

Интеллектуальный сетевой экран для защиты веб-приложений

SolidWall
Web Application
Firewall

КТО **МЫ** ТАКИЕ?

2010

**CTF команда
Bushwhackers**
Внутренний проект
по безопасности

2014

SolidWall WAF
Стартовала
разработка продукта

BUSHWHACKERS

9 место
в Team rating 2019 г.

2007

**Лаборатория информационной
безопасности ВМК МГУ**

2011

Компания SolidLab
Внутренний проект
трансформировался в компанию

solidwall

solidlab

**АКАДЕМИЧЕСКОЕ
СООБЩЕСТВО**
Московский
государственный
университет
им. М.В. Ломоносова

ВЕБ-ПРИЛОЖЕНИЯ ДЛЯ ОРГАНИЗАЦИЙ



Государственные
информационные системы

Критичные и фиксированные
системы

Социальные сети

Электронные магазины

Медиа-ресурсы

Электронный
документооборот

Системы управления
ресурсами предприятия

Мобильные
приложения

Системы ДБО

Личные кабинеты

B2B решения

Торговые площадки

Облачные сервисы

ПОЧЕМУ НУЖНО ЗАЩИЩАТЬ ВЕБ-ПРИЛОЖЕНИЯ

Бизнес

- Веб-приложения критичны для бизнеса
- Веб-приложения — слабое звено в периметре защиты организации

Разработка

- В организациях зачастую работает собственная разработка
- Сложная архитектура, заимствованные компоненты
- Недостаточное внимание разработчиков к вопросам ИБ
- Не хватает времени на выпуск безопасного продукта

Безопасность

- Веб-приложения — ключевая цель злоумышленников (наряду с социальной инженерией)
- Векторы атак меняются: от RCE к непосредственной эксплуатации
- В веб-приложениях также сосредоточены внутренние угрозы (ERP, CRM, ЭДО и др.)

```
1 #!/usr/bin/env python3
2 # encoding: utf-8
3
4
5 def main():
6     with open('flag.txt', 'r') as f:
7         flag = f.read()
8         flag = ''.join(map(lambda c: bin(ord(c))[2:
9             ], flag))
10        for c in flag:
11            t = input('> ')
12            if t not in '01':
13                print('Bad character')
14                break
15            if t != c:
16                print('Wrong character')
17                break
18        else:
19            print('OK')
20
21 if __name__ == '__main__':
22     main()
```

ВЛИЯНИЕ СОВРЕМЕННЫХ ТРЕНДОВ

Усложнение разрабатываемых приложений,
большой объем задач по разработке

Сокращение времени для выпуска
продукта (Time to production)

Использование заимствованных компонентов
и повторное использование собственных

Высокий уровень кастомизации логики
приложений

Моб. приложения API и микросервисы

Активный релизный цикл

Недостаток ресурсов и компетенций
у разработчиков

Увеличение технологических
возможностей атак

Развитие киберпреступности (вовлечение
талантливой молодежи)

