Вебмониторэкс

защита веб-приложений и API

API: от аудита к защите

Тимофей Горбунов
Сергей Одинцов

История компании

Вебмониторэкс
защита веб-приложений и API

Основание компании в РФ

2013

wallarm

Выход на международный рынок

2016

Отделение российского бизнеса в независимую компанию

2022

Вебмониторэкс
защита веб-приложений и API

11 лет Опыта разработки решений по защите веб-приложений

>50% R&D остались в России в команде Вебмониторэкс

Вэбмониторэкс в 2025 году

Вебмониторэкс
защита веб-приложений и API

80+
Технологических интеграций

60+
Технических специалистов среди сотрудников

200+
Реализованных проектов в России

Топ-100
Крупнейших ИБ-компаний в России

Технологическая база международного уровня

Продукты в реестре российского ПО

Техническая поддержка 24/7/365

Открытость и обратная связь по всем продуктам

Технологический и инновационный лидер, ориентированный на практический результат

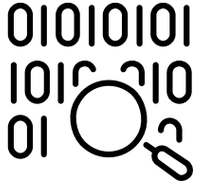
Платформа «Вебмониторэкс»

Защищает от атак на веб-приложения, микросервисы и API

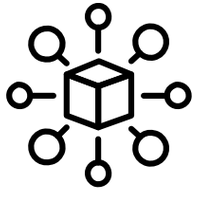
Вебмониторэкс
защита веб-приложений и API

Продукт ПроWAF

Firewall
веб-приложений

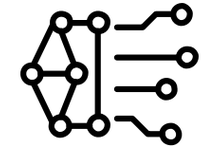


Сканер
периметра и уязвимостей

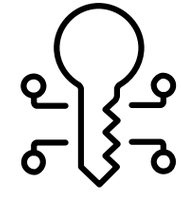


Модуль
перепроверки атак

Линейка продуктов ПроAPI



ПроAPI Структура



ПроAPI Тестирование

ПроAPI Защита

Вебмониторэкс
защита веб-приложений и API

01

Проблематика в защите API

Что обычно «смотрит наружу»

Вебмониторэкс
защита веб-приложений и API

- Публичные веб-приложения
- Корпоративный сайт
- Внешние API

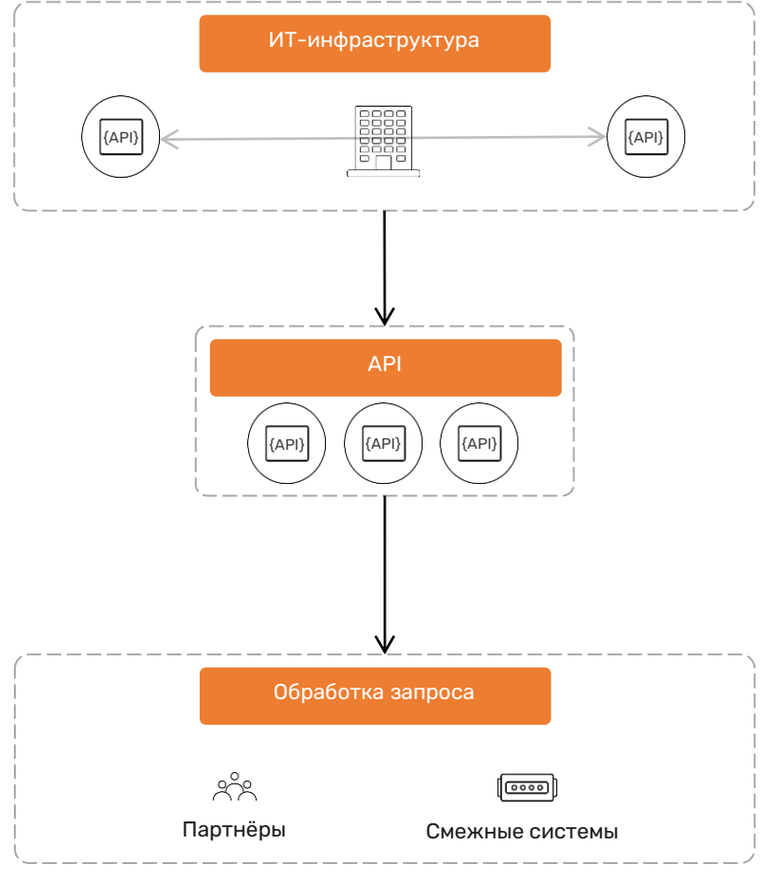
- Внутренние ресурсы для дочерних компаний и подрядчиков, выходящие за периметр
- Пользовательские и административные веб-интерфейсы business-critical систем
- **Неконтролируемое кросс-системное взаимодействие через API**

Как применяется

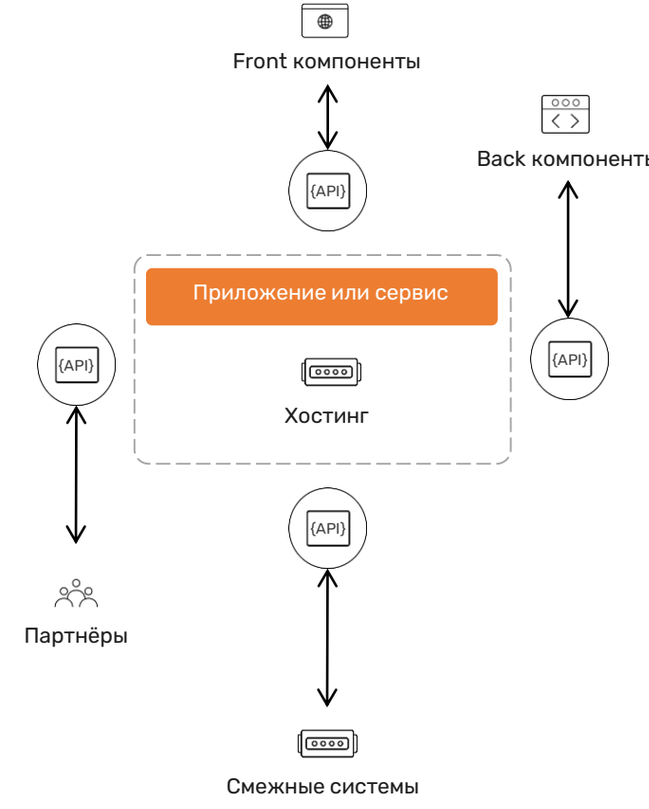
Вебмониторэкс
защита веб-приложений и API

