софтлайн решения

softline ОБЛАКО

WAF как сервис: от аналитики угроз к практическому подключению

Роман Зацепин
Менеджер продукта
облачных сервисов безопасности
Софтлайн Облако

Для чего WAF нужен бизнесу

Защищает выручку и конверсию: отсеивает вредные запросы и «серые» злоупотребления, которые портят клиентский путь (всплески регистрации, накрутки, попытки подобрать аккаунты, странные запросы к формам)

Снижает риск мошенничества и компрометации аккаунтов — прикрывает вход, личные кабинеты, платежные сценарии, бонусы/промо-механику

Поддерживает стабильность цифровых каналов: сайт/ЛК/API легче переживают пики, аномалии и нестандартный трафик

Ускоряет запуск и изменения: базовый защитный контур уже есть, меньше поводов «тормозить релиз из-за ИБ»

Сокращает операционные издержки вокруг инцидентов: меньше ручных разборов, меньше «пожаров», меньше отвлечений команд на внезапные веб-проблемы

Для чего WAF нужен ИТ/ИБ департаментам

Фильтрует типовые классы веб-атак и автоматизацию: сканирование, подборы, инъекции, попытки обхода логики

Защищает веб-формы и API на уровне правил: методы, URL, параметры, заголовки, шаблоны запросов

Делает угрозы видимыми через личный кабинет: понятная статистика какие именно атаки, по каким CVE, откуда, куда и с какой динамикой

Помогает реагировать вовремя: уведомления и алёрты по триггерам (всплески, конкретные векторы, критичные URL/эндпоинты)

Упрощает разбор инцидентов для команды: фильтры, контекст по событиям и быстрый путь «посмотреть → решить → запросить изменение правил»

Готовит отчёты, которые помогают принимать решения: короткие сводки «что блокировали/что пропускали/что требует внимания» — без ручной сборки из логов

Почему WAF ещё нет у вас?

1. **Бюджет и приоритеты:** безопасность конкурирует с продуктовой и ИТ-повесткой
2. **Эксплуатация и кадры:** нет выделенной команды, которая будет сопровождать WAF постоянно
3. **Риск false positive:** важно не «сломать» легитимные сценарии и конверсию.
4. **Долгий путь внедрения:** инфраструктура, контуры, сертификаты, тестирование, согласования
5. **Высокая динамика изменений:** частые релизы = правила надо регулярно актуализировать
6. **Сложно измерить эффект:** «купили безопасность» трудно перевести в понятные KPI
7. **Неясная зона ответственности:** кто принимает решения, кто вносит изменения, кто отвечает за последствия

> ***Как помогает SaaS-подход?*** *Снижает инфраструктурную нагрузку и барьер старта — вы фокусируетесь на политике и бизнес-приоритетах, а платформа WAF уже готова к работе*

Как организовать владение WAF без новых рисков и нагрузки

WAF-инициативы чаще ломаются не на «плохих атаках», а на четырёх вещах:

1 **Скорость выхода на защиту**
Сократить путь до «первой защищённой транзакции» — без долгого инфраструктурного проекта.

2 **Платформа без ручной боли**
Доступность, масштабирование, обновления, сертификаты, мониторинг — чтобы это было предсказуемо и не превращалось в отдельный продукт внутри ИТ

3 **Правила без перегибов**
Тюнинг политики так, чтобы снижать false positive и не бить по бизнес-сценариям (логин, формы, API, ЛК)

4 **Понятная ответственность и процесс изменений**
Кто принимает решения по политике, как вносятся изменения, как согласуются исключения — чтобы не было «серой зоны»

