

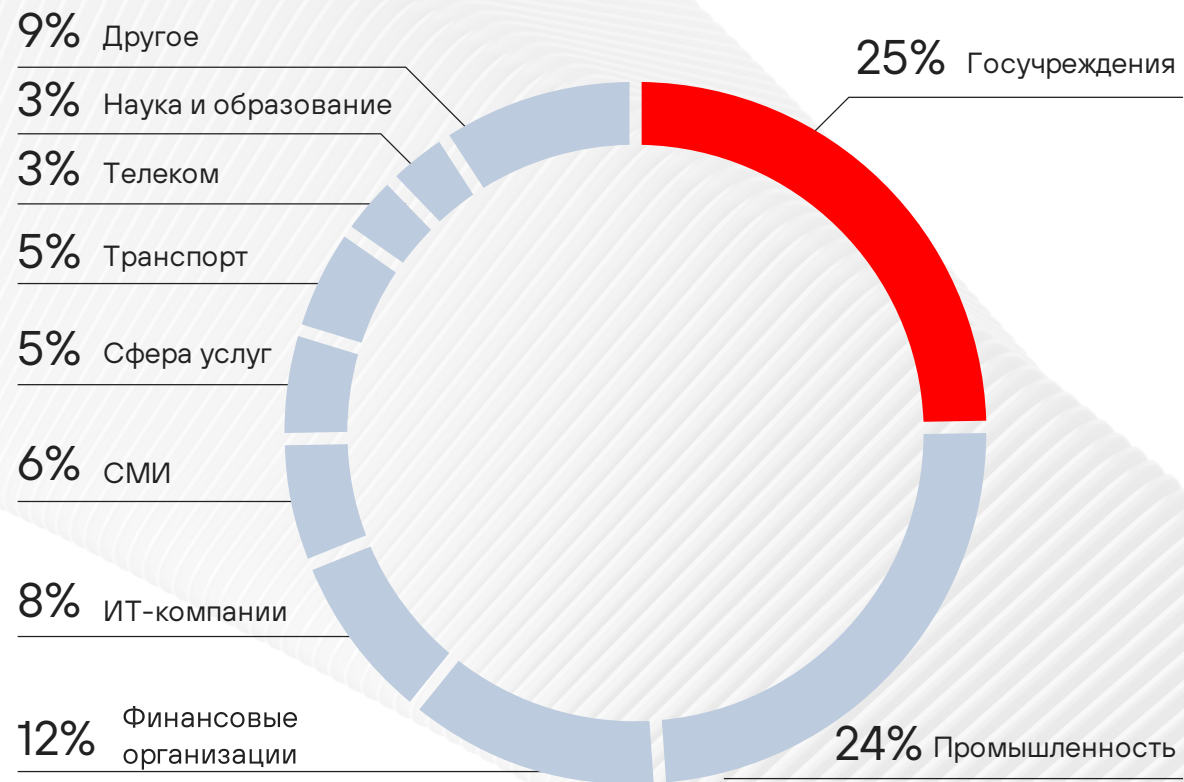
Обнаружение высоко- квалифицированных атак внутри сети

Киберагрессия

- С 2022 года Россия находится в условиях кибервойны.
- Каждая третья атака является целевой.
- Утечки данных помогают преступникам подготовиться к последующим АРТ-атакам и нанести ущерб бизнесу.



