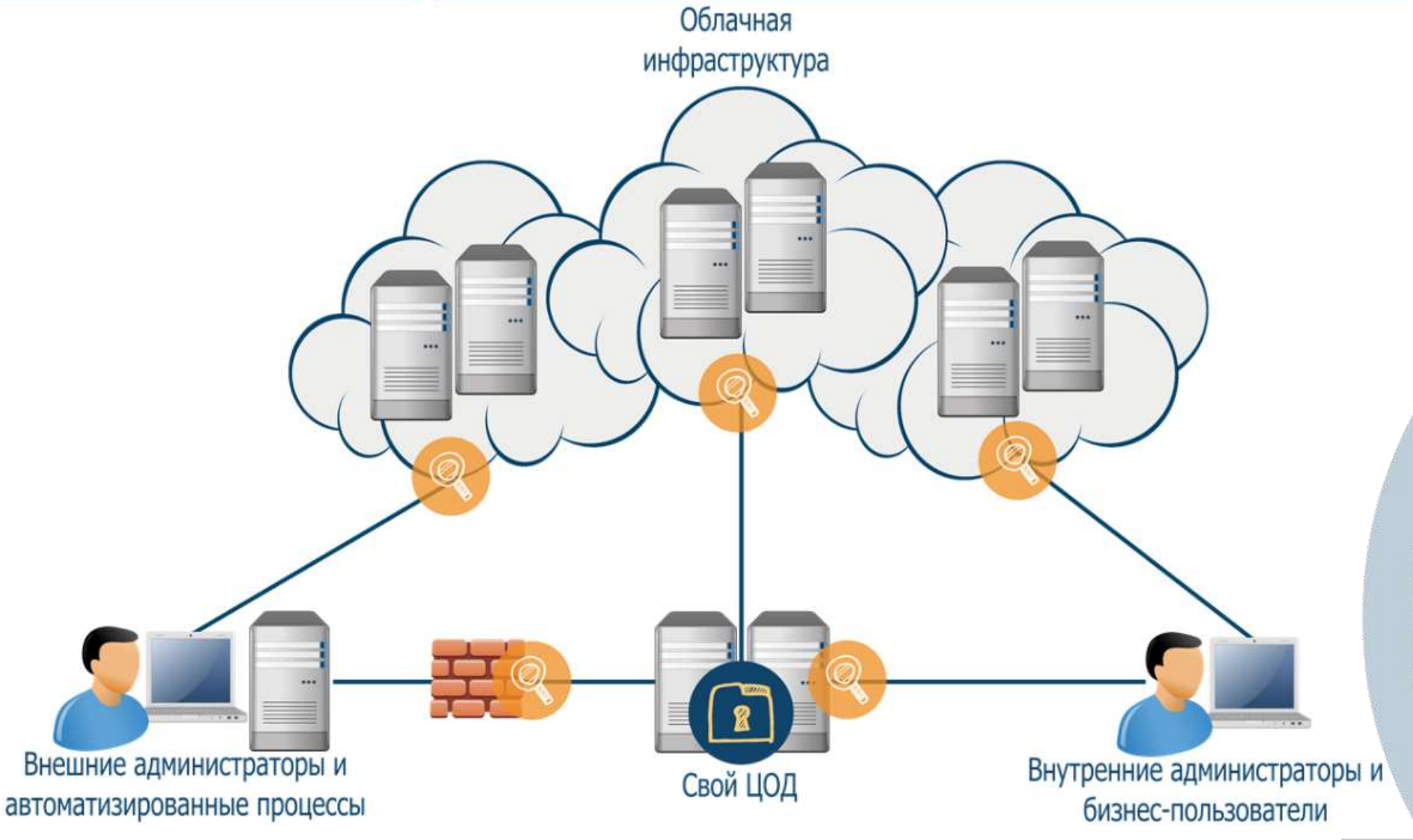
У вас есть DPL и IPS решения?
Вы контролируете их с помощью зашифрованных каналов связи (RDP, SSH, SFTP, TLS)?

Если администратор Windows или UNIX попытается украсть данные или повредить системы, Вы можете его остановить?

А собрать точные данные о том, что именно он делал?

Внешние консультанты, администраторы имеют свои пароли для входа в критичные системы?

Они используют пароли доступа, которые принадлежат внутренним администраторам?


Облачная
инфраструктура
Внешние администраторы и
автоматизированные процессы
Свой ЦОД
Внутренние администраторы и
бизнес-пользователи

ПРОЗРАЧНО, БЕЗ АГЕНТОВ	1. Быстрая установка, 2. Виртуальная или «железная» установка, 3. «Бастион» или «Прозрачный» режимы
СТРОГАЯ АУТЕНТИФИКАЦИЯ	1. Комбинированный контроль доступа, 2. LDAP, OTP, SecurID, сертификаты, 3. Совместные аккаунты
АУДИТ ТРАФИКА	1. Аудит SSH, SSL, RDP, SFTP, 2. Центральное хранилище результатов аудита
ИНТЕГРАЦИЯ	1. Передача расшифрованного трафика в DLP, IDS, AV, SIEM
УПРАВЛЕНИЕ	1. Действия в режиме реального времени, 2. Сообщения и отчеты