Как выглядит WAF по сервисной модели

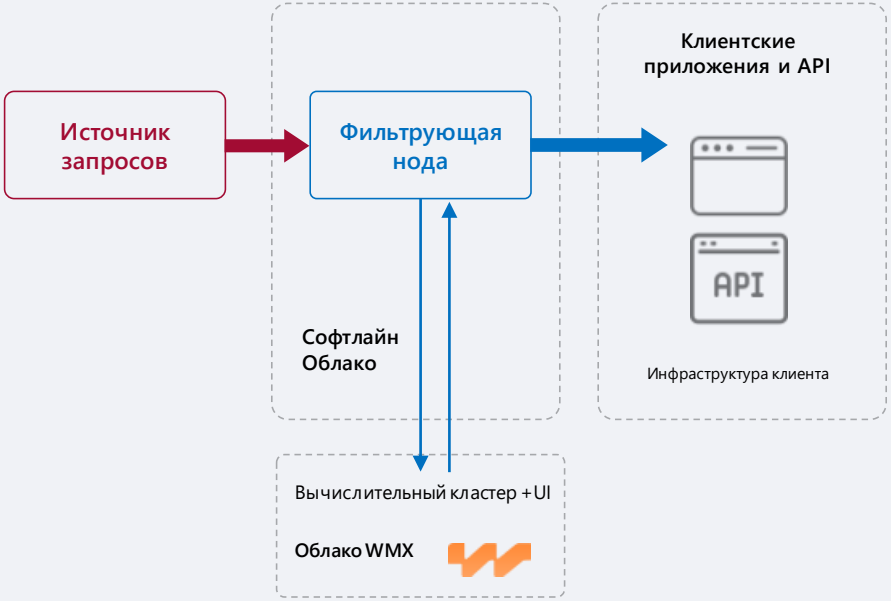
Что входит в сервис:

- ✓ размещение и эксплуатация фильтрующих нод в облаке Софтлайн
- ✓ обновления платформы
- ✓ масштабирование
- ✓ поддержка инфраструктуры и личного кабинета
- ✓ изменения правил по вашему запросу и консультации

Важно!
В вашу инфраструктуру ничего не устанавливается!

Ключевой эффект:
вы убираете инфраструктурную и эксплуатационную часть владения WAF и быстрее получаете защищённый контур.

Администрирование и реакция – полностью под вашим контролем с нашей поддержкой 24/7



Честно сравниваем WAF в своей инфраструктуре и по сервисной модели

Что именно снимает с вас SaaS модель, даже если сам WAF от одного и того же вендора?

Свой WAF обычно означает, что на вас ложится:

- инфраструктура (ноды/сеть/балансировка/API к вычислительному кластеру)
- масштабирование и отказоустойчивость
- обновления платформы и компонентов
- отдельная экспертиза на эксплуатацию
- тюнинг правил и исключения руками
- долгий проект внедрения и длинный старт

В SaaS модели:

- фильтрующие ноды в нашей облачной инфраструктуре
- эксплуатация доступности/масштабирования платформы
- обновления “по умолчанию”
- поддержка и понятный процесс изменений
- правила/исключения — реализуем по вашему запросу

Тезисный план ~~«внедрения»~~ подключения

1. **Сформулируйте цель пилота и критерии успеха**
   Какие приложения/домены, какие сценарии критичны, что считаем результатом.

2. **Передайте минимальные вводные**
   Короткая анкета + сертификаты/техпараметры для подключения.

3. **Подключаем сервис и выдаём доступ**
   Разворачиваем фильтрацию в нашей инфраструктуре, подключаем мощности, открываем личный кабинет.

4. **Запускаем в режиме мониторинга**
   Собираем картину трафика и событий без влияния на бизнес-сценарии

5. **Точечно настраиваем правила и исключения и переходим к блокировке**
   Включаем аккуратно там, где правила проверены и согласованы

6. **Фиксируем результаты и планируем продуктив**
   Проверяем производительность/качество детекта, получаете рекомендации по продуктивному режиму и уровню поддержки.

ADDoS и WAF – про одно и то же?

ADDoS — про доступность: перегрузка сети/соединений/HTTP-потока (L3–L7)