Для пользователя

Для компании



Для разработчика



Основные проблемы

Вебмониторэкс
защита веб-приложений и API

Много доступных API

Много версий API с разными параметрами, нет понимания, какие точки несут наибольшую угрозу

Нет наблюдаемости

Непонятно что происходит с API, какие изменения, что происходит от момента дизайна до публикации

Нет инструмента автоматизации

Без требований к API не получается организовать процесс их контроля, при наличии требований – не получается автоматизировать

Основная угроза: доступность данных

Вебмониторэкс
защита веб-приложений и API

Личных данных

Защита персональных, медицинских и банковских данных всегда находится в высоком приоритете, а их утечка ведет к значительным рискам

Бизнес-данных

Изменения в данных, на которых основывается бизнес – наиболее критичная угроза

Конфиденциальных данных

У каждой компании есть данные, раскрытие которых может привести к серьезным репутационным и финансовым потерям

Рост количества API

Вебмониторэкс
защита веб-приложений и API

на 167%

увеличилось количество API
за последний год

66%

организаций управляют более чем 100 API
в 2024 году

в 5 раз

увеличилось количество эндпоинтов
по сравнению с началом 2023 года

59%

организаций управляют более чем 100 API
в 2023 году

Исследование Salt Security

Виды API:

- REST
- SOAP
- RPC
- Web Socket
- GraphQL

Рост атак на API

Вебмониторэкс
защита веб-приложений и API

в 4 раза

увеличилось количество атак на веб-ресурсы российских компаний в 2024 году

Исследование ГК «Солар»

84%

организаций сообщили об инцидентах безопасности API за 2024

Исследование Akamai

Trello Breach
(январь 2024)

Скомпрометированы данные более 15 миллионов пользователей

Dropbox API Keys Breach
(май 2024)

Доступ к токенам аутентификации, данным многофакторной аутентификации, хешированным паролям и информации о клиентах

Dell API Breach
(май 2024)

Доступ к порталу партнёров Dell и 49 миллионам записей клиентов

Cox Communications API Breach
(июнь 2024)

Угроза миллионам модемов, позволяющая манипулировать конфигурациями сети

Что делать?

Вебмониторэкс
защита веб-приложений и API

Инвентаризировать

Собирать полную картину: что, где, как и на каких технологиях работает

Документировать

Создавать Open API Specification (OAS) – важнейший компонент, описывающий работу каждого API, который есть далеко не у всех компаний

Анализировать

Внедрять и использовать на этапе разработки code review, статические анализаторы, линтеры

Тестировать

Автоматизировать тестирование, что позволит проводить его на регулярной основе и выявлять угрозы до релиза

Вебмониторэкс
защита веб-приложений и API

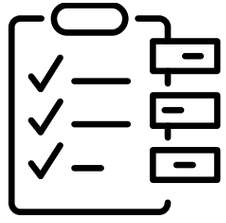
02

Подходы к защите API

Этапы реализации защиты API

Вебмониторэкс
защита веб-приложений и API

Этап I: Знать



- Что есть в текущих API, из чего они состоят
- Какие данные передаются, какие точки используются
- Какие уязвимости и угрозы в API
- Когда происходит что-то аномальное на endpoint

Этап II: Защищать

- Контролировать расхождения с согласованной спецификацией (политикой)
- Заблокировать те endpoint, которые несут угрозу
- Автоматизировать реагирование при обнаружении угрозы (BOLA, обнаружение PII)

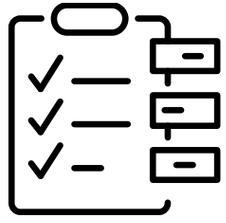
Этап III: Не допускать

- Фиксировать «нормальный» трафик запросов к API
- Блокировать все что не описано в OAS
- Блокировать все запросы с признаком утечки секретов
- Выявлять проблемные endpoint в API (Shadow API)

Результат каждого этапа

Вебмониторэкс
защита веб-приложений и API

Этап I: Знать



- Сформулированы требования к командам разработки и инфраструктуры – политика управления API
- Инструмент отслеживания аномалий в API, первичный контроль цикла разработки
- Структурированная информация об уязвимостях и угрозах API

Этап II: Защищать

- Фиксация расхождений опубликованного и разрабатываемого API
- Автоматизация проверки требований политики API на стадии планирования, разработки и реализации API
- Блокировка эксплуатации уязвимостей до завершения исправлений приложения

Этап III: Не допускать

- Автоматическое соответствие политике управления API
- Полноценный контроль цикла разработки API
- Мониторинг всей цепочки передачи запросов приложений
- Полное доверие функционирующим процессам управления API

Вебмониторэкс
защита веб-приложений и API

03

Компоненты линейки ПроAPI

API – это целый новый мир

Вебмониторэкс
защита веб-приложений и API

ПроAPI Структура

Инвентаризация API, мониторинг изменений

- Визуализация структуры API
- Мониторинг изменений в структуре API
- Выявление наличия чувствительных данных
- Оценка рисков
- Экспорт построенной структуры в файл
- Валидация OAS
- Отслеживание атак на эндпоинты API (BOLA)

