

---

# 중국 내 웹 사이트의 성능 및 보안 최적화

---

중국의 거대하고 복잡하며 빠르게 성장하는 인터넷 경제를 활용하기 위한 전략

---

## 핵심 요약

중국 은 인터넷으로 연결되는 인구 수로 볼 때 단연코 세계 최대의 시장입니다. 그러나 네트워크의 복잡성과 언제나 존재하는 사이버 공격 위협으로 인해 해당 시장으로의 진입이 마냥 쉽지만은 않습니다. 기업들이 이러한 장애를 극복하고 중국 사용자를 위한 웹 사이트 경험을 최적화할 수 있도록 Cloudflare는 글로벌 성능 및 보안 네트워크 서비스를 중국으로 확장했습니다.

## 온라인 비즈니스를 중국으로 확장하는 과정에서의 문제

중국 은 거대한 온라인 경제가 빠르게 성장하므로 다양한 비즈니스에 있어서 매력적인 시장이 되고 있습니다. [10억 명이 넘는 중국인이 인터넷에 연결되어 있습니다.](#) 이는 세계 최대 인터넷 이용 인구입니다. 그리고 [8억 1,200만 명이 넘는 사람들이 2021년 상반기에 온라인 구매를 했습니다.](#) 이 기간 동안 전체 온라인 지출은 Covid-19 팬데믹으로 인한 경제 불안정 때문에 전년 대비 다소 감소했지만, [중국 경제는 여전히 Covid-19 이후에 두 자릿수 성장을 경험했으며 전자 상거래 시장은 2020년에 12.5% 성장했습니다.](#)

다른 지역의 시장에서와 마찬가지로 중국에서 사업을 운영하는 글로벌 기업은 현지 시장의 기대에 부응하기 위해 서비스와 온라인 경험을 시장에 맞추어야 합니다. 안타깝게도 중국의 인터넷 규정, 기본 인프라, 위협 환경 때문에 글로벌 기업이 현지 소비자가 기대하는 품질의 경험을 제공하기 어렵게 하는 여러가지 독특한 문제가 생겨납니다. 이러한 어려움으로는 다음과 같은 것들이 있습니다.

- 단편화된 네트워크와 열악한 로컬 피어링으로 인한 속도 지연
- 모바일 웹사이트 성능 트레이드오프
- 지속적인 중국 내 사이버 공격

본 백서에서는 그러한 문제를 자세히 설명하고, 이를 극복하기 위한 전략을 설명하며, Cloudflare가 도움이 되는 방법을 제시합니다.

### 인터넷 병목 현상 및 열악한 로컬 피어링 때문에 발생하는 지연 시간

많은 소비자와 같이 중국인들의 온라인 경험 기대 수준도 높습니다. [HSBC 보고서에 따르면, 중국은 전 세계적으로 전자 상거래 시장을 선도하며 지배하고 있습니다.](#) 또한 [business.com 분석에서는 중국의 전자 상거래 시장이 전 세계에서 가장 큰 것으로 인정되었습니다.](#)

안타깝게도 기업들은 종종 중국 사용자를 위해 사이트가 신속하고 안정적으로 동작하도록 하는데 있어 어려움을 겪습니다.

그 이유 중 한 가지는 네트워크 병목 현상입니다. 중국 안팎으로 이동하는 모든 인터넷 트래픽은 베이징, 상하이, 광저우의 세 IXP(인터넷 익스체인지 포인트) 중 하나를 통과하게 됩니다. 사용량이 많은 기간 동안 해당 IXP는 정체되어 중국 외부에서 호스팅되는 웹 사이트의 로드 시간을 크게 증가시키게 됩니다. [일련의 테스트에 따르면 TED 웹 사이트는 최대 브라우징 기간 동안 상하이에서 최초 로딩 시 8초에서 38초 사이가 소요된 반면, 비슷한 기간 동안 뉴욕에서는 5초에서 8초 사이가 소요되었습니다.](#)

---

이러한 병목 현상을 피하기 위해 일부 글로벌 기업은 중국의 3개 IXP 중 하나와 인접한 데이터 센터에서 웹 사이트를 호스팅하기로 합니다. 예를 들어, 홍콩은 광저우 IXP에 가깝거나 중국 국경 내의 서버에 있습니다. 하지만 해당 접근 방식은 피어링이 제대로 되지 않은 제한된 수의 로컬 ISP(인터넷 서비스 공급자)라는 또 다른 주요 네트워크 문제 때문에 여전히 위험에 노출됩니다.

