



ПроWAF от WMX: реальная защита веб-приложений, а не обещания

Продукт ПроWAF
Фролов Евгений, Pre-sale инженер WMX



О компании

История компании

12 лет

опыта разработки решений
по защите веб-приложений

Основание
компании в РФ

2013



Отделение российского бизнеса
в независимую компанию

2022



Сертификация ФСТЭК России

2024

Запуск линейки ПроAPI

2025

>50%

R&D остались в России
в команде WMX



Преимущества



Высокая производительность:
ПроWAF не замедляет веб-трафик при высоких нагрузках.



Простота и скорость внедрения:
установка и запуск занимают 60 мин и не требуют выделенной команды внедрения.



Минимум затрат: администрирование ПроWAF занимает не более 15 минут в день.



Точность детекта: минимальное число ложноположительных срабатываний, акцент на реальные угрозы.



Уникальная методика выявления угроз:
собственная база детектов на основе 12 лет борьбы с веб-атаками.



Соответствие требованиям регуляторов:
сертификат ФСТЭК России по МЭ Г4, реестр отечественного ПО, репозиторий Ассоциации ФинТех.



Легкое масштабирование: оперативное подключение новых веб-приложений к защите.

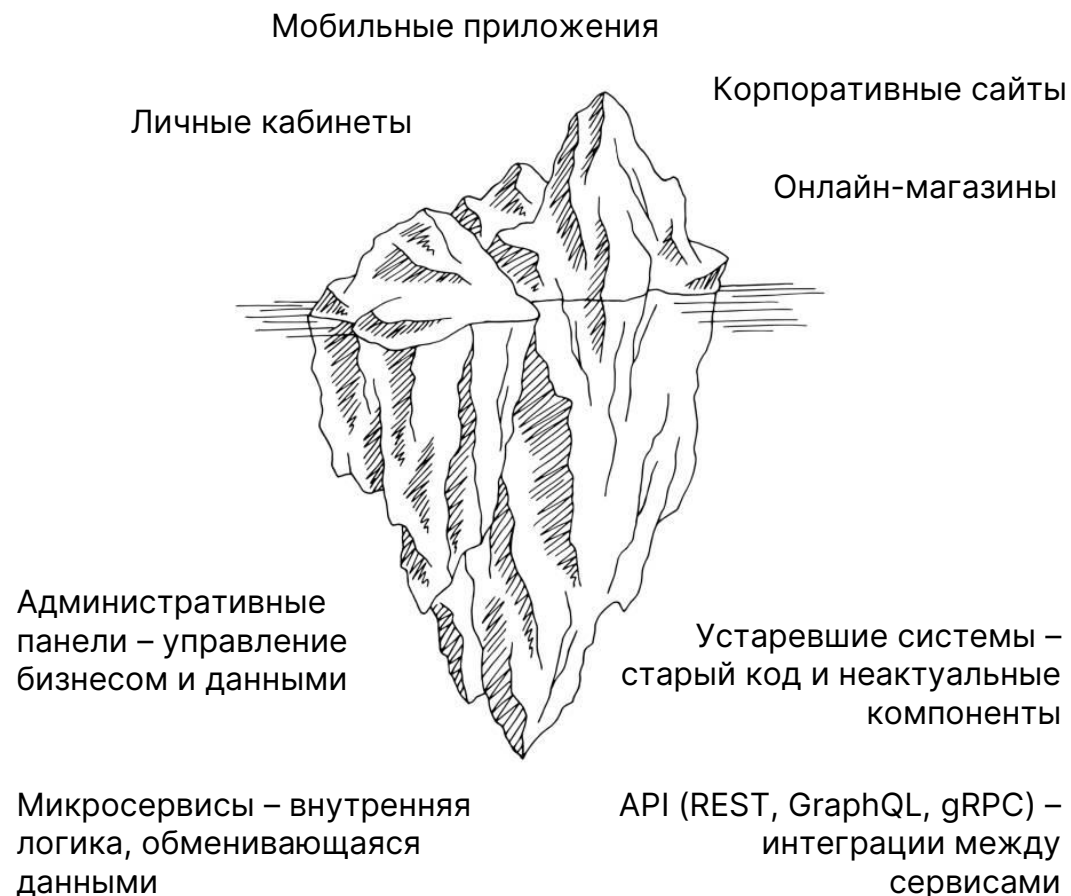


Интуитивно понятный интерфейс:
легко настраиваемые правила, просмотр и аналитика событий и атак.

