



# Impact Report



ESG

**We are proud to share our 2023 Impact Report. It is a collection of our work over the past year to advance our mission — to help build a better Internet — and to find new ways to help the Internet do good in the world.**

Cloudflare is officially a teenager. We launched on September 27, 2010. This year we celebrated our thirteenth birthday, and like most kids, it was an important and exciting year for our company.

At the same time, it is impossible to ignore all of the ways that the world has become more complicated over the past year. Although we continue to be inspired by the resilience and resolve of Ukrainian people, the war in Ukraine continues with no sign of abatement. All of us watched in horror at the recent terrorist attacks by members of Hamas on Israeli citizens, and the ongoing suffering resulting from the war in Gaza.

In addition to conflicts on the ground, we also see increased attacks on the Internet: outages in Gaza, cyber attacks in Israel, Internet shutdowns stifling protests in Iran and elsewhere, sophisticated attacks like the HTTP/2 Rapid Reset vulnerability, and increased attacks on journalists and independent media. We are also deeply concerned about the growing number of regulations and other legal requirements in a number of countries that could threaten the future of an open and interconnected Internet.

As we release this year's report, despite all of these challenges, our company remains committed to our mission to help build a better Internet, which feels more important now than ever.

- As part of the White House's Back to School Safely: K-12 Cybersecurity Summit, we announced a program to provide free services to help protect under-resourced K-12 public school districts in the United States. Our Cybersafe Schools initiative is a continuation of our effort to help protect important but underfunded critical infrastructure around the world.

- This year was one of amazing growth for AI. Cloudflare announced our goal to bring affordable, powerful AI inference to anyone, anywhere on Earth, along with new transparency, controls, and privacy protections to help support responsible development.
- We celebrated the 9th anniversary of Project Galileo by reporting on cyber attack trends against vulnerable organizations like those that support LGBTQ+ rights, human rights defenders, reproductive rights, and civil society in Ukraine. We also announced a new partnership with the CyberPeace Institute to help small development and humanitarian organizations better protect themselves and share threat intelligence.
- We continued our effort to help build a more sustainable Internet. This year, an independent study found that migrating from on-premises hardware to Cloudflare's cloud-based services can reduce related carbon emissions between 78% and 96%. We also announced our commitment to set carbon reduction targets through the Science Based Targets initiative (SBTi).

Most importantly, we are proud to continue working with and supporting people and organizations around the world that are standing up for the Internet.



**Matthew Prince**  
Co-Founder & CEO,  
Cloudflare



**Michelle Zatlyn**  
President & COO,  
Cloudflare



# Contents

## Introduction

- 2 Letter from the founders
- 4 Expanding our impact
- 5 Spotlight 2023: Shielding schools from online attacks
- 6 Celebrating Birthday Week 2023

## A better Internet is principled

- 8 Engaging with and protecting civil society online
- 10 Project Galileo
- 11 Helping keep elections safe and secure
- 12 Athenian Project
- 13 Engineering privacy into the Internet
- 14 Working together to secure the Internet
- 15 Complying with privacy and security certifications
- 16 Committing to human rights principles
- 17 Building trust through transparency
- 18 Operating with integrity

## A better Internet is for everyone

- 20 Democratizing access to responsible artificial intelligence
- 21 Securing infrastructure with Project Safekeeping
- 22 Helping promote democratic values online
- 23 Supporting access to an open Internet
- 24 Expanding our network and improving access
- 25 Building community at Cloudflare
- 26 Prioritizing diversity at Cloudflare
- 27 Improving the Internet through transparency

## A better Internet is sustainable

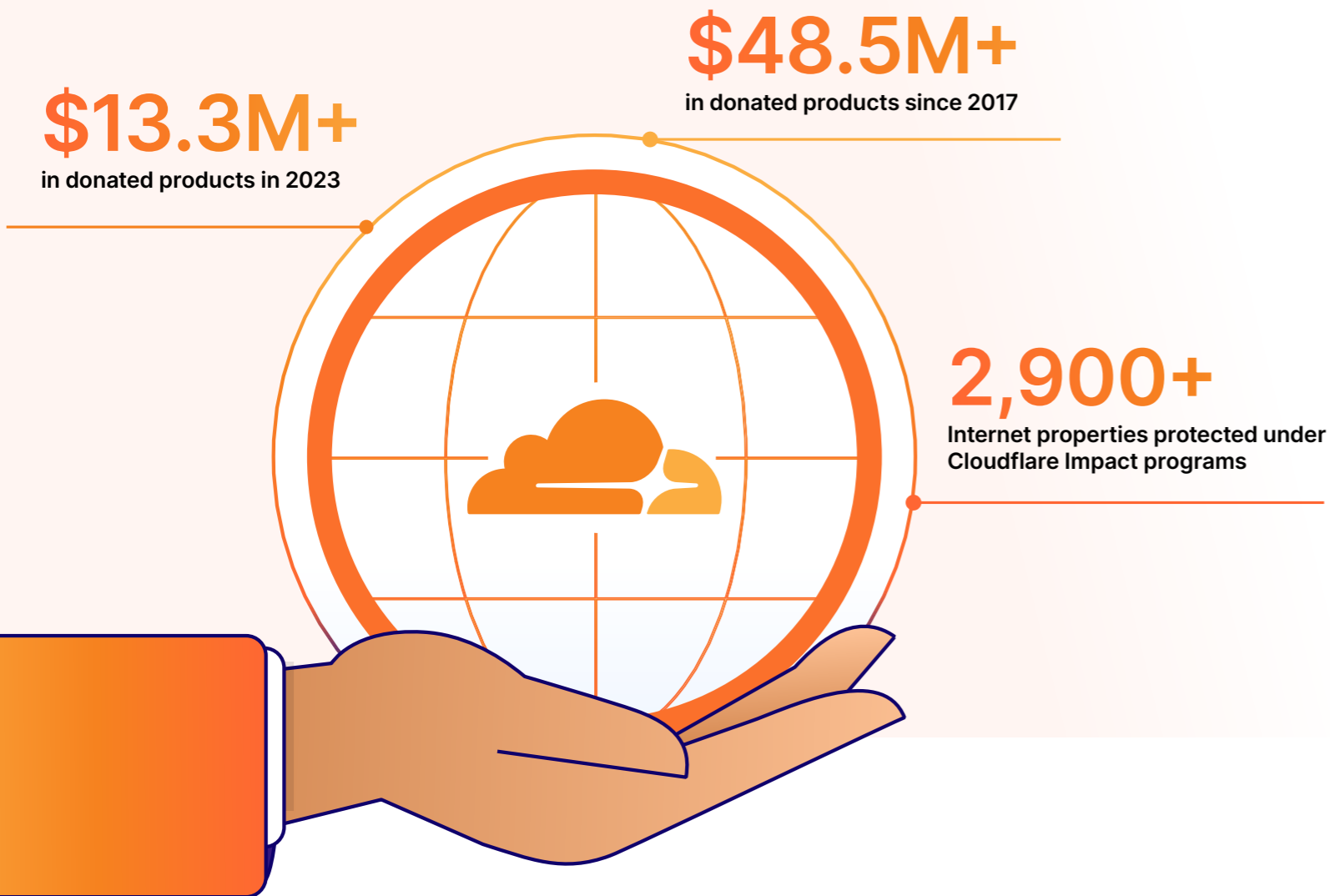
- 29 Cutting emissions by moving to the cloud
- 30 Cloudflare sustainability
- 31 Tracking Cloudflare emissions
- 32 Restoring forests and habitats

## Appendix

- 34 Compliance tables
- 44 Emissions verification letter

# Expanding our impact

Cloudflare Impact encompasses our programs that help Cloudflare and the Internet do good in the world, including our environmental, social, and governance initiatives.



## Most Loved Workplaces

We held onto our spot on Newsweek's 100 Most Loved Workplaces 2023, keeping our ranking of #55. Newsweek and BPI surveyed more than two million employees across companies, asking about collaboration, values, and respect.



## Growing our presence in Portugal

In November, we were honored by the tech magazine Exame Informática for our beneficial impacts on the Portuguese economy. Cloudflare received a Fast Mover award in the area of employment because of the growth of our tech talent team and our local investments.

## SUSTAINABLE DEVELOPMENT GOALS



## 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.



## Pledge 1%

Through our commitment to Pledge 1%, Cloudflare pledges 1% of our time and products to give back to our communities.

# Spotlight 2023: Shielding schools from online attacks

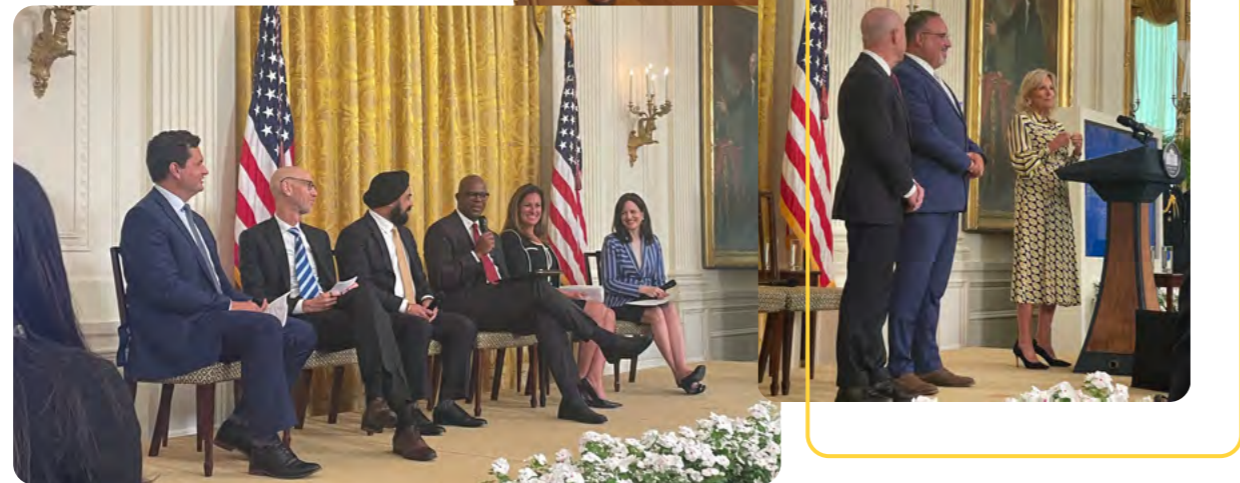
## Cloudflare announced Project Cybersafe Schools at the White House's Back to School Safely: K-12 Cybersecurity Summit in August 2023.

Cloudflare provides eligible school districts with Zero Trust cyber security solutions that help minimize exposure to harmful online content and common cyber threats such as phishing and credential harvesting. We provide these products for free and with no time limit.

This program was inspired by ongoing conversations with fellow members of the Joint Cyber Defense Collaborative. Cloudflare worked with officials from the Cybersecurity & Infrastructure Security Agency (CISA), the Department of Education, and the White House to determine how we could partner to protect K-12 schools in the United States from cyber threats, particularly since small schools often lack the resources and capacity to combat evolving threats.

[Apply for Project Cybersafe Schools at cloudflare.com/lp/cybersafe-schools.](https://cloudflare.com/lp/cybersafe-schools)

Matt Schneider and Zaid Zaid from Cloudflare. ▾






The White House's Back to School Safely: K-12 Cybersecurity Summit. >>

## Project Cybersafe Schools



### Program participants



### Eligibility requirements

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

### The offering

-  **Area 1 Cloud Email Security**  
Safeguards inboxes by stopping sophisticated threats such as phishing and credential harvesting.
-  **Gateway DNS Filtering**  
Protects against threats by preventing users from reaching unwanted or harmful online content.



Every day, our schools face cyber attacks that can slow Internet access, threaten leaks of confidential student data, and hinder their ability to teach children in a secure online space."

Matthew Prince, CEO and Co-Founder, Cloudflare

# Celebrating Birthday Week 2023

Cloudflare is now 13! Each year, we celebrate our birthday with a full week of announcements about new products and features that we think of as giving back to the Internet.

