Денис Прохорчик
Директор направления
по развитию бизнеса
облачных продуктов

Кирилл Герасменко
Ведущий менеджер
по развитию бизнеса AppSec

PT AF PRO / PT Cloud AF

Экспертный межсетевой экран для любого бизнеса

А зачем вообще защищать веб-приложения?

- Страшилки: атак много и будет еще больше! +50% каждый год!
- Рост онлайн-трафика
- Репутационные риски — множество публикаций в СМИ
- Лояльность клиентов
- Утечки данных у соседей
- Оборотные штрафы
- Быть в курсе

Как защитить приложения

Внешний аудит защищенности

black-box, white-box testing

- Инвентаризация периметра
- Отчеты о подтвержденных уязвимостях
- Риски эксплуатации

Межсетевой экран уровня веб-приложений

web application firewall (WAF)

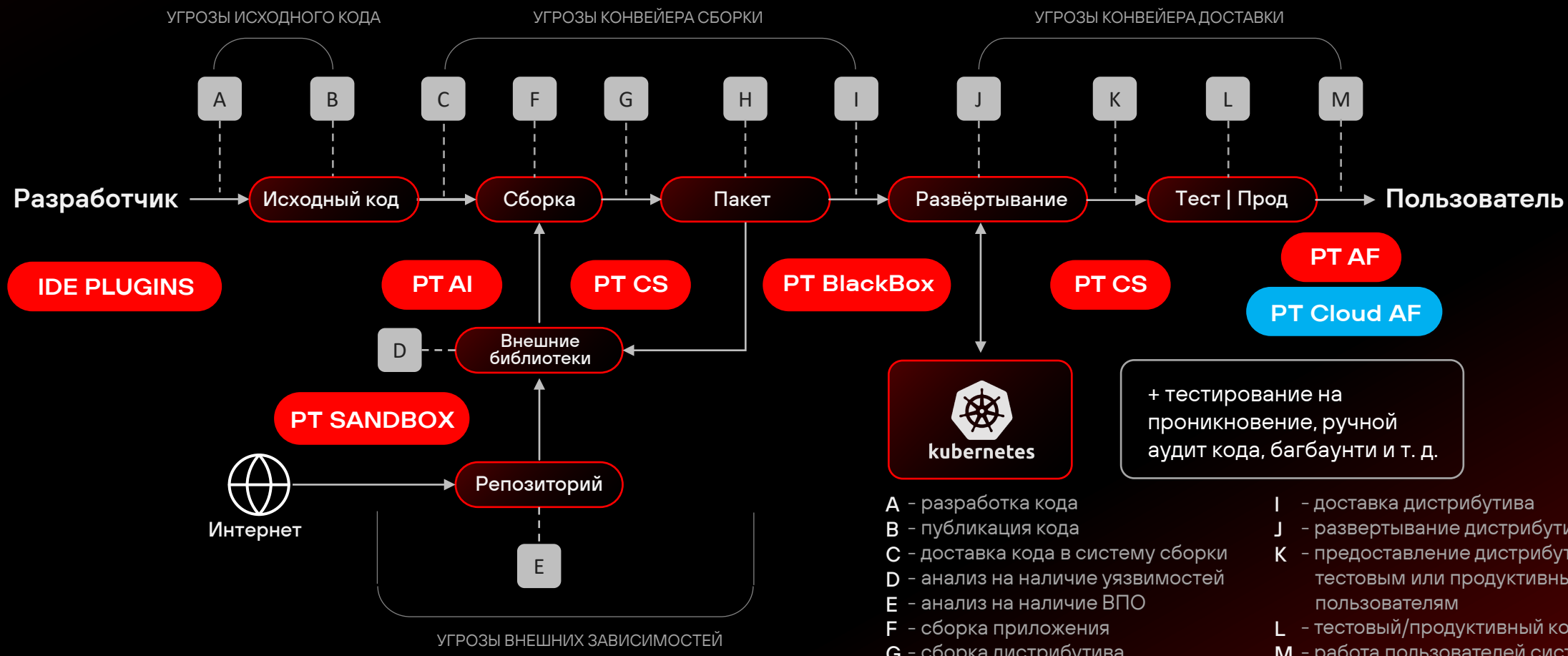
- Оперативная защита от эксплуатации выявленных уязвимостей
- Проактивная защита от угроз нулевого дня

