PT Application Firewall

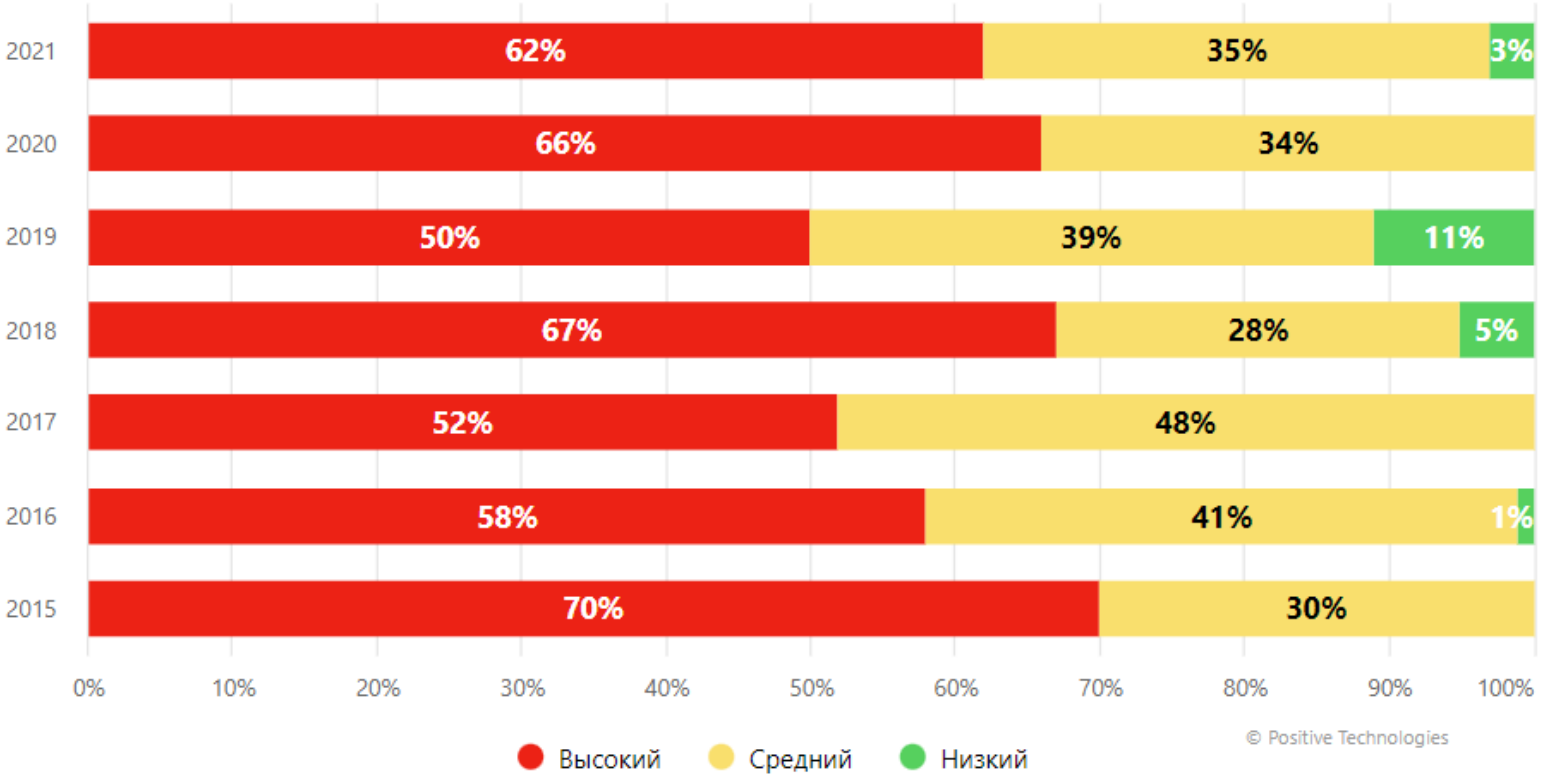
Гибкий инструмент для защиты веб-сервисов компании

