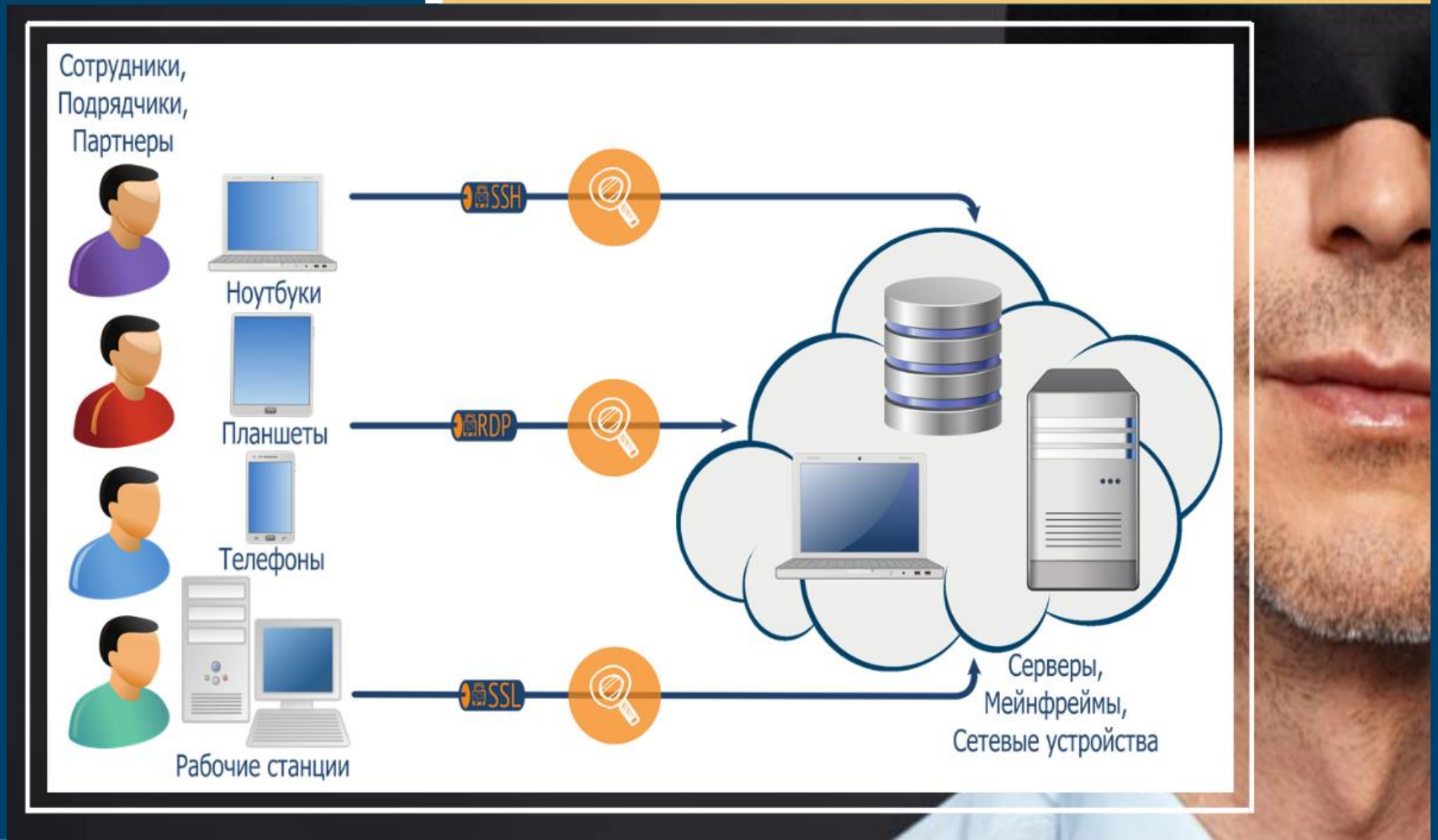
