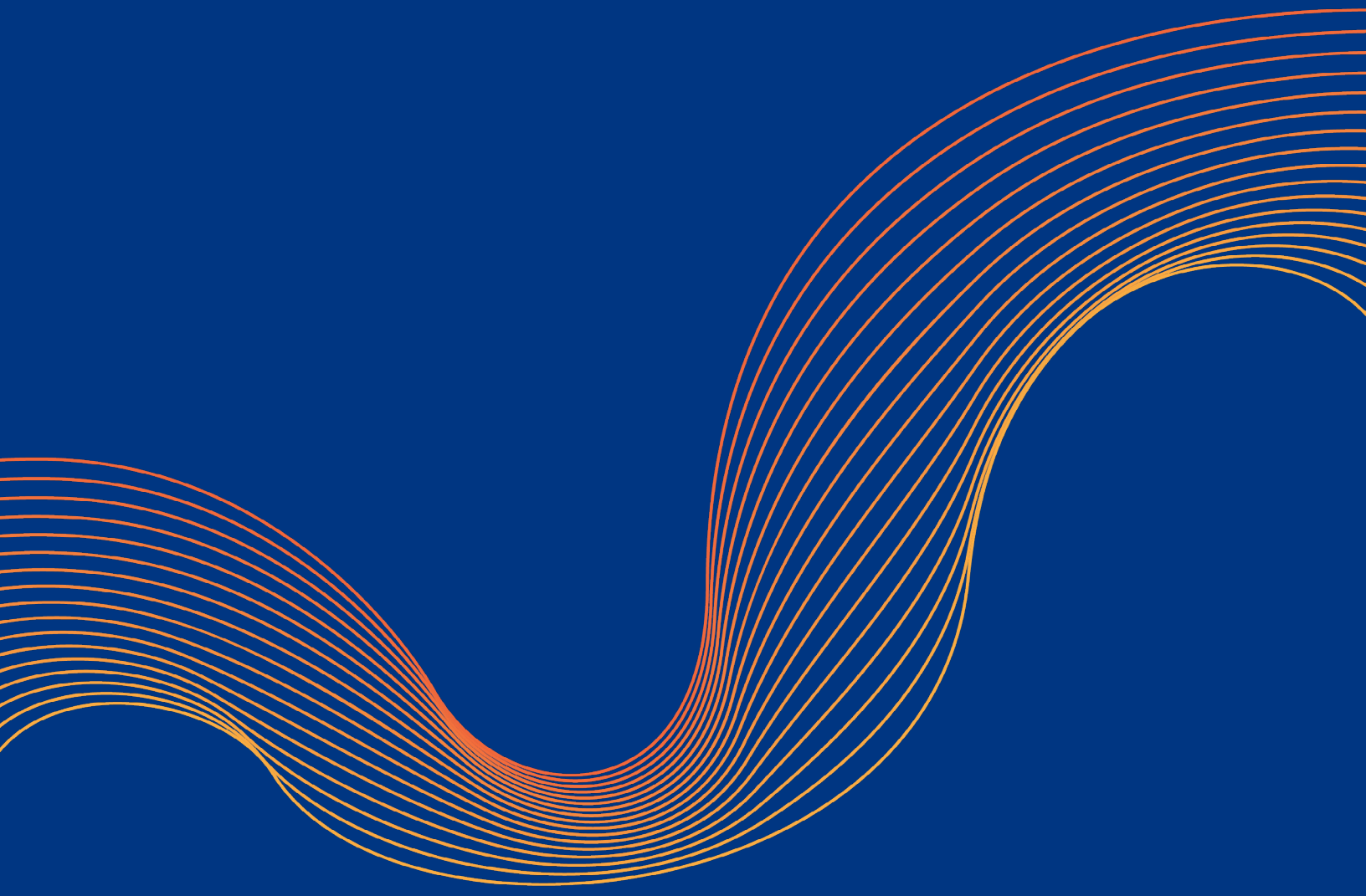
WHITEPAPER

CLOUDFLARE

Optimize website performance and security in China

Strategies for tapping into China's massive, complex and rapidly growing Internet economy



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Executive Summary

China is home to the world's largest Internet-connected population. However, network complexity and the ever-present threat of cyber attacks can make it hard to tap into this market. To help organizations overcome these hurdles and better optimize their website experience for users in China, Cloudflare has seamlessly extended its global performance and security network services into China.

The challenges of expanding an online business to China

China's vast, rapidly growing online economy makes it an appealing market for a variety of businesses. Over 900 million Chinese citizens are connected to the Internet — the world's largest Internet-connected population — and over 749 million of those people made an online purchase in the first half of 2020. Overall online spending dipped somewhat during that period compared to previous years, due in large part to broader economic instability caused by the Covid-19 pandemic — but many sectors still experienced double-digit online growth over the course of the year.

As with any regional market, global businesses operating in China must adapt their services and online experiences to meet local expectations. Unfortunately, China's Internet regulations, underlying infrastructure and threat landscape present a variety of unique challenges that can make it harder for global businesses to deliver the quality of experience local consumers expect. These challenges include:

- Latency caused by fragmented networks and poor local peering
- Mobile website performance trade-offs
- Persistent domestic cyberattacks

This paper explains those challenges in detail, describes strategies for overcoming them, and shows how Cloudflare can help.

