



The EU Digital Networks Act

April 2026



Cloudflare's connectivity cloud

Connect.Protect.Build

SASE & Workspace Security

- ZTNA (with MCP Server Portals)
- SWG (with AI Usage Controls)
- CASB (with AI Posture Management)
- Email Security
- Data Loss Prevention
- Remote Browser Isolation
- Digital Experience Monitoring

App Security & Perf Services

- AI Security for Apps
- Bot Management (with AI Crawl Control)
- WAF with Rate Limiting
- API Protection
- Load Balancing
- L7 DDoS Protection
- CDN and DNS
- Origin Shield

Developer Services

- AI inference
- AI Gateway
- Agentic SDK and Workflows
- Serverless compute
- Full stack applications
- Object & key-value storage
- SQL database
- Media optimization and delivery

Network Services

Network-as-a-Service Firewall-as-a-Service L3 & L4 DDoS Protection Network Interconnect Smart Routing IDS/IPS

Cloudflare Programmable Global Network

Artificial Intelligence/Machine Learning


Threat, Network Intelligence

Cloudflare operates a global network

500Tbps
of network capacity (and growing)

215 billion
cyber threats blocked every day (Q4 2025)

 **330+** cities
in 125+ countries

 **w/210+** cities
for AI inference powered by GPUs

 **40+ PoPs**
in Europe

 **13,000**
directly connected networks

 **~349**
connections at Internet Exchanges



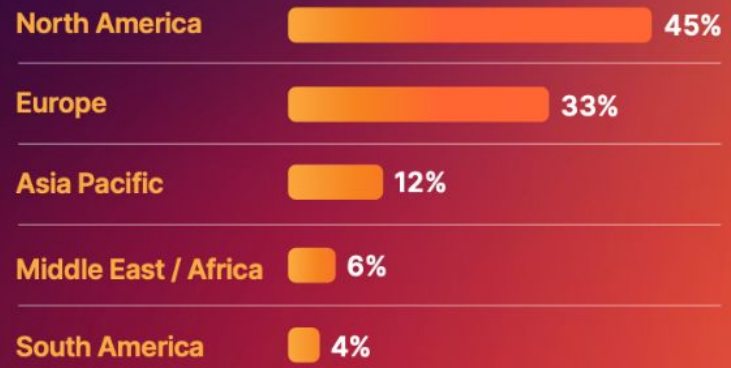
Project Galileo

EST. 2014

3,000+ Internet properties | **120+** countries | **57** partners to help identify at-risk sites

325.2 million average number of daily attacks Cloudflare mitigates for participants | **9.9 billion** average number of monthly attacks Cloudflare mitigates for participants

Project Galileo participants by country



Learn more and apply at cloudflare.com/galileo.

Human rights defenders, journalists, and humanitarian organizations are often vulnerable to cyberattacks. In collaboration with 57 civil society partners, Cloudflare protects public interest groups from attacks intended to silence them online.

