

## Magic Transit

Cloudflare Magic Transit는 귀사의 네트워크 인프라, 데이터 센터, 퍼블릭 클라우드 서비스를 DDoS 공격으로부터 보호합니다

### 온프레미스, 클라우드 호스팅 및 하이브리드 네트워크를 위한 분산 서비스 거부(DDoS) 방어

#### 빠르고 신뢰할 수 있는 DDoS 방어

조직이 DDoS 공격의 대상이 되는 것은 이제 '여부'가 아니라 '언제'가 될 것인지의 문제입니다. DDoS 공격으로부터 네트워크 인프라를 보호하려면 위협 인텔리전스와 속도, 용량의 조합이 필요합니다. 볼륨메트릭 공격은 레거시 솔루션을 쉽게 압도할 수 있습니다. 대부분의 클라우드 기반 DDoS 완화 솔루션은 스크러빙 센터를 통해 트래픽을 백홀하여, 대기 시간이 크게 증가하고 성능 저하를 유발합니다.

- 거의 즉각적인 완화 시간(TTM)
- 모든 단일 데이터 센터에서 제공되는 DDoS 완화
- 몇 분 만에 완료되는 간편한 온보딩
- 단일 관리 지점



그림 1: 모든 Cloudflare 데이터 센터에서 제공되는 DDoS 방어

#### 업계를 선도하는 DDoS 방어

Magic Transit은 Gartner® Peer Insights™ ‘고객의 소리’ DDoS 완화 솔루션 부문에서 [고객의 선택](#)으로 선정되었습니다.

## 이점



### 현대적인 아키텍처

449 Tbps에 달하는 타의 추종을 불허하는 네트워크 용량을 330개 지점에서 제공합니다. Cloudflare는 스크러빙 센터로트 래픽을 백홀하지 않으며, 많은 고객이 Cloudflare로 이전한 후 성능이 개선되었다고 보고합니다.



### 포괄적인 방어

Cloudflare는 매일 평균 2,340억 건의 사이버 위협을 차단합니다. 복잡하고 새로우며 정교한 공격을 더 효과적으로 방어하기 위해 위협 인텔리전스를 공유합니다. Magic Transit은 대부분의 공격을 3초 이내에 완화하는 자동화된 방어 기능을 제공합니다.



### 사용 편의성

자체 IP 주소 사용(BYOIP) 또는 Cloudflare 임대 IP를 통해 몇 분 만에 온보딩할 수 있습니다. Cloudflare의 '상시 가동' 보호 기능으로 설정 후 신경 쓸 필요가 없습니다. 분석, 알림 및 로그를 위한 단일 콘솔 또는 API를 통해 모든 구성이 가능합니다.