Комплексное решение по защите и оптимизации работы веб-ресурсов

Строение, архитектура, возможности

6 Основных Направлений Использования

БЕЗОПАСНОСТЬ

DDoS Атаки

Атакующий трафик ухудшает доступность или производительность и приводит к непредсказуемым затратам на восстановление инфраструктуры.

Вредоносные боты

Вредоносные боты наносят вред приложениям путем копирования содержимого, кражи учетных записей, автоматического заполнения учетных данных и мошеннических действий

Утечка данных

Злоумышленники крадут данные клиента, такие как учетные данные пользователя, данные кредитной карты и другую конфиденциальную информацию

ПРОИЗВОДИТЕЛЬНОСТЬ

Медленная работа приложений и APIs

Объемные страницы и географическая удаленность ресурсов замедляют работу веб-страниц, приложений и API.

Медленная работа мобильных приложений

Мобильные клиенты вводят ограничения по производительности и доставке контента, которые ухудшают работу приложений на стороне пользователя

Недоступность приложений

Перегруженная или недоступная инфраструктура мешает пользователям воспользоваться приложением

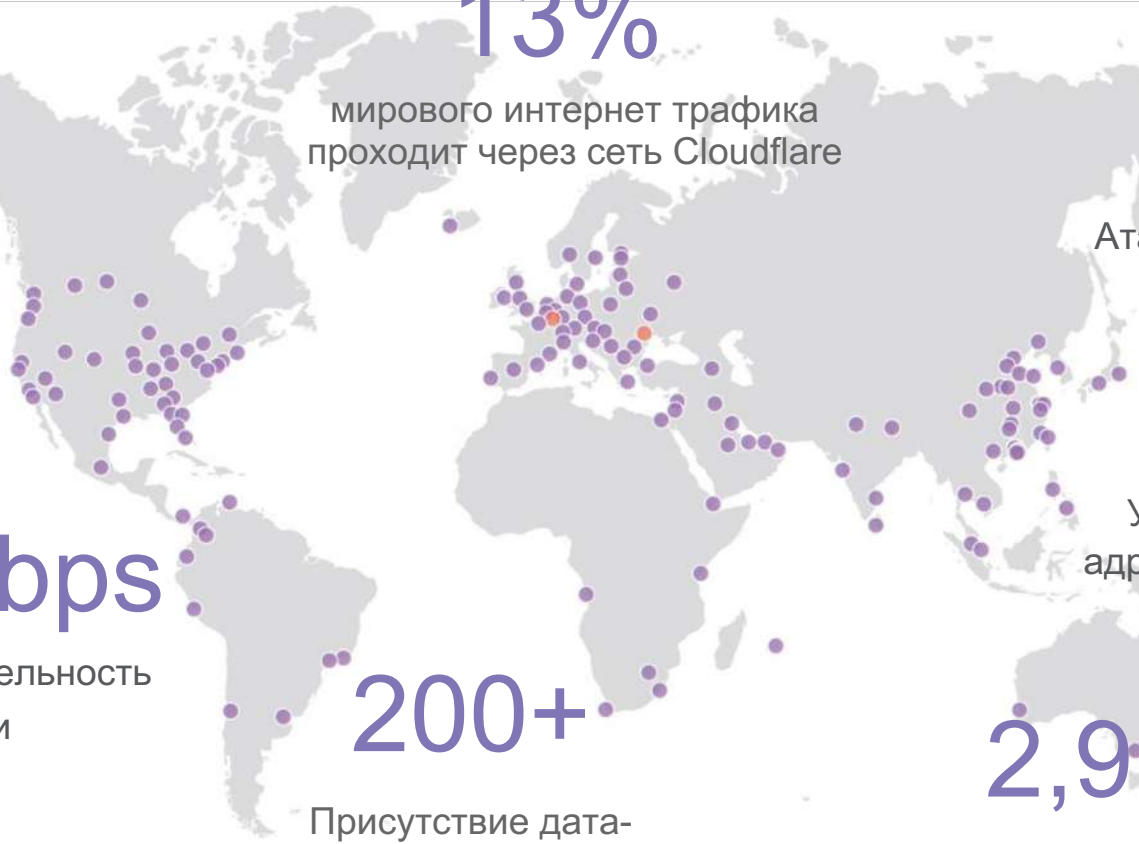
CLOUDFLARE | SOFTPROM

Одна из крупнейших глобальных anycast сетей

13%
мирового интернет трафика проходит через сеть Cloudflare

25M
Веб доменов

76B
Атак заблокировано



1B+
Уникальных IP адресов ежедневно

59 Tbps
производительность сети

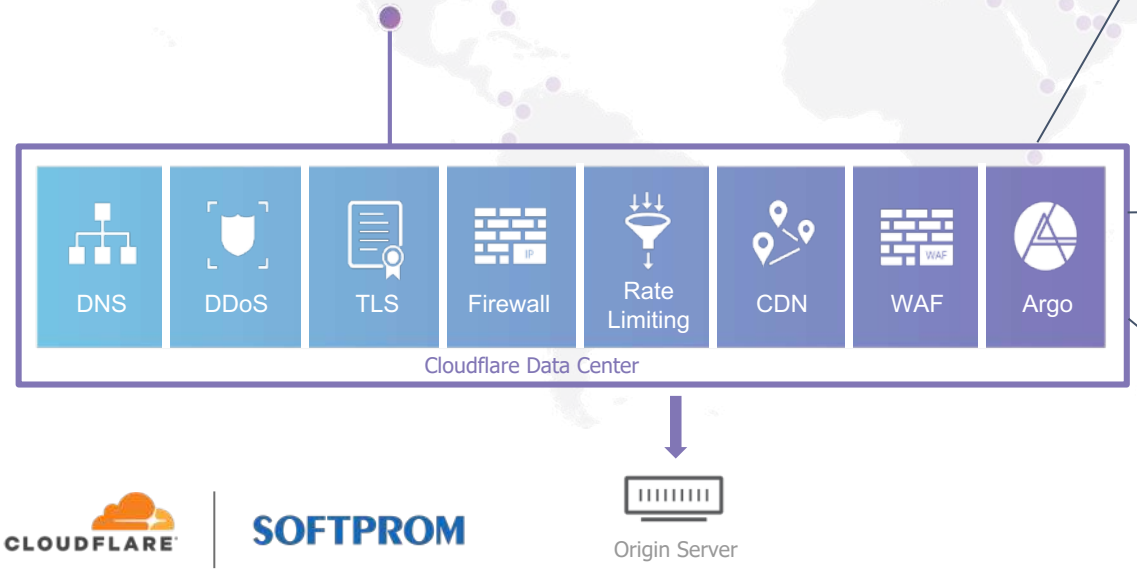
200+
Присутствие дата-центров в городах

2,9 M+
Клиентов

CLOUDFLARE | SOFTPROM

Каждый дата-центр имеет весь доступный функционал

Cloudflare это **Network Edge-as-a-service**
работающий как глобально распределённый **reverse прокси**
предоставляемый по технологии **anycast DNS**.



Масштабируемая глобальная сеть с современной, унифицированной архитектурой в каждом дата-центре