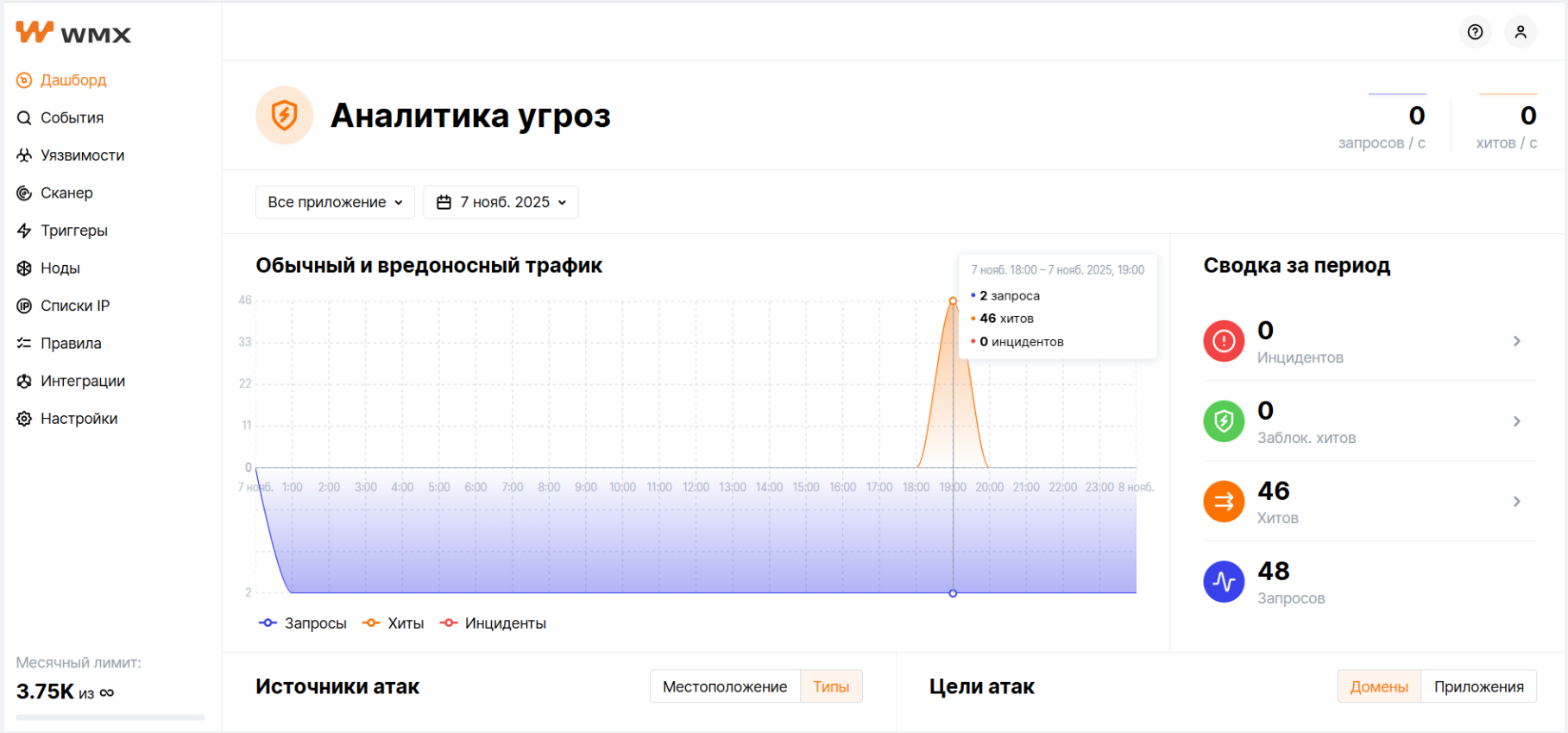
WAF — про корректность и безопасность HTTP(S): что именно несёт запрос к URL/API и как он ведёт себя

Примеры по типам атак:

- **ADDoS (L3/L4):** UDP flood, SYN flood, TCP connection flood
- **ADDoS (L7):** HTTP GET/POST flood, “slow" атаки (Slowloris / slow POST)
- **WAF (HTTP):** SQLi, XSS, LFI/RFI, command injection
- **WAF (Auth/логика):** brute force/credential stuffing, обход бизнес-логики через параметры/URL

> ADDoS удерживает сервис «в онлайне», **WAF** — не пропускает вредные запросы в приложение и не позволяет получить доступ к данным

Первый день из жизни сайта в онлайне



Инфраструктура. Надёжная. Защищённая.