ПроAPI Тестирование

Заблаговременное выявление уязвимостей

- Проверка API по OAS
- Фаззинг эндпоинтов и параметров API
- Детектирование DoS-уязвимостей и аномалий
- Поиск инъекций
- Поиск уникальных уязвимостей API

ПроAPI Защита

Валидация трафика API в рамках OAS

- Усиление защиты REST и GraphQL API
- Предотвращение утечек данных
- Валидация JWT токенов
- Обнаружение Shadow API
- Блокировка запросов
- Централизованное управление

Описание процесса

Вебмониторэкс
защита веб-приложений и API

ПроAPI Структура (знать, защищать)

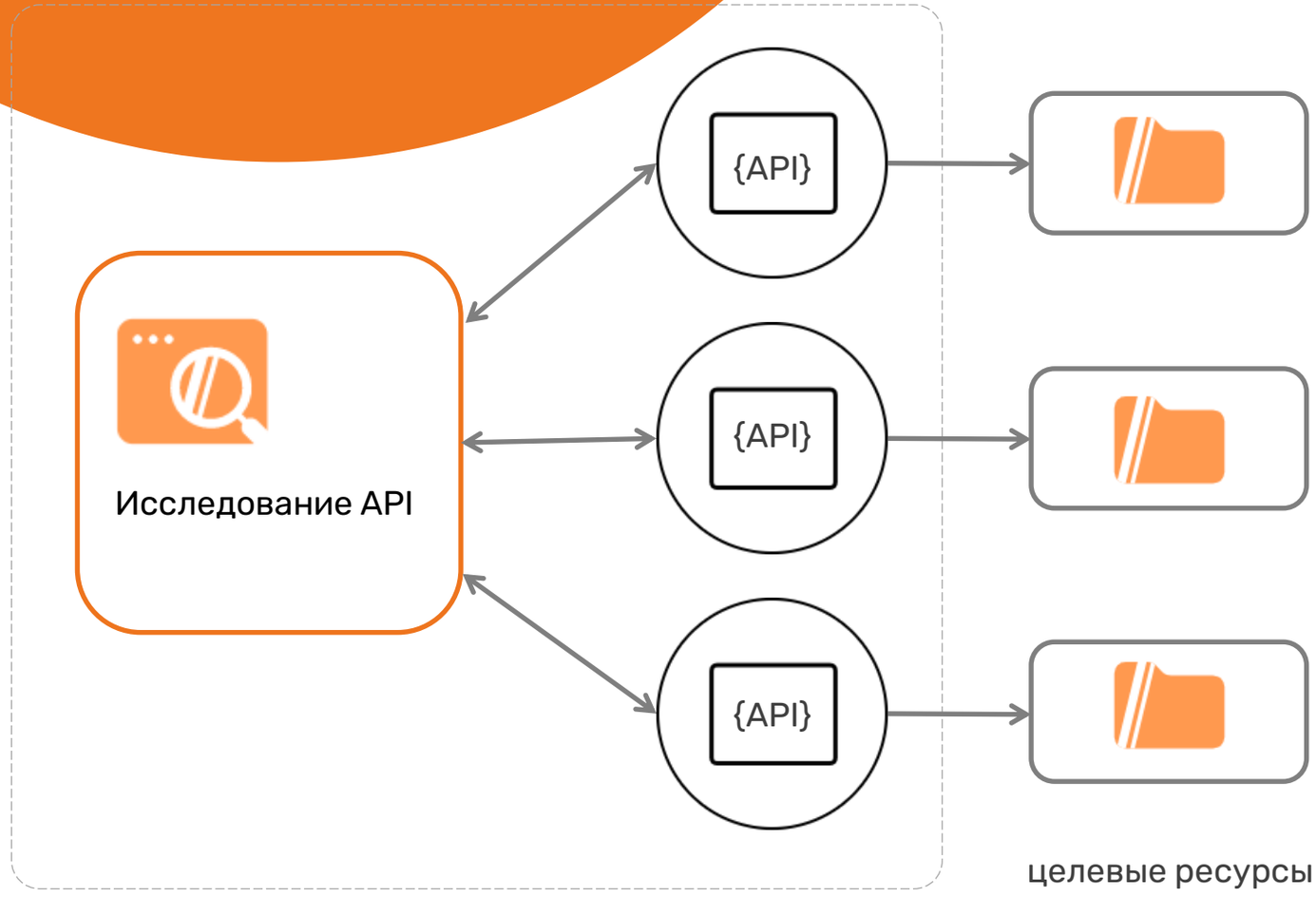
Вебмониторэкс
защита веб-приложений и API

Модуль сбора OAS по трафику, предназначенный для обеспечения визуализации и анализа API, формирования политики API, блокирования наиболее критичных угроз API

- Проверка реальной API по OAS, предоставленной командой разработки (выявить shadow и orphan API)
- Визуализация и анализ корректности построения API (на основе запросов к эндпоинтам и параметрам)
- Инструмент блокирования угроз и уязвимостей для эндпоинтов и маршрутов в API
- Выявление наличия чувствительных данных, передаваемых в эндпоинтах
- Расчет уровня риска для эндпоинтов