Построение безопасной разработки

DevSecOps

- Выявление и устранение уязвимостей на ранних этапах — написания кода и сборки приложения

Наш стек



A - разработка кода
B - публикация кода
C - доставка кода в систему сборки
D - анализ на наличие уязвимостей
E - анализ на наличие ВПО
F - сборка приложения
G - сборка дистрибутива
H - дистрибутив
I - доставка дистрибутива
J - развертывание дистрибутива
K - предоставление дистрибутива тестовым или продуктивным пользователям
L - тестовый/продуктивный контур
M - работа пользователей системы

01

PT AF PRO / PT Cloud AF

Разная поставка — единая экспертиза для любого бизнеса

PT Cloud AF

SMB, e-comm, cloud native

- Ежемесячная подписка, OPEX
- Не требуется размещать компоненты в своей инфраструктуре
- Подключение за считаные минуты через поставщика услуг
- Риски простоя у поставщика услуг
- Доступ к необходимым функциям
- Всегда актуальная (последняя) версия продукта, быстрая доставка обновлений
- Обработка трафика поставщиком услуги, хранение событий безопасности — у вендора
- Не подлежит сертификации ФСТЭК

PT AF PRO

LE, Гос. сектор, банки, мед.

- Срочные лицензии с передачей прав, CAPEX. Доступны бессрочные лицензии
- Обработка трафика и хранение событий безопасности внутри периметра инфраструктуры
- Полный доступ ко всем функциям
- Сертификат ФСТЭК
- Место в стойке, электропитание
- Сопровождение (настройка, обновление, обслуживание) у эксплуатанта
- Возможна работа без доступа в интернет

Эволюция PT Application Firewall

PT AF 3

- С 2013 года на рынке
- 700+ инсталляций
- Лидер рынка LE

2023

On-premise

PT AF PRO

- Новое поколение AF
- Мультитенантность
- Гибкость и масштабируемость

2023

Cloud-решение

PT Cloud AF

- Услуга
- Быстрый запуск
- Простота управления

Q4 2023

Лучшая экспертиза на рынке WAF

10+ лет

С 2013 года защищает заказчиков более 700 компаний по всему миру

Red team, pentest

Раньше других узнаем о новых уязвимостях, потому что наши специалисты тестируют на проникновение ИТ-инфраструктуры сотен компаний, а также имитируют реальные атаки

Positive Research

Глобально и среди клиентов исследует защищенность веб-приложений и тренды, публикует отчеты

Bug Bounty

Единственный WAF, который не боится участвовать в Bug Bounty. За успешную эксплуатацию уязвимостей белые хакеры могут претендовать на выплаты, а вендор улучшает защиту своего продукта. Клиент получает]защищенный продукт

PT AF PRO | PT Cloud AF

PT ESC

Следит за появлением новых уязвимостей в веб-приложениях и оперативно выпускает пакеты экспертизы

Standoff 365

На платформе специалисты компаний эксплуатируют PT AF, настраивая защиту от 10 000 белых хакеров. Компаниям это позволяет повышать навыки тестирования безопасности, а вендору — собирать обратную связь, чтобы непрерывно улучшать продукт

Преимущества PT Application Firewall

Анализирует трафик и приоритизирует уязвимости

- Глубокая экспертиза и накопленная база знаний
- Аналитика и отчетность в режиме реального времени
- Интуитивный и информативный дашборд
- Маппинг уязвимостей
- Машинное обучение

Защищает от уязвимостей и блокирует атаки

- Производительность и надежность
- Анализ угроз в реальном времени
- Расширенная защита от угроз
- Обнаруживает и останавливает атаки на ранних этапах
- Пользовательские правила
- Управление ботами
- Шифрование SSL (TLS)
- Шифрование ГОСТ TLS
- Защита от DDoS
- Защита API

