CLOUDFLARE

웹 애플리케이션 방화벽.

SQL 삽입, 교차 사이트 스크립팅 공격 등으로부터 웹 사이트를 보호

Cloudflare의 WAF(웹 애플리케이션 방화벽)는 애플리케이션 계층을 대상으로 한다고 OWASP에서 밝힌 취약점 및 위협을 비롯한 SQL 삽입, XSS(교차 사이트 스크립팅) 및 제로데이 공격으로부터 웹 사이트를 보호합니다. 주요 고객으로는 Alexa 상위 50개 기업, 금융기관, 전자 상거래 회사 및 대기업 등이 있습니다. 당사의 DDoS 방어와 완벽하게 통합된 WAF 는 매일 수백만 건의 공격을 차단하고, 새로운 위협이 등장할 때마다 이를 자동으로 학습합니다.

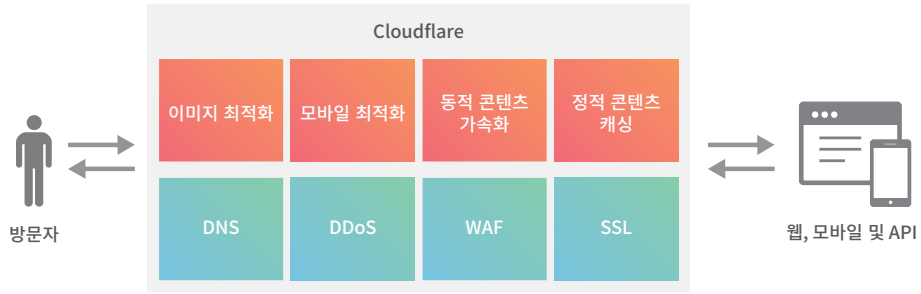
요구 사항에 맞게 사용자 지정할 수 있는 강력한 규칙 엔진

Cloudflare의 WAF는 기본 제공되는 ModSecurity 규칙 집합을 실행하여 OWASP에서 확인된 가장 중요한 웹 애플리케이션 보안 결함에 대한 보호를 제공합니다. 또한 기존 규칙 집합 및 사용자 지정 규칙을 처리할 수있습니다. 규칙을 시행하는 데는 30초도 걸리지 않습니다.

클라우드 배포와 DDoS 완화 및 CDN

클라우드 기반 서비스인 Cloudflare WAF에는 설치 및 유지 관리할 하드웨어나 소프트웨어가 필요하지 않습니다. 클릭 한 번으로 WAF를 배포하고 요구 사항에 맞게 사용자 지정하십시오.

전체 Cloudflare 서비스에 통합되어 있어 추가 기능을 무료로 사용할 수 있습니다. DDoS 공격으로부터 웹 사이트를 보호하고 글로벌 콘텐츠 전송 네트워크를 사용하여 실행 속도를 높일 수 있습니다.



주요 특징:

- DDoS 완화와 완벽하게 통합된 계층 7 보호를 제공하는 강력한 기본 규칙 집합과 광범위한 사용자 지정을 통해 다양한 위협으로부터 **자동 보호**
- **초고속 0.3ms 처리 시간** - 즉각적인 글로벌 업데이트 지원
- **PCI DSS 요구 사항 6.6 준수** - Cloudflare의 WAF를 사용하여 PCI를 비용 효율적으로 준수
- **실시간 보고** - 강력한 로깅 기능으로 현재 발생하는 사항을 즉시 확인 가능
- **클라우드 배치** - 하드웨어, 소프트웨어 또는 튜닝이 필요 없음