Интегрированный набор функций безопасности, производительности и надёжности

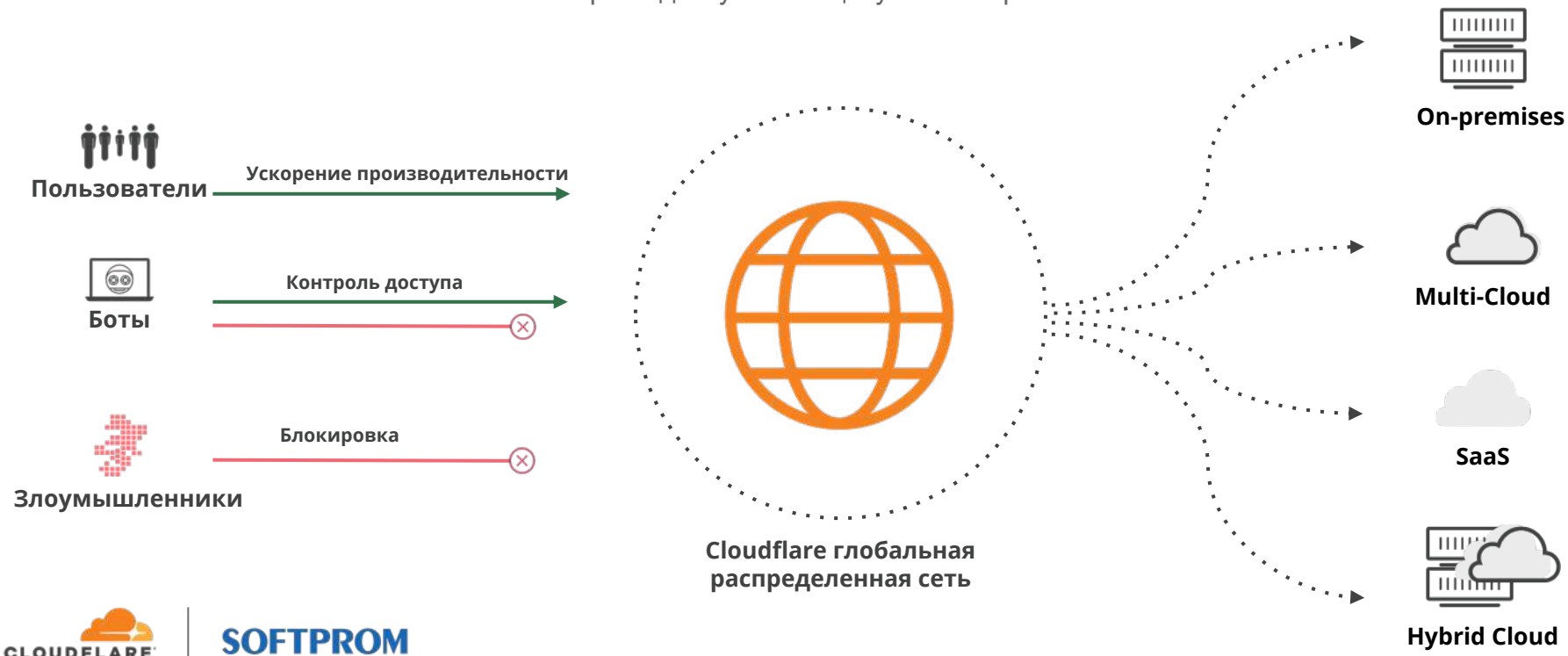
Быстрая адаптация, простая настройка

CLOUDFLARE | SOFTPROM

Как работает Cloudflare?

Cloudflare располагается между веб-трафиком клиента
и его веб-серверами, API и IoT-устройствами.

Запросы проксируются через глобальную сеть Cloudflare которая обеспечивает производительность,