От синтаксических атак к логическим
и переборным

Направленные атаки, 0-day и 1-day атаки

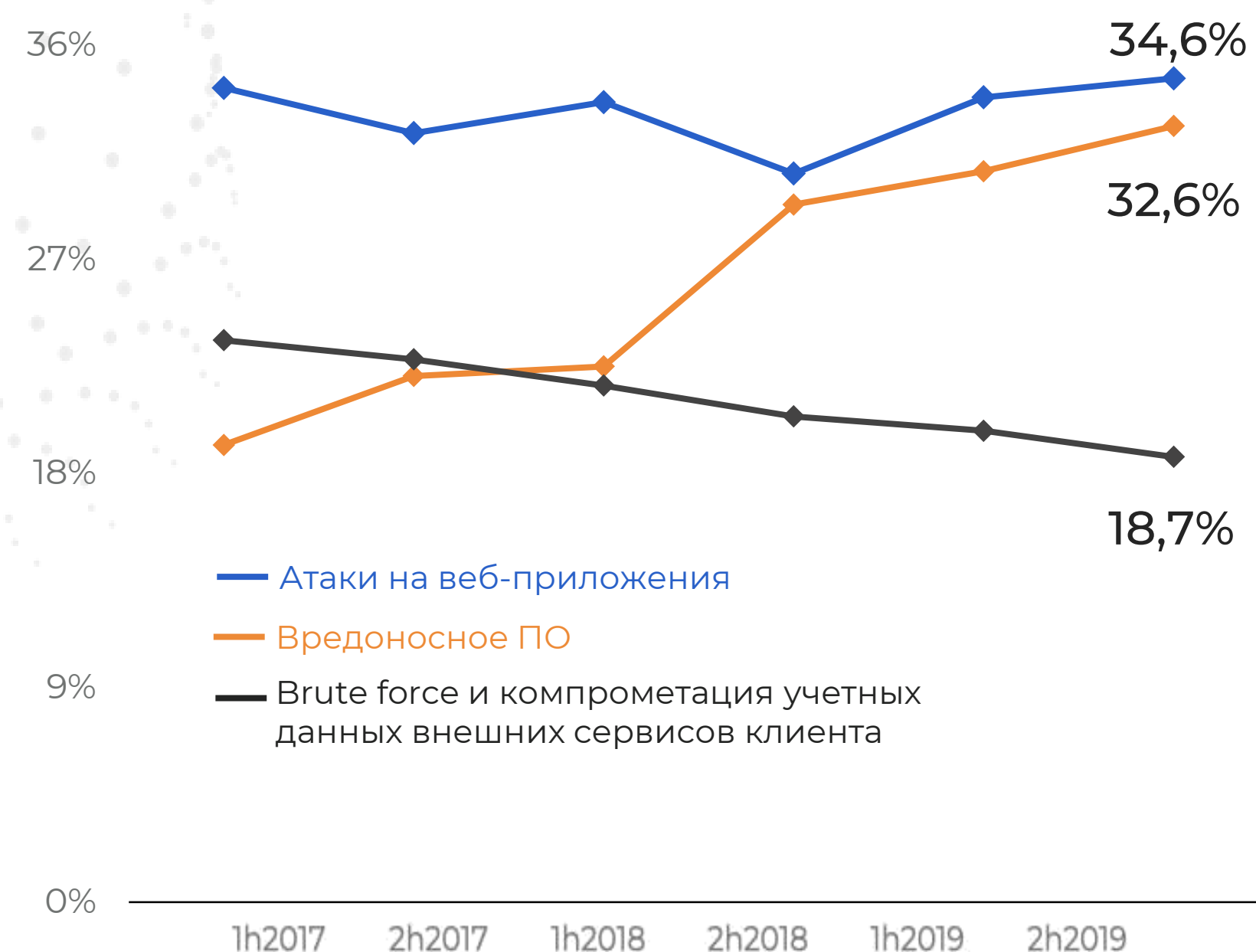
DoS и DDoS атаки

Атаки на API, бэкенды и смежные сервисы

Несанкционированное использование
внутренних приложений

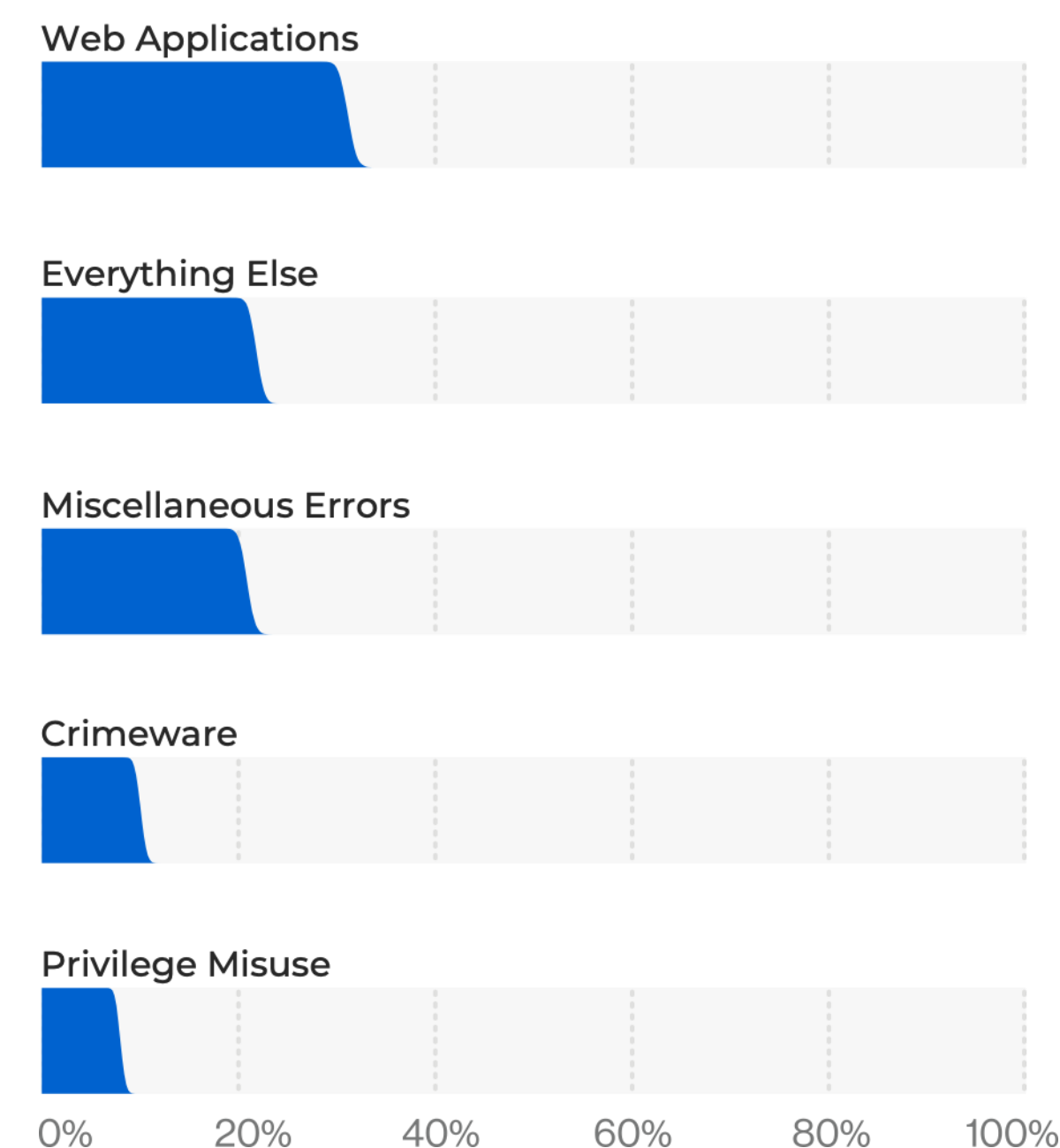
ВЕБ-ПРИЛОЖЕНИЯ — ОСНОВНАЯ МИШЕНЬ ЗЛОУМЫШЛЕННИКОВ

Ключевые направления атак в общей массе инцидентов за последние три года

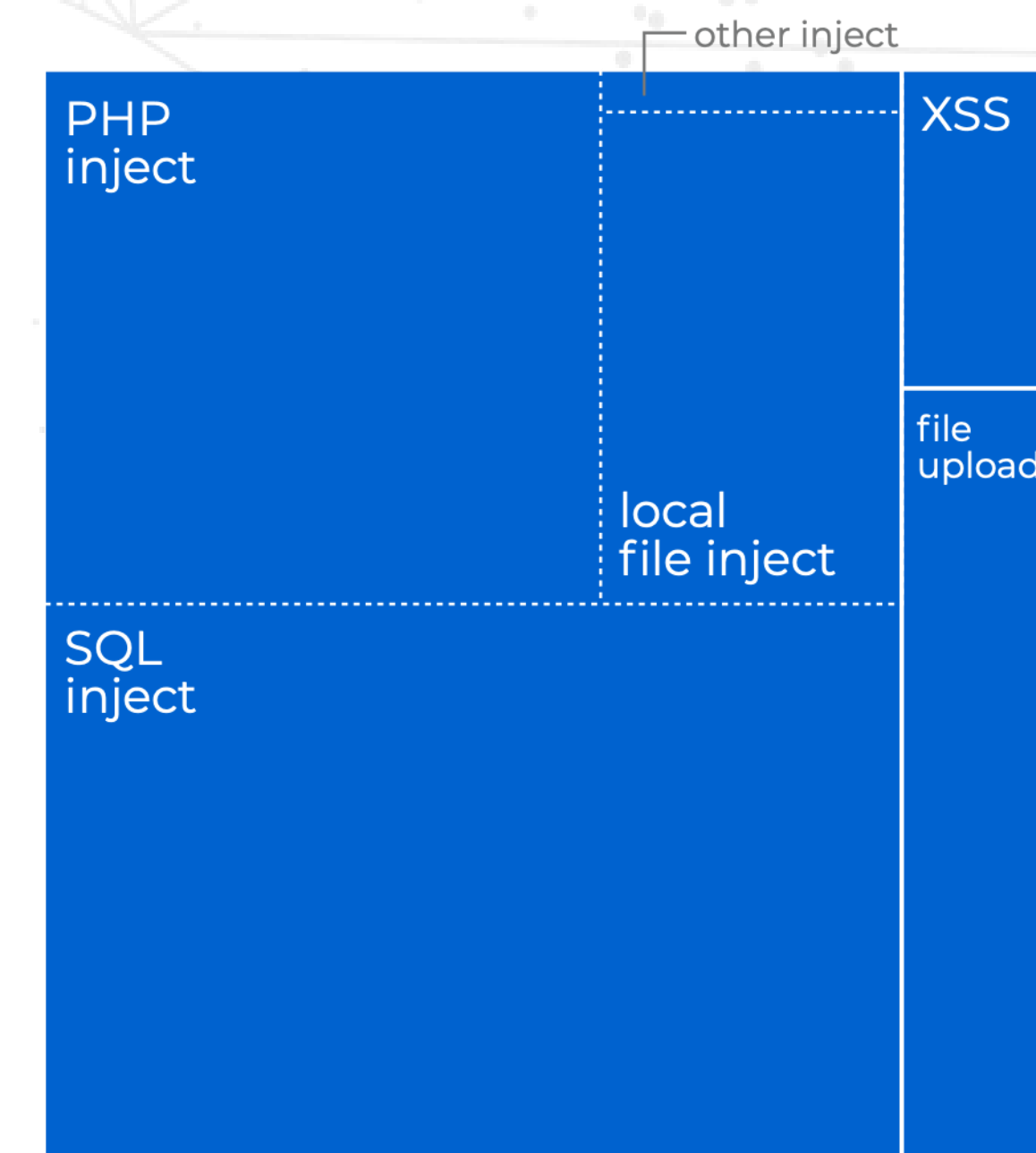


Согласно отчетам Центра мониторинга и реагирования на кибератаки Solar JSOC

Patterns in breaches (Top 5) and Web application attack blocks



According to Verizon 2020 Data Breach Investigations Report



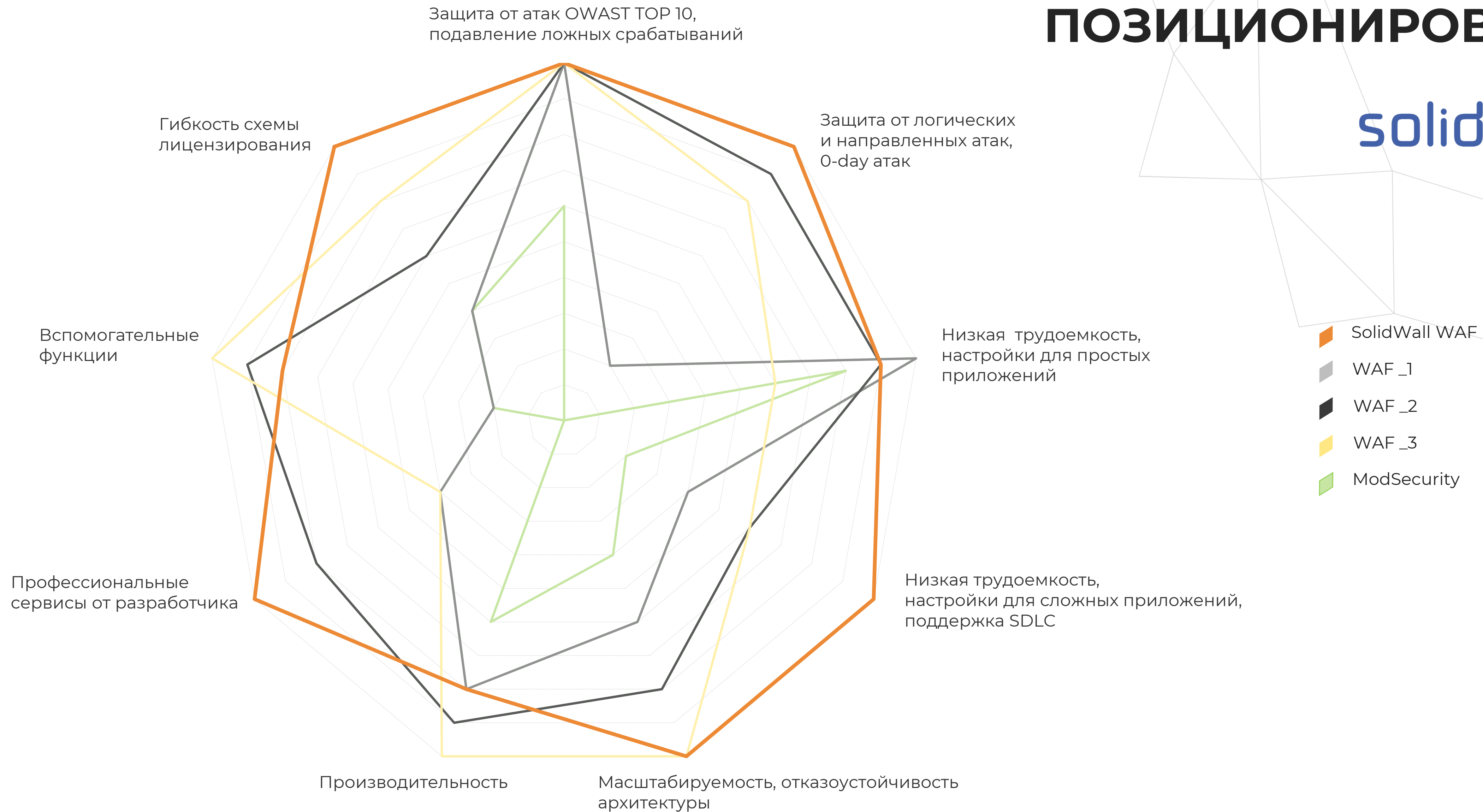


СООБЩЕСТВО OWASP И РЕЙТИНГ OWASP TOP 10



ПОЗИЦИОНИРОВАНИЕ

solidwall 



ОСНОВНЫЕ СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ



Защита от атак
OWASP Top 10



Защита от
логических атак



Защита
от переборных
атак и ботов



Защита от атак
на 0-day и 1-day
уязвимости



Защита от
мошенничества



Защита API
и мобильных
приложений

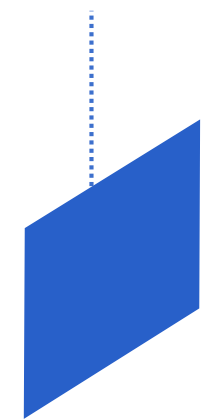


Защита от DoS
и DDoS – атак



Защита
внутренних
систем и UBA

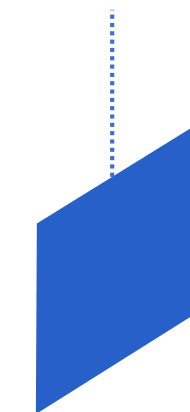
ПРЕИМУЩЕСТВА SOLIDWALL WAF



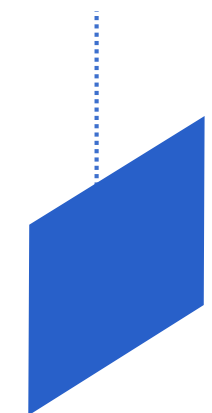
Предоставляется в виде облачного решения или размещается на площадке заказчика



Максимально широкий набор сценариев использования среди аналогичных решений



Широкий набор профессиональных сервисов от разработчика решения



Быстрое подключение и минимальные затраты ресурсов на сопровождение



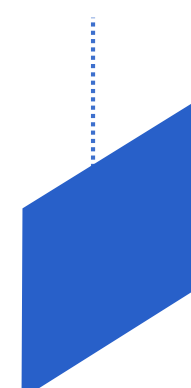
