



Impact Report

2024

Contents

Introduction

- 3 Growing our impact
- 4 Fighting for the open Internet
- 5 Building an innovation economy
- 6 2024 spotlight: Project Galileo 10th anniversary event
- 7 Celebrating our 14th anniversary — Birthday Week 2024
- 8 Sustainability @ Cloudflare

A better Internet is principled

- 10 Protecting the democratic process in the year of elections
- 12 Athenian Project
- 13 Project Galileo
- 14 Protecting and engaging with civil society
- 15 Engineering privacy into the Internet
- 16 Working together to secure the Internet
- 17 Building trust through transparency
- 18 Complying with privacy and security certifications
- 19 Implementing our human rights principles
- 20 Operating with integrity

A better Internet is for everyone

- 22 Reaffirming our commitment to free
- 23 Empowering the open source community
- 24 Responsible AI for everyone
- 25 Investing in technical standards efforts
- 26 Anatomy of a DDoS attack
- 27 Cloudflare Radar
- 29 Radar in focus: connection tampering
- 30 Project Cybersafe Schools
- 31 1.1.1.1
- 32 Exploring life @ Cloudflare
- 33 Creating a sense of belonging
- 34 Recruiting @ Cloudflare
- 35 Measuring diversity at Cloudflare

A better Internet is sustainable

- 37 Next-generation hardware
- 38 Reimagining how and where we work
- 39 Tracking greenhouse gas emissions
- 40 Fighting back against bad bots

Appendix

- 42 Compliance tables
- 52 Emissions verification letter

Growing our impact

Cloudflare Impact is part of our mission to help build a better Internet, and how we are helping make the Internet a force for good.

Most Loved Workplaces

Cloudflare was again listed in Newsweek’s 100 Most Loved Workplaces, keeping our ranking of #55. Newsweek and BPI surveyed more than two million employees across companies, asking about collaboration, values, and respect.



Also voted Most Loved Workplaces for:

- Parents and Caregivers
- Young Professionals
- LGBTQ+



Fortune Change the World

for Cloudflare’s Project Galileo



Reuters Events Sustainability Awards

Social Impact Award Finalist for Cloudflare’s Project Galileo



Pledge 1%

Cloudflare pledges 1% of our time and products to give back to our communities.



Best Companies to Work for in Technology in Portugal (Teamlyzer)

Technology professionals in Portugal voted Cloudflare as the best company to work for in technology in Portugal in 2024.

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.

\$15M+

in donated products in 2024

\$63M+

in donated products since 2017

3,700+

Internet properties protected under Cloudflare Impact programs

33

states received free Cloudflare services through the Athenian Project during the 2024 election cycle

Fighting for the open Internet

The Internet is a miracle. The connection of diverse networks with common standards enables us to exchange data around the world in a way that is resilient, interoperable, and accessible to anyone. Today, we depend on it for economic growth and innovation, access to information and free expression, and rule of law and democratic principles.

Cloudflare is proud to be part of the global community standing up for the Internet.



Supporting multistakeholder Internet governance

Participating in Internet standards development

Advocating for network neutrality

Monitoring places where the Internet is not open

Protecting human rights and democratic institutions

Deploying standards that improve the privacy and security of data flows

Building an innovation economy

Our goal is to be the infrastructure for the next generation.

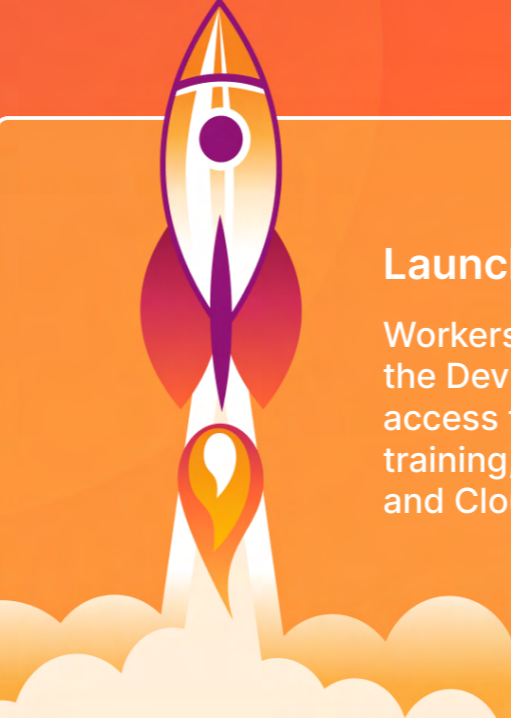


Next-Generation Networks

Networks of the future must be faster, more secure, more private, and more reliable. Integrating new technologies like AI and smart devices demands low-latency, interconnected networks that are close to users and support a diverse cloud ecosystem.

