

Cloudflare WAF

최신 애플리케이션 보안을 위한 WAF

애플리케이션 보안 과제

애플리케이션은 그 어느 때보다 비즈니스에 중요합니다. 그래서 끊임없이 공격자의 표적이 되고 있고, 이로 인해 공격면이 확장됩니다.

새로운 zero-day 익스플로잇으로부터 보호, 회피 시도 감지, 계정 탈취로 이어지는 자격 증명 스테핑의 위험 줄이기, 데이터 손실 방지, 애플리케이션에 대한 맬웨어 업로드 스캐닝까지 걱정거리는 다양합니다.

이러한 걱정거리는, API를 보호하고 봇을 차단하며 클라이언트 측 위험을 완화하는 광범위한 통합 보안 상태에 애플리케이션 보호를 포함시켜야 할 필요성과 맞물리게 됩니다. 과도한 관리 문제로 팀에 부담을 주지 않으면서 이 모든 필요성을 충족해야 합니다.



Cloudflare WAF

Cloudflare 웹 애플리케이션 방화벽(WAF)은 애플리케이션을 안전하고 생산적으로 유지하는 Cloudflare 첨단 애플리케이션 보안 포트폴리오의 초석입니다. Cloudflare WAF만이 완벽한 보안 가시성을 제공하고, OWASP 공격과 새로운 익스플로잇에 대해 계층화된 보호 기능을 제공하며, 머신 러닝을 통해 회피 공격과 새로운 공격을 감지하고, 계정 탈취를 차단하며, 데이터 손실을 감지하는 동시에 애플리케이션이 호스팅되는 모든 곳에서 애플리케이션을 보호합니다. API 보안 및 봇 완화 등 Cloudflare의 강력한 애플리케이션 보안 기능은 WAF와 완벽하게 통합되어 제공되며, 세계 최초의 클라우드 연결성 중 하나에서 제공되는 것과 동일하게 강력한 규칙 엔진이 더해집니다.



공격에 대한 가시성 확보 및 간편한 온보딩

Cloudflare에서는 완화 여부와는 무관하게 모든 트래픽을 시각화할 수 있는 차별화된 보안 분석을 제공합니다. 위협 환경에 대한 즉각적인 가시성으로 실질적인 투자 수익률을 얻을 수 있고, 온보딩 후 즉시 공격 트래픽과 보호 기능을 구축해야 하는지 팀에서 파악할 수 있습니다.



새로운 공격 신속 방어

연간 수만 건의 취약점이 발견되에도 불구하고 Cloudflare의 WAF는 새로 발견된(zero-day) 취약점 악용을 차단하는 새로운 관리형 규칙을 신속하게 추가하고 있습니다. 머신 러닝 기반 WAF Attack Score로 Cloudflare의 관리형 규칙을 보완하여 취약점을 차단하고 회피 행위를 감지합니다.



방대한 전역 네트워크에서 제공되는 위협 인텔리전스

보안 효율성은 최고의 데이터를 보유하는 것에서 시작되며, Cloudflare의 방대한 전역 네트워크에서는 인터넷의 20%를 프록시하여 위협 환경에 대한 독보적인 인사이트를 제공합니다. 이 데이터로 머신 러닝 모델을 구동하여 기존의 서명 기반 감지와 함께 높은 정확도로 공격 시도를 찾고 완화합니다.

애플리케이션 보안 과제

Cloudflare에서는 더욱 효과적으로 보호합니다.

저희는 계층화된 보호 기능으로 효과적인 WAF 보안을 제공합니다.

- 보안 분석
- 여러 관리형 규칙 집합
- 사용자 지정 규칙
- 머신 러닝 감지
- 중요한 데이터 감지
- 도용된 자격 증명 확인
- 차단 레이트 리미팅
- 멀웨어 방지 업로드 스캔

