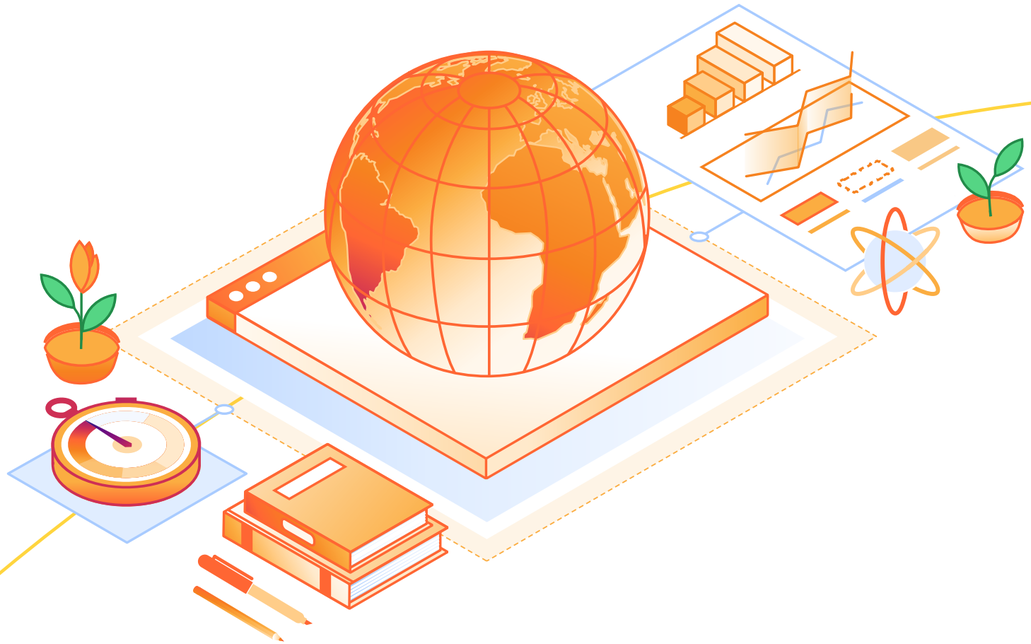
2025

CLOUDFLARE

Impact Report

Contents



Impact

Cloudflare's mission is to help build a better Internet.
Our Impact Report explains what that means and why we do it.

TIME magazine recognition

TIME100 Most Influential Companies of 2025

Cloudflare recognized as a leader in web protection and securing elections with our Athenian Project.

TIME America's Best Midsize Companies

Cloudflare recognized on 2025 list, ranked by employee satisfaction, revenue growth, and sustainability transparency.

$19 million+

in donated Cloudflare products in 2025

$83 million+

in donated products since 2017

4,000+

Internet properties under Cloudflare Impact programs

33 states

are receiving free Cloudflare services through the Athenian Project in 2025

UN Global Compact

As a signatory to the UN Global Compact, we are continually working toward the UN Ten Principles and the Sustainable Development Goals (SDGs), with annual reporting on our progress.

2025 awards and recognition

Newsweek Global Most Loved Workplaces

Newsweek America's Greatest Workplaces for Gen Z

Forbes Best Midsize Employers

Reuters Events Sustainable Business Awards

Fortune Change the World

Built In 100 Best Large Companies 2025

Other awards include:

- Fast Company Next Big Things in Tech
- Fast Company Most Innovative Companies: #3 in Enterprise
- CRN AI 100: The 20 Hottest AI Cybersecurity Companies April 2025
- CRN Cloud 100: The 20 Coolest Cloud Security Companies of 2025

New business model for the Internet

AI is changing how we access content on the Internet. Cloudflare believes this creates an opportunity to rethink how we value unique and original content online.

Search engines to answer engines

AI is changing how users access content online, making today's ad-driven model obsolete. Cloudflare data shows that, while AI models continue to scrape content, because they are designed to provide direct answers—they are much less likely to drive traffic to websites.

Learn more about AI bots and crawler activity at Cloudflare Radar.

Protecting and modernizing the Internet ecosystem

To maintain the open Internet we have today, with its wide range of different voices, website owners of all sizes need tools that enable them to participate in an AI-driven economy. AI companies not only need sustainable access to high-quality and original content, but also infrastructure and standards modernized for AI applications and agents.

Reward better content

Web traffic and clicks have never been a good measure of value. We think AI has the opportunity to reshape the economics of the Internet to reward actual knowledge creation and other high-quality, unique, and local content.

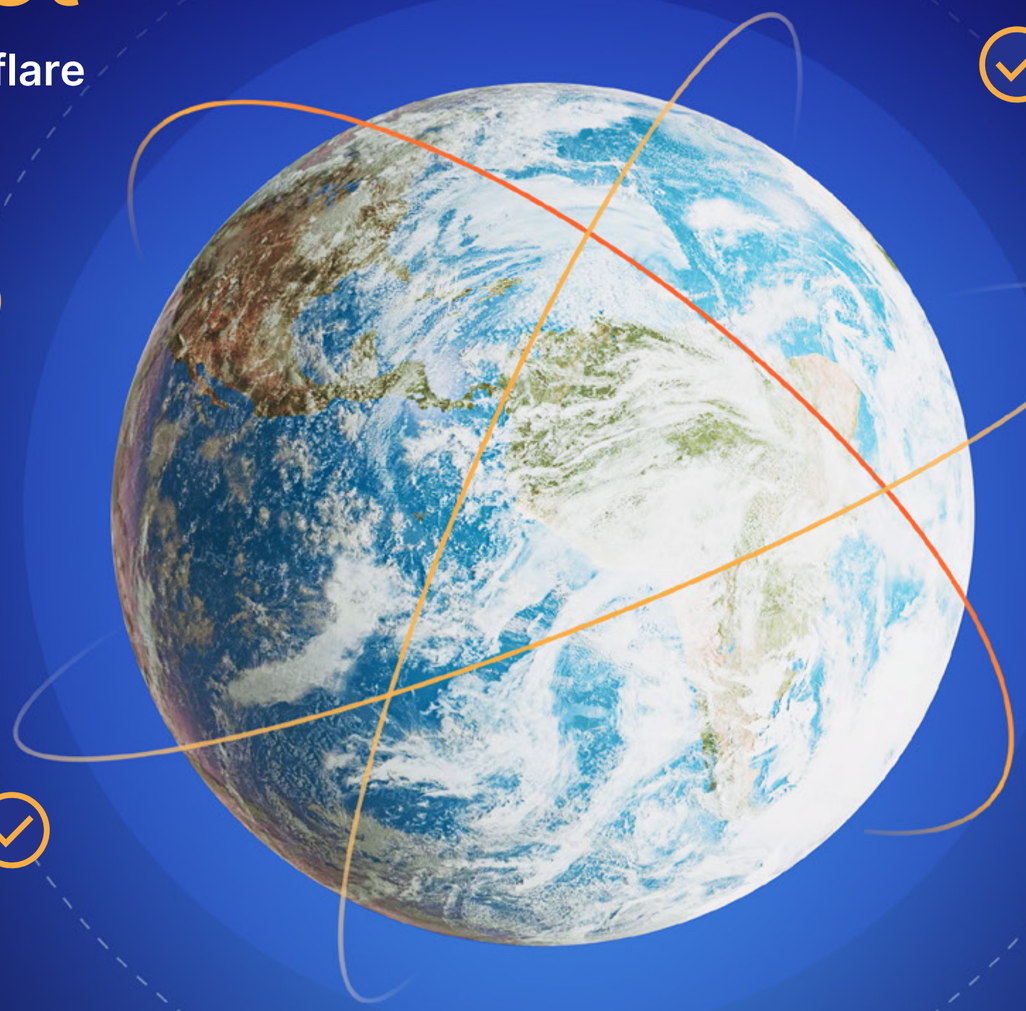
Cloudflare >> Connect 2025

TIME100 AI 2025
Matthew Prince
Co-founder and CEO, Cloudflare

We can shape the future, together.

Helping protect the open Internet

As the Internet evolves, Cloudflare remains committed to open Internet principles.



- Open standards
- Permissionless innovation
- Democratized AI access
- Unique and independent voices
- Security and privacy
- Multistakeholder governance
- Human rights

2025 SPOTLIGHT

Giving control back to creators

Cloudflare is working with the world's leading publishers, content creators, and AI companies to help build a sustainable economic model for the future of the Internet.

Creating incentives for amazing content

Earlier this year, working with leading publishers and AI companies, Cloudflare announced we would enable website operators to block AI crawlers on their site. Our goal is to help facilitate a mutually beneficial relationship between publishers and AI companies—replacing unilateral scraping with a framework to permit negotiation and mutual consent.

Visibility and control

AI Crawl Control empowers creators to work with AI companies by showing how their work is being used and setting rules to Allow, Block, or Charge crawlers based on their source or intent. We are also working with AI companies to communicate their purpose more transparently—whether it's training, inference, or search—to help build trust and efficiency across the AI web.

Allowing content owners to charge for access BETA

Establishing an open, collaborative, and standardized market that allows AI companies to pay for the content they use is essential to the future of the Internet. Cloudflare is developing a pay per crawl tool, which allows our customers to set prices and automatically collect payment from AI crawlers. We think this is one solution to help solve this problem, and look forward to working with partners across the Internet on other similar ideas.

Content Independence Day: No AI crawl without compensation!

Matthew Prince

"Almost 30 years ago, two graduate students at Stanford University—Larry Page and Sergey Brin—began working on a research project they called Backrub. That, of course, was the project that resulted in Google. But also something more: it created the business model for the web."

Read the full blog post here.

> At TIME, we're committed to advancing innovation without compromising the integrity of original journalism. Cloudflare's initiative is a meaningful step toward building a healthier AI ecosystem—one that respects the value of trusted content and supports the creators behind it."
>
> Mark Howard, Chief Operating Officer, TIME

How AI Crawl Control works

Monitor
AI crawler activity

Manage
access

Block
with a single click

Charge BETA
AI companies for access

TRUSTED BY

ADWEEK · The Arena Group · The Atlantic · Atlas Obscura · AP · BuzzFeed · Condé Nast · Dotdash meredith · dcn · Drupal | Acquia · DDC · Evolve Media · Fortune · GJ · Hard Candy · (h[s]) Hyperscience · iab. Tech Lab · Independent Media · linkup · News Media Alliance · O'Reilly · Pinterest · PMC · ProRata.ai · Quora · Raptive · SimpleFeed · sky news · Snopes · SourceForge · sourn · stackoverflow · stocktwits · Sustainable Media · Universal Media · Universal Music Group · TIME · Webflow · Ziff Davis

Birthday Week

2025 was our 15th birthday! We celebrate our birthday weeks by launching new products and initiatives that we think of as gifts back to the Internet.

15 Years

Read Cloudflare's annual Founders Letter

Look back at Birthday Week 4: Universal SSL encryption

In 2014, Cloudflare announced that we would provide Universal SSL encryption for all websites using the free version of our service. As a result, the number of websites online that supported encrypted connections doubled overnight. Today, more than 95% of the web is encrypted, and we're proud of the role we played in making that happen.

Learn more about Cloudflare's 2025 Birthday Week announcements.

Highlights from past Birthday Weeks

2011
Free automatic IPv6

2014
Universal SSL

2015
Expansion to China

2016
Dedicated SSL certificates

2017
- Unmetered DDoS protection
- Cloudflare Workers

2018
The Bandwidth Alliance

2019
WARP available to all

2020
- Free, privacy-first analytics
- Cloudflare Radar

2021
- Email security DNS wizard
- Cloudflare Email Routing
- Cloudflare R2 object storage with zero egress fees

2022
- Unmetered rate limiting
- Post-quantum upgrades for Cloudflare Tunnel

2023
- Workers AI
- Encrypted Client Hello

2024
AI audit and control

Sustainability

Sustainability is part of Cloudflare's mission, business, and culture.

Removing and offsetting historic emissions

Cloudflare is proud to report that we have completed our commitment to offset or remove emissions associated with powering our network from our launch until our first renewable energy purchase in 2018. In partnership with 3Degrees, we have invested in verified sustainability projects totaling approximately 31,000 metric tons of carbon dioxide equivalent (C02e). This multi-year project was a company-wide collaboration, uniting our Engineering, Infrastructure, Finance, Legal, and Impact teams. It represents our commitment to accountability and to building a more sustainable Internet.

Cloudflare contributed to the following projects:

- Pacajai REDD+ Project, Brazil
- Boone Forestry Improved Forest Management Project, Kentucky, US
- BioLite Improved Stove Programme I, Uganda
- BioLite Improved Stove Programme II, Uganda
- Clinton Landfill Gas Collection and Combustion Project, Illinois, US

Climate-related financial risk disclosures NEW!

In 2015, the G20 Finance Ministers and Central Bank Governors asked the Financial Stability Board (FSB) to develop disclosure recommendations to help financial markets and investors better understand financial risks associated with climate change. The FSB established the Task Force on Climate-Related Financial Disclosures (TCFD), which later published the TCFD framework that has become one of the benchmarks in global climate reporting. Earlier this year, Cloudflare partnered with Shift Advantage to conduct a company-wide analysis of our potential transition and physical risks under various climate scenarios. Using those findings, Cloudflare is publishing its first climate-related financial risk disclosures, which are available in the Appendix section of this report.

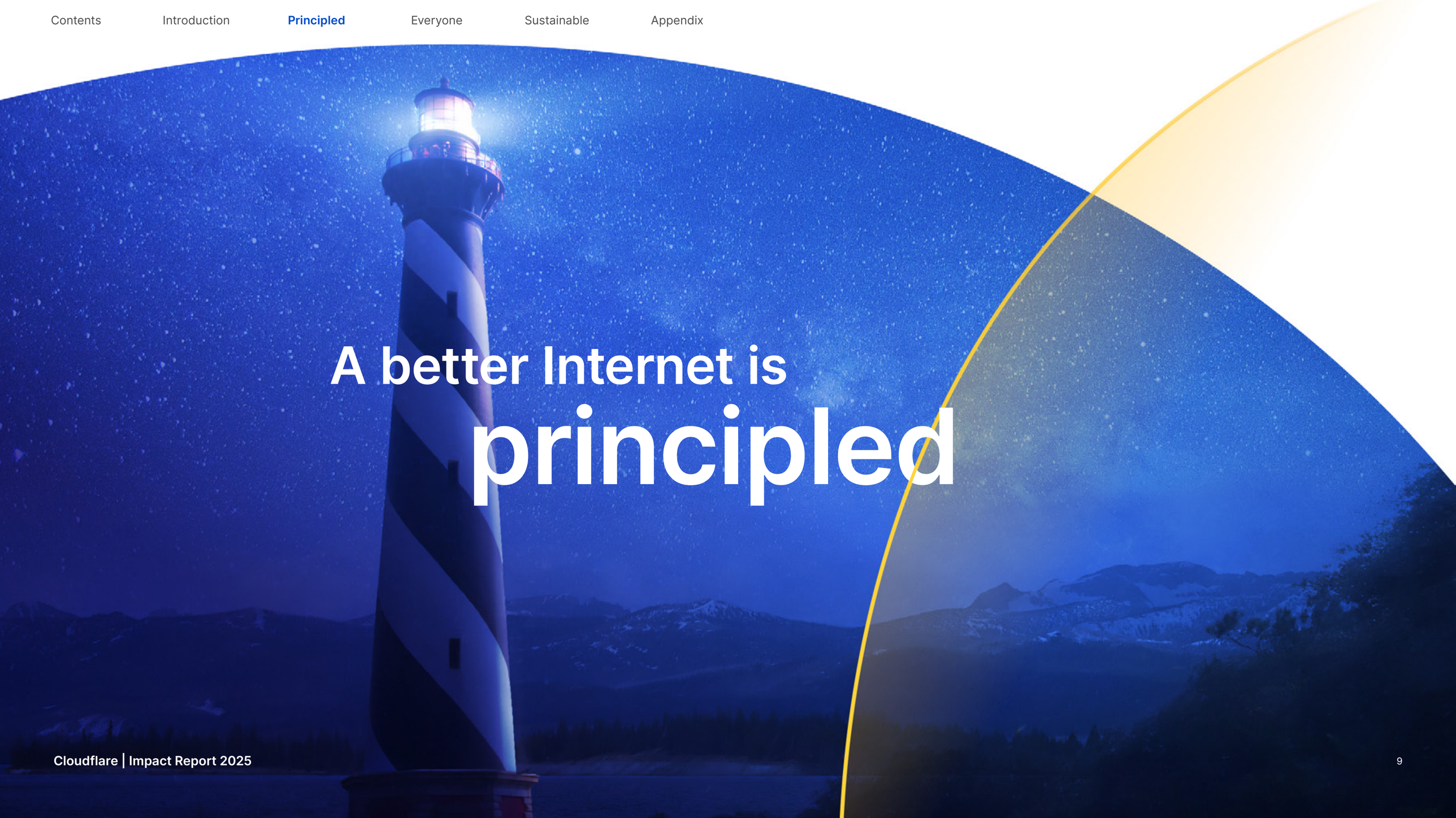
Our sustainability commitments

In 2025, Cloudflare achieved its commitment to offsetting or removing historical emissions associated with powering our network.

Cloudflare powers its operations with 100% renewable energy.

Cloudflare is committed to publishing its company-wide emissions on an annual basis.

Cloudflare has committed to setting near-term company-wide emissions reduction targets in line with climate science with the Science Based Targets initiative (SBTi).