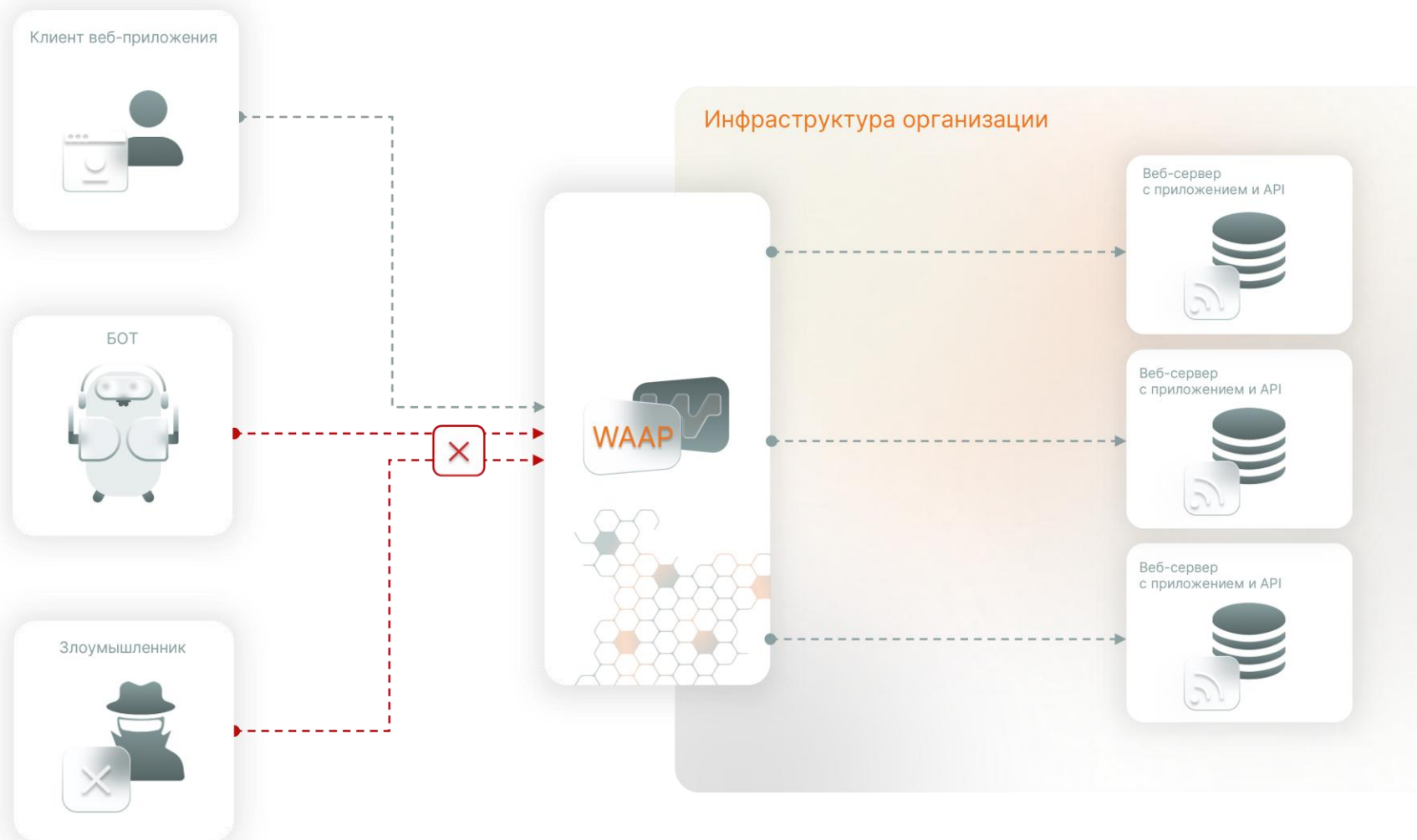


Почему веб уязвим?