## Enabling the future

Cloudflare announced a series of new products and services including Workers AI, AI Gateway, and Vectorize that are designed to make AI inference more open, accessible, scalable, affordable, and transparent for everyone. We also announced new partnerships and integrations with some of the leading companies in AI development: NVIDIA, Microsoft, Hugging Face, Databricks, and Meta.

## Connectivity cloud

A connectivity cloud is a new approach for delivering the many services that organizations need to secure and connect their digital environment. It's a unified, intelligent platform of programmable cloud-native services that enable any-to-any connectivity between all networks, cloud environments, applications, and users. It includes a huge array of security, performance, and developer services — not with an eye to replace everything everywhere, but with the ability to fit in wherever needed and consolidate many critical services onto a single platform.

## Making CAPTCHAs more accessible and private (now for everyone)

Cloudflare's CAPTCHA replacement product Turnstile is now available to anyone for free, regardless of whether they are using our services. Cloudflare's CAPTCHA replacement requires no human interaction, and is easier and more accessible for users with a visual or auditory disability. It also does not track users or collect their personal data for advertising.

Visit [cloudflare.com/birthday-week](https://cloudflare.com/birthday-week) to get the full recap of all of our Birthday Week 13 announcements.



# A better Internet is principled.

# Engaging with and protecting civil society online

Meaningful consultation with civil society, human rights defenders, journalists, and other stakeholders is a fundamental part of helping build a better Internet. Ensuring these communities are able to contribute and provide feedback on our work is an important part of our mission.

We are proud to continue supporting vulnerable communities online by providing access to free services that help protect against DDoS and other cyber attacks.



## Engaging with human rights defenders

Cloudflare was pleased to sponsor RightsCon 12 in Costa Rica in 2023, which included more than 8,100 participants from 174 countries. RightsCon is hosted by Access Now, and is the world's leading summit on human rights in the digital age. Human rights defenders and a variety of other activists join RightsCon to articulate their security needs and on-the-ground experiences, and engage with companies on the future of the Internet and related technologies. We also see similar communities engage at events like the Global Gathering, an event in Lisbon hosted by Team COMMUNITY that brought together digital defenders working at the intersection of human rights and technology, and the Internet Governance Forum (IGF).

Cloudflare had the opportunity to meet in person with many of our Project Galileo partners and participants at these events to discuss how to improve our support for human rights defenders through Project Galileo, improve transparency of Internet events, and better protect vulnerable voices online.

8,100 participants

174 countries



Photos courtesy of Access Now. >>





## Partnering with CyberPeace Institute

Cloudflare is working with the CyberPeace Institute to make it easier for small development and humanitarian organizations to protect themselves with Cloudflare's Area 1 email security tools, and share threat intelligence about cyber attacks. As part of the partnership, CyberPeace Institute will onboard organizations participating in their CyberPeace Builders programs directly onto Cloudflare services through Project Galileo. CyberPeace Institute will be able to collectively manage security services and monitor attack trends across the program.

## Sharing information about attacks against civil society

More than 2,400 civil society and nonprofit Internet properties are protected by Cloudflare security services through Project Galileo. As a result, Cloudflare is in a unique position to monitor cyber attack trends targeting some of the most vulnerable and important voices on the Internet. Earlier this year, Cloudflare published a report analyzing cyber attacks against organizations working in the areas of LGBTQ+ issues, reproductive rights, and human rights to better equip researchers and targeted organizations with best practices for safeguarding their websites and data.

## Welcoming new partners

We were excited to welcome two new partners to our Project Galileo network this year. The International Press Institute defends media freedom, drawing on its global network of editors, media executives, and journalists. Meanwhile, the Center for Digital Resilience operates digital security and wellness programs for civil society in high-risk environments.



**As a global press freedom organization, we see every day how autocrats and powerful individuals are using the Internet to stifle journalism and free speech. We also know this firsthand, as we have been targeted by cyber attacks. Working with Cloudflare's Project Galileo gives us and our network of independent media around the world the tools to both defend ourselves and gain a better understanding of techniques used by the malevolent actors to attack the media."**

**Frane Maroević, Executive Director,**  
International Press Institute

## Nine years of Project Galileo

Cloudflare launched Project Galileo in 2014 with the simple goal of protecting free expression online. Through the program, Cloudflare provides free cyber security services to important yet vulnerable voices, like artistic groups, journalists, humanitarian organizations, and the voices of political dissent, which are commonly targeted with cyber attacks intended to take them offline.

Over the last nine years, the program has seen remarkable growth. Not only in terms of our partner organizations or the number of organizations receiving free services through the program, but also the number of expansions and other projects that were developed by working with this extraordinary group and continue to make the Internet a more secure place.

For example, Cloudflare partnered with the Digital Defense Fund to extend Project Galileo to provide digital security tools for abortion access advocates, made additional security services available to Project Galileo participants to protect not only public websites but also internal networks, worked with Project Galileo partners to develop Internet shutdown alerts through Cloudflare Radar, and worked with a number of government agencies to promote privacy-enhancing technologies and other tools for human rights defenders.

To learn more,  
please visit  
[cloudflare.com/galileo](https://cloudflare.com/galileo).



# Project Galileo

EST. 2014

Humanitarian organizations, artistic groups, and the voices of political dissent are often vulnerable to cyber attacks. In collaboration with 50+ civil society partners, Cloudflare protects public interest groups from attacks intended to silence them online.

Learn more and apply at [cloudflare.com/galileo](https://cloudflare.com/galileo)

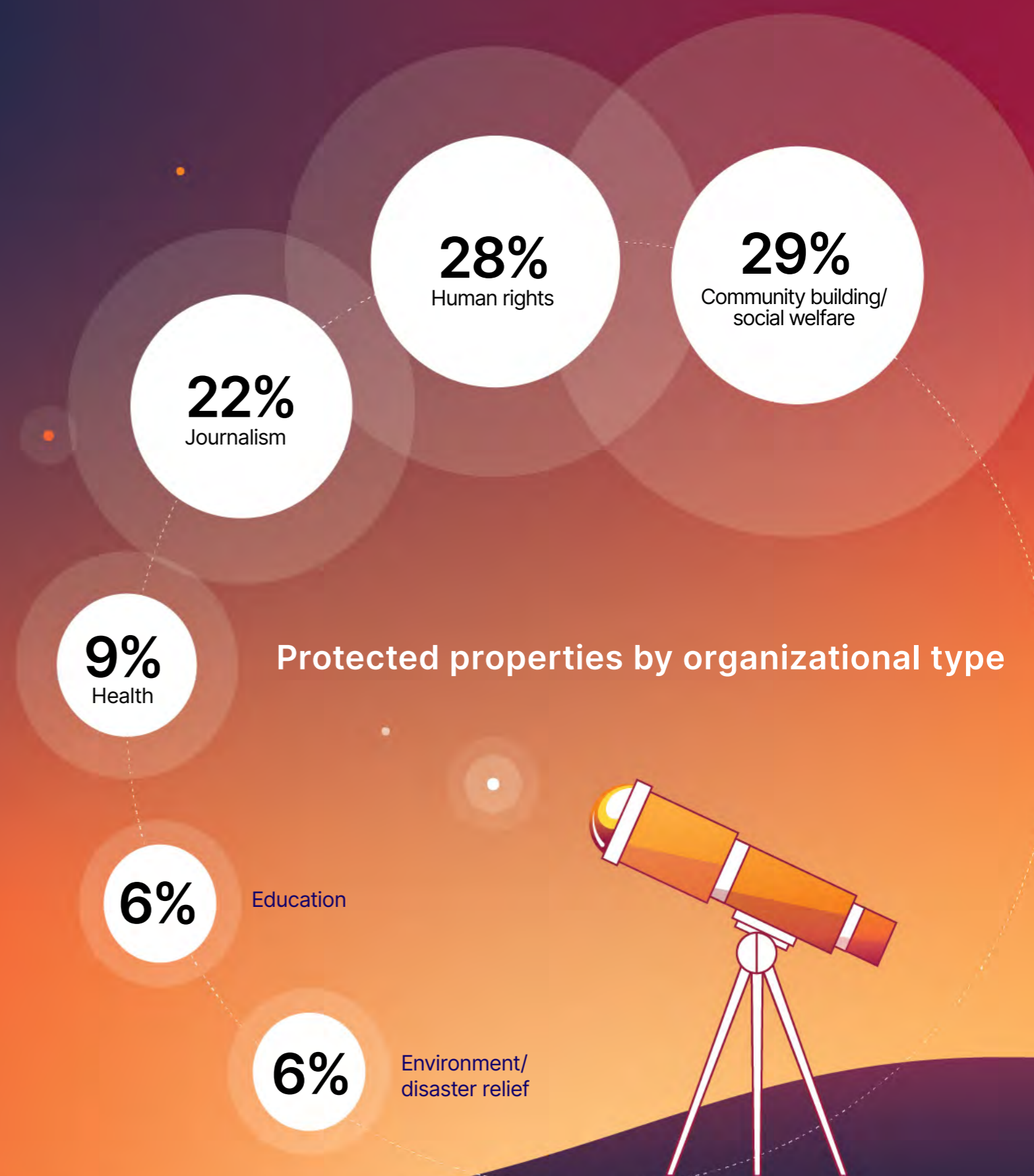
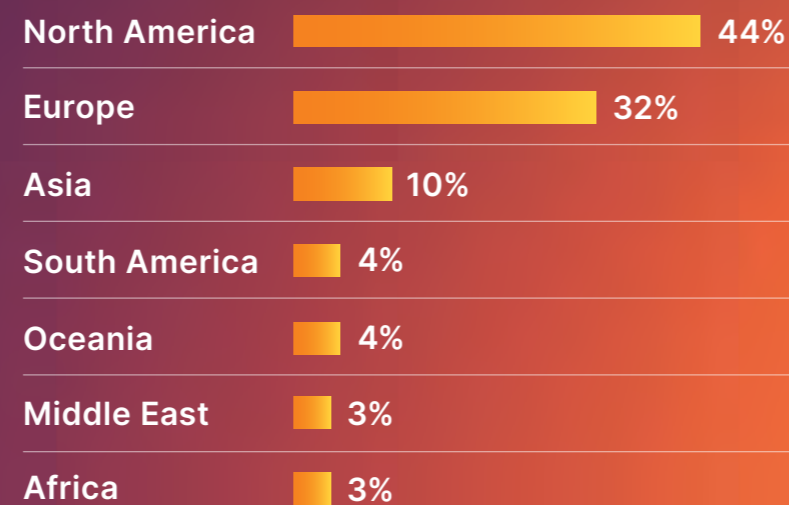


**2,400** | **111**  
Internet properties | countries

**67.7 million**  
average number of daily attacks  
Cloudflare mitigates for participants

**2 billion** | **50+**  
average number of monthly attacks  
Cloudflare mitigates for participants | partners to help identify at-risk sites

## Protected properties by region



# Helping keep elections safe and secure

We believe the Internet can play a key role in ensuring access to information and promoting democracy. By offering free support to groups within the election ecosystem, Cloudflare’s goal is to help preserve confidence in the electoral process, promote transparency, and encourage voter participation.



## Athenian Project

Cloudflare provides access to our highest level of protection and performance services for free to US state and local governments to help protect their election-related websites and internal networks, including information on voting and polling places, voter data, and the reporting of election results. 390 state and local government Internet properties in 33 US states receive free Cloudflare services through the Athenian Project.

Cloudflare is working with the International Foundation for Electoral Systems (IFES) to expand its free security services to election management bodies all over the world. For example, earlier this year, Cloudflare and IFES held security briefings for government officials, in North Macedonia and Kosovo, including on emerging threats and how to safeguard their election websites and networks.

390

state and local government domains

33 US

states receive free Cloudflare services through the Athenian Project

## Cloudflare for Campaigns

In partnership with Defending Digital Campaigns, we offer a suite of products tailored to the needs of political campaigns, particularly smaller campaigns that lack significant in-house cyber security resources. Under this partnership, we currently protect 97 political campaigns and 20 political parties in the United States.