Гибкая настройка с учетом особенностей защищаемых приложений. Осуществляется проще, чем у других решений



Масштабируемость и отказоустойчивость уровня Enterprise



Различные исполнения и тарифные планы для обеспечения оптимальной стоимости владения



Работа в режиме блокировки с минимальным уровнем ложных срабатываний

УНИКАЛЬНЫЕ ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ

1 Готовые модели для всех аспектов работы приложения

Универсальные модели работы защищаемого приложения, которые строятся от его архитектуры, а не от видов атак, позволяют использовать WAF во множестве сценариев и быстро адаптировать его под новые задачи.

2 Эффективное подавление ложных срабатываний

Инструменты раннего подавления на основе сигнатурного анализа и моделей нормальной работы приложений, применяющие алгоритмы машинного обучения, дают возможность максимально быстро вводить WAF в эксплуатацию и снижают вероятность появления ложных срабатываний.

5 Интерпретируемое машинное обучение

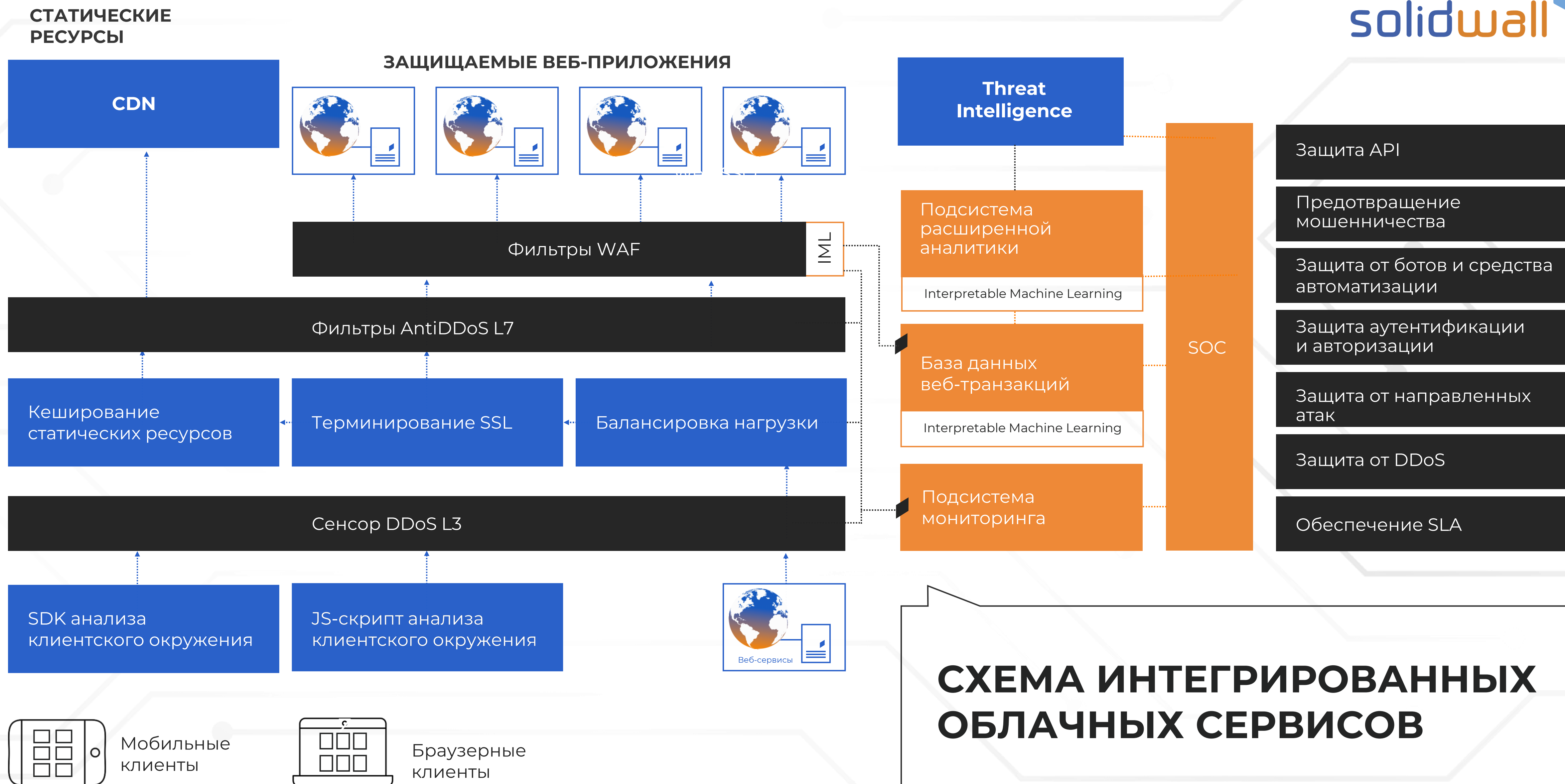
SolidWall WAF поддерживает интеллектуальные алгоритмы машинного обучения, которые позволяют минимизировать затраты ресурсов на настройку WAF. Все результаты машинного обучения в случае необходимости могут быть проанализированы и скорректированы оператором Системы.

3 Эффективный анализ бизнес-логики

SolidWall WAF – единственное на рынке решение, реализующее полноценную реконструкцию бизнес-логики работы приложения. Информация о выполняемых пользователем логических действиях и их параметрах может быть использована для тонкой настройки защиты или экспортирована в другие системы.