Latency caused by Internet bottlenecks and poor local peering

Like many consumers, people in China have high expectations for online experiences. A recent PwC report identified China as the world's most advanced ecommerce market, and found that its consumers are far more likely than global consumers to pay for purchases, research product information, and complete other buying journey steps online (as opposed to in-person).

Unfortunately, organizations often struggle to make their sites perform quickly and reliably for users in China.

One reason is network bottlenecks. All Internet traffic traveling in and out of China passes through one of three Internet Exchange Points (IXPs): in Beijing, in Shanghai, or in Guangzhou. During high-usage periods, these IXPs can become congested and significantly increase load times for websites hosted outside of China. One series of tests found that the TED website took between 8 and 38 seconds to load for the first time in Shanghai during a peak browsing period, compared to a range of 5 to 8 seconds in New York during a comparable period.

To avoid these bottlenecks, some global companies choose to host their websites in data centers close to one of China's three IXPs — e.g. Hong Kong to be close to the Guangzhou IXP — or on servers within China's borders. However, these approaches are still at risk from another major network challenge: a limited number of poorly peered local Internet Service Providers (ISPs).

Companies who are familiar with China's Internet landscape may already know that three state-owned ISPs dominate the market: China Telecom, China Mobile and China Unicom. Each of these ISPs dominates in a certain part of the country. They also engage in comparatively little peering, or the practice of connecting separate networks at IXPs. A 2017 Mlytics study found that the most peered network in China was only connected to two IXPs, compared to 66 in North America and 71 in Europe.

What this means is that even domestic Internet traffic often must cover a large amount of network distance in order to travel a relatively short geographical distance, resulting in additional latency for end-users.

How to overcome bottlenecks and poor local peering

Faced with these web performance challenges, many global organizations doing business in China choose to use a content delivery network (CDN) to cache static (or non-user-specific) website content in data centers close to end-users, so that many of their requests do not have to travel all the way back to an origin server. Organizations should consider CDNs that:

- **Have a large and well-peered network**. The more data centers a CDN has, the closer it will be to end-users. And the more peered it is with China's three major ISPs, the fewer network hops end-user requests will have to take.
- **Can resolve DNS queries within China.** The DNS resolution process — the process by which domain names are converted into IP addresses — can add latency if its traffic must travel in and out of China, even if other site content is cached locally.
- **Minimize website HTML, CSS, and Javascript code.** These types of code are the building blocks of most websites, telling end-users' browsers what the site should look like. Minification is the process of removing unnecessary characters from code, reducing its overall size — and thus making it take up less bandwidth when traversing a network. Less bandwidth means the site loads faster.
- **Use serverless code on the network edge to create custom rules for responding to requests.** Serverless code is code that is not confined to a particular server that a developer controls. When it runs on the network edge, serverless code exists across a large network of data centers. This means the code can easily and quickly apply special rules to specific end-user traffic. For example, an organization could write serverless code on a China-based network that enforces special rules for mobile users, for slower Internet connections, and many other use cases.

Cloudflare's network partnership with JD Cloud, along with our global performance services, can help overcome both traffic bottlenecks and poor peering. Jump to the next section of this paper to see how.

Persistent domestic cyberattacks

As in any region, websites operating in China face a variety of security threats.

One such threat is distributed denial-of-service (DDoS) attacks, which bombard servers or network infrastructure with so much junk traffic that it is unable to respond to legitimate requests. A 2017 report by Talos Intelligence found that domestic DDoS-for-hire services — which allow non-expert users to easily launch attacks by using an existing botnet of infected devices — were expanding rapidly in China.

Since then, Chinese law enforcement agencies have shut down several major DDoS botnets, including one in 2019 that had infected over 200,000 devices and launched attacks as large as 200 Gbps. But other botnets are still active — such as DoubleGuns, whose operators are still at large at the time of this paper's publication.

Websites in China must also prevent attempts to access private data and development environments. In 2018, attackers exploited a vulnerability in a popular PHP framework in an attempt to access the servers of over 45,000 Chinese websites. Attacks on the framework began less than 24 hours after its vulnerability was publicized. Similarly, in 2020, two China-based attackers were indicted for illegally accessing hundreds of companies' private networks over the course of ten years, again by taking advantage of a variety of web application vulnerabilities.

What's more, organizations who want to protect private data in China may not be able to draw from their usual toolkit. Chinese networks do not support modern encryption standards like TLS 1.3 and Encrypted Server Name Identification (ESNI), creating more chances for unauthorized observers to snoop on traffic.

How to defend against persistent domestic cyberattacks in China

Increases in DDoS attacks around the world have made DDoS mitigation services — and other application security tools like web application firewalls (WAFs) — a table stakes security requirement for any active website. China is no different. When looking for such protection in this market, organizations should consider:

- **DDoS mitigation from the network edge, rather than limited 'scrubbing centers'.** Although almost every modern DDoS mitigation service operates in the cloud, many rely on a limited number of data centers to filter, or 'scrub,' malicious traffic. Backhauling traffic to these 'scrubbing centers' for inspection can require extra network hops and thus cause latency and disruption to users — especially in China, with its networking limitations. To provide DDoS mitigation without impacting Internet performance in China, organizations should consider cloud services that offer DDoS mitigation in every edge data center without adding additional network hops.