Успешные атаки



Киберагрессия

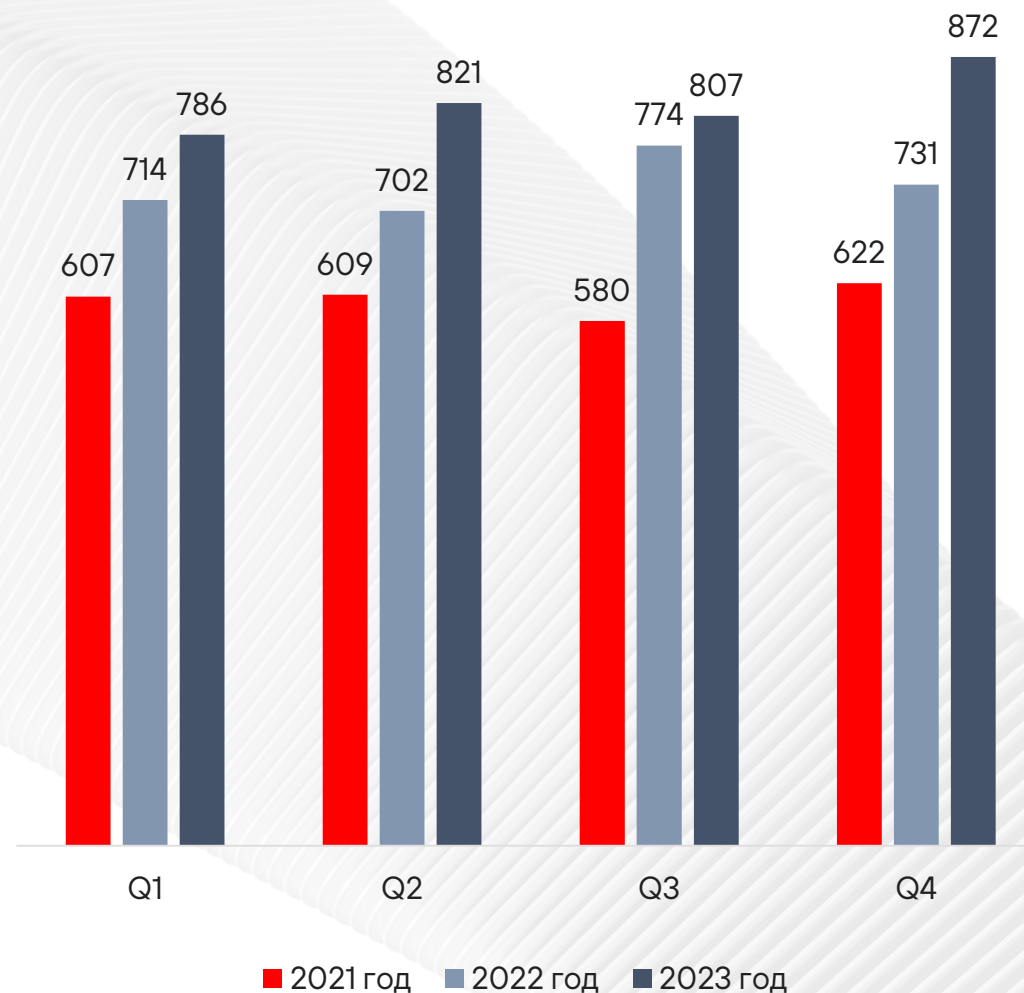


Последствия

- Утечки государственных секретов и коммерческой тайны
- Нарушение основной деятельности и остановка бизнеса
- Шантаж, вымогательство



**Необходим инструмент ИБ,
который быстро внедряется
и точно выявляет сложные угрозы**



PT Network Attack Discovery

1

Точно выявляет сложные сетевые атаки и сокращает время обнаружения хакеров до 1 часа

2

Упрощает расследования инцидентов и показывает слабые точки в сети

3

Сокращает время реагирования на приоритетные угрозы службе ИБ

PT NAD — для решения задач ИБ

Контроль активов



Инвентаризует узлы по сетевому отпечатку



Обнаруживает нарушения регламентов ИБ

Нетипичное поведение узлов



Находит аномалии в сетевом трафике



Профилирует сетевые узлы и определяет приложения

180 техник и тактик атакующих



Обнаруживает попытки эксплуатации уязвимостей и видит факты их успешной эксплуатации