контроль доступа и защиту ваших приложений



CLOUDFLARE | SOFTPROM

Решения Cloudflare применимы для любого вида деятельности

CLOUDFLARE | SOFTPROM

Enterprise клиенты Cloudflare

Avito

YOU DO

PARI MATCH

mgid

SEMRUSH

meamm

soft2bet

LogMeIn
Be Limitless.

HubSpot

ForexClub

FORRESTER®

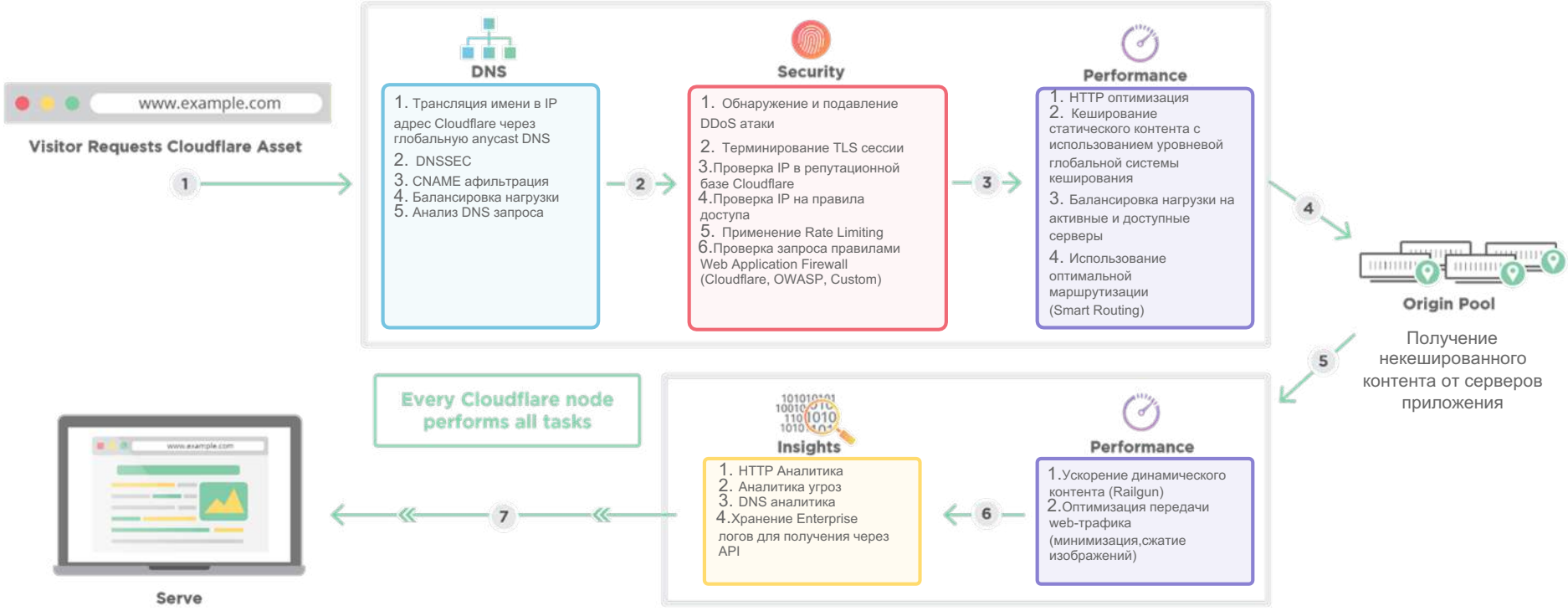
Cloudflare был признан лидером в Forrester WaveTM:
Решения по защите от DDoS, 1 квартал 2021 года