Positive Technologies

ptsecurity.com

Актуальность

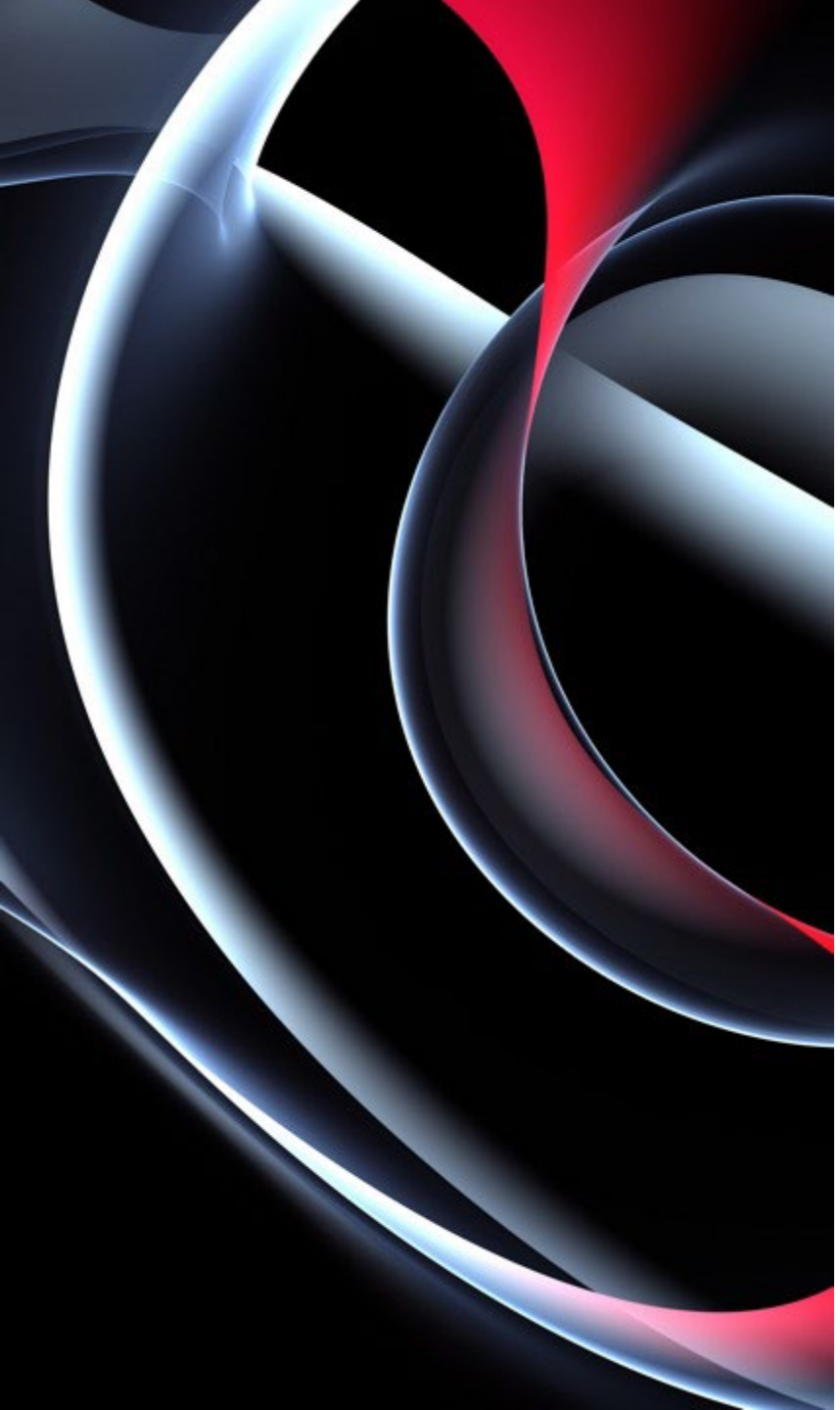
Доля веб-приложений, содержащих уязвимости высокой степени риска, составила **66%***



Доля уязвимых веб-приложений в зависимости от максимальной степени риска уязвимостей

- В абсолютном большинстве веб-приложений (98%) злоумышленники имеют возможность проводить атаки на пользователей*
- В среднем веб-приложения имеют две критически опасных уязвимости
- В 17% веб-приложений оказались возможными атаки на ресурсы ЛВС

* Уязвимости и угрозы веб-приложений в 2020–2021



Репутационные угрозы

Данные 44 тысяч клиентов брокера «Альфа-Кредит» находились в открытом доступе

Посвященный защите информации сайт допустил утечку данных

Персональные данные 12 млн клиентов российских МФО выставлены на продажу

В даркнете выставлена на продажу SQLi-уязвимость на PickPoint.ru

Последствия компрометации приложений

ПОЛУЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФРАСТРУКТУРЕ КОМПАНИИ

- Удаленный запуск кода (RCE)
- Подделка запросов со стороны сервера (SSRF)

Последствия: кража конфиденциальных данных, нарушение работы внутренней инфраструктуры компании.