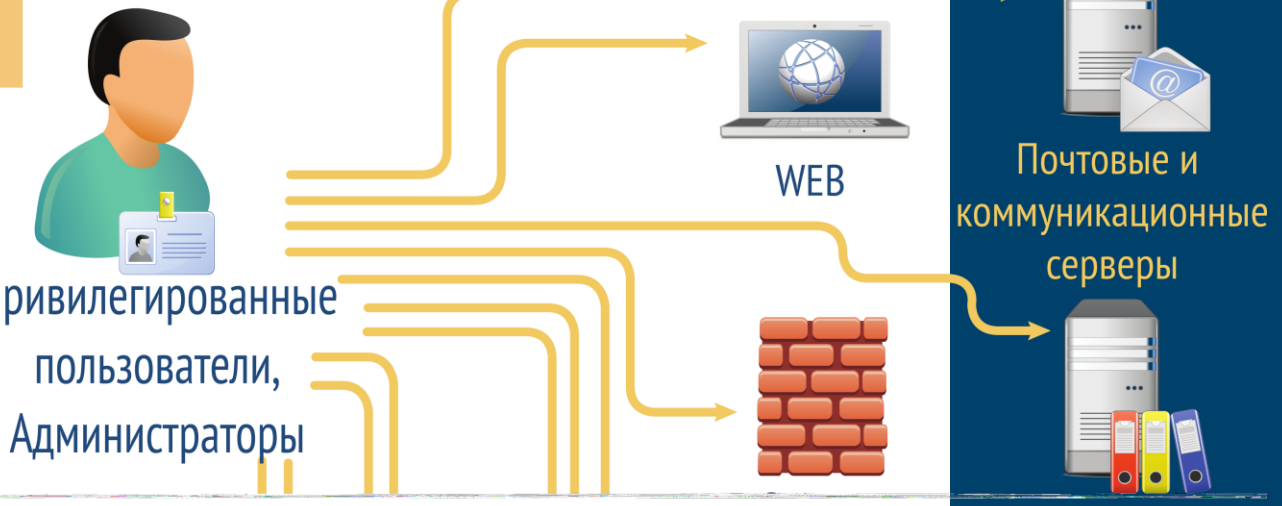
WHO IS MISTER PU?

