

UDV NTA

Ключевой элемент сетевой видимости
и раннего обнаружения кибератак



UDV Group – ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

200+

разработчиков в штате

Распределённая команда со штаб-квартирой в Екатеринбурге

1000+

инсталляций

Проекты по защите АСУ ТП и корпоративных сетей

10+

патентов

Собственный исследовательский центр в области кибербезопасности

10

лет на рынке

Подтвержденный опыт интеграции в крупных предприятиях нефтегазовой отрасли, энергетики, металлургии и других

Текущие вызовы кибербезопасности

Каждая компания находится под перманентной угрозой от профессионалов

[Число кибератак в России и в мире](#)

Среднее время реагирования на угрозу – более 270 дней

2/3 нарушений ИБ пропускается специалистами

[IBM Security Report 2023](#)

Время реагирования определяет ущерб

Реагирование спустя 200 дней после инцидента увеличивает стоимость восстановления более чем на \$1 млн

[IBM Security Report 2023](#)

Защищать сеть снаружи уже недостаточно – необходимо видеть происходящее внутри, чтобы **быстро и эффективно реагировать на угрозы**

UDV NTA

UDV NTA — система анализа сетевого трафика для обнаружения кибератак, которая позволяет видеть активность как на периметре, так и внутри сети.

Продукт помогает специалистам по ИБ выявлять подозрительную активность и предотвращать атаки до их завершения, минимизируя или полностью исключая потенциальный ущерб и повышая уровень безопасности сети.

Возможности UDV NTA



Определение поверхности потенциальной атаки

Задача

Понять, что именно планируем защищать и какие сервисы сейчас активно используются, чтобы выявить слабые места и оценить имеющиеся риски

Как?

UDV NTA предоставляет:

- механизмы выявления активов из копии сетевого трафика
- визуализацию карты сети
- глубокий анализ сетевого трафика до уровня приложений

Результат

- {✓} Снижается риск появления «слепых зон» в инфраструктуре
- {✓} Уменьшается поверхность атаки за счёт полной сетевой прозрачности

Проверка векторов атаки

Задача

Размышляя как нарушитель, проверить возможные варианты точек входа в инфраструктуру и дальнейших шагов

Как?

UDV NTA предоставляет информацию о незащищенных участках инфраструктуры (например, учетные данные в открытом виде или избыточный удаленный доступ)

Результат

{✓} Снижается количество или полностью исключаются уязвимые места, которые могут привести атакующего к ключевым системам

Раннее обнаружение и локализация угроз ИБ в реальном времени

Задача

Основная задача при реализации угрозы — понять поведения и замысел нарушителей на протяжении всей цепочки кибератак

Как?

UDV NTA объединяет обнаружение на основе IDS или внутренних механизмов с контекстом на основе глубокого анализа сети, чтобы быстро подтвердить или опровергнуть оповещение

Результат

- {✓} Снижается среднее время реакции на атаку (MTTR)
- {✓} Предотвращается возможность повторного проникновения

Выявление скрытых угроз

Задача

Усилить проактивный поиск угроз и достоверно оценивать их

Как?

Благодаря встроенным модулям машинного обучения, UDV NTA производит статистический анализ, акцентируя внимание на подозрительных взаимодействиях

Результат

- {✓} Выявляется туннелирование протоколов
- {✓} Выявляются устройства, использующие программное обеспечение для подключения сгенерированным доменам (DGA)

Снижение рисков ИБ при работе с поставщиками услуг

Задача

Учесть риски ИБ при проведении работ подрядными организациями, на которые не распространяется политика ИБ компании

Как?

UDV NTA позволяет контролировать доверенные другим организациям доступы для проведения работ и сигнализировать при наличии кибератаки

Результат

{✓} Улучшается видимость работ в цепочке поставок

Сценарии применения UDV NTA

Соответствие законодательным требованиям и регулятивным нормам

{✓} 152 ФЗ

{✓} 187 ФЗ

{✓} NIST SP 80061 R2

{✓} ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций

{✓} Решение задачи импортозамещения:
UDV NTA включен в Реестр
российского ПО (реестровая запись
№27786 от 06.05.2025)