Выявляет хакерские инструменты и перемещение атакующих внутри периметра



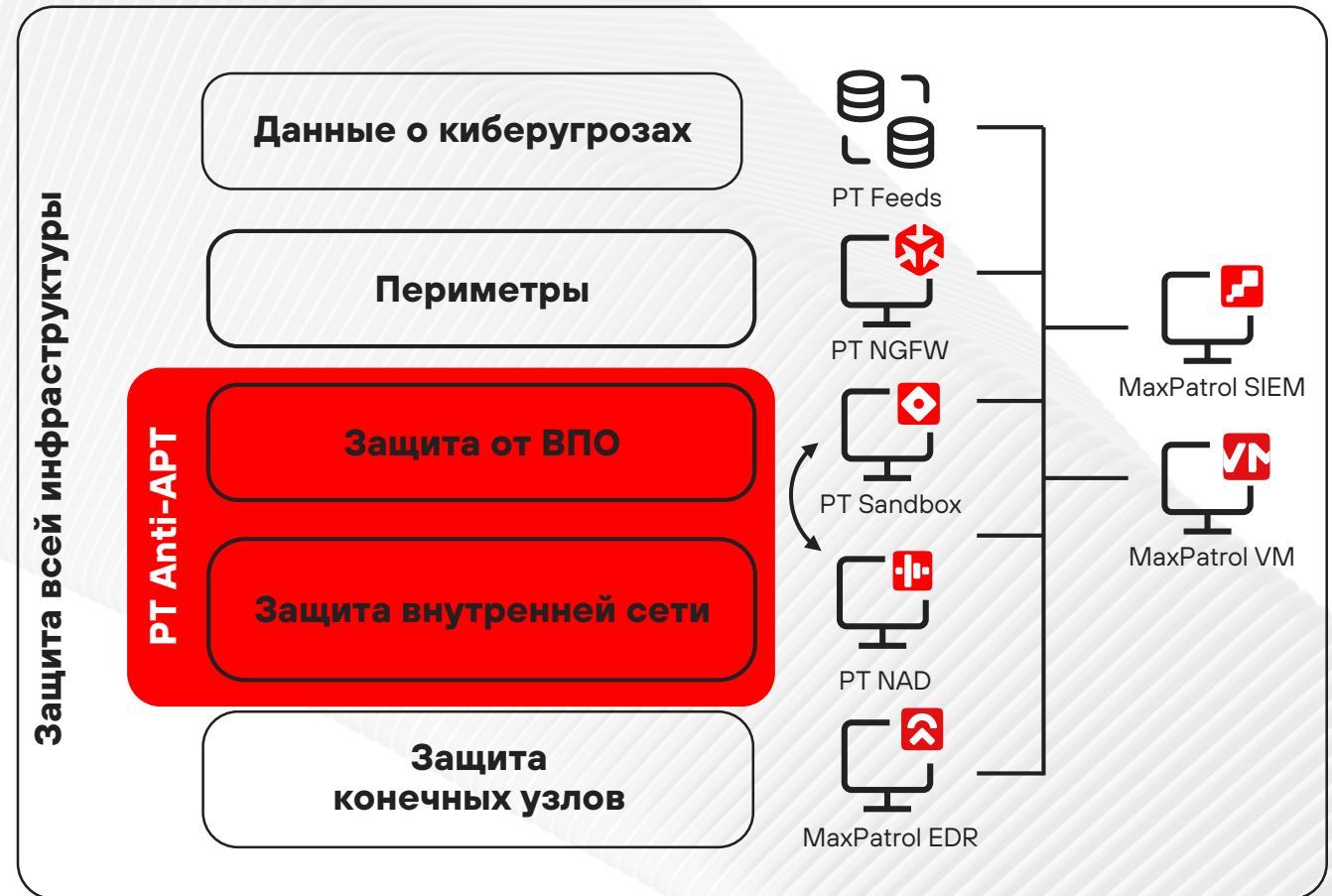
Определяет угрозы в зашифрованном трафике



Определяет зараженные узлы и подключения к C2

PT NAD — идеальное дополнение к SIEM и EDR

- Дополняет EDR, закрывая слепые пятна на уровне сети
- Обогащает SIEM-систему сетевым контекстом и ускоряет реагирование
- PT NAD входит в тройку флагманских продуктов Positive Technologies



↻ PT Sandbox производит анализ файлов и возвращение вердиктов, передаваемых из PT NAD, а также в почтовом, сетевом и веб-трафике.