- **Человеческий фактор:** Программисты допускают ошибки. Ошибки в коде – это бреши в защите.
- **Скорость vs Безопасность:** В погоне за скоростью разработки, тестирование безопасности часто упускается из виду.
- **Технологическое разнообразие:** Сложность современных веб-приложений, использующих множество технологий, кратно увеличивает количество потенциальных уязвимостей.
- **Устаревший код:** Код, написанный много лет назад, становится легкой мишенью для автоматизированных сканеров уязвимостей.



WAF или WAAP?



Web Application and API Protection:

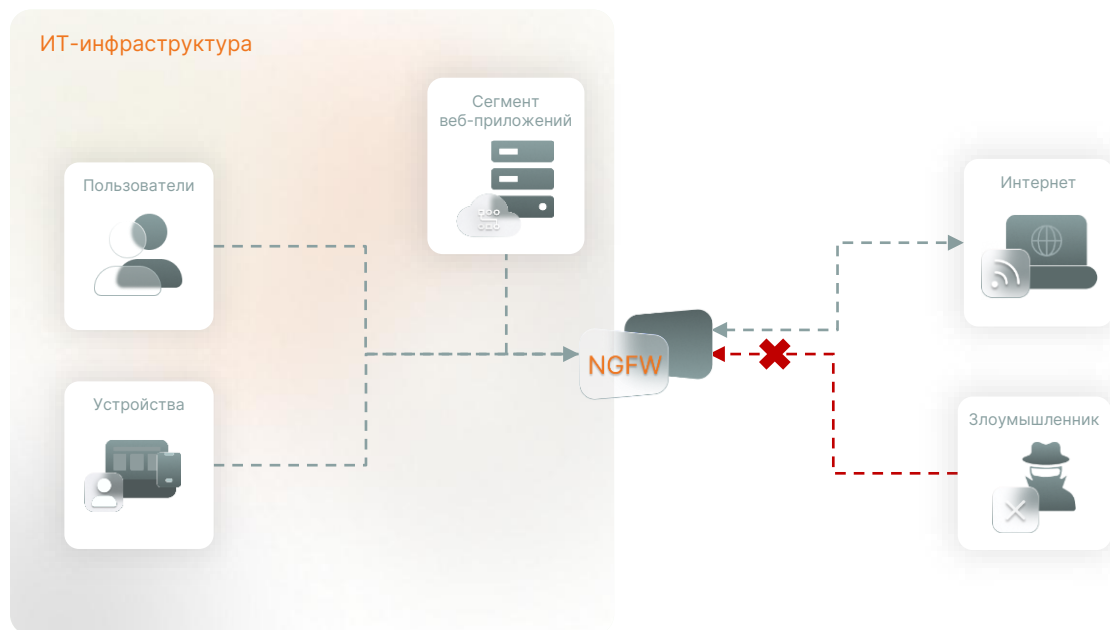
- Многими считается следующим поколением WAF
- Учитывает особенности API, но не концентрируется на них
- Встроенные механизмы Anti-Bot и Anti-DDoS L7
- Преимущественно облачный