A better Internet is principled

Project Galileo

EST. 2014

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

3,000+ Internet properties

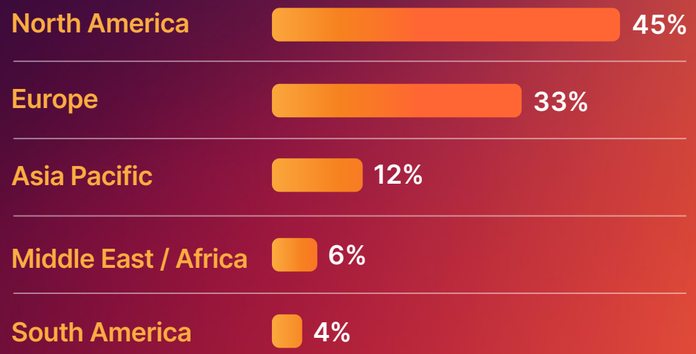
120+ countries

57 partners to help identify at-risk sites

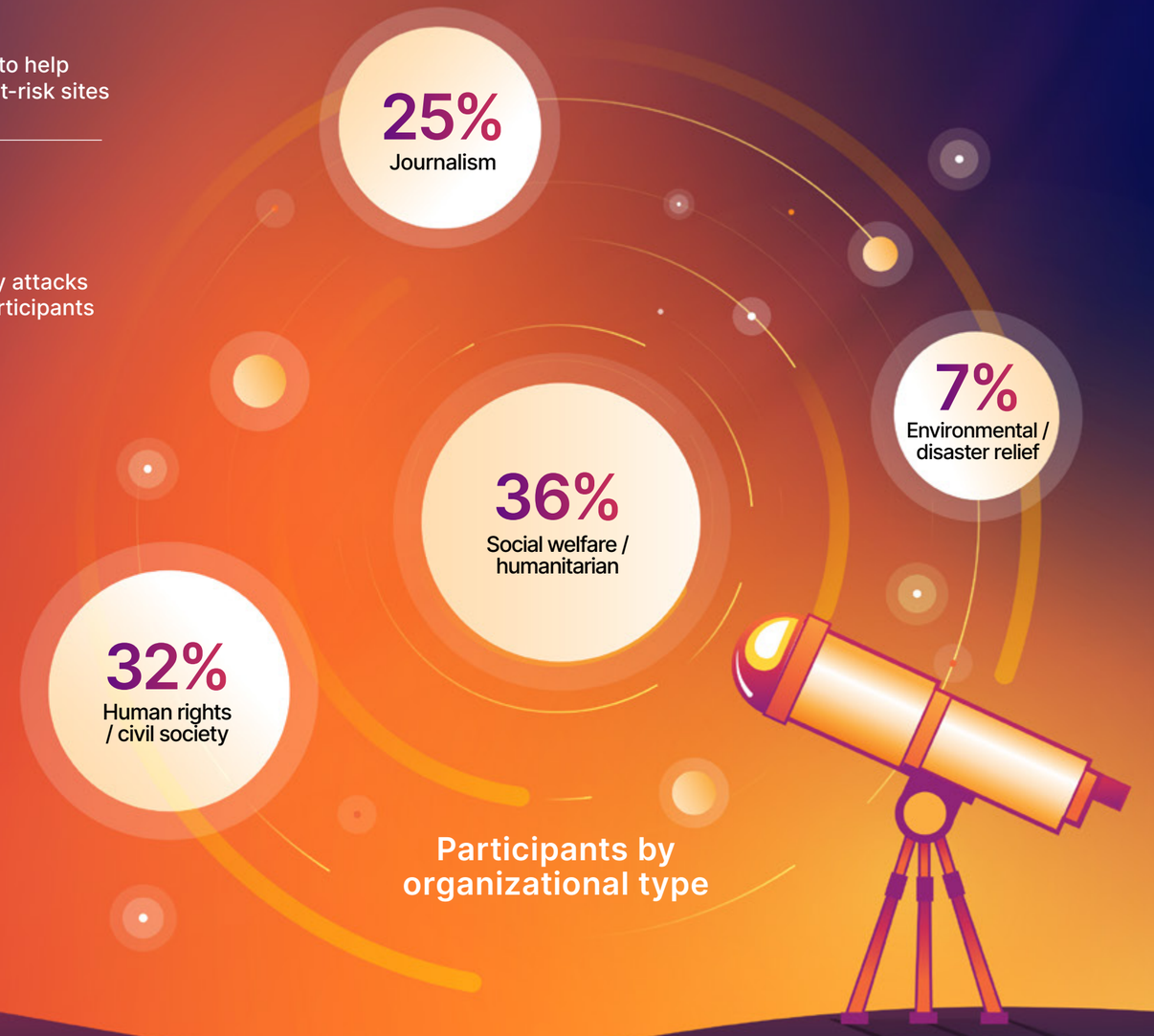
325.2 million average number of daily attacks Cloudflare mitigates for participants

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.



Participants by organizational type

Democracy and human rights

Democracy and human rights are prerequisites for the open Internet. They help define what it should be and provide the framework to defend it.

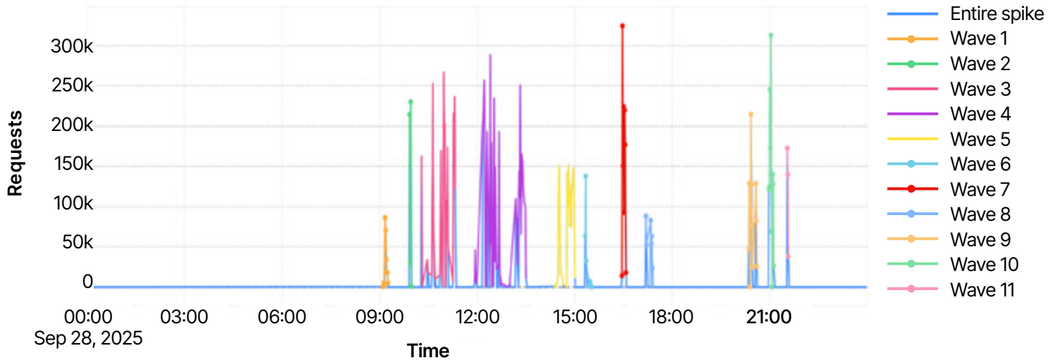
Cloudflare helps protect important voices and democratic institutions online, works with civil society to promote cybersecurity and open policies and technologies, and engages with stakeholders to apply human rights principles across our business and network.

Helping protect elections in Moldova

The Moldova Central Election Commission (CEC) is responsible for managing the election process in Moldova, including setting election dates, managing polling stations, and providing information to the public. In September, the CEC onboarded to Cloudflare through the Athenian Project shortly before the recent Moldovan parliamentary elections. Despite a significant foreign influence campaign, including persistent cyberattacks against Moldovan government institutions, Cloudflare was proud to help ensure the CEC's work serving Moldovan voters was uninterrupted.

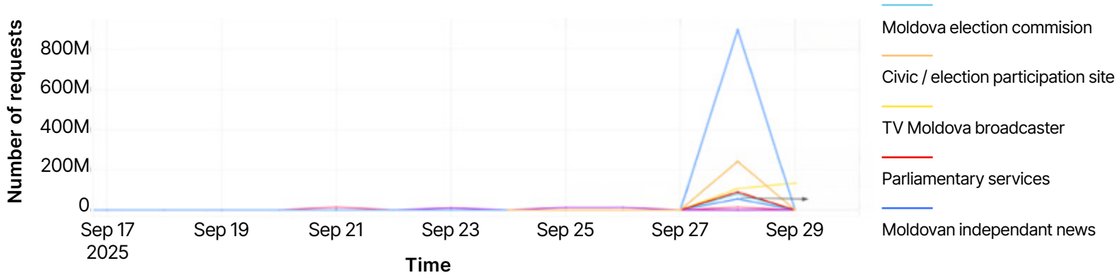
> Cloudflare's support was essential for Moldova's parliamentary elections, ensuring uninterrupted access to real-time results for citizens at home and abroad. Their resilient infrastructure allowed us to withstand heavy DDoS attacks and protect the integrity of the democratic process."
>
> Anatolie Golovco, Cybersecurity and Digital Transformation Expert in the Office of the Prime Minister of Moldova

Detected attack waves for cec.md spike



Top mitigated zones: DDoS mitigated requests

17-09-2025 to 29-09-2025 (UTC)



Email security now available in Cloudflare for Campaigns NEW!

Phishing attacks are a significant cybersecurity threat to political campaigns, causing data breaches, leaks, and misinformation. In 2020, we launched Cloudflare for Campaigns to provide free cybersecurity services to political campaigns and parties in the United States. Working with partners at Defending Digital Campaigns (DDC), Cloudflare announced earlier this year that it would also make Email Security services available for free to organizations participating in the more than 60 US political campaigns and other organizations participating in Cloudflare for Campaigns.

> DDC is thrilled that Cloudflare is expanding their product offerings to campaigns with the addition of Email Security. This new offering further exemplifies Cloudflare's extraordinary and generous commitment to protecting campaigns."
>
> Michael Kaiser, President and CEO of Defending Digital Campaigns

DEMOCRACY AND HUMAN RIGHTS

Free tools to protect local news from AI crawlers with Project Galileo

Media organizations are facing significant challenges in transitioning to the AI-driven web, particularly local news. As users increasingly turn to AI models for information, less of their web traffic is visiting actual news sites. Less traffic often means less advertising, fewer subscriptions, and lost revenue.

Cloudflare recently announced that Project Galileo will now include access to Bot Management and AI Crawl Control. These services will help participants, including 750 journalists, independent news organizations, and other nonprofits supporting news-gathering around the world, protect their websites from AI crawlers—for free.

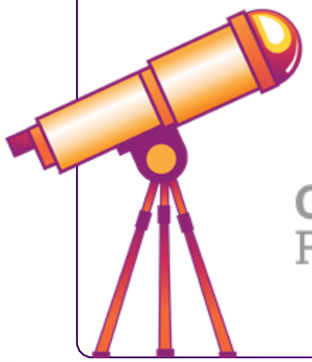
> In an era defined by AI and digital disruption, providing robust tools to independent media isn't just support—it's a lifeline."
>
> Meera Selva, CEO of Internews Europe

> Independent media's ability to fulfill its democratic function by gathering news and distributing trusted information depends on generating revenues free from political or business influence. By monitoring and monetizing the crawling of publishers' sites, media can protect their intellectual property while developing new revenue streams to support their quality journalism."
>
> Ryan Powell, Head of Innovation and Media Business at the International Press Institute

Welcoming new partners to Project Galileo

Partner organizations are responsible for reviewing and approving applications by organizations interested in joining Project Galileo. Cloudflare is proud to now work with 57 of the leading nonprofit organizations around the world to help make free cybersecurity services available to organizations in need.

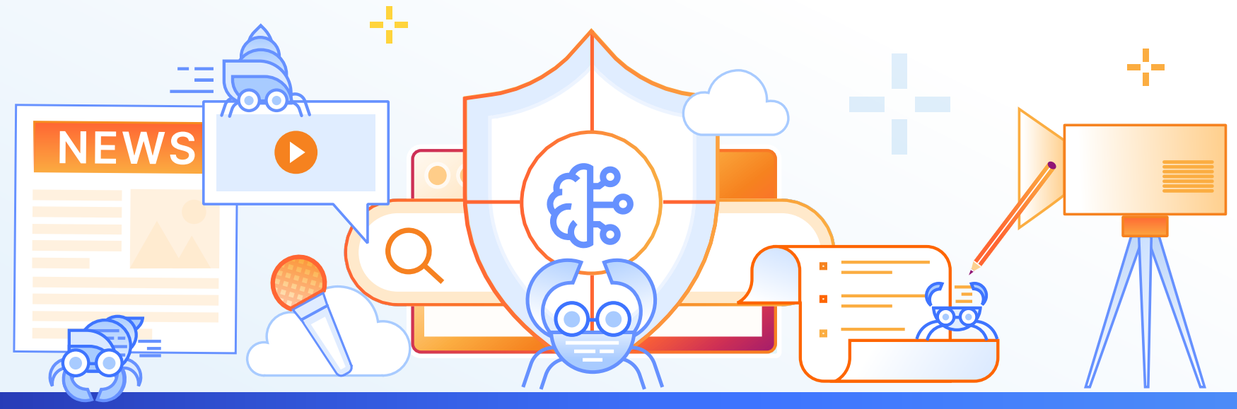
In 2025, Cloudflare welcomed three new partners to the program: EngageMedia, the Open Culture Foundation, and the NGO Information Sharing and Analysis Center (NGO-ISAC).



OpenCulture Foundation_

NGO-ISAC BETTER TOGETHER

EngageMedia



DEMOCRACY AND HUMAN RIGHTS

IN FOCUS

Cyberattacks on civil society

Cloudflare publishes annual data regarding cyberattacks detected against organizations protected under Project Galileo. Our goal is to help policy makers, researchers, and the public understand the challenges these organizations face in operating online and serving their communities.

↑240% increase

Cloudflare saw a 240% increase in attacks on organizations protected under Project Galileo in 2025.

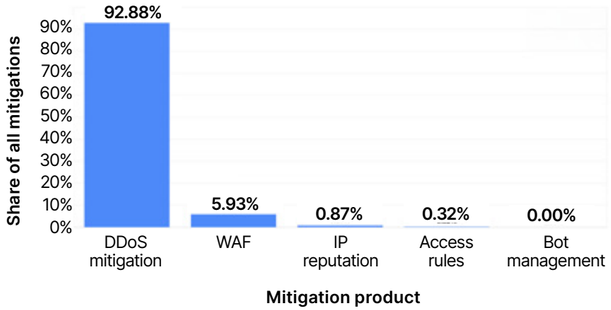
Project Galileo participants include organizations focusing on journalism, human rights, protecting the environment, education, humanitarian relief, and more from over 120 countries. Because participants vary in geographic distribution, mission, size, and structure, Cloudflare data regarding cyberattacks can offer useful insight into the cybersecurity environment facing nonprofit organizations generally.

2025 spotlight: Journalism

Journalists and news organizations experienced the highest volume of cyberattacks of any group protected under Project Galileo. Overall, Cloudflare mitigated an average of 352.2 million attacks per day on all program participants, with 290 million of those targeting independent news and media organizations. Attacks against journalists are also increasing in intensity. For example, in 2024, daily traffic spikes never crossed 4 billion requests. In 2025, however, Cloudflare detected a multi-day event where traffic peaked at nearly five times that volume.

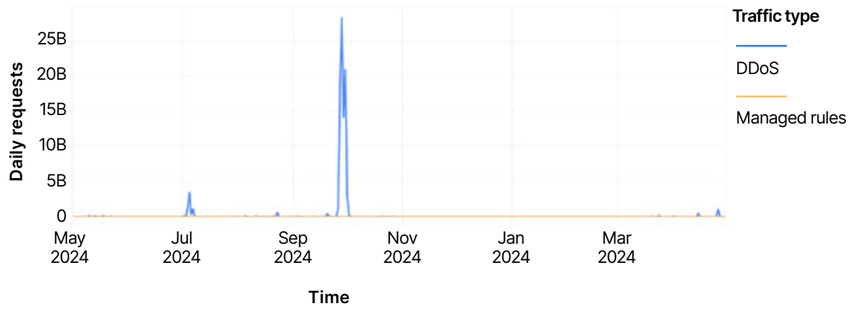
Journalism

Mitigated traffic broken down by product group



Journalism

Mitigated traffic over time

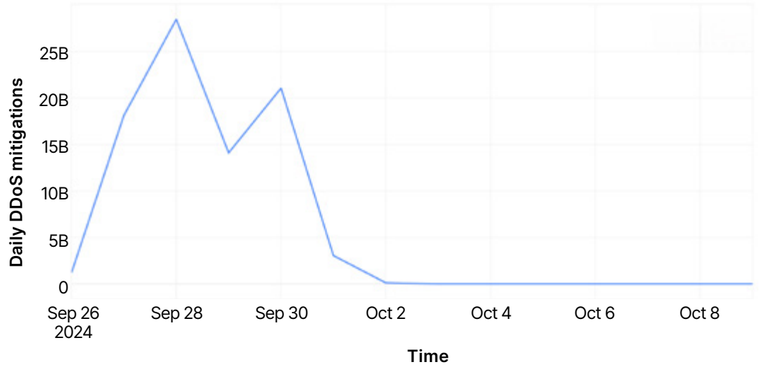


Case study: Belarusian Investigative Center

The Belarusian Investigative Center (BIC) is an independent nonprofit newsroom dedicated to exposing corruption and debunking disinformation from authoritarian regimes, primarily in Belarus and Russia. On September 27, 2024, the organization experienced a cyberattack and applied for Project Galileo.

The following day, the organization experienced a significant cyberattack generating over 27 billion requests per second. “Cloudflare’s team responded to our application within 24 hours … That fast reaction was crucial. Once we onboarded, the DDoS attacks immediately stopped,” said Wladyslaw, IT manager for the Belarusian Investigative Center.

DDoS traffic to investigatebel.org



DEMOCRACY AND HUMAN RIGHTS

IN FOCUS

Cyberattacks on civil society

Project Galileo participants in their own words

"Cybersecurity tools for us mean the difference between being able to save wildlife lives and not. It's that simple."

Founder, 5W Foundation

"Our mission is to make environmental data and science accessible so people can take meaningful action for the planet."

Jackie Gallagher, Director, Greenpeace Canada Education Fund

"As a solely volunteer-driven organization ... we do not have 100-gigabit routing equipment, big WAF appliances, multiple points of presence, or other techniques to help with large-scale attacks."

Systems Chair, Organization for Transformative Works

"We just didn't have the resources to pay for high-end protection, and that's when we found Project Galileo."

Belmar Santanilla Gutiérrez, Webmaster and IT lead at InSight Crime

"Our members have been jailed, beaten, poisoned, and our friends have been murdered. In addition, there have also been active digital campaigns and narratives aimed against us."

Nadya Tolokonnikova, Founder, Pussy Riot

"Without Cloudflare's protection, our website and app would be vulnerable to attacks, potentially impeding our ability to provide timely and reliable information to those who need it most and hindering our efforts to solve urgent cases via the helpline, especially those relating to journalists, activists, and women facing gender-based violence."

Aws Al-Saadi, President and Founder, Tech4Peace

"Joining Project Galileo was critical, our websites were frequently attacked, and we lacked the resources to defend ourselves effectively."