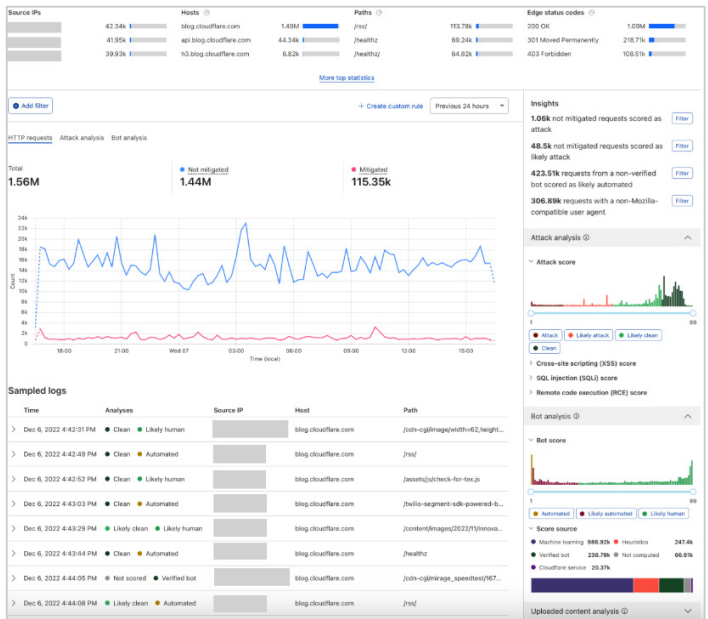
Cloudflare는 더 빠르게 응답합니다.

저희는 익스플로잇으로부터 더 빠르게 보호합니다. HTTP/2 Rapid Reset, Log4j 등 여러 주요 취약점의 경우 다른 WAF 벤더보다 하루 더 빠르게 여러 관리 규칙을 적용할 수 있었습니다.

Cloudflare는 애플리케이션 보안을 완벽하게 통합합니다.

Cloudflare WAF는 API Gateway, 봇 관리 등 나머지 애플리케이션 보안 포트폴리오와 완벽하게 통합되어 모두가 Cloudflare의 클라우드 연결성을 통해 단일 경로로 제공됩니다.

WAF 보안 분석



기업 보안용 WAF

SIEM 통합, SOC 레디

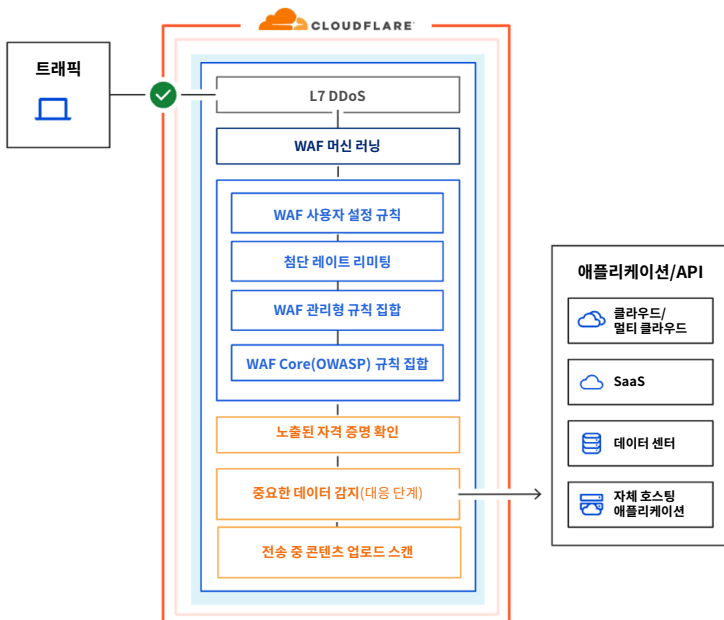
Cloudflare API 및 원시 로그 통합 덕분에 SIEM과 통합하거나 Cloudflare의 인텔리전스를 이용해 보안 운영 센터(SOC)를 가동하기가 쉽습니다.

더 간편해진 DevSecOps

당사의 기본 Terraform 통합 솔루션은 애플리케이션 보안을 DevOps 접근법에 쉽게 통합해줍니다.

Cloudforce One 지원

Cloudflare 애플리케이션 보안은 위협 운영 팀인 Cloudforce One에서 위협 인텔리전스를 받아 새로운 인텔리전스, TTP에 기반한 새로운 감지 기능으로 위협을 차단합니다.