На самом деле - первые два часа сайта в онлайне – 46 атак

События

attacks incidents 07/11/2025

Фильтр | Поиски | Отчет

Все атаки, Инциденты | Тип | 7 нояб. 2025 | Приложение | IP | Домен | Код ответа | Цель | Тип источника | Местоположение | CVE и эксплойты | Протоколы API | Протоколы аутентификации

46 атак 46 хитов

Сортировать по последнему запросу

Дата ▼ / ДЛИТЕЛЬНОСТЬ	Хиты	Пэйлоады	Топ IP / Источник	Домен / Путь / ПРИЛОЖЕНИЕ	Код	Параметр	Активная проверка
7 ноя 2025, 18:59	1	1 RCE	75.157.196.239	93.90.222.159 /index.php demoslwmx.ru	404	QUERY_NAME	
7 ноя 2025, 18:59	1	1 RCE	75.157.196.239	93.90.222.159 /index.php demoslwmx.ru	404	URI	
7 ноя 2025, 18:59	1	1 Path Traversal	75.157.196.239	93.90.222.159 /index.php demoslwmx.ru	404	QUERY › lang	
7 ноя 2025, 18:59	1	1 RCE	75.157.196.239	93.90.222.159 /app/vendor/phpunit/phpunit/src/Util/PH	404	POST	

Роман Зацепин

Менеджер группы облачных сервисов безопасности Софтлайн Облако

Roman.Zatsepin@softline.com

cloud.softline.ru

Инфраструктура. Надёжная. Защищённая.

софтлайн РЕШЕНИЯ

Трендовые веб-угрозы и отраслевая аналитика атак. Почему WAF — это гарантия стабильности бизнеса?

Чебанов Игорь,
Менеджер по работе с партнерами

wmx

Трендовые веб-угрозы и отраслевая аналитика атак

В кого целятся веб-атаки?

* данные аналитики веб-атак, отраженных межсетевым экраном веб-приложений WMX ПроWAF

В 2025 году WMX ПроWAF отразил **1,2 млрд веб-атак** на клиентов.

Это на **15% выше** показателей 2024 года.

По оценке экспертов, около **40% успешных кибератак** на российские компании сегодня начинаются именно со взлома веб-приложения организации.

Как атаковали хакеры в 2025?

Финсектор

В 2025 году каждая организация из финансовой отрасли столкнулась в среднем **с 8,6 млн веб-атак***

Основная угроза — удаленное исполнение вредоносного кода в серверной части веб-приложения (**RCE-атаки**).

Как это?
RCE — внедрив код, хакер заставляет операционную систему, в которой запущено приложение, выполнять определенные команды.

Последствия:
- кража данных, хранящихся в приложении;
- полный контроль над приложением;
- распространение атаки по всей инфраструктуре компании.

* данные аналитики веб-атак, отраженных межсетевым экраном веб-приложений WMX ПроWAF

Как атаковали хакеры в 2025?

Онлайн-торговля

В 2025 году каждый интернет-магазин столкнулась в среднем с **5 млн веб-атак** *

Основная угроза — **межсайтовый скриптинг (XSS)**

Как это?
Злоумышленник внедряет вредоносный код в веб-страницу, и пользователь видит в своем браузере уже измененный контент.

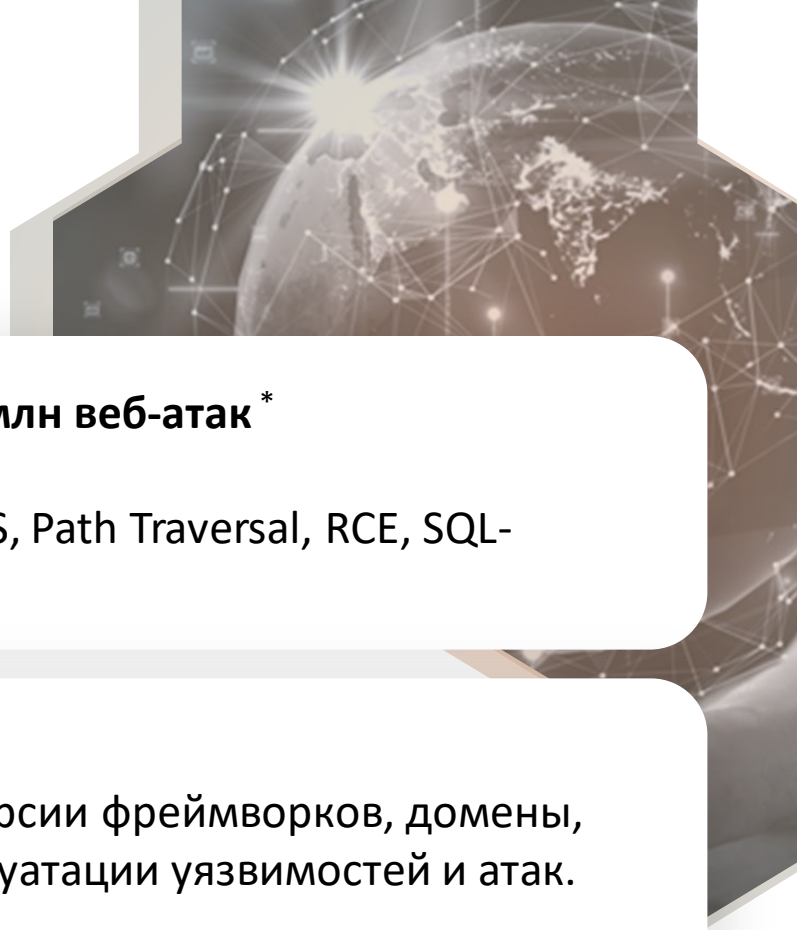
Последствия:

- кража пользовательских аккаунтов, персональных и платежных данных;
- кража бонусных баллов и промокодов покупателей;
- манипуляции с корзиной покупок (100 товаров за 1 рубль и т.п), что ведет к прямому финансовому ущербу.

* данные аналитики веб-атак, отраженных межсетевым экраном веб-приложений WMX ПроWAF

Как атаковали хакеры в 2025?

ИТ-компании



В 2025 году каждая организация из ИТ отрасли столкнулась в среднем с **5,4 млн веб-атак** *

Основная угроза — **автоматизированные сканирования** и в равной доли XSS, Path Traversal, RCE, SQL-инъекции.

Как это?
Сначала автоматические сканеры изучают компоненты веб-приложения (версии фреймворков, домены, структура API, TLS-версии и т.п). Дальше эти данные используются для эксплуатации уязвимостей и атак.

Последствия:

- утечка корпоративных данных компании и ее клиентов;
- через ИТ-подрядчика хакеры атакуют его заказчиков, развивая атаку на другие компании и отрасли;
- удар по репутации ИТ-компании, отток клиентов и финансовый ущерб.

* данные аналитики веб-атак, отраженных межсетевым экраном веб-приложений WMX ПроWAF

wmx

Громкие веб-атаки последних лет

Совсем недавние атаки

React2Shell: уже в декабре 2025 исследователи по ИБ заявляли о трех успешных атаках на российский бизнес через эту уязвимость. Под удар попали неназванная страховая компания, ритейлер автозапчастей и ИТ-подрядчик. После взлома сервера веб-приложения, хакеры пытались установить на скомпрометированной машине майнер XMRig и развернуть ботнет.

Дефейс российских сайтов: В мае 2023 года произошёл массовый дефейс российских веб-серверов через уязвимость в системе управления CMS «Битрикс».
Среди жертв хакеров были крупные ритейлеры и финорганизации.

Более ранние атаки

В 2018 году хакеры внедрили вредоносный **JavaScript-код в исходный код платёжной страницы сайта British Airways**. Под угрозой оказались все пользователи, бронировавшие билеты через официальный сайт или приложение компании. Суммарно в руки преступников попали личные и финансовые данные 380 тысяч человек.

В 2017 году международное кредитное бюро **Equifax** подверглось взлому. Веб-уязвимость находилась в Apache Struts — это фреймворк, используемый многими ведущими организациями для создания веб-приложений. В итоге атаке были украдены данные почти 200 млн клиентов компании. Помимо репутационного ущерба компания понесла и финансовые потери, т.к. суд обязал ее выплатить компенсацию пострадавшим.

wmx

Почему WAF — это гарантия стабильности бизнеса?

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.

Какие ключевые риски предотвращает WAF?