97

political campaigns

20

political parties in the United States

## Project Galileo

Cloudflare protects more than 65 Internet properties in the United States that work on a range of topics related to voting rights and promoting free and fair elections. For those organizations, Cloudflare mitigated 19.13 million threats between November 1, 2022, and August 31, 2023, an average of 62,927 threats per day.

19.13M

threats

62,927

threats per day



“We rely on Cloudflare to help keep our online services secure so that we can focus on our mission of engaging and activating voters to expand and secure American democracy.”

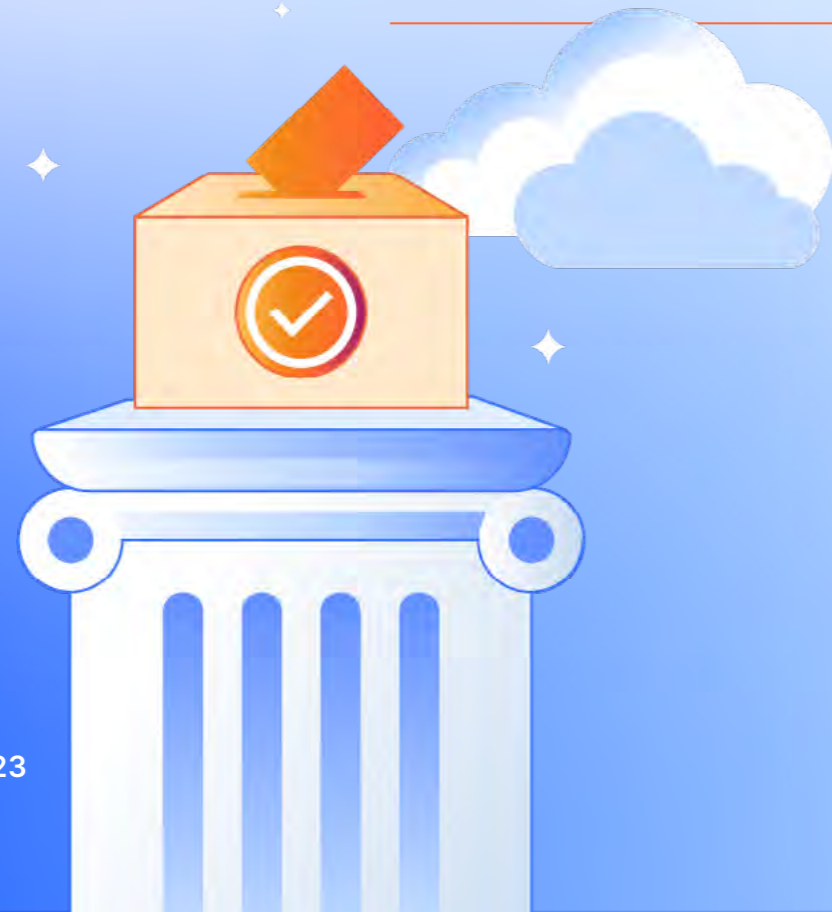
Peter Gluck, Chief Technology Officer, Vote.org

# Athenian Project

EST. 2014

We created the Athenian Project to ensure that state and local governments have the highest level of protection and reliability for free, so that their constituents have access to election information and voter registration.

Learn more and apply at [cloudflare.com/athenian](https://cloudflare.com/athenian)



## Election security at a glance

390

Internet properties protected

6

countries

33 US states

receive free Cloudflare services through the Athenian Project

213.78 million

threats to government election websites mitigated between November 1, 2022, and August 31, 2023, an average of 703,223 threats per day

“

Security is the cornerstone of any democratic process, and free and fair elections are no exception. Security products like those from Cloudflare become even more critical in an increasingly digital world. With Cloudflare, we have effectively mitigated numerous cyber threats, ensuring citizens uninterrupted access to electoral information in Kosovo. This has significantly fostered trust and transparency in our electoral processes.”

Kreshnik Spahiu, Director of the Information Technology Department, Central Election Commission of Kosovo

“

The International Foundation for Electoral Systems (IFES) is proud to partner with Cloudflare to provide election commissions around the world with cutting-edge security and tools through the Athenian Project, helping to secure their election infrastructure against cyber threats and ensuring public access to important voting information.”

Dr. Tarun Chaudhary, Cybersecurity and Diplomacy Advisor, IFES

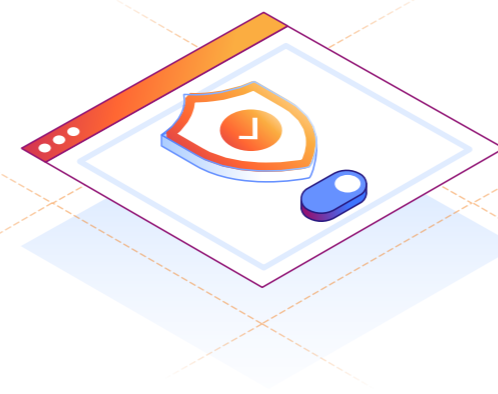
“

Cloudflare is a technology enabler for the State Election Committee (SEC) in North Macedonia, and its tools help us ensure that early election results will be accessible to the general population, thus promoting visibility and transparency.”

Vladislav Bidikov, Cybersecurity Task Force Member, State Election Commission of North Macedonia

# Engineering privacy into the Internet

The Internet was not built with privacy in mind. We are proud to support a variety of partners working to build privacy-enhancing technologies that make accessing content online more private and secure for everyone.



## More private web browsing with Cloudflare and Microsoft Edge

Cloudflare partnered with Microsoft to support a fast and secure virtual private network (VPN) directly within the Microsoft Edge web browser. Users can now turn on Microsoft's Edge Secure VPN in the Microsoft Edge settings and Cloudflare will automatically start protecting users from third-party cookies and other IP address and web browsing trackers.

Cloudflare is supporting Microsoft's Edge Secure VPN through our Privacy Proxy Platform. Using an open-source standard, our Privacy Proxy Platform establishes an encrypted tunnel and sends reliable and ordered byte streams through that tunnel. The platform also leverages other parts of Cloudflare's privacy-oriented infrastructure including 1.1.1.1 for encrypted DNS, a token proxy based on Privacy Pass for client authentication, and Geo-egress to choose an accurate IP address without exposing users' precise location.

## Benefits of the Edge Secure Network VPN

- ✓ Automatic browser traffic security
- ✓ Connection encryption
- ✓ Online tracking prevention
- ✓ Location privacy

[Learn more about Microsoft's Edge Secure Network VPN.](#)

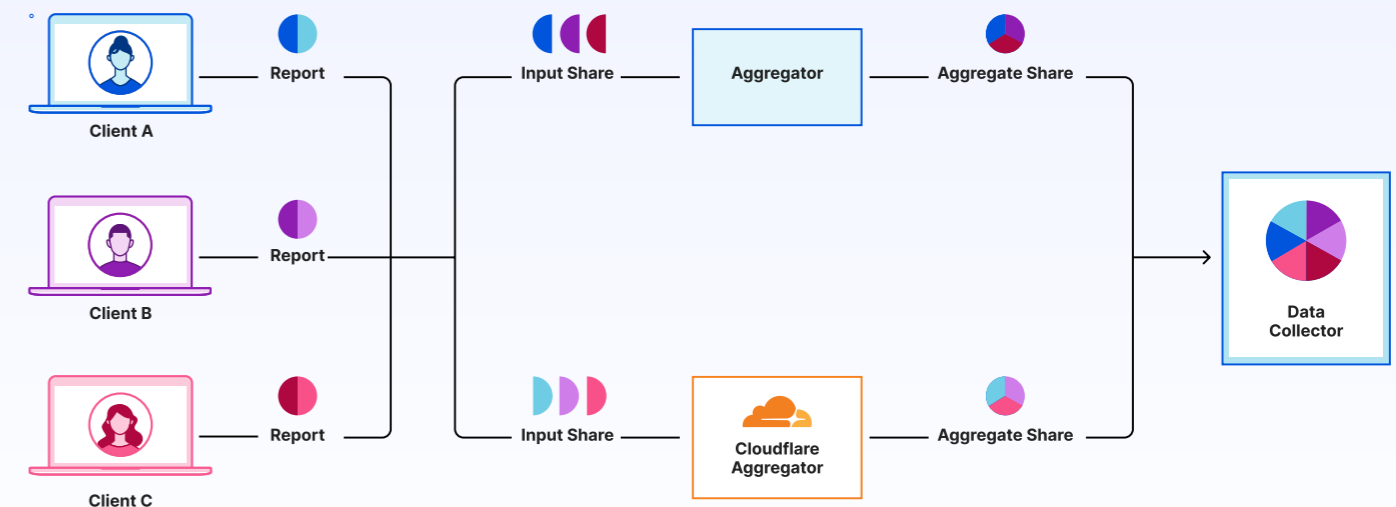
## Open standard for privacy-enhancing data collection and measurement

Cloudflare's research team has been working with a variety of stakeholders in a Privacy Preserving Measurement group at the Internet Engineering Task Force (IETF) to develop ways to collect and analyze data while also preserving privacy.

One of the open-source techniques that Cloudflare is helping develop is the Distributed Aggregation Protocol (DAP), which uses cryptography principles to allow a data collector to perform calculations on a data set without actually seeing the complete underlying data.

### Privacy-enhancing technologies supported by Cloudflare

- [Universal SSL/TLS Encryption](#)
- [Privacy Pass](#)
- [Cloudflare Data Localization Suite](#)
- [Privacy-First Web Analytics](#)
- [1.1.1.1 with WARP](#)



# Working together to secure the Internet

**Collaboration and information sharing are critical to effective cyber security. Cloudflare supports a number of initiatives that bring together public and private experts to help reduce cyber threats for everyone.**

## Sharing information on cyber threats

There is broad recognition that public-private partnerships are an increasingly essential part of modern cyber security. Organizations like the US Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC) and Information Sharing and Analysis Centers (ISACs) bring together government and private sector experts to share information about threats and vulnerabilities to improve cyber security for everyone. Cloudflare is pleased to help support these efforts to improve cyber security. During the course of this year, Cloudflare participated in JCDC's work on strengthening protections for high-risk communities that are targeted by foreign state actors, such as civil society organizations that support journalists and researchers, as well as other information sharing efforts.

## Uncovering the HTTP/2 Rapid Reset vulnerability

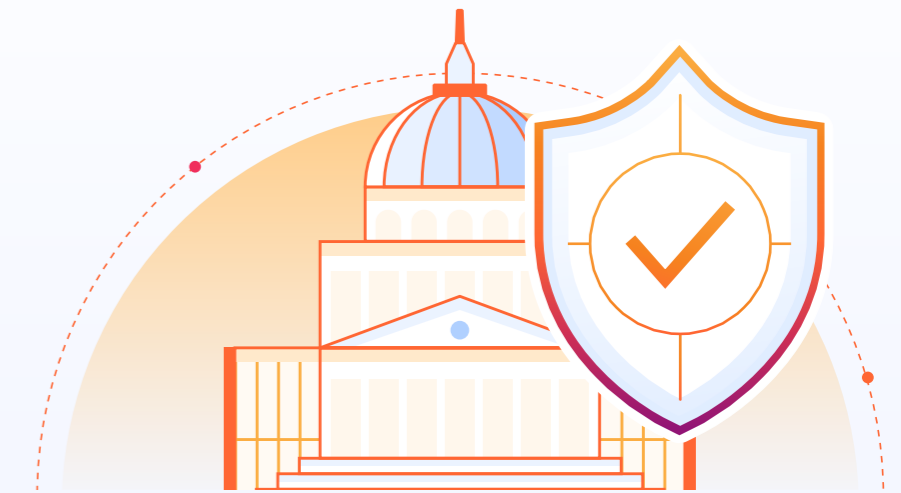
Earlier this year, Cloudflare detected a novel cyber attack vector that resulted in a series of record-breaking DDoS attacks on Cloudflare's network and across the Internet. Now known as "HTTP/2 Rapid Reset," the new type of attack was noteworthy not only because of its potential scale and intensity — Cloudflare recorded a peak of approximately 201 million requests per second on its network — but also because rather than targeting a software vulnerability with limited impact, the attacks exploited a foundational web protocol used for loading webpages all over the Internet.