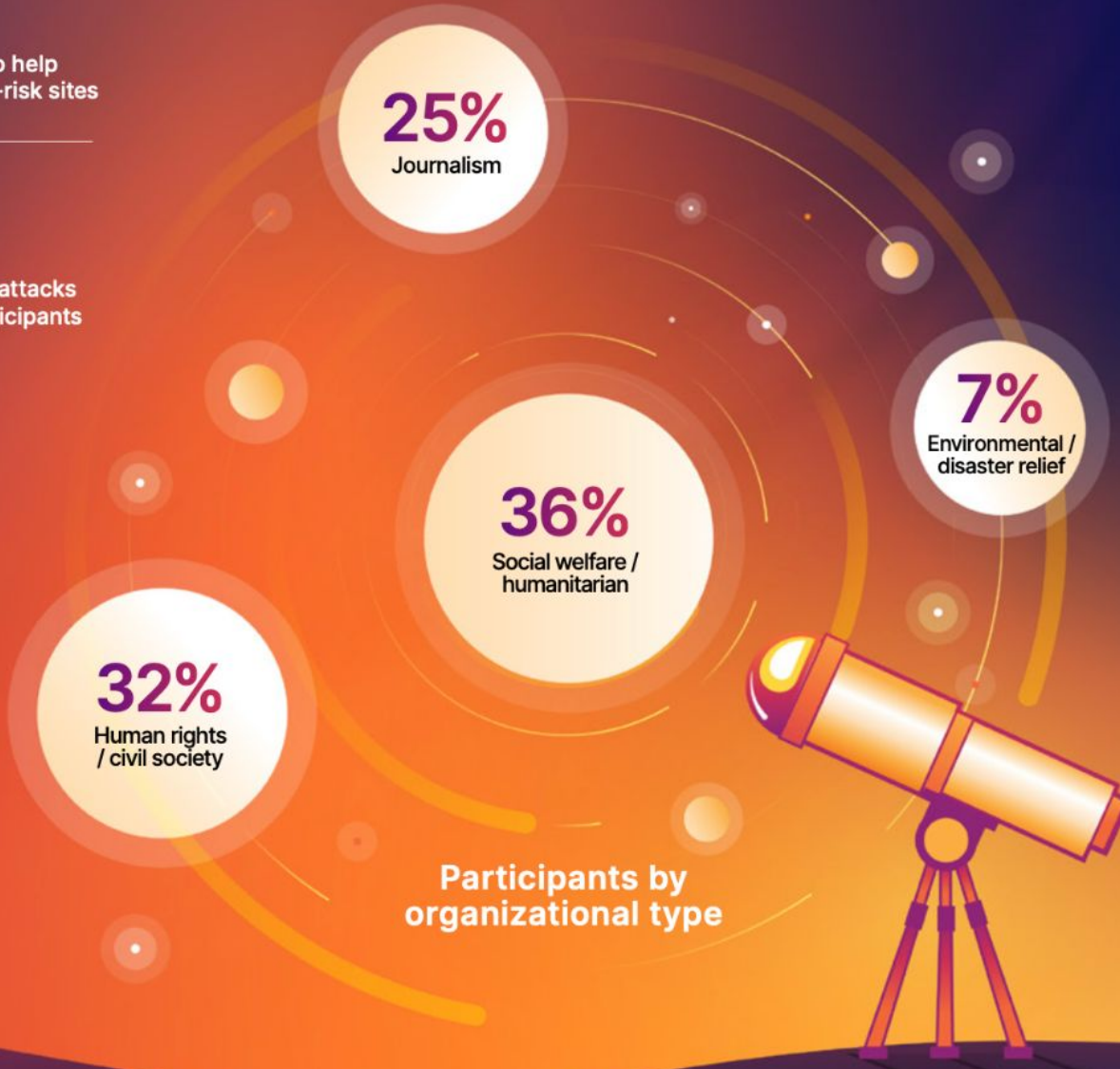
Services available for free through Project Galileo include:

Application services

- Bot management **NEW!**
- AI crawl control **NEW!**
- DDoS mitigation
- DNS and advanced SSL/TLS
- Content delivery network
- Web app and API protection

Cloudflare One: Secure access service edge

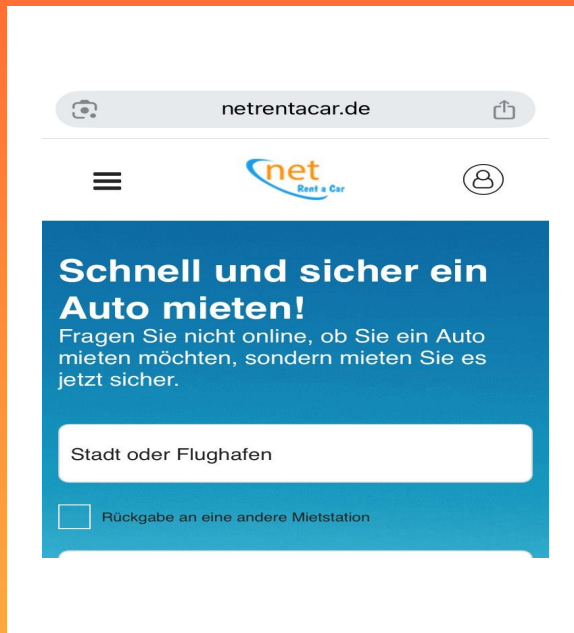
- Zero trust network access
- Secure web gateway
- Data loss prevention
- Cloud access security broker
- Email security
- Remote browser isolation