Компрометация персональных и платежных данных пользователей:

- ↘ Утечка персональных данных
- ↘ Кража платёжной информации
- ↘ Раскрытие коммерческой тайны
- ↘ Репутационный ущерб
- ↘ Санкции и штрафы

Финансовые убытки, понесенные во время простоя веб-ресурсов:

- ↘ Отсутствие заказов
- ↘ Уход клиентов к конкурентам

Затраты на восстановление веб-ресурсов:

- ↘ Финансовые затраты
- ↘ Нагрузка на сотрудников ИБ

wmx

Российская платформа защиты веб-приложений и API

Продукт ПроWAF

История компании

12 лет опыта разработки решений по защите веб-приложений

2013 — Основание компании в РФ

2022 — Отделение российского бизнеса в независимую компанию

2024 — Сертификация ФСТЭК России
Запуск линейки ПроAPI

2025 — Запуск модуля SmartBot Protection

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

Лидер российского рынка защиты веб-приложений и API

70+

Технических специалистов среди сотрудников

300+

Довольных клиентов в России

3

Дистрибьютора

Топ-100

Крупнейших ИБ-компаний в России

80+

Технологических интеграций

150+

Партнеров-интеграторов

Продукт ПроWAF

Фильтрующая нода

Работа с проходящим трафиком:

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

Вычислительный кластер

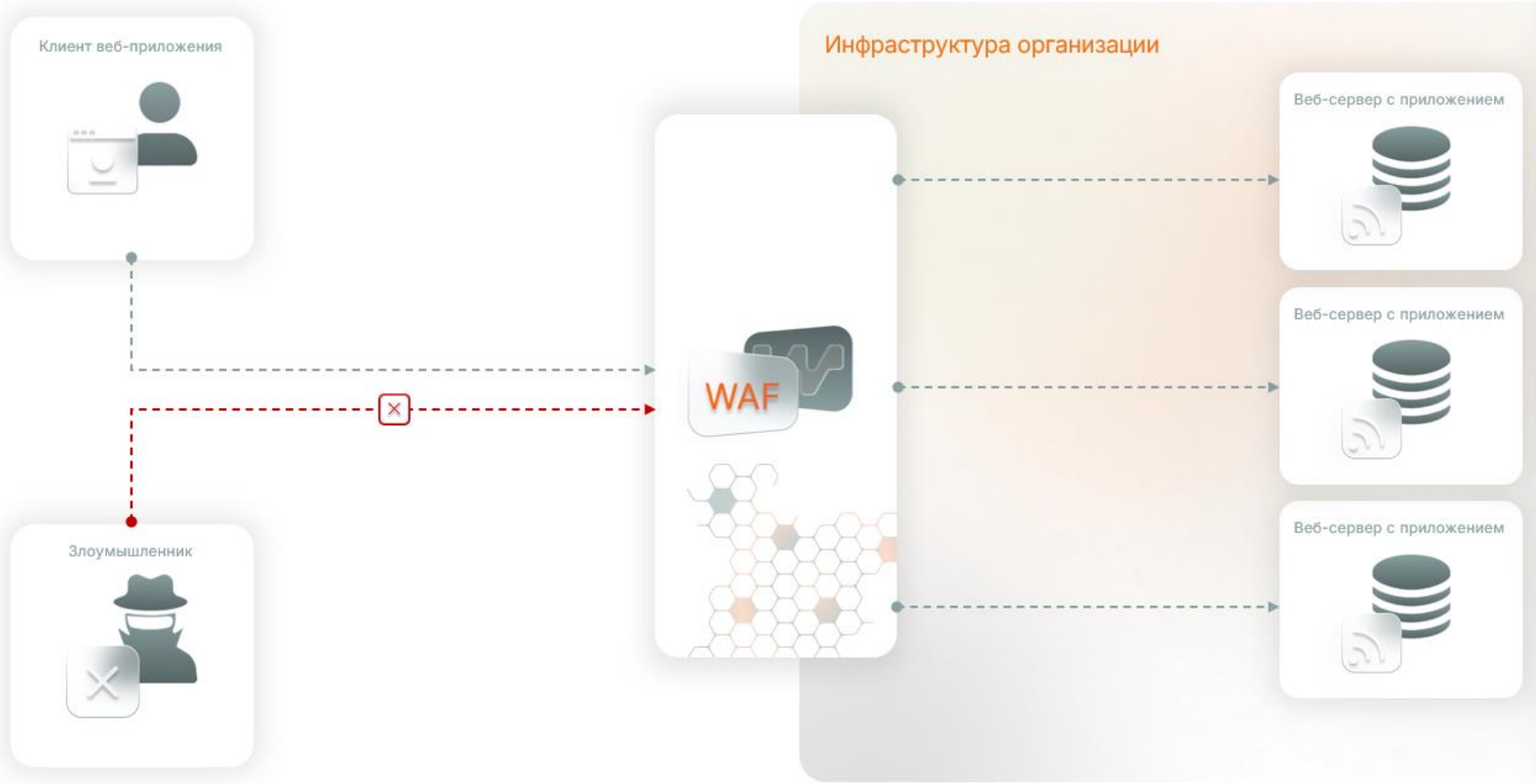
Консоль управления фильтрующими нодами:

