NGENIX

Эшелонированная защита веб-приложений от кибератак

Веб под атакой

NGENIX

Веб-ресурсы, приложения и интерфейсы, используемые во всех сферах цифровой экономики РФ, стали одной из главных мишеней для кибератак в период геополитического кризиса.

Наиболее распространенные векторы атак:

- **DDoS на уровне сети и приложений**
- **Эксплуатация уязвимостей**
- **Зловредные боты и транзакционный фрод**
- **Атаки на цепочку поставок**

70 тыс. атак отражено в 2024 году на платформе NGENIX

≤500K RPS
интенсивность 90% всех атак

5M RPS
максимальная интенсивность

90% атак
на уровне приложений

60% атак
на бизнес-логику приложений (API, авторизация, поиск)

Киберриски для современных веб-приложений

NGENIX

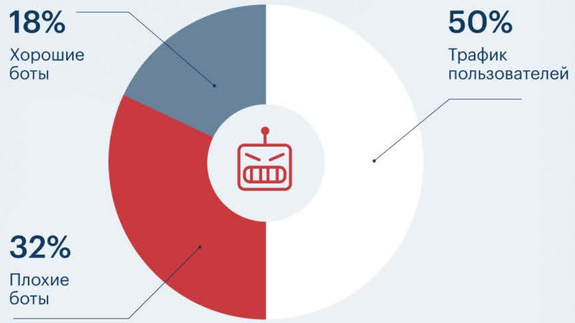
DDoS-атаки = риск потери доступности. Риск стоимостью **~20 млн в год**!*

Кого атакуют чаще всего?

Данные: ГК «Солар»

Нелегитимные боты = рост затрат, нагрузки и бизнес-рисков

Доля бот-трафика в 2024 году



Данные: Imperva

Взломы = высокие репутационные, финансовые и административные риски

В первой половине 2024 года более 50% атак привели к утечке данных:

26 ноября 2024 года Государственная дума приняла законопроекты, ужесточающие ответственность за утечки персональных данных. Для компаний ввели оборотный штраф в размере от 1% до 3% годовой выручки.

Данные: Positive Technologies

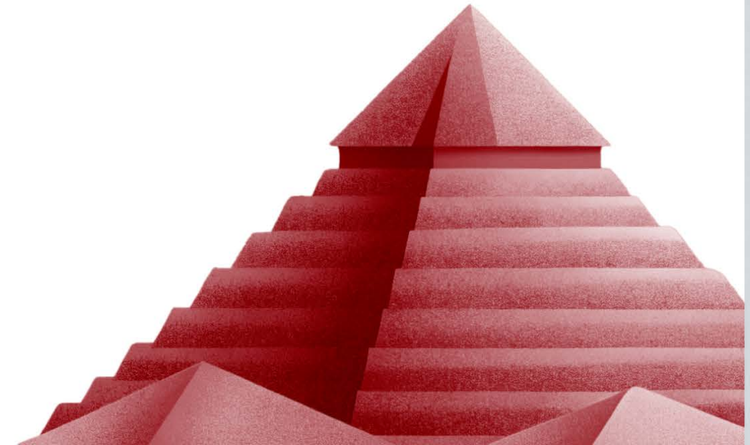
*Среднестатистическая российская компания теряет 20 млн руб в год из-за недоступности, вызванной DDoS-атаками

Управление ИБ-рисками для веб-ресурсов

NGENIX

Для веб-ресурсов традиционные подходы к ИБ-рискам неэффективны

Формальные меры снижения киберрисков могут ограничивать скорость, доступность и функционал веб-ресурсов.



Веб-ресурс — объект совместной ответственности ИТ- и ИБ-команд

Доступность и производительность веб-ресурса зависит от объединения усилий ИТ и ИБ и устранения противоречий в их подходах.