중국의 인터넷 환경에 익숙한 기업은 이미 세 개의 국영 ISP인 China Telecom, China Mobile, China Unicom이 시장을 장악하고 있음을 알고 있을 것 입니다. 이들 ISP는 각각 중국의 특정 지역에서 지배적입니다. 이들은 또한 상대적으로 적은 피어링 또는 IXP에서 별도의 네트워크를 연결하는 관행적 특성을 가지고 있습니다. [2017년 Mlytics 연구](#)에 따르면 중국에서 가장 많이 피어링된 네트워크는 2개의 IXP에만 연결되어 있는 반면, 북미에서는 66개, 유럽에서는 71개에 연결되어 있습니다.

이는 국내 인터넷 트래픽도 비교적 짧은 지리적 거리를 이동하기 위해 종종 긴 네트워크 거리를 커버해야 한다는 사실을 의미하며, 최종 사용자에게는 추가적인 대기 시간이 발생하게 됩니다.

### 병목 현상 및 열악한 로컬 피어링을 극복하는 방법

이러한 웹 성능 문제에 직면하며 중국에서 사업을 영위하는 대다수의 글로벌 기업은 콘텐츠 전송 네트워크(CDN)를 통해 최종 사용자와 인접한 데이터 센터에서 정적(또는 비사용자별) 웹 사이트 콘텐츠를 캐시하기로 선택합니다. 따라서 이들 기업의 요청 중 대다수가 원본 서버로 돌아갈 필요가 없게 됩니다. 기업들은 다음과 같은 CDN을 고려해야 합니다.

- **규모가 크며 피어링이 제대로 된 네트워크가 있어야 합니다.** CDN에 데이터 센터가 많을수록 최종 사용자와 더욱더 가까워집니다. 그리고 중국의 3대 ISP에서 더 많은 커버리지가 가능하도록 최종 사용자가 요청해야 하는 네트워크 홉이 줄어듭니다.
- **중국 내에서 DNS 쿼리를 해결하는 것이 가능합니다.** DNS 확인 프로세스(도메인 이름이 IP 주소로 변환되는 프로세스)는 트래픽이 중국 안팎으로 이동해야 할 경우 다른 사이트 콘텐츠가 로컬로 캐시된 경우에도 대기 시간을 늘어나게 할 수 있으며, 중국 내 DNS 쿼리를 해결하는 방식은 이 대기 시간을 줄일 수 있게 합니다.
- **웹 사이트 HTML, CSS, 자바스크립트 코드를 최소화합니다.** 해당 유형의 코드는 대부분의 웹 사이트를 구성하는 요소이기 때문에 최종 사용자의 브라우저에 사이트가 어떤 모습이어야 하는지를 알려줍니다. 최소화는 코드에서 불필요한 문자를 제거해서 전체 크기를 줄여 네트워크를 통과할 때 대역폭을 덜 차지하도록 만들어 주는 프로세스입니다. 대역폭이 적으면 사이트 로드 속도가 빨라집니다.
- **네트워크 에지에서 서버리스 코드를 통해 요청에 응답하기 위한 사용자 설정 규칙을 만듭니다.** [서버리스 코드](#)는 개발자가 제어하는 특정 서버에 국한되지 않는 코드입니다. [네트워크 에지에서 실행 시](#) 서버리스 코드는 데이터 센터의 대규모 네트워크에 존재합니다. 이는 코드가 특정 최종 사용자 트래픽에 특수 규칙을 쉽고 신속하게 적용하는 것이 가능하다는 것을 의미합니다. 예를 들어, 조직은 모바일 사용자, 느린 인터넷 연결, 기타 다양한 사용 사례에 관한 특별 규칙을 시행하는 중국 기반 네트워크에서 서버리스 코드를 작성하는 것이 가능합니다.