Автоматизирует процессы обеспечения информационной безопасности приложений

- Горизонтальное масштабирование
- Гибкость
- Удобство в использовании
- Автоматические обновления
- Доступ к API
- Балансировка нагрузки
- Соответствие стандартам регуляторов

Анализ трафика и приоритизация уязвимостей

Глубокая экспертиза и накопленная база знаний

PT AF разработан на основе результатов многочисленных пентестов, которые регулярно проводят хакеры компании Positive Technologies. В компании работают продвинутые пентестеры, которые знают, как взломать и защитить веб-приложения. Этот накопленный практический опыт и знания легли в основу разработки PT AF

Аналитика и отчетность в режиме реального времени

Эксперты компании Positive Technologies предоставят вам подробные и информативные аналитические отчеты, которые помогут контролировать безопасность вашего приложения и выявлять потенциальные угрозы

Интуитивный и информативный дашборд

При входе в PT AF вы сразу увидите дашборд, который позволяет оценить ситуацию и понять, атакуют вас или нет. PT AF автоматически сортирует и ранжирует выявленные атаки и с помощью уникальной технологии построения атак визуализирует угрозы, выделяя наиболее важные из них

Маппинг уязвимостей

PT AF выявляет уязвимость, сопоставляет с базой CVE/CWE. CVE, или Common Vulnerabilities and Exposures, представляет собой общедоступный список известных уязвимостей в программных продуктах. Этот каталог служит отправной точкой для выявления потенциальных рисков и управления ими. CWE, или Common Weakness Enumeration, — набор стандартизированных названий и описаний распространенных угроз программного обеспечения

Машинное обучение

PT AF использует машинное обучение для выявления угроз. Эксперты компании Positive Technologies разработали собственные ML-модели, которые позволяют находить уязвимостив области удаленного выполнения команд на сервере злоумышленниками.
С помощью метода POST с Content-Type: multipart/form-data на защищаемый бэкенд отправляется полезная нагрузка, сгенерированный с помощью Metasploit Framework. Данные полезной нагрузки сравниваются с обученной моделью, и в случае превышения порога вероятности срабатывает правило Metasploit shell code upload

Защита от уязвимостей и блокировка атак

Анализ угроз в реальном времени

PT AF использует анализ угроз в реальном времени для блокировки вредоносного трафика до того, как он достигнет вашего приложения

Обнаруживает и останавливает атаки на ранних этапах

Автоматическая корреляция инцидентов позволяет обнаруживать и останавливать атаки на ранних этапах их развития, отсеивая нерелевантные события и концентрируя внимание на действительно опасных атаках, а также существенно сокращая время их обнаружения

Производительность и надежность

У PT AF нет лимитов по производительности. Он обеспечит непрерывную защиту ваших веб-приложений и их доступность для пользователей. Наши эксперты создали продукт так, чтобы он работал каждую секунду, 24/7

Пользовательские правила

PT AF позволяет создавать собственные правила для запрета вредоносного трафика, уникального для вашего приложения

Расширенная защита от угроз

PT AF использует расширенные механизмы защиты от угроз, в том числе от внедрения SQL-кода, выполнения межсайтовых сценариев и дополнительных интернет-угроз. Точность обнаружения и низкий уровень ложноположительных срабатываний обеспечиваются за счет уникальных математических моделей парсера по грамматикам. Благодаря этому PT AF защищает от всех рисков, описанных в перечне OWASP TOP-10 (Open Web Application Security Project), и даже больше

Управление ботами

Продукт обнаруживает и блокирует вредоносный ботовый трафик, обеспечивая доступность вашего сайта только для легитимных пользователей

Защита от уязвимостей и блокировка атак

Шифрование SSL и TLS

PT AF предлагает шифрование SSL и TLS для безопасного взаимодействия клиента и сервера