주요 기능	이점
보안	
애플리케이션/계층 7을 아우르는 심층 패킷 분석	SQL 삽입, 교차 사이트 스크립팅 공격 등의 수천 가지 위협으로부터 표준 및 사용자 지정 웹 애플리케이션을 항상 보호합니다.
SSL	오버헤드 또는 추가 대기 시간 없이 SSL 연결을 종료합니다. 인증서를 업로드하거나 값비싼 하드웨어 솔루션에 투자하지 않고도 SSL 암호화 트래픽에 WAF 정책을 적용합니다.
GET 및 POST HTTP/S 요청의 경우	다양한 HTTP/S 트래픽 범위 포함
URL별 사용자 지정 규칙 집합	WAF 보호에서 특정 URL 또는 하위 도메인을 포함/제외하여 도메인을 테스트하거나 특정 하위 도메인을 포함/제외할 수 있습니다.
DDoS 완화 통합	전체 스택을 DDoS로부터 보호하며, 추가 구현이 필요하지 않습니다.
IP 평판 데이터베이스 통합	10억 개 이상의 고유 IP에 대한 실시간 인텔리전스를 사용해 악의적인 트래픽을 차단하며, 추가 구현이 필요하지 않습니다.
가상 패치	서버를 패치하거나 코드를 업데이트하기 전에 취약점을 수정하여 패치 및 테스트 업데이트에 더 많은 시간을 할애할 수 있습니다.
IP 또는 위치 정보로 제한	특정 IP 주소나 국가의 트래픽을 블랙리스트/화이트리스트에 추가하여 특정 IP 또는 국가의 해커로부터 보호할 수 있습니다.
낮은 가양성(false positive)	전반적인 가양성 비율이 1/50M이므로 합법적인 트래픽이 도달되도록 보장합니다.
CDN 서비스와 완벽하게 통합되어 아웃바운드 콘텐츠 변환 제공	사이트 방문자의 웹 대기 시간이 감소하며, 추가 구현이 필요하지 않습니다.
규칙 집합	
보안 중심 연구와 결합된 자동 학습	보안 팀에서 자동으로 배포하는 패치를 통해 제로 데이 취약점이나 새로운 위협을 방어합니다.
ModSecurity 논리 및 포맷과의 호환성	기존 규칙 집합을 쉽게 가져와 기존 보호 기능을 유지 관리할 수 있습니다.
핵심 OWASP ModSecurity 규칙 집합	OWASP(Open Web Application Security Project)에서 가장 심각한 결함이라고 확인한 OWASP 취약점을 보호하며, 추가 요금 없이 기본으로 제공됩니다.
제로 데이 Cloudflare 규칙 집합	Cloudflare의 보안 팀의 협력을 통해 고객층에서 확인된 위협으로부터 고객을 보호하며, 추가 요금 없이 기본으로 제공됩니다.
주요 CMS 및 전자 상거래 플랫폼을 위한 플랫폼별 규칙 집합	WordPress, Joomla, Plone, Drupal, Magneto, IIS 등의 플랫폼을 추가 비용 없이 즉시 보호합니다.
사용자 지정 규칙	Business 및 Enterprise 고객의 경우, 기본으로 포함된 웹 애플리케이션에 고유한 상황을 추가 비용 없이 해결해 줍니다.
WAF 설정	
차단	공격을 차단하면 웹 사이트에 게시되기 전의 모든 작업이 중지됩니다.
시뮬레이션	가양성을 테스트하려면 WAF를 시뮬레이션 모드로 설정하십시오. 인증 또는 차단 없이 가능한 공격에 대한 대응을 기록합니다.
인증	인증 질문 페이지에서는 웹 사이트로 이동하려는 방문자에게 캡차(CAPTCHA) 제출을 요청합니다.
임계값/민감도 설정	민감도에 따라 트리거 빈도를 조절하는 규칙 설정
사용자 지정 가능한 차단 페이지	방문자가 차단되었을 때 볼 수 있는 페이지를 사용자 지정합니다(예: "도움을 받으려면 이 번호로 전화하십시오.") Enterprise 고객에게 제공됩니다.
보고	
실시간 로깅	WAF를 미세 조정하는 데 도움이 되는 가시성 확보
원시 로그 파일에 액세스	Enterprise 고객은 모든 WAF 요청을 포함하는 심층 분석을 수행할 수 있습니다.
관리	
SLA가 제공되는 서비스를 기반으로 하는 고가용성	Business 및 Enterprise 고객에게는 100% 가동 시간이 보장되며, 그렇지 못할 경우 위약금이 지불됩니다.
하드웨어, 소프트웨어 또는 튜닝이 필요 없음	약간의 DNS 변경으로 등록
PCI 인증	Cloudflare 서비스는 레벨 1 서비스 공급자 인증을 받았습니다.