Cloudflare 및 JD Cloud의 네트워크 파트너십은 글로벌 성능 서비스와 함께 트래픽 병목 현상과 열악한 피어링을 극복하는 데 도움이 됩니다. 이 백서의 다음 섹션으로 이동하여 내용을 확인하십시오.

---

## 지속적인 중국 내 사이버 공격

다른 지역과 마찬가지로 중국에서 운영되는 웹 사이트도 여러 가지 보안 위협에 노출되어 있습니다.

여기에 해당하는 위협 중의 하나는 DDoS(분산 서비스 거부) 공격으로, 서버나 네트워크 인프라에 정크 트래픽이 짧은 시간 내 폭증해 정상적인 요청에 응답이 불가능한 상태를 만듭니다. [Talos Intelligence의 2017년 보고서](#)에 따르면 전문가가 아닌 사용자가 감염된 장치의 기존 봇넷으로 쉽게 공격을 시작할 수 있도록 하는 DDoS 실행 대행 서비스가 중국 내 빠르게 퍼지고 있는 것으로 확인되었습니다.

그 이후 중국 사법 기관은 2019년에 [200,000개 이상의 장치](#)를 감염시키고 200Gbps에 달하는 공격을 시작한 봇넷 1개를 포함한 다수의 주요 DDoS 봇넷을 차단했습니다. 그러나 [DoubleGuns](#)와 같은 다른 봇넷은 여전히 활동하고 있으며 해당 봇넷의 운영자는 본 백서가 배포될 당시에도 여전히 활발히 활동하고 있었습니다.

중국의 웹 사이트는 또한 개인 데이터 및 개발 환경에 대한 정상적이지 않은 접속 시도를 방지할 수 있어야 합니다. 2018년에 공격자들은 45,000개가 넘는 중국 웹 사이트의 서버에 접속하기 위해 [인기 있는 PHP 프레임워크의 취약점을 악용했습니다](#). 프레임워크에 대한 공격은 취약점이 공개된지 24시간도 지나지 않아서 시작되었습니다. 마찬가지로, 2020년에는 중국에 기반을 둔 두 명의 공격자가 다양한 웹 응용 프로그램 취약성을 악용하여 10년간 수백 개 회사의 프라이빗 네트워크에 불법적으로 접속한 혐의로 기소되었습니다.

게다가 중국에서 개인 데이터를 보호하고자 하는 기업들은 일반적인 도구 키트 사용이 불가능할 수 있습니다. 중국 네트워크에서는 TLS 1.3 및 암호화된 서버 이름 식별(ESNI)과 같은 최신 암호화 표준을 지원하지 않으므로 무단 관찰자가 트래픽을 스누핑할 가능성이 높습니다.

## 중국 내에서의 지속적인 사이버 공격을 방어하는 방법

[전 세계적으로 증가하는 DDoS 공격으로](#) 인해 DDoS 완화 서비스 및 웹 애플리케이션 방화벽(WAF)과 같은 기타 응용 프로그램 보안 도구는 모든 웹 사이트의 기본적인 보안 요건이 되었습니다. 중국도 다르지 않습니다. 이 시장에서 보안을 추구하기 위해서는 기업은 다음을 고려해야 합니다.

- **제한된 '스크리빙 센터'가 아닌 네트워크 에지에서 DDoS 완화.** 거의 모든 최신 DDoS 완화 서비스가 클라우드에서 작동되지만, 대부분의 경우 제한된 수의 데이터 센터에 의존하여 악의적 트래픽을 필터링 또는 '스크리빙'합니다. 검사를 위해 해당 '스크리빙 센터'로 트래픽을 백홀하기 위해서는 추가 네트워크 홉이 필요하며 따라서 특히 네트워킹 제한이 있는 중국에서 사용자의 사용에 지연 및 중단을 초래할 수 있습니다. 중국에서 인터넷 성능에 영향을 주지 않고 DDoS 완화를 제공하기 위해서 조직은 네트워크 홉을 추가하지 않고 모든 에지 데이터 센터에서 DDoS 완화를 제공하는 클라우드 서비스를 고려해야 합니다.
- **남용 차단을 위한 속도 제한.** 고정밀도의 계층 7 DDoS 공격을 완화하고, API 악용을 차단하여 가용성을 보장하며, 무차별 로그인 공격으로부터 중요한 고객 정보를 보호하고, 리소스 소모로부터 원본 서버를 보호할 수 있는 세부 제어를 보유하는 것이 필수적입니다. 동시에 트래픽 급증으로 인한 예측할 수 없는 비용을 방지해야 합니다.