ПОЛУЧЕНИЕ ЗЛОУМЫШЛЕННИКОМ ДОСТУПА К УЧЕТНОЙ ЗАПИСИ ПОЛЬЗОВАТЕЛЯ

- Межсайтовое выполнение сценариев (XSS)
- Перебор паролей (brute force)
- Подбор учетных данных (credential stuffing)

ОСТАНОВКА БИЗНЕС-ПРОЦЕССОВ

- Злоупотребление логикой работы приложения (web form abuse)
- DDoS-атака

Последствия: финансовые и репутационные потери для компании, недоступность сервисов КИ.

УТЕЧКА ВАЖНЫХ ДАННЫХ

- Внедрение SQL-кода
- Доступ к исходному коду приложений (Git, SVN)
- Неавторизованный доступ к объектам (IDOR)

Последствия: продажа персональных данных в даркнете, репутационный ущерб при освещении в СМИ, крупные штрафы регуляторов (GDPR, 152-ФЗ).

Веб-сервисы периметра

Поддержка Нет поддержки

IN-HOUSE

Клиентские сервисы, порталы, мобильные API

Время исправления уязвимости

OPEN SOURCE

Jira, Gitlab, файлообменники, техподдержка, Wiki

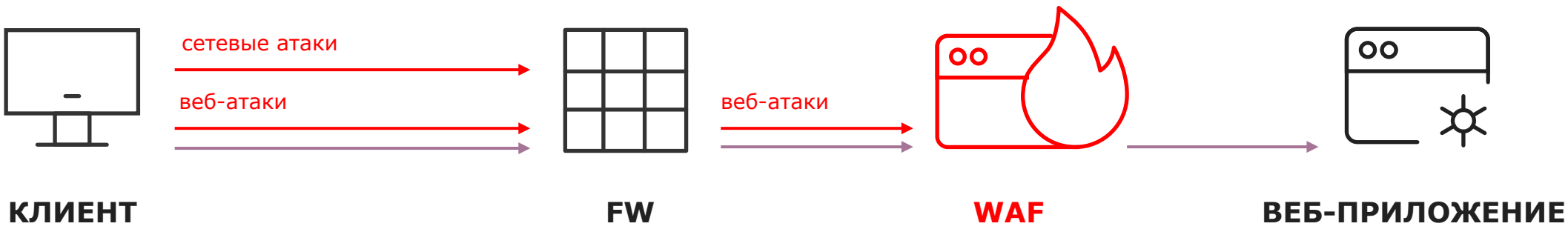
VENDOR

ДБО, OWA, Skype, учебные и кадровые порталы

Как защитить веб-приложения

WAF как одно из средств защиты веб-приложений

- Глубоко (до седьмого уровня) разбирает трафик, специализируется на анализе HTTP и HTTPS
- Учитывает бизнес-логику работы приложений
- Детектирует и предотвращает распределенные по времени атаки
- Защищает API веб-приложения



Ценность

ПОДДЕРЖИВАЕТ НЕПРЕРЫВНОСТЬ БИЗНЕС-ПРОЦЕССОВ

PT Application Firewall обеспечивает защиту от DDoS-атак уровня приложений (седьмой уровень), эксплуатации уязвимостей и связанных с бизнес-логикой приложений.

МИНИМИЗИРУЕТ РИСК УТЕЧКИ ИНФОРМАЦИИ

PT Application Firewall блокирует современные атаки на веб-приложения, устраняет угрозы из списка OWASP Top 10 и классификации WASC, а также автоматически обнаруживает имеющиеся в приложении уязвимости и защищает от их эксплуатации.