Защита API

PT AF защищает не только веб-приложения, но и ваши API

Шифрование ГОСТ TLS

PT AF обеспечивает шифрование с применением отечественных криптоалгоритмов, которое полностью соответствует требованиям государственных регуляторов

Защита от L7 DoS

PT AF защищает от DoS, обеспечивая доступность вашего приложения даже во время хакерских атак

Автоматизация процессов в PT AF PRO

Горизонтальное масштабирование

PT AF можно быстро и легко масштабировать, поскольку решение работает на платформе Kubernetes. Наши клиенты могут самостоятельно добавлять любое количество новых веб-приложений под защиту продукта в рамках лицензии

Гибкость

Решение может поставляться клиенту в соответствии с потребностями его бизнеса. PT AF может быть развернут на инфраструктуре клиента (on-premise), обеспечивая повышенную автономность и защищенность данных, или в «облаках» — приватных или публичных

Балансировка нагрузки

PT AF предоставляет возможности балансировки нагрузки, которые помогают равномерно распределять трафик между веб-серверами, что приводит к сокращению времени загрузки

Доступ к API

PT AF предоставляет доступ к API, что позволит вам автоматизировать и интегрировать рабочие процессы безопасности с вашим приложением

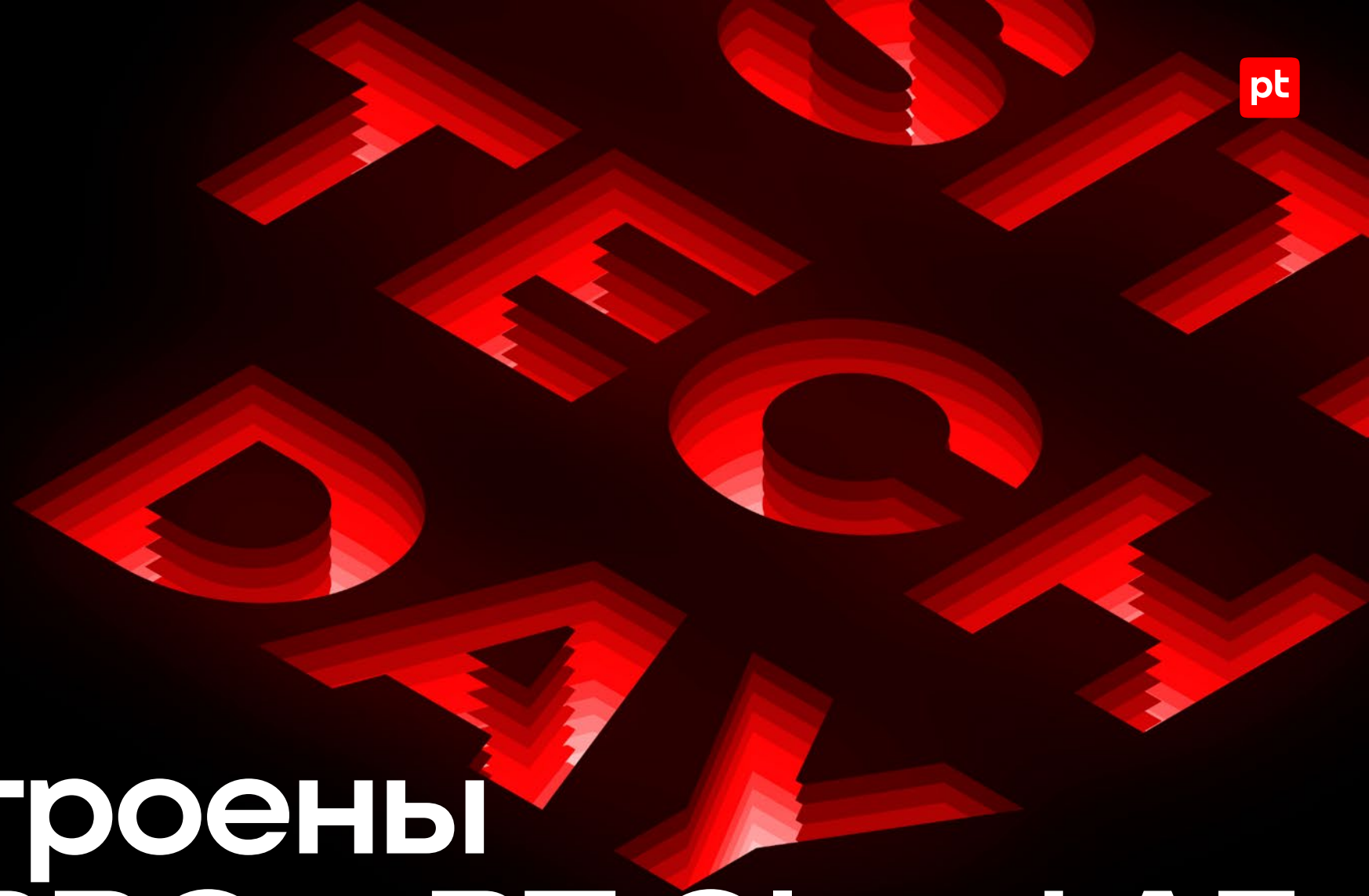
Удобство в использовании

Продукт разработан на основе многочисленных исследований пользователей и на практике доказал свое удобство в использовании

Соответствие стандартам регуляторов

PT AF имеет сертификацию ФСТЭК, обеспечивает соответствие Указу № 250. 151-му закону и требованиям ЦБ, а также PCI DSS