웹 애플리케이션 보안	
여러 WAF 규칙 집합의 계층형 보호	여러 규칙 집합을 이용하여 어떠한 요청 구성 요소에서도 악의적인 페이로드를 차단합니다. 1. Cloudflare 관리형 규칙 2. OWASP 핵심 규칙 집합 3. 모든 공격을 차단하기 위한 사용자 지정 규칙 방대한 트래픽을 대상으로 검증을 거친 새로운 관리형 규칙이 오탐률을 최저 수준으로 낮춰줍니다.
zero-day 보호를 위해 업데이트된 규칙	패치나 업데이트가 제공되기 전에, 새로운 공격과 zero-day 취약성으로부터 보호하기 위해 Cloudflare 보안 팀이 규칙을 지속적으로 업데이트합니다.
머신 러닝 감지	계층형 규칙 집합을 보완하는 머신 러닝 모델로 우회 시도를 막습니다. 규칙에는 전체 WAF 공격 점수, XSS 공격 점수, SQLi 공격 점수, RCE 공격 점수의 네 가지 공격 점수를 사용할 수 있습니다.
주요 CMS 및 전자 상거래 플랫폼을 위한 플랫폼별 규칙 집합	WordPress, Joomla, Plone, Drupal, Magneto, IIS 등의 플랫폼을 추가 비용 없이 즉시 보호합니다.
사용자 설정 규칙 구성	규칙 또는 규칙 집합을 배포할 때 BLOCK, MANAGED CHALLENGE, JS CHALLENGE, SKIP, LOG, LEGACY CAPTCHA, CUSTOM RESPONSES 등의 작업을 사용하여 포지티브 또는 네거티브 보안 모델을 만듭니다.
첨단 레이트 리미팅	각 IP에 레이트 리미팅을 적용하거나 헤더 속성(예: 키, 쿠키, 토큰), ASN, 국가를 사용하여 애플리케이션과 API를 노리는 악용, DDoS, 무차별 대입 시도를 차단합니다.
중요한 데이터 감지	개인 식별 정보, 재무 정보, 신용카드 번호, API 키와 같은 비밀 등 중요한 데이터가 포함되어 있는 응답을 감지합니다.
노출된 자격 증명 확인	최종 사용자 계정이 탈취되기 전에 도난당한 자격 증명을 이용한 자격 증명 스테핑 공격을 감지합니다.
콘텐츠 업로드 스캔	WAF Content Scanning은 업로드된 파일을 스캔하여 맬웨어를 검사하며, 사용자는 사용자 지정 규칙을 생성하여 요청의 다른 매개변수와 그 신호를 결합할 수 있습니다.
SSL/TLS	애플리케이션에 대한 SSL 트래픽을 완전히 오프로드 및 구성합니다.
더욱 낮아진 오탐률	방대한 트래픽을 대상으로 검증을 거친 새로운 규칙이 오탐률을 최저 수준으로 낮춰줍니다.
gRPC 및 웹소켓 지원	gRPC 및 웹소켓 엔드포인트에 대한 프록시 및 보안 트래픽.
사용자 지정 가능한 차단 페이지	해당하는 방문자 세부 정보로 차단 페이지를 사용자 설정합니다.
더욱 광범위한 Cloudflare 제품군과 완전 통합	애플리케이션 성능, 지리적 경로 트래픽, 에지 컴퓨팅 활용을 개선합니다.

가시성, 보고, 프로그래밍 기능	
보안 분석	머신 러닝으로 점수를 매겨 잠재적인 공격을 모두 시각화합니다.
실시간 로깅 및 원시 로그 파일 액세스	WAF를 미세 조정할 수 있도록 가시성 확보. 모든 WAF 요청을 아우르는 심층 분석을 시행합니다.
페이로드 로깅	사건 분석을 위해 악의적 페이로드를 기록하고 암호화합니다.
SIEM 통합	기존 SIEM으로 로그를 직접 푸시 또는 풀링합니다.
Terraform 통합	애플리케이션 보안을 CI/CD 워크플로우에 통합합니다.
관리	
단일 콘솔 관리	단일 콘솔을 이용한 간소화된 관리로 글로벌 애플리케이션 보안 및 성능을 배포하고 관리합니다.
계정 수준 관리	모든 도메인에 맞는 하나의 계정 수준 WAF 구성을 통해 WAF를 관리하는 시간을 절약합니다.
SLA를 적용한 높은 가용성	SLA 위반의 경우 재정적 페널티를 포함한 100% 가동 시간을 보장합니다.
하드웨어, 소프트웨어 또는 튜닝이 필요 없음	DNS의 간단한 변경으로 배포합니다.
PCI 인증	Cloudflare는 레벨 1 서비스 공급자 인증을 보유하고 있습니다.
FedRAMP 인증	애플리케이션 보안을 포함한 정부용 Cloudflare 제품군은 FedRAMP 인증을 받았습니다.



더 자세히 알아보까요? [애플리케이션 보안 데모 시리즈](#)에 등록하세요.