

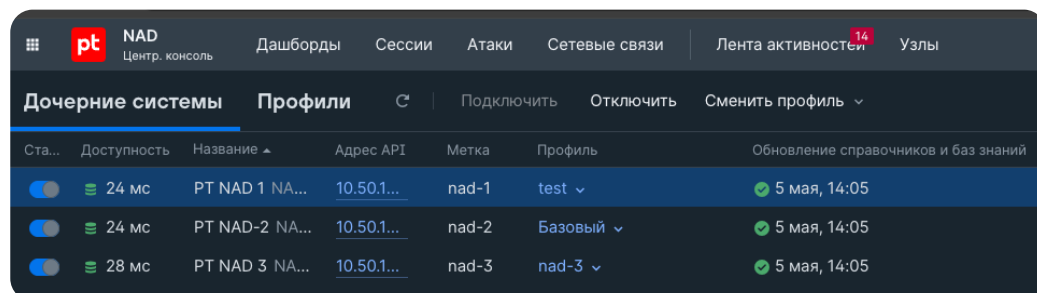


■ positive technologies

Центральная консоль в РТ NAD

ЕДИНОЕ ОКНО МОНИТОРИНГА ВСЕХ ИНСТАЛЛЯЦИЙ PT NAD

Центральная консоль позволяет выстроить в едином интерфейсе процессы мониторинга, анализа угроз и сдерживания злоумышленника, обеспечивая полный контроль трафика на всех инсталляциях PT NAD.



Главный экран центральной консоли с несколькими инсталляциями PT NAD

Раньше вы сталкивались с необходимостью

- Мониторинга геораспределенной инфраструктуры в режиме одного окна
- Мониторинга большой инфраструктуры (например, трафик в ЦОД)
- Большого количества персонала для мониторинга

Ключевые возможности консоли



Мониторинг трафика из множества инсталляций PT NAD



Доступ к исходной копии трафика любой инсталляции



Инвентаризация узлов всех контролируемых сетей



Удобная визуализация



Управление контентом



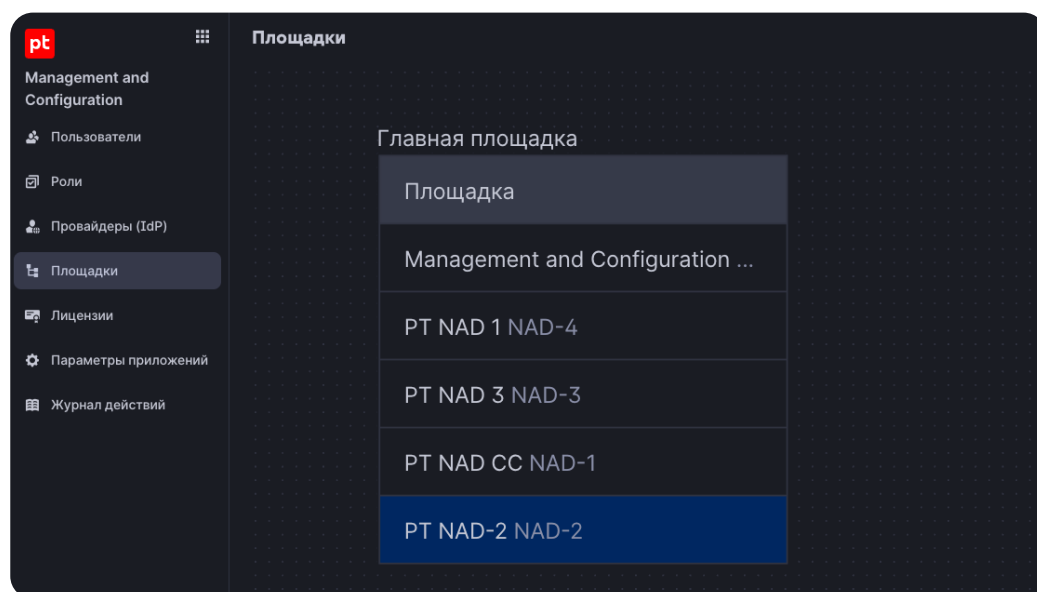
Легкое подключение новых инфраструктур к мониторингу



Тонкая настройка прав: пользователь получает доступ только к определенным инсталляциям

КАК НАЧАТЬ РАБОТУ

- 1** Обеспечьте IP-связность PT NAD и центральной консоли
- 2** Зарегистрируйте все инсталляции PT NAD и центральную консоль в PT MC ¹
- 3** Обратитесь в техподдержку, чтобы получить технологическую лицензию на использование центральной консоли