- 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

Схема работы WAF



Многоуровневая защита

- Анализ входящих HTTP запросов
- Блокировка опасного трафика
- Выявление уязвимостей
- Защита от эксплуатации уязвимостей
- Анализ сетевого периметра

Преимущества

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

Простота и скорость внедрения: установка и запуск за 60 мин,
не требуется выделенная команда 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.

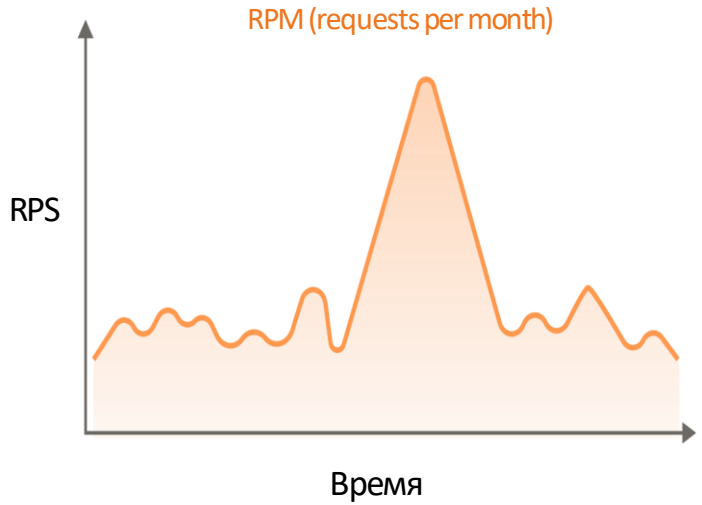
Легкое масштабирование:
оперативное подключение новых веб-приложений к защите.

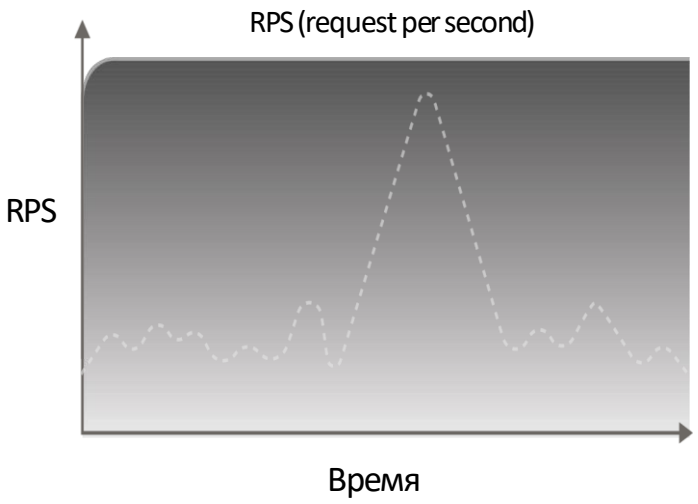
Интуитивно понятный интерфейс: легко настраиваемые правила, просмотр и аналитика событий и атак.

Собственный центр аналитики уязвимостей

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

Лицензирование





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

Контакты

wmx.pro

info@wmx.pro

+7 (495) 740 35 44

Habr

Телеграм

ВКонтакте

Сайт

Роман Зацепин

Менеджер группы облачных сервисов безопасности
Софтлайн Облако

Roman.Zatsepin@softline.com

cloud.softline.ru

Инфраструктура. Надёжная. Защищённая.

софтлайн РЕШЕНИЯ