Продукт для инвентаризации API

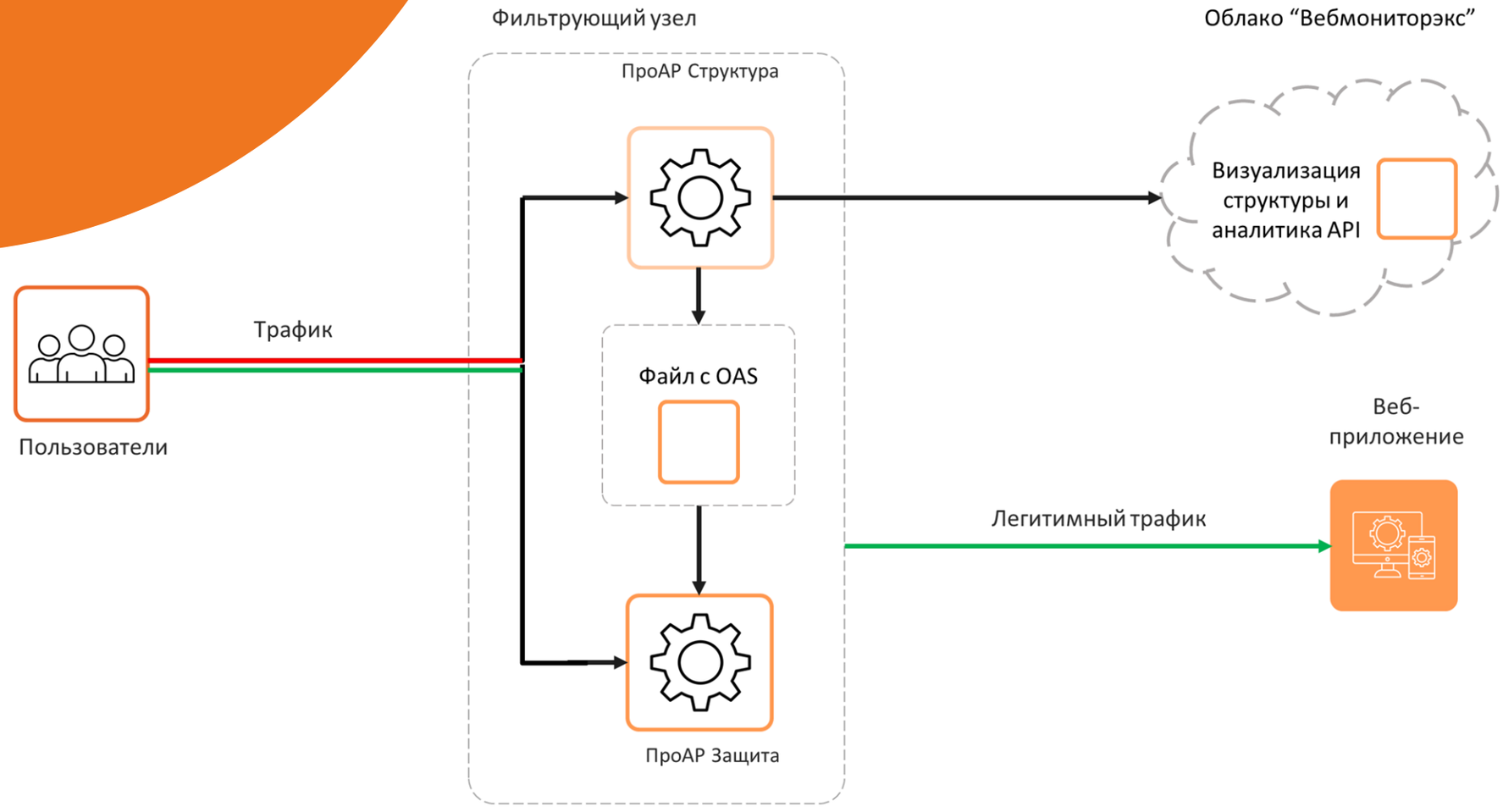
Вебмониторэкс
защита веб-приложений и API



- Механизм защиты API построен на основе **поведенческого ИИ**
- Технология быстро, точно и автоматически **подстраивается к изменяющимся параметрам API,** учитывая особенности каждой конкретной API и контекст ее работы.
- Независимо от того, где работают приложения, на каком технологическом стэке они основаны и сколько трафика потребляет ресурс, вы можете защитить **любые API веб-приложения или веб-сайты** от любых атак.

