



Корпоративная система контроля доступа

ООО «НТБ» 2021





ЗАЧЕМ ОН НУЖЕН?

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



Контролировать
подрядчиков,
обслуживающих
конечное оборудование



Выявлять нанесение вреда
ресурсам компании
системными администраторами



Иметь доказательства
факта компрометации
целевого сервера



Быстро реагировать
на инциденты



Минимизировать затраты за счет
применения масштабируемого
виртуального устройства



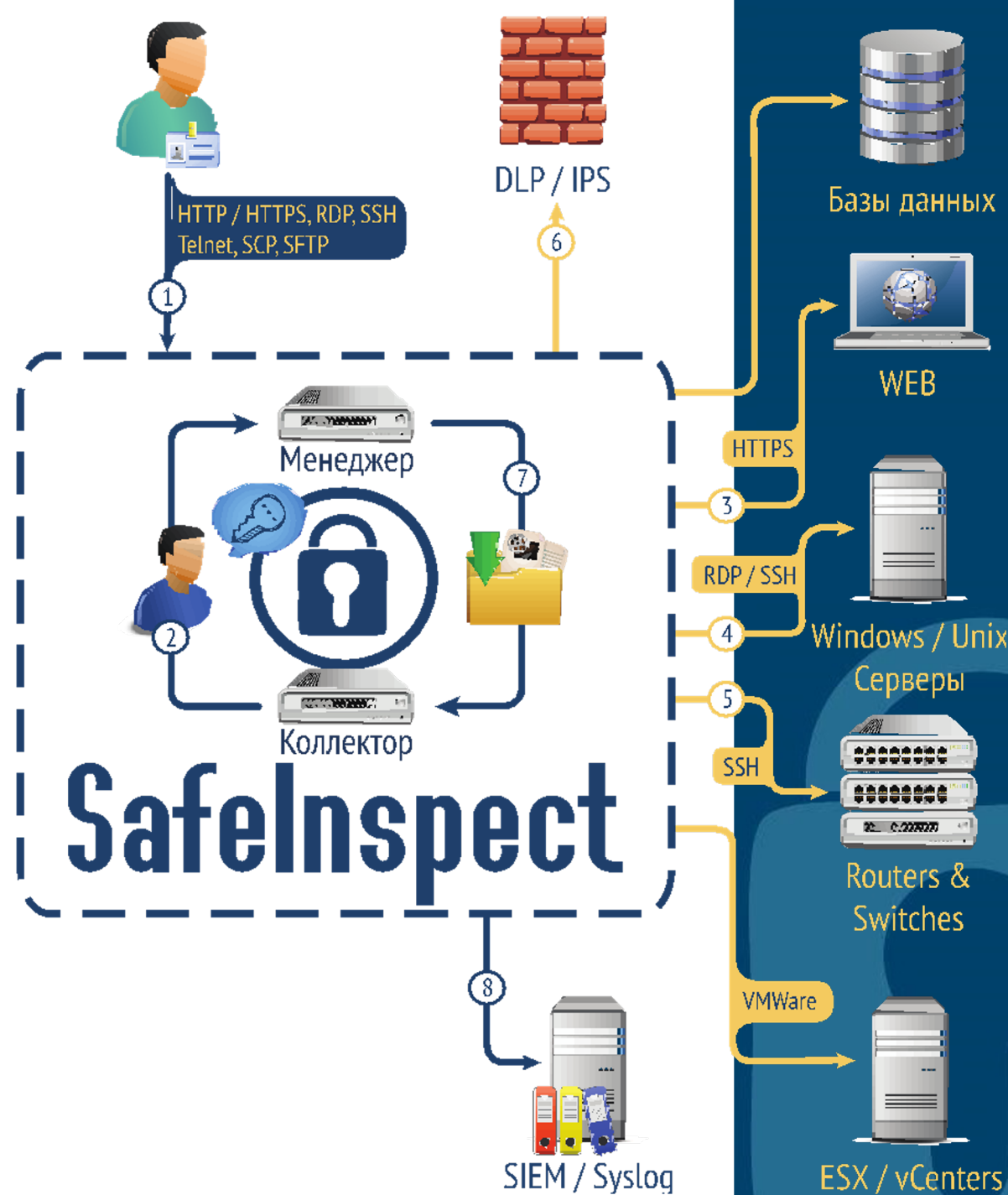
Анализировать
поведение
злоумышленника

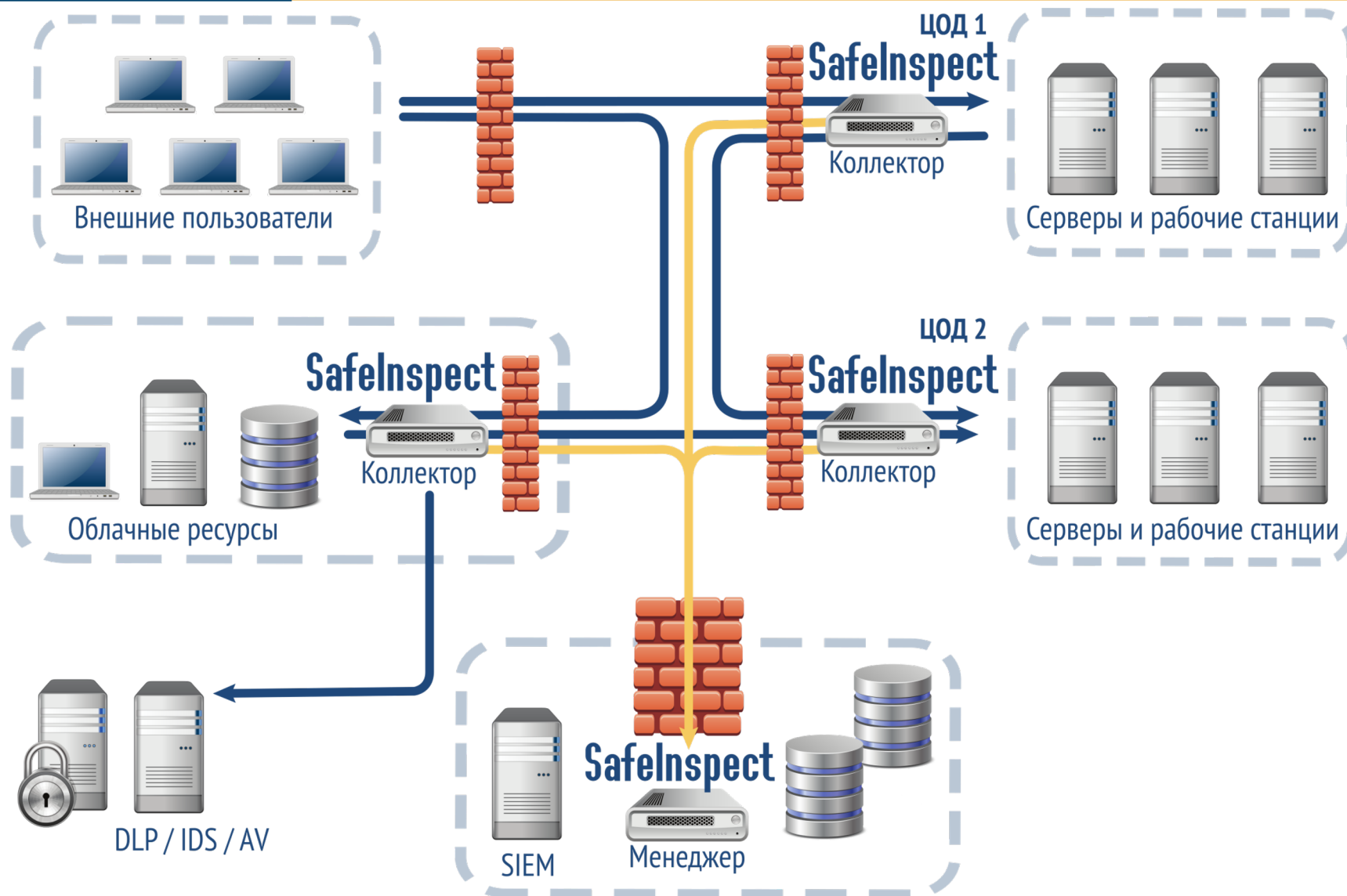


ИНТЕГРАЦИЯ

Два сценария:

- ПРОЗРАЧНЫЙ (L2/L3) - система устанавливается в «разрыв» соединения с серверами;
- БАСТИОН - для доступа к серверам необходимо явно подключаться к portalу системы.