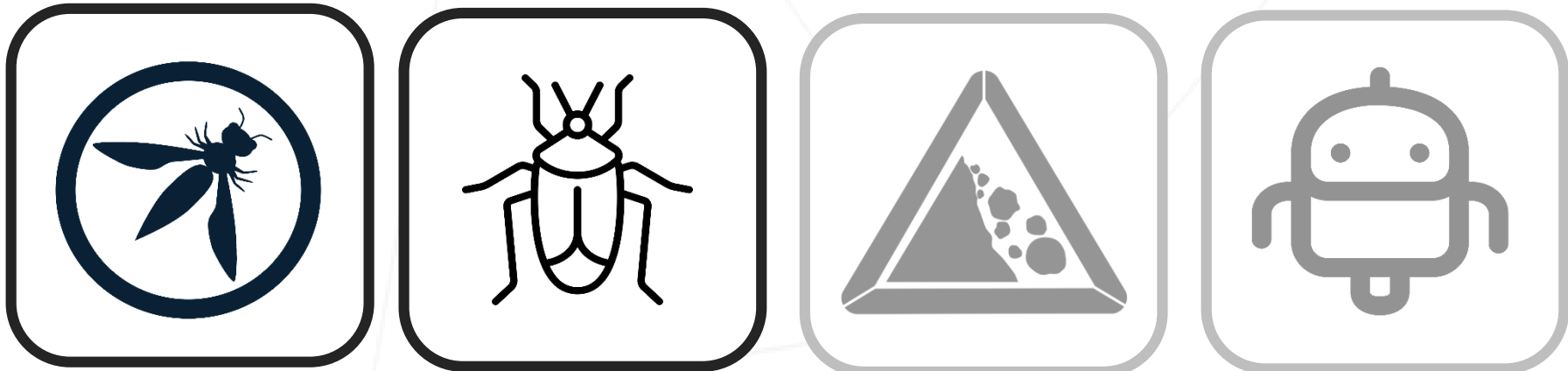
4 Комплексные алгоритмы защиты от переборных атак и ботов

SolidWall WAF имеет многоуровневую защиту от переборных атак и средств автоматизации, которая включает в себя позитивную модель, рейт-лимитинг, анализ поведения пользователей и другие механизмы, которые работают на уровне бизнес-логики и за счет анализа запросов, проходящих через WAF. Полнофункциональный анализ клиентского окружения может быть подключен в случае необходимости.

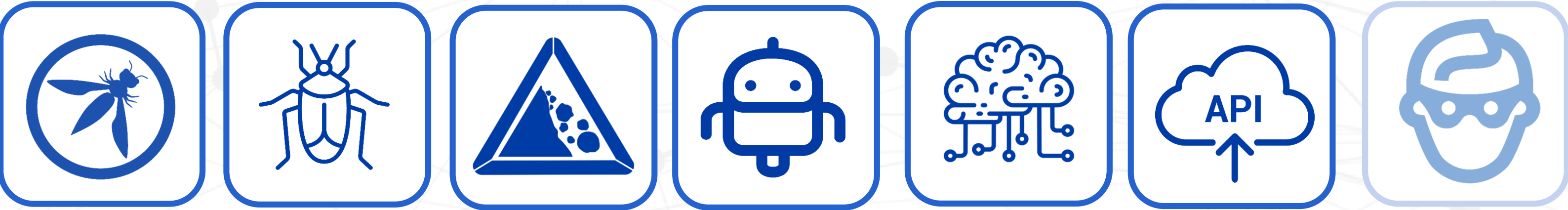


СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ (SAAS)

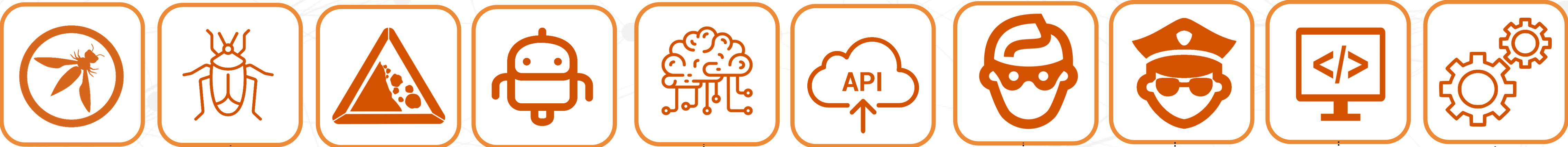
T1



T2



T3



Защита от атак OWASP Top 10

Виртуальный патчинг

Защита от DoS и DDoS атак

Защита от переборных атак и ботов

Защита от логических атак

Защита API

Защита от мошенничества

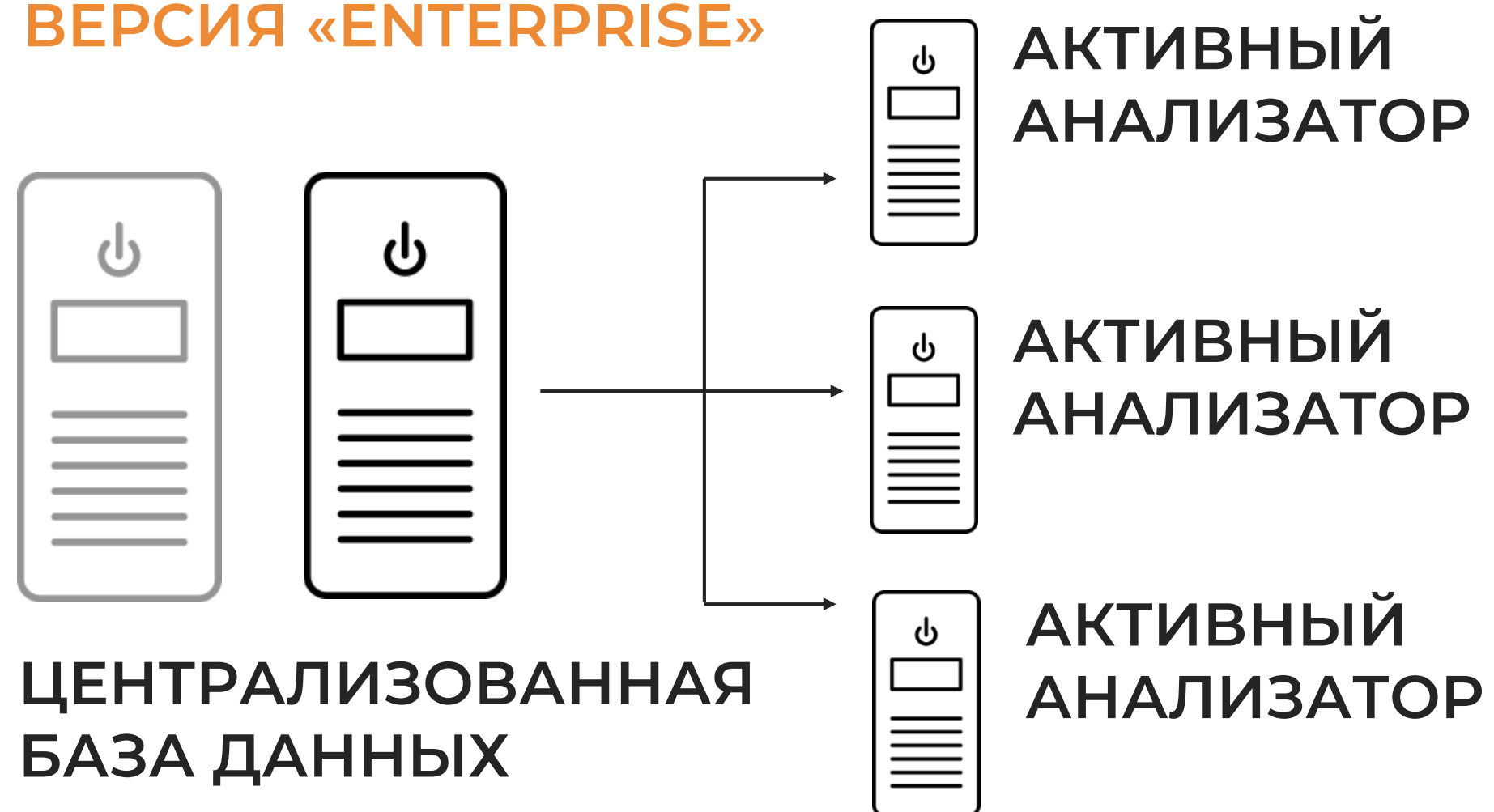
Защита внутренних систем/UBA

Индивидуальная конфигурация

Интеграция с SDLC

STANDALONE РЕШЕНИЕ

ВЕРСИЯ «ENTERPRISE»



