

Cloudflare for Public Sector

Cloudflare offers governments and public health and educational institutions a global, highly resilient cloud network with built-in security and performance capabilities.

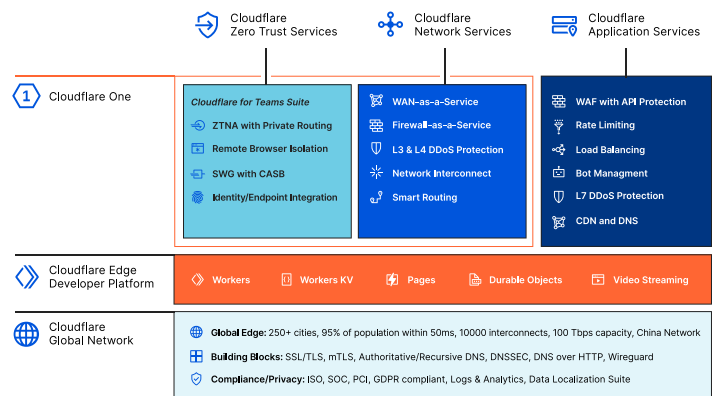
Government agencies, public schools and public health networks have seen a dramatic increase in traffic to their websites during the pandemic and an increase in cyber attacks. At the same time, many employees and contractors have had to work from home, putting a strain on the IT systems, presenting new security risks. The existing legacy infrastructure proved to be brittle and complex, so many agencies and public organizations turned to the Internet and the cloud, but required the security and reliability and the control of a private data center.

Cloudflare's solutions make the Internet more secure, faster and more reliable and can work with hybrid or multi-cloud environments. Our solutions solve complex networking and security challenges, but hide complexity from the end-users. Because they are easy to deploy and to manage, our solutions save time and have a low total cost of ownership. From one dashboard, our customers can customize and analyze the security and performance of their website and network. We have built security into every component of the network. Cloudflare's 100 Tbps network blocks an average of 57 billion threats per day, including some of the largest DDoS attacks ever recorded. Each and every login, request, and response that goes through our network strengthens the machine learning that we apply to detect and block threats at the edge, before they ever reach your organization.

Cloudflare has several public/private partnership initiatives:

1. Project Fair Shot provides Cloudflare's new Waiting Room service for free for any government, municipality, hospital, pharmacy, or other organization responsible for distributing COVID-19 vaccines.
2. The Athenian project, which provides free security and performance for state and local election websites.
3. Project Galileo, providing free security for organizations working in human rights, civil society, journalism, or democracy.

An Integrated, Global Cloud Edge Network



“There is only so much you can plan and test in terms of preparedness on the security side and after implementing Cloudflare and many other security precautions, we felt confident we had a security platform in place where we could adjust and respond to threats and high demand in real-time.”

Stacey Mahaney, Chief Information Officer,
Missouri Secretary of State

Why do public sector organizations choose Cloudflare?

Provide a secure online experience

Public sector end-users want online experiences that are fast and they can trust. Cloudflare's comprehensive security services provide in-depth protection, without impacting performance.

Secure remote workforce

Provide secure access to internal applications for any user — regardless of device or location — with seamless authentication at the network edge.

Mitigate DDoS Attacks

Public sector websites and networks can be attacked for a variety of reasons. Cloudflare's network can handle the largest DDoS attacks, and mitigates close to the attack source for faster response times.

Protect employees' Internet

Keep users and data safe from known and unknown threats on the Internet.

Lower TCO and increase agility

Get operational agility with reduced capital expenditure. Replace on-premise hardware with network and security functions delivered and billed as a service.

Protect network infrastructure

Stop attacks on on-premise infrastructure and hybrid cloud deployments, giving them consistent uptime and fast performance.

“With Cloudflare Waiting Room, we can see everything fill up over time, but it happens at a pace that's manageable. To be able to breathe a little bit and watch the numbers, watch the registrations happen, watch all the slots fill up, it's really great.”



Tyler Penney

**Web services administrator,
County of San Luis Obispo**

Why Cloudflare?

Network scale

Cloudflare sits in front of millions of internet properties, with points-of-presence in 250+ cities, in more than 100 countries. Every point-of-presence runs every Cloudflare service, which means we can mitigate attacks faster, without the need to backhaul traffic to a central location.

Shared Intelligence

All nodes in Cloudflare's network gather insights about the traffic patterns and share them with all the other nodes. This allows our products to make better decisions, whether it's our firewall, smart routing, bot management or DDoS mitigation.

Ease of use

In a world of limited resources, Cloudflare's integrated security stack and intuitive management interface make it easy to configure, deploy and maintain a defense-in-depth strategy. We protect any environment, or configuration, from on premises, to cloud-based or hybrid.