udv|group

UDV NTA 2.0

Интеллектуальная система анализа сетевого трафика для раннего обнаружения кибератак. Дополняет сетевую видимость пониманием бизнес-контекста и формирует покрытие сети 360°

Актуальные угрозы ИБ требуют полной видимости сети

01

Защита периметра больше не гарантирует безопасность

Злоумышленник может изначально находиться внутри инфраструктуры или получить доступ через легитимную учетную запись

02

Продолжительные, скрытые и целенаправленные атаки

После проникновения злоумышленники могут долго находиться в инфраструктуре, оставаясь незамеченными для традиционных средств защиты

03

Теневые активы становятся потенциальными точками проникновения

Площадь атаки увеличивается за счет использования сотрудниками нелегитимных облачных сервисов, общедоступных нейросетей, BYOD-устройств

Какие задачи решает?

Устранение слепых зон в инфраструктуре

Обнаружение неавторизованных устройств в сети и мониторинг сетевой безопасности в сегментах, где невозможно использование агентов

Обнаружение атак и расследование

Максимальный контекст по инциденту за счет корреляции событий ИБ от хостов с данными об их сетевых взаимодействиях, применения актуальной экспертизы UDV Threat Intelligence и ретроспективный анализ копии сетевого трафика

Сокращение времени реагирования

Интеллектуальный помощник помогает приоритизировать инциденты, дает рекомендации по реагированию с учетом контекста конкретного бизнеса (активы, процессы и регламенты) и формирует отчеты

Преимущества UDV NTA

01 Использует на 50% меньше вычислительных ресурсов

UDV NTA 2.0 требует на ~50% меньше CPU и RAM по сравнению с аналогичными решениями при сопоставимом уровне анализа трафика

02 Максимальная видимость сети

- Корреляция событий ИБ от хостов с их сетевой активностью «из коробки»
- Индикация любого протокола уровня приложения по запросу пользователя

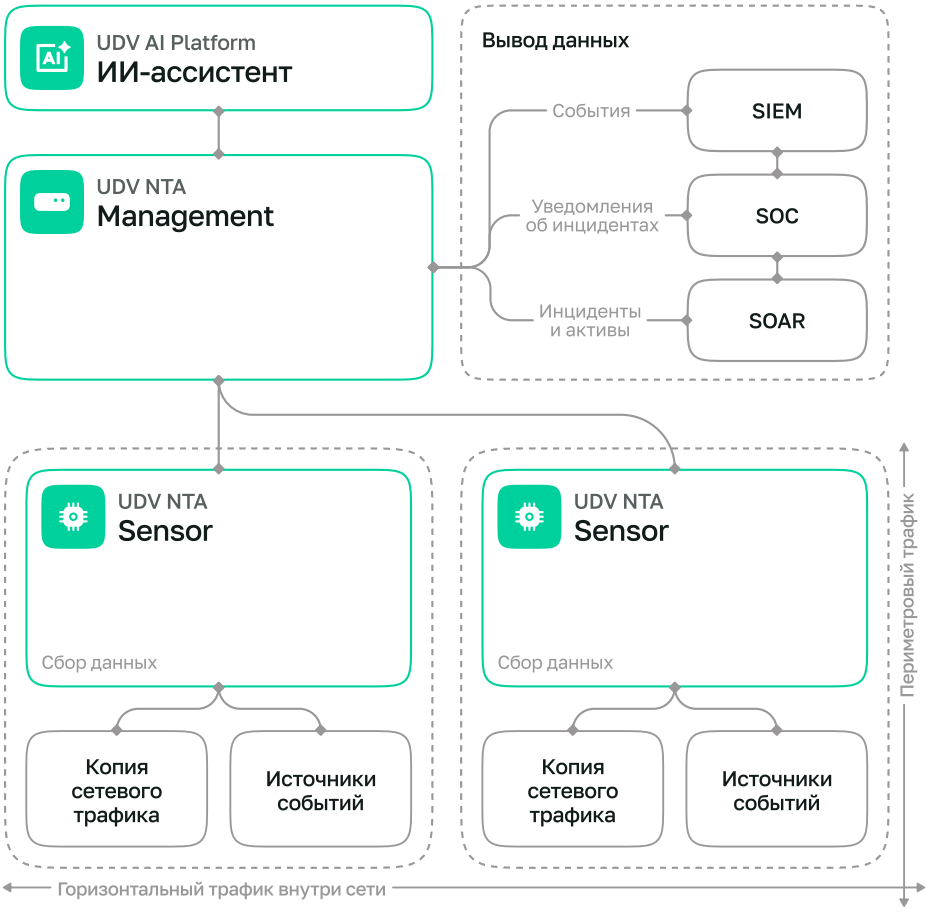
03 Учитывает контекст бизнеса

- Помогает приоритизировать инциденты и дает рекомендации по реагированию — с учетом информации об активах, бизнес-процессах и регламентов вашей компании
- Формирует персонализированные отчеты за пару минут

04 Обнаруживает актуальные угрозы и быстро локализует инцидент

- Автообновляемая экспертиза вендора UDV Threat Intelligence и возможность подключить собственную базу индикаторов компрометации
- Переход в 2 клика от инцидента к карте сети с визуализацией затронутых узлов и их сетевых взаимодействий

Архитектура решения



UDV AI Platform
ИИ-ассистент

- Разбор инцидента и рекомендации по реагированию с учётом бизнес-процессов компании
- Отчёты по запросу — от сводки за смену до поиска закономерностей за месяц
- Работа с продуктом без глубокой экспертизы в NTA
- LLM-независимость: локальная модель или маскирование данных

UDV NTA
Management

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

UDV NTA
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

Лицензирование

Стоимость лицензии на ПО складывается из базовой части (фиксированная сумма в зависимости от пропускной способности анализируемого трафика) и количества доп. точек съема трафика (фиксированная сумма за точку). ИИ-ассистент лицензируется отдельно.

Хотите обсудить ваш проект или договориться о демонстрации?

www.udv.group