ОСНОВНЫЕ ВОЗМОЖНОСТИ

- Запись и воспроизведение сессий:
SSH (*nix)
RDP (Windows)
HTTP(s)
Telnet, TN3270 и т.д.
- Определение и аудит подканалов:
SCP, SFTP, X11 и др. (SSH)
Буфер обмена, подключаемые устройства (RDP)
- Индексация содержимого, поиск по ключевым словам
- Оптическое распознавание символов в RDP (OCR)

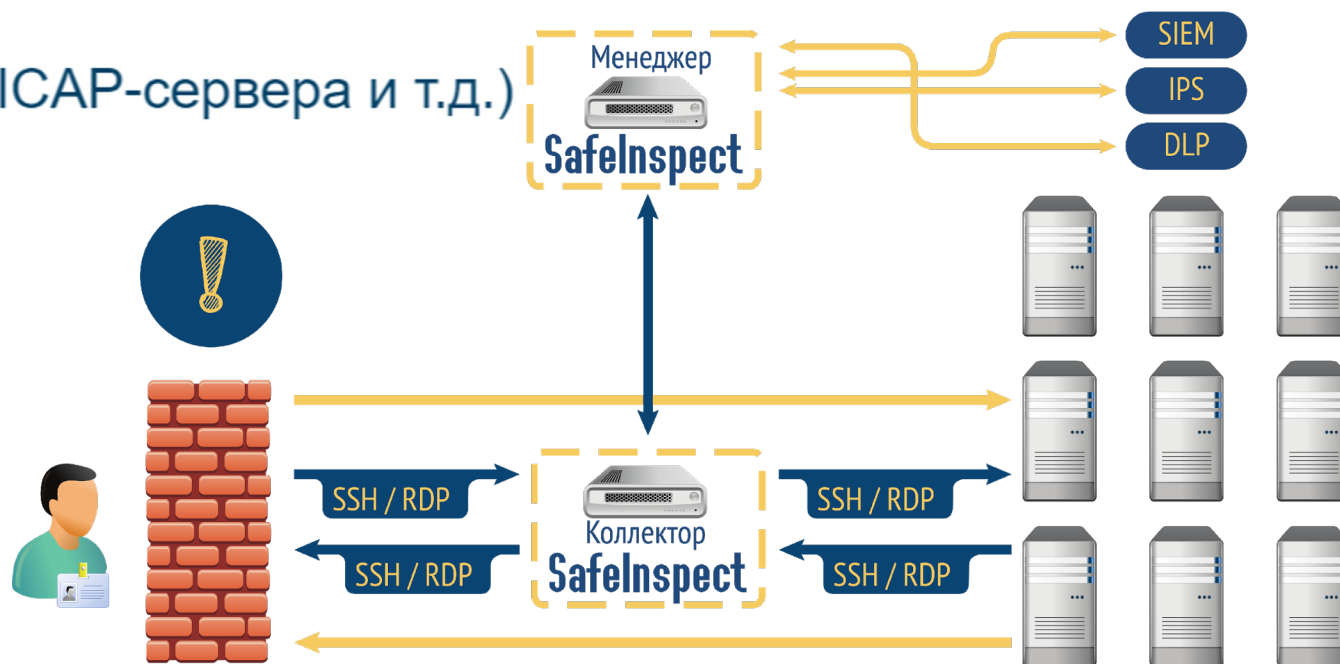




ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ ЗАЩИТЫ И КОНТРОЛЯ

Интегрируется со следующей инфраструктурой и процессами:

- Пользовательские каталоги: AD, RADIUS, RSA SecurID
- SIEM – Syslog/LEEF/CEF (IBM QRadar, RSA key, Splunk и т.д.)
- IDS
- DLP (RSA DLP, McAfee, ICAP-сервера и т.д.)



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



Спасибо за внимание!