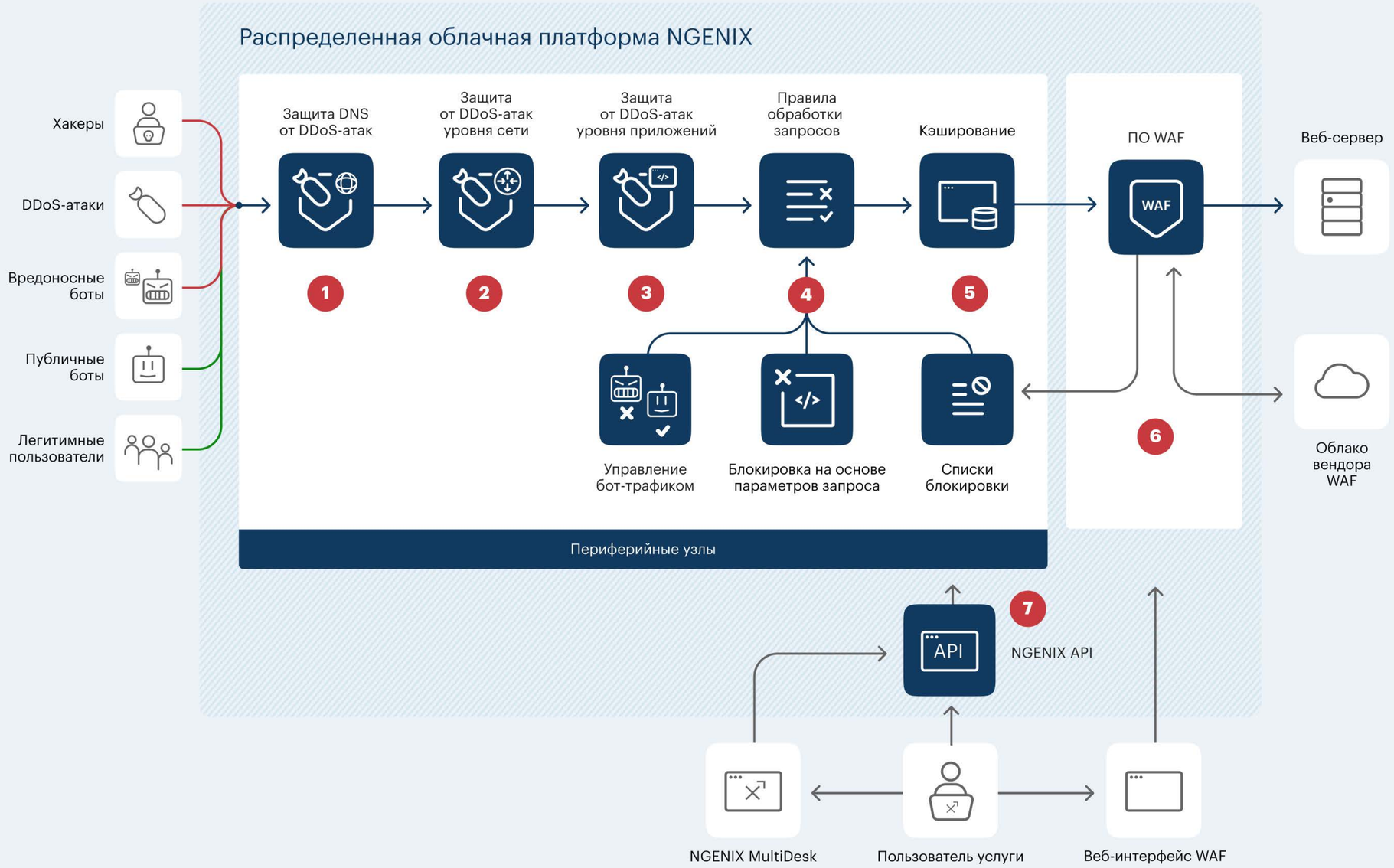
Подходы к защите веба, которые зачастую неэффективны

NGENIX

- Защита только на L3
- Централизованная очистка трафика
- Незащищенный DNS
- DIY
- Защита с помощью WAF
- Защита «без раскрытия»