Gartner

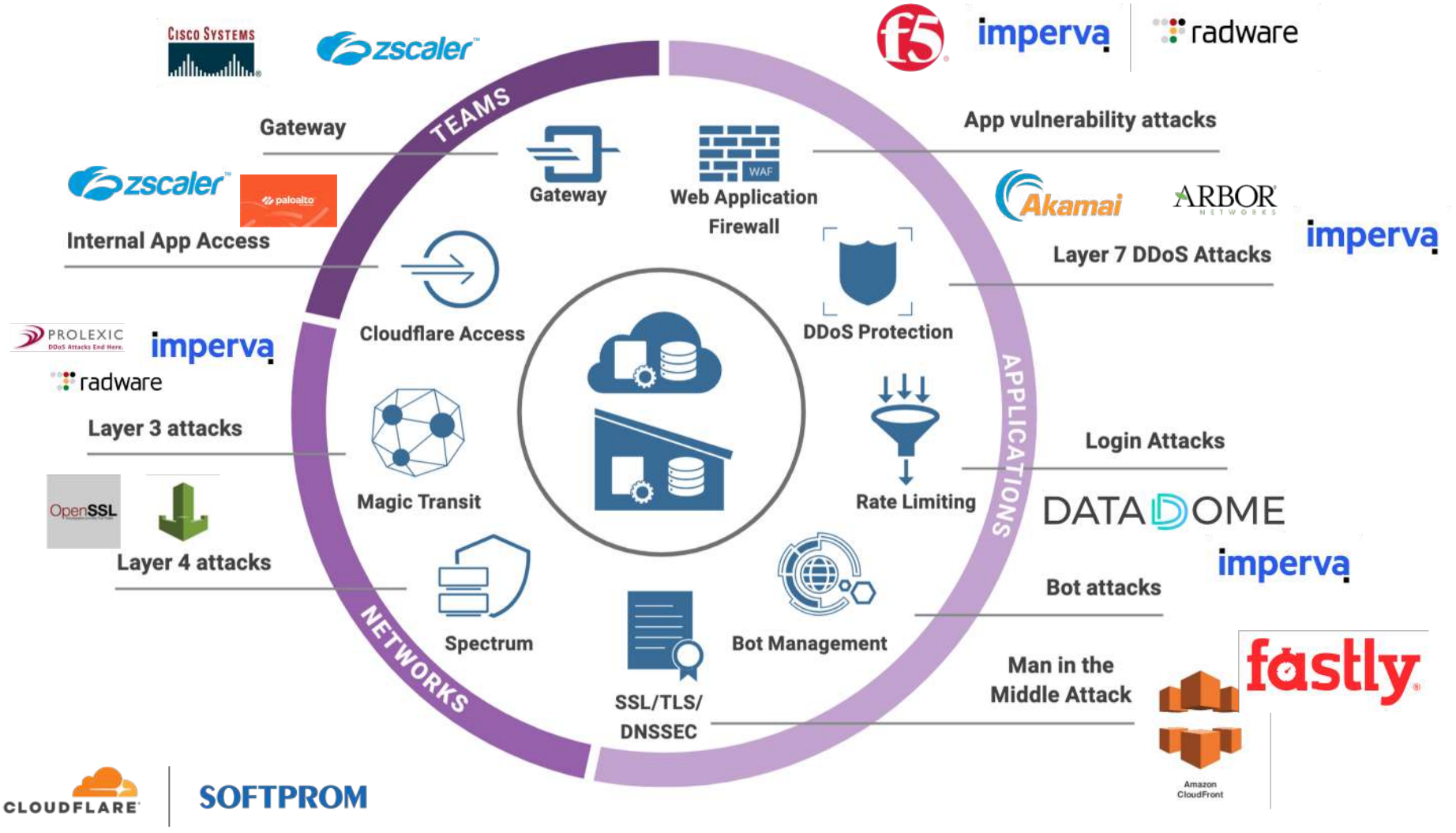
Cloudflare был назван претендентом в
Gartner Magic Quadrant для Web Application Firewalls, 2017

CLOUDFLARE | SOFTPROM

Процедура обработки запроса



CLOUDFLARE | SOFTPROM


TEAMS
APPLICATIONS
NETWORKS
Gateway
Gateway
Web Application Firewall
WAF
App vulnerability attacks
Internal App Access
Cloudflare Access
DDoS Protection
Layer 7 DDoS Attacks
Layer 3 attacks
Magic Transit
Rate Limiting
Login Attacks
Layer 4 attacks
Spectrum
Bot Management
Bot attacks
SSL/TLS/ DNSSEC
Man in the Middle Attack
Amazon CloudFront
Cisco Systems
zscaler
f5
imperva
radware
zscaler
paloalto
Akamai
ARBOR NETWORKS
imperva
PROLEXIC
DDoS Attacks End Here.
imperva
radware
OpenSSL
DATADOME
imperva
fastly
CLOUDFLARE
SOFTPROM