ПАРАДОКС

СЛЕПОТА ОТ ПРИМЕНЕНИЯ КРИПТОГРАФИИ!

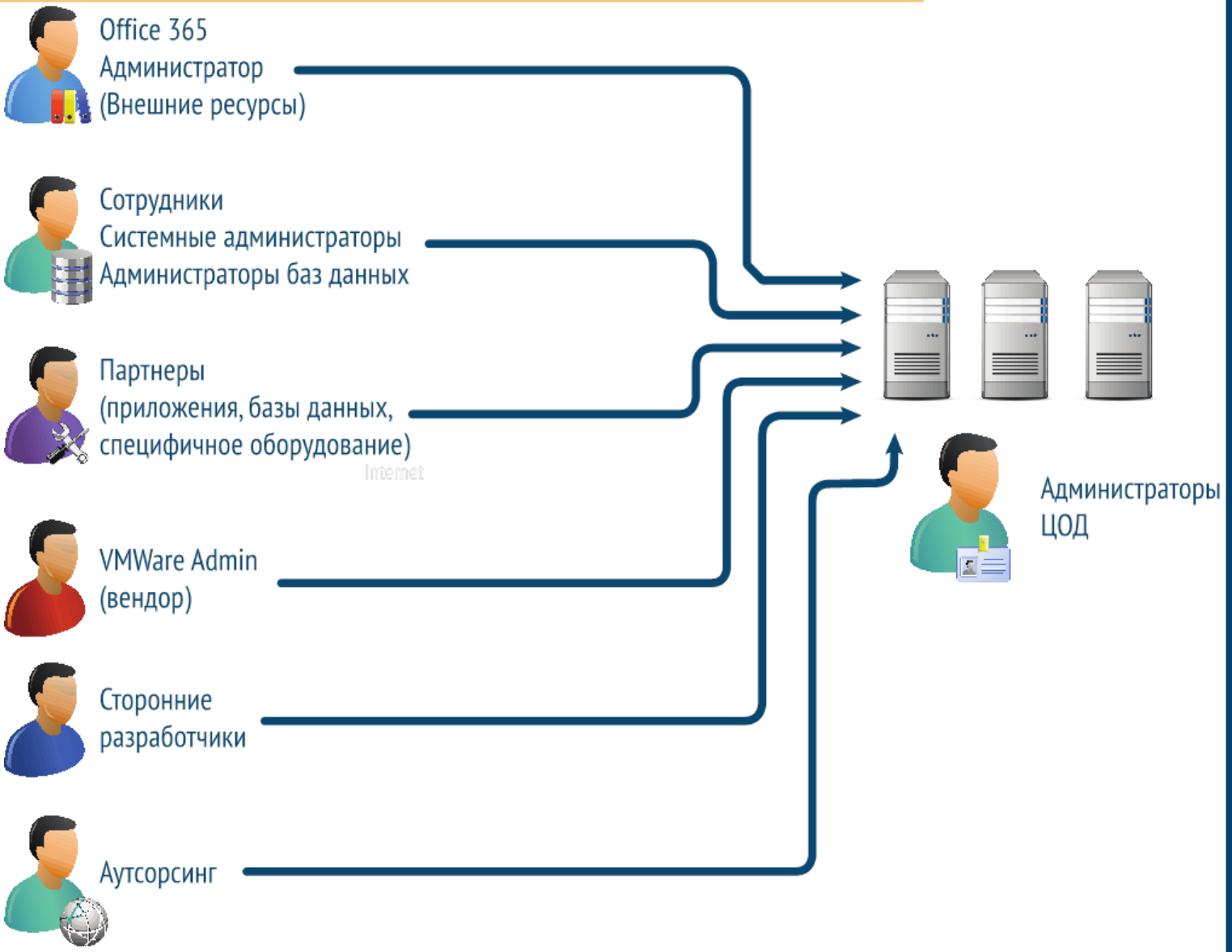


PRIVELEGED USER – КТО ОН?



Учетные записи с высокими привилегиями
(Administrator, Root, Cisco, Oracle и др.)

ПРОБЛЕМА



- Разное оборудование требует разных администраторов
- Для разных ресурсов требуются специалисты нескольких компаний
- Нескольким администраторам требуется доступ к одним и тем же ресурсам
- Трудно понять что делал admin на серверах или в оборудовании АСУ ТП

ПРОБЛЕМА

Скачивали запрещенный контент на рабочем месте

Обходили политики безопасности в личных целях

Скачивали конфиденциальные данные

Использовали права для доступа к важным корпоративным данным

Читали сообщения электронной почты коллег

Удаляли и изменяли логи с целью сокрытия следов нарушений

70%

организаций не в состоянии регулярно проводить оценку поставщиков на соответствие нормативным требованиям по ИБ

60%

организаций не в состоянии регулярно проводить оценку поставщиков на соответствие политике безопасности своей организации

40%

организаций не в состоянии обеспечить сотрудников инструкцией по классификации критичных данных