АККУМУЛИРУЕТ ЭКСПЕРТИЗУ

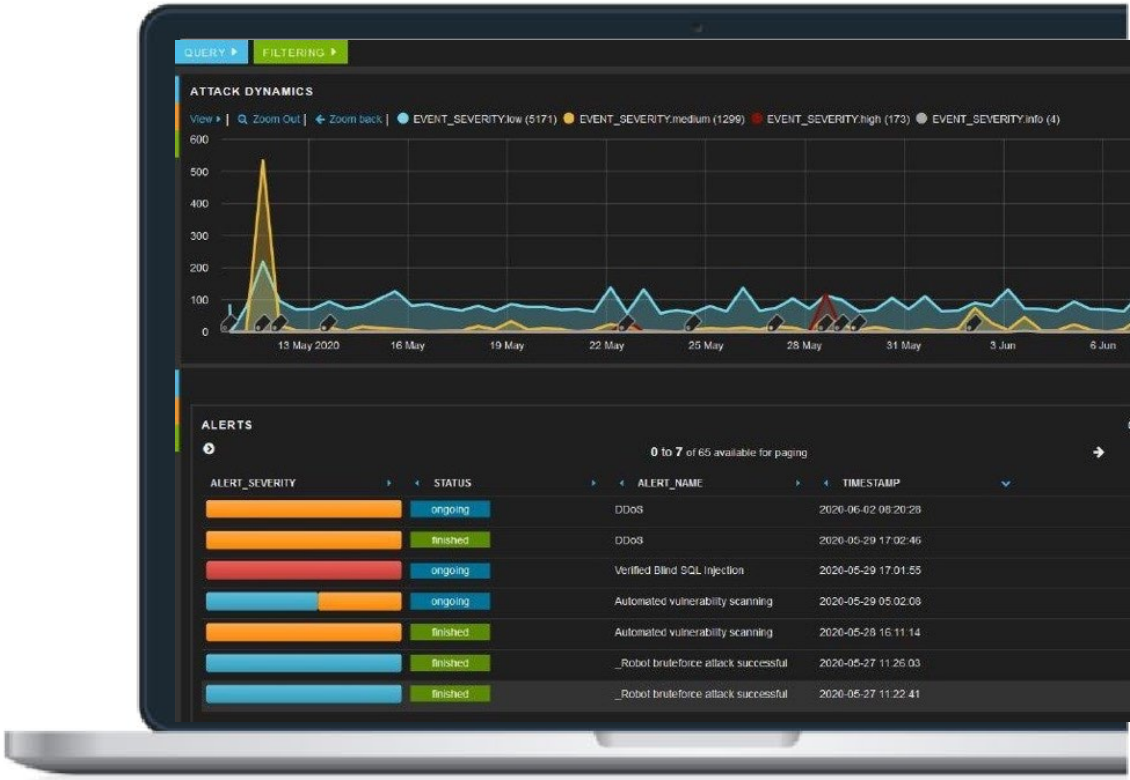
Специалисты отдела анализа защищенности приложений регулярно пополняют базу знаний продукта информацией об уникальных уязвимостях, обнаруженных в реальных приложениях.

ПОМОГАЕТ В ВЫПОЛНЕНИИ ТРЕБОВАНИЙ СТАНДАРТОВ

PT Application Firewall помогает соблюдать требования PCI DSS и других международных, государственных и корпоративных стандартов безопасности. Решение зарегистрировано в реестре российского ПО, имеет действующий сертификат ФСТЭК России и сертификат соответствия Республики Казахстан.