Edita Šmaković, Multimedia Coordinator, Youth Initiative for Human Rights in Serbia

"Without [Project Galileo], we wouldn't be able to afford the tools it provides and we would struggle to hang on."

Daryl Cagle, Founder, Cagle Cartoons

"I'm a doctor, not a cybersecurity expert."

Alexandre Wettstein, Founder and Medical Coordinator, Fair Future Foundation

"Cloudflare is just such a wonderful security product that we wouldn't be able to take advantage of at the cost."

Kat Kimmons, Director of Technology, Immigrant Legal Resource Center (ILRC)

"We continue to amplify voices that authoritarian regimes would rather silence."

John Caldwell, Manager and Digital Security Specialist, Pussy Riot

DEMOCRACY AND HUMAN RIGHTS

Independent assessment of Cloudflare operations

The Global Network Initiative (GNI) is a nonprofit organization launched in 2008. GNI members include Information and Communications Technology (ICT) companies, civil society organizations (including human rights and press freedom groups), academic experts, and investors from around the world. Its mission is to protect and advance freedom of expression and privacy rights in the ICT sector by setting a global standard for responsible decision making and serving as a multistakeholder voice in the face of government restrictions and demands.

Companies that participate in GNI are required to be independently assessed every two to three years to determine if they are making a good faith effort to implement the GNI Principles. The GNI Assessment evaluates company policies and processes around governance, due diligence and risk management, privacy and freedom of expression, and transparency. Cloudflare completed its second GNI Assessment in 2025 and its first that included an independent auditor. Cloudflare will release a public summary of those results following the GNI Board's review in early 2026.

Evaluating the impact of our services

Human rights impact assessments are intended to help companies understand, assess, and address potential human rights impacts caused by their operations. In 2025, Cloudflare hired Article One, a strategy and management consultancy with expertise in human rights and responsible technology, to conduct the company's first independent human rights assessment of its services. Specifically, Cloudflare asked Article One to evaluate its free service offerings and the company's management of those services.

Cloudflare is committed to respecting human rights under the UN Guiding Principles on Business and Human Rights, and implementing the GNI Principles.

Learn more about Cloudflare's human rights commitments and work

- Cloudflare Human Rights Policy
- Privacy and data protection
- Our approach to abuse
- Applying human rights frameworks to our approach to abuse
- Our approach to law enforcement
- Cloudflare Transparency Report
- Reporting abuse
- Third Party Code of Conduct

Athenian Project

EST. 2017

We created the Athenian Project to provide state and local governments with the highest level of cybersecurity protection and reliability for their election websites at no cost. This ensures constituents can securely access election information and register to vote.

Services available for free through Athenian Project include:

- **DDoS attack mitigation**
- **Malicious bot mitigation**
- **Web application firewall (WAF)**
- **Content delivery network (CDN)**
- **Rate limiting**
- **Zero trust and secure access service edge (SASE) tools**
- **And many others!**

Learn more and apply at cloudflare.com/athenian.

Election security at a glance

441+
Internet properties protected

7
countries

33 US states
receive free Cloudflare services through the Athenian Project

200 million
DDoS attacks blocked between September and November 2024, an average of about 3.9 million threats per day to state and local governments running elections in the United States.

> As the official election authority for Onslow County, we understand that our website is a critical source for accurate and timely election information. Protecting the integrity and availability of that information is essential to maintaining public trust. Through Cloudflare's Athenian Project, we receive enterprise-grade security and resiliency at no cost to Onslow County taxpayers. This support allows us to safeguard our election infrastructure while ensuring that citizens have reliable access to trusted election data."
>
> **Ted Norris, Deputy IT Director at Onslow County, North Carolina**

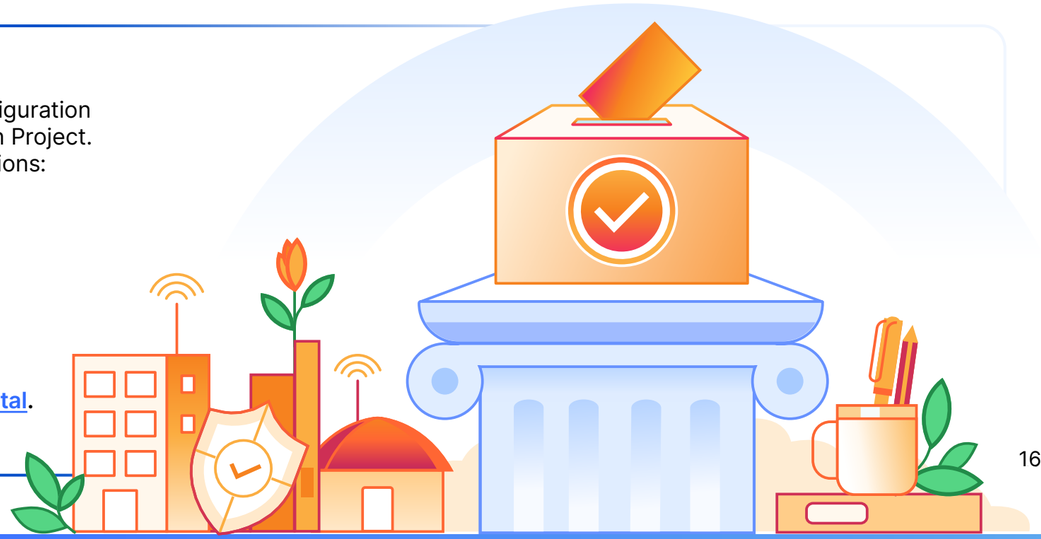
> Cloudflare's Athenian Project was an easy choice to securely deliver our official election information. Their support was absolutely essential, making sure all our residents from Rock Island County to folks serving overseas have seamless, uninterrupted access to real-time election results. We saw the attempts to disrupt things, but their robust network allowed us to shrug off some pretty serious traffic spikes and DDoS attacks, completely safeguarding the transparency and integrity of our vote count."
>
> **Kurt Davis, Director of Information Technology at Rock Island County, Illinois**

Cloudflare Election Security Guide

Each election cycle, Cloudflare provides up-to-date security configuration recommendations to election entities participating in the Athenian Project. Here are some of our most frequent and important recommendations:

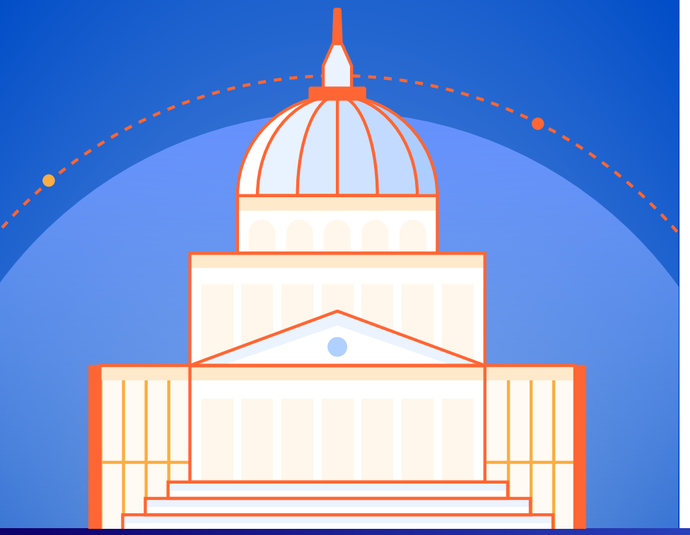
- Protect accounts with two-factor authentication (2FA)
- Enable SSL encryption
- Deploy a web application firewall (WAF)
- Deploy DDoS mitigation services
- Obscure origin IP address

For more information, visit Cloudflare Social Impact Projects Portal.



Working together

The Internet is best when it is collaborative. We work with public sector agencies, non-governmental institutions, developers, hackers, and the public to improve security online and advance our mission.



Working with Giga to increase capacity for measuring online school connectivity

Giga was launched in 2019 by the Broadband Commission for Sustainable Development, UNICEF, and the International Telecommunication Union (ITU) with a goal of connecting every school on the planet to the Internet. Giga Maps is an online tool that allows governments to geolocate schools, measure their real-time connectivity status, and identify the most effective connectivity solutions. Earlier this year, Cloudflare and Giga announced a new partnership that will provide free access to Cloudflare's Speed Test tool to help the Giga team provide more accurate, real-time assessments of Internet connectivity at schools around the world.

> "The potential of this partnership is nothing short of exciting."
>
> Thomas Davin, Global Director, UNICEF Office of Innovation
>
> unicef

Public-private partnerships

The National Cybersecurity Center of Excellence (NCCoE) is a program operated by the National Institute of Standards and Technology (NIST) that serves as a crucial hub for the private sector, government, and academia to address the most pressing cybersecurity challenges. Cloudflare is a core collaborator on three high-priority NCCoE projects: migrating to Post-Quantum Cryptography, automation of the NIST Cryptographic Module Validation Program, and the Cyber AI Profile.

Working with the public

Bug bounty programs are used by organizations to work with the public to proactively identify security vulnerabilities in their software, websites, or networks. In exchange for reporting potential vulnerabilities to organizations directly, ethical hackers receive compensation for their time and effort. Cloudflare operates a public bug bounty program hosted by HackerOne, and a VIP bug bounty program which we launched as part of our commitment to the Secure by Design pledge in 2024.

- Cloudflare bug bounty program
- Cloudflare Public bug bounty (hosted by HackerOne)
- Cloudflare VIP Bug Bounty program
- Resolving a request smuggling vulnerability in Pingora
- QUIC action: Patching a broadcast address amplification vulnerability

Disrupting RaccoonO365

RaccoonO365 is a financially motivated criminal enterprise operating a phishing-as-a-service platform designed to enable subscribers to launch their own credential harvesting campaigns. According to Microsoft, since July 2024, RaccoonO365's kits have been used to steal at least 5,000 Microsoft credentials from 94 countries. In September 2025, in coordination with Microsoft and US law enforcement, Cloudflare executed a coordinated takedown of all identified RaccoonO365 domains, protected users from accessing compromised webpages, and terminated their accounts to prevent re-registration.

This coordinated effort was intended to permanently dismantle the group's ability to operate. Cloudflare also published a comprehensive description of the group's tactics, procedures, and assets to help protect the broader Internet community.

Learn more about RaccoonO365 and other Cloudflare security investigations here.

Privacy and data protection

Privacy allows people the space to learn, question, form opinions, and participate in democratic society. The promise of the Internet is not just access to information, but also the freedom and privacy necessary to make that access meaningful.

Cloudflare is helping make the Internet more private for everyone by building new technologies, providing free privacy-enhancing services, and subjecting ourselves to independent verification.

AI and the future of data protection

AI offers unprecedented opportunities for innovation and workplace efficiency. However, it also creates new vulnerabilities, including cyber threats and data leakage. Cloudflare is helping make AI more secure for everyone by protecting AI models from cyberattacks, providing developers with tools to control costs and prevent usage spikes, preventing employees from leaking sensitive data, and blocking malicious AI bots.

Minimizing data collection

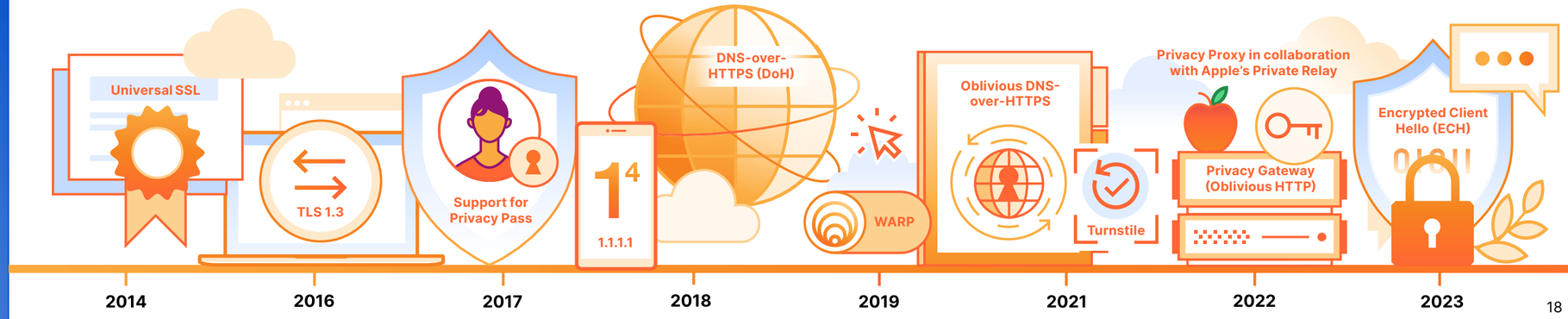
Websites rely on user data for essential functions like security and performance, but this often comes at the cost of privacy. Cloudflare has engineered anonymized alternatives to these tools.

We developed Turnstile, a CAPTCHA replacement, and helped champion the Privacy Pass standard to allow website owners to verify that a visitor is human without tracking their data or compromising their experience. Similarly, we developed a web analytics tool that provides aggregated traffic insights to site owners without tracking or profiling individual users.

> There are some companies in the room today that engage very actively on standards-setting processes. Cloudflare is one of them. They have been really quite vocal about privacy-enhancing aspects in standards-setting processes. And so, it's one of those examples where we see that business actually can commit to human rights in their standards-setting engagement."
>
> Isabel Ebert, PhD, Human Rights Officer
> Office of the United Nations High Commissioner for Human Rights
> *The impact of technical standards on human rights in the case of digital technologies WSIS+20 Forum, High-Level Event*

Learn more about our privacy work

- Universal SSL encryption
- 1.1.1.1 with WARP
- DNS-over-HTTPS (DoH)
- Oblivious DNS-over-HTTPs (ODoH)
- Privacy Gateway
- Encrypted Client Hello



PRIVACY AND DATA PROTECTION

Certifications and reports

ISO 27001:2022
Implementation of an Information Security Management System (ISMS) and security risk management processes certification.

ISO 27701:2019
An international privacy standard for protecting and managing the processing of personal data. We have been ISO 27701 certified as a PII Processor and PII Controller since 2021.

ISO 27018:2019
Extends an Information Security Management System (ISMS) to protect personal data when being processed in a public cloud.

FedRAMP Moderate
Cloudflare maintains FedRAMP Moderate authorization, allowing federal agencies to adopt Cloudflare's performance, security, and zero trust solutions.

SOC 2 Type II
A security certification that consists of a technical audit and a requirement to outline and follow comprehensive information security policies and procedures.

PCI DSS 4.0
Helps payment processors and financial institutions mitigate the risk of credit card fraud. We maintain PCI DSS Level 1 compliance and have been PCI compliant since 2014.

Global CBPR
Global Cross-Border Privacy Rules (Global CBPR) system.

Global PRP
The Global Privacy Recognition for Processors (Global PRP) system.

EU Cloud Code of Conduct
An officially approved GDPR Article 40 Code of Conduct. Adherence to the code means that Cloudflare commits to implementing data protection policies and security measures that align to the GDPR.

Cyber Essentials
Cyber Essentials defines a set of security controls and guidance for organizations of all sizes, developed by the United Kingdom's National Cyber Security Centre.

C5:2020
Ensures cloud service providers adhere to a baseline of information security criteria. This auditing standard was created by Germany's Federal Office for Information Security (BSI).

ENS
Spain's national security framework (Esquema Nacional de Seguridad).

IRAP
Information Security Registered Assessors Program, Cloudflare for Government-Australia.

BSI Qualification
German government's Federal Office for Information Security qualification for qualified providers of DDoS mitigation services.

WCAG 2.1 AA and Section 508
Cloudflare's Dashboard completes Voluntary Product Accessibility Template (VPAT) in compliance with international standards set forth by the Web Content Accessibility Guidelines (WCAG) 2.1 AA and in conformance with legal standards set forth by Section 508 of the Rehabilitation Act.

1.1.1.1 Public DNS Resolver Privacy Examination
A Big Four accounting firm conducted a first-of-its-kind privacy examination to determine whether the 1.1.1.1 resolver was effectively configured to meet Cloudflare's privacy commitments.

Learn more about Cloudflare's privacy and data protection policies and resources

- Trust Hub
- Privacy Policy
- GDPR Compliance
- US privacy law compliance

Transparency

We are transparent because we think it helps build trust and makes the Internet more reliable, accountable, and innovative.

Transparency Report updates

Part of maintaining trust in how we operate our network is being transparent about the requests we receive to access customer information and address abuse. Our Transparency Report provides information about the number and type of legal requests for customer information and abuse reports we receive. It also includes the general principles that guide our handling of reports and requests, and information on trends and notable developments based on data from the reporting period.

In 2025, we made notable changes to our report to better align with provisions in the EU's Digital Services Act (DSA). For example, we divided the information into two parts: Legal Requests for Information and Abuse Process Report. The first report provides information on law enforcement, government, and civil requests for customer information. The second describes Cloudflare's processes for handling abuse reports and responding to legal requests to terminate or restrict access to those services for certain users. The reports include new types of information, including additional types of law enforcement requests, categories of hosted content abuse, our automated steps to mitigate phishing and technical abuse, and average response time for certain types of reports.

Incidents and outages

Our goal is to build the world's most reliable and resilient network. Resiliency means not only highly available core systems and an architecture with no single points of failure, but also processes to ensure rapid, transparent recovery when incidents do occur. Cloudflare mobilizes a whole-of-company engineering response to major incidents, including detailed, public post mortems that explain exactly what happened, how we fixed it, and what we are doing to make sure it does not happen again.

Read more about how Cloudflare uses transparency as part of its resiliency efforts

- Cloudflare outage on November 18, 2025
- Post mortem on the Cloudflare Control Plane and Analytics Outage
- Major data center power failure (again): Cloudflare Code Orange tested

TRANSPARENCY

IN FOCUS

Requests for customer information

Cloudflare periodically receives legal requests to access customer information. An essential part of earning and maintaining trust is being transparent about those requests and how we respond.