PT NAD – ЭТО ...

**Обнаружение атак
и аномалий**

Правила
и репутационные
списки

Поведенческие
и статистические
модули

Ретроспективный
анализ

Машинное обучение

Расследование

Сетевые связи

Профилирование
узлов

Импорт
и экспорт сырого
трафика

Воспроизведение
трафика

**Проактивный поиск
угроз**

Язык запросов

Метаданные

Сырой трафик

Извлечение объектов
из трафика

Экспертиза

Исследование новейших
инструментов, техник
и тактик атакующих

Расследование кибератак

Мониторинг
APT-группировок

Передовые технологии

Уникальная технология DPI для детального разбора трафика

Экосистемность

Интеграция с MaxPatrol SIEM, PT Sandbox,
PT XDR, PT Threat Intelligence Feeds

Интеграция с продуктами других вендоров

Отличия PT NAD от других систем сетевой безопасности

	PT NAD (класс NTA/NDR)	IDS	IPS (NGIPS)	NGFW/UTM
Методы выявления атак	Статический, статистический и поведенческий анализ сессий, профилирование узлов и поиск отклонений, машинное обучение	Статический анализ	Статический и поведенческий анализ, машинное обучение	Статический и поведенческий анализ, машинное обучение
Автоматическая блокировка атак	Нет	Нет	Да	Да
Выявление аномалий, исследование подозрительной активности и приоритизация данных (улик/следов компрометации)	Да	Нет	Нет	Нет
Работа с шифрованным трафиком	Альтернативные методы	Нет	Использование MITM («человек посередине»)	Использование MITM («человек посередине»)
Обнаружение атак на контроллер домена	Да	Нет	Нет	Частично (на основе политик безопасности)
Обнаружение перемещения хакеров внутри периметра	Да	Нет	Нет	Нет
Проактивный поиск угроз (threat hunting)	Да	Нет	Нет	Нет
Возможность расследований на основе метаданных и копии трафика	Да (хранит все сессии, вне зависимости от того, обнаружена угроза или нет)	Нет	Частично (только в случае выявления атак)	Частично (только в случае выявления атак)
Извлечение файлов из трафика и передача их в сторонние системы	Да	Да	Да	Да

Кейс: расследование атаки шифровальщика



С помощью PT NAD служба ИБ:

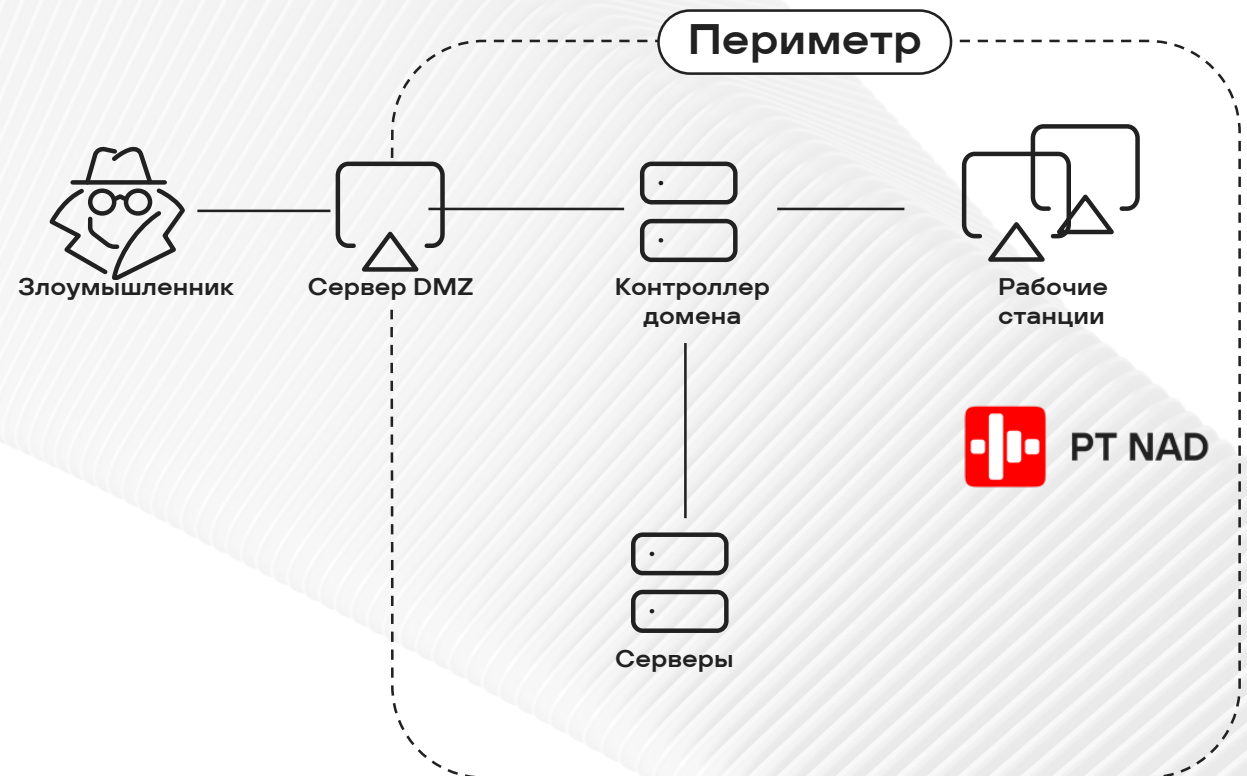
- выявила массовые аномалии во время шифрования домена
- определила предполагаемую точку проникновения и все ресурсы, которыми завладели злоумышленники
- обнаружила шаги атакующих на всем протяжении атаки



Ваших соседей пошифровали!
Прямой репортаж с места событий

[Читать статью](#)

Шифрование инфраструктуры



Кейс: обнаружение АРТ-атаки



Обнаруживает попытки эксплуатации уязвимостей и проверяет факты успешной компрометации узла



Выявляет применение хакерского инструментария для сетевой разведки и перемещения внутри периметра



Определяет подбор учетных записей внутри сети



Обнаруживает признаки закрепления атакующих в инфраструктуре



Точно обнаруживает атаки внутри корпоративного домена, которые ведут к реализации недопустимых для бизнеса событий