Сервисы Cloudflare

CLOUDFLARE FOR INFRASTRUCTURE

SECURITY

- Rate Limiting
- WAF
- IoT Security
- Bot Management
- SSL/TLS
- Magic Transit
- DDoS Protection
- Secure Origin Connection

PERFORMANCE & RELIABILITY

- Cache
- Domain Name System (DNS)
- Stream
- Intelligent Routing
- Image Optimization
- Load Balancing

CLOUDFLARE FOR TEAMS

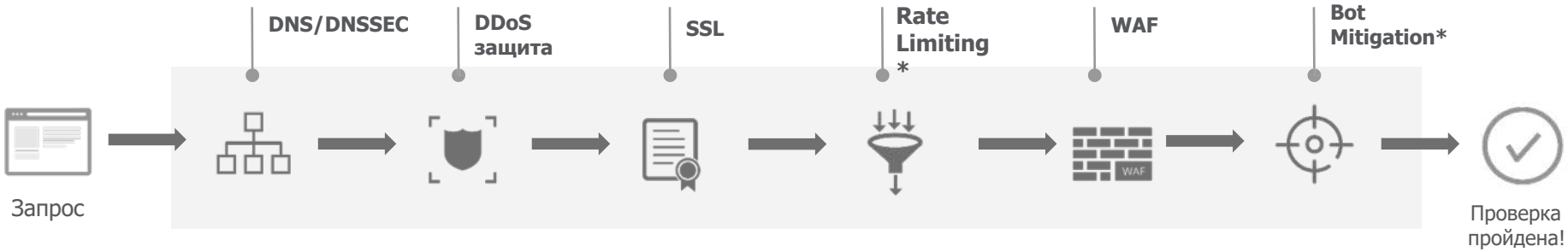
- Access
- Gateway

SERVERLESS APPLICATION PLATFORM

- Workers
- Workers KV
- Analytics
- Mobile SDK

Все функции могут быть легко активированы через панель инструментов и API.
Внесенные изменения вступят в силу на глобальном уровне в течение 30 секунд.

Сервисы безопасности Cloudflare



Orbit*
Безопасные и аутентифицированные соединения между IoT устройствами и сервером.

Spectrum*
Защита TCP приложений и портов от объемных DDoS-атак и кражи данных.

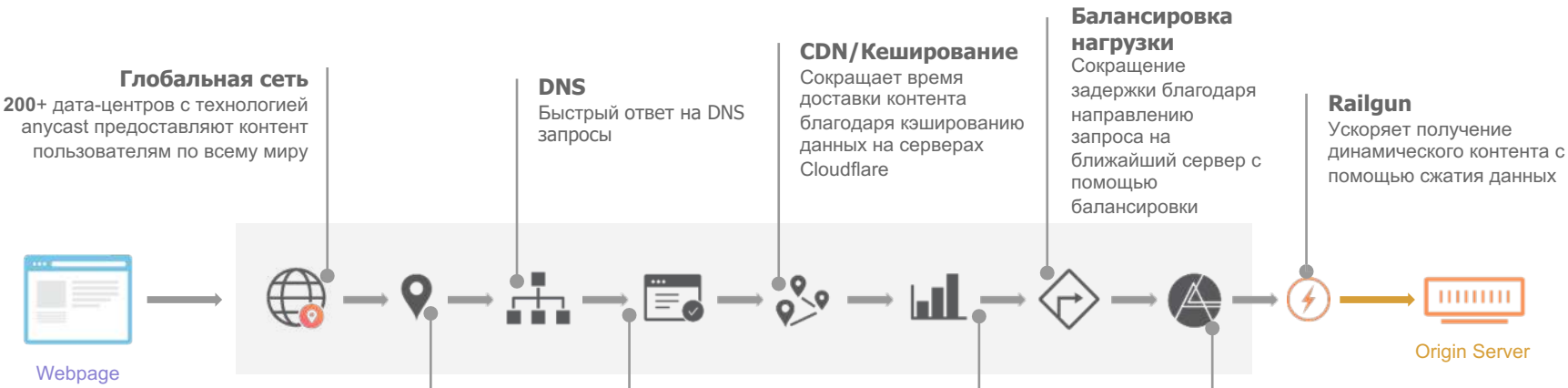
Access*
Защита, проверка подлинности и отслеживание доступа пользователей к любому домену, приложению или странице в консоли Cloudflare.

Argo Tunnel*
Создание зашифрованного туннеля между исходным сервером приложения и ближайшим центром обработки данных с ограничением доступа по другим каналам

Workers*
Запуск JavaScript Service Workers для кастомизации и настройки приложений на серверах Cloudflare.