02



Как устроены PT AF PRO и PT Cloud AF

O PT AF PRO

Management

- Orchestration

kubernetes

- Databases

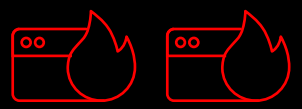
PostgreSQL ClickHouse RabbitMQ MINIO

- Monitoring

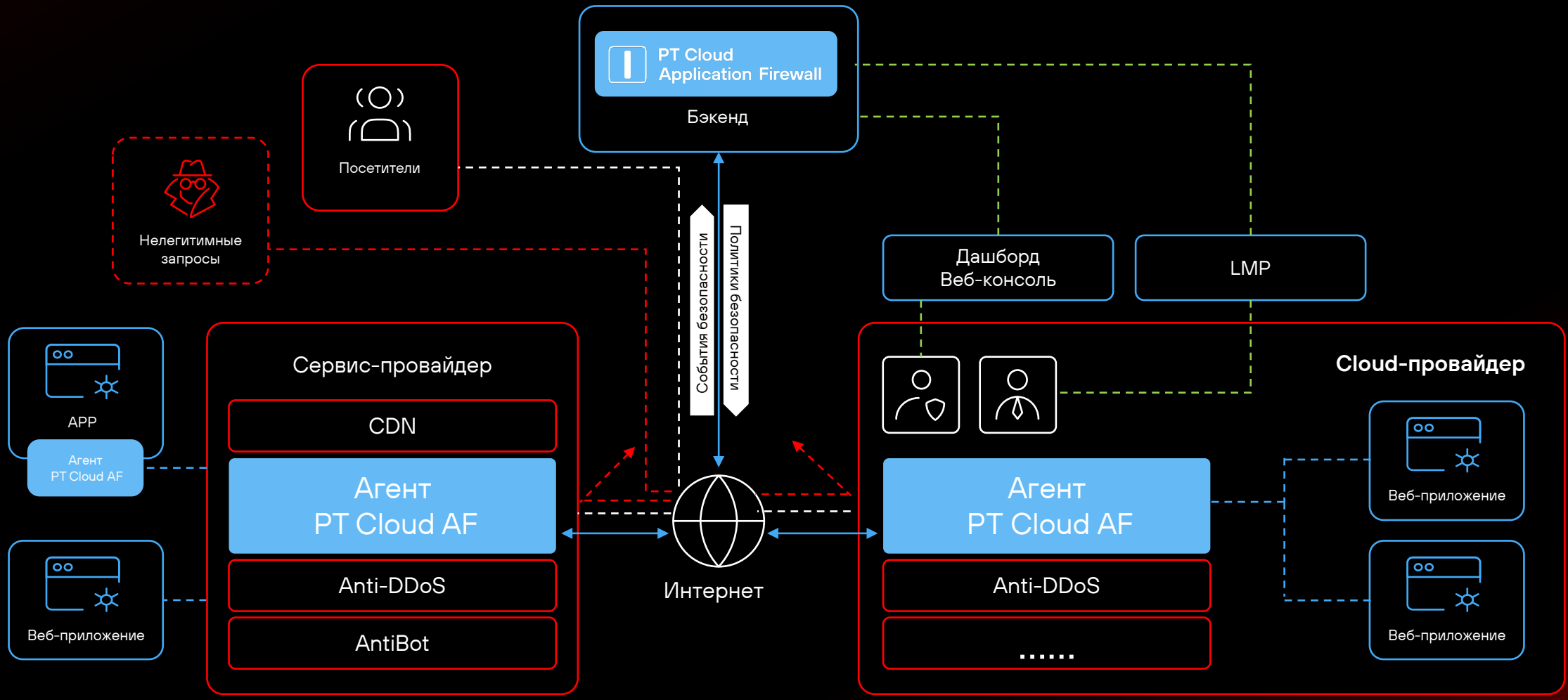
Grafana VICTORIA METRICS

Traffic-processing

- Attack detection



Как работает PT Cloud AF



03

Особенности PT Cloud AF

О PT Cloud Application Firewall и целевой аудитории

Целевая аудитория PT Cloud AF

Не конкурируем с решением on-premise PT AF PRO, но открываем новые рынки WAF
Хотим сделать ИБ доступным для компаний любого размера
Для тех, кто хочет получать безопасность как сервис (OPEX), без затрат на инфраструктуру и команду ИБ

Наша целевая аудитория:

- E-commerce, ритейл
- Интернет-магазины и финансовые организации (страховые, займы, брокеры, криптовалютные компании)
- Информационные ресурсы и порталы
- Образовательные и научные учреждения (университеты, институты, проектные организации, школы)
- Разные агрегаторы (билетов, концертов, отелей, путешествий, кредитов)
- Букмекерские конторы
- Компании, для которых веб-приложение является точкой контакта с клиентами либо несет важную информационную или бизнес-функцию
- Продвинутые cloud-native- и IT-компании

Мы не предлагаем продукт медицинским учреждениям, организациям из госсектора и компаниям, которым необходим сертификат ФСТЭК, а также крупному бизнесу, нацеленному на решения on-premise

Авторизованные технологические партнеры (АТП)

Авторизованные cloud-провайдеры

Поставщики облачных решений, коммерческие центры обработки данных, оказывающие облачные услуги, а также услуги информационной безопасности на базе собственной инфраструктуры

Пример: VK Cloud, Beeline Cloud, Megafon Cloud, Oxygen, K2 Cloud, Nubes и другие.

Услуги: SaaS WAF*, Managed WAF*

Авторизованные сервис-провайдеры

Компании, предоставляющие комплексные услуги информационной безопасности как сервис