Require due process

Before producing customer data, we require that all law enforcement, government, or third-party requests we receive adhere to the due process of law and are subject to appropriate judicial oversight.

Respect privacy

It is Cloudflare's overriding privacy policy that any personal information provided to us by our customers is just that: personal and private. Our respect for our customers' privacy applies with equal force to requests from law enforcement, government, or private third parties.

Provide notice

Unless legally prohibited, it is our policy to notify our customers of any legal request where we may produce their information, whether it comes from law enforcement, government, or private third parties.

Cloudflare will challenge requests that do not comply with due process, are overly broad in scope, that conflict with privacy laws of a person's country of residence, or that unduly restrict our ability to notify customers of those requests.

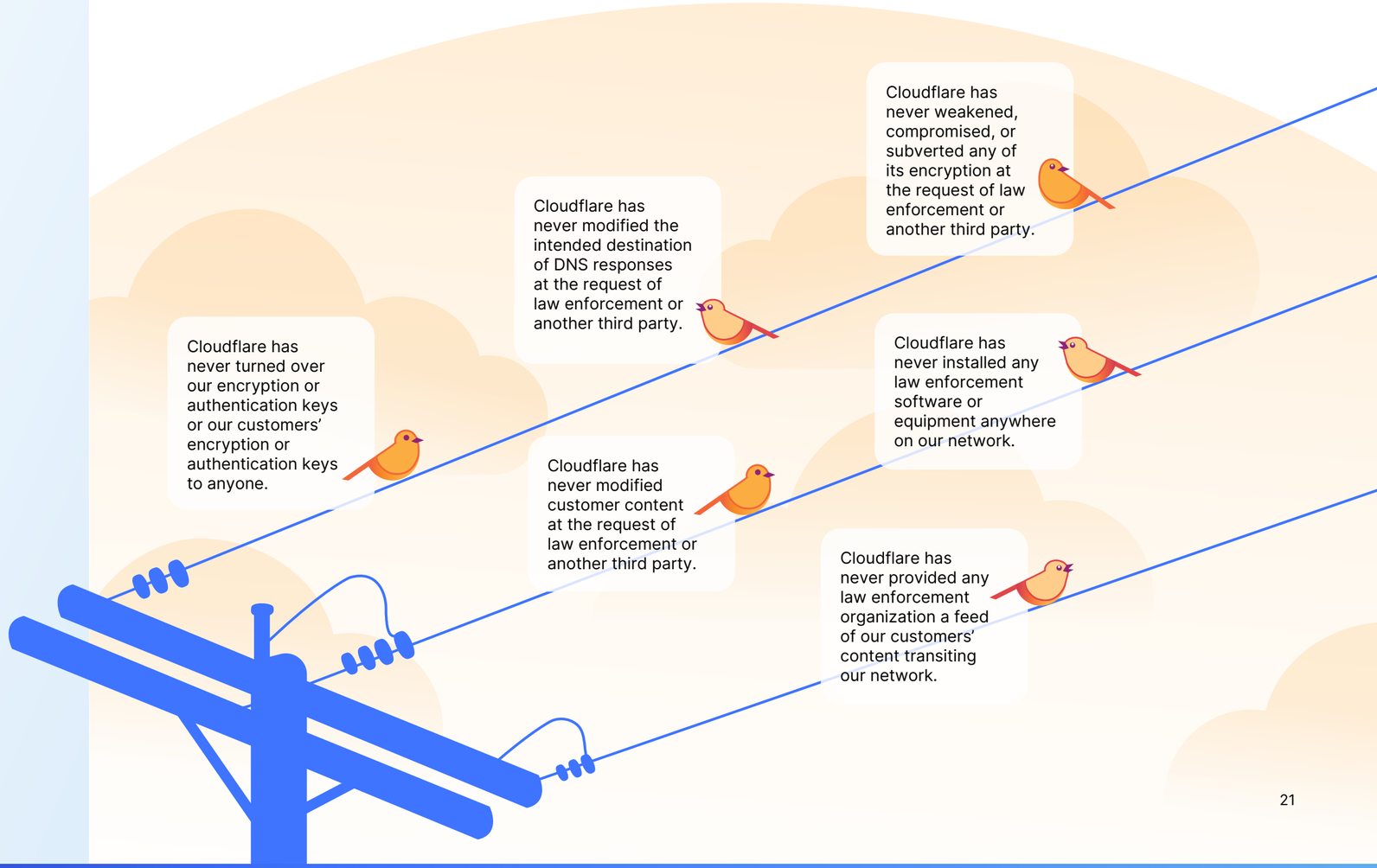
Warrant Canaries

Warrant Canaries are a public list of actions we have never taken on our network. They help our customers understand how we have acted in the past and how we intend to act in the future.

Cloudflare first published its list of Warrant Canaries in 2020. If Cloudflare were compelled to take action that would potentially violate one of those commitments, we would resist through all available legal remedies in order to protect our customers from unlawful requests or requests inconsistent with international human rights principles.

For more information on Cloudflare's approach to legal requests for information, visit:

- Trust Hub
- Law enforcement
- Transparency Report



TRANSPARENCY

Ethics

Anti-corruption

We are committed to working against corruption consistent with Principle 10 of the UN Ten Principles, as well as the United States Foreign Corrupt Practices Act, the United Kingdom Bribery Act of 2010, and other applicable laws.

Our policy against corruption is reflected in our Code of Business Conduct and Ethics, as well as our Third Party Code of Conduct, additional internal policies, and our employee handbook. All Cloudflare employees complete annual training on bribery and corruption. All suppliers, resellers, and partners are screened at onboarding to ensure we do not partner with companies at high risk for corruption.

Ethical conduct

Our Code of Business Conduct and Ethics addresses topics such as fair and accurate reporting, fair dealing and legal compliance, conflicts of interest, anti-harassment, nondiscrimination, health and safety at work, and fair competition.

Fair labor and modern slavery

We are committed to the ILO Declaration on Fundamental Principles and Rights at Work, as well as Principle 3 of the UN Ten Principles regarding freedom of association and effective recognition of the right to collectively bargain. Cloudflare explicitly prohibits human trafficking and the use of involuntary labor. These policies are reflected in our Modern Slavery Act Statement for Fiscal Year 2024.

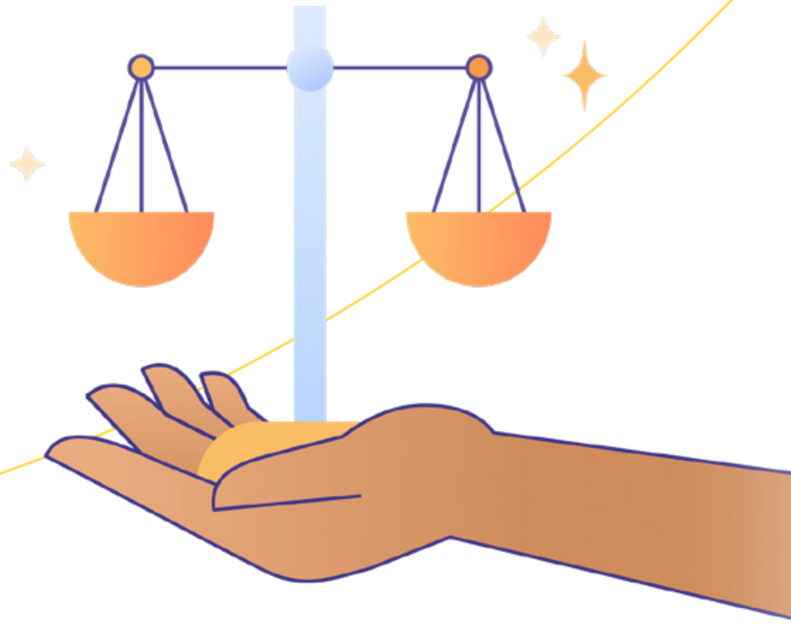
Cloudflare strives to work only with third parties who are committed to operating with the same level of ethics and integrity as we do. In addition to our Code of Business Conduct and Ethics, we have a Third Party Code of Conduct, specifically formulated with our suppliers, resellers, and other partners in mind. It covers such topics as human rights, fair labor, environmental sustainability, anti-bribery and anti-corruption, trade compliance, anti-competition, conflicts of interest, data privacy and security, and government contracting.

Sanctions compliance

Our commitment to compliance includes programs that prohibit us from doing business with sanctioned parties. Our robust compliance program includes safeguards designed to prevent sanctioned parties from signing up for service. We actively screen our customers, resellers, vendors, and partners to identify links to sanctioned parties and countries. Our contracts include commitments from our customers, resellers, vendors, and partners that they will comply with all applicable sanctions laws.

Learn more about our Legal Compliance work

- Code of Business Conduct and Ethics
- FY2024 Modern Slavery Act Statement
- Third Party Code of Conduct
- The challenge of sanctioning the Internet



A better Internet is for everyone

Free services

We believe in the power of serving everyone. We design our products to be easy to access and adopt, which also makes them easy to give away.

Competitive advantage

One cost of running Cloudflare's network is bandwidth—the traffic that traverses our network. Because millions of websites use Cloudflare's free service, thousands of Internet service providers (ISPs), who want direct access to those websites, agree to peer directly with our network and exchange traffic at no cost. As a result, Cloudflare is one of the most peered networks in the world. The more free customers using Cloudflare, the more ISPs and other networks want to peer with us for free, which allows us to continue offering free services.

Customers using our free services also help us build better products. Because roughly 20% of websites sit behind Cloudflare, our network sees diverse traffic and cyberattacks from all over the world, which can be used to automatically improve our products for all customers. Free customers also help us with quality assurance on new products and features immediately and at incredible scale.

Innovation at scale

Customers using our free services also help us build better products. Because roughly 20% of websites sit behind Cloudflare, our network sees diverse traffic and cyberattacks from all over the world, which can be used to automatically improve our products for all customers. Free customers also help us with quality assurance on new products and features immediately and at incredible scale.

> When you believe in the power of serving everyone, you can make sure that those entities that need security the most have access to it."
>
> **Alissa Starzak, Deputy Chief Legal Officer and VP of Global Public Policy, Cloudflare**
> *Cloudflare Global Connect 2025, Las Vegas, NV*

> We believe the best way to make the Internet faster and more secure is to put powerful features into the hands of as many people as possible."
>
> **Dane Knecht, CTO, Cloudflare**
> *Birthday Week 2025*

Everyone deserves security

Making security products accessible means making them not only affordable, but also easy enough for anyone to adopt and deploy. Free customers represent a broad audience, from tech enthusiasts, to those simply looking to build a website, to journalists and human rights defenders working in difficult jurisdictions. Focusing on serving our free customers, and making our products simple and effective, has also allowed us to help protect some of the most vulnerable and important voices online.

Cloudflare Free plan

- **AI Crawl Control**
- **Network Security**
  (Zero Trust Network Access, Secure Web Gateway)
- **Developer Tools**
  (Workers, Pages, and R2 Storage)
- **Privacy-Enhancing DNS Resolver**
  (1.1.1.1)
- **Web Application Firewall (WAF)**
- **Content Delivery Network (CDN)**
- **DDoS Protection**
- **SSL Encryption**

Access to innovation, everywhere

Cloudflare brings AI within milliseconds of every person on Earth, giving anyone the power to launch the next great idea.

Bringing AI access and development to the edge

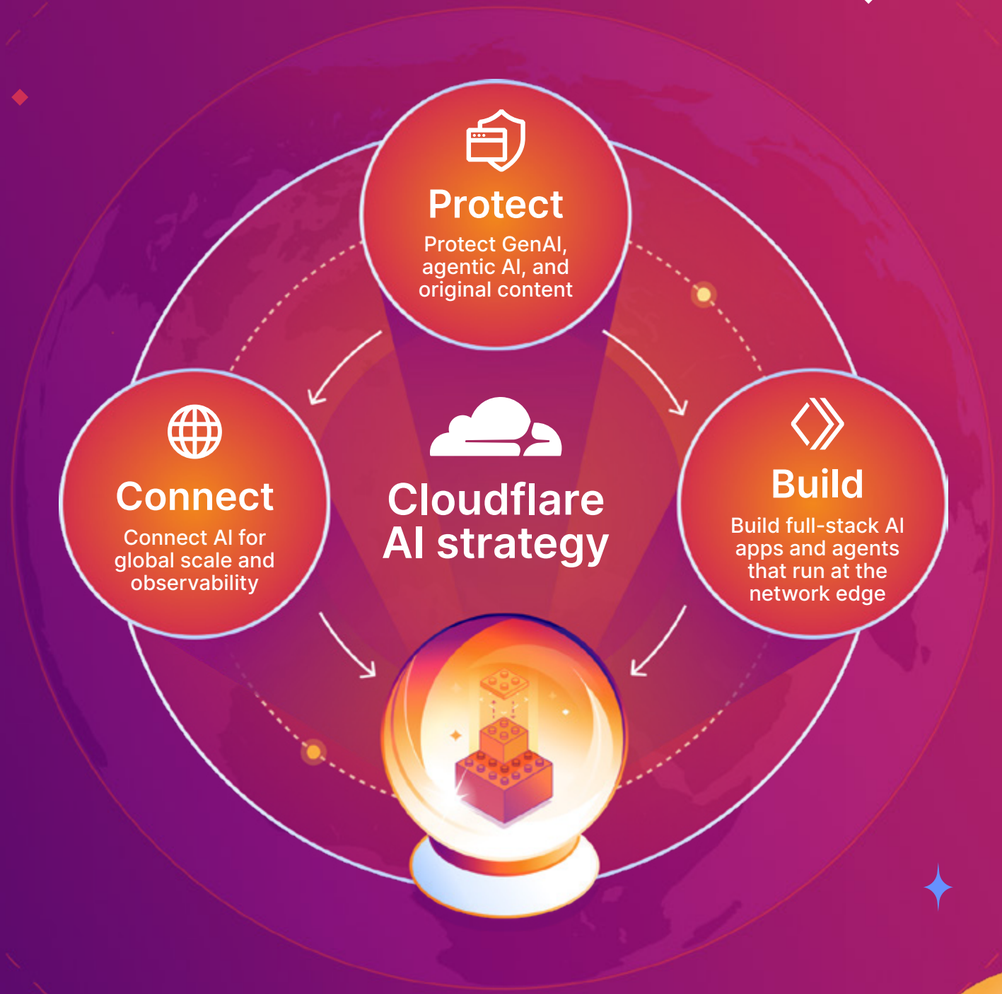
Inclusive AI must be accessible everywhere. Cloudflare operates in over 330 cities, bringing access to world-class models and applications within 50 milliseconds of 95% of Internet users. This proximity not only allows developers to build and deploy their ideas—using scalable compute, inference, databases, and storage, and without building data centers or managing hardware—but also ensures the low latency necessary for consumers to use AI technologies at scale.

Empowering local solutions

The best solutions are built locally. Cloudflare champions regional innovation by hosting diverse, locally optimized models fine-tuned to specific languages and cultures. Our developer platform is already integrated with locally-developed, open source AI models in India, Japan, and Southeast Asia.

Choice and control

Like the Internet, AI should be open and distributed. Cloudflare integrates with over 50 leading AI models, allowing developers to switch, combine, and control their applications while supporting a diverse AI ecosystem. We pair this flexibility with built-in observability and security, allowing builders to understand where their data is flowing and protect it with global threat intelligence.



Launching the next wave of startups

Cloudflare developer tools make it easier for anyone—not just engineers—to write code and build AI applications. We also provide startups with additional support including access to mentorship, technical assistance, and funding opportunities through our Workers Launchpad program.

Learn more about our startup programs at cloudflare.com/forstartups.

Startups building on Cloudflare in 2025

4,237 startups | **124** countries

500+ AI startups

175 startups in Workers Launchpad

$2 billion in financing

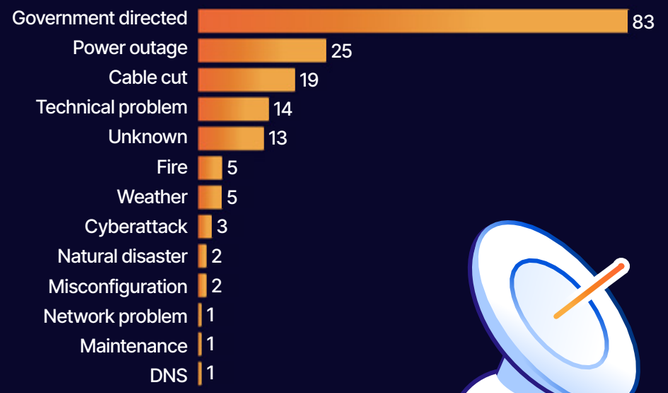
Cloudflare Radar

EST. 2020

Free public resource that aggregates anonymized data from Cloudflare services and makes it possible for anyone to monitor and investigate Internet patterns, trends, attacks, shutdowns, and anomalies around the world. View our full 2025 Year in Review here.