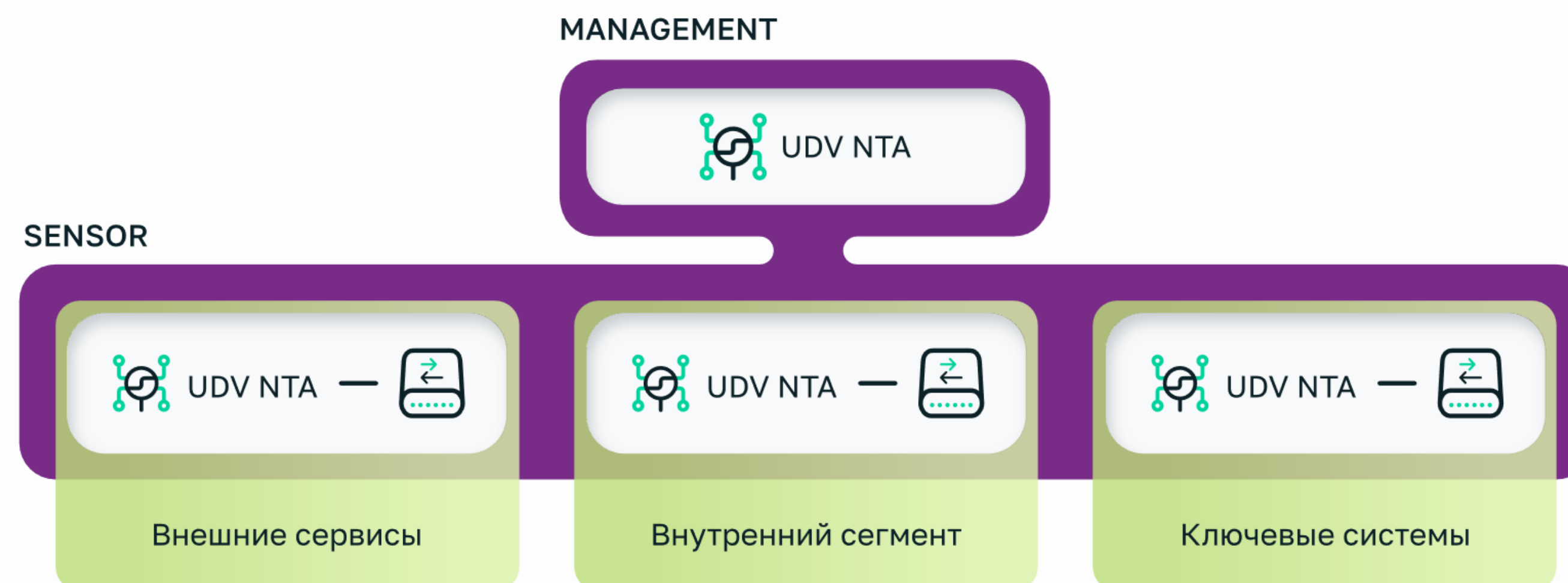
Архитектура UDV NTA

MANAGEMENT

- Нормализация и корреляция событий
- Формирование инцидентов и отображение панелей мониторинга
- Хранение метаданных сетевого трафика
- Централизованное управление сетью сенсоров

SENSOR

- Анализ сетевого трафика
- Разбор протоколов передачи данных
- Запись и хранение копии сетевого трафика
- Хранение полученных из сети файлов
- Прием событий ИБ от узлов сети



Преимущества UDV NTA

Оптимальный баланс ресурсов и стоимости

UDV NTA эффективно использует вычислительные ресурсы и требует на ~50% меньше по сравнению с аналогичными решениями

Объектный подход к анализу сети

Автоматически определяет устройства и связывает их с сетевыми действиями

Объединение данных для точного обнаружения угроз

Максимальное покрытие за счет обработки и корреляции с сетевой активностью событий ИБ от устройств в сети

Максимальный контекст

Позволяет в пару кликов перейти к деталям сетевого события и исследовать специфичные поля протоколов приложений для проактивного поиска угроз

С чего начать?

Консультация

Напишите нам на commercial@udv.group.
Мы свяжемся с вами, обсудим ваши задачи и требования

Персональная демонстрация

Проведем презентацию функционала и интерфейса продукта

Тест-драйв продукта

Дадим доступ к тестовой инфраструктуре и расскажем о возможных сценариях применения продукта

Пилотный проект

Развернем программное обеспечение в выделенном участке вашей сети, поможем с настройками и запуском



Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group

Telegram

@udv_group