Cloudflare makes it easier for anyone to write code, build applications, and launch new ideas anywhere in the world.

Cloudflare was built for this future.



Launching the next startup

Workers Launchpad, Cloudflare for Startups, and the Dev Alliance provide small businesses with access to free Cloudflare services, investors, training, technical support, partner companies, and Cloudflare-sponsored launch events.



New startups building on Cloudflare in 2024

115 startups	22 countries
40 participating venture capital funds	
\$2 billion in financing	

To learn more about the newest startups launching on Cloudflare, please visit the [Cloudflare blog](#).

2024 spotlight Project Galileo 10th anniversary event

Cloudflare celebrated the 10th anniversary of Project Galileo, our program that provides free cyber security services for nonprofit organizations, by hosting a discussion with civil society and government experts on how to better protect journalists, activists, and humanitarian organizations online.



To view the entire Project Galileo 10th anniversary event, please visit [Cloudflare TV](#).



Eileen Donahoe, Special Envoy and Coordinator for Digital Freedom, US State Department; Matthew Prince, Co-Founder and CEO, Cloudflare; Jason Pielemeier, Executive Director, Global Network Initiative >>



By onboarding Buka into Project Galileo, we were able to help them restore their site's functionality. And now Buka's website is equipped to withstand even the most sophisticated attacks, ensuring that their critical reporting continues uninterrupted, exactly at the time where the Republic of Srpska government is looking to close and restrict independent, civic voices in that part of Bosnia and Herzegovina."

Damon Wilson, President and CEO, National Endowment for Democracy



If you have any doubts about Cloudflare's role in the world, think again."

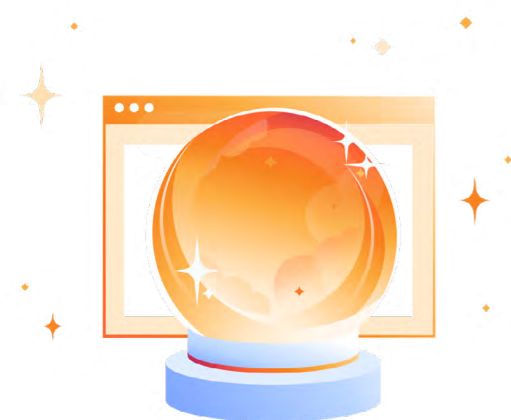
Eileen Donahoe, Special Envoy and Coordinator for Digital Freedom, Bureau of Cyberspace and Digital Policy, US Department of State



<< Adrien Ogée, Chief Operations Officer, CyberPeace Institute; Alissa Starzak, Deputy CLO, Global Head of Policy, Cloudflare; Jennifer Brody, Deputy Director of Policy and Advocacy for Technology and Democracy, Freedom House; Emily Skahill, Cyber Operations Planner, Joint Cyber Defense Collaborative, Cybersecurity & Infrastructure Security Agency, US Department of Homeland Security

Celebrating our 14th anniversary — Birthday Week 2024

Since our first anniversary, we have used Birthday Week to launch products that we think of as gifts back to the Internet.



Supporting content creators in the age of AI

The Internet relies on website owners and content creators willing to share information with users. In return, website owners are able to generate advertising revenue based on the number of users that visit their site. AI bots operate differently. Rather than directing users to a website, they pull others' content to train their models or make it available on their own interfaces. Cloudflare is helping put website owners back in control of their content by providing tools that can block, audit, and control how AI bots access their websites.



Speed Brain: helping webpages load 45% faster, for free

Part of Cloudflare's mission is making the Internet faster. Speed Brain helps eliminate browser wait times by preloading content of a webpage a user is most likely to visit, which can help reduce load times by as much as 45%. Speed Brain limits its predictions to a user's activity on a single website, and does not follow users around the web. Cloudflare has made Speed Brain available to all of its customers for free.