Пример интерфейса – Регистрация в PT MC

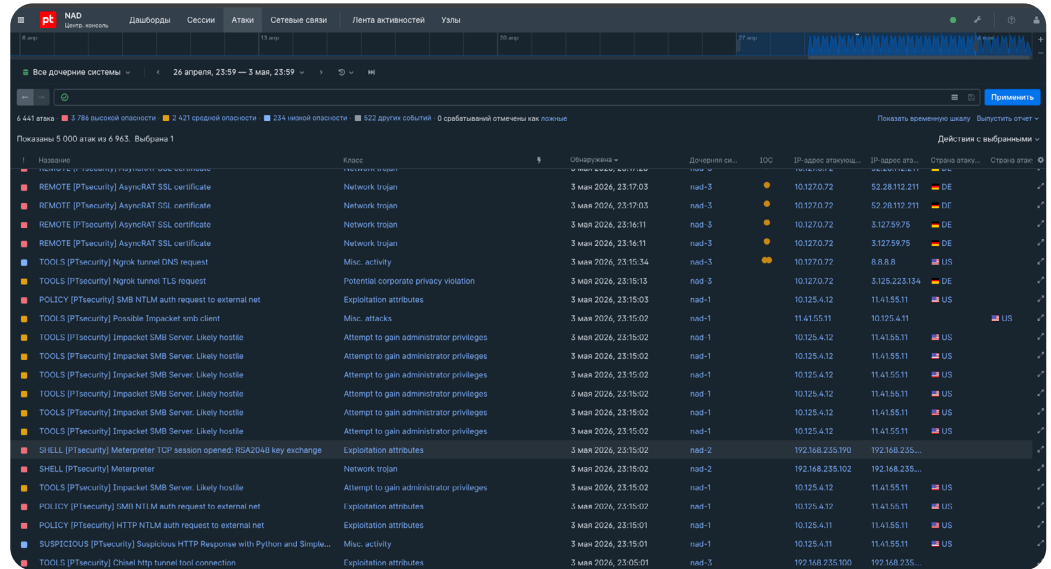
**КОЛИЧЕСТВО ИНСТАЛЛЯЦИЙ PT NAD,
ПОДКЛЮЧЕННЫХ К ЦЕНТРАЛЬНОЙ
КОНСОЛИ, НЕ ОГРАНИЧЕНО**



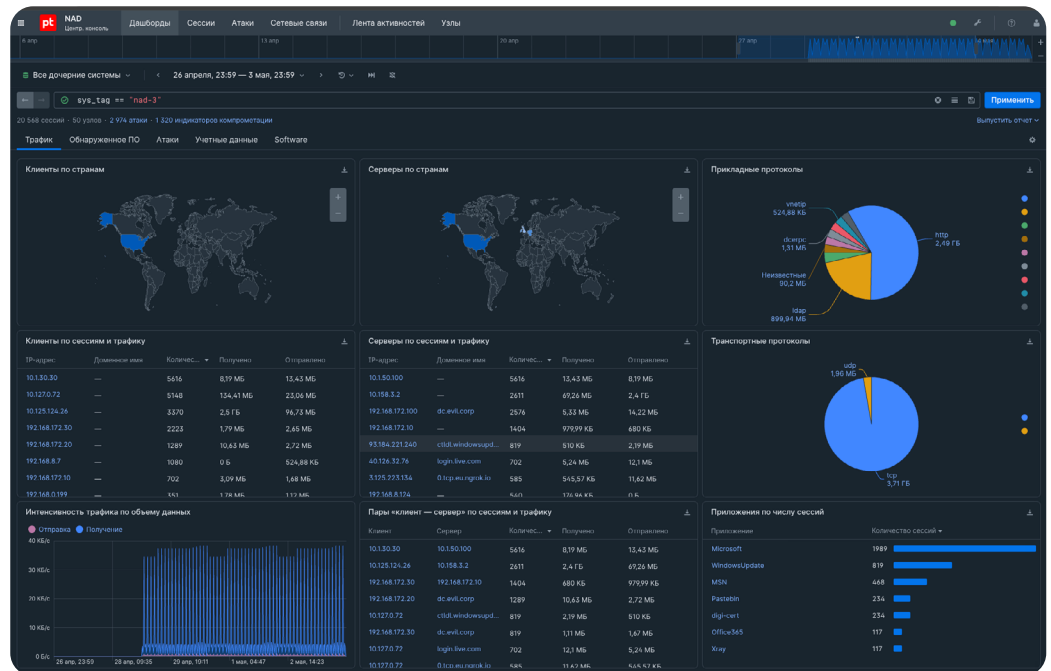
КАК ПОЛЬЗОВАТЬСЯ

1. Использование центральной консоли повторяет работу в обычном интерфейсе PT NAD, но есть небольшие дополнения:

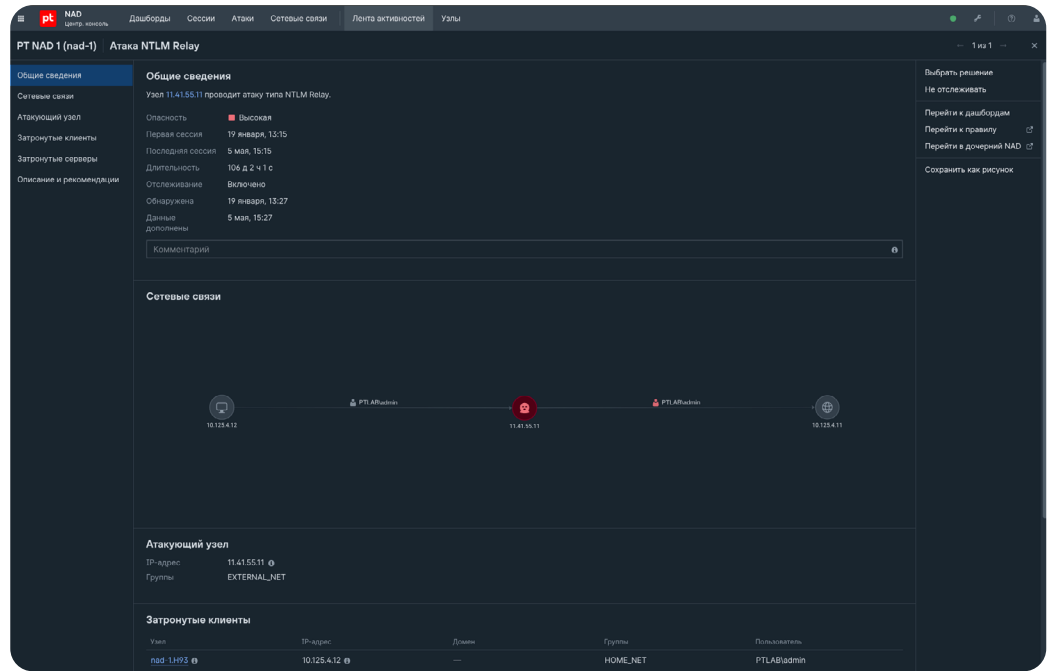
- В консоли отображается информация о принадлежности той или иной сессии к конкретной установке PT NAD



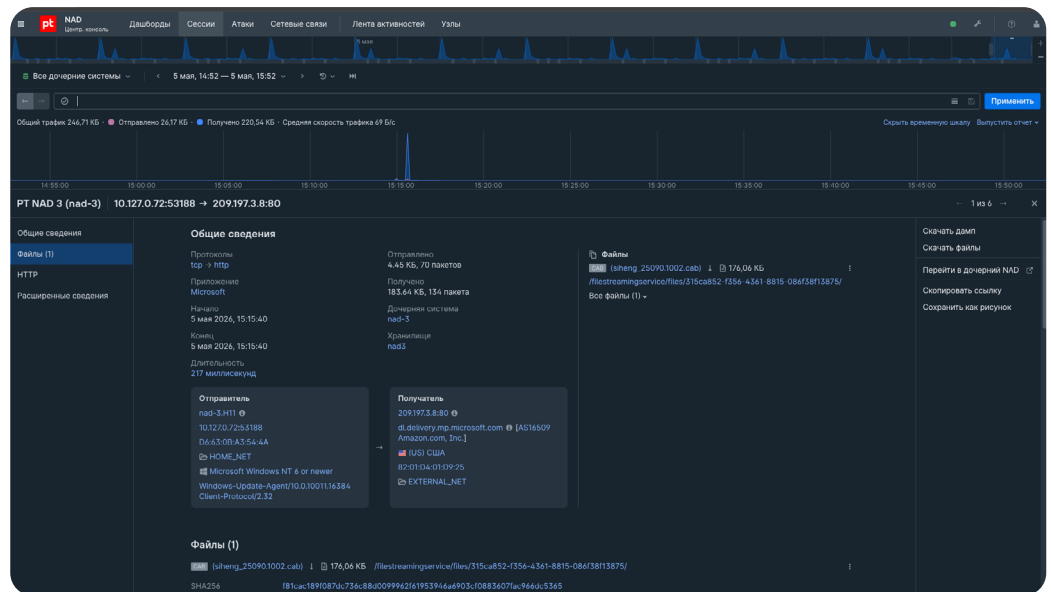
- Специальный фильтр `sys_tag == "nad-3"` позволяет отфильтровать сессии из конкретной установки PT NAD