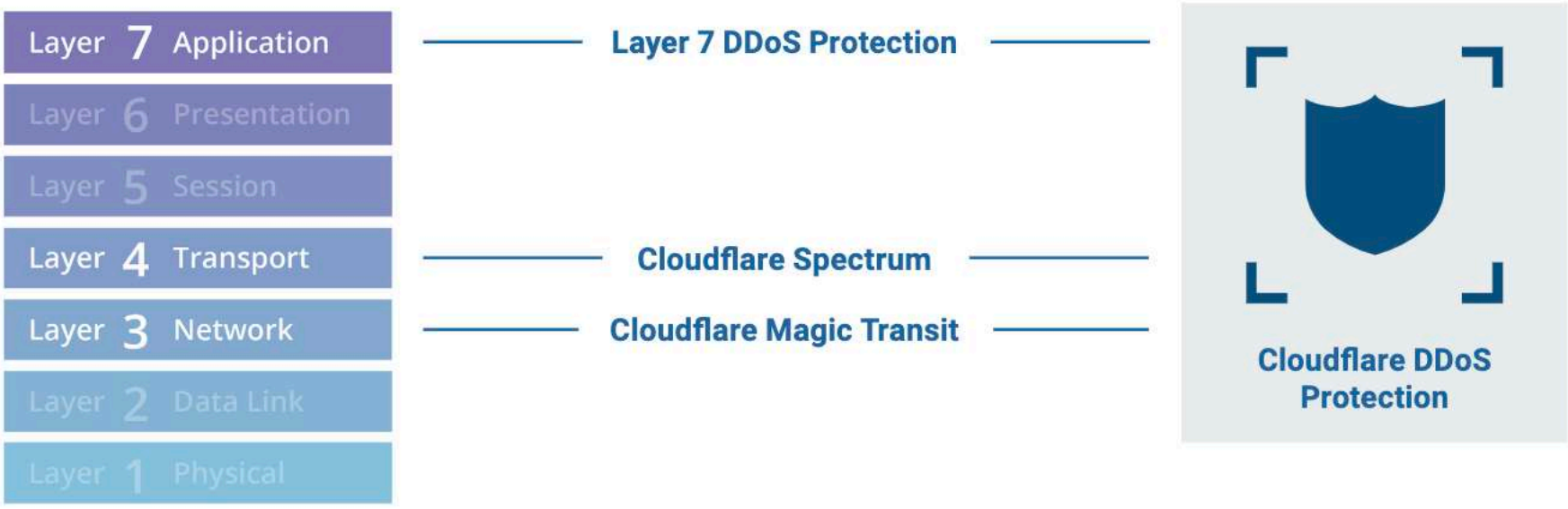
CLOUDFLARE | SOFTPROM

Сервисы производительности Cloudflare



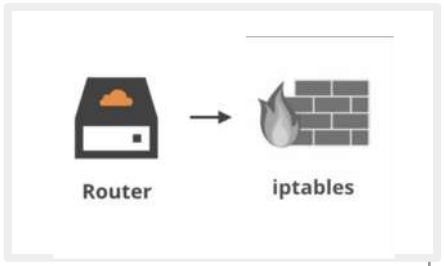
CLOUDFLARE | SOFTPROM

Cloudflare DDoS

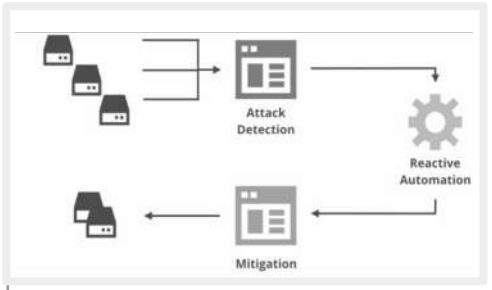


CLOUDFLARE | SOFTPROM

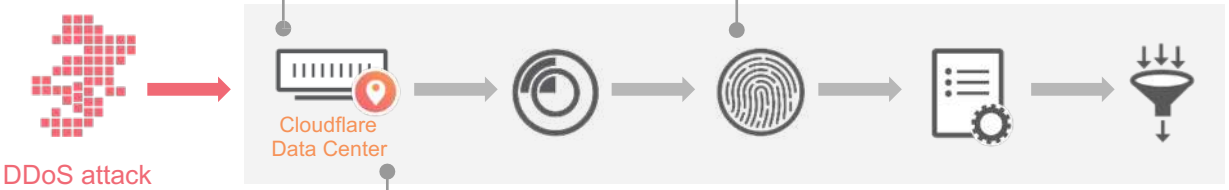
Cloudflare DDoS – Технические преимущества



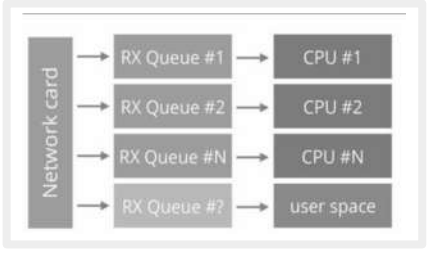
Динамически управляемые iptables
Динамически отбрасываются пакеты на сетевых интерфейсах Cloudflare. Разработанные нами высокопроизводительные фильтры позволяют нам обрабатывать значительные объемы сетевого трафика.