ПРИМЕР №1

ФИНАНСОВАЯ ОРГАНИЗАЦИЯ

- Несколько ЦОД

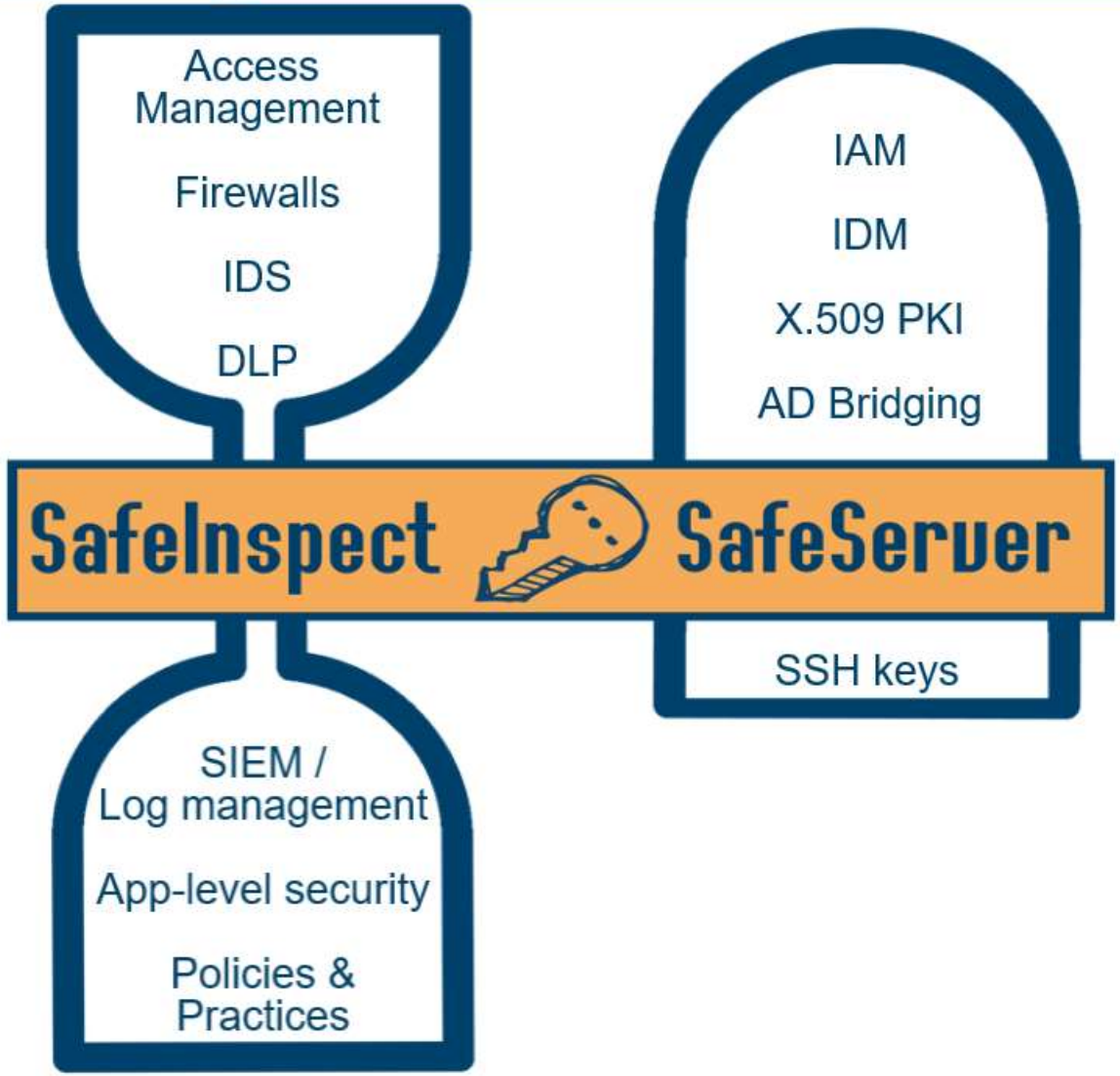
- Много администраторов и консультантов – представителей вендора

- Много внутренних администраторов

- Нет возможности мониторить их удаленные соединения или зашифрованный трафик

- Необходимо выполнять требования PCI-DSS и требования банка России

Делаем систему безопасности консистентной



POLL 1

Что наиболее критично в отношении привилегированного доступа и зашифрованных каналов передачи данных?

1. Мониторинг и контроль облачного доступа?

2. Мониторинг и контроль внутренних администраторов?

3. Мониторинг и контроль внешних консультантов/вендоров?

4. Мониторинг и контроль не интерактивных (машина – машина) соединений?

5. Контроль зашифрованных входящих /исходящих сессий и контента?

POLL 2

Какова ситуация с моей инфраструктурой (средой)?

1. У меня есть инструменты, которые выполняют все текущие и перспективные требования?

2. У меня есть инструменты, но они не выполняют всех моих требований ?

3. У меня нет таких инструментов и нет крайней необходимости в их наличии.

4. У меня нет таких инструментов, но я ищу сейчас инструменты, которые будут выполнять мои требования.

ЧТО ДЕЛАТЬ СЕЙЧАС?

Защитите себя! Скачайте SafeInspect и SafeServer
с сайта www.newinfosec.ru

Запустите пилотный проект по тестированию или анализу.

Не уверены в необходимости?
Закажите аудит инфраструктуры SSH
и узнаете много нового о своей компании!

Контакты:
ООО «Новые технологии безопасности»
Москва, ул. Трубная, 12
Телефон/Факс: +7 (495) 787 99 36
www.newinfosec.ru