- **자동으로 신속하게 업데이트되는 WAF.** 중국 내 공격자는 새로운 웹 응용 프로그램 취약성을 매우 신속하게 악용할 수 있다는 것을 입증했습니다. 기업들은 자체 WAF 규칙 생성을 통해 모든 것을 해결하길 바랄 수 있으나, 자체 위협 인텔리전스와 업데이트 기능에만 의존해서는 안 됩니다. 기업들은 관찰된 위협의 광범위한 풀을 기반으로 자동으로 업데이트되는 웹 애플리케이션 방화벽을 고려해야 합니다. 그리고 기업들 자체의 규칙 업데이트가 필요할 때는 이러한 변경 사항이 가능한 한 빨리 배포될 수 있는 환경 안에 있어야 합니다.
- **사용자 정의가 가능한 암호화 옵션.** TLS 1.3 및 ESNI 부재 시 전송 중인 데이터의 보호를 위해 기업들은 사용자 정의가 가능한 다양한 암호화 방법을 제공하는 보안 서비스를 고려해야 합니다.

중국 네트워크의 일부로 제공되는 Cloudflare의 보안 서비스는 지연 없는 DDoS 완화 및 글로벌 위협 인텔리전스에 기초한 신속한 업데이트 WAF를 제공합니다. 자세한 내용은 본 백서의 다음 섹션으로 이동하세요.

## Cloudflare가 중국에서 운영되는 글로벌 웹 사이트를 지원하는 방법

Cloudflare는 전 세계 100개국 200개의 글로벌 도시에서 데이터 센터 네트워크를 운영합니다. 2022년 3월 현재, 중국 내 38개 도시에 걸쳐 데이터 센터 45곳이 분산되어 있습니다. 이들 데이터 센터는 각각 콘텐츠 전송, DNS 확인, DDoS 완화, WAF 시행, 서버리스 코드 실행 등을 포함하여 광범위한 보안, 성능, 안정성 서비스를 수행할 수 있습니다. 해당 서비스는 모든 단일 데이터 센터에서 제공되기 때문에 최종 사용자와 매우 인접한 곳에서 기능이 발휘되어 지연 시간이 줄어들고 네트워크에 최신 위협 및 네트워크 상태에 대한 상세한 최신 정보가 제공됩니다. 뿐만 아니라 기업들은 단일 대시보드를 통해 이러한 서비스를 모두 관리할 수 있습니다.

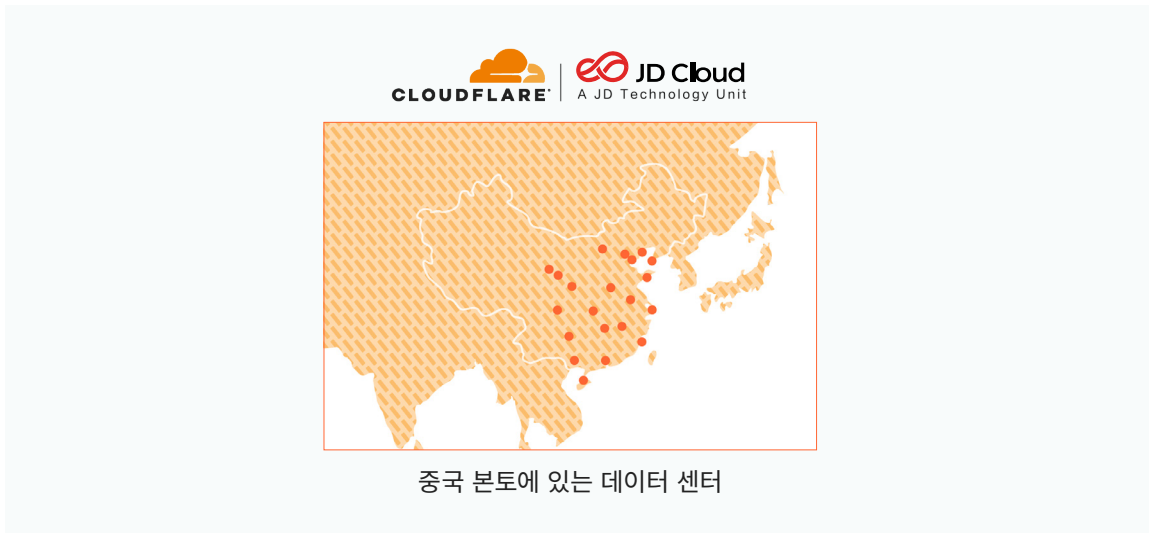
Cloudflare는 2015년부터 기업들이 중국에 기반을 둔 서비스 방문자들에게 안전하고 빠르며 안정적인 인터넷 경험을 제공하도록 지원해 왔습니다. 이러한 서비스를 개선하기 위해 당사는 최근 중국 인터넷 대기업인 JD.com의 클라우드 및 지능형 기술 사업부인 JD Cloud와 파트너십을 시작했습니다.