Схема установки

Вебмониторэкс
защита веб-приложений и API



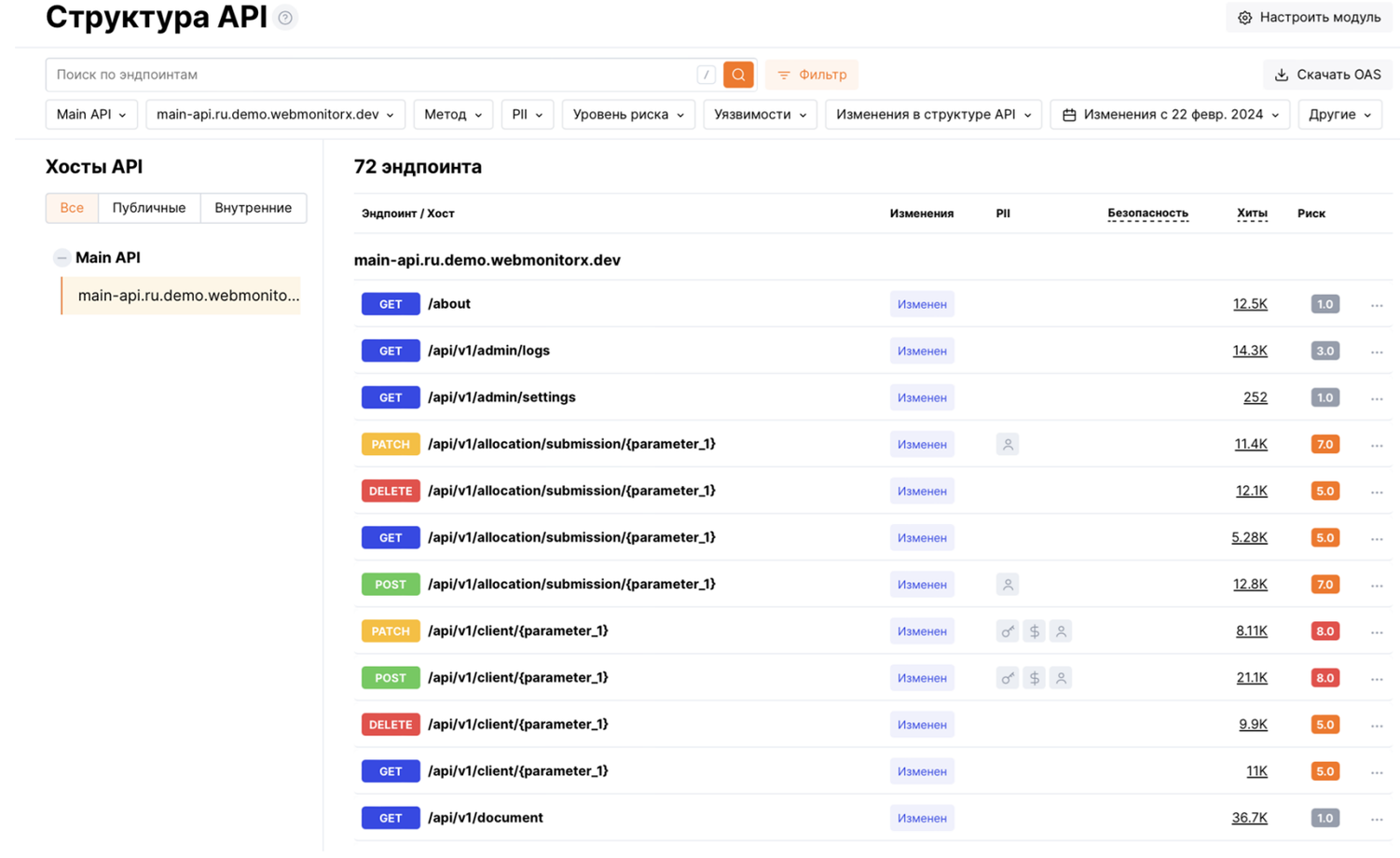
Функции продукта

Вебмониторэкс
защита веб-приложений и API

- Ранжирование эндпоитов по риску
- Показ уязвимостей, ПДн
- Показ точек аутентификации
- Показ потенциальных точек для BOLA
- Выгрузка спецификации или фрагмента
- Навигация по спецификации, именам параметров и типам передаваемых данных, типам содержимого

Планируется реализовать:

- Анализ ответов
- Сбор и отображение статистики по эндпоинтам
- Фиксирование и корректировка спецификации построенной на основе трафика



ПроAPI Тестирование (знать, не допускать, защищать)

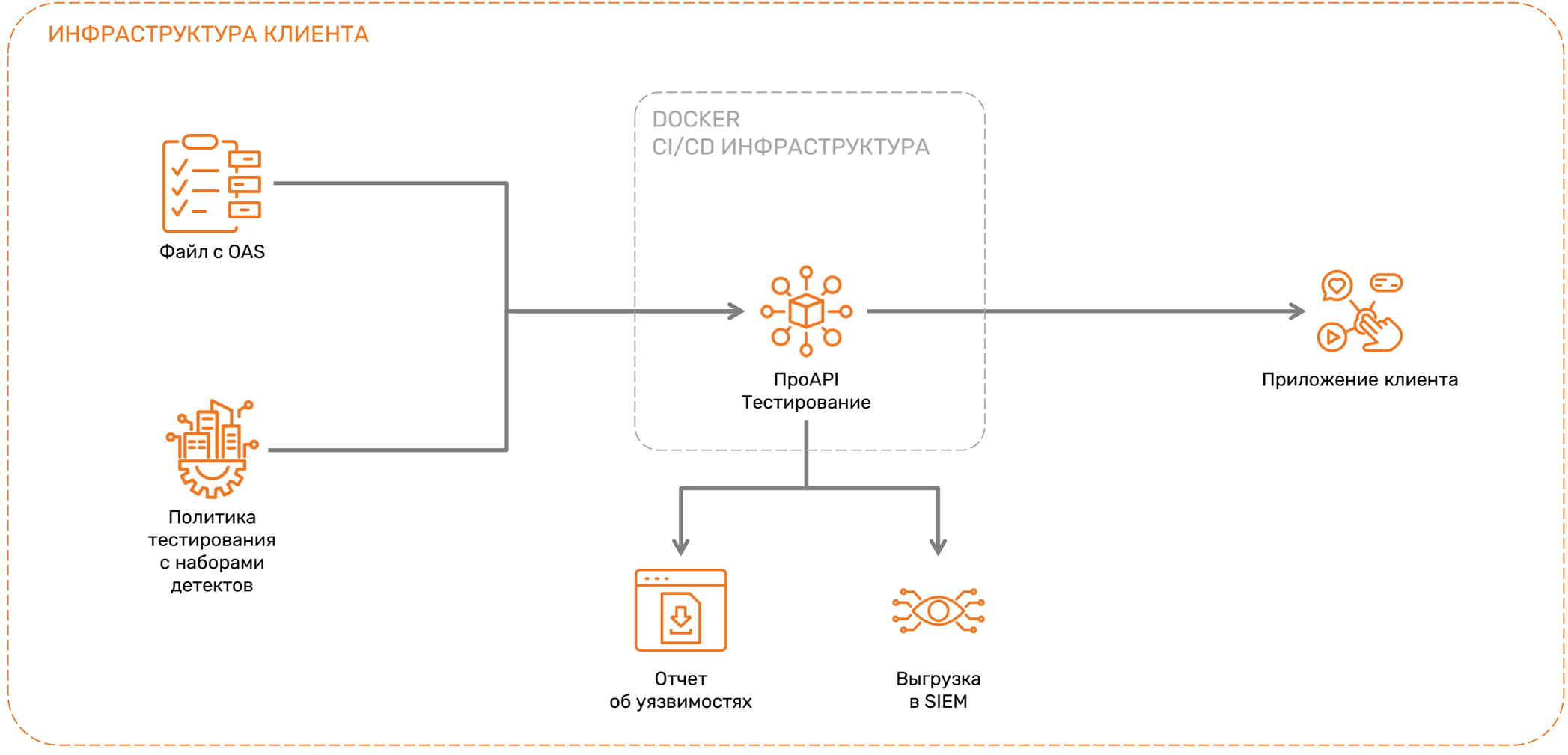
Вебмониторэкс
защита веб-приложений и API