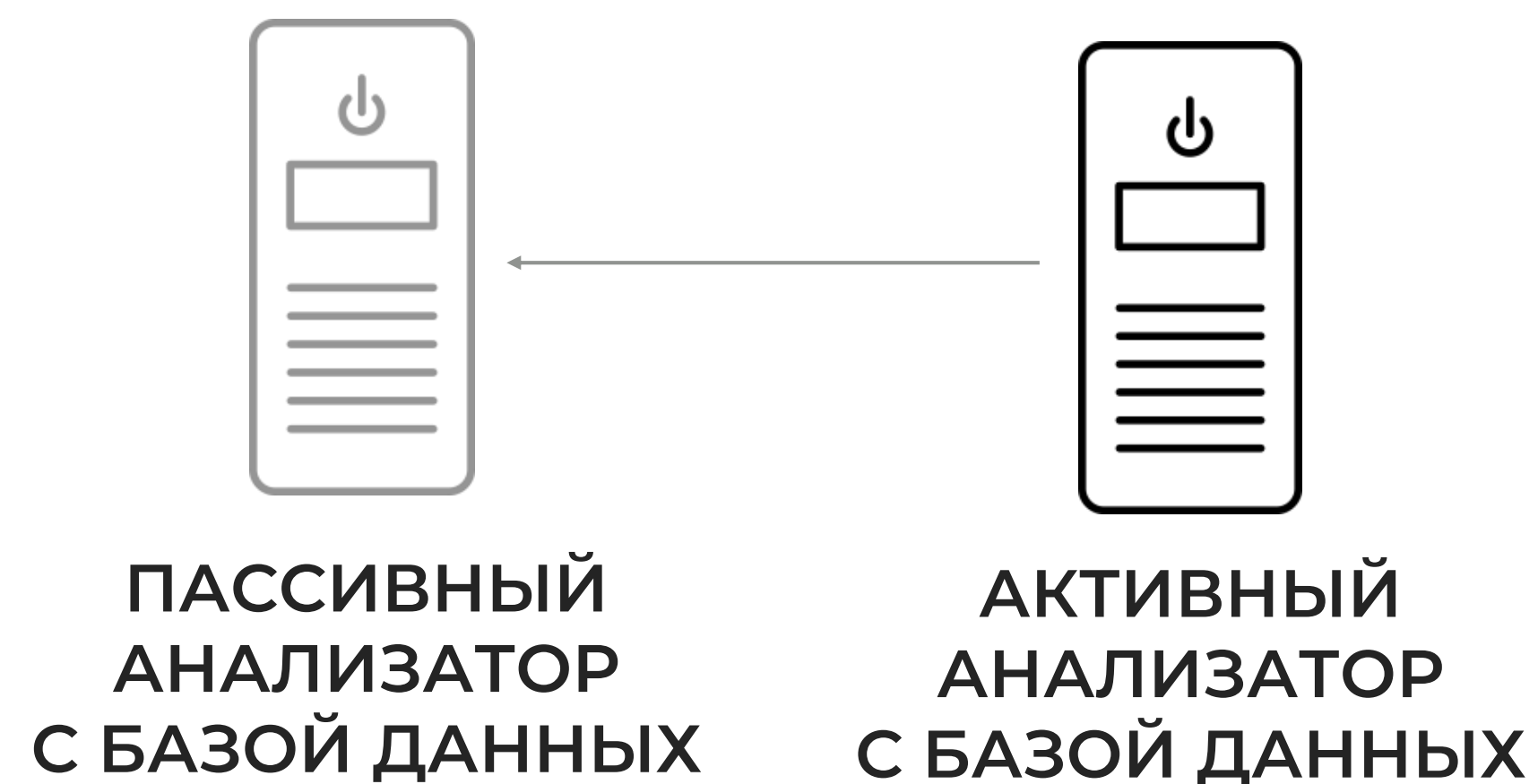
Выделенный узел БД и централизованное управление несколькими анализаторами в режиме Active/Active для версии Enterprise

Анализатор и БД находятся на одном узле для версии Professional

Неограниченное количество приложений

Поддержка режима multi-tenant (для облачных провайдеров)

ВЕРСИЯ «PROFESSIONAL»



Режимы работы: «в разрыв», «на зеркальном трафике», анализ логов веб-сервера

Терминирование SSL и балансировка нагрузки

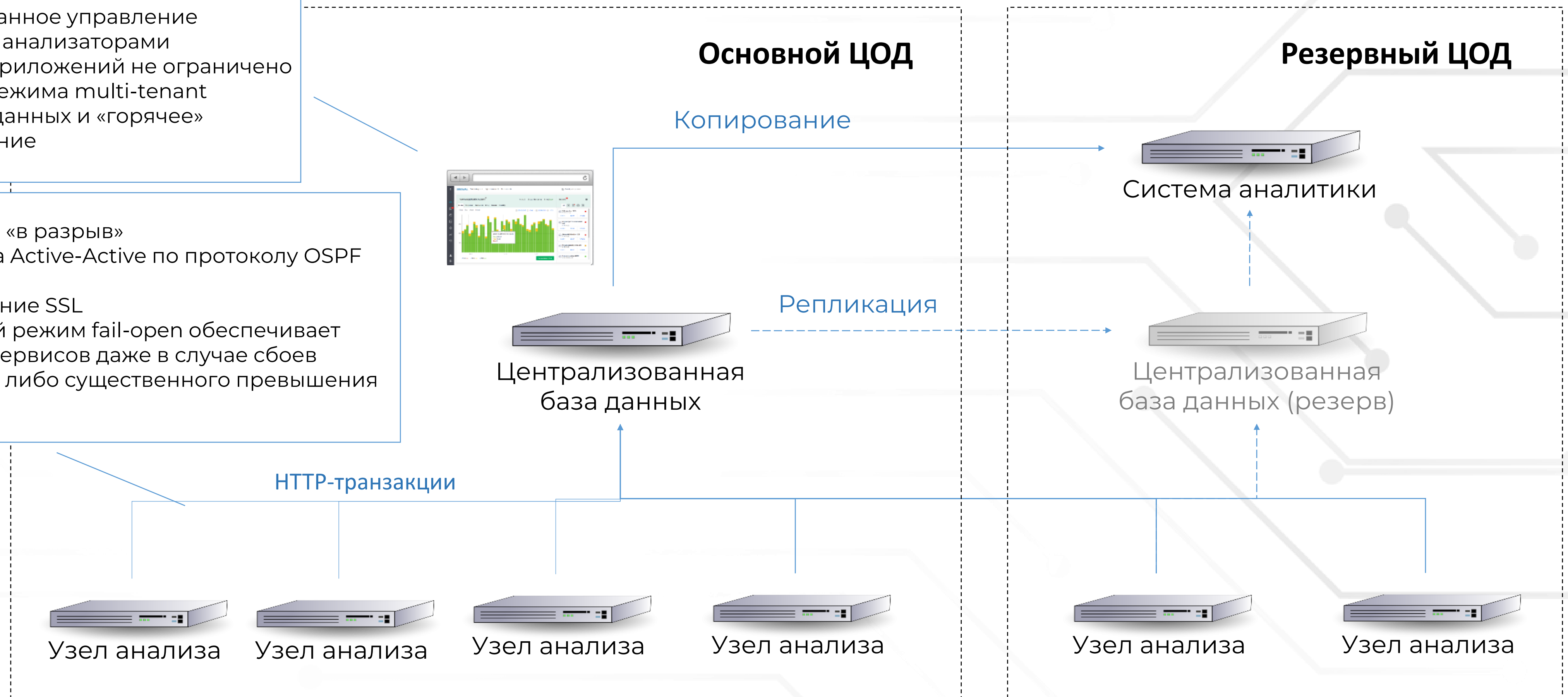
Репликация данных и «горячее» резервирование

Программный режим «fail open» обеспечивает доступность сервисов даже в случае сбоев модулей WAF либо существенного превышения нагрузки