Cloudflare responds to 203 billion requests on our **free plan** every day



Car rental service



netrentacar.de

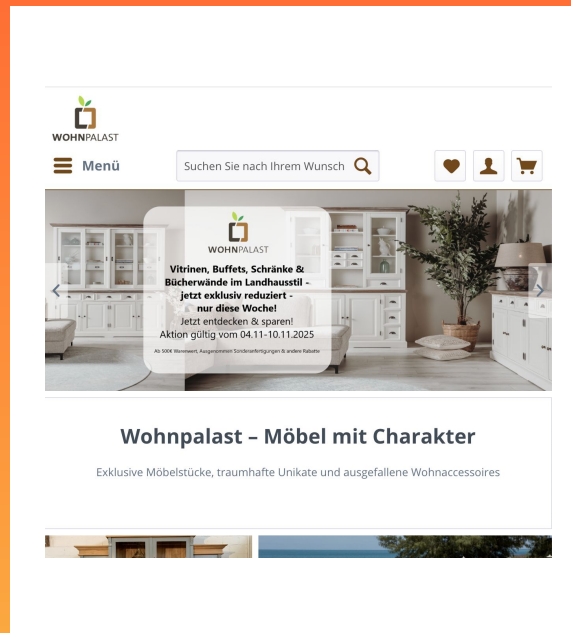
net Rent a Car

Schnell und sicher ein Auto mieten!
Fragen Sie nicht online, ob Sie ein Auto mieten möchten, sondern mieten Sie es jetzt sicher.

Stadt oder Flughafen

Rückgabe an eine andere Mietstation

Furniture store



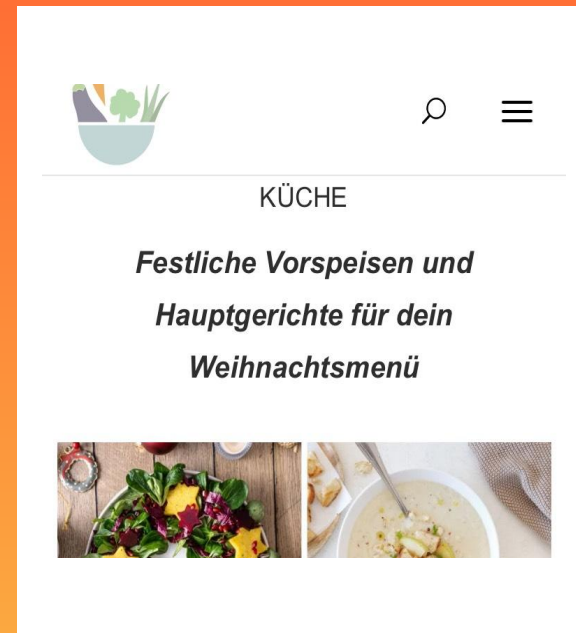
WOHNPALAST

Menü Suchen Sie nach Ihrem Wunsch

Vitrinen, Buffets, Schränke & Bücherwände im Landhausstil - jetzt exklusiv reduziert - nur diese Woche!
Jetzt entdecken & sparen!
Aktion gültig vom 04.11.-10.11.2025


Wohnpalast - Möbel mit Charakter
Exklusive Möbelstücke, traumhafte Unikate und ausgefallene Wohnaccessoires