Автоматическое смягчение атаки
Эвристический анализ всего трафика для автоматического построения политик по обработке данным существенно уменьшает необходимость человеческого вмешательства в настройку.



Эффективность использования CPU Возможность обработки больших объемов за счет эффективного использования выделенных процессорных ресурсов позволяет обрабатывать миллионы пакетов в секунду.



CLOUDFLARE | SOFTPROM

Web Application Firewall

Cloudflare's WAF обслуживает 27 млн. веб-ресурсов, и ежедневно обнаруживает более 850 миллионов угроз.

WAF производит проверку запросов в три этапа. Изменение настроек распространяется по всем дата-центрам в течение 30 секунд

Информация, полученная при обслуживании этого трафика, поступает в набор правил Cloudflare-specific rule sets, которые в свою очередь блокируют более 65% этих угроз.

1. **Набор правил OWASP ModSecurity**:

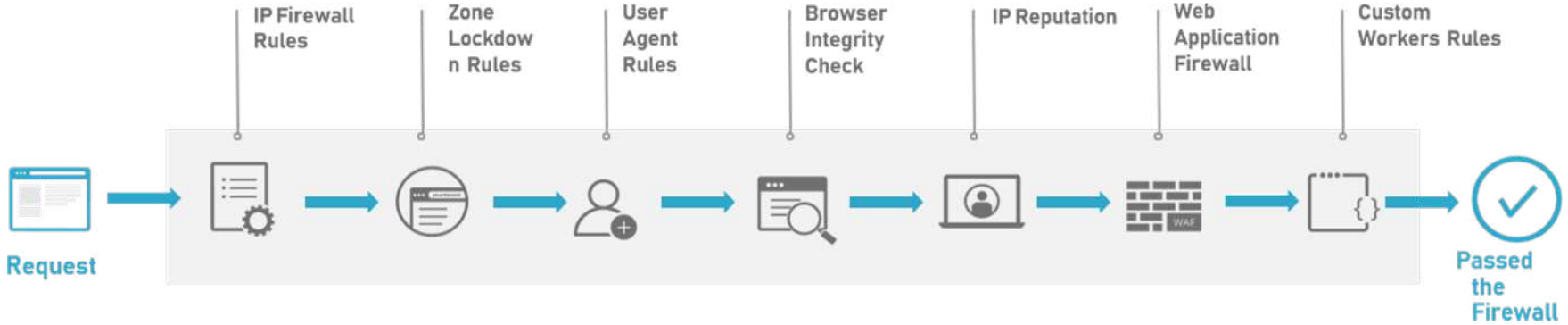
   Защита наиболее распространенных уязвимостей с использованием настраиваемых пороговых значений

2. **Набор правил Cloudflare Managed Ruleset:**

   Защита от zero-day атак и неизвестных атак увеличивает безопасность вашего приложения.

3. **Настраиваемые правила**:

   Вы можете использовать собственные фильтры Firewall для лучшего соответствия вашему приложению.



CLOUDFLARE | SOFTPROM

Защита приложения на уровне L7

Web Application Firewall (WAF)

Наш WAF включает проверку с помощью 3-х наборов сигнатур, занимающую менее 1 мс. Изменения в наборах распространяются глобально в пределах 30 сек.

1. **OWASP ModSecurity**: Наиболее распространенные уязвимости с возможностью настройки чувствительности срабатывания.
2. **Cloudflare Managed Ruleset**: Специальные наборы правил, позволяющие защититься от zero-day атак и произвести виртуальный патчинг.
3. **Custom Rules**: Возможность создавать собственные индивидуальные сигнатуры и правила для вашего приложения.

Реакция защиты:

- **Block**: Блокировка вредоносного запроса до того, как он достигнет вашего сервера.
- **Challenge:** защита с помощью CAPTCHA для предотвращения автоматических атак
- **Simulate**: Режим, который просто регистрирует событие без каких-либо дополнительных действий. Этот режим подходит для детальной настройки и обнаружения любых ложных срабатываний перед внедрением.

CLOUDFLARE | SOFTPROM

Доступ к ресурсам в Китае

Общая панель управления

Доступ к управлению параметрами трафика ресурсов, расположенных в *Китае*

CLOUDFLARE | SOFTPROM

Cloudflare Workers

- Запуск JavaScript скриптов на серверах Cloudflare в более чем 200+ дата-центрах по всему миру.
- Поскольку Cloudflare Workers запускается в дата-центре Cloudflare, а не в пользовательском браузере, появляется возможность использовать сложные механизмы и работать с любым браузером или API клиентом .