이제 이 네트워크가 기업들이 이전 섹션에서 다룬 문제를 극복하는 데 어떻게 도움이 되는지를 알아보겠습니다.

## Cloudflare가 지연 시간을 극복하는 방법

Cloudflare 및 JD Cloud의 중국 네트워크는 다음을 제공합니다.

- **Argo Smart Routing:** 클라이언트에서 원본으로 데이터를 전송하고 다시 가져오면 대기 시간이 발생할 수 있습니다. 캐싱을 통해 정적 콘텐츠는 네트워크 정체체를 피할 수 있지만, 동적 콘텐츠는 인터넷의 가용성, 신뢰성, 성능에 의존합니다. 이는 느린 로드 시간, 제한 시간 초과, 연결 끊김, 악화된 최종 사용자 경험으로 이어질 수 있습니다. **Argo Smart Routing**에는 **정체를 실시간으로 감지하고 웹 트래픽을 가장 빠르고 신뢰할 수 있는 네트워크 경로에 걸쳐 라우팅하기 위한 고유한 기능이 있습니다.** Cloudflare 고객과 사용자의 Cloudflare 네트워크에 대한 요청은 어떤 시점에서 다양한 인터넷 요소가 어떻게 작동하고 있는지 이해하는 데 도움이 됩니다. Argo Smart Routing은 Cloudflare가 **동적으로 트래픽을 가장 빠른 경로를 통해 원본으로 라우팅하기 위해 수집하는 타이밍 데이터를 사용하여** 성능을 개선합니다. 평균적으로 Argo는 웹 자산 성능을 약 30% 개선합니다. 또한 이는 판매 및 고객 보유 증가로 이어집니다.
- **중국 내부의 많은 데이터 센터에서 정적 콘텐츠를 캐싱하고 제공하여** 최종 사용자가 어디에 위치하든 더 짧은 대기 시간 및 더 빠른 페이지 로드 시간을 제공합니다. 당사의 네트워크는 모든 중국 ISP와 밀접하게 연결되어 있기 때문에 트래픽이 필요로 하는 네트워크 홉 수가 줄어듭니다.



중국 본토에 있는 데이터 센터

- **중국 내 선택적 DNS 확인으로** 응답 시간이 더욱 빨라졌습니다.
- 효율적인 라우팅 및 패킷을 처리할 수 있는 **IPv6**(인터넷 프로토콜 버전 6) 사용이 가능합니다.
- Cloudflare 대시보드에서 확인란을 선택하여 손쉽게 활성화가 가능한 자동 최소화 기능으로 **웹 사이트 코드를 최소화**할 수 있습니다.
- Cloudflare 중국 네트워크의 모든 데이터 센터에서 운영되는 Cloudflare Workers 서비스를 사용한 **서버리스 컴퓨팅**. 활용해 사용자 지정 방식으로 특정 요청에 응답하고 기존 응용 프로그램을 보강하는 것이 가능합니다. 인프라의 구성 또는 유지 관리 없이도 완전히 새로운 것을 생성하는 것도 가능합니다.