Recipe website

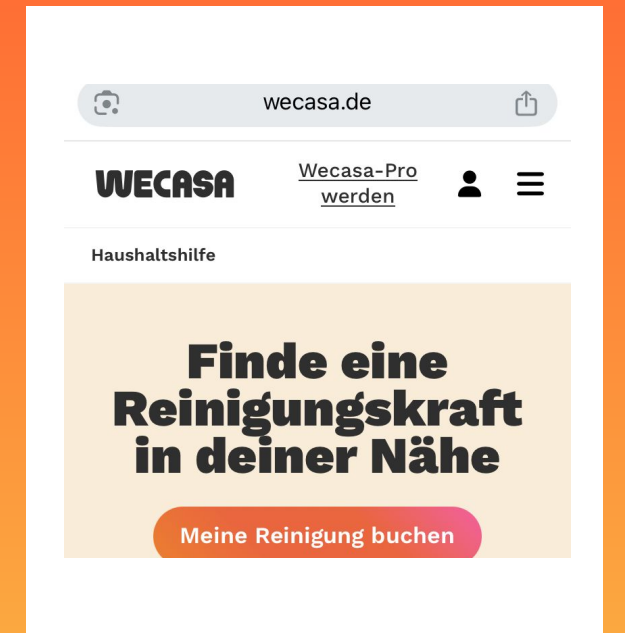


KÜCHE

Festliche Vorspeisen und Hauptgerichte für dein Weihnachtsmenü



Cleaning service



wecasa.de

WECASA Wecasa-Pro werden

Haushaltshilfe

Finde eine Reinigungskraft in deiner Nähe

Meine Reinigung buchen

Benefits of caching and CDNs



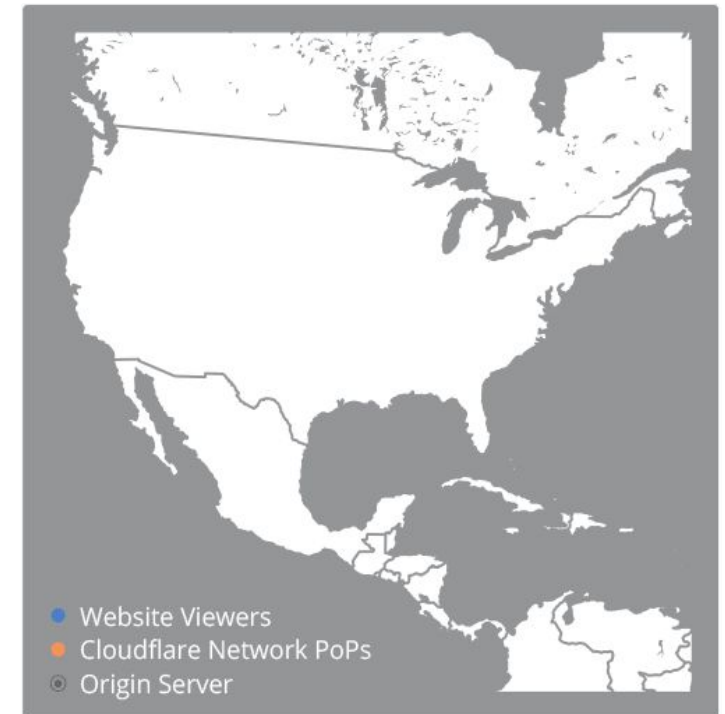
Improved **quality of experience**



Increased **network and energy efficiency**



More dynamic **competition and innovation**



These ultimately benefit the broader Internet community, including content providers, ISPs and consumers.

The proposed expansion of the DNA scope runs counter the EU's wider simplification and digital infrastructure goals



Simplification Goal

The Commission seeks to **reduce administrative burdens** and **streamline rules** for telcos to facilitate fiber and 5G rollout.



The DNA's Scope Risk

Expanding the regulatory net to CDNs and Cloud services **increases red tape**, and **compliance costs**, hindering innovation and investments in private network infrastructure.

Why CDNs and cloud networks should not be regulated like traditional telcos

A "one-size-fits-all" approach fails to recognize the **distinct technical layers** of the internet stack.

Complementary layer



CDNs sit on top of public networks to optimize performance; they **do not provide last-mile connectivity**.

Regulated elsewhere



CDNs and Cloud services already adhere to **NIS2**, the **Digital Services Act**, and the **Data Act**.

Not in line with public policy rationale



Regulating CDNs under telecom rules creates **uncertainty** and regulatory burden without improving the protection of end-users.

Economic impact



Regulating private networks **disincentivizes investments** in local infrastructure and the **provision of low cost/free services**.

Preserving IP interconnection and resilience

99%

of Internet traffic exchange relies on settlement-free peering.

The "Backdoor" Network Fee Threat

Proposed "voluntary conciliation" mechanisms (Art. 192) create a regulatory wedge between partners. They risk forcing CDNs and other networks to pay termination monopolies, a direct reversal of the EU's commitment against network usage fees.

Disputes remain rare, indicating that there is **no significant market failure** necessitating regulatory intervention.

Key Policy Recommendations

| Article | Recommendation |
|--|---|
| Article 9 (General Authorisation) | Clarify Scope. Explicitly state that CDNs and providers of cloud services fall outside the scope of General Authorisation. |
| Articles 66, 189 (Interconnection obligations, Dispute Resolution) and related articles | Exclude Cloud/CDNs. Preventing "network fees through the backdoor" by ensuring mandatory arbitration and interconnection regulations do not apply to non-telco actors. |
| Arts. 191, 192, 193 | Delete or significantly amend. Avoid regulating commercial matters in a market where no failure exists. |

Thank you