As one of the first organizations to detect this exploit, Cloudflare worked across industry to defend against and mitigate the vulnerability. To that end, we worked with Google and AWS to publish an official disclosure of the [vulnerability](#); we published additional information dissecting the attacks, vulnerability, and how to address it on our [blog](#) (also available on DHS website [here](#)); and conducted extensive outreach to government and other experts to help raise awareness of the issue.

“

**Successfully mitigating this threat for every critical infrastructure organization, customer, and the Internet at-large is the lifeblood of what Cloudflare stands for. We are one of the only companies equipped to identify and address threats of this magnitude, at the speed required to maintain the integrity of the Internet.”**

**Matthew Prince, CEO and Co-Founder, Cloudflare**



## Securing Internet routing

In July 2023, the Federal Communications Commission held a public workshop to address the security of the Border Gateway Protocol.

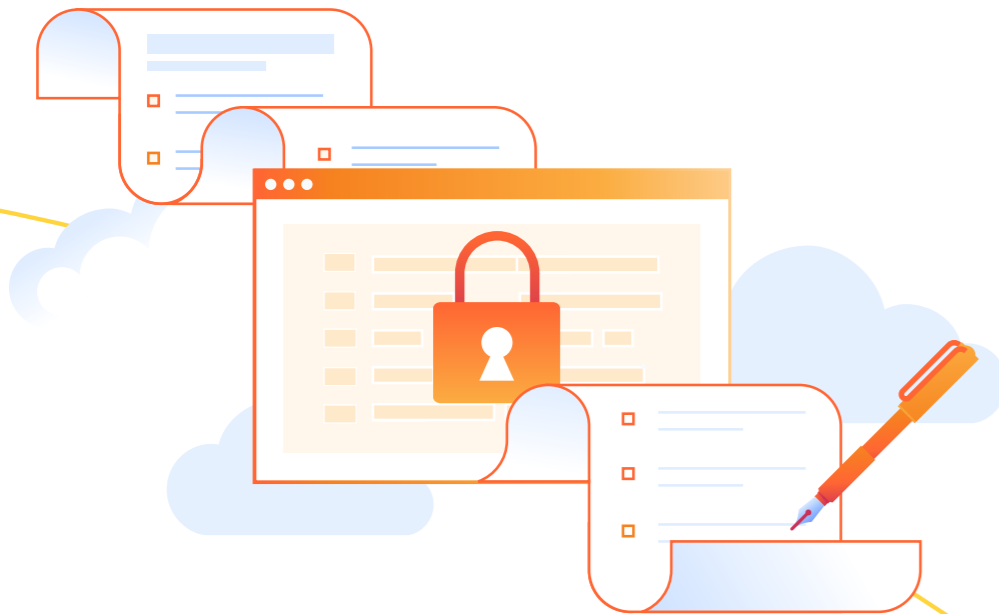
The goal of the public workshop was to spotlight “the critical importance of addressing risks associated with BGP in light of the risk of consumer harm posed by unsecured Internet routing and explored effective security practices to mitigate these vulnerabilities.”

As part of the workshop, the FCC asked Cloudflare to present on the current state of Border Gateway Protocol security, mitigations through Resource Public Key Infrastructure (RPKI), our community outreach on routing security, and data available on Cloudflare Radar on traffic anomalies, confirmed Internet outages, BGP route leaks, and BGP origin hijacks.

We will continue to engage with the FCC and other network providers to improve routing security and the overall health of the Internet ecosystem.

# Complying with privacy and security certifications

Privacy is at the heart of everything we do. We seek to build and maintain trust in Cloudflare's ability to keep personal data private and follow security best practices. Here is a sample of the certifications we have completed as part of our commitment to privacy and security.



## ISO 27001:2013

Enables organizations to secure data and reduce the risk of attacks by outlining a set of globally accepted management procedures and information security controls.

## ISO 27018:2019

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

## PCI DSS 3.2.1

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.

## 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.

## 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.

## 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).

## EU 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.



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

[Trust Hub](#)

[Privacy Policy](#)

[GDPR Compliance](#)

[US Privacy Law Compliance](#)



# Committing to human rights principles

Cloudflare is committed to respecting human rights under the UN Guiding Principles on Business and Human Rights, and to protecting and advancing privacy and freedom of expression as part of the Global Network Initiative.

## 75th Anniversary of the Universal Declaration on Human Rights (UDHR)

In 2023, the UN Human Rights Office (OHCHR) held a yearlong initiative to celebrate the 75th Anniversary of the UDHR. The UDHR is one of the most important documents in the history of human rights. The UDHR, drafted by representatives from all over the world, established the universal requirement to protect fundamental human rights. It was adopted by the UN General Assembly on December 10, 1948. On the 75th Anniversary, Cloudflare was proud to join with a number of companies that participate in the UN's B-Tech Community of Progress in issuing a joint statement on our ongoing commitment to the UDHR and the UN Guiding Principles on Business and Human Rights and encouraging other organizations to do the same.

## Assessing our progress

The Global Network Initiative (GNI) completed its fourth assessment cycle in 2023, which also included Cloudflare's first self-assessment of its human rights practices related to the GNI Principles.

GNI is a nonprofit organization launched in 2008, and its members include 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.



All GNI company members are required to undergo periodic assessments of their progress implementing the GNI principles, which are based on internationally recognized laws and standards for human rights, and include governance, due diligence, risk management, transparency, and engagement requirements. Because this was Cloudflare's first assessment cycle, our own internal human rights team conducted the evaluation and presented our report to the GNI board of directors. In future cycles, Cloudflare will be evaluated by an independent assessor.

### Learn more about Cloudflare's human rights commitments and work

[Cloudflare Human Rights Policy](#)

[Privacy & Data Protection](#)

[Our Approach to Abuse](#)

[Applying Human Rights Frameworks to Our Approach to Abuse](#)

[Cloudflare's Approach to Law Enforcement](#)

[Cloudflare Transparency Report](#)

[Reporting Abuse](#)





# Building trust through transparency

Trust is the foundation of our business. We work to earn our stakeholders' trust through transparency, including our blog, product guides, white papers, reports, and audits.

## Trust Hub

The Trust Hub is a central location to access information about Cloudflare's work on privacy and data protection, security and compliance, technologies, abuse policies, and approach to government requests. The Trust Hub includes frequently asked questions, country-specific data privacy information, and links to Cloudflare white papers and blog posts on privacy and data security topics, including GDPR and data localization.

## Transparency Report

In our Transparency Report, we publish detailed information on legal requests we have received to disclose information about our customers, restrict access to content on our network, and respond to other types of abuse claims. Over the past decade, we have also worked to expand the types of data we report, which now include information about our abuse practices related to hosted content, registrar services, IPFS/Ethereum gateways, and child safety.

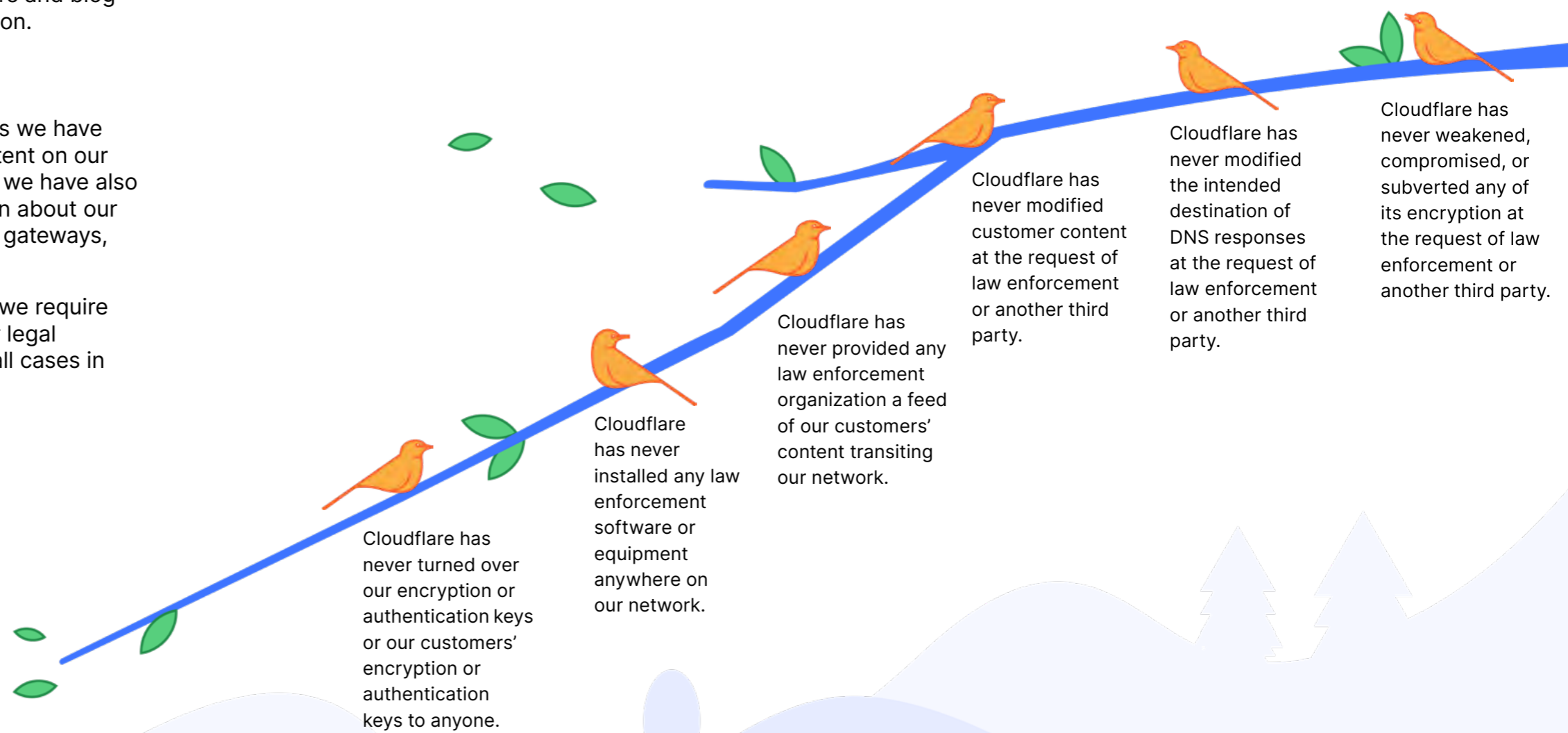
We also break down the types of requests we receive and the legal process we require before providing particular types of information. We review every request for legal sufficiency before responding with data and provide notice to customers in all cases in which we are not legally prohibited from doing so.

### Warrant Canaries

This list of actions we have never taken on our network, called Warrant Canaries, helps our customers understand how we have acted in the past and how we intend to act in the future. It also keeps customers informed about potential law enforcement or other legal orders that prevent us from disclosing them.

If Cloudflare were asked to do any action on this list, we would exhaust all legal remedies in order to protect our customers from what we believe are illegal or unconstitutional requests.

This list is kept up to date on [cloudflare.com/transparency](https://cloudflare.com/transparency).



# Operating with integrity

**We hold ourselves to the highest standards across all aspects of our business.**

## 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, non-discrimination, 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 2022.

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, and that they are not, nor are they providing our services to, sanctioned parties or entities located or based in sanctioned countries.



# A better Internet is for everyone.

# Democratizing access to responsible artificial intelligence

Our goal is to have as dramatic an impact on AI development as we have in other areas: helping bring affordable, powerful AI inference to anyone, anywhere on Earth.