SafeInspect

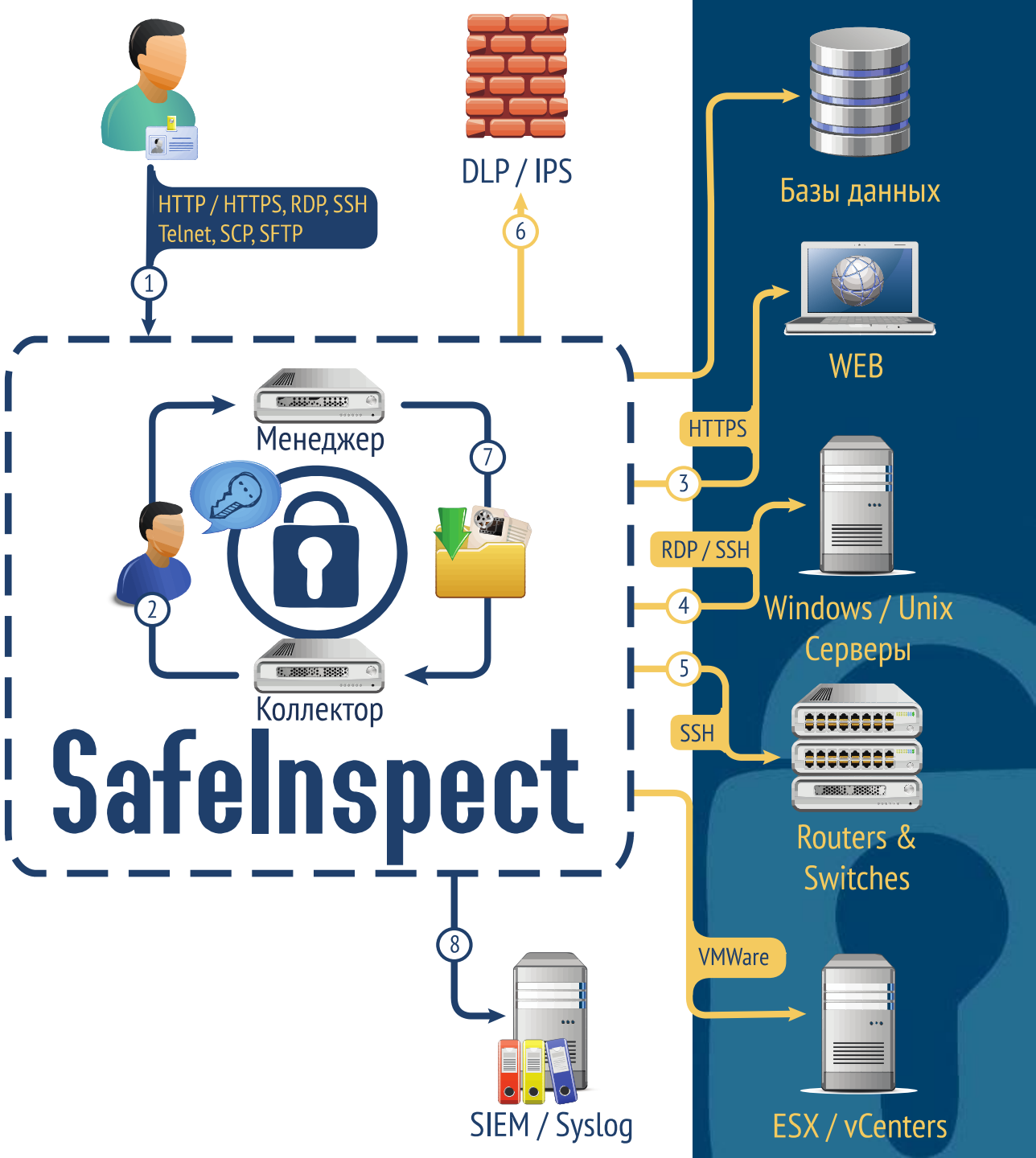
Полнофункциональная платформа для контроля привилегированных учетных записей в информационных системах – как классических, так и облачных

- Контроль широко используемых протоколов;
- Регистрация действий в виде видеозаписи;
- Индексация, быстрый поиск события;
- Контроль зашифрованных каналов;
- Работа без использования агентов;
- Двухуровневый контроль подключений;
- Двухфакторная аутентификация;
- Контроль доступа в реальном времени;
- Аудит файловых операций;
- Статистика и отчеты о действиях;
- Сбор информации для расследований инцидентов.

ИНТЕГРАЦИЯ

3 варианта:

- ПРОЗРАЧНЫЙ - система устанавливается в «разрыв» соединения с серверами;
- МАРШРУТИЗАТОР - соединения с серверами направляются в систему, а она маршрутизирует их на сервера;
- БАСТИОН - для доступа к серверам необходимо явно подключаться к порталу системы.



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

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