Visit cloudflare.com/birthday-week to get all of our Birthday Week 14 announcements.

Highlights from past Birthday Weeks



Sustainability @ Cloudflare

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



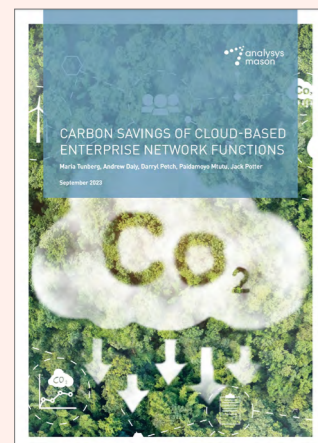
Cloudflare’s 12th-generation servers are

145%

more performant and

63%

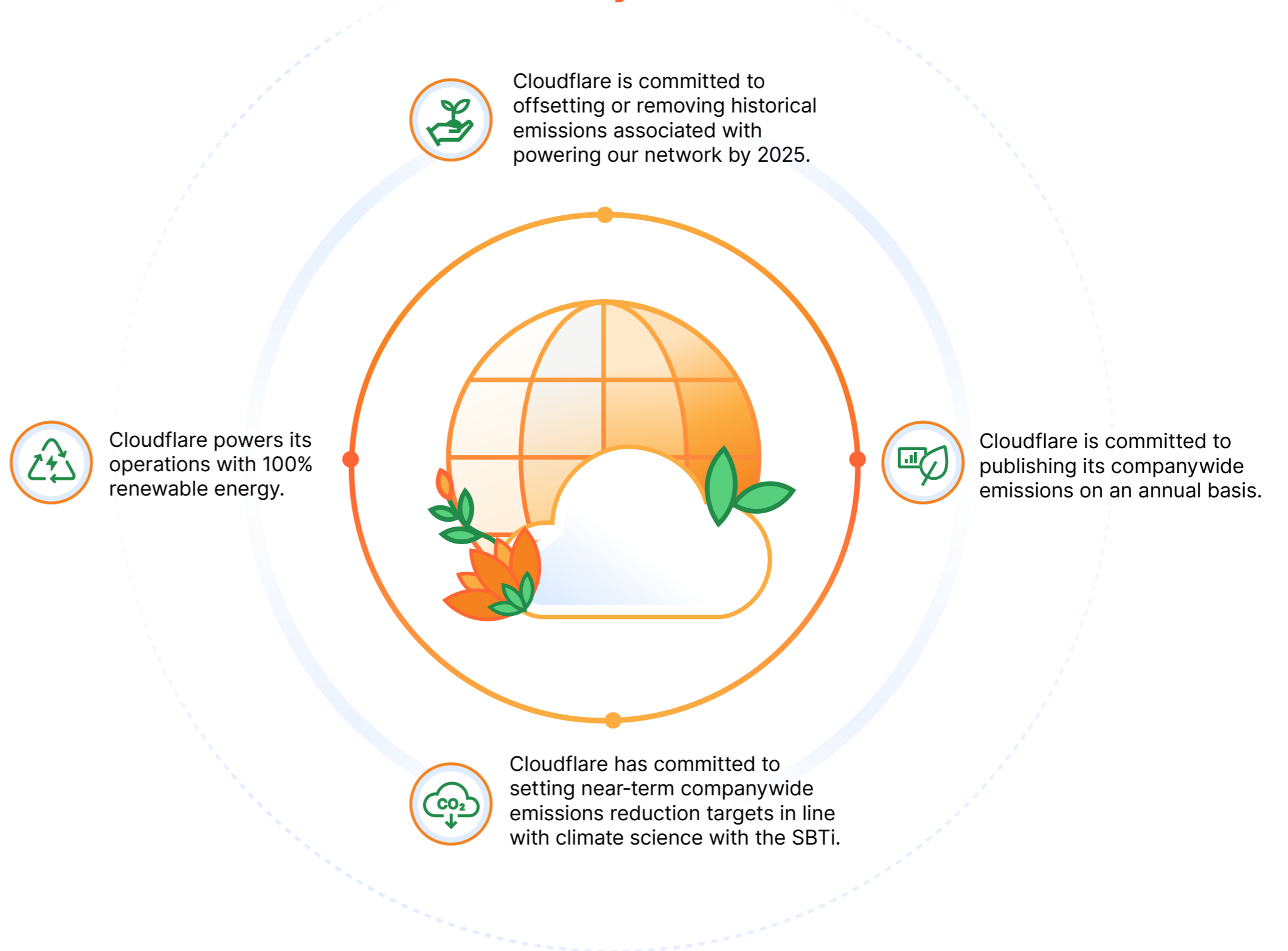
more energy efficient.