---

## Cloudflare가 지속적인 국내 사이버 공격을 처리하는 방법

Cloudflare 중국 네트워크에 통합된 보안 서비스를 사용하여 기업들은 다음을 수행하는 것이 가능합니다.

- **DDoS 공격을 완화합니다.** 중국에 있는 모든 데이터 센터는 공격을 완화할 수 있기 때문에 네트워크에 적법한 요청을 잃지 않고 대규모 공격을 흡수할 수 있는 엄청난 용량을 제공합니다. 트래픽 검사는 최종 사용자와 인접한 곳에서 이루어지므로 최종 사용자의 요청은 잠재적으로 원거리에 위치한 '스크러빙 센터'로 백홀되는 긴 프로세스를 피하는 것이 가능합니다. 그리고 중국의 네트워킹 문제 때문에 Cloudflare는 자동 경로 공격 트래픽의 재라우팅을 허용하는 고유한 자동화된 트래픽 엔지니어링 기능을 제공합니다. 이러한 모든 기능은 중국 내외의 합법적인 트래픽에 있어서의 성능 저하를 방지합니다.
- Cloudflare WAF를 통한 WAF는 **응용 프로그램 취약성 보호**. 관리 규칙 집합(예: OWASP 및 Cloudflare 독점 규칙 구현)으로 알려진 공격 벡터를 막으며, 아울러 최신 위협을 자동으로 막기 위해 네트워크에 걸쳐 위협 인텔리전스의 지속적인 흐름을 이용합니다. 또한 조직에서는 자체적인 규칙을 쉽게 생성할 수 있으며 이를 단 몇 분 만에 전체 네트워크에 걸쳐 전파할 수 있습니다. 2021년에 적용된 개선은 더 많은 트래픽을 다루기 위해 WAF가 더 빠르고 배포되고 원활하게 확장될 수 있도록 합니다. WAF는 또한 규칙 상태를 작업과 분리하여 더 나은 제어를 제공하는 규칙 집합을 업데이트했습니다. 사용자는 이제 고급 필터링, 대량 편집, 규칙 태그 등을 통해 더 나은 규칙을 즐길 수 있습니다.
- **속도 제한**은 WAF 사용자 설정 규칙과 통합되었으며 DDoS 공격, 무차별 대입 로그인 시도, 원본 서버 과부하, API와 응용 프로그램을 대상으로 하는 기타 남용 유형 등으로부터 보호합니다. 사용자는 임계값을 구성하고, 트래픽을 정의하며, 응답을 사용자 지정하고, 웹 사이트, 응용 프로그램, API 엔드포인트의 특정 URL에 대한 가치 있는 통찰력을 얻을 수 있습니다.
- **TLS 1.2를 통해 데이터를 암호화하고** Cloudflare 대시보드에서 자체 인증을 쉽게 관리합니다.

## 자세한 정보 알아보기

---

Cloudflare의 중국 네트워크 서비스는 모든 Cloudflare Enterprise 요금제 고객에게 제공됩니다. Cloudflare의 중국 네트워크 서비스는 또한 중국 네트워크에 온보딩하려면 유효한 인터넷 콘텐츠 공급자(ICP) 라이선스를 필수적으로 요구하는 중국 법과 규제를 완벽히 준수합니다.

중국의 인터넷 경제가 계속 성장함에 따라 새로운 보안 및 성능 문제가 불가피하게 나타날 것입니다. 중국에서의 지속적인 성장을 위하여 Cloudflare에서는 당사 네트워크의 기업들이 해당 문제에 신속하게 대응하고 원활한 사용자 경험에 대한 기준을 계속 높일 수 있도록 하려고 계획하고 있습니다.

Cloudflare와 통화해서 오늘 중국에서 여러분의 웹 프레즌스 최적화를 시작하세요!

Cloudflare 중국 네트워크에 대한 자세한 내용은 [cloudflare.com/network/china/](https://cloudflare.com/network/china/) 를 방문하거나 Cloudflare 담당자에게 문의하세요.



---

© 2022 Cloudflare Inc. 판권 소유. Cloudflare 로고는 Cloudflare의 상표입니다.  
기타 모든 회사 및 제품 이름은 관련된 각 회사의 상표일 수 있습니다.