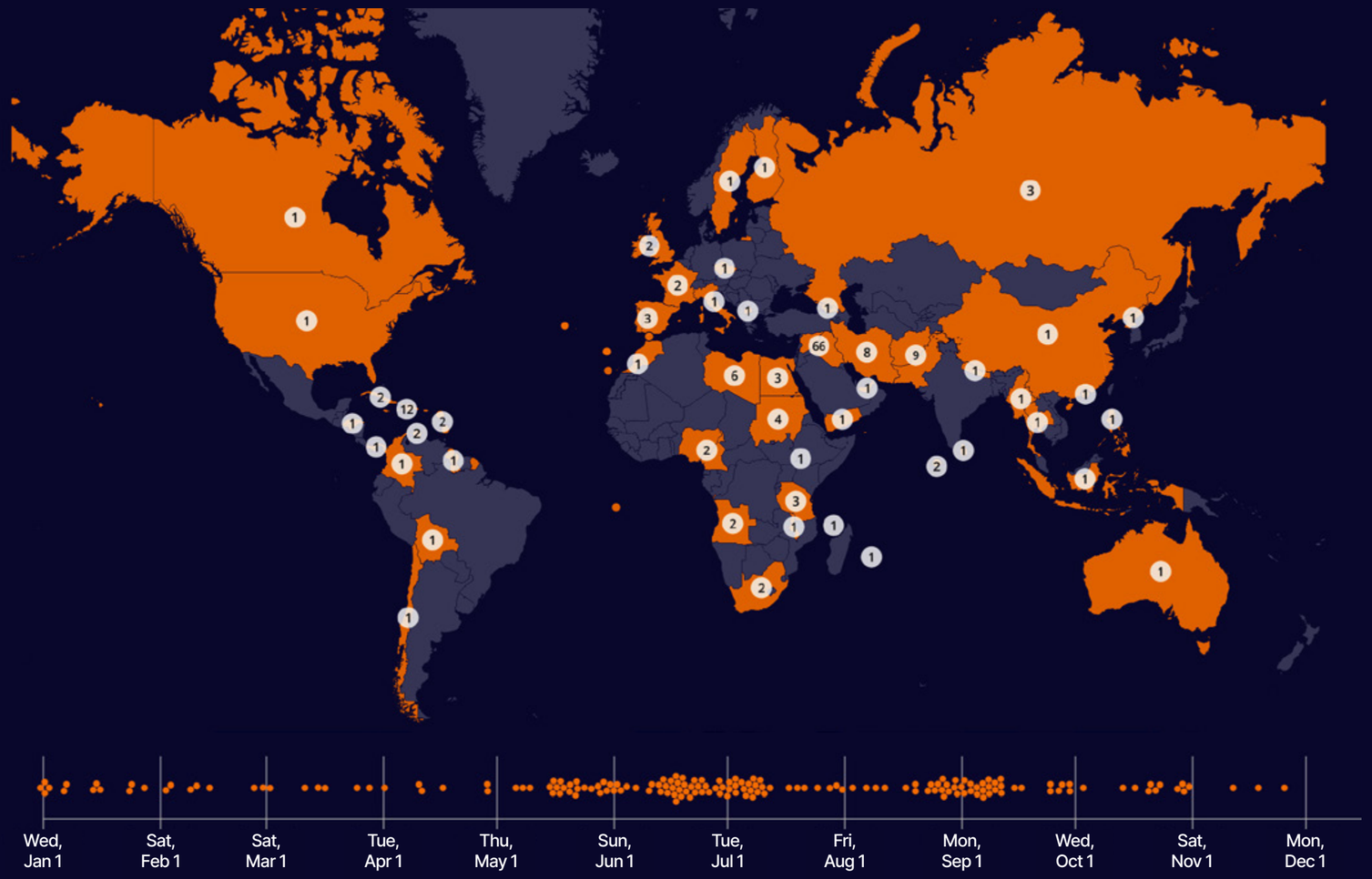
Causes of Internet outages

13 causes observed globally



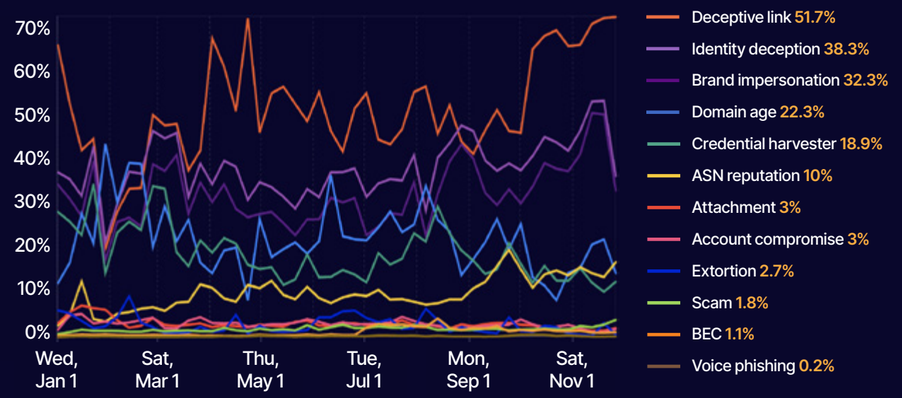
Internet outages

174 major Internet disruptions observed globally



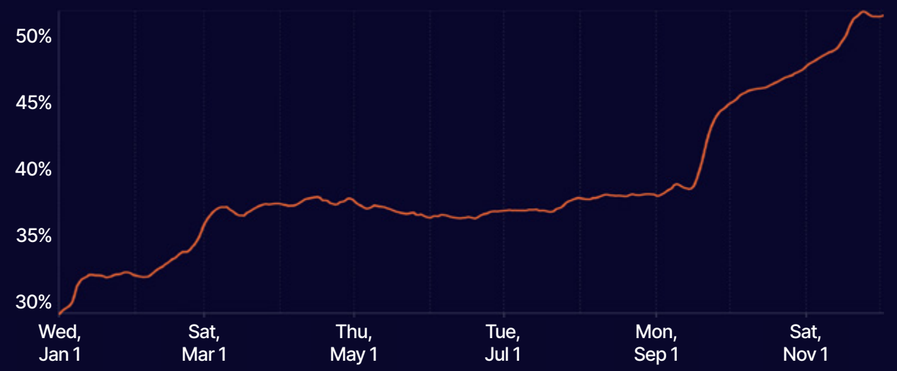
Top email threats: Threat categories worldwide

52% of malicious emails contained a deceptive link



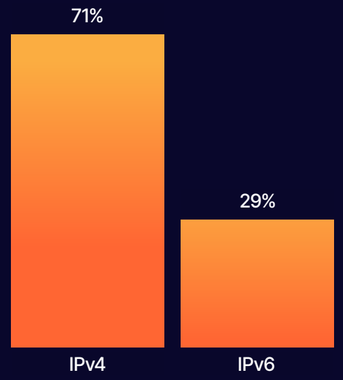
Post-quantum encrypted traffic worldwide

52% of TLS 1.3 traffic is using post-quantum encryption



IPv6 adoption

29% of dual-stack traffic is over IPv6



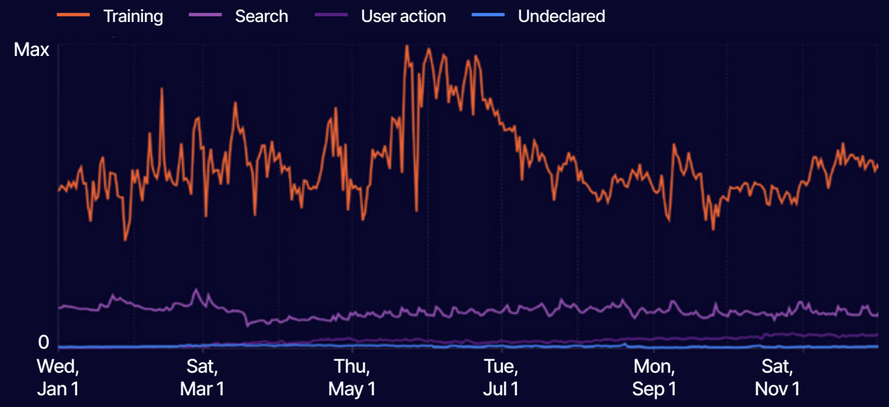
Internet services

Top 10 most popular worldwide

Rank	Service
#1	Google
#2	Facebook
#3	Apple
#4	Microsoft
#5	Instagram
#6	AWS
#7	YouTube
#8	TikTok
#9	Amazon
#10	WhatsApp

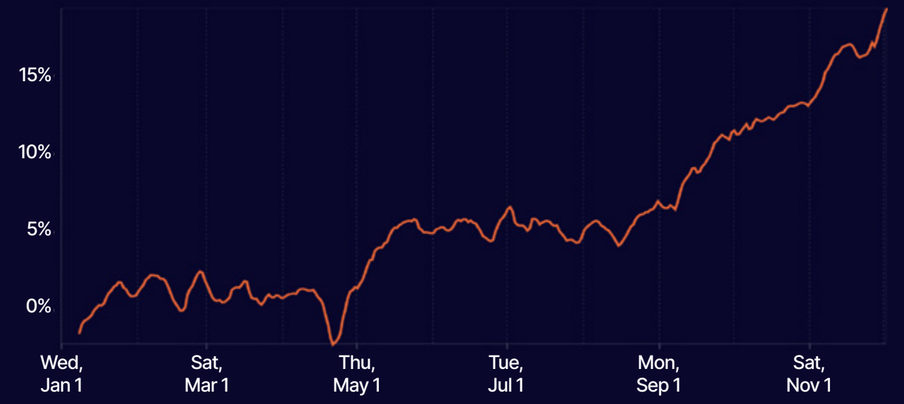
AI bot traffic by crawl purpose worldwide

Training was the most active crawl purpose



Internet traffic growth

19% growth in worldwide Internet traffic

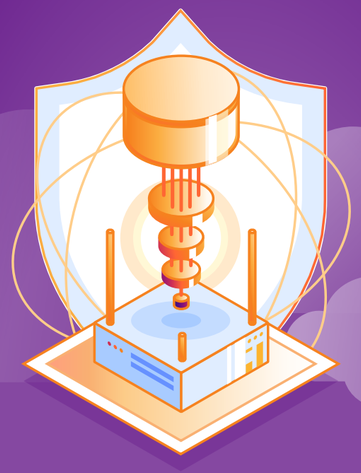


Post-quantum cryptography

Encryption is a prerequisite for privacy, security, and freedom of expression online. Cloudflare is helping the Internet prepare for the post-quantum world by making advanced cryptography available to everyone—for free and by default.

50%

of human-initiated traffic with Cloudflare is now using post-quantum encryption

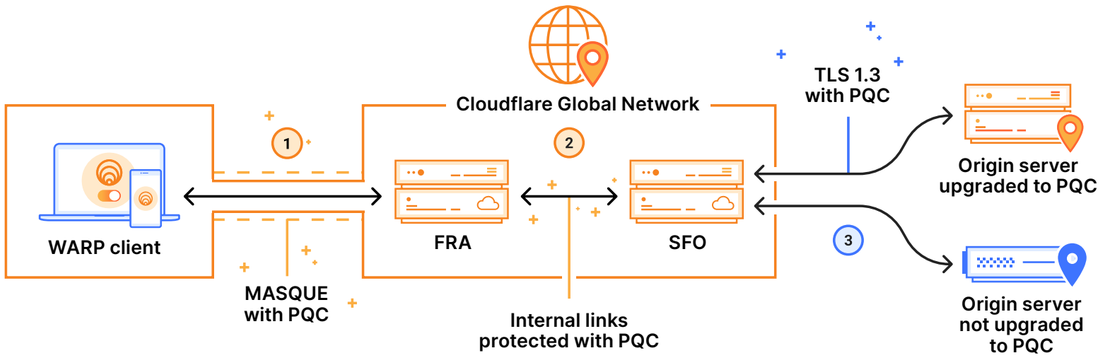


Post-quantum cryptography for everyone

It has long been Cloudflare's mission to provide the public with access to essential security tools that are free and easy to use. The same is true for post-quantum cryptography (PQC). In 2023, Cloudflare announced that we would provide PQC for free by default for all customers, helping to secure their websites, APIs, cloud tools, and remote employees against future threats.

WARP now includes PQC NEW!

Cloudflare has expanded these protections to individual users by upgrading our WARP client to support post-quantum key agreement. This upgrade ensures that anyone using the free WARP app has their outgoing network traffic wrapped in a post-quantum encrypted MASQUE tunnel. Although quantum computers are not yet able to break standard encryption, implementing these protections today is critical. It defends users against "harvest now, decrypt later" attacks, where bad actors steal encrypted data today in the hopes of decrypting it as quantum technology matures.

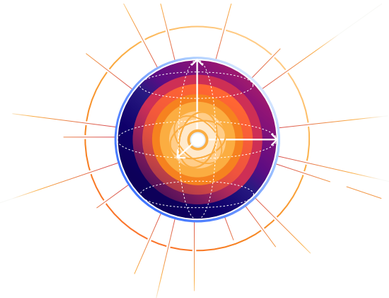


Cloudflare consumer WARP client (1.1.1.1) is now upgraded to post-quantum key agreement

"Running code" to help develop new standards

Cloudflare is also working with the Internet Engineering Task Force (IETF) to tackle one of the most difficult post-quantum challenges: certificates. Quantum computers are expected to be able to crack today's TLS certificates, which would allow them to impersonate a server and intercept user traffic. The current challenge with the proposed post-quantum signatures is that they are significantly larger—2,420 bytes compared to just 64 bytes for current signature algorithms. This results in more round trips over the network and noticeable latency for the user. Cloudflare is helping to design, implement, and test the next generation of TLS certificates—known as Merkle Tree Certificates—that will enable a smooth transition to post-quantum.

State of the post-quantum Internet in 2025



In the last week of October 2025, we reached a major milestone for Internet security: The majority of human-initiated traffic with Cloudflare is using post-quantum encryption, mitigating the threat of harvest-now/decrypt-later. Read the full blog.

Learn more about Cloudflare's work on post-quantum cryptography

- Policy, privacy and post-quantum: Anonymous credentials for everyone
- Keeping the Internet fast and secure: Introducing Merkle Tree Certificates
- You don't need quantum hardware for post-quantum security
- NIST's first post-quantum standards
- Cloudflare now uses post-quantum cryptography to talk to your origin server
- No, AI did not break post-quantum cryptography
- Post-quantum crypto should be free, so we're including it for free, forever

Open source

Open source is more than code. It is the spirit of collaboration and interoperability that drives the Internet forward.

Cloudflare has a long history of supporting open source projects—both through external projects that we support and our own projects shared with the community.

Supporting the future of the open web

Open source software democratizes innovation, allowing anyone to inspect, improve, and share code. This transparency produces software that is often reliable, adaptable, and easier to maintain.

Cloudflare's infrastructure was built on a foundation of open source software. We think continuing to support the open source community is essential to our business and the future of the Internet. In 2024, Cloudflare launched Project Alexandria, which significantly expanded the scope of free services we offer to support open source projects.

Here are some examples of exciting open source projects building with Cloudflare:

- **Ladybird:** A truly independent web browser and engine. Rather than building on top of Chromium—like most modern browsers—Ladybird is being built from the ground up to prioritize privacy, performance, and security.
- **Omarchy:** A modern Linux developer environment designed for accessibility. Omarchy removes the complexity of systems configuration, allowing developers to get up and running instantly.
- **Astro:** A modern web framework designed for high-performance, content-driven websites. Astro pioneered a new architecture that strips away unnecessary code, delivering lightning-fast performance. It has rapidly become a favorite tool for developers building the next generation of the web.
- **TanStack:** A suite of powerful developer tools that help solve some of the hardest problems in modern application development. TanStack provides the ideal engine for complex web applications, offering robust primitives for managing server state, routing, and data-intensive user interfaces.

> Cloudflare's support of Omarchy has ensured we have the fastest ISO and package delivery from wherever you are in the world ...The combo of a super CDN, great R2 storage, and the best DDoS shield in the business has been a huge help for the project."
>
> David Heinemeier Hansson, Creator of Omarchy and Ruby on Rails

Contributing code

Working with the open source community is a two-way relationship. We believe we have an obligation to give back in the same way that we have benefited from others. Cloudflare has released a number of our most important technologies including Quiche, Workerd, and Pingora. We do this not only to show our support for the open source community, but also because we believe releasing software allows us to find and fix bugs faster, out-innovate our competitors, and continue to attract the best talent.

Want to join Project Alexandria?

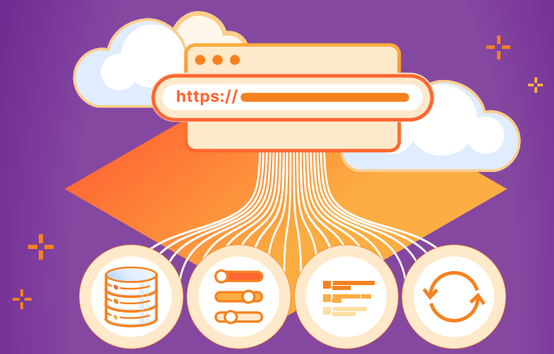
If you are an open source project that meets the following requirements, apply here.

- Operate solely on a nonprofit basis and / or otherwise align with the project mission
- Be an open source project with a recognized OSS license

Open, interoperable standards

Standards are the foundation of the open Internet. They provide the common technical language that has enabled the Internet to grow into a global network where anyone can build products and test ideas.

Cloudflare participates in standards bodies because we believe that protocols—based on technical merit and consensus—are essential to ensuring the Internet remains inclusive, secure, and competitive.



Web Bot Auth

Web traffic is increasingly dominated by automated clients—including AI crawlers, agents, and search summaries. Distinguishing these bots from malicious traffic is critical for security and for ensuring that AI companies can access data efficiently. Current practices rely on IP addresses and easily spoofed User-Agent headers, which are becoming too slow and inaccurate for modern web traffic. To solve this, Cloudflare engineers are collaborating with industry leaders in the IETF Web Bot Auth Working Group, developing new standards that allow bots to cryptographically authenticate their identity reliably.

Media Over QUIC (MoQ)

To enable the next generation of real-time media, Cloudflare is participating in the development of MoQ at the IETF. We launched the first global MoQ relay network to validate the protocol against the realities of the Internet. By open-sourcing implementation and collaborating with partners to address practical ecosystem challenges, Cloudflare is helping to build a robust, vendor-neutral foundation for the next generation of live media.

AI Preferences

AI Preferences will enable content creators to specify how their content ought to be treated by AI companies. Cloudflare believes that this is a critical capability on the modern Internet and is rapidly building systems to help promote a healthy ecosystem that compensates content creators and owners for their contributions.

Learn more about Cloudflare's work on Internet standards

- TLS 1.3
- Privacy Pass
- QUIC
- ECH
- WinterCG
- Privacy-Preserving Measurement
- MASQUE

34

Requests for Comment published by Cloudflare engineers since 2012

Requests for Comments (RFCs) are the architectural blueprints of the Internet. Cloudflare engineers actively contribute to RFCs that serve as the foundations of security, privacy, and interoperability.