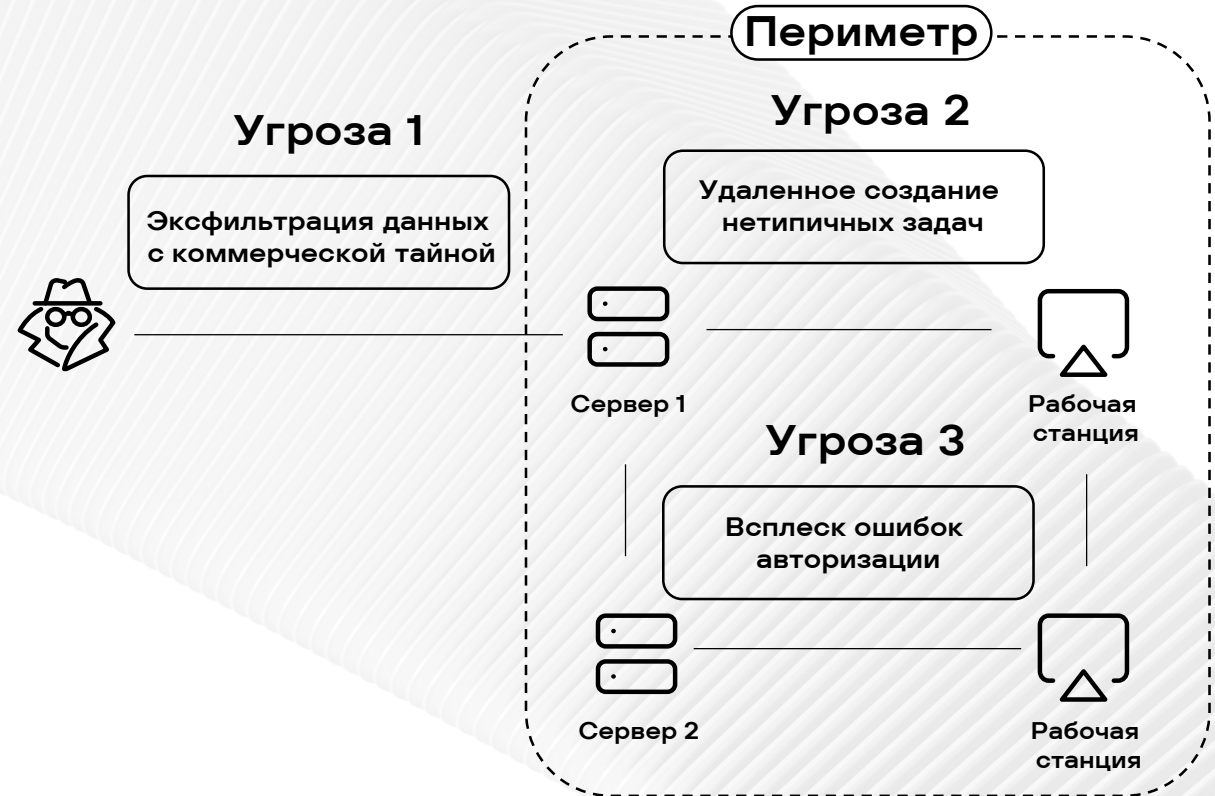
Кейс: поиск аномалий



PT NAD

Профилирует поведение всех сетевых устройств и находит **отклонения (аномалии)** от типичного поведения с помощью передовых технологий машинного обучения

Нетипичное поведение устройств внутри сети невозможно обнаружить с помощью NGFW, UTM и IPS/IDS



Варианты поставки и модель лицензирования



Поставка

Hardware appliance

- Развертывание на физическом сервере
- Производительность — до 10 Гбит/с на одном сенсоре

Virtual appliance

- Развертывание на виртуальной машине
- Производительность — до 1 Гбит/с на одном сервере



Годовое лицензирование

Базовая лицензия

- Определяется по пропускной способности (1, 2, 5, 10, 20, 50 или 100 Гбит/с)

Инфраструктурные лицензии

- Ядро системы
- Сенсоры для разбора протоколов и анализа трафика (до 1000, 5000 и 10 000 Мбит/с)

Опыт клиентов



Антон Мельник,
начальник управления ИБ
АО «ОЭК»

PT NAD — полезный инструмент для мониторинга безопасности сети. После внедрения продукта мы почти моментально увидели первые результаты, которые помогли нам снизить риски безопасности и улучшить защищенность инфраструктуры.



ГЕНБАНК

Дмитрий Ларин,
начальник управления ИБ
АО «Генбанк»

PT NAD зафиксировал 5700 потенциальных угроз, включая 90 угроз высокой опасности. При этом результаты мониторинга сети «Генбанка» не выявили успешных проникновений в сеть организации.

Команда РТ NAD



Старт разработки

2015



Сотрудников

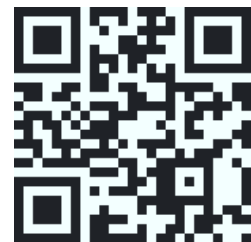
100+

- R&D
- PT ESC
- Data Science



Человеко-лет

>200



Телеграм -чат РТ NAD
t.me/PTNADChat



Проверь свою сеть

 Знакомство с продуктом