

Cloudflare Page Shield

Защитите цепочку поставок своих веб-приложений и обеспечьте защиту конечных пользователей от атак на стороне клиента.

Рост атак на стороне клиента

«Слепые зоны», создаваемые сторонними зависимостями

Чтобы максимально оптимизировать работу веб-сайтов, компании расширяют функциональность веб-сайтов с помощью таких возможностей, как чат-боты или аналитика, полученная от других (сторонних) компаний или разработчиков. Злоумышленники стремятся скомпрометировать такие сторонние зависимости, чтобы похитить личные данные, которые конечные пользователи вводят на веб-сайте, доставить вредоносное ПО, выполнить майнинг криптовалют или совершить последующие атаки.

Выявление и нейтрализация атак на цепочку поставок

Page Shield защищает конечных пользователей веб-сайтов от атак на стороне клиента, нацеленных на уязвимые зависимости JavaScript. Page Shield получает информацию непосредственно из браузера о том, какие файлы и модули JavaScript загружаются, проводит анализ для обнаружения вредоносных сценариев, дает вам возможность осуществлять мониторинг всех активных сценариев, исходящих соединений, а также предупреждает вас всякий раз, когда файл JavaScript демонстрирует вредоносное поведение.

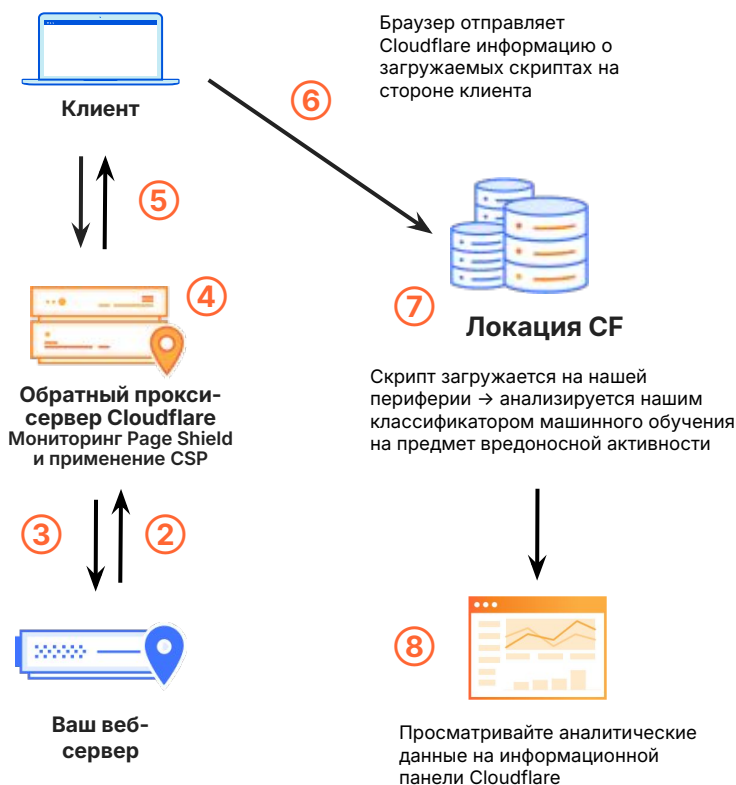


Рис. 1. Архитектура Cloudflare Page Shield



Интеллектуальное предотвращение атак

Обеспечьте полный мониторинг цепочки поставок веб-приложений и нейтрализуйте атаки на цепочку поставок, постоянно отслеживая активные сценарии, изменения в сценариях и соединения, которые они создают.



Автоматические оповещения об угрозах

Получайте мгновенные уведомления при обнаружении новых скриптов, помеченных как вредоносные или загруженных с неизвестных доменов.



Обеспечьте соответствие требованиям

Снижайте риски, связанные со сторонними поставщиками, и выполняйте нормативные требования на стороне клиента, такие как GDPR, [PCI DSS 4.0](#) и другие. Page Shield поможет вам удовлетворить эти требования без каких-либо дополнительных усилий.

Функции, которые позволяют вам взять под контроль цепочку поставок веб-приложений и защитить среды браузеров конечных пользователей

Page Shield	
Script Monitor	Отображает информацию о сторонних сценариях, загруженных на страницы вашего домена.
Connection Monitor	Отображает информацию о соединениях, выполняемых сценариями на страницах вашего домена.
Cookie Monitor (Монитор файлов cookie)	Отображает информацию о файлах cookie, обнаруженных в HTTP-трафике.
Атрибуция страниц	Позволяет узнать, на какой странице впервые появился скрипт, и просмотреть список последних случаев появления скрипта на ваших страницах.
Оповещения о новых ресурсах и о новых доменах	Сконфигурируйте и настройте уведомления о новых обнаруженных сценариях или сценариях, загруженных с неизвестных доменов.
Обнаружение вредоносных сценариев и оповещение о них	Обнаруживает вредоносные сценарии на ваших страницах с помощью сбора и анализа информации об угрозах и машинного обучения.
Обнаружение и оповещение об изменении кода	Обнаруживает любые изменения в сценариях и подключениях, загружаемых на ваши страницы. Оповещения можно настроить на более или менее частую отправку.
Обнаружение вредоносных подключений и оповещение о них	Обнаруживает, осуществляет ли сценарий подключение к вредоносному домену, например к домену управления и контроля или облачному хранилищу, указывая на эксфильтрацию данных.
Политики	Политики определяют ресурсы, разрешенные вашим приложениям, с помощью директив Content Security Policy (CSP). Политики могут журналировать нарушения и обеспечивать позитивную модель безопасности, определяя список разрешенных ресурсов и блокируя ресурсы, не включенные в политики.



Готовы увидеть Page Shield в действии? Подпишитесь на бесплатную [оценку рисков на стороне клиента](#) уже сегодня.