Here are two such standards our team helped produce this year:

- The Concealed HTTP Authentications Scheme
- DNSSEC Trust Anchor Publication for the Root Zone

Project Cybersafe Schools

EST. 2023

Project Cybersafe Schools supports eligible K-12 public school districts with a package of security solutions—for free, and with no time limit. Cloudflare launched the program at the White House's Back to School Safely: K-12 Cyber Security Summit in 2023 in cooperation with the Department of Homeland Security and the Department of Education.

233 school districts

277,000+ students and staff members protected

30 states across the country

Types of threats mitigated

- Multi-channel phishing
- Credential harvesting
- Social engineering attacks via email
- Unwanted and harmful online content

Eligibility requirements

- Located in the United States
- K-12 public school districts
- No larger than 2,500 students per district

> We were amazed to see that **Cloudflare caught nearly 4,000 malicious emails** in the first month of implementation! We are confident that Cloudflare will continue to keep our district and infrastructure safe from harmful threats."
>
> Matt Champion, Technology Coordinator, Quitman School District, Quitman, Mississippi

> Being able to leverage multiple layers of security helps us be more robust in protecting our student and teacher devices and ensure our learning environment is successful, safe, and productive in the current digital landscape."
>
> Randy Saeks, Network Manager, Glencoe School District 35, Glencoe, Illinois

Apply for Project Cybersafe Schools at **cloudflare.com/lp/cybersafe-schools**.

1.1.1.1

Fast. Free. Private.

EST. 2018

1.1.1.1 is a public DNS resolver that helped pioneer the principle of privacy-first. The Domain Name System (DNS) is the phonebook of the Internet. It translates domain names like example.com into numeric IP addresses that are used to connect users to websites. Unlike many other resolvers, 1.1.1.1 does not track user activity or sell data to advertisers. It also helps make DNS queries faster and more secure by incorporating cutting-edge security features like strong encryption, ODoH, DNSSEC, and query name minimization.

2.2 trillion

queries per day on average (over Q3 2025)

~12 ms

average latency
(October 2025, dnsperf.com)

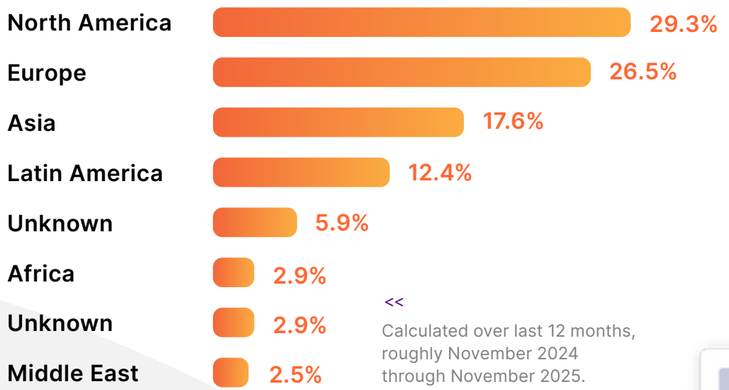
Learn more at
one.one.one.one

What is encrypted DNS?

Traditional DNS queries were sent in plain text, which allowed Internet service providers (ISPs) and other third parties to track users' activity and develop profiles on their online behavior. Protocols like DNS over HTTPS (DoH) and DNS over TLS (DoT) encrypt those queries and help prevent third-party surveillance.

Oblivious DNS over HTTPS (ODoH) takes encryption a step further by ensuring that no single entity sees both the identity of the user making a DNS request and the domain they are visiting. Cloudflare is proud to have worked with a number of partners including Apple, Microsoft, and Mozilla to develop and deploy secure DNS technologies for millions of users.

Distribution of 1.1.1.1 queries by region



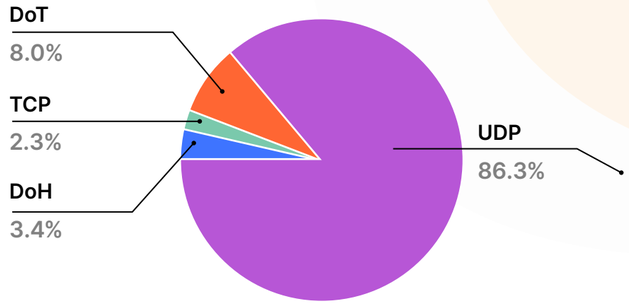
<< Calculated over last 12 months, roughly November 2024 through November 2025.

NEW!

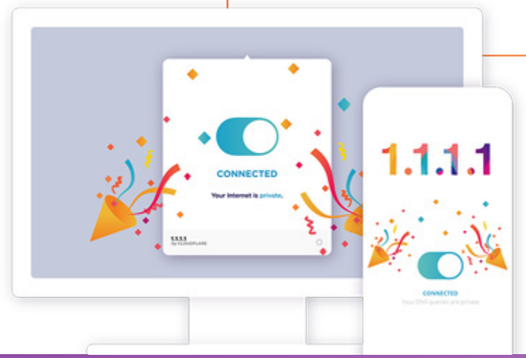
DNS statistics now available on Cloudflare Radar

Cloudflare Radar has expanded its capabilities to allow anyone to view resolver data gathered from 1.1.1.1. Users can now monitor global trends in DNS encryption and DNSSEC adoption, and explore a brand-new section dedicated to Top-Level Domains (TLDs).

Distribution of 1.1.1.1 queries by DNS transport protocol



This graphic shows the number of encrypted DNS queries (DoT and DoH) received by 1.1.1.1 from December 2024 to November 2025. Our goal is to continue to increase those numbers each year to help protect and encrypt users' web traffic.



Community

Our Employee Resource Groups (ERGs) are the cornerstone to Cloudflare's community, striving to foster belonging and support for all our team.

94–95%

of Cloudflare employees feel a strong connection to our mission and believe their work is important.

Cloudflare ERGs

Employee Resource Groups (ERGs) are employee-led and company-supported groups, intended to promote underrepresented and/or marginalized employees or groups of employees, joined together based on shared characteristics, life experiences, or initiatives. Our ERGs are led by volunteer employees helping to build a sense of belonging through connecting and celebrating culture, special events, and mentorship.

- Afroflare
- Arabflare
- Asianflare
- Careflare
- Cloudflarents
- Crossflare
- Desiflare
- Flarability
- Greencloud
- Judeoflare
- Latinflare
- Mindflare
- Nativeflare
- Persianflare
- Proudflare
- Soberflare
- Turkflare
- Vetflare
- Womenflare

<< Communities are important for building networks of support and fostering a sense of belonging. At Cloudflare, we facilitate ours through our teams and cross-functional partners, but also through the growth of our ERGs.

+1,111

NEW!

1,111 Intern-ets

This year we announced our plan to hire 1,111 interns over the course of 2026. Being an intern at Cloudflare means working on real problems and creating tangible impact. As the age of AI is beginning, our 2026 class of interns will have a special focus: to ramp up the creative and widespread application of AI with a fresh approach.

Intern-ets won't be on the sidelines of our projects—they'll be embedded in our teams around the world, working directly with our engineers, shipping code, and helping make the Internet a better place. Our internship opportunities will be listed here.

Recruiting

Building teams that drive innovation is part of our mission.

Our values are key to our company culture and our recruitment process, and we take them seriously when extending offers to join our team.

We are principled.

We are curious.

We are transparent.

SkillBridge Official Partner

The US Department of Defense SkillBridge program pairs service members who are preparing to exit the military with organizations that can provide hands-on experience in both private and public sectors.

We are proud to announce that to further improve our search for top talent, we have joined the SkillBridge initiative as an official industry partner. Since joining the program, our second SkillBridge intern has accepted an offer of full-time employment from Cloudflare, and we are continuing to ramp up toward a goal of five SkillBridge internships a year.

> “Through this program, I gained exposure to various facets of the company, tackled engaging and complex customer challenges, and been warmly embraced by a supportive team in an incredibly positive environment.”
>
> **Nick Kuntz, SkillBridge Intern**

Grace Hopper Celebration

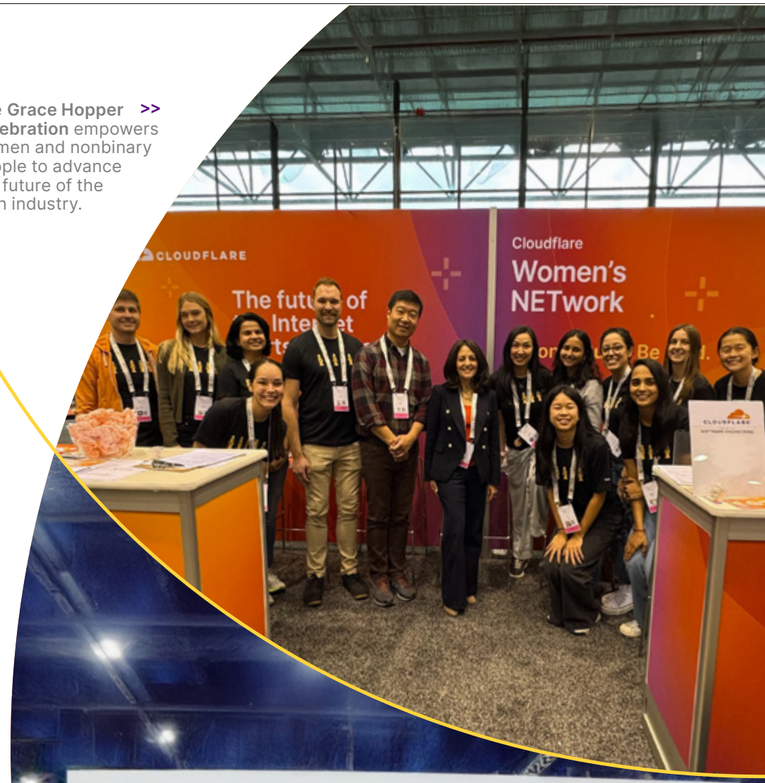
At this year’s Grace Hopper Celebration in Chicago, our team engaged with thousands of women and nonbinary people in tech over three days. Our highlights of the conference were our Chief Strategy Officer, Stephanie Cohen, speaking on the main stage, conducting 54 on-site interviews, and receiving 1,300 resumes from participants.

AFROTECH

Focused on uplifting Black professionals in tech, AFROTECH brings together Black technologists for networking and professional development. For the third consecutive year, we provided scholarships, doubling the number from previous years, to support technical students from Texas in attending and participating in the conference.

Learn more about Cloudflare recruitment efforts here.

The **Grace Hopper Celebration** empowers women and nonbinary people to advance the future of the tech industry. >>



Our team

Diverse teams are a competitive advantage.

Cloudflare capabilities

- Be curious to learn and grow
- Communicate clearly, directly, and transparently
- Do the right thing
- Embrace diversity to make Cloudflare better
- Get your work across the finish line
- Lead with empathy and assume good intentions

Diverse teams are more effective, innovative, and better positioned to drive long-term growth, and without an equitable and inclusive working environment, diverse teams won't succeed. At Cloudflare we see that helping cultivate and maintain an inclusive workplace where our teams can be their full selves results in our best work.

US Overall race / ethnicity

55.39% White

25.36% Asian

8.09% Hispanic or Latino

5.43% Black or African American

3.41% Two or more races

1.01% Middle Eastern or Mediterranean

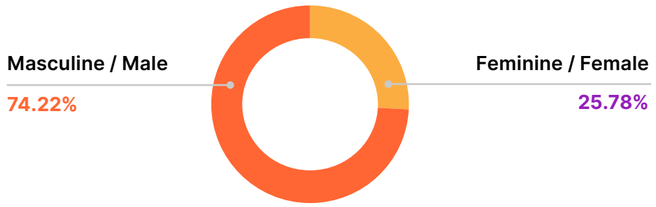
0.61% Other

0.42% American Indian or Alaska native

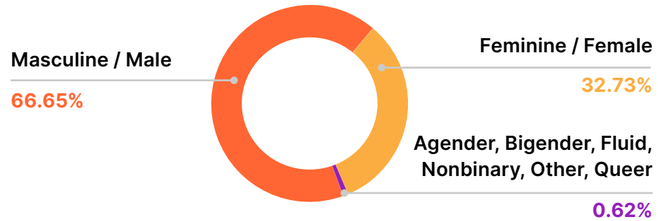
0.29% Native Hawaiian or Other Pacific Islander

Data presented here reflects only the information shared by employees who volunteer to disclose their representation data.

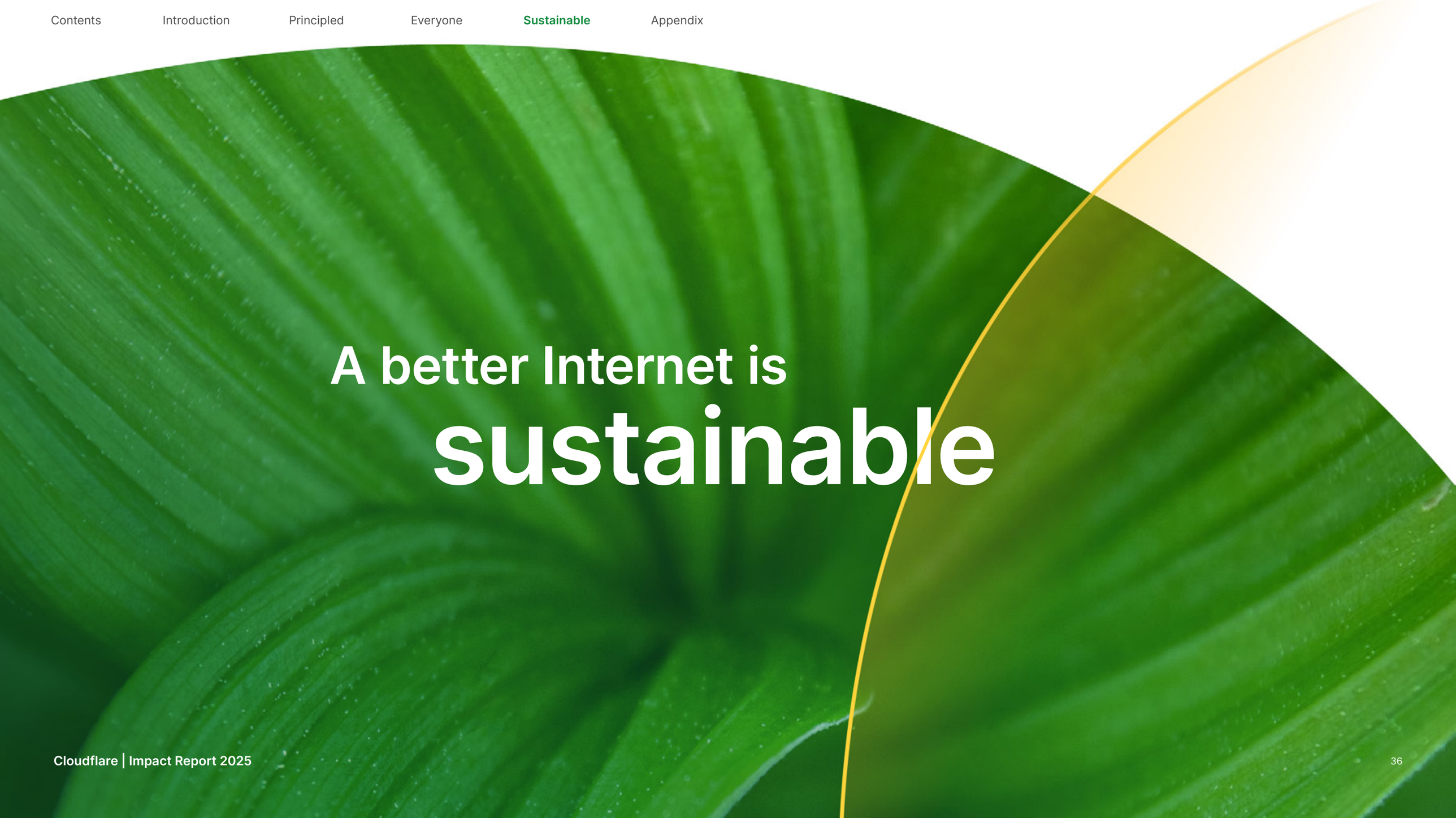
Leadership gender identity



Overall gender identity



Cloudflare has committed to the EU Charter, the UK Tech Talent Charter, and the German Diversity Charter for employee equity.



A better Internet is sustainable

Network

Cloudflare operates one of the world's largest networks. Every request, task, and service we process more efficiently helps reduce costs and make the Internet more sustainable.

Smaller footprint, bigger impact

Cloudflare's 12th generation (Gen 12) servers are our most powerful and power-efficient ever—delivering 84% more requests per second (RPS) per kilowatt (kW) compared to our previous Gen 11 model. Because each unit is more powerful and efficient, we have been able to reduce the total number of servers in our fleet while still meeting our growing network needs.

For example, in 2025 we decommissioned and replaced over 2,700 legacy Gen 10 and 11 servers with a consolidated fleet of 1,661 Gen 12 servers. Using nearly 40% less physical hardware to serve a higher volume of network traffic improves our efficiency while simultaneously reducing embodied carbon, transportation, and electronic waste.

AI and the future of data center cooling

Modern AI chips (GPUs) generate significantly more heat than traditional processors (CPUs). As a result, data center and network operators around the world are evaluating enhanced cooling techniques, particularly the transition from air cooling to liquid cooling technologies.