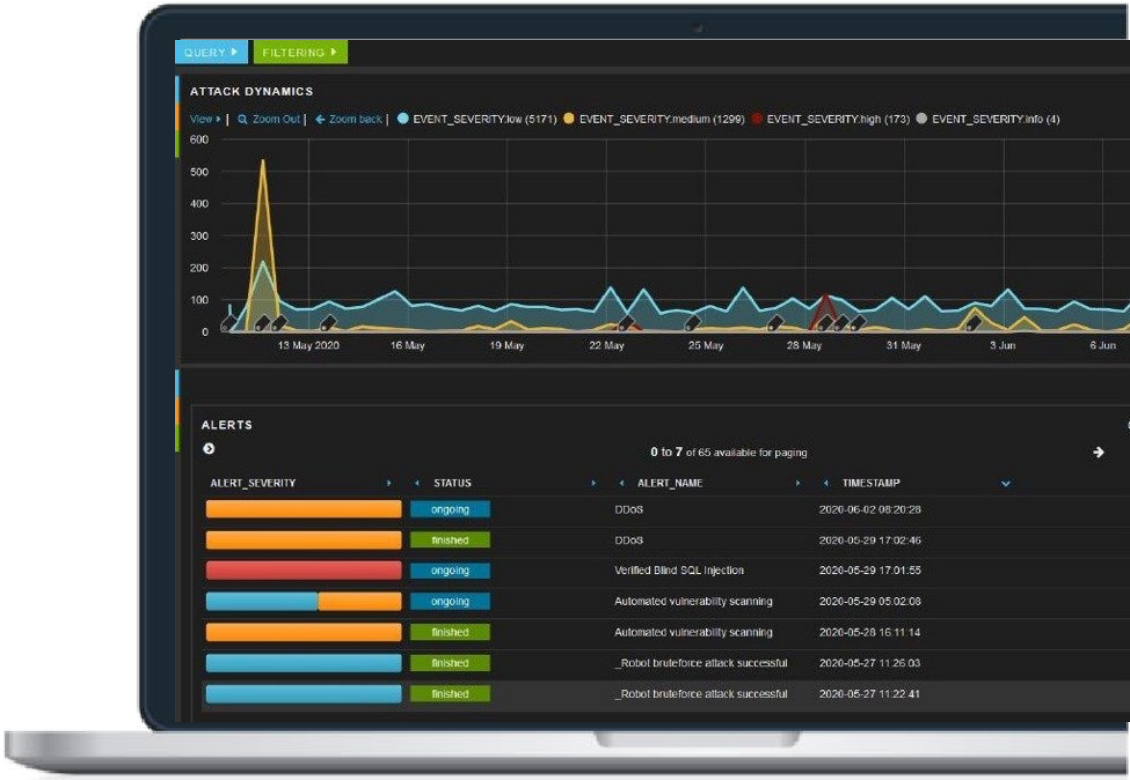
PT Application Firewall 3

- Экспертный продукт
- Сертифицирован ФСТЭК
- С широким набором интеграций
- Зарекомендовал себя на рынке



Защитные механизмы

- OWASP Top 10 Protectors
- Механизмы корреляции и пользовательских правил
- Машинное обучение
- Интеграции
- WAF.js



PT AF 4

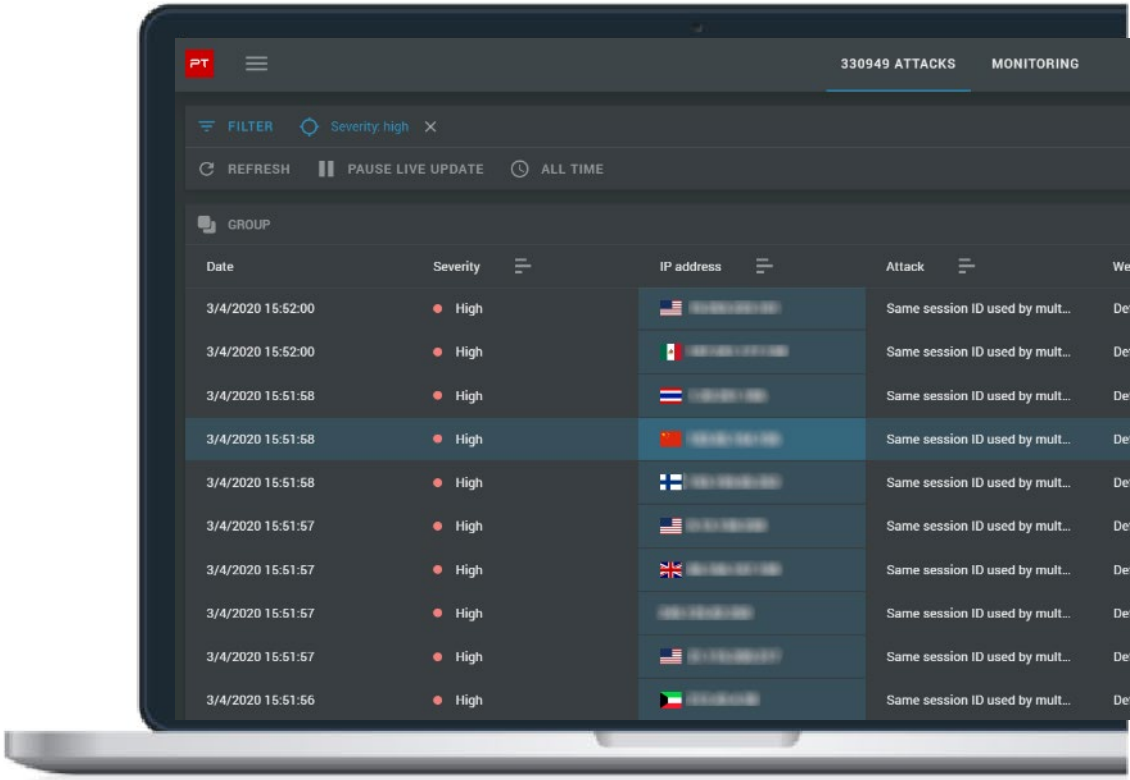
Новый инструмент защиты веб-сервисов компании