Разница между NGFW и WAF

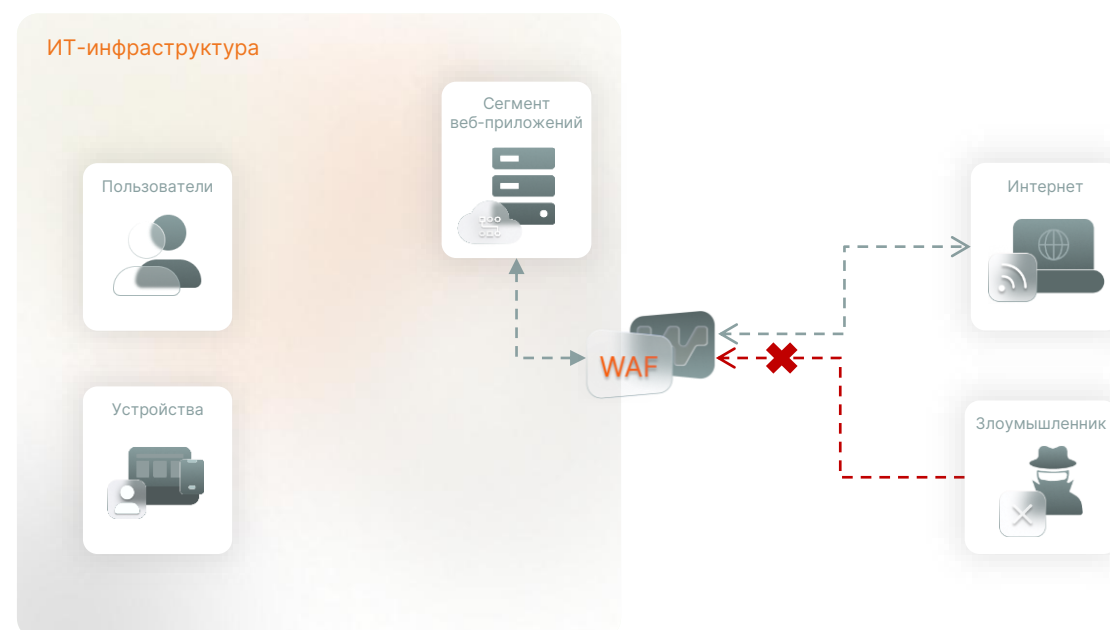
NGFW

Являясь многофункциональным устройством, работает со всем трафиком, что ведет к большой загрузке вычислительных ресурсов и увеличению ложно-положительных срабатываний.



WAF

Ориентирован только на веб-трафик (L7), поэтому имеет более точные настройки и требует меньших вычислительных мощностей, идеально работает в паре с NGFW.



NGFW не эффективен против ряда атак

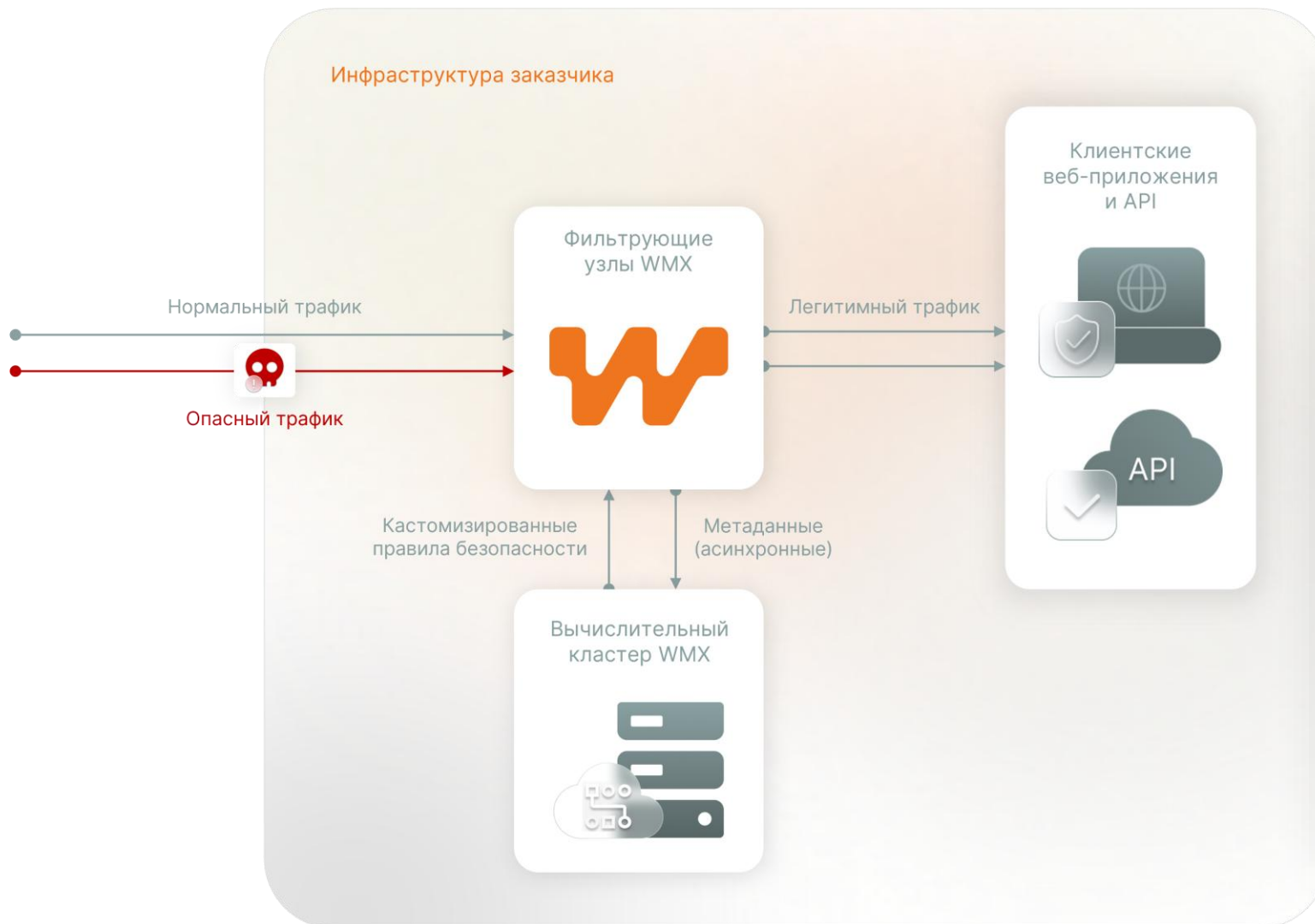
- Специализированные HTTP-атаки из списка OWASP TOP-10
- SQL-инъекции (SQL Injection)
- XSS-атаки (Cross-Site Scripting)
- DDoS-атаки (Distributed Denial of Service) на уровне приложений (L7)
- CSRF-атаки (Cross-Site Request Forgery)
- Подстановка учетных данных (credentials stuffing)
- Атаки на API
- Противодействие обходам captcha