Инструмент для поиска ошибок, уязвимостей, включая 0-day уязвимости в веб-приложениях и API на основе OAS

- Проверка API по OAS, указанной вручную или полученной из ПроAPI «Структуры»
- Нативная интеграция в цикл разработки API, в CI/CD пайплайне
- Фаззинг эндпоинтов и параметров API для покрытия того, что не описано в в OAS
- Поиск инъекций, покрытие OWASP TOP 10 & OWASP
- API TOP 10

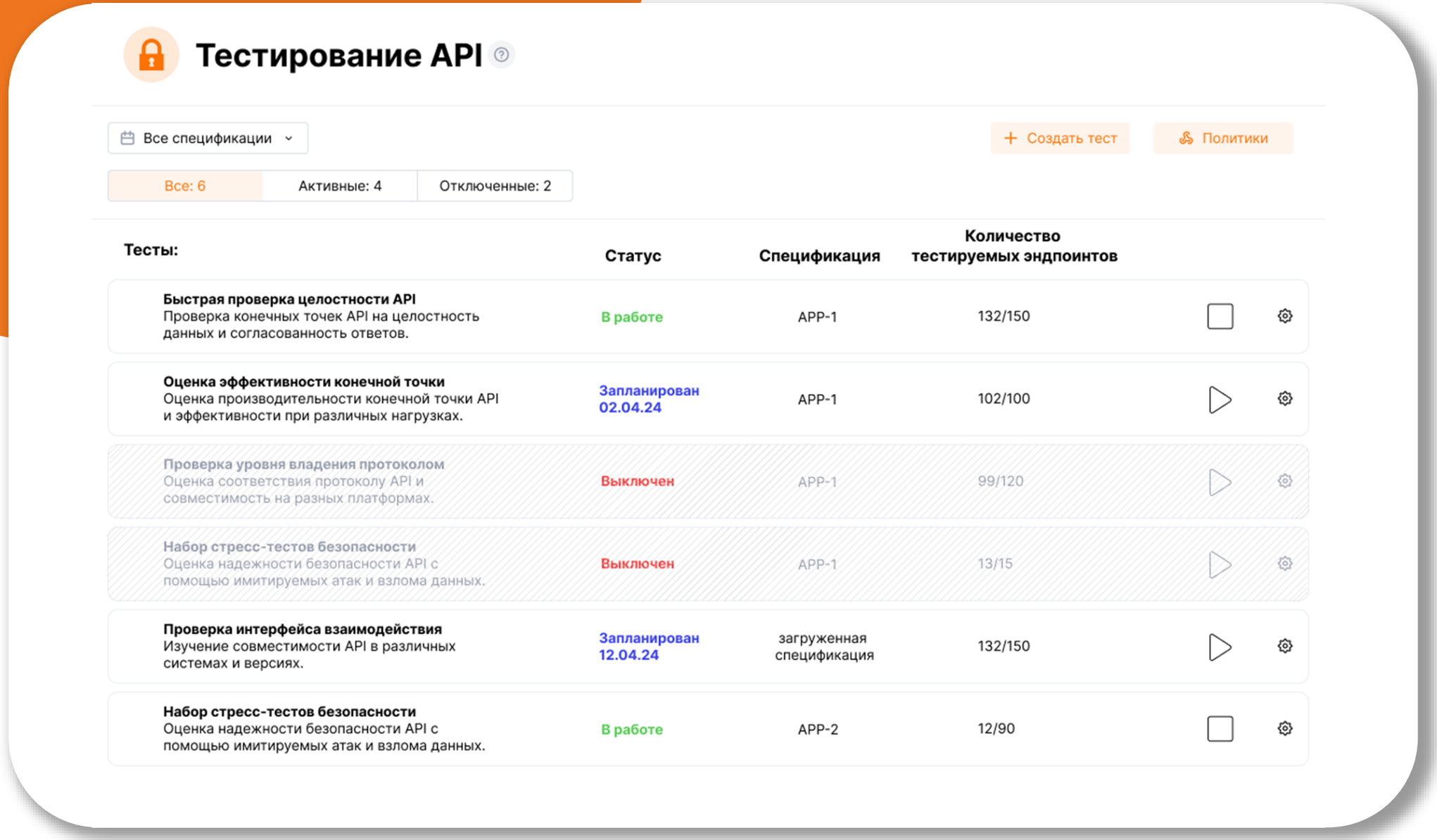
Схема установки

Вебмониторэкс
защита веб-приложений и API



Интерфейс

Вебмониторэкс
защита веб-приложений и API



ПроAPI Защита (знать, не допускать, защищать)