Positive Technologies

ptsecurity.com

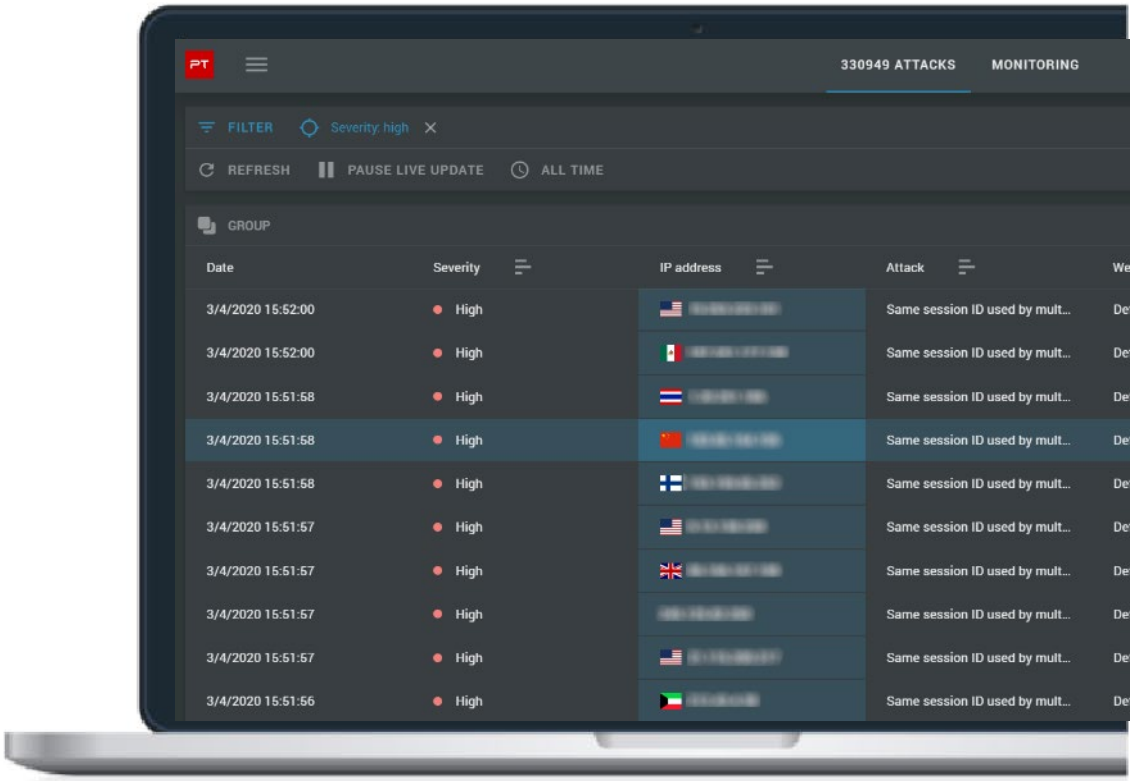
PT Application Firewall 4

- Гибкость и масштабируемость
- Мультитенантная архитектура
- Внешние агенты
- Новый продукт