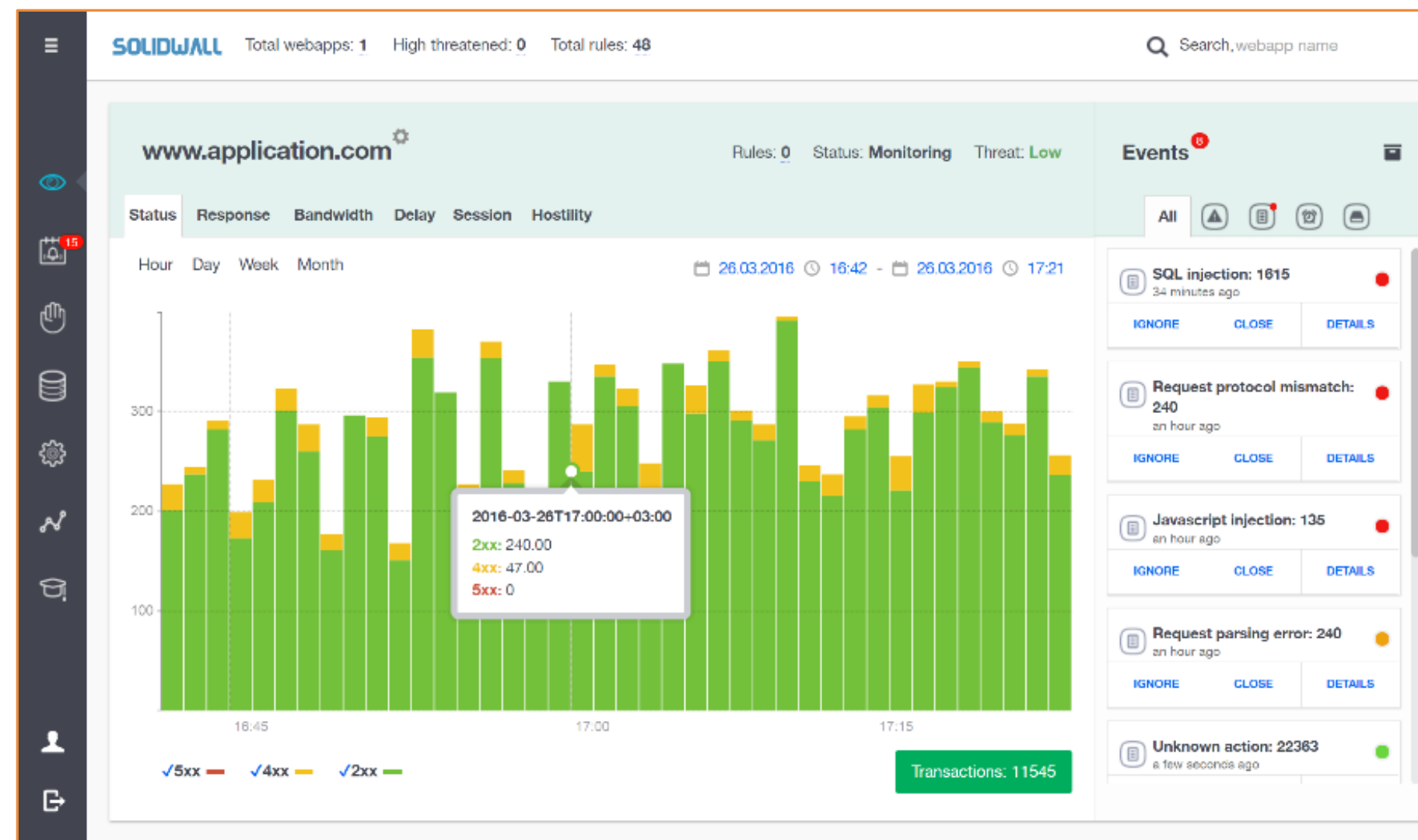
УСТАНОВКА НА ПЛОЩАДКЕ ЗАКАЗЧИКА

- Централизованное управление несколькими анализаторами
- Количество приложений не ограничено
- Поддержка режима multi-tenant
- Репликация данных и «горячее» резервирование

- Схема работы «в разрыв»
- Балансировка Active-Active по протоколу OSPF или на L7
- Терминирование SSL
- Программный режим fail-open обеспечивает доступность сервисов даже в случае сбоев модулей WAF либо существенного превышения нагрузки



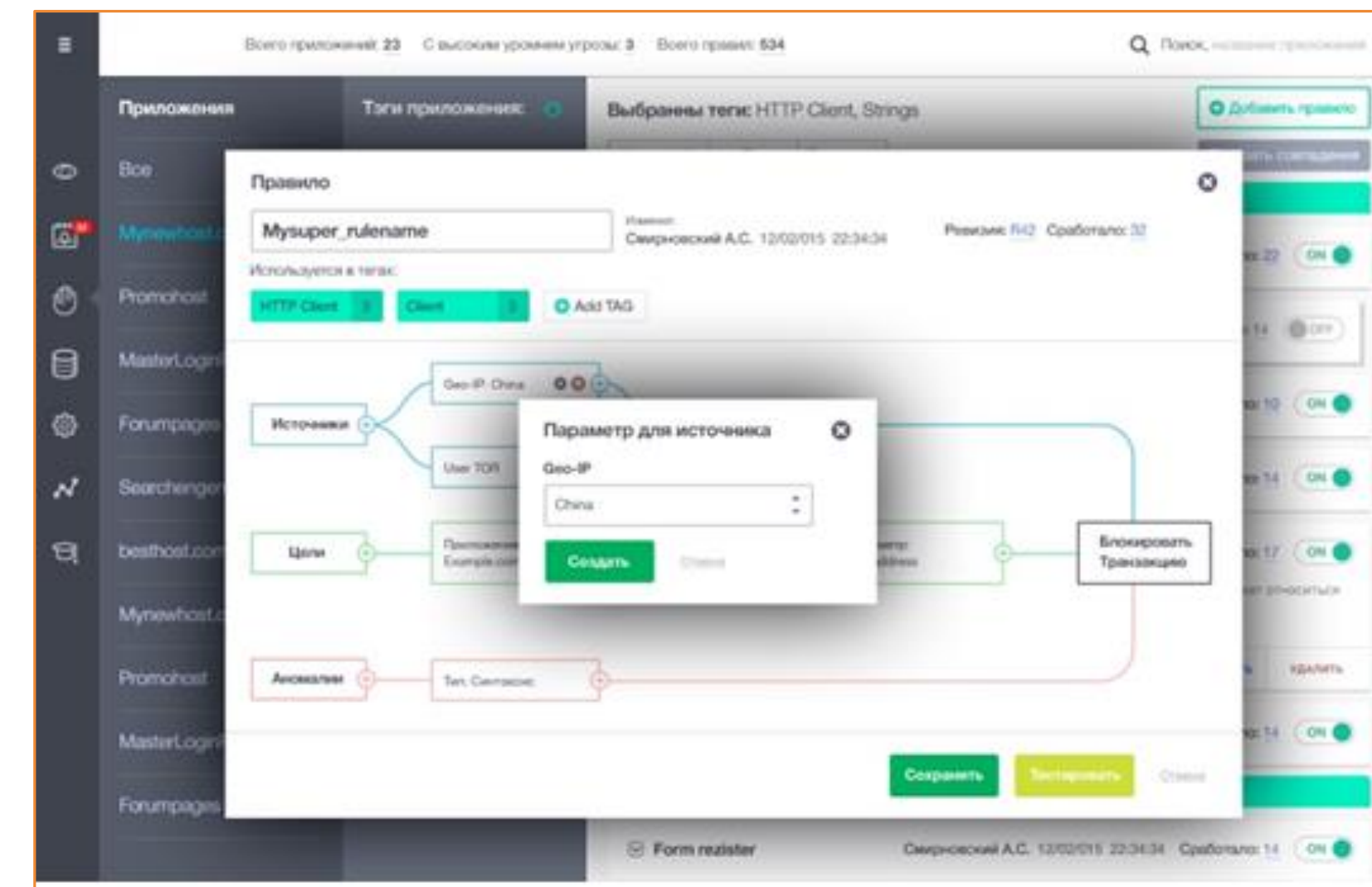
ИНТЕРФЕЙС УПРАВЛЕНИЯ



Динамический веб-интерфейс, реализованный с использованием HTML5, JavaScript и AJAX