- В карточках Ленты активностей явно прописано, в какой инсталляции PT NAD она сформирована

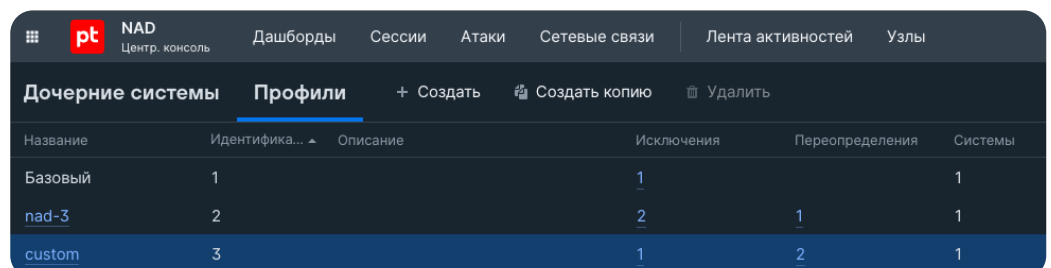


2. Из центральной консоли можно скачивать дампы трафика и файлов любой подключенной инсталляции PT NAD

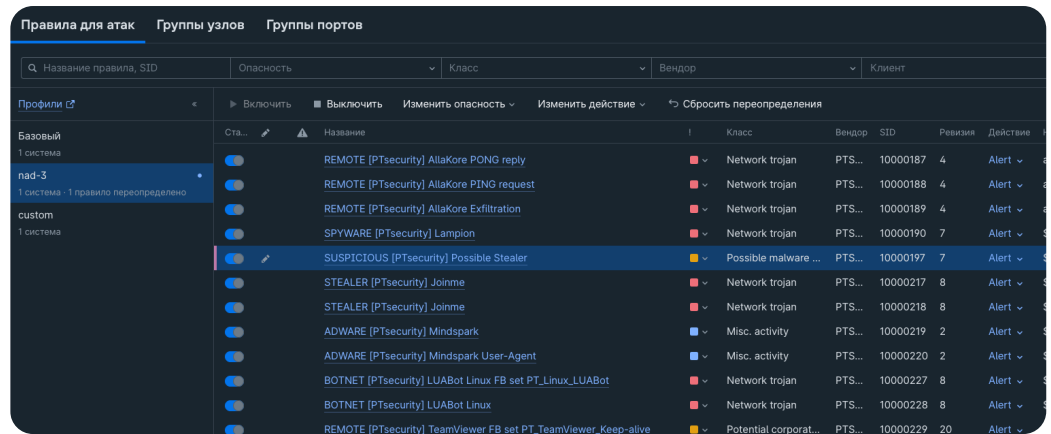


3. Важная особенность — можно управлять контентом и исключениями всех инсталляций PT NAD прямо в центральной консоли

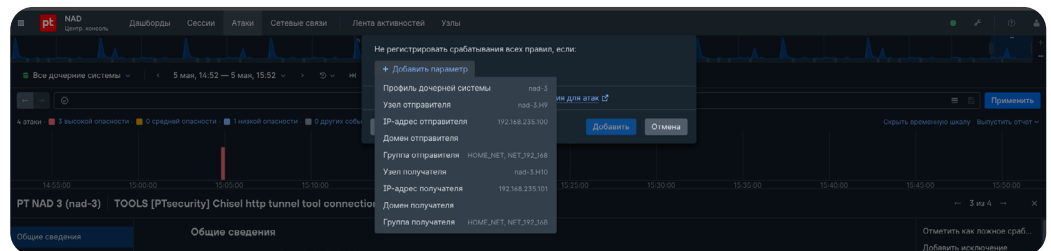
- В консоли есть профили, которые можно присваивать одной или нескольким инсталляциям PT NAD



- Можно управлять сигнатурами на всех инсталляциях, которым присвоен профиль



- Можно добавлять исключение для конкретного профиля – оно применится ко всем инсталляциям, которым присвоен профиль



ВАЖНО ЗНАТЬ



Коммуникация между консолью и инсталляциями **безопасна** благодаря шифрованию каналов связи и взаимной аутентификации