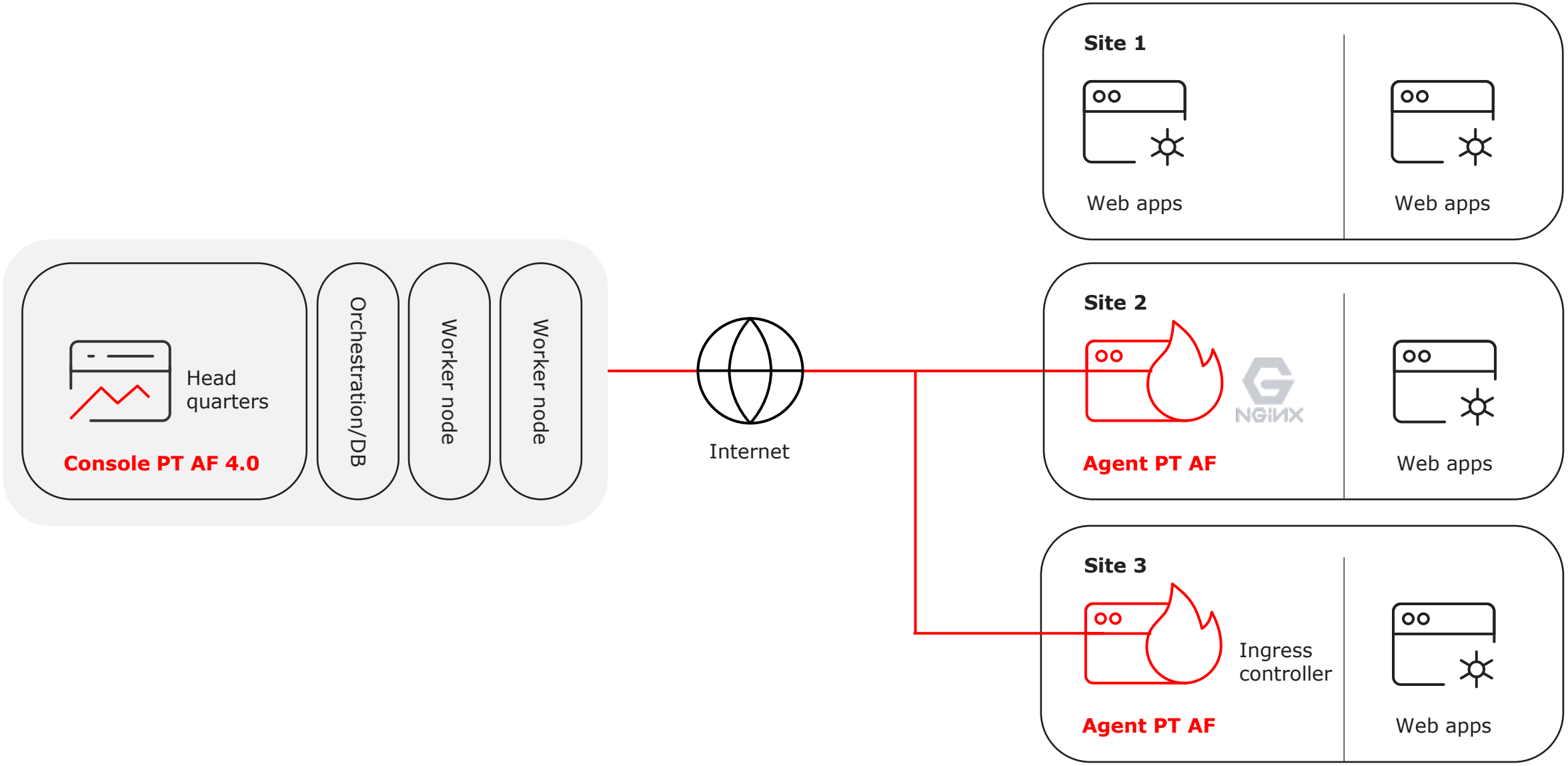


Функции PT AF 4

- Устранение угроз из списка OWASP Top 10
- Защита протоколов: Json, GraphQL, JWT, XML
- Парсер грамматик
- Предопределенные профили защиты (LAMP, ASP.NET, Apache Struts, Node.js)
- Rate limit
- Machine learning



Архитектура



Варианты развертывания

Standalone

Management

- Orchestration — kubernetes
- Databases — PostgreSQL, ClickHouse, RabbitMQ, MINIO
- Monitoring — Grafana, Prometheus

Traffic-processing

- Attack detection

Cluster

Management

- Orchestration — kubernetes
- Databases — PostgreSQL, ClickHouse, RabbitMQ, MINIO
- Monitoring — Grafana, Prometheus

Traffic-processing

- Attack detection

Management

- Orchestration — kubernetes
- Databases — PostgreSQL, ClickHouse, RabbitMQ, MINIO
- Monitoring — Grafana

Traffic-processing

- Attack detection

Management

- Orchestration — kubernetes
- Databases — PostgreSQL, ClickHouse, RabbitMQ, MINIO