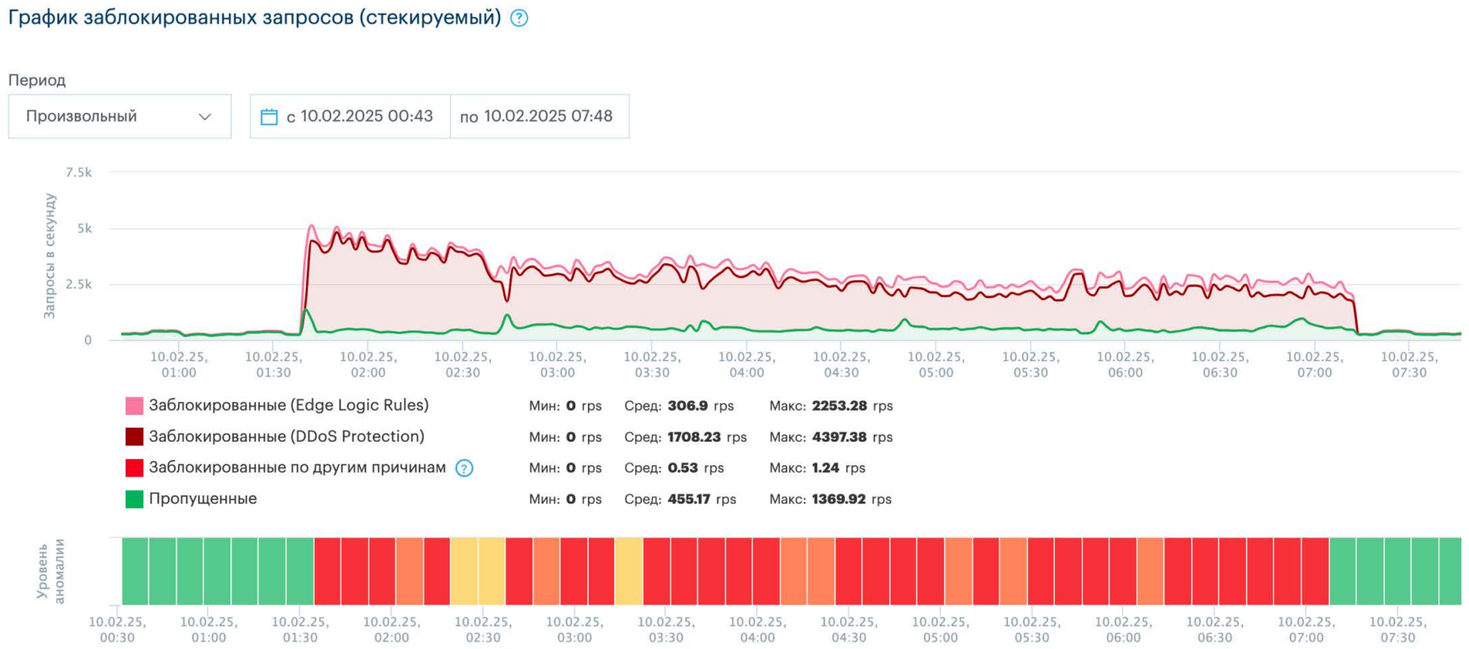
Организовать эффективную защиту от DDoS-атак поможет профессиональная команда, у которой есть опыт, компетенции и инфраструктура.