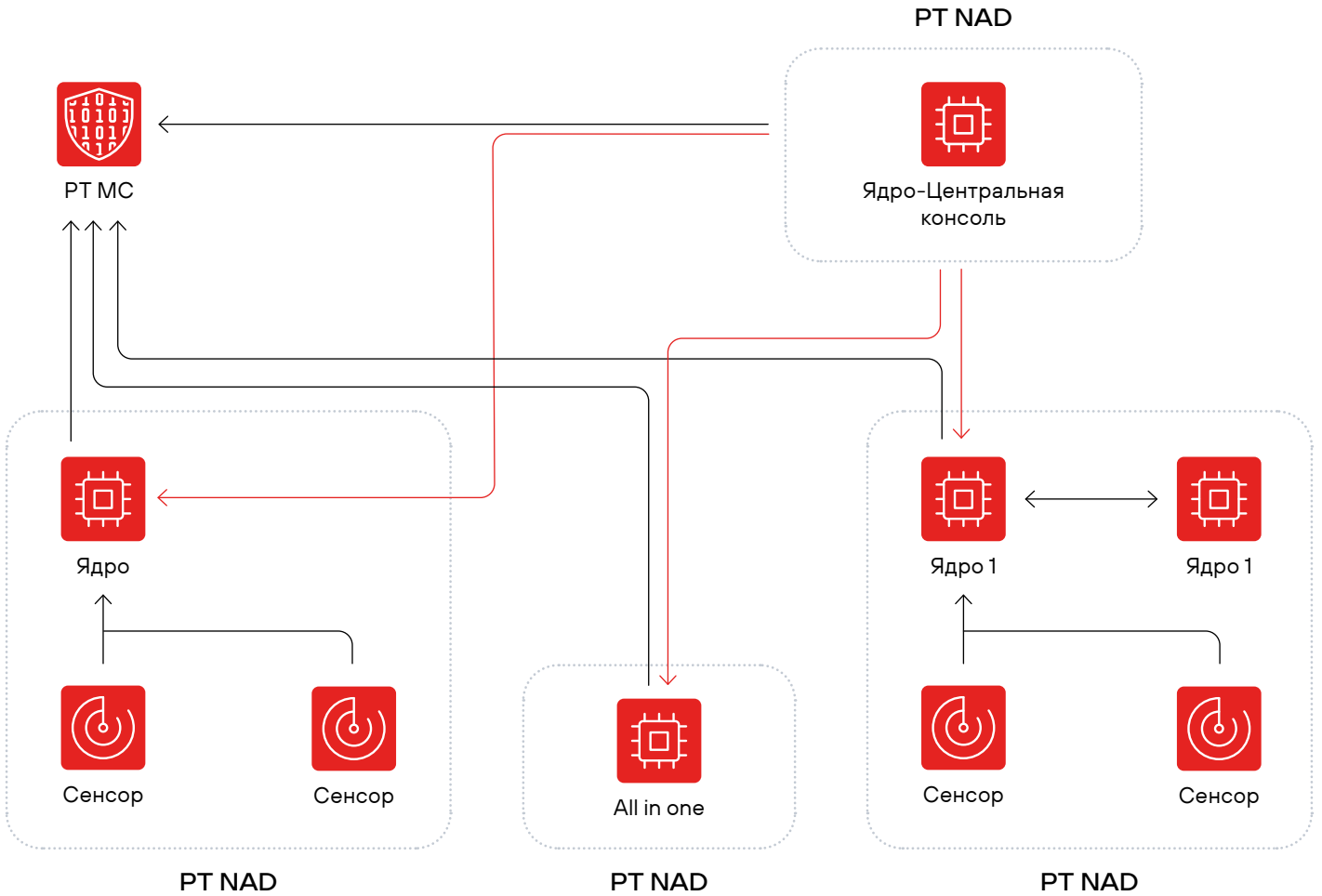


Центральная консоль **не хранит данные** из подключенных PT NAD – в случае нарушения IP-связности мониторинг не остановится



Аппаратные требования к центральной консоли **не зависят от количества** подключенных инсталляций

СХЕМА РАБОТЫ ЦЕНТРАЛЬНОЙ КОНСОЛИ



РЕЗУЛЬТАТ ДЛЯ ВАС



Сокращение времени расследования инцидентов за счет получения всей необходимой информации в едином интерфейсе



Повышение эффективности SOC — не нужно тратить время на переключение между инсталляциями



Централизация мониторинга — теперь одна команда может мониторить много инсталляций одновременно



Присоединяйтесь
к комьюнити **PT NAD**