Cloudflare is helping developers create AI applications that are more open, accessible, scalable, and affordable. We are also building controls and privacy features that will support responsible AI development.

## Accessible to everyone

Until recently, running or developing AI applications required developers to both understand machine learning techniques and be able to build and manage the infrastructure to power them. Although there has been extraordinary progress in making AI models more available, there are still fundamental barriers to entry for most developers to be able to leverage and scale AI in their applications. Current AI models are either based on closed, proprietary models that do not address privacy needs required by users, or they are open-source solutions but still not accessible enough to every developer. Earlier this year we launched our AI inference as a service platform called Workers AI, which will make building AI applications more open, accessible, affordable, serverless, and privacy-focused.

## AI observability, reliability, and control

AI-powered applications are providing incredible opportunities for the public and developers to create new types of online services. However, as with any new technology, one of the most significant challenges facing developers is how to create responsible products that also include necessary transparency and controls. Earlier this year, Cloudflare launched AI Gateway, which was designed to sit between developer applications and AI APIs, and analyze data and traffic passing back and forth. These insights will allow developers to better understand how their applications are being used. In addition, AI Gateway will also allow developers to set up additional controls like caching and rate limiting that can help prevent unnecessary queries and help control costs.



## Building a global AI network

One of the biggest challenges small companies and individual developers face in building and scaling AI inference is accessing sufficient GPUs to power their applications. By adding NVIDIA GPUs across our network and making them accessible through Workers AI, Cloudflare's goal is to allow any developer to run their AI models, from their own code, regardless of where they are hosted and without ever needing to set up supporting infrastructure. We are working to have GPUs in place in over 100 cities and 40 countries by the end of 2023, and nearly everywhere Cloudflare operates by the end of 2024, within milliseconds of nearly every device connected to the Internet.

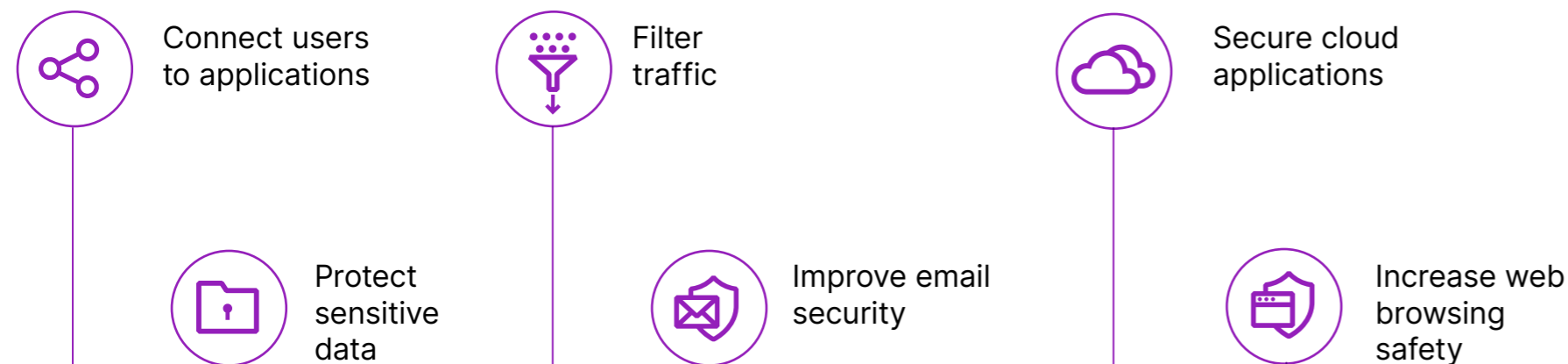
## Block unwanted AI crawlers

Training AI models requires large amounts of data. As a result, many companies and organizations attempting to create AI models are scraping data from across the Internet. Protecting personal information online from AI crawlers will likely become increasingly important. Part of our mission is to build privacy into everything that we do. To that end, Cloudflare security services now include specific categories that allow all customers to prohibit AI crawler bots from scraping their websites for data. In addition, to help AI bot developers build more responsible data collection methods, our team published public criteria for a bot to be considered responsible by our security services.

# Securing infrastructure with Project Safekeeping

In 2022, we launched Project Safekeeping to support critical yet vulnerable infrastructure such as neighborhood hospitals, water treatment facilities, and local energy providers. These types of entities can be obvious targets for attack since they support the basic functioning of communities.

Through Project Safekeeping, we offer free Zero Trust tools to help organizations:



To be considered for the program, infrastructure entities must meet these requirements:

- ✓ Located in Japan, Australia, Germany, Portugal, or the United Kingdom
- ✓ Considered critical infrastructure by governments in their respective localities
- ✓ Up to 50 people and/or less than USD \$10 million in annual revenue/ balance sheet total

# Helping promote democratic values online

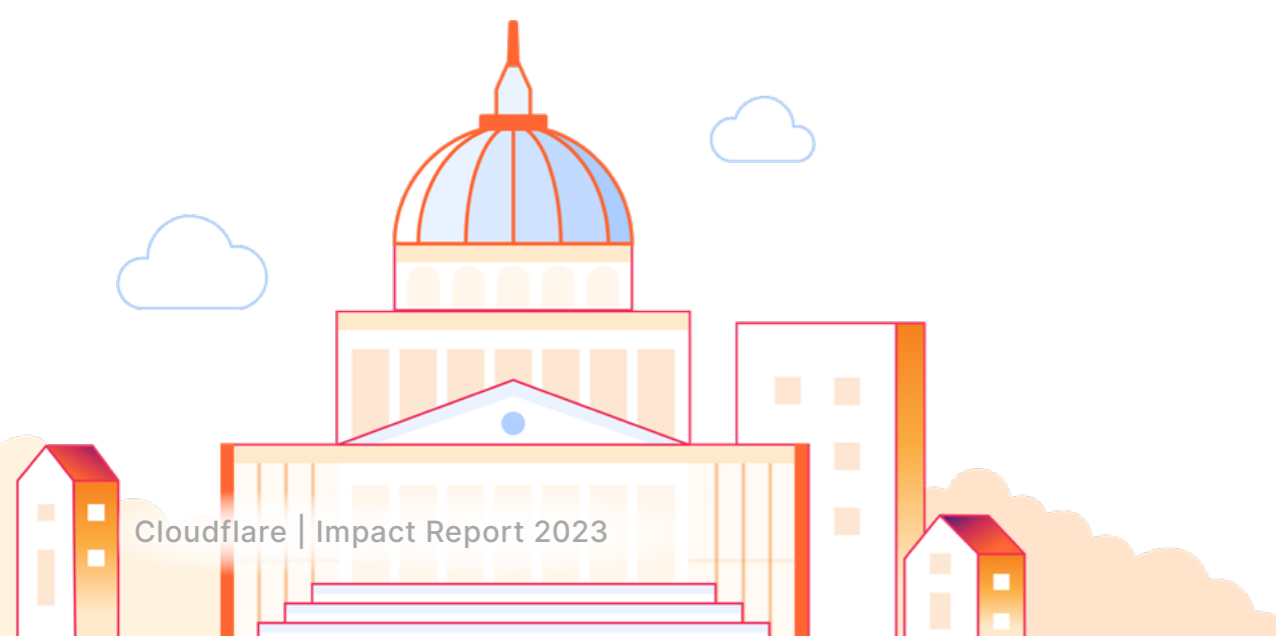
Democracies built on respect for human rights and the rule of law are an important part of protecting a free and open Internet. Companies have a vital role in upholding and protecting democratic norms, and we are proud to contribute to those efforts through our engagement, advocacy, and technology.

## What is the Summit for Democracy?

The first Summit for Democracy was held by the United States government in 2021 and brought together over 100 countries as well as leaders like the President of the European Commission and the United Nations Secretary-General in an effort to strengthen collaboration and respond to the challenges facing democracies around the world.

The 2023 Summit, which was hosted by the United States, Costa Rica, the Netherlands, the Republic of Korea, and the Republic of Zambia, was focused on partnering with the private sector to promote an affirmative vision for technology by countering misuse and shaping emerging technologies to strengthen democracy and human rights.

**100+**  
participating countries



## Cloudflare's 2023 Summit for Democracy commitments



### Democratizing post-quantum cryptography

Cloudflare believes everyone should have access to the next era of cyber security standards — instantly and for free. To that end, Cloudflare has committed to including post-quantum cryptography for free by default to all customers — including individual web developers, small businesses, nonprofits, and governments. Cloudflare will also publish vendor-neutral roadmaps based on NIST standards to help businesses secure any connections that are not protected by Cloudflare.



### Working with researchers to document Internet censorship and shutdowns

Cloudflare commits to working with researchers to share data about Internet shutdowns and selective Internet traffic interference and to make the results of the analysis of this data public and accessible.



### Engaging with civil society on Internet protocols and the development of privacy-enhancing technology

Cloudflare believes that meaningful consultation with civil society is a fundamental part of building an Internet that advances human rights. As we work with Internet standards bodies and Internet providers on the next generation of privacy-enhancing technologies and protocols, like protocols to encrypt Domain Name System records and Encrypted Client Hello (ECH) and privacy-enhancing technologies like OHTTP, we commit to direct engagement with civil society and human rights experts on standards and technologies that might have implications for human rights.

# Supporting access to an open Internet

**Everyone should have access to a fast and open Internet. Cloudflare is part of a diverse group of stakeholders sharing information and advocating to improve access and preserve open Internet principles.**

## **Maintaining a level playing field for individuals, vulnerable communities, and small businesses**

Central to an open Internet is the principle of net neutrality, the idea that network service providers should treat all Internet traffic equally. This concept helps fulfill the original promise of the Internet: anyone online has the ability to access the information of their choosing.

A number of jurisdictions have recently proposed measures that would alter this basic framework, such as proposals where delivery of traffic might depend on a sender's willingness or ability to pay. Cloudflare is part of a coalition of companies, civil society organizations, and consumer groups that advocate against policies or regulations that would alter net neutrality through network usage fees, mandatory paid peering arrangements, or any other proposal that would unfairly advantage large businesses or allow providers to make decisions about what content individuals using their service can access. For example, earlier this year, Cloudflare filed public comments encouraging the EU not to favor fast lanes on the Internet for large tech companies or undermine free peering arrangements.

## **Improving performance and choice for consumers**

Earlier this year the US government announced its "Internet for All" initiative, which provides \$65 billion to help close the digital divide in the United States through investment in broadband deployment and digital equity plans. Cloudflare has published information to support this effort, describing how factors like latency can affect Internet performance in underserved communities.

In addition, the US Federal Communications Commission (FCC) recently announced a potential new rule that would require Internet providers to display standardized information about the speed, quality, and cost of Internet service for their customers. The goal of the regulation is to allow consumers to make more informed choices on their Internet provider, including by having access to better information on how their Internet actually performs. Cloudflare strongly supports the FCC effort, and filed public comments to suggest additional items that should be included, including latency and jitter.

## **Helping more communities access the Internet**

According to the United Nations, almost half of the world's population currently does not have access to the Internet. Even in communities that are able to invest in WiFi antennas or fiber cables, connection to the Internet remains prohibitively expensive. Cloudflare is helping support those communities by offering free connection services to the Internet for rural, nonprofit, and local community networks, particularly in underserved areas.

**Learn more about our work at [cloudflare.com/pangea](https://cloudflare.com/pangea).**



# Expanding our network and improving access

Cloudflare is building and expanding a global network that not only brings our customers as close as possible to their users, but also makes the Internet faster, more secure, and more reliable for local communities all over the world.

Over the last 13 years, Cloudflare’s network has grown from a single data center to more than 310 cities in over 120 countries. Each new data center, location, and interconnection helps bring the Internet and our free services closer to the people requesting access to them.

An important part of our network growth strategy is investing in underserved areas in order to help improve Internet performance. For example, in 2023, Cloudflare made major investments to our network in Africa; we now have a presence in 26 cities on the continent. Because of our new locations, expansions within our existing locations, and increased peering with other networks, we are serving users locally rather than backhauling traffic to faraway cities.