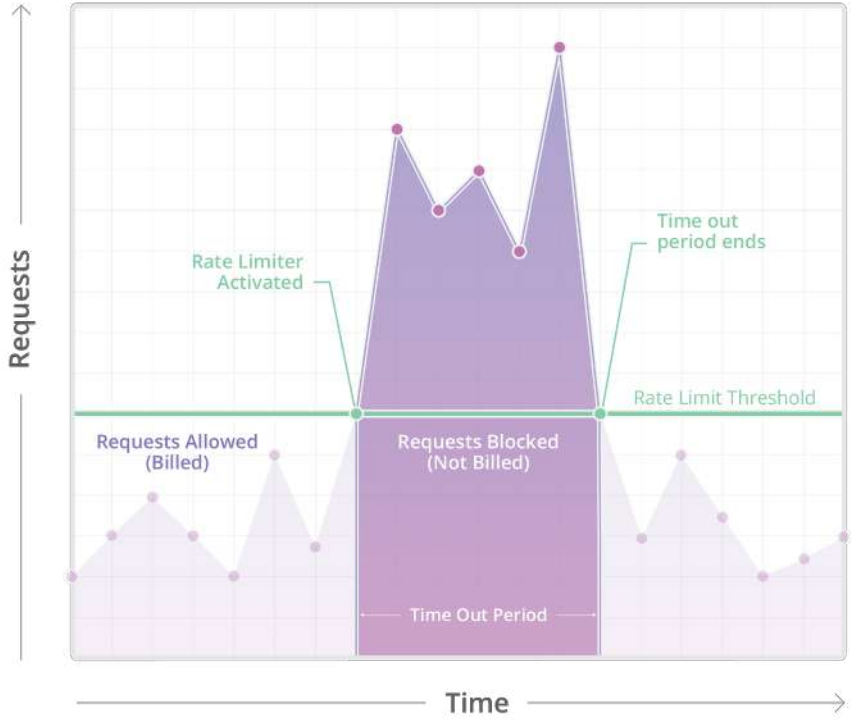
Используя сервис Cloudflare Worker, пользователи могут:

- ✓ Быстро получать ответ в то время как исходный сервер не доступен
- ✓ Применять индивидуальные механизмы авторизации и аутентификации
- ✓ Производить быстрые исправления на сайте без необходимости обновления исходного сервера
- ✓ Использовать индивидуальные алгоритмы для определения кеширования
- ✓ Использовать HTML шаблоны для получения только динамического контента с исходного сервера
- ✓ Создавать собственные правила безопасности и фильтры, чтобы блокировать нежелательных посетителей и ботов
- ✓ Генерировать параллельные запросы к разным сервисам и объединять ответы
- ✓ Проверять достоверность запросов перед направлением их на исходный сервер.

CLOUDFLARE | SOFTPROM

Cloudflare Rate Limiting

Ограничение количества запросов с одного IP адреса



Аккуратная DDoS защита

- Точная DDoS защита с широкими возможностями по конфигурации

Защита клиентских данных

- Защита чувствительных данных от брут-форс атак

Обеспечение доступности

- Предотвращение отказа в работе сервиса путем ограничения количества HTTP запросов

Контроль расходов

- Предотвращение непредвиденных расходов, вызванных скачками трафика или атаками путем установки пороговых значений, допускающих только легитимный трафик.

Больше информации

https://www.cloudflare.com/rate-limiting/

CLOUDFLARE | SOFTPROM

On-Demand сервис vs. Cloudflare Always On

Использование скраббинг-центров

- Длительное время переключения (до 300 сек.)
- Асимметричная маршрутизация
- Большие задержки
- Обычно требует ручной настройки и регулярного тестирования

Always-On

- Нулевое время включения
- Симметричная маршрутизация
- Нет дополнительной задержки
- Немедленное, автоматическое подавление, без необходимости «переключения»

CLOUDFLARE | SOFTPROM

Дополнительные Возможности Cloudflare

- Load Balancing – Глобальная и локальная балансировка запросов.
- Stream – Универсальное решение для видео-контента.
- Argo - Smart Routing многоуровневое кеширование.
- Bot Management – Управление доступом для ботов с возможностью обучения.
- Argo Tunnel - Защита исходного сервера с помощью построения туннеля.
- DNS Firewall - Улучшенный Firewall для вашей DNS-инфраструктуры.
- SSL for SaaS - Защита, шифрование и ускорение пользовательских SaaS ресурсов.
- Orbit – Защита и ускорение IoT-устройств.
- Secure Registrar – Безопасная регистрация доменов.
- Magic Transit – Защита целых IP-подсетей от DDoS-атак, а также ускорение сетевого трафика. Он использует глобальную сеть Cloudflare для смягчения атак, с помощью протокола BGP для анонсирования ваших IP-адресов и GRE для передачи очищенного трафика к серверам активы, будь то локальные, частные или общедоступные облачные среды
- Cloudflare for Teams – обеспечение быстрого, безопасного и беспрепятственного доступа в Internet и к приложениям с любого устройства в любом месте. Аутентифицированный доступ к ресурсам без VPN.