Вебмониторэкс
защита веб-приложений и API

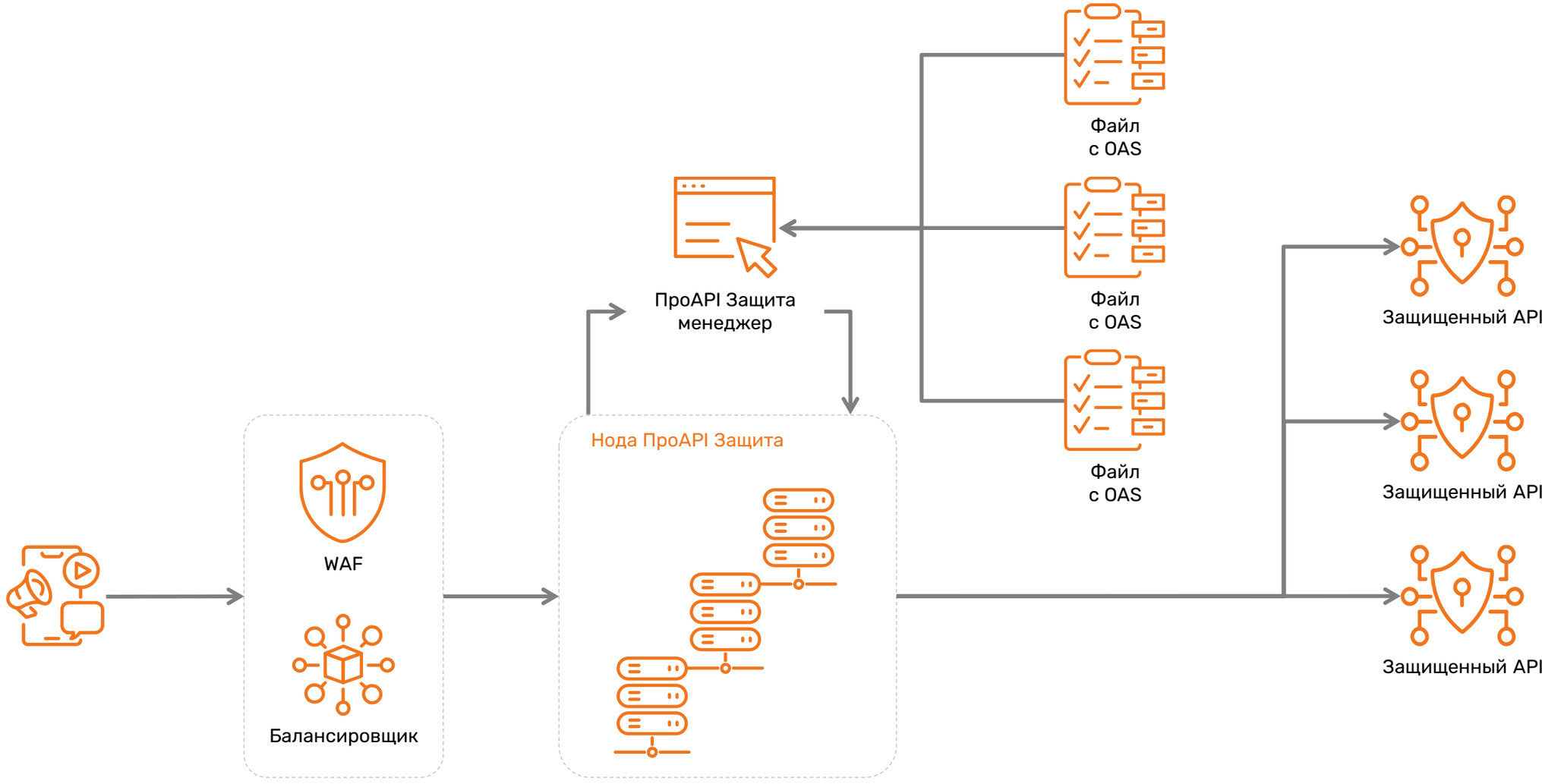
Инструмент для фиксации OAS и валидации запросов к API в рамках позитивной модели

Может быть использован, как локальный компонент, без подключения к облаку, так и с возможностью интеграции с облачным ЛК

- Усиление защиты REST API путем проверки запросов на соответствие заявленной спецификации OpenAPI 3.0 (позитивная модель)
- Предотвращение утечек данных путем проверки ответов приложения на соответствие заявленной спецификации
- Валидация JWT токенов в OAuth 2.0 аутентификации
- Обнаружение Shadow API – теневой версии API, которая может содержать устаревшие, небезопасные, незащищенные, развернутые для отладки методы и эндпоинты и может стать причиной утечек данных и компрометации системы
- Блокировка запросов с утекшими токенами, куками и прочим