Traffic-processing

- Attack detection

Traffic-processing

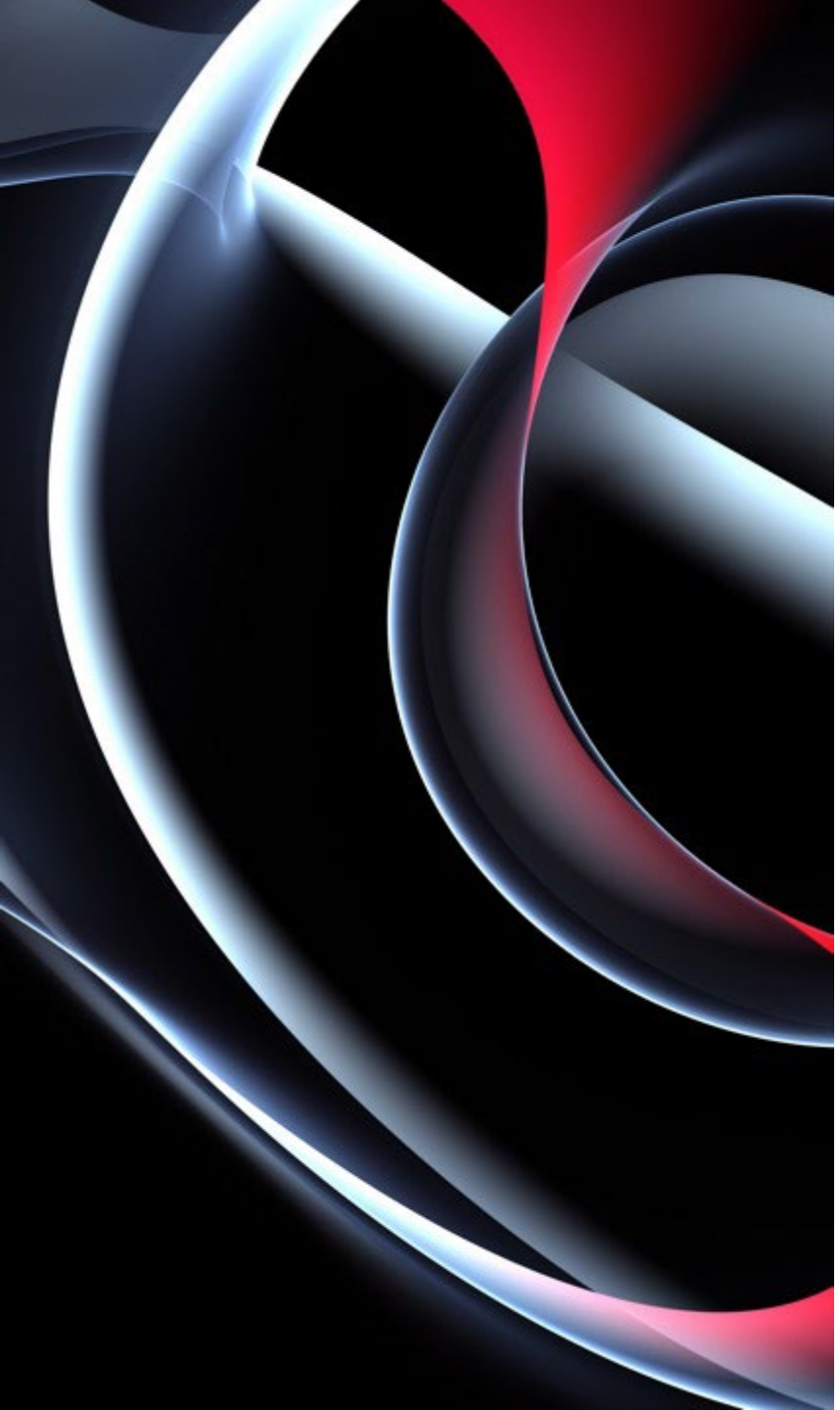
- Attack detection

Agent

NGINX

PT AF 4 vs. PT AF 3

	3.x	4.x
Сценарии развертывания	• Sniffer • Transparent Proxy • Reverse Proxy • Forensic	• Reverse Proxy • Agents
Кластеризация	2–4 узла (ограничена)	3–5–7–… узлов (не ограничена)
Лицензирование	Запросов в секунду (RPS)	Пропускная способность (Мбит/с). **Агенты: без ограничений**
Защитные механизмы	Корреляции Пользовательские правила WAF.js Валидация XML	Rate limit reCAPTCHA JWT, GraphQL, XML 30+ новых протекторов Парсер грамматик
Автоматизация и мониторинг	Частичное покрытие в API	Полное покрытие в REST API Grafana
Интеграции	SIEM (Syslog) SAST (виртуальные патчи, RVP) AV DLP (ICAP) NGFW	SIEM (Syslog)
Сертификация	Сертификат ФСТЭК Реестр российского ПО	—



Как попробовать

Заявка: заполните на странице PT AF на сайте или свяжитесь с персональным менеджером Positive Technologies или компании — партнера PT

Подготовка пилотного проекта: подписание NDA, демонстрация PT AF и оценка объемов пилотного проекта, определение целей, задач, формата отчета

Пилотное внедрение, мониторинг силами специалистов Positive Technologies или компании-партнера

Отчет о найденных атаках, оценка соответствия поставленных целей и задач полученным результатам

Спасибо за внимание

Positive Technologies

ptsecurity.com