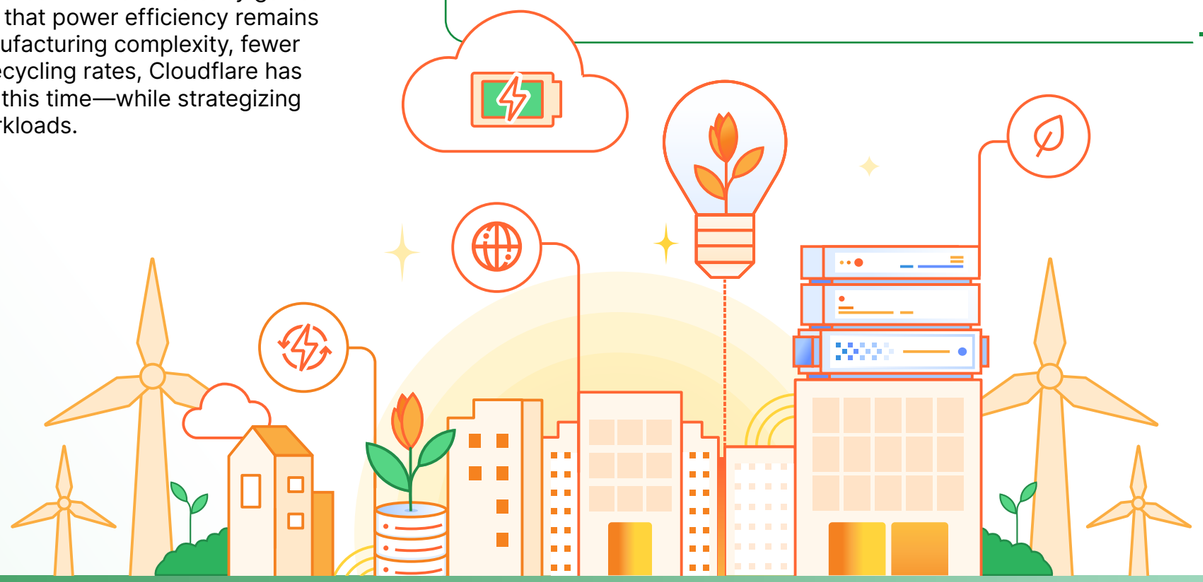
Cloudflare's infrastructure team continuously evaluates new components to maximize server efficiency. Earlier this year, Cloudflare presented data at the Open Compute Project EMEA Summit demonstrating that for our edge workloads, current liquid cooling solutions offered minimal efficiency gains over our optimized air-cooling designs. Given that power efficiency remains comparable, yet air cooling requires less manufacturing complexity, fewer specialized materials, and allows for higher recycling rates, Cloudflare has elected to continue its air-cooling strategy at this time—while strategizing thoughtfully for innovation specific to our workloads.

Learn more about Cloudflare's 12th generation servers:

- Thermal design supporting Gen 12 hardware: Cool, efficient, and reliable
- Cloudflare Gen 12 Server: Bigger, better, cooler in a 2U1N form factor
- Designing Edge Servers with Arm CPUs to Deliver 57% More Performance Per Watt

Learn more about how Cloudflare uses modular design, open source firmware, and recycling to help reduce waste and emissions:

- How we're making Cloudflare's infrastructure more sustainable
- A more sustainable end-of-life for your legacy hardware appliances with Cloudflare and Iron Mountain



Places

Open and accessible workplaces foster collaboration, innovation, and well-being. Our design philosophy emphasizes sustainability, light, and flexibility, ensuring that our offices are destinations where people can connect and thrive.

NEW!

Announcing New York, Bengaluru, and Mexico City!

Cloudflare opened three new offices in 2025. As with all our offices, we hope these new locations will allow us to connect more closely with customers, prospects, and partners in those regions. Our team is particularly excited about our new office and technology hub in Bengaluru, which will help Cloudflare gain access to one of the largest and most dynamic tech professional communities in the world.

Opening Cloudflare offices to startups and innovators

Starting in January 2026, Cloudflare will open doors at our San Francisco, Austin, London, and Lisbon offices to entrepreneurs and startups outside of our team who need space to innovate. Specifically, Cloudflare will offer complimentary, all-day coworking access to dedicated workspaces for registered participants.

Want to build your startup in a Cloudflare office?

- Come build with us: Cloudflare's new hubs for startups
- Cloudflare for Startups

PLACES

IN FOCUS

Walls of entropy

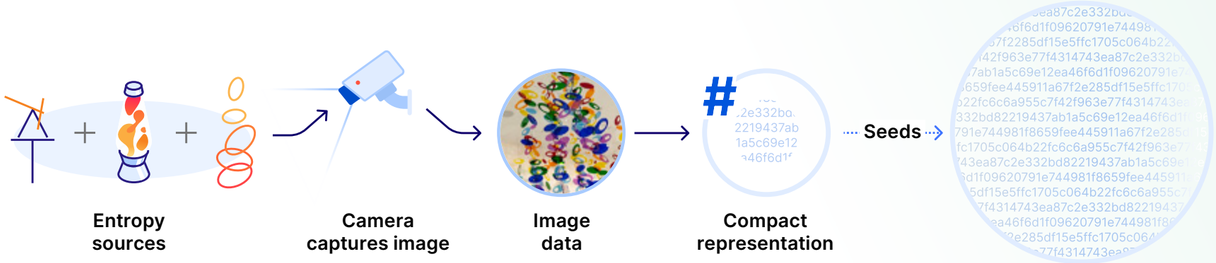
Chaos is the root of encryption. Cloudflare uses lava, waves, light, and motion to generate the randomness we use to power encryption for our network and the public.

Turning chaos into security

TLS encryption demands true unpredictability. Cloudflare meets this need with ‘walls of entropy’ that capture physical chaos. Ranging from our original lava lamps in San Francisco to our new 2025 wave-motion machines in Lisbon, cameras translate these non-repeating fluid dynamics into the random bytes that secure the Internet.

Democratizing trust: The League of Entropy

Public trust in systems like elections and lotteries rely on unbiased randomness. The League of Entropy—a coalition of universities, NGOs, and tech companies—provides this through a free, decentralized beacon. By combining independent sources, we avoid the risks of a single-party random number generator. Cloudflare is proud to be a founding member contributing our physical entropy walls to help ensure verifiable fairness.



Emissions

Cloudflare has published its annual greenhouse gas emissions since 2020 to help our stakeholders and customers understand the climate impact generated by our global network and operations.

Greenhouse gas emissions

Cloudflare uses ISO 14064 and the Greenhouse Gas Protocol, a leading standard that helps organizations understand, account for, and report their environmental impact. The protocol provides a framework for organizations to consistently track their climate impact across their supply chains and operations, with our emissions analysis reviewed and verified by an independent third party (see Appendix). By annually reporting the scope and scale of our emissions, Cloudflare is able to track our environmental impact year-over-year and our carbon footprint.

Since the start of Cloudflare's emissions reporting, Cloudflare has published companywide its Scope 1 (direct emissions) and Scope 2 (indirect emissions) GHG emissions.

In 2025, we expanded our reporting to include Scope 3 (emissions from our supply chain), including all other indirect emissions produced in our supply chains. Cloudflare's initial focus for Scope 3 has been sources of supply chain emissions directly related to our network, products, and services. This focus allows our stakeholders and customers to have a more accurate accounting of their emissions resulting from their usage of our services.

To account for its Scope 2 emissions, Cloudflare makes offset and renewable energy purchases in the same amount of renewable energy credits as we consume in all of our data centers and facilities around the world.

Emissions category	Carbon dioxide equivalent (CO_2e) in metric tons (MT)	Percent of calculated total
Scope 1	198	100%
Scope 2 (Location-based)[1]		
Facilities	1611	3%
Network	61,171	97%
Scope 2 (Market-based)	0	100%
Scope 3 (Market-based)[2]	43,071	100%
Total (Market-based)[3]	**43,071**	**100%**

[1] Location-based emissions reflect the average emissions intensity of grids on which energy consumption occurs.

[2] Market-based emissions reflect emissions from electricity that an organization has purposefully chosen. For more information on Cloudflare's renewable energy purchases, see Renewable Energy and Offset Purchases.

[3] Total (Market-based) emissions include Cloudflare's 2024 verified offsets and renewable energy purchases.

Bots and trees

2025 marks two important milestones in our effort to destroy bad bots online and help account for their climate impact. This year, we will officially reach 100,000 total trees donated—and we will make our smallest donation ever.

We are proud of both.

1,957

Number of trees Cloudflare will plant to account for 2025 bot-fighting activities

100,000+

Number of trees donated to date

Looking back

In 2019, Cloudflare announced our Bot Fight Mode service would be available for free for all of our customers. The goal was to trap bad bots online by forcing them to complete compute-heavy but meaningless tasks and prevent them from reaching our customers. We also announced that we would account for the extra energy attackers expended trying to solve these challenges by donating to reforestation projects through our partner, One Tree Planted.

Engineering ourselves out of the problem

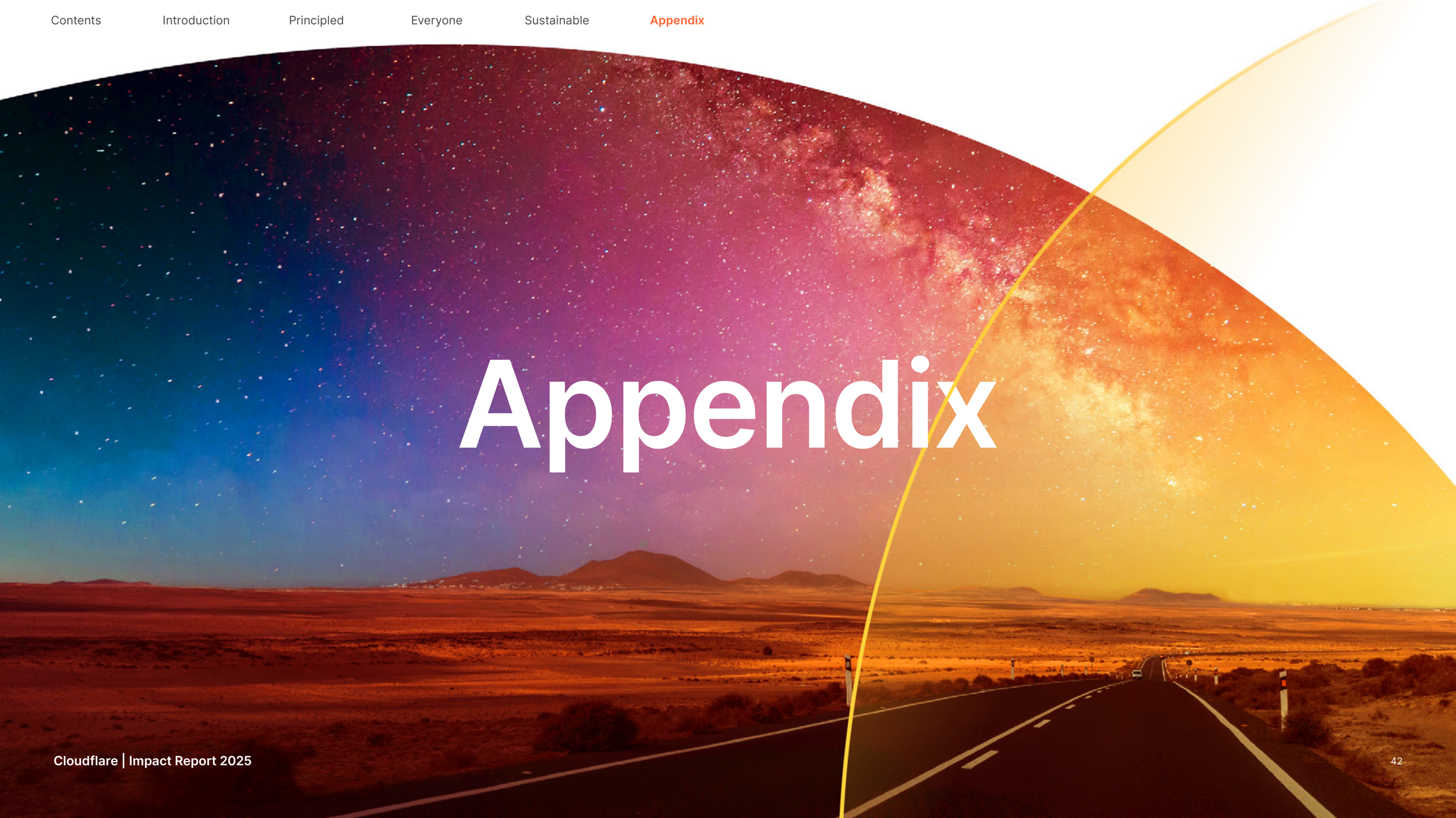
A central tenet of sustainability is to address a problem at its source, rather than mitigating its effects. Each year, Cloudflare has seen a reduction in the amount of CPU burned by our Bot Fight Mode—not because fewer bots have been trapped, but because our defenses have become more successful.

Rather than stalling bots in endless challenges and burning CPU and energy, our network has become more adept at blocking them entirely. While this means that each year our donation to One Tree Planted has decreased, it also means we have engineered a more efficient solution that causes both Cloudflare and attackers to consume less energy in the first place.

Learn more about One Tree Planted projects supported by Cloudflare

- Artibonite Watershed, Dominican Republic
- Monarch Butterfly Reserve, Mexico
- Kubu Raya Regency, Indonesia
- Leiria Pine Forest, Portugal
- Forrest Fire Recovery in British Columbia, Canada
- Kumirmari Island, West Bengal, India
- Victoria Park, Nova Scotia, Canada

Photos of Portugal and Dominican Republic tree planting projects, courtesy of One Tree Planted >>



Appendix

GRI standards | SASB | TCFD

GRI standard	Disclosure	Answer
GRI 2: General disclosures	2-1 Organizational details	Cloudflare, Inc. 101 Townsend Street, San Francisco, CA Cloudflare office locations 10-K filing
	2-3 Reporting period, frequency and contact point	This annual report covers all of Cloudflare's global operations. The reporting period is calendar year (CY) 2025, unless otherwise stated. 10-K filing 10-Q filing Contact point: impact@cloudflare.com
	2-5 External assurance	Cloudflare's greenhouse gas emissions were externally verified. No other section of this report was externally verified.
	2-7 Employees	10-Q Diversity, Equity, and Inclusion at Cloudflare Cloudflare does not have a significant portion of its organizational activities performed by workers who are not employees.
	2-9 Governance structure and composition	Proxy statement
	2-23 Policy commitments	Sustainability resources: • Governance Documents • Code of Business Conduct and Ethics • Third Party Code of Conduct • Modern Slavery Act Statement • Human Rights Policy • Trust Hub • Privacy Policy
	2-25 Processes to remediate negative impacts	Human Rights Policy Cloudflare Trust Hub: Our approach to abuse
	2-28 Membership associations	Cloudflare participates in the following trade associations: BSA, ITI, i2c, CCIA, TechUK, Eco, Bitkom, Germany Secure Online (Deutschland sicher im Netz), ISPA, American Chamber of Commerce Japan, US-India Business Council, National Association of Chief Information Officers, Australian Information Industry Association, Wirtschaftsrat, digitalswitzerland, and US-China Business Council.

GRI standards | SASB | TCFD

GRI standard	Disclosure	Answer
GRI 201: Economic performance	201-2: Financial implications and other risks and opportunities due to climate change	10-K filing See TCFD disclosures
GRI 205: Anti-corruption	205-2: Communication and training about anti-corruption policies and procedures	All employees, including senior managers, complete training on bribery and anti-corruption at onboarding, and as part of annual training and certification. Cloudflare conducts a thorough screening of each supplier, reseller, and partner at onboarding and with real-time monitoring to ensure the company is not partnering with companies that pose a high risk of corruption.
	205-3: Confirmed incidents of corruption and actions taken	Cloudflare is aware of no incidents of corruption as described in 205-3 among its employees. As a result, no employee was dismissed or disciplined for corruption. Cloudflare is aware of no incidents of corruption among its contracted business partners. As a result, no related contract was terminated or discontinued on that basis. Cloudflare is aware of no associated legal cases brought against Cloudflare or its employees.
GRI 206: Anti-competitive behavior	206-1: Legal actions for anti-competitive behavior, anti-trust, and monopoly practices	Cloudflare was involved in no legal actions regarding anti-competitive behavior, antitrust, or monopoly practices.
GRI 207: Tax	207-1: Approach to tax	Cloudflare's tax strategy and decisions are evaluated by internal tax professionals and are supplemented by the advice of outside advisers. The executive finance organization as a whole plays a role in all tax decisions and tax planning opportunities. Cloudflare's approach to compliance is conservative and disciplined. Its internal tax team monitors the activities of the business, ensuring that appropriate care is applied in relation to all processes that could materially affect its compliance with its tax obligations. Cloudflare is committed to accurately filing its tax returns and remitting tax payments on a timely basis. Furthermore, Cloudflare actively monitors changes in tax laws, regulations, rules, and reporting requirements as part of its routine procedures in financial and tax reporting.
GRI 302: Energy	302-1: Energy consumption within the organization	Cloudflare consumed no non-renewable energy as defined under GRI 302 in CY2024. Cloudflare consumed 185.89 gigawatt hours (GWh) total energy in CY2024. All consumed energy was obtained through grid electricity. Cloudflare matched its grid consumed electricity with renewable energy purchases as part of its commitment to 100% renewable energy. Cloudflare did not sell any renewable energy in 2024.

