CLOUDFLARE

데이터시트

# Cloudflare API Shield

Cloudflare를 API 보안 게이트웨이로 사용하면 API가 전례 없던 수준으로 비즈니스 성장을 이끌어줍니다.

세계는 API를 통해 돌아갑니다. 전 세계 인터넷 트래픽의 약 58%가 API와 관련되어 있습니다. 공격자들도 이 사실을 알고 있고, 그렇기 때문에 Gartner는 API가 조만간 가장 흔한 공격 벡터가 될 것으로 예측하고 있습니다.

Cloudflare API Shield는 API 탐색 및 혁신적인 계층화된 보안을 통해 API를 안전하고 생산적으로 유지해줍니다. API Shield는 Cloudflare의 애플리케이션 보안 포트폴리오의 일부로, 봇을 막고, DDoS 공격을 좌절시키고, 애플리케이션 공격을 차단하고, 공급망 공격을 모니터링할 수도 있습니다.

당사의 애플리케이션 보안 제품들은 성능 제품군과 긴밀하게 연동되며, 세계에서 가장 연결성이 좋은 글로벌 클라우드 플랫폼을 통해 제공됩니다.

## API 보안 혁신

API Shield는 계층화된 API 보안을 제공함과 동시에 사용 중인 모든 API를 탐색합니다. Cloudflare의 세계적인 수준의 네트워크 및 애플리케이션 계층에서의 DDoS 방어가 API Shield와 함께 보호 성능을 한층 강화합니다.

### API 탐색

자동 API 탐색을 통해 모든 API 엔드포인트를 탐색하고 모니터링하면서 섀도우 API를 없애고 API를 더 잘 관리할 수 있습니다.

### 더 강력한 인증

상호 TLS(mTLS)를 통해 인증서 기반 ID를 인증합니다. Cloudflare가 관리하는 이 허용 목록 모델은 유효한 인증서가 없는 요청을 차단해주기 때문에 모바일 및 IoT 장치에 있어서 중요한 역할을 합니다. Cloudflare는 도용된 자격 증명이 사용되었는지 또한 검사합니다.

### API 스키마 유효성 검사

API 스키마를 시행하는 능동적 보안 모델로 API를 보호하십시오. OpenAPI v3 스키마가 적용되어 있어 이 스키마를 기준으로 요청에 대한 유효성 검사가 자동으로 이루어집니다. 이 스키마를 준수하지 않는 모든 작업은 차단됩니다.

### 남용 및 데이터 손실 방지

첨단 이상 감지 기능이 API의 특정 용량에 대한 이해를 바탕으로 악의적인 볼류메트릭 API 트래픽을 차단합니다. Cloudflare 네트워크는 API 응답을 통해 중요한 정보가 새나가는 것을 감지하고 차단하는 데이터 손실 방지 기능 또한 제공합니다.

# 주요 API 보안 위험

API가 가지는 보안 문제를 바탕으로 OWASP는 염두에 두어야 하는 상위 10개의 API 보안 위협 목록을 공개했습니다. Cloudflare는 모든 OWASP API 위협에 대해 도움을 줄 수 있습니다. 일부 상위 문제는 아래에 설명되어 있습니다.

### 취약한 개체 수준 권한 부여

취약한 개체 수준 권한 부여(BOLA)는 요청 내의 개체 ID를 조작해 중요한 데이터에 허가받지 않고 접근하는 것을 의미합니다. BOLA를 통해 공격자들은 ID를 바꾸는 것만으로도 접근 권한을 가지지 못한 개체(데이터)에 접근할 수 있습니다.

### 손상된 사용자 인증

인증은 매우 중요하지만 대개는 잘못된 방식으로 도입됩니다. 공격자들은 결함(혹은 인증의 부재)을 악용해 부정한 방법으로 로그인하거나 다른 사용자의 ID를 도용합니다. 시스템이 고객/사용자를 올바르게 인증하지 못하면 API 보안이 손상됩니다.

### 리소스 부족 및 속도 제한

적절한 남용 방지 및 요청 가능한 리소스의 크기 혹은 개수를 제한하는 레이트 리미팅 없이는 API는 무차별 암호 대입 공격 및 서비스 거부 공격에 취약할 수밖에 없으며, 결국 API 서버 성능이 저하됩니다.

### 부적절한 자산 관리

잘못된 자산 관리는 현재의 생산 API와 가치가 낮아진 API를 추적하는 API 탐지 기능이 없을 때 일어나며, 섀도우 혹은 로그 API로 이어집니다. 이는 미흡한 API 활동 기록 때문에도 일어날 수 있습니다.

---

# 세계적 수준의 애플리케이션 보안

### 가장 정밀한 보호

API 위협, 봇과 공격에 대한 정밀한 보호를 통해 항상 보안과 비즈니스를 모두 챙깁니다. Cloudflare는 대규모 기업에 대해서도 검증 및 적응되었습니다.

### 방대한 통합 성능

무분별한 Acquisition 코드 베이스는 없습니다. 대신, 단일 콘솔에서의 통합 보안을 통해 위협 차단 성능이 지속적으로 강화됩니다. CDN, DNS, 트래픽 가속 등의 성능이 모두 내장되어 있습니다.

### 포괄적인 보안 상태

Cloudflare는 항상 완벽하고 엔터프라이즈 레디 상태이며 비용 효율적인 보안 성능을 제공합니다. Cloudflare는 결코 강력한 보안 상태를 구축하기 위해서 값비싼 애드온 또는 제삼자 마켓플레이스 통합 기능을 요구하는, 그 성능이 제한된 기본 솔루션으로 귀사를 괴롭히지 않습니다.


## Cloudflare 리더십

조직은 Cloudflare 글로벌 네트워크를 엔터프라이즈 보안의 경계로 삼아 보다 효율적인 애플리케이션 보안 상태를 구축할 수 있습니다. Cloudflare 애플리케이션 보안 포트폴리오는 그 강력한 성능과 방대한 범위로 무수히 많은 찬사를 받아 왔습니다. Gartner는 Cloudflare WAF를 2021 소비자의 선택으로 선정했습니다. Frost & Sullivan은 Cloudflare를 Global Holistic Web Protection 혁신 리더로 선정하고, IDC와 Forrester는 DDoS 리더로 선정했습니다.

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/3948.2022NOV4