Продукт ProWAF

Как работает ProWAF



- Анализирует входящий трафик на приложение
- Определяет и защищает от атак в режиме реального времени
- Показывает аналитику угроз/атак в интуитивно понятном интерфейсе
- Автоматизирует защиту трафика на веб-приложение (сокращает трудозатраты на внедрение, настройку и обслуживание)

Продукт ProWAF

Фильтрующая нода

Работа с проходящим трафиком:

- Анализ трафика на периметре сети
- Блокировка действий злоумышленника
- Блокировка автоматизированных активностей

Вычислительный кластер

Консоль управления фильтрующими нодами:

- Централизованное и понятное управление настройками безопасности
- Система аналитики и отчетности
- Средства интеграции

Средства построения комплексной защиты:

- Подсистема исследования и предупреждения атак
- Подсистема блокировки массовых атак
- Подсистема автоматического реагирования на события безопасности
- Сканер периметра и уязвимостей



Глубокий анализ запросов



Интеллектуальный парсинг

- Работает без конфигурации
- Не требует схемы
- Автоматически распознает форматы данных
- Применяет необходимые парсеры/декодеры
- Применяет цепочки парсеров

Модели работы WAF

Позитивная модель WAF

- Требуется создание профиля для каждого защищаемого приложения
- Требуется обновление настройки после каждого релиза
- Большое количество ложно-положительных срабатываний
- Отсутствие реакции на zero-day

Негативная модель WAF

- Обнаруживает атаки сразу после установки
- Поддерживает непрерывный процесс безопасной разработки
- Позволяет сделать гибкую настройку для снижения ложноположительных срабатываний
- Изучение каждого запроса на наличие атаки
- Защита от zero-day

Первый на рынке WAF, анализирующий весь трафик



Собственный центр аналитики уязвимостей

- Автоматическое обновление правил детекта
- Детектируем и блокируем 0-day из коробки
- Защищаем от OWASP угроз
- Агрегируем и анализируем данные об уязвимостях из различных источников



Подсистема исследования и предупреждения атак



- Выявление атакующего элемента запроса:
 - в реальном времени под высокой нагрузкой для протоколов HTTP и HTTPS, gRPC, WebSocket;
 - декодирование, нормализация и токенизация для вложенных типов данных;
 - парсинг данных внутри WebSocket соединений с учетом вложенных кодировок (json, gzip, xml).
- Определение и систематизация типов и классов атак.
- Перепроверка возможности реализации атаки на веб-приложение с аналогичными, но видоизмененными запросами.
- Virtual Patching – ограничение доступа к уязвимым частям приложения до их устранения.