These direct interconnections with Internet providers, mobile carriers, and wholesale IP connectivity providers allow individuals across Africa to experience reliable and low-latency access to the Internet and Cloudflare’s services.

## Cloudflare’s presence in Africa



26  
cities



The Cloudflare booth at AfricaCom. >>



## Network spotlight: Angola

In June 2023, we expanded our network presence in Angola.

When routed locally to one of our points of presence in Luanda, Internet users experience an average latency of 24 milliseconds between their devices and our network. This allows for fast traffic delivery for websites using Cloudflare network services and developer tools.

Without Cloudflare’s local presence, the average latency would rise to 98 milliseconds, a 300% increase in latency.

Although a reduction measured in milliseconds may not sound substantial, it represents a significant boost in terms of user experience. Shortening the distance between users and servers means decreasing how long a user waits for a website to load.

Throughout Cloudflare’s 13-year history, we have seen how making the Internet faster in a region can have a clear impact on traffic: if the experience is faster, people usually do more online.



# Building community at Cloudflare

Diversity, equity, and inclusion are priorities at Cloudflare — we want to ensure a sense of belonging and community for all employees. Our Employee Resource Groups (ERGs) are employee-led, and each has a designated executive sponsor.

These communities come together to celebrate their cultures, support each other, organize educational initiatives, and promote professional development.



<< Cloudflare employees attend the AfroTech conference in November 2023.



Afroflare



Asianflare



Cloudflarents



Desiflare



Flarability



Greencloud



Judeoflare



Latinflare



Mindflare



Nativeflare



Persianflare



Proudflare



Soberflare



Turkflare



Vetflare



Womenflare







# Prioritizing diversity at Cloudflare

To make progress on Cloudflare’s most ambitious goals — including helping build a better Internet, protecting vulnerable voices, improving privacy measures, promoting trust in democracy, and respecting human rights — we know we need a diverse team and an inclusive environment where people feel like they can do their best work.

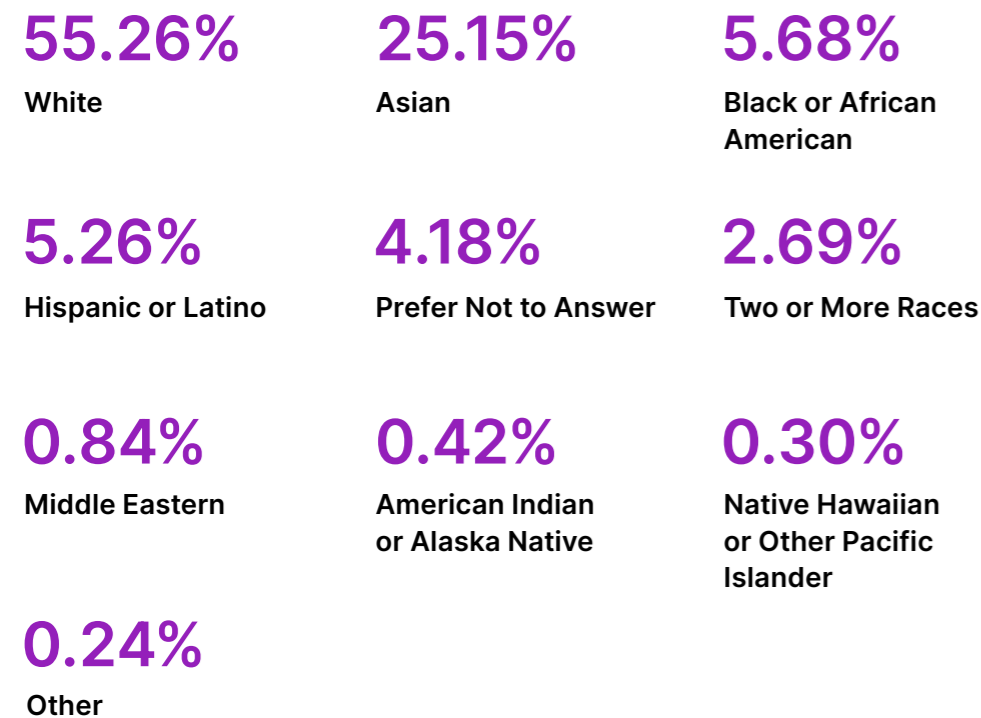
When evaluating applicants and reviewing employee performance, we use the Cloudflare Capabilities, which are the values we consider the foundation of our culture.

Learn more about our efforts on diversity, equity, inclusion education, and recruiting at [cloudflare.com/diversity-equity-and-inclusion](https://cloudflare.com/diversity-equity-and-inclusion).

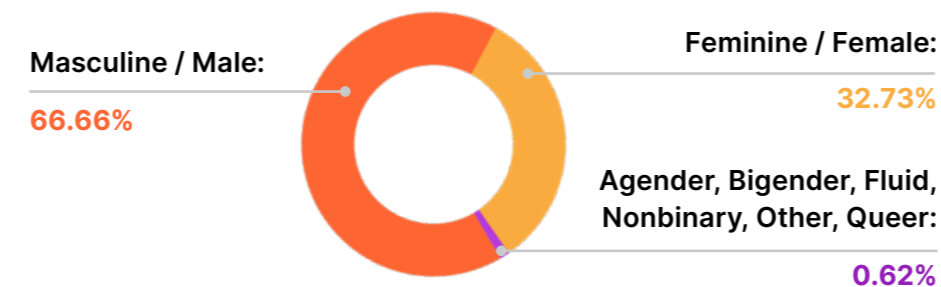
## Cloudflare Capabilities

-  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

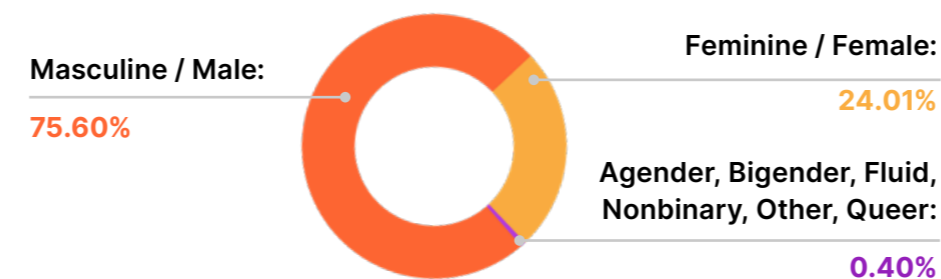
### US Overall Race/Ethnicity



### Overall Gender Identity



### Leadership Gender Identity



# Improving the Internet through transparency

Sharing information about how the Internet functions is essential to maintaining its accessibility, resilience, and reliability. It is also the foundation for a free and open Internet and protecting human rights online.

Cloudflare Radar is a free public resource that aggregates anonymized data from Cloudflare services and makes it possible for anyone to monitor and investigate Internet patterns, trends, shutdowns, and anomalies around the world.

## Detecting BGP route leaks and origin hijacks

BGP is the glue that keeps the Internet together. It is a routing protocol used by organizations and networks to examine available paths on the Internet, and exchange information on the most efficient routes. Internet routing can be disrupted by issues like route leaks, where networks erroneously share routing information, or BGP origin hijacks, where a bad actor intentionally reroutes Internet traffic for malicious purposes, such as stealing information.

To help improve BGP routing security for everyone, network operators (along with researchers, journalists, or anyone else) can now use Cloudflare Radar and the [Cloudflare Radar API](#) to learn about and be notified of route leaks and BGP origin hijacks in near real time. In addition, information about the adoption of routing security practices at a network level is available on Cloudflare Radar Routing pages.

## Alerts on Internet outages, shutdowns, and anomalies

Internet outages are caused by a number of things, such as natural disasters, technical malfunctions, and government-directed shutdowns. Technical, civil society, and human rights organizations help monitor Internet shutdowns to ensure that governments or other responsible parties are held accountable for Internet disruptions that violate international human rights. Cloudflare is proud to support those efforts through the Cloudflare Radar Outage Center (CROC), and beginning this year, through a customizable alert feed that provides up-to-date information on Internet outages and traffic anomalies.



# A better Internet is sustainable.

# Cutting emissions by moving to the cloud

A 2023 study by the management consultancy Analysys Mason found that migrating from on-premises network hardware to Cloudflare’s cloud-based services can decrease related carbon emissions between 78% and 96%.

The study compared the energy consumption and associated emissions of a typical network and security services like wide area networking (WAN), load balancing, firewalls, and DDoS mitigation provided via traditional on-premises hardware compared to Cloudflare’s cloud-based services.

A key finding was that the combination of migrating those services to Cloudflare’s global network, which is shared by millions of customers around the world, and consolidating multiple different network and security functions on a single network like Cloudflare’s could dramatically reduce related energy consumption and emissions.

“

On-premises equipment consumes power constantly but is only utilised for part of the day and part of the week. By contrast, cloud infrastructure is much more highly utilised, and has less wasted capacity. Cloudflare’s global scale and aggregation of heterogeneous demand means that its infrastructure is used by thousands of businesses, and as one business’s demand falls away, another business’s demand will be picking up.”

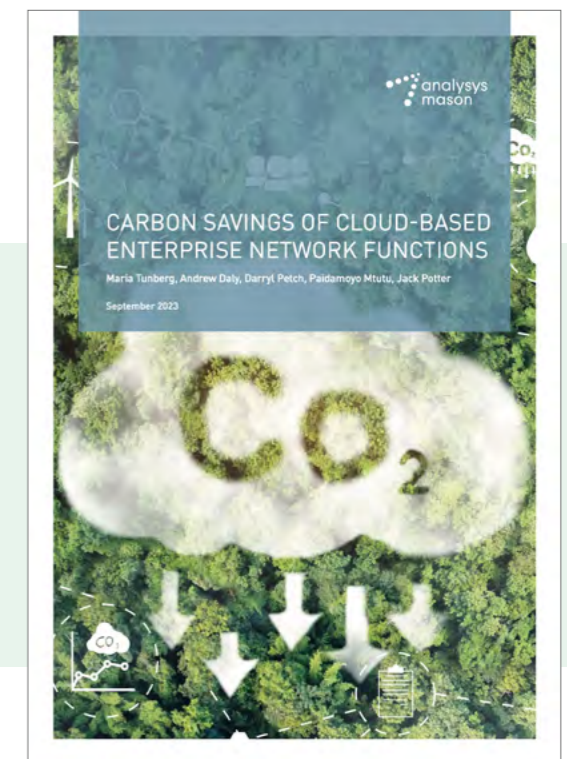
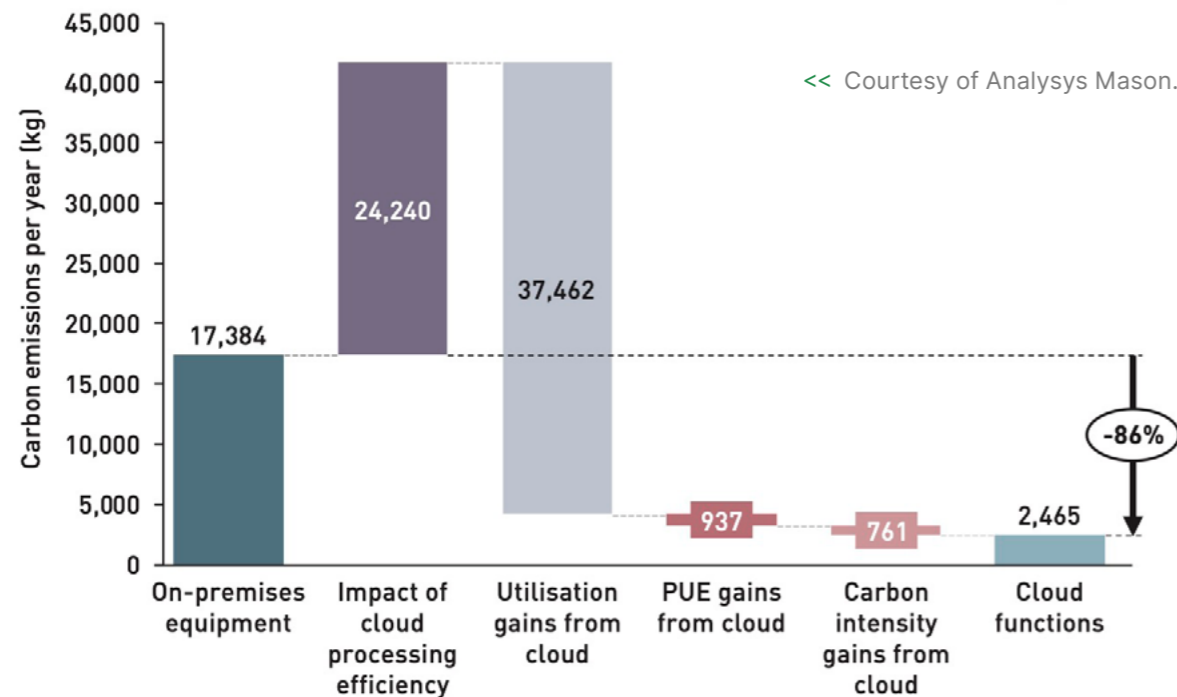
Analysys Mason, Carbon Savings of Cloud-Based Network Functions

“

The best way to reduce your IT infrastructure’s carbon footprint is easy: move to the cloud.”

