CLOUDFLARE

КРАТКИЙ ОБЗОР ПРОДУКТА

WAF Cloudflare

WAF для современной защиты приложений

Проблемы безопасности приложений

Приложения как никогда важны для бизнеса, поэтому они постоянно становятся мишенью злоумышленников, что приводит к расширению поверхности атаки.

Проблемы варьируются от необходимости сохранения защиты от появляющихся эксплойтов zero-day до обнаружения попыток уклонения, необходимости снижения риска подстановки учетных данных, которая приводит к захвату учетной записи, до обнаружения утечек данных и даже сканирования загрузки вредоносных программ в приложения.

К этим опасениям добавляется необходимость сделать защиту приложений частью более широкой унифицированной системы средств информационной безопасности, которая также охватывает защиту API, противодействие ботам и снижение рисков на стороне клиента. И все это должно осуществляться без излишней нагрузки на команды и без создания дополнительных сложностей в управлении.

WAF Cloudflare

Межсетевой экран веб-приложения (WAF) от Cloudflare — ключевой элемент нашего портфолио передовых сервисов безопасности приложений, которые обеспечивают безопасность и работоспособность приложений. Только экран WAF от Cloudflare предоставляет полные возможности мониторинга безопасности, обеспечивает многоуровневую защиту от атак OWASP и новых эксплойтов, обнаруживает уклонения и новые атаки с помощью машинного обучения, блокирует захват учетных записей, обнаруживает утечки данных и выполняет многие другие задачи, защищая приложения независимо от места их размещения. Предоставляемые нами мощные возможности обеспечения безопасности приложений, такие как безопасность API и нейтрализация ботов, полностью интегрированы с нашим межсетевым экраном WAF, используют один и тот же мощный движок правил и предоставляются через одну из первых в мире connectivity cloud.

Мониторинг атак и простое подключение

Мы предлагаем дифференцированную аналитику безопасности для визуализации всего трафика, как с нейтрализованными, так и не нейтрализованными угрозами. Немедленный мониторинг ландшафта угроз обеспечивает ощутимую отдачу от инвестиций, позволяя командам понимать трафик атак и средства защиты, которые они должны создать непосредственно после подключения.

Быстрая защита от новых атак

На основе десятков тысяч уязвимостей в год наш WAF быстро добавляет новые управляемые правила для блокировки эксплойтов недавно обнаруженных уязвимостей (уязвимостей нулевого дня). Наши управляемые правила блокируют эксплойты и дополнены WAF attack scores, полученными с помощью машинного обучения, для обнаружения обходов защиты.

Сбор и анализ информации об угрозах при поддержке обширной глобальной сети

Эффективность безопасности начинается с наличия лучших данных, и наша обширная глобальная сеть обрабатывает 20% трафика Интернета, что дает нам беспрецедентное представление о ландшафте угроз. Эти данные позволяют использовать модели машинного обучения, которые наряду с традиционными обнаружениями на основе сигнатур позволяют с высокой точностью находить и нейтрализовывать попытки атак.

Проблемы безопасности приложений

Cloudflare защищает более эффективно.

Мы обеспечиваем более эффективную безопасность WAF с помощью многоуровневых средств защиты:

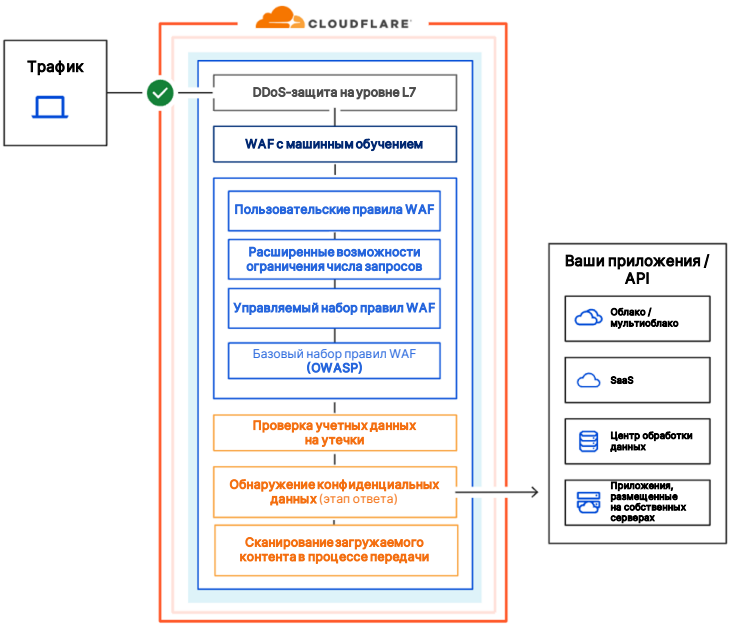
- Аналитика безопасности
- Несколько управляемых наборов правил
- Пользовательские правила
- Обнаружения на основе машинного обучения
- Обнаружение конфиденциальных данных
- Проверка украденных учетных данных
- Расширенные возможности ограничения числа запросов
- Сканирование загружаемых файлов на наличие вредоносного ПО