Подсистема блокировки массовых атак



Защита приложения от автоматизированных атак, нацеленных на сбор информации:

- Brute-force – перебор пар логин-пароль
- Credential Stuffing – перебор пароля к учетной записи
- Directory Busting – перебор директорий сайта с целью идентификации используемых сервисов
- Блокировка по IP-адресам



Подсистема автоматического реагирования



Умные уведомления (триггеры) основываются на разных событиях:

- Скорость атаки на приложение
- Количество IP в атаке
- Коды ответа приложения
- Тип атаки
- Прочие настраиваемые события

Уведомления доступны через почту, telegram и другие сервисы

Возможные кастомизированные действия:

- Блокировка IP
- Комплексная блокировка



Сканер периметра и уязвимостей



Классика MITTRE ATT&CK: атака начинается с Reconnaissance – исследования объекта атаки.

Сканер воспроизводит технику сканирования злоумышленников:

- Сбор данных об объектах сетевого периметра
- Поиск типовых уязвимостей и проблем безопасности
- Поиск уязвимостей на узлах, находящихся в периметре компании
- Актуализация информации о найденных ранее уязвимостях

Сканер способен обнаруживать все распространённые типы уязвимостей (в соответствии с рекомендациями OWASP Top-10), таких как SQLi, XSS, XXE и т.п.

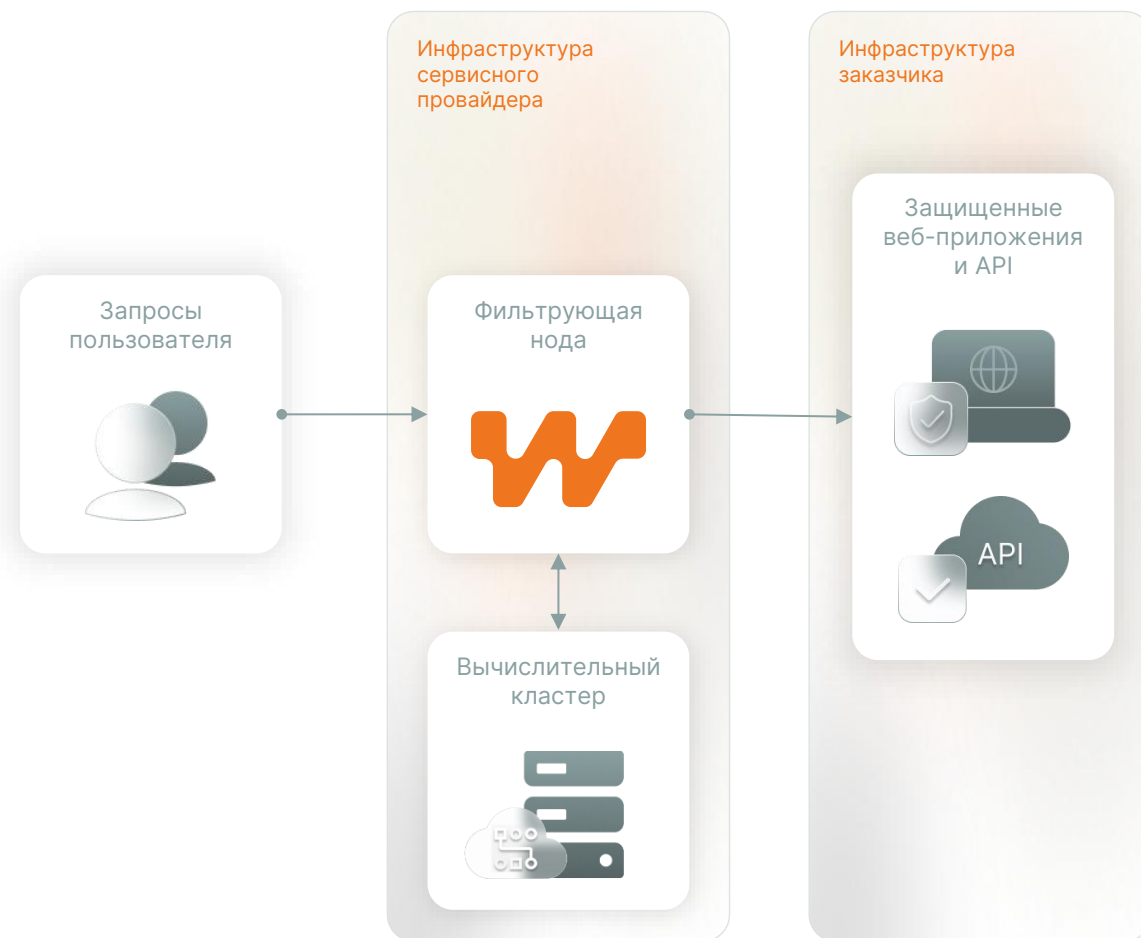


Что с внедрением?