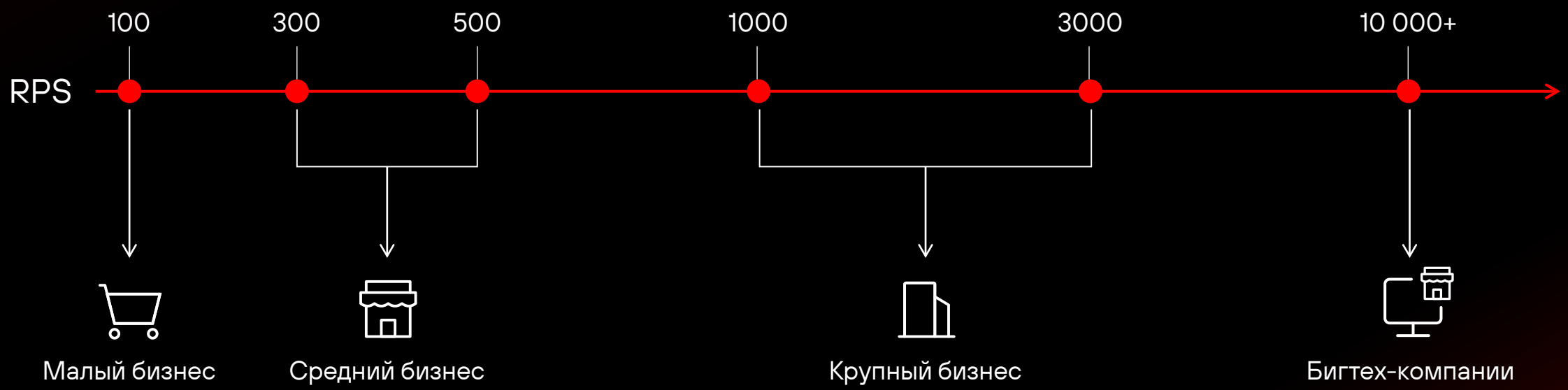
Пример: StormWall, Ngenix, Servicepipe, Qrator, «Лаборатория Касперского» и другие

Не продают WAF как сервис отдельно.
Услуги: min Anti-DDoS + SaaS WAF, Anti-DDoS + Managed WAF

Опционально: CDN, AntiBot и другие

Со списком авторизованных технологических партнеров можно ознакомиться по ссылке Cloud/Service провайдеры (ptsecurity.com) или ptcloud.ru
Если нужного партнера нет в списке, уточните у менеджера по работе с клиентами. Партнер может быть на стадии подписания договора с Positive Technologies

Лицензионная модель



1. Ежемесячная подписка
2. Лицензируем только общий трафик в RPS
3. Пропустим весь легитимный трафик
4. В стоимость подписки включена базовая ТП

Мы только стартанули, но уже преуспели

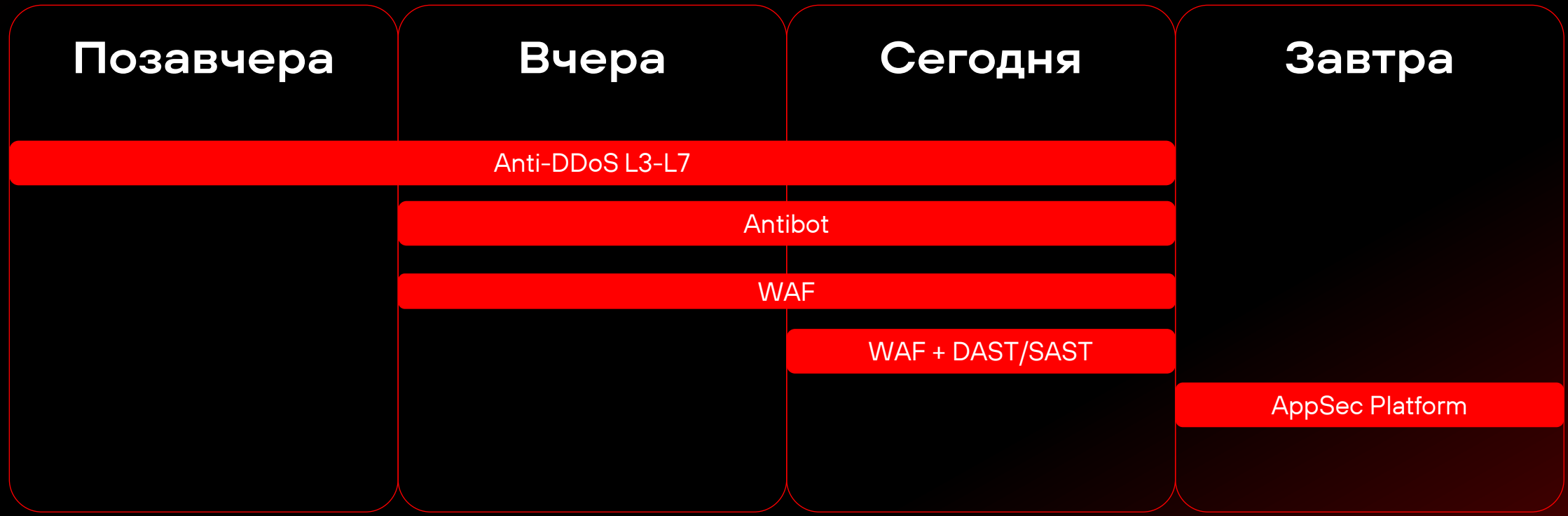
Отрасли, где уже предоставляется сервис на базе PT Cloud AF