GRI standards | SASB | TCFD

GRI standard	Disclosure	Answer
GRI 302: Energy *(continued)*	302-3: Energy intensity	Based on 2024 total revenue and energy data, Cloudflare consumed .001078 megawatt hours (MWh) of energy for every dollar of revenue generated.
	302-4: Reduction of energy consumption	Cloudflare has applied to join the Science Based Targets initiative (SBTi), and has started work developing carbon reduction targets.
GRI 303: Water and effluents	303-1: Interactions with water as a shared resource	Based on Cloudflare's business model and operations, water and effluents as described in 303-1 through 303-5 are not a material issue for the company. Cloudflare's water consumption is primarily the result of consumption at its office facilities, which are generally leased facilities in multi-tenant buildings. Cloudflare continues to take steps to reduce the amount of water consumed at its facilities. For example, as part of redesigning its San Francisco office in 2022, Cloudflare installed a 500-gallon rainwater harvesting tank that is now used for plant watering.
GRI 305: Emissions	305-1: Direct (Scope 1) GHG emissions	See emissions data, page 40. Cloudflare recorded Scope 1 location-based emissions of 198 metric tons (MT) carbon dioxide equivalent (CO2e) in 2024. Cloudflare used the operational control consolidation approach, under the GHG Protocol. Emissions Inventory 2024
	305-2: Energy indirect (Scope 2) GHG emissions	See emissions data, page 40. Cloudflare recorded the following Scope 2 emissions in 2024: Location-based emissions: 62,782 metric tons (MT) carbon dioxide equivalent (CO2e). Market-based emissions: 0 MT CO2e. Emissions Inventory 2024
	305-3: Other indirect (Scope 3) GHG emissions	Cloudflare Emissions Inventory 2024
	305-4: GHG emissions intensity	Based on its CY2024 location-based emissions, Cloudflare emitted .000038 MT (CO2e) per dollar of revenue generated. Cloudflare emitted 0 market-based emissions in CY2024.
	305-5: Reduction of GHG emissions	Cloudflare has committed to setting near-term company-wide emissions reductions in line with climate science with the Science Based Targets initiative (SBTi).

GRI standards | SASB | TCFD

GRI standard	Disclosure	Answer
GRI 306: Waste	306-1: Waste generation and significant waste-related impacts	Cloudflare's most significant waste-related impact is electronic waste related to the company's global network, particularly servers and networking equipment. To mitigate the waste-related impact associated with its network, Cloudflare has implemented sustainability principles at every stage of its hardware design, procurement, servicing, and decommissioning processes. To process remaining waste, Cloudflare contracts with third-party providers to maximize value and reduce waste. Cloudflare will continue to work with all of its suppliers to obtain additional data on its waste-related impacts.
GRI 308: Supplier environmental assessment	308-1: New suppliers that were screened using environmental criteria	Third Party Code of Conduct
GRI 403: Occupational health and safety	403-1: Occupational health and safety management system	Cloudflare's global Safe and Healthy Workplace Policy confirms Cloudflare's commitment to maintaining a safe and healthy work environment for its employees, customers, vendors, and all others with whom employees come into contact during their work. Among other topics, the policy explains the responsibility that is shared for following Cloudflare's safety policies and instructions, encourages the reporting of potential hazards as well as injuries and accidents to the company, describes its reporting process, and shares additional health and safety resources and programs that are provided by Cloudflare. Cloudflare maintains global incident response plans which include accident reporting procedures, safety monitoring, and incident after action review.
	403-2: Hazard identification, risk assessment, and incident investigation	Cloudflare's health and safety program includes office health and safety audits. Results of the audit are reviewed by the Places, Physical Security, Employee Legal, and People teams for proactive hazard identification and remediation. The program also includes a post-incident after-action review to identify incident causes and implement necessary prevention measures.
	403-5: Worker training on occupational health and safety	At all office locations, Cloudflare conducts evacuation drills and has safety signage in place. We've also implemented global workplace violence prevention training in all offices.
	403-9 Work-related injuries	Cloudflare experienced no high-consequence work-related injuries in 2025.
	403-10: Work-related ill health	Work-related ill health is reported according to our Incident Response Plan. Upon notification, measures are taken to document the incident, contain the spread, and reduce impact. Incidents impacting multiple employees are reviewed for root cause analysis and implementation of preventative measures.
GRI 404-1: Diversity and equal opportunity	404-1: Average hours of training per year per employee	Of the employees who participated in development training for 2025, they completed a total of 36,738 hours. On average, each employee completed 6.40 hours of training.
GRI 405-1: Diversity and equal opportunity	405-1: Diversity of governance bodies and employees	Cloudflare Diversity, Equity, and Inclusion

GRI standards | SASB | TCFD

GRI standard	Disclosure	Answer
GRI 405-2: Diversity and equal opportunity	405-2: Ratio of basic salary and remuneration of women to men	Cloudflare conducts an internal pay parity analysis at least once a year. We also look at comp outcomes across gender and ethnicity following our compensation planning process. Cloudflare has committed to the EU Charter, the UK Tech Talent Charter, and the German Diversity Charter. Cloudflare Diversity, Equity, and Inclusion
GRI 407: Freedom of association and collective bargaining	407-1: Operations and suppliers in which the right to freedom of association and collective bargaining may be at risk	Cloudflare recognizes and respects its employees' right to freedom of association and collective bargaining within federal and local laws and regulations. Cloudflare is also committed to the ILO Declaration on the Fundamental Principles and Rights at Work. Please see the Cloudflare Impact page for a link to the Human Rights Policy. Cloudflare is not aware of any operations in 2025 in which the rights of employees to freely associate or collectively bargain were at risk.
GRI 408: Child labor	408-1: Operations and suppliers at significant risk for incidents of child labor	Cloudflare is committed to the ILO Declaration on the Fundamental Principles and Rights at Work, including the prohibition on the use of child labor in its operations or among its suppliers. Human Rights Policy Third Party Code of Conduct Modern Slavery Act Statement
GRI 409: Forced or compulsory labor	409-1: Operations and suppliers at significant risk for incidents of forced or compulsory labor	Cloudflare continues to explicitly prohibit forced or compulsory labor in its operations and among its suppliers. Modern Slavery Act Statement Cloudflare is not aware of any of its operations or suppliers that have significant risks for incidents of forced or compulsory labor. Although Cloudflare has identified no significant risk of forced or compulsory labor, it continues to regularly review its partners, resellers, suppliers, and vendors to ensure compliance with its policy.
GRI 414: Supplier social assessment	414-1: New suppliers that were screened using social criteria	Cloudflare's procurement team implemented a new software tool in 2025 that will enable the company to screen suppliers against risks, including environmental, social, and governance criteria.
GRI 415: Public policy	415-1: Political contributions	Cloudflare made no political contributions in 2024, and does not operate a Political Action Committee.
GRI 418: Customer privacy	418-1: Substantiated complaints concerning breaches of customer privacy and losses of customer data	Please see TC-SI-230a.1.

GRI Standards | **SASB** | TCFD

SASB - Technology and communications sector — Software and IT services

Topic	Code	Accounting metric	Answer
Environmental footprint of hardware infrastructure	TC-S1-130a.2	(1) Total water withdrawn, (2) total water consumed; percentage of each in regions with High or Extremely High Baseline Water Stress	See GRI 303.
	TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	Cloudflare includes both energy efficiency and carbon intensity in its data center strategic planning. Cloudflare also continuously designs and deploys energy-efficient hardware in its data centers to minimize its overall energy footprint per workload.
Data privacy and freedom of expression	TC-SI-220a.1	Description of policies and practices relating to behavioural advertising and user privacy	Privacy Policy Cloudflare Cookie Policy
	TC-SI-220a.2	Number of users whose information is used for secondary purposes	Cloudflare only processes personal information of customers and end users (as defined in our Privacy Policy) for the purposes of providing the Cloudflare service, which includes ongoing assessment of traffic patterns, security threats, and network operations in order to monitor the health of and improve the service.
	TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Cloudflare did not experience any monetary losses as the result of legal proceedings associated with customer privacy.
	TC-SI-220a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	Cloudflare receives requests for different kinds of data on its users from US and foreign governments, courts, and those involved in civil litigation. It provides a detailed report on these requests in the semiannual Transparency Report.

GRI standards | **SASB** | TCFD

SASB - Technology and communications sector — Software and IT services

Topic	Code	Accounting metric	Answer
Data privacy and freedom of expression *(continued)*	TC-SI-220a.5	List of countries where core products or services are subject to government required monitoring, blocking, content filtering or censoring.	An essential part of earning and maintaining the trust of our customers is being transparent about the legal requests for customer information that we receive from government entities and private parties. To this end, and consistent with the transparency reporting obligations under the European Union's (EU) Digital Services Act (DSA), Cloudflare publishes semiannual updates to our Transparency Report on the requests we have received to disclose information about our customers. We list on our Transparency Center some things that Cloudflare has never done and would resist through all available legal remedies in order to protect our customers from illegal or unconstitutional requests. More details regarding how Cloudflare responds to legal demands can be found in our Trust Hub. In 2024, Cloudflare expanded the content of its report to better align with provisions included in the Digital Services Act. For example, it now includes categories of hosted content abuse, automated steps Cloudflare has taken to mitigate phishing and technical abuse, average response time to certain abuse reports, and additional types of law enforcement requests. Cloudflare also provides machine-readable versions of its data, alongside "additional content" descriptions, which provide information on trends and notable developments. Cloudflare also recently separated its Transparency Report into two parts. The company's Report on Legal Requests for Information includes information on law enforcement, government, and civil requests for customer information. The company's Abuse Processes Report addresses Cloudflare's processes for handling reports of abuse on websites using our services, and response to legal requests to terminate or restrict access to those services for certain users. Transparency Report
Data security	TC-SI-230a.1	(1) Number of data breaches, (2) percentage that are personal data breaches, (3) number of users affected	Earlier this year, a threat actor breached Salesloft Drift, which operated a chat agent integrated with Cloudflare's Salesforce instance. As a result, the threat actor was able to access Cloudflare customer contact information and support case data stored in our Salesforce instance. In three instances, individuals that had provided Cloudflare with their Social Security numbers (which is not information Cloudflare solicits or requires from customers) were provided notice in accordance with applicable US state data breach notification laws. Cloudflare experienced no other incidents involving personally identifiable information (PII) requiring notification under applicable data protection law. For detailed information regarding the Salesloft and Salesforce breach, visit the Cloudflare Blog.
	TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Cloudflare has implemented a formal security and privacy program that adheres to industry standards such as ISO 27000, 27701, and 27018; PCI DSS; SOC 2 Type II; Global CBPR, Global PRP, FedRAMP Moderate; ENS, IRAP and C5; and has been evaluated by third-party assessors against the requirements. Cloudflare Trust Hub

GRI standards | **SASB** | TCFD

SASB - Technology and communications sector — Software and IT services

Topic	Code	Accounting metric	Answer
Environmental footprint of hardware infrastructure	TC-S1-130a.1	(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable	Cloudflare consumed 177.89 gigawatt hours (GWh) total energy in CY2024. All consumed energy was obtained through grid electricity. Cloudflare matched its grid consumed electricity with renewable energy purchases as part of its commitment to 100% renewable energy. Cloudflare did not sell any renewable energy in 2024. Emissions Inventory 2024
Recruiting and managing a global, diverse and skilled workforce	TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore	Percentage of employees that are foreign nationals per country: • US 11% • Canada 15% • UAE 100% • UK 37% • Netherlands 57% • China 0% • Portugal 34% • France 22% • Korea 3% • Singapore 36% • Japan 16% • Malaysia 3% • Germany 34% • Mexico 4% • Belgium 100% • Australia 20% • India 0% • Sweden 13% Percentage of employees located offshore: 0%
	TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	Cloudflare diversity, equity, and inclusion
Intellectual property protection and competitive behaviour	TC-SI-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations.	Cloudflare incurred no monetary losses resulting from anti-competitive behavior regulations.

GRI standards | **SASB** | TCFD

SASB - Technology and communications sector

Software and IT services

Topic	Code	Accounting metric	Answer
Managing systemic risks from technology disruptions	TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Transparency is one of Cloudflare's core values. We believe in being transparent about our products, decision-making, and impacts, as well as any performance, disruptions, or outages associated with our network. Apart from formal Sustainability disclosures, the company regularly provides detailed information on its blog and in other public disclosures about such incidents, including their scope, effect, and technical details. Cloudflare is potentially subject to regulatory obligations related to similar network disruptions or related incidents, including potentially under the NIS2 Directive. As a result, Cloudflare elected not to disclose information under TC-SI-550a.1; however, we will continue to communicate with the public regarding future service issues consistent with our regulatory obligations as appropriate.
	TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	10-Q Filing

GRI standards | SASB | **TCFD**

TCFD	Accounting metric	Answer
Section 1. Governance	A. Describe the board's oversight of climate-related risks and opportunities.	The Nominating and Corporate Governance Committee is responsible for overseeing policies and practices related to environmental or climate-related matters and initiatives. The committee receives annual briefings from management on those issues. See Nominating and Corporate Governance Committee Charter.
	B. Describe management's role in assessing and managing climate-related risks and opportunities.	Cloudflare's climate commitments, including assessment of risks and opportunities, were approved by the company's senior executive team. In 2025, the company hired an external consulting firm to conduct an independent climate risk assessment as recommended in the TCFD framework. As part of the exercise, a cross-functional team of executives, department heads, and senior managers—including Legal, Public Policy, Finance, Infrastructure, Places, Impact, Investor Relations, and Product—assessed physical and transition risks and opportunities facing the company. The findings from that assessment will help guide future risk assessments moving forward. Cloudflare's Impact team is responsible for day-to-day management of the company's climate commitments, disclosures, and strategy. The Impact team also briefs the Board of Directors on relevant climate issues annually.
Section 2. Strategy	A. Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term.	As part of its climate risk assessment exercise, Cloudflare identified the following climate-related risks over the short, medium, and long term: regulatory risks, related to environmental disclosure and hardware requirements; reputational risk associated with inconsistent expectations among regulators and markets; physical risks, including network locations and potential disruption from climate-related events, rising temperatures, and higher demand for energy and cooling services. In terms of opportunities, part of Cloudflare's core business is providing cloud-based enterprise networking services to compete with legacy on-premises hardware. In addition to performance and other benefits, this migration could also provide a significant energy and climate efficiency gain. Numerous studies have documented the energy efficiency gains associated with migrating to cloud services, including an independent study commissioned by Cloudflare in 2023. Providing a more efficient alternative to legacy on-premises hardware could create opportunities for Cloudflare as businesses and regulators scrutinize energy consumption associated with IT infrastructure.
	B. Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning.	Energy consumption is a cost of operating Cloudflare's network. As a result, Cloudflare has a direct business incentive to prioritize energy efficiency investments in its hardware, network, and products. Cloudflare's investments in energy efficiency are fully integrated into the company's standard operating and capital budgets, rather than being treated as standalone or separate climate initiatives.

GRI standards | SASB | **TCFD**

TCFD	Accounting metric	Answer
Section 2. Strategy *(continued)*	C. Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario.	Cloudflare conducted a climate scenario analysis of the company's risk and mitigation under two scenarios developed by the Intergovernmental Panel on Climate Change (IPCC). The first was a worst-case ("business as usual") high emissions scenario (RCP 8.5), and the second was an intermediate scenario with emissions peaking around 2040 and then declining (RCP 4.5). The analysis found that Cloudflare could experience additional risk associated with regulatory changes, compliance costs, extreme weather events, and chronic temperature increases, which could raise costs and result in temporary outages at individual data center locations. However, the analysis also found that the company had mitigation strategies associated with those risks, notably the resilience and redundancy of its global network, network efficiency investments, climate commitments and reporting, and compliance efforts. The analysis also found potential opportunities as described in subsection (A).
Section 3. Risk management	A. Describe the organization's processes for identifying and assessing climate-related risks.	In 2025, Cloudflare conducted an independent climate scenario analysis that featured a comprehensive assessment of regulatory, reputational, extreme weather, and rising temperature risks. Individual teams also incorporate climate and resilience factors into their specific operational and strategic planning. The company continues to implement measures across the organization to mitigate these risks.
	B. Describe the organization's process for managing climate-related risks.	Cloudflare continues to take steps across the organization to manage climate-related risks. Cloudflare's climate scenario analysis identified a number of initiatives across the company for managing climate-related risks, including the resilience and redundancy of its global network, network efficiency investments, climate commitments and reporting, and compliance.
	C. Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management.	Climate risks are regularly evaluated by teams managing processes with potential climate impacts, including Legal, Public Policy, Finance, Infrastructure, Places, and Impact. Cloudflare will continue to assess the findings of its recent climate scenario analysis to determine if further integration into risk management processes is required.
Section 4. Metrics and targets	A. Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process.	See Cloudflare's 2024 Emissions Inventory. See also GRI, SASB disclosures.

GRI standards | SASB | **TCFD**

TCFD	Accounting metric	Answer
Section 4. Metrics and targets *(continued)*	B. Disclose Scope 1 and Scope 2, and, if appropriate, Scope 3 greenhouse gas emissions and the related risks.	See Cloudflare's 2024 Emissions Inventory.
	C. Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets.	Cloudflare has committed to setting near-term targets consistent with SBTi requirements.

Emissions verification letter

Stakeholder Letter

Cloudflare
101 Townsend St
San Francisco, CA 94107

Shift Advantage
3004 NE 47th Ave.
Portland, OR 97213

6/23/2025

Dear Patrick,

Shift Advantage is pleased to provide consulting and advisory services to Cloudflare to support the calculation of Cloudflare's 2024 greenhouse gas emissions. Shift Advantage conducted this independent and impartial limited level of assurance verification of Cloudflare's annual emissions disclosure data in accordance with the standard ISO 14064-part 3 2nd Edition, 2019-04, Annex A against criteria as set forth in the Greenhouse Gas Protocol. This letter is to clarify matters set out in the assurance report. It is not an assurance report and is not a substitute for the assurance report. This letter and the assurance report, including the opinion(s), are solely for Cloudflare's benefit. Shift Advantage consents to the release of this letter but without accepting or assuming any liability on Shift Advantage's part to any other party who has access to this letter or assurance report.

The assurance report covers Cloudflare's 2024 calendar year operations. For Cloudflare's GHG emissions report Cloudflare uses an operational control approach that includes global offices and data centers. Cloudflare's emissions report covers Scope 1, Scope 2, and a portion of Scope 3 GHG emissions (3.1- Purchased Goods and Services, 3.2- Capital Goods, 3.4- Upstream Transportation and Distribution, and 3.5- Waste).

Madison Spinelli
Shift Advantage
www.shiftadvantage.com

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

REV:BDES-8459.2025DEC18