Эшелоны защиты платформы NGENIX



Кейс 1: Защита от DDoS

NGENIX



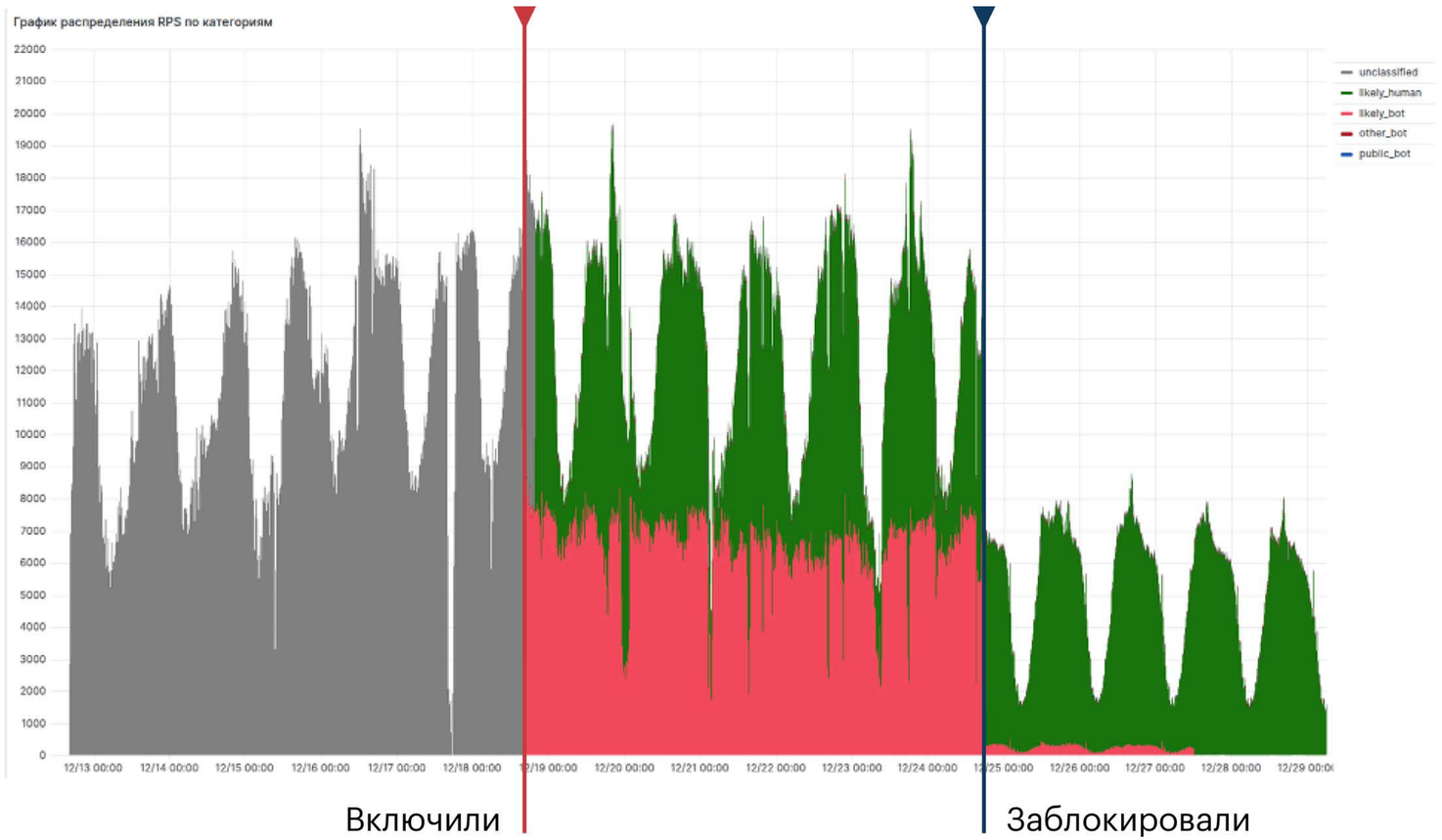
Преимущества эшелонированной защиты NGENIX:

- Защита от DDoS-атак на уровне сети и приложений
- Защищенный DNS
- Возможность настроить собственные правила блокировки
- Без перенаправления в центры очистки
- Защита от атак в обход платформы