- **WAFs that update automatically — and quickly.** Domestic attackers in China have proven themselves capable of taking advantage of new web application vulnerabilities very quickly. Organizations may want to be able to create their own WAF rules, but they should not rely solely on their own threat intelligence and ability to make updates. They should consider web applications firewalls that update automatically based on a wide pool of observed threats. And when the organization does want to make its own rule updates, it should feel confident that those changes will propagate as quickly as possible.
- **Customizable encryption options.** To protect data in transit in the absence of TLS 1.3 and ESNI, organizations should consider security services that offer a wider range of customizable encryption methods.

Cloudflare's security services, which are available as part of our China Network, offer no-latency DDoS mitigation and a quick-updating WAF that draws from global threat intelligence. Jump to the next section of this paper to learn more.

How Cloudflare supports global websites operating in China

Cloudflare operates a network of data centers spanning 200 global cities in 100 countries. Each of these data centers can perform a wide range of security, performance, and reliability services, including content delivery, DNS resolution, DDoS mitigation, WAF enforcement, serverless code execution, and much more. Since each of these services operates in every single data center, they can function very close to end-users — helping to reduce latency, and giving our network a detailed, up-to-date view of the latest threats and network conditions. What's more, organizations can manage all of these services from a single dashboard.

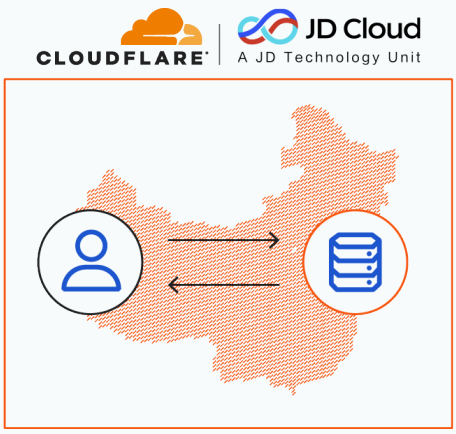
Cloudflare has helped organizations deliver a secure, fast, and reliable Internet experience for China-based visitors since 2015. In order to further improve those services, we recently launched a partnership with JD Cloud, the cloud and intelligent technology business unit of Chinese Internet giant JD.com. Through this partnership, we provide a dedicated network in mainland China that will ultimately grow to 150 data centers by the end of 2023.

Here is how this network will help organizations overcome the challenges covered in the previous section.

How Cloudflare helps overcome latency

Cloudflare and JD Cloud's network in China offers:

- **Caching and serving of static content from many data centers inside China**, delivering lower latency and faster page load times — no matter where end-users are located. Our network is closely interconnected with all Chinese ISPs, reducing the number of network hops traffic must take.



Cached content is sent between visitor in China and data center inside of China

- **Optional DNS resolution inside China**, again resulting in faster response times.
- The ability to **use Internet Protocol version 6** (IPv6), which enables efficient routing and packet processing.
- The ability to **minimize website code** through our Auto Minify feature, which can be easily activated by checking a box in the Cloudflare dashboard.
- **Serverless computing** through the Cloudflare Workers service, which operates in every data center in our China network. It allows you to respond to certain requests in customizable ways, augment existing applications. And even create entirely new ones without configuring or maintaining infrastructure.

How Cloudflare helps handle persistent domestic cyberattacks

The security services integrated into our China network allow organizations to:

- **Mitigate DDoS attacks.** Every one of our data centers in China can mitigate attacks, giving the network an immense capacity to absorb the largest attacks without losing legitimate requests — and without relying on Cloudflare data centers elsewhere in the world. Since traffic inspection happens close to end-users, their requests are spared the lengthy process of being backhauled to a potentially distant 'scrubbing center.' And due to the networking challenges in China, Cloudflare provides unique automated traffic engineering capabilities that allows for automatic rerouting of attack traffic. All of these features prevent performance penalties for legitimate traffic inside and outside of China.
- **Protect web application vulnerabilities** with the Cloudflare WAF. In addition to stopping the OWASP Top 10 application threats, the WAF draws on a continuous flow of threat intelligence from across our network to automatically stop the latest threats. In addition, organizations can easily create their own rules — and propagate them across the entire network in minutes.
- **Encrypt data using TLS 1.2**, and easily manage their own certifications from the Cloudflare dashboard.

LEARN MORE

As China's Internet economy continues to grow, new security and performance challenges will inevitably emerge. Cloudflare's plans for ongoing growth in China positions companies on our network to respond quickly to those challenges and continue raising the bar for seamless user experiences.

To learn more about the Cloudflare China Network, visit cloudflare.com/network/china/ or connect with your Cloudflare representative.

© 2020 Cloudflare Inc. All rights reserved. The Cloudflare logo is a trademark of Cloudflare. All other company and product names may be trademarks of the respective companies with which they are associated.