Cloudflare реагирует быстрее.

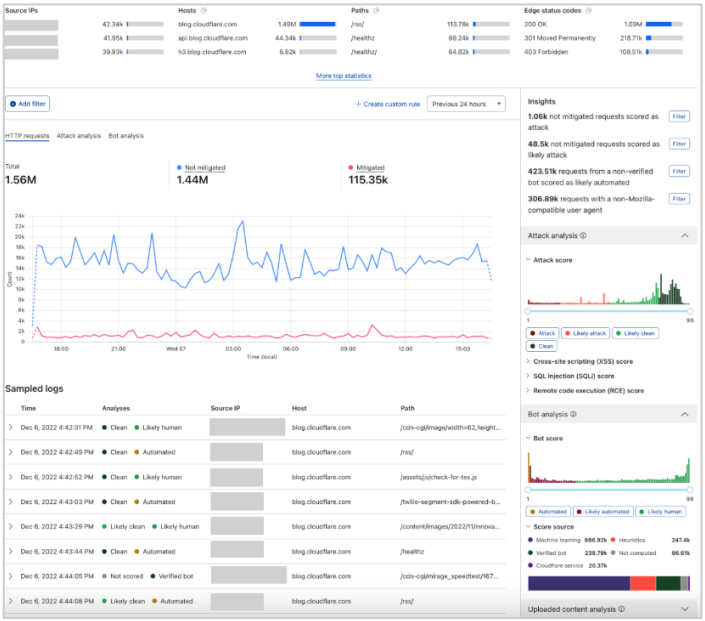
Мы быстрее защищаем от эксплойтов. Для серьезных уязвимостей, таких как быстрый сброс HTTP/2, Log4j и многих других, мы ввели несколько управляемых правил на один рабочий день быстрее, чем другие поставщики WAF.

Cloudflare полностью интегрирует защиту приложений.

Наш WAF полностью интегрирован с остальными компонентами нашего портфеля безопасности приложений, включая API Gateway и Управление ботами, и все это реализуется за один проход из облака connectivity cloud Cloudflare.



Аналитика безопасности WAF



WAF для корпоративной безопасности

Интеграция с SIEM, готовность для SOC

С помощью Cloudflare API и интеграции с необработанными логами подключить систему к вашей SIEM или обеспечить работу вашего центра безопасности (SOC) с использованием разведданных, предоставляемых Cloudflare, будет легко.

DevSecOps становится проще

Благодаря готовой интеграции с Terraform включение в DevOps безопасности приложений становится привычным делом.

При поддержке Cloudforce One

Система безопасности приложений Cloudflare получает информацию об угрозах от Cloudforce One, нашей команды по борьбе с угрозами, и блокирует их с помощью новых обнаружений на основе появляющейся информации и тактики, методов и процедур (TTP).