Matthew Prince, CEO and Co-Founder, Cloudflare

Read the full report on [Carbon Savings of Cloud-Based Network Functions](#).



# Cloudflare sustainability

## Cloudflare is joining the Science Based Targets initiative (SBTi)!

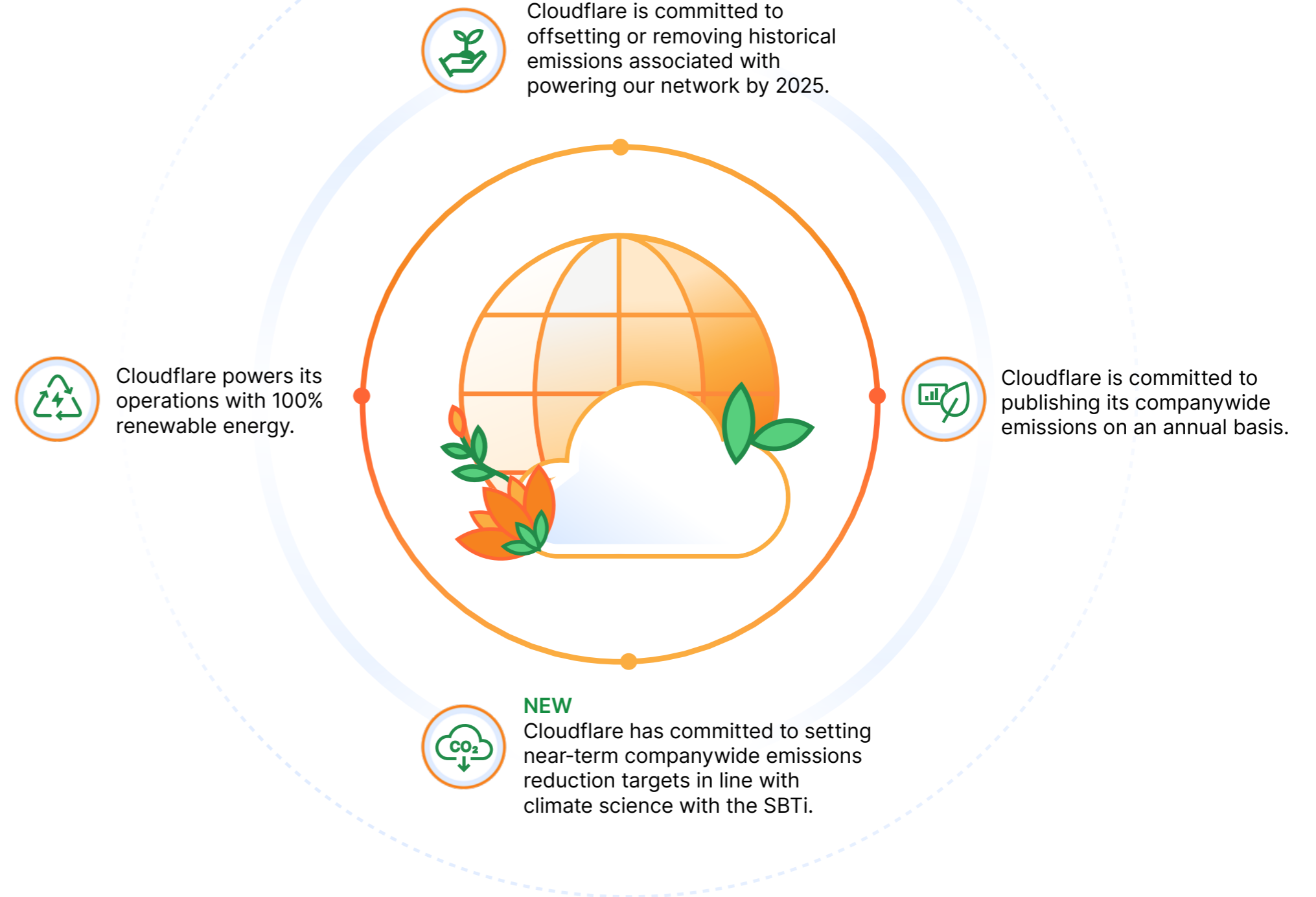
We are proud to announce that Cloudflare has committed to setting near-term companywide emissions reductions in line with climate science with the SBTi.

SBTi requires companies to achieve verifiable emissions reductions across their operations and supply chain without the use of carbon offsets. These short-term reduction goals must be consistent with the Paris Climate Agreement goal of limiting global warming to 1.5 degrees above pre-industrial levels.

The initiative is a collaboration between the Carbon Disclosure Project (CDP), UN Global Compact, World Resources Institute, and World Wide Fund for Nature (WWF).

**Over the next two years, Cloudflare will work to develop its carbon reduction plan for submission to SBTi, which independently assesses and approves company targets. We look forward to keeping everyone updated on our progress!**

## Our commitments



# Tracking Cloudflare emissions

## Greenhouse gas (GHG) emissions

In September, we published our third greenhouse gas (GHG) emissions inventory for 2022 data. We separated our calculations into Scope 1 and Scope 2.

Our [emissions analysis](#) was conducted pursuant to the [GHG Protocol](#) and ISO 14064, and reviewed and verified by an independent third party (see Appendix). Cloudflare classifies all energy consumed by its networking hardware as Scope 2 emissions.

Emissions Category		Carbon Dioxide Equivalent (CO2e) in Metric Tons (MT)	Percent of Calculated Total
Scope 1		137	100%
Scope 2 (Location-based)		20,982	100%
	Facilities	865	4%
	Network	20,117	96%
Scope 2 (Market-based)		0	100%
Total (Market-based) <sup>1</sup>		0	100%

<sup>1</sup>Total (market-based) emissions include Cloudflare's 2022 verified offsets and renewable energy purchases.



# Restoring forests and habitats

Since 2019, Cloudflare has invested in reforestation projects as part of our mission to destroy bad bots online.

Cloudflare Bot Fight Mode and Super Bot Fight Mode are tools that website owners use to combat bad bots by rerouting them to computationally intensive but meaningless tasks, a process that helps improve site performance and user experience.

Since this process results in increased CPU usage, though, we have been donating to tree planting projects to help account for the bad bots caught in Cloudflare defenses. After running the calculations, we will be planting 28,812 trees to account for our bot-fighting activities this year.

**50,000**  
trees planted to date

**20,000**  
trees in progress



## Learn more about other One Tree Planted projects supported by Cloudflare

[Victoria Park, Nova Scotia, Canada](#)

[Kumirmari island, West Bengal, India](#)

[Forest fire recovery in British Columbia, Canada](#)



Photos of Mexico and Portugal tree planting projects courtesy of One Tree Planted. >>





# Appendix

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
GRI 2: General Disclosures	2-1 Organizational details	Cloudflare, Inc. 101 Townsend Street, San Francisco, CA <a href="#">Cloudflare Office Locations</a> <a href="#">10-K Filing</a>
	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) 2023, unless otherwise stated.  <a href="#">10-K Filing</a> <a href="#">10-Q Filing</a>  Contact point: <a href="mailto:impact@cloudflare.com">impact@cloudflare.com</a>
	2-5 External assurance	Cloudflare's greenhouse gas emissions were externally verified. See GRI 305. No other section of this report was externally verified. See Shift Advantage verification letter, page 44.
	2-7 Employees	<a href="#">10-Q</a> <a href="#">Diversity, Equity, and Inclusion at Cloudflare</a>  Cloudflare does not have a significant portion of its organizational activities performed by workers who are not employees.
	2-9 Governance structure and composition	<a href="#">Proxy Statement Filing</a>
	2-23 Policy commitments	<a href="#">ESG resources:</a> <ul style="list-style-type: none"> <li>• Governance Documents</li> <li>• Code of Business Conduct and Ethics</li> <li>• Third Party Code of Conduct</li> <li>• Modern Slavery Act Statement</li> <li>• Human Rights Policy</li> <li>• Trust Hub</li> <li>• Privacy Policy</li> </ul>
	2-25 Processes to remediate negative impacts	<a href="#">Human Rights Policy</a> <a href="#">Cloudflare Trust Hub: Our approach to abuse</a>
	2-28 Membership associations	Cloudflare participates in the following trade associations: BSA, i2c, CCIA, TechUK, Eco, Asia Internet Association, Bitkom, Germany Secure Online (Deutschland sicher im Netz), American Chamber of Commerce Japan, Communications Alliance, and US-China Business Council.

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
<b>GRI 201: Economic Performance</b>	201-2 Financial implications and other risks and opportunities due to climate change	<a href="#">10-K Filing</a>
<b>GRI 205: Anti-corruption</b>	205-2 Communication and training about anti-corruption policies and procedures	<p>All employees, including senior managers, complete training on bribery and corruption at onboarding, and as part of annual training and certification.</p> <p>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.</p> <p>Cloudflare has selected an anti-bribery and anti-corruption training course for its third parties, and is preparing for rollout in 2024.</p>
	205-3 Confirmed incidents of corruption and actions taken	<p>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.</p> <p>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.</p> <p>Cloudflare is aware of no associated legal cases brought against Cloudflare or its employees.</p>
<b>GRI 206: Anti-competitive Behavior</b>	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.
<b>GRI 207: Tax</b>	207-1 Approach to tax	<p>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.</p> <p>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.</p>
<b>GRI 302: Energy</b>	302-1 Energy consumption within the organization	<p>Cloudflare consumed no non-renewable energy as defined under GRI 302 in CY2022.</p> <p>Cloudflare consumed 63.18 gigawatt hours (GWh) total energy in CY2022. 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 2022.</p> <p><a href="#">Emissions Inventory 2022</a></p>

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
<b>GRI 302: Energy</b> <i>(continued)</i>	302-3 Energy intensity	Based on 2022 total revenue and energy data, Cloudflare consumed .000065 megawatt hours (Mwh) of energy for every dollar of revenue generated.
	302-4 Reduction of energy consumption	Cloudflare has committed to setting near-term companywide emissions reductions in line with climate science with the Science Based Targets initiative (SBTi).
<b>GRI 303: Water and Effluents</b>	303-1 Interactions with water as a shared resource	<p>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.</p> <p>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.</p>
<b>GRI 305: Emissions</b>	305-1 Direct (Scope 1) GHG emissions	<p>See emissions data, page 31.</p> <p>Cloudflare recorded Scope 1 location-based emissions of 137 metric tons (MT) carbon dioxide equivalent (CO2e) in 2022. Cloudflare used the operational control consolidation approach, under the GHG Protocol.</p> <p><a href="#">Emissions Inventory 2022</a></p>
	305-2 Energy indirect (Scope 2) GHG emissions	<p>See emissions data, page 31.</p> <p>Cloudflare recorded the following Scope 2 emissions in 2022:</p> <p>Location-based emissions: 20,982 metric tons (MT) carbon dioxide equivalent (CO2e).</p> <p>Market-based emissions: 0 MT CO2e.</p> <p><a href="#">Emissions Inventory 2022</a></p>
	305-3 Other indirect (Scope 3) GHG emissions	Cloudflare is in the process of collecting data to calculate its Scope 3 emissions.
	305-4 GHG emissions intensity	<p>Based on its CY2022 location-based emissions, Cloudflare emitted .000022 MT (CO2e) per dollar of revenue generated.</p> <p>Cloudflare emitted 0 market-based emissions in CY2022.</p>
	305-5 Reduction of GHG emissions	Cloudflare has committed to setting near-term companywide emissions reductions in line with climate science with the Science Based Targets initiative (SBTi).