Сервисы защиты NGENIX отражают атаки на L7 мощностью до

5M+ RPS

Кейс 2: Защита от ботов



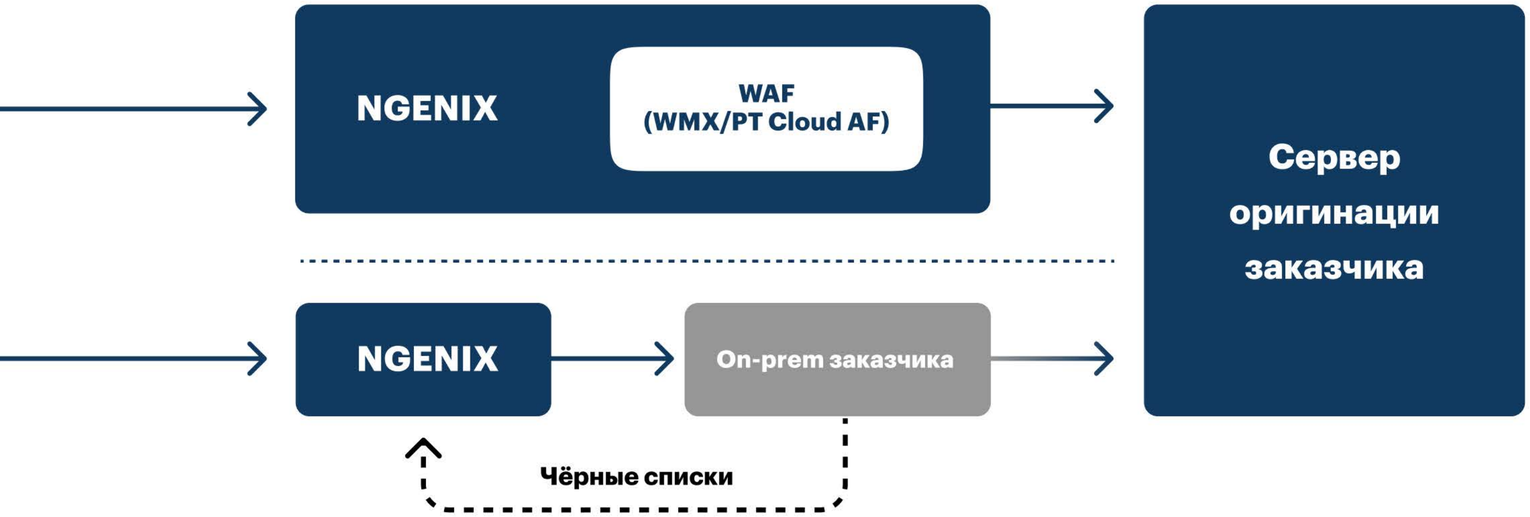
Преимущества эшелонированной защиты NGENIX:

- Применяем жесткие меры валидации только к подозрительным запросам
- Различные методы митигации для бот-атак различной сложности (снижение false positives)
- Наиболее точные данные о категориях трафика

Сокращаем объемы паразитного трафика почти **вполовину**

Кейс 3: Защита от взломов с помощью WAF

NGENIX



Преимущества эшелонированной защиты NGENIX:

- Очистка трафика до обработки запроса на WAF
- Устойчивость и стабильная работа при высоких нагрузках в десятки тысяч RPS
- Снижение эксплуатационной стоимости всей инфраструктуры WAF
- Возможность синхронизации черных списков WAF и платформы NGENIX

Сокращаем в разы нагрузку на инфраструктуру WAF

NGENIX — разработчик самой крупной распределенной облачной платформы

NGENIX

Высокая производительность под легитимной нагрузкой и при фильтрации атак

Эшелонированная защита;

Высокоточное детектирование ботов и DDoS-атак;

Масштабируемый WAF

Сервисное сопровождение командой экспертов

Прозрачность и контроль для ИБ- и ИТ- команд заказчика

Распределенная облачная платформа NGENIX

Франкфурт · Алматы · Минск · Ереван

1 000+ проектов под защитой

7 Тбит/с · **50 узлов** · **20 сервисов**

Лучшая на рынке профессиональная поддержка

NGENIX

Круглосуточная мультиканальная поддержка

24/7

Публичный статус состояния платформы и сервисов

Удобный клиентский портал и API

API

Полноценная пользовательская документация

Высокая скорость реакции на обращения

Технический аккаунт-менеджер

SLA до 99,95%

Автоматизация диагностики пользовательских подключений

Преимущества единой платформы с эшелонированной архитектурой защиты

NGENIX

Комплексное решение с единой архитектурой

- Совместимость продуктовых функций
- Единый SLA
- Единый портал упрвления услугой
- Единое окно техподдержки

Высокая масштабируемость и надежность

- Готовность к массивным атакам
- Готовность к всплескам легитимной нагрузки
- Эластичная облачная инфраструктура

Готовность к различным видам атак

- Новая атака для вашего веб-ресурса уже не новая для команды NGENIX
- 17+ лет опыта в поддержке highload-приложений

Прогнозируемый бюджет

Оплата только легитимной нагрузки

NGENIX

Делаем Рунет безопасной и предсказуемой средой для цифрового бизнеса.

Рекомендовано для импортозамещения
Программное обеспечение NGENIX внесено в Единый реестр российского ПО (№ 2023663744)

Спасибо!

Узнайте о нас больше и запланируйте бесплатный пилот

ngenix.net