Возможность управления с использованием REST API

Централизованное управление всеми узлами инсталляции из единого интерфейса



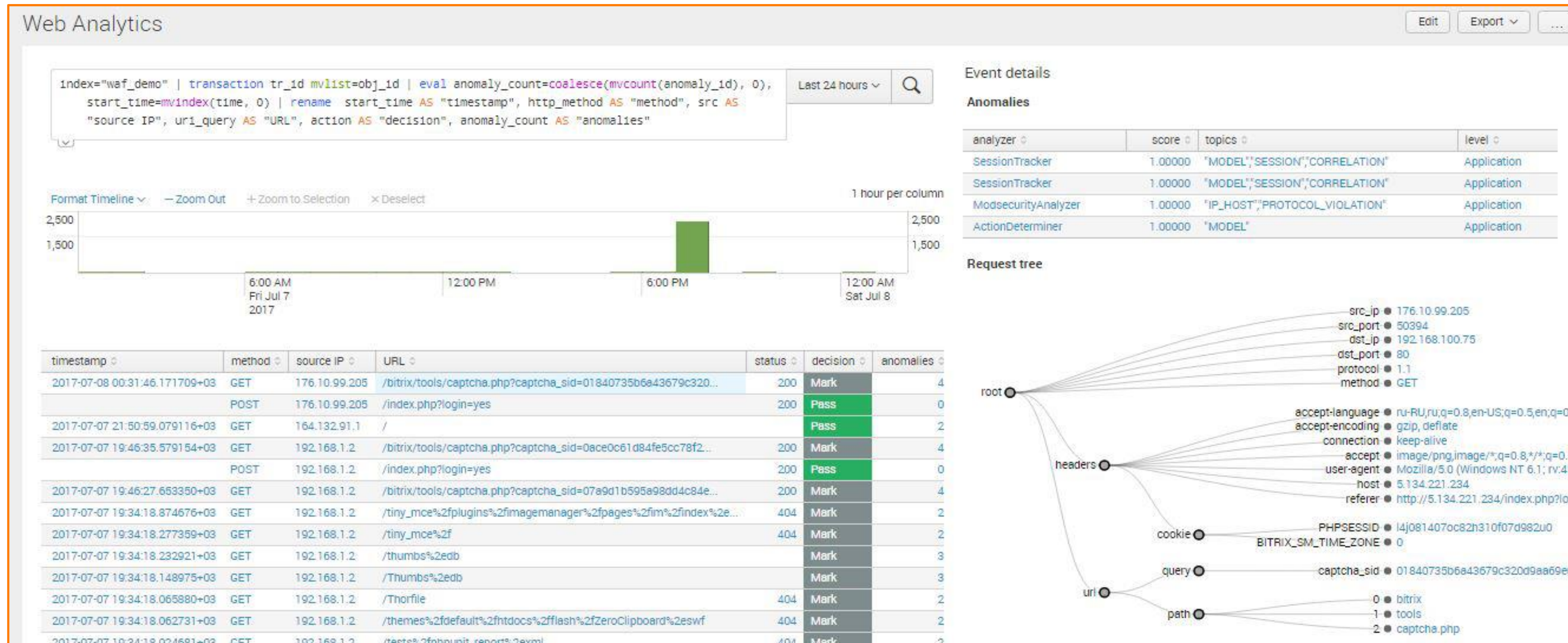
Графическое визуальное представление моделей для упрощения использования

Удобная система мониторинга с набором панелей и группировкой событий ИБ

Версионность всех настроек

Ролевой доступ к функциям интерфейса и подробный аудит действий пользователей

РАСШИРЕННАЯ АНАЛИТИКА И ВНЕШНЯЯ ИНТЕГРАЦИЯ



Континент TLS



SNMP ICAP



Prometheus

ПРОФЕССИОНАЛЬНЫЕ СЕРВИСЫ

РАСШИРЕННОЕ СОПРОВОЖДЕНИЕ SOLIDWALL WAF

Регламентные работы

- Мониторинг «здоровья» инсталляции
- Обновление WAF и устранение ошибок в работе решения
- Устранение ложных срабатываний
- Реагирование на инциденты, критичные для Заказчика

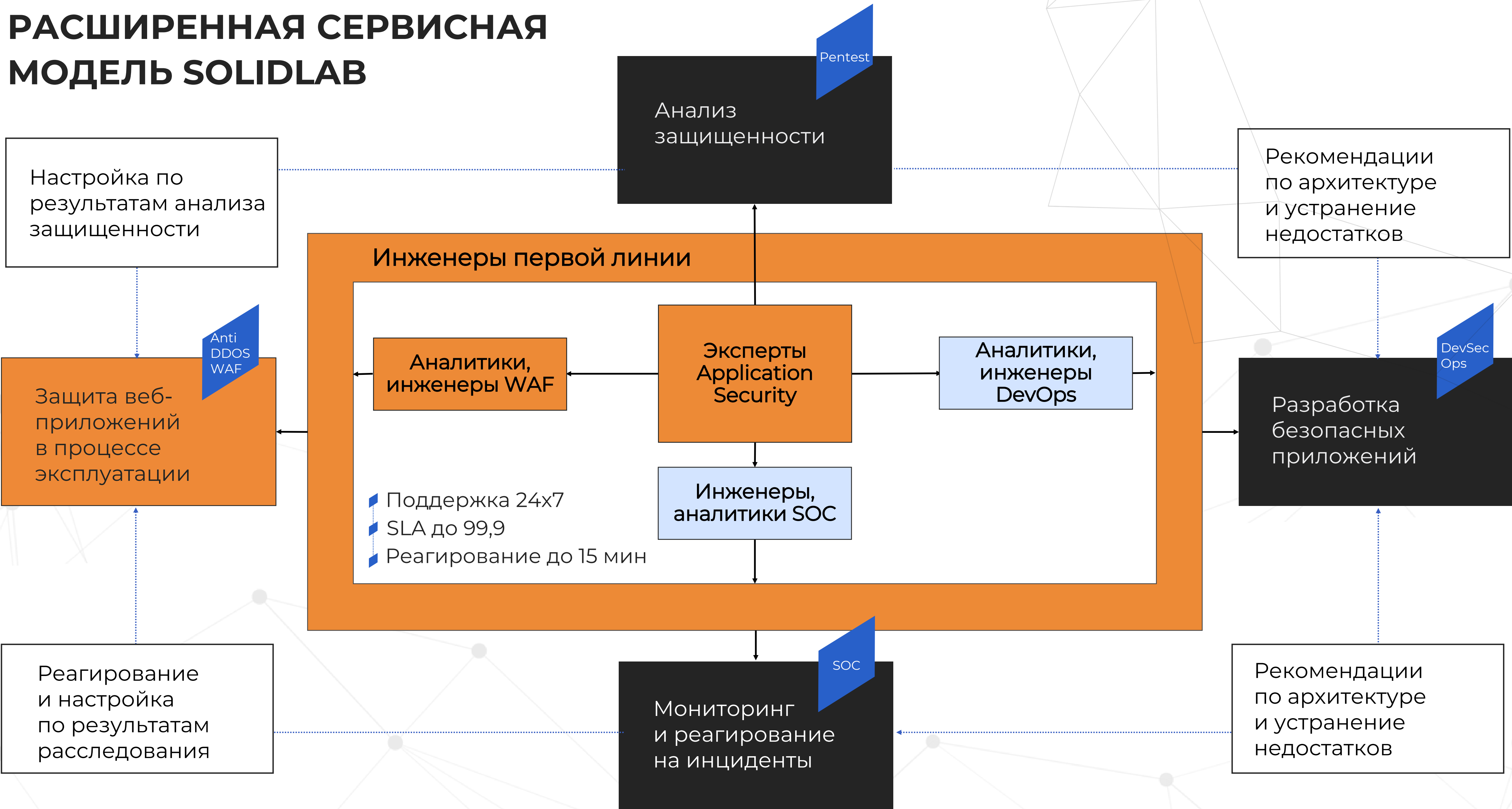
Работы в рамках дополнительных часов профессиональных сервисов

- Тонкая настройка WAF под изменения приложений заказчика
- Ретроспективный анализ событий, настройка WAF для защиты от переборных атак и ботов
- Расследование инцидентов
- Разработка периодических аналитических отчетов
- Экспертные консультации по вопросам безопасной разработки