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
<b>GRI 306: Waste</b>	306-1 Waste generation and significant waste-related impacts	<p>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 a third-party provider at its data centers for decommissioning, recycling, and destruction services.</p> <p>As a result, according to Cloudflare's supplier, 83,157 pounds of electronic waste was diverted from landfills in 2023. In addition, according to Cloudflare's supplier and based on the US EPA's Waste Reduction Model (WARM), these landfill diversions led to 58.07 MT CO<sub>2</sub>e of avoided greenhouse gas emissions. Cloudflare will continue to work with all of its suppliers to obtain additional data on its waste-related impacts.</p>
<b>GRI 308: Supplier Environmental Assessment</b>	308-1 New suppliers that were screened using environmental criteria	<a href="#">Third Party Code of Conduct</a>
<b>GRI 401: Employment</b>	401-1 New employee hires and employee turnover	In 2023 (as of November 1, 2023), Cloudflare hired 897 employees and experienced a turnover rate of 14.6% (as of November 1, 2023).
	401-3 Parental leave	Cloudflare's global parental leave policy allows a minimum of 16 paid weeks of bonding leave time for all qualifying new parents, with no interruption in health benefits. This is in addition to any local, state, and federal benefits.
<b>GRI 403: Occupational Health and Safety</b>	403-1 Occupational health and safety management system	<p>Cloudflare's global Safe &amp; 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.</p> <p>Cloudflare maintains global incident response plans that include accident reporting procedures, safety monitoring, and incident after-action review.</p> <p><a href="#">Code of Business Conduct and Ethics</a></p>
	403-2 Hazard identification, risk assessment, and incident investigation	<p>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.</p> <p>The program also includes a post-incident after-action review to identify incident causes and implement necessary prevention measures.</p>

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
<b>GRI 403: Occupational Health and Safety</b> <i>(continued)</i>	403-5 Worker training on occupational health and safety	At all office locations, Cloudflare conducts evacuation drills and has safety signage in place.
	403-6 Promotion of worker health	Cloudflare provides employees with a variety of benefits and programs to promote worker health.  Employee access to non-occupational health services includes healthcare insurance, an employee assistance program (EAP), family forming benefits, and an on-demand digital mental health and well-being platform.
	403-9 Work-related injuries	Cloudflare experienced no fatalities as a result of work-related injury in 2023.  Cloudflare experienced no high-consequence work-related injuries in 2023.
	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.
<b>GRI 404: Training and Education</b>	404-1 Average hours of training per year per employee	Of the employees who participated in development training for 2023, they completed a total of 4,886 hours. On average, each employee completed 3.1 hours of training.
<b>GRI 405: Diversity and Equal Opportunity</b>	405-1 Diversity of governance bodies and employees	<a href="#">Diversity, Equity, and Inclusion at Cloudflare</a>
	405-2 Ratio of basic salary and remuneration of women to men	Cloudflare conducts an internal pay parity analysis at least once a year. Cloudflare has committed to the EU Charter, the UK Tech Talent Charter, and the German Diversity Charter.  <a href="#">Diversity, Equity, and Inclusion at Cloudflare</a>
<b>GRI 407: Freedom of Association and Collective Bargaining</b>	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.  <a href="#">Human Rights Policy</a>  Cloudflare is not aware of any operations in 2023 in which the rights of employees to freely associate or collectively bargain were at risk.

## GRI Standards

## SASB

GRI Standard	Disclosure	Answer
<b>GRI 408: Child Labor</b>	408-1 Operations and suppliers at significant risk for incidents of child labor	<p>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.</p> <p><a href="#">Human Rights Policy</a> <a href="#">Third Party Code of Conduct</a></p>
<b>GRI 409: Forced or Compulsory Labor</b>	409-1 Operations and suppliers at significant risk for incidents of forced or compulsory labor	<p>Cloudflare continues to explicitly prohibit forced or compulsory labor in its operations and among its suppliers.</p> <p><a href="#">Modern Slavery Act Statement</a></p> <p>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.</p>
<b>GRI 414: Supplier Social Assessment</b>	414-1 New suppliers that were screened using social criteria	Cloudflare's procurement team implemented a new software tool in 2023 that will enable the company to screen suppliers against risks, including environmental, social, and governance criteria.
<b>GRI 415: Public Policy</b>	415-1 Political contributions	<p>Cloudflare made no political contributions in 2023, and does not operate a Political Action Committee.</p> <p>Cloudflare participates in several trade associations and industry groups; however, none of those organizations is primarily organized for the purpose of making political contributions. For more information, see 2-28.</p>
<b>GRI 418: Customer Privacy</b>	418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data	Cloudflare did not receive any substantiated complaints concerning breaches of customer privacy and losses of customer data in 2023.

## GRI Standards

## SASB

## SASB - Technology &amp; Communications Sector

## Software &amp; IT Services

Topic	Code	Accounting Metric	Answer
<b>Environmental footprint of hardware infrastructure</b>	TC-S1-130a.1	(1) Total energy consumed, (2) percentage grid electricity and (3) percentage renewable	Cloudflare consumed 63.18 gigawatt hours (GWh) total energy in CY2022. 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 2022.  <a href="#">Emissions Inventory 2022</a>
	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.
<b>Data privacy &amp; freedom of expression</b>	TC-SI-220a.1	Description of policies and practices relating to behavioural advertising and user privacy	<a href="#">Privacy Policy</a> <a href="#">Cloudflare Cookie Policy</a>
	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.  <a href="#">Transparency Report</a>



## GRI Standards

## SASB

## SASB - Technology &amp; Communications Sector

## Software &amp; IT Services

Topic	Code	Accounting Metric	Answer
<b>Data privacy &amp; freedom of expression</b> <i>(continued)</i>	TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	<p>An essential part of earning and maintaining the trust of Cloudflare customers is being transparent about the requests Cloudflare receives from law enforcement and other governmental entities. To this end, Cloudflare publishes semiannual updates to its Transparency Report on the requests it has received to disclose information about Cloudflare customers. In addition, Cloudflare maintains a list of warrant canaries on its website, which list actions Cloudflare has never taken, and commits to exhausting all legal remedies in order to protect its customers from what the company believes are illegal or unconstitutional requests.</p> <p>Cloudflare also may receive written requests from law enforcement, government agencies, or foreign courts to block access to content based on the local law of the jurisdiction. Because of the significant potential impact on freedom of expression, Cloudflare will evaluate each content blocking request on a case-by-case basis, consistent with its Human Rights Policy, analyzing the factual basis and legal authority for the request. If Cloudflare determines that the order is valid and requires Cloudflare action, it may limit blocking of access to the content to those areas where it violates local law, a practice known as “geoblocking.” Cloudflare will attempt to clarify and narrow overbroad requests when possible. Cloudflare reports on these requests in its semiannual Transparency Report.</p> <p>Cloudflare has also received a small number of legal requests related to blocking or filtering content through the 1.1.1.1 Public DNS Resolver. Because such a block would apply globally to all users of the resolver, regardless of where they are located, it would affect end users outside of the blocking government’s jurisdiction. Cloudflare therefore evaluates any government requests or court orders to block content through a globally available public recursive resolver as requests or orders to block content globally.</p> <p>Given the broad extraterritorial effect, as well as the different global approaches to DNS-based blocking, Cloudflare has pursued legal remedies before complying with requests to block access to domains or content through the 1.1.1.1 Public DNS Resolver or identified alternate mechanisms to comply with relevant court orders. To date, Cloudflare has not blocked content through the 1.1.1.1 Public DNS Resolver.</p> <p><a href="#">Transparency Report</a></p>
<b>Data security</b>	TC-SI-230a.1	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of users affected	Cloudflare did not experience any data breaches involving personally identifiable information (PII) requiring notification under applicable data protection law.
	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 risk program that adheres to industry standards such as ISO 27000, 27701, and 27018; PCI DSS; SOC 2 Type II; and C5; and has been evaluated by third-party assessors against the requirements.

GRI Standards

SASB

SASB - Technology & Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Answer
Recruiting and managing a global, diverse & 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: <ul style="list-style-type: none"> <li>• Australia: 12%</li> <li>• Canada: 14%</li> <li>• France: 30%</li> <li>• Germany: 34%</li> <li>• Japan: 12%</li> <li>• Mexico: 0%</li> <li>• Netherlands: 69%</li> <li>• Portugal: 43%</li> <li>• Singapore: 63%</li> <li>• UAE: 100%</li> <li>• UK: 57%</li> <li>• US: 10%</li> <li>• India: 0%</li> <li>• South Korea: 0%</li> <li>• China: 0%</li> </ul> Percentage of employees located offshore: 0.03% (1 out of 3592)
	TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	<a href="#">Diversity, Equity, and Inclusion at Cloudflare</a>
Intellectual property protection & competitive behavior	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 anticompetitive behavior regulations.

GRI Standards

SASB

SASB - Technology & Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Answer
<b>Managing systemic risks from technology disruptions</b>	TC-SI-550a.1	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	<p>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 ESG 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.</p> <p>Beginning in 2024, Cloudflare expects it will be subject to one or more regulatory disclosure requirements related to similar network disruptions or related incidents, including potentially under the NIS2 Directive. As a result, Cloudflare will no longer 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.</p>
	TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	<a href="#">10-Q Filing</a>

# Emissions verification letter

Cloudflare  
101 Townsend St  
San Francisco, CA 94107

Shift Advantage  
5925 NE 18th Ave  
Portland, OR 97211

6/6/2023

Dear Patrick,

Shift Advantage is pleased to provide consulting and advisory services to Cloudflare to support the calculation of Cloudflare's 2022 greenhouse gas emissions. Shift Advantage conducted this independent and impartial limited level of assurance verification (Verification) in accordance with ISO 14064-part 3 2nd Edition, 2019-04, Annex A. 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 2022 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 and Scope 2 emissions. Scope 3 emissions are excluded. The Verification has confirmed the accuracy and completeness of the information provided to substantiate Cloudflare's 2022 GHG emissions reporting. Cloudflare's total reported emissions are 21,119 MT CO<sub>2</sub>e. Verified emissions by scope are as follows:

- Scope 1 Emissions: Direct emissions associated with natural gas used to heat offices - 137 MT CO<sub>2</sub>e
- Scope 2 Emissions: Indirect emissions associated with purchased electricity in offices and colocated data centers – 20,982 MT CO<sub>2</sub>e (location based)

Shift Advantage has found no evidence that Cloudflare's 2022 GHG emissions reports or data were incorrect, as everything was found to be presented fairly and in accordance with stated criteria in line with the GHG Protocol Corporate Accounting and Reporting Standard and the ISO 14064 Standard.



Eric Brody – Principal Shift Advantage



Dan Tremblay – Lead Verifier Shift Advantage



© 2023 Cloudflare Inc. All rights reserved.  
The Cloudflare logo is a trademark of Cloudflare. All other  
company and product names may be trademarks of the  
respective companies with which they are associated.

Call: 1 888 99 FLARE  
Visit: [www.cloudflare.com/impact](https://www.cloudflare.com/impact)

REV:BDES-5077.2023DEC14