Безопасность веб-приложений	
Многоуровневые средства защиты на основе различных наборов правил WAF	Блокировка вредоносного кода в любом элементе запроса с помощью различных наборов правил: 1. Управляемые правила Cloudflare 2. Базовые наборы правил OWASP 3. Пользовательские правила для блокировки любых атак Новые управляемые правила тестируются на большом объеме трафика, чтобы свести к минимуму количество ложных срабатываний.
Обновляемые правила для защиты от уязвимостей нулевого дня	Правила постоянно обновляются специалистами по безопасности Cloudflare, обеспечивая защиту от новых атак и эксплойтов уязвимостей нулевого дня еще до появления исправлений или обновлений.
Обнаружения на основе машинного обучения	Останавливайте попытки обхода правил с помощью моделей машинного обучения, дополняющих многоуровневые наборы правил. Для них доступны четыре оценки атак: общая WAF attack score, оценка XSS-атак, оценка SQLi-атак и оценка RCE-атак.
Специальные наборы правил для основных платформ CMS и электронной коммерции	Получите готовую защиту для таких платформ как WordPress, Joomla, Plone, Drupal, Magento, IIS и другие, без дополнительной оплаты.
Настройка пользовательских правил	Создайте положительную или отрицательную модель безопасности, используя следующие действия при применении правил или наборов правил: БЛОКИРОВАТЬ, УПРАВЛЯЕМАЯ ПРОВЕРКА, JS-ПРОВЕРКА, ПРОПУСТИТЬ, ЖУРНАЛИРОВАТЬ, УСТАРЕВШАЯ САРТСНА, ПОЛЬЗОВАТЕЛЬСКИЕ ОТВЕТЫ.
Расширенные возможности ограничения числа запросов	Останавливайте вредоносные действия, DDoS-атаки и попытки подбора пароля, нацеленные на приложения и API, ограничивая число запросов для отдельных IP-адресов, либо по атрибутам заголовка (например, ключ, cookie, токен), номеру автономной системы (ASN) или стране.
Обнаружение конфиденциальных данных	Обнаруживайте ответы сервера, содержащие конфиденциальные данные, такие как персональные данные, финансовая информация, номера кредитных карт или секретные данные, например ключи API.
Проверка учетных данных на утечки	Обнаруживайте атаки с подстановкой украденных учетных данных, чтобы предотвратить захват учетных записей конечных пользователей.
Сканирование загружаемого контента	WAF Content Scanning проверяет загруженные файлы на наличие вредоносного ПО, а также позволяет комбинировать его сигналы с другими параметрами запроса при создании пользовательских правил.
SSL/TLS	Полностью разгружайте и настраивайте SSL-трафик вашего приложения.
Меньше ложных срабатываний	Новые правила тестируются на большом объеме трафика, чтобы свести к минимуму количество ложных срабатываний.
Поддержка gRPC и Websocket	Проксируйте и защищайте трафик для конечных точек gRPC и Websocket.
Настраиваемые страницы блокировки	Настраивайте страницы блокировки с соответствующей информацией для посетителей.
Полная интеграция с портфелем сервисов Cloudflare	Повышение производительности приложений, геомаршрутизация трафика и использование периферийных вычислений.

Возможности мониторинга, отчетность и программируемость	
Аналитика безопасности	Визуализация всех потенциальных атак на основе оценок, полученных с помощью машинного обучения.
Журналирование в режиме реального времени и доступ к необработанным журналам.	Получайте полную видимость для точной настройки WAF; проводите детальный анализ всех запросов к WAF.
Журналирование полезной нагрузки	Журналирование и шифрование вредоносной полезной нагрузки для анализа инцидентов.
Интеграции с SIEM	Отправка (push) или получение (pull) логов напрямую в используемую вами SIEM-систему.
Интеграция Terraform	Включайте средства безопасности безопасности приложений в рабочие процессы CI/CD.
Управление	
Единая консоль управления	Оптимизированное управление с помощью единой консоли для развертывания и администрирования глобальной безопасности и производительности приложений.
Управление на уровне учетной записи	Экономьте время на настройке WAF на уровне учетной записи с помощью единой конфигурации для всех доменов.
Высокая доступность — SLA	Гарантия 100 % доступности с финансовой компенсацией в случае нарушения SLA.
Не требуется установка оборудования, ПО или дополнительная настройка	Развертывание выполняется путем простого изменения DNS.
Сертификация PCI	Cloudflare имеет сертификатом поставщика услуг уровня 1.
Одобрение FedRAMP	Наш пакет Cloudflare для государственных учреждений, включая безопасность приложений, одобрен FedRAMP.

Хотите узнать больше? Зарегистрируйтесь на нашу серию демонстраций средств защиты приложений.