Cloudflare Page Shield

웹 애플리케이션 공급망을 보호하고 클라이언트 측 공격으로부터 최종 사용자를 보호합니다.

증가하는 클라이언트 측 공격

타사 종속성으로 인한 사각지대

뛰어난 웹 경험을 제공하기 위해, 기업은 챗봇이나 분석 도구와 같은 기능을 다른 회사(타사)나 개발자로부터 도입하여 웹 사이트 기능을 개선합니다. 공격자는 이러한 타사 종속성을 악용하여 최종 사용자가 사이트에 입력한 개인 데이터를 탈취하거나, 맬웨어를 유포하고, 암호화폐 채굴을 수행하거나, 후속 공격을 진행하려고 합니다.

공급망 공격 식별 및 완화

Page Shield는 취약한 JavaScript 종속성을 겨냥하는 클라이언트 측 공격으로부터 웹 사이트 최종 사용자를 보호합니다. Page Shield는 브라우저에서 직접 로드되는 JavaScript 파일 및 모듈 정보를 수집하고, 악성 스크립트를 감지하기 위한 분석을 수행하며, 모든 활성 스크립트와 아웃바운드 연결 현황을 가시화합니다. 또한 JavaScript 파일에서 악성 행위가 감지될 때마다 경고를 발령합니다.

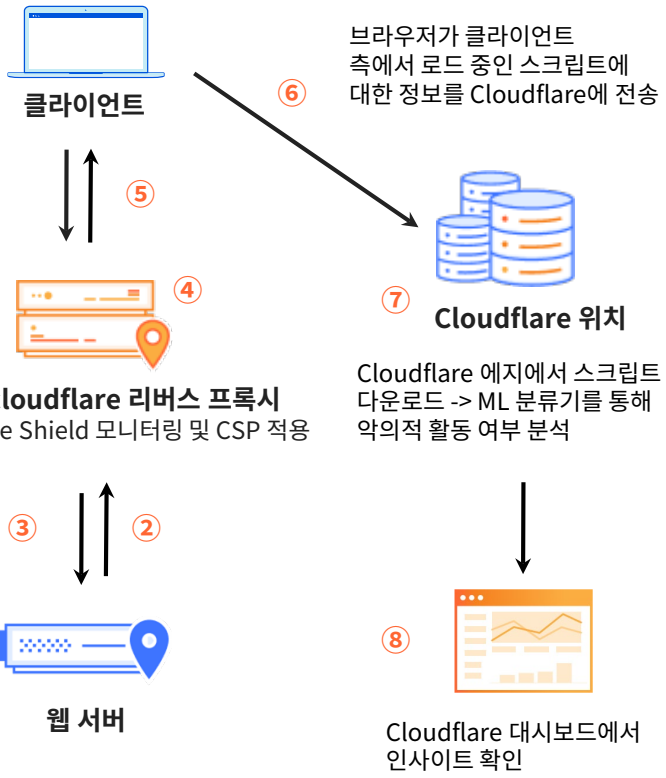

그림 1: Cloudflare Page Shield 아키텍처

지능적인 공격 방지

웹 애플리케이션 공급망에 대한 완전한 가시성을 확보하고, 활성 스크립트, 스크립트 변경 사항, 연결을 지속적으로 모니터링하여 공급망 공격을 완화하세요.

자동 위협 알림

새로운 스크립트가 감지되거나, 악의적인 것으로 표시되거나, 알 수 없는 도메인에서 로드될 때 즉시 알림을 받습니다.

규제 준수 요건 충족

타사 벤더의 위험을 줄이고 GDPR, PCI DSS 4.0과 같은 규정의 클라이언트 측 요구 사항을 해결하세요. Page Shield를 사용하면 추가적인 노력 없이도 이러한 요구 사항을 충족할 수 있습니다.

웹 애플리케이션 공급망을 제어하고 최종 사용자의 브라우저 환경을 보호할 수 있는 기능

Page Shield	
스크립트 모니터	도메인 페이지에 로드된 타사 스크립트에 대한 정보를 표시합니다.
연결 모니터	도메인 페이지 내 스크립트가 생성한 연결에 대한 정보를 표시합니다.
쿠키 모니터	HTTP 트래픽에서 감지된 쿠키에 대한 정보를 표시합니다.
페이지 귀속성	스크립트가 처음 나타난 페이지를 찾고, 해당 스크립트의 최근 발생 목록을 확인할 수 있습니다.
새 리소스 알림 및 신규 도메인 알림	새로 감지된 스크립트 또는 알 수 없는 도메인에서 로드된 스크립트에 대한 알림을 구성하고 사용자 지정할 수 있습니다.
악성 스크립트 감지 및 알림	위협 인텔리전스와 머신 러닝을 사용하여 페이지에서 악성 스크립트를 감지합니다.
코드 변경 감지 및 알림	페이지에 로드된 스크립트와 연결의 모든 변경 사항을 감지합니다. 알림 빈도를 더 자주 또는 덜 자주 받도록 설정할 수 있습니다.
악성 연결 감지 및 알림	스크립트가 데이터 유출을 나타내는 명령 및 제어 도메인 또는 클라우드 스토리지와 같은 악성 도메인에 연결되는지 감지합니다.
정책	정책은 콘텐츠 보안 정책(CSP) 지침을 통해 애플리케이션에서 허용되는 리소스를 정의합니다. 정책을 통해 위반 사항을 기록하고, 리소스 허용 목록을 정의하는 긍정적 보안 모델을 적용하며, 정책에 포함되지 않은 리소스를 차단할 수 있습니다.

Page Shield를 직접 확인할 준비가 되셨나요? 지금 바로 Cloudflare 무료 클라이언트 측 위험 평가에 등록하세요.