- АНО
- Информагентства/реклама
- ИТ, разработка ПО
- Обработка данных и размещение информации
- ИТП, строительство, надзор
- Консалтинг
- Лотереи и азартные игры
- Образование
- Пассажирские перевозки
- Почтовые услуги
- Производство
- Торговля
- Финансы

04

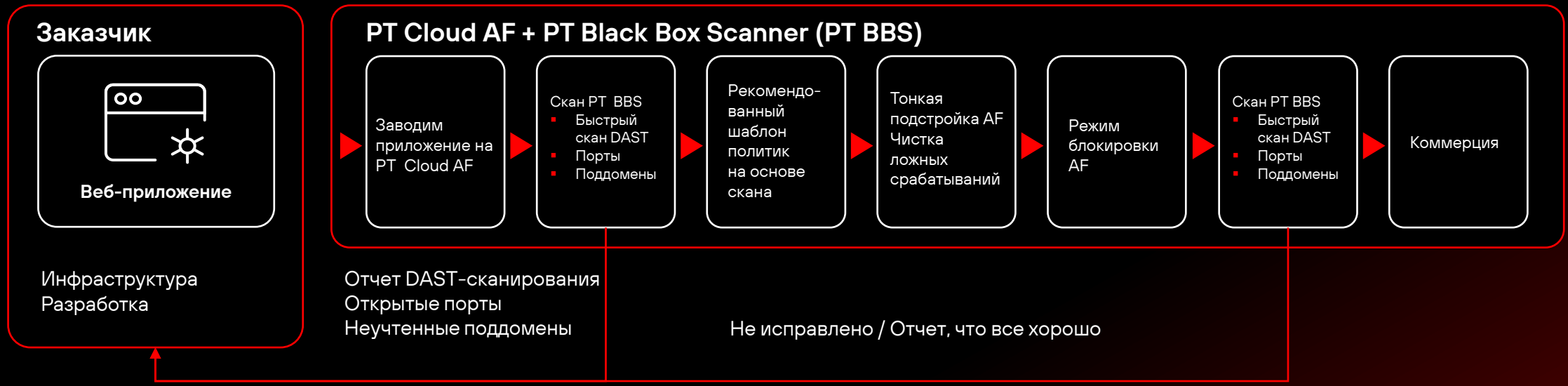
Продуктовая синергия AppSec

Эволюция защиты веб-приложений



Сегодня — продуктовая синергия и коллаборация

PT Cloud AF + PT Black Box Scanner = быстрее и точнее



5 шагов
к безопасности

1

Бесплатное тестирование

Выбираем технологического партнера Сканируем PT Black Box Scanner

2

Начинаем «пилот»

Анализируем результаты скана и стартуем за 1 день

3

Индивидуальная настройка

Подключим продукт и адаптируем его под ваше приложение

4

Чекап защищенности

Убедимся, что все готово. Приложение работает штатно, найденные уязвимости закрыты

5

Коммерция и полный контроль

Заходите в личный кабинет и смотрите, как чувствует себя ваше приложение

Бесплатное тестирование

Лучший способ понять, насколько PT Cloud Application Firewall полезен, — протестировать его на вашем приложении

Спасибо!