# Magic Firewall

기업 네트워크 및 클라우드 인프라용 클라우드 네이티브 네트워크 방화벽

## 네트워크 전체를 위한 서비스형 방화벽

**장비를 관리할 부담 없이 일관된 보안 정책을 전역적으로 적용합니다**

Cloudflare Magic Firewall에서 제공하는 확장 가능한 고급 서비스형 방화벽(FWaaS) 보호 기능으로 모든 지사, 데이터 센터, 클라우드, 최종 장치에 일관된 보안 정책을 적용합니다

Magic Firewall을 포함한 모든 Cloudflare 서비스는 Cloudflare의 광범위한 전역 네트워크를 통해 제공되므로, 귀사의 비즈니스 요구 사항에 맞춰 보안을 확장할 수 있습니다. 원치 않는 트래픽을 자동으로 필터링합니다. 헤어피닝, 보안 병목 지점, 장비 관련 가동 중단이 더 이상 발생하지 않습니다.

### 성능 저하 없음

보안 정책을 적용하기 위해 트래픽을 중앙 데이터 센터로 백홀링하지 마세요. Cloudflare 데이터 센터에서 전역적으로 제공되는 보안 서비스를 통해 트래픽은 항상 최적의 경로를 유지합니다.

### 하드웨어 추가 불필요

개별 물리 또는 가상 방화벽 장비를 관리하는 데 더 이상 시간을 낭비하지 마세요. 보안 정책이 몇 초 만에 Cloudflare 네트워크 에지에서 전역적으로 자동으로 배포됩니다.

### 포괄적인 보안

Cloudflare 네트워크에서는 매일 2,270억 건의 사이버 위협이 감지되고 차단됩니다. 지능형 및 프로그래밍 가능 전역 네트워크로 구동되는 단일 보안 플랫폼.

| Magic Firewall 기능 | |
|---|---|
| **표준** | **고급(추가 기능)** |
| • 프로토콜, 포트, IP 주소, 패킷 길이, 비트 필드 일치 등을 기반으로 한 필터링<br>• 방화벽 및 네트워크 구성을 관리하는 단일 대시보드<br>• 대시보드 또는 API를 통한 트래픽 분석 사용 가능<br>• Magic Transit 및 Magic WAN에 포함됨 | • Cloudflare One과의 원활한 통합<br>• IP 목록 사용자 지정 가능<br>• 관리형 위협 인텔리전스 IP 목록(익명성 도구, 봇넷, 맬웨어, 오픈 프록시, VPN 포함)<br>• 사용자 국가 위치에 따른 지리적 차단<br>• 침입 감지 시스템(IDS) |

## 왜 Cloudflare를 이용해야 할까요?

### 모든 데이터 센터, 모든 서비스

소스에서 최대한 가까운 곳에서 트래픽을 처리하여 방화벽의 작업 부하를 줄임

### 단일 경로, 다중 계층 보호

Cloudflare의 전역 Anycast 네트워크는 실시간 네트워크 문제를 감지하고 가장 효율적인 네트워크 경로로 트래픽을 라우팅하여 정체를 피함

### Cloudflare에 직접 연결

공용 인터넷을 우회하고 Cloudflare Network Interconnect를 사용하여 직접 연결

## 추가 리소스

- 웨비나: '레거시 방화벽 도우미와의 작별: 네트워크가 마땅히 누려야 할 보호 받기'
- 참조 아키텍처: https://developers.cloudflare.com/reference-architecture/diagrams/network/protect-public-networks-with-cloudflare/