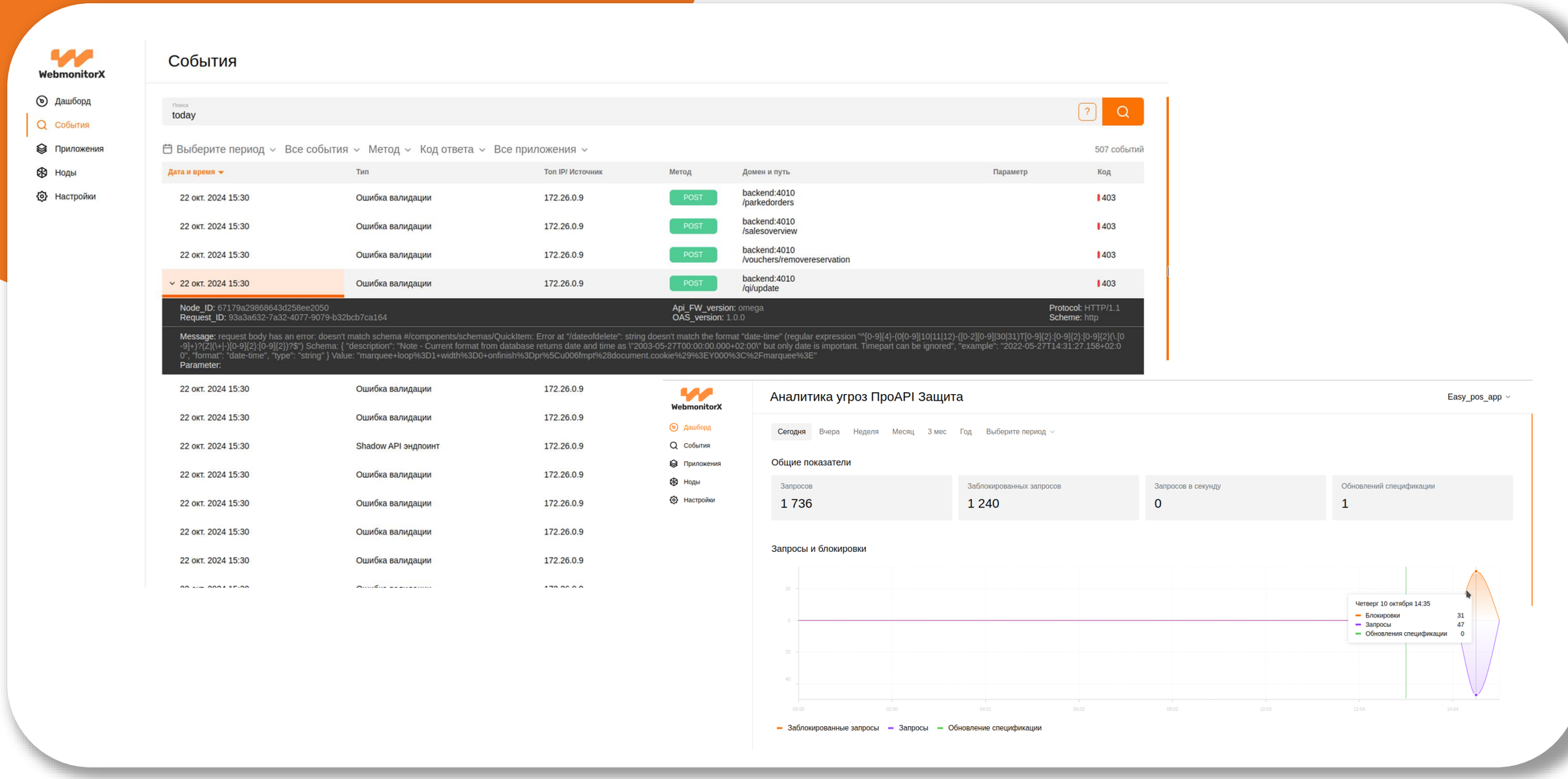
Схема установки

Вебмониторэкс
защита веб-приложений и API



Интерфейс

Вебмониторэкс
защита веб-приложений и API



Карта покрытия по OWASP

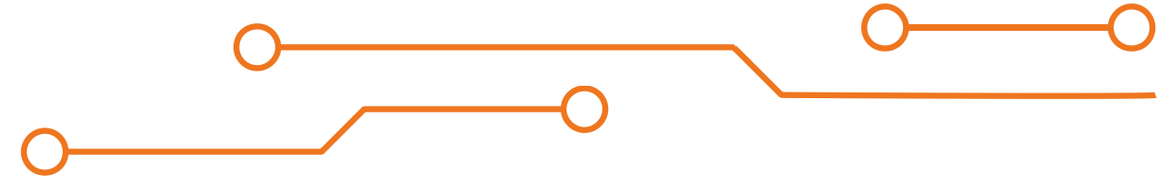
Вебмониторэкс
защита веб-приложений и API

Покрываем

- Broken Object Level Authorization
- Broken Authentication
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Server Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management

В разработке

- Broken Object Property Level Authorization
- Unsafe Consumption of APIs



Вебмониторэкс
защита веб-приложений и API

04

Кейсы внедрения

Пример проекта

СБЕР АВТО x Вебмониторэкс
защита веб-приложений и API

Задачи

Инфраструктура компании построена на основе микросервисов, взаимодействующих друг с другом по API, для которых необходимы учёт и мониторинг их изменений (5 веб-приложений, 3 мобильных приложения, 5 API, 1 интеграционный API)

Условия выбора продукта

- Совместимость с существующей инфраструктурой
- Использование в процессе безопасной разработки
- Техническая поддержка

Результат

Внедрены продукты: ProWAF, ProAPI Структура, ProAPI Тестирование и ProAPI Защита

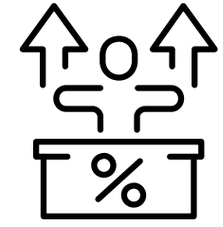
Преимущества платформы «Вебмониторэкс» для «СберАвто»

- Минимальное количество специалистов, необходимое для поддержки решений
- Минимальное время, затрачиваемое специалистами на поддержку решения (20%)
- Возможность обновления всех API раз в две недели
- Обеспечение безопасности веб-приложений и API
- Интеграция с другими процессами для обогащения
- Интеграция в процесс безопасной разработки
- Совместимость с облачной инфраструктурой
- Интеллектуальный подход
- Низкий уровень ложных срабатываний
- Поддержка процесса CI/CD

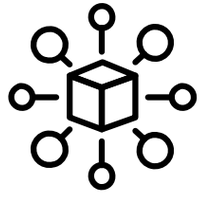
Присутствие в отраслях

Вебмониторэкс
защита веб-приложений и API

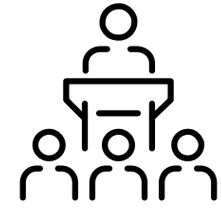
ИТ сектор



Финансовый сектор



E-commerce



Государственный сектор

Вебмониторэкс

защита веб-приложений и API

webmonitorx.ru

info@webmonitorx.ru

+7 495-740-35-44

Habr

Телеграм

ВКонтакте