Поддерживаемые интеграции:

- SOC
- SIEM
- Российские ОС
- Веб-серверы и API-шлюзы
- Через API-системы, через webhook и другими способами

Установка в инфраструктуру сервисного провайдера

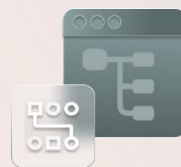


Встроимся в любую инфраструктуру

Универсальная установка



автоматически определяем
версии операционной
системы



устанавливаем все
необходимые зависимости

Веб-серверы и API-шлюзы:

NGINX

NGINX

ANGIE

Angie (PRO и стандарт)

Поддерживаемые операционные системы:



Альт ОС



Астра ОС



RedOS 7.x



Debian
10.x 11.x



Ubuntu

Ubuntu
18.x 20.x 22.x



CentOS 7.x

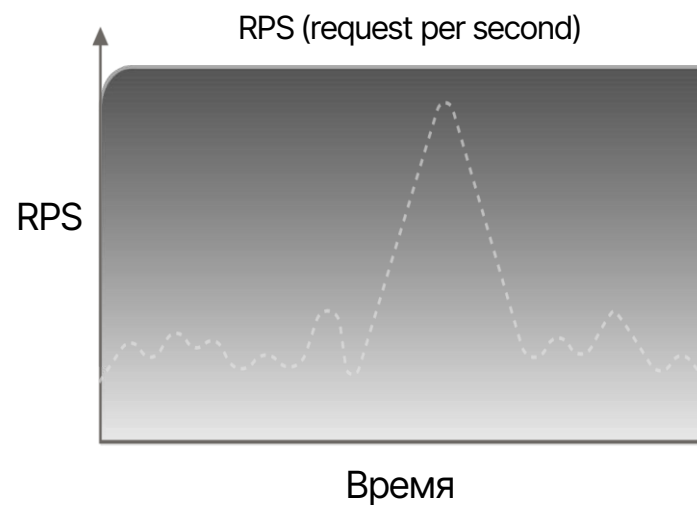
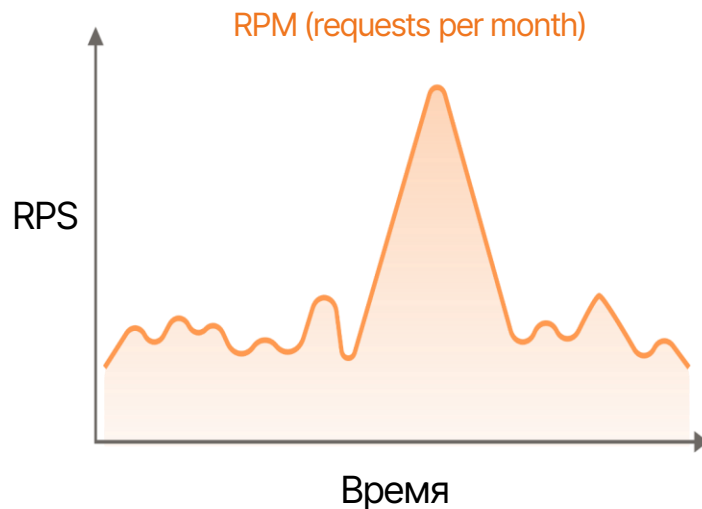




Лицензирование

Лицензирование

Оплата за фактическое количество трафика, а не за расчётную пиковую нагрузку



- Срочная и бессрочная лицензии
- Гибкое ценообразование по используемым функциям платформы
- Основная метрика лицензирования – RPM



Контакты



wmx.pro



info@webmonitorx.ru



+7 495 740 35 44



Нabr



Телеграм



ВКонтакте



Сайт