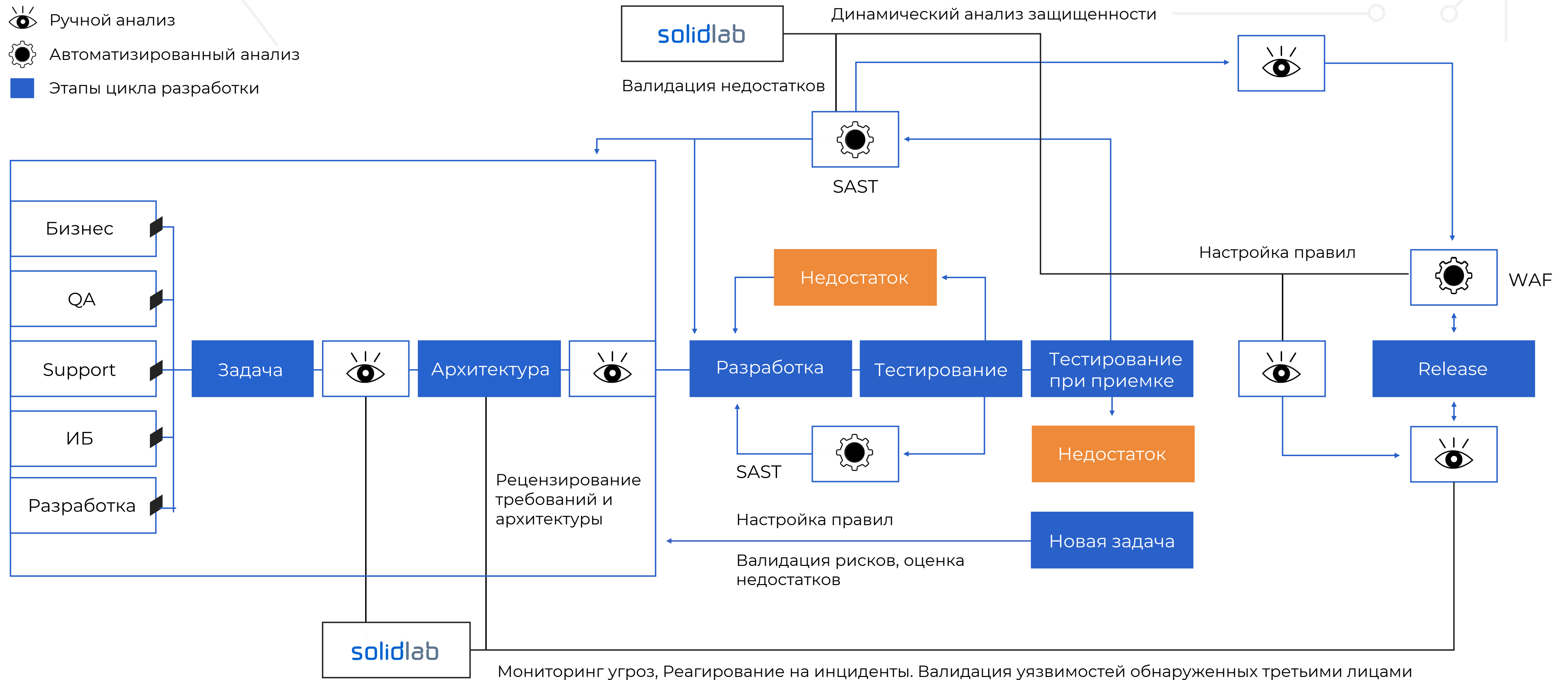
ПРЯМОЕ/СОВМЕСТНОЕ СОПРОВОЖДЕНИЕ

Услуги оказывают высококвалифицированные российские специалисты, имеющие значительный опыт в области противодействия интернет-угрозам

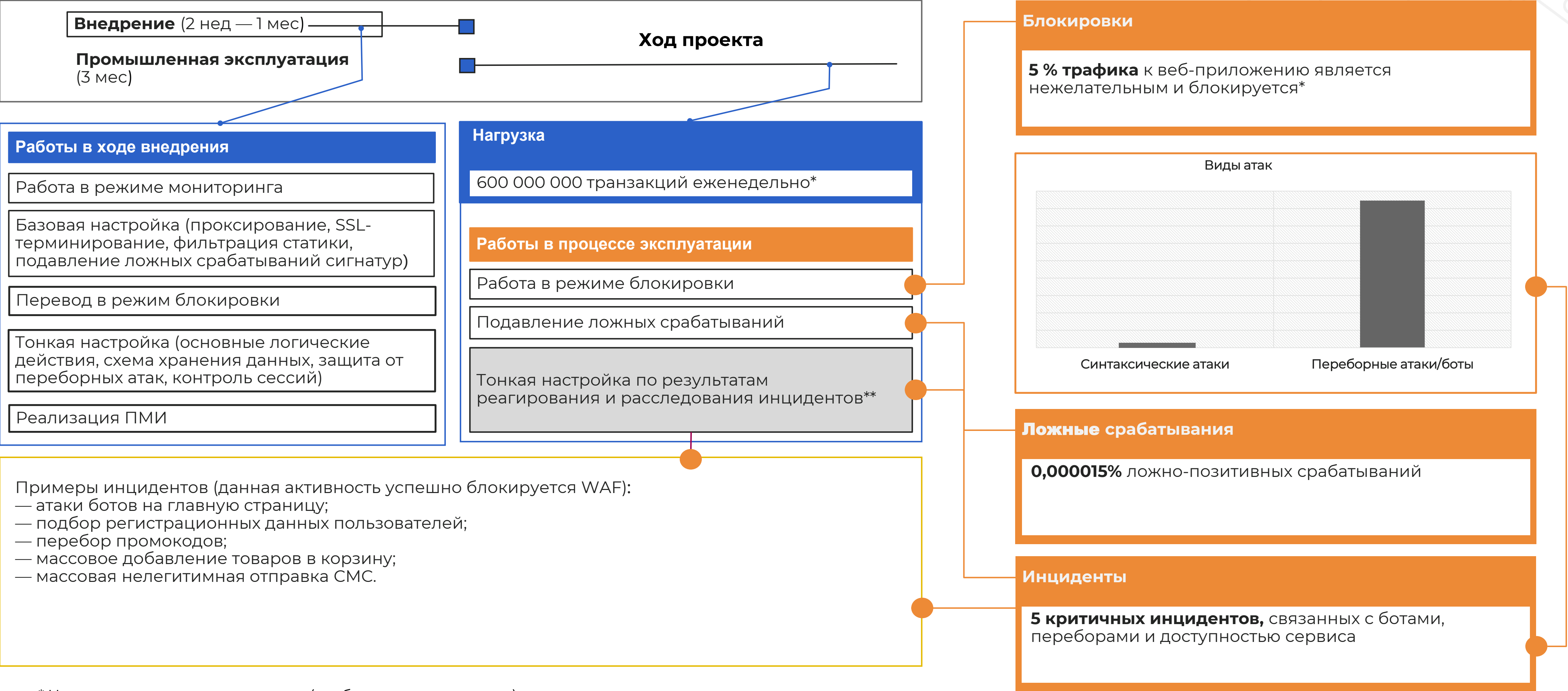
РАСШИРЕННАЯ СЕРВИСНАЯ МОДЕЛЬ SOLIDLAV



WAF В ОБЩЕЙ СХЕМЕ APPLICATION SECURITY



ОСОБЕННОСТИ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ



* Не включая статические ресурсы (изображения, стили и т.п.)
** Существенные инциденты, выявленные вручную по результатам мониторинга



SolidSoft, российский разработчик решений по защите веб-приложений, в 2014 году был выделен в самостоятельную компанию из лаборатории безопасности [SolidLab](#).

Команда следует практическому подходу к ИБ, определяя реальный уровень защищенности организаций, предупреждая риски кражи конфиденциальных данных и проникновения кибергрупп в инфраструктуру компаний.

Флагманский продукт

- Интеллектуальный сетевой экран уровня приложений SolidWall WAF: анализирует и фильтрует трафик веб-ресурсов и мобильных приложений.

Услуги

- Анализ защищенности приложений и инфраструктуры. Тестирование на проникновение.
- Внедрение процессов разработки защищенных приложений. DevSecOps.
- Мониторинг, реагирование и расследование инцидентов. Security Operation Center.

79 NPS

показатель
лояльности
клиентов

98%

заказчиков
удовлетворены
качеством
сервиса

> 300

успешных
проектов

Клиенты



Лицензии и реестры



SolidWall WAF включен в Единый реестр российских программ приказом Минцифры России от 30.12.2020 №799.



Лицензия ФСТЭК № 1741 от 16.05.2017 на деятельность по разработке и производству средств защиты конфиденциальной информации.

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

Сулейман Халилов, начальник отдела
информационной безопасности банка Expressbank



Профессионализм, четкое видение конечного результата, а также высокий уровень компетенции специалистов SolidSoft позволили в сжатые сроки обеспечить безупречный результат. Компания всегда оперативно отвечает на все наши запросы, в результате работа становится более комфортной и плодотворной. Мы уверены, что наше сотрудничество будет долгосрочным и надежным.

Серов А.Ю., руководитель дирекции по обеспечению
безопасности департамента обеспечения
деятельности СЗРЦ Банка ВТБ (ПАО)



Северо-Западный региональный центр Банка ВТБ (ПАО) благодарит ООО «Солидлаб» за успешное завершение проекта по совершенствованию защиты системы дистанционного банковского обслуживания «Клиент-Телебанк» от внешних атак на основе «Интеллектуального сетевого экрана для защиты веб-приложений SolidWall, а также за его эффективную поддержку в процессе эксплуатации в Банке.



unibank



ВТБ



TINKOFF



CENTRAL BANK
OF THE REPUBLIC OF AZERBAIJAN



открытие | БАНК



INTERNATIONAL BANK
OF AZERBAIJAN

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

Александр Орешков, руководитель департамента информационной безопасности группы «М.Видео-Эльдорадо»

М.видео

Благодаря совместной работе с компаниями StormWall и SolidSoft мы смогли запустить систему защиты высокого уровня с точки зрения качества и функциональности.

РД

QIWI
всё проще

М.видео



Билайн

@mail.ru
group

WIFIRE

Avito

X5RETAILGROUP