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%.

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

Our sustainability commitments

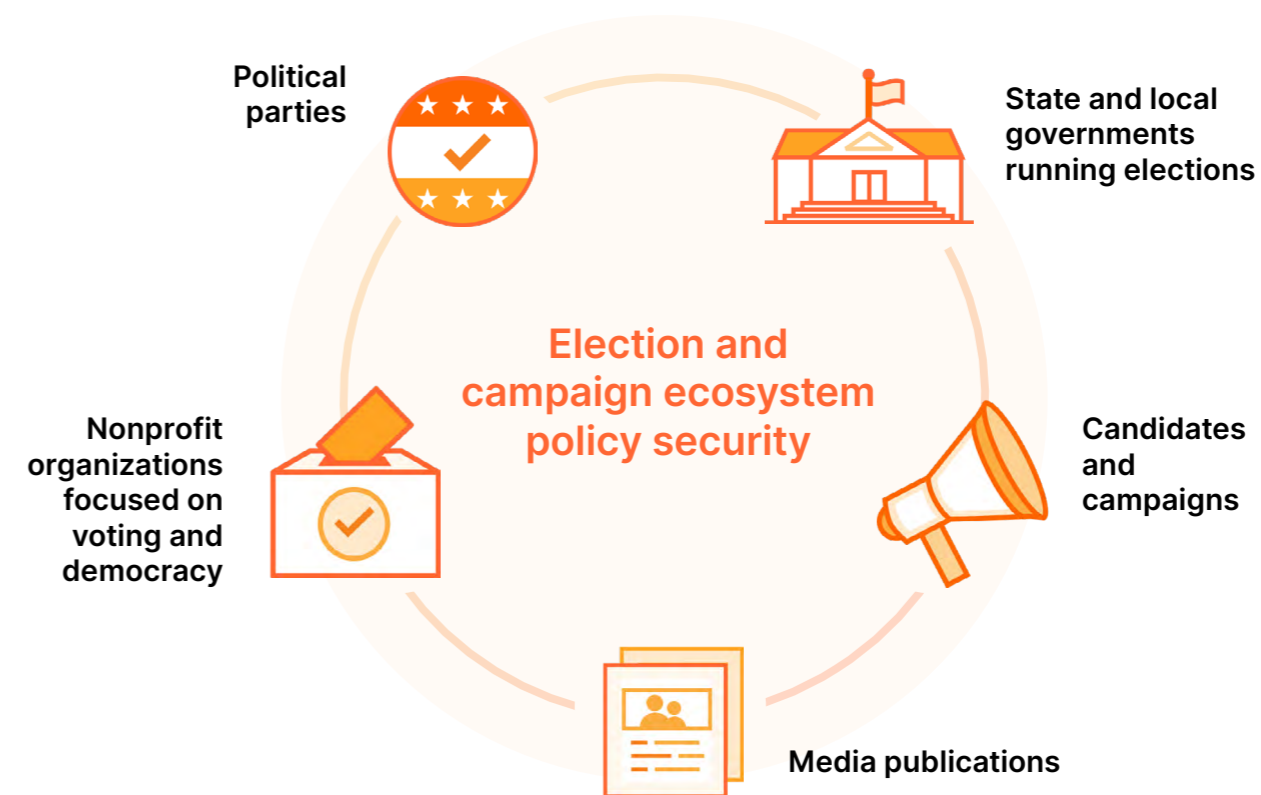




A better Internet is **principled.**

Protecting the democratic process in the year of elections

More than 70 countries held elections in 2024. Half of the world's population was eligible to vote. Cloudflare provides free cyber security services to governments and organizations across the election ecosystem that help ensure they stay online.



Preparing for the US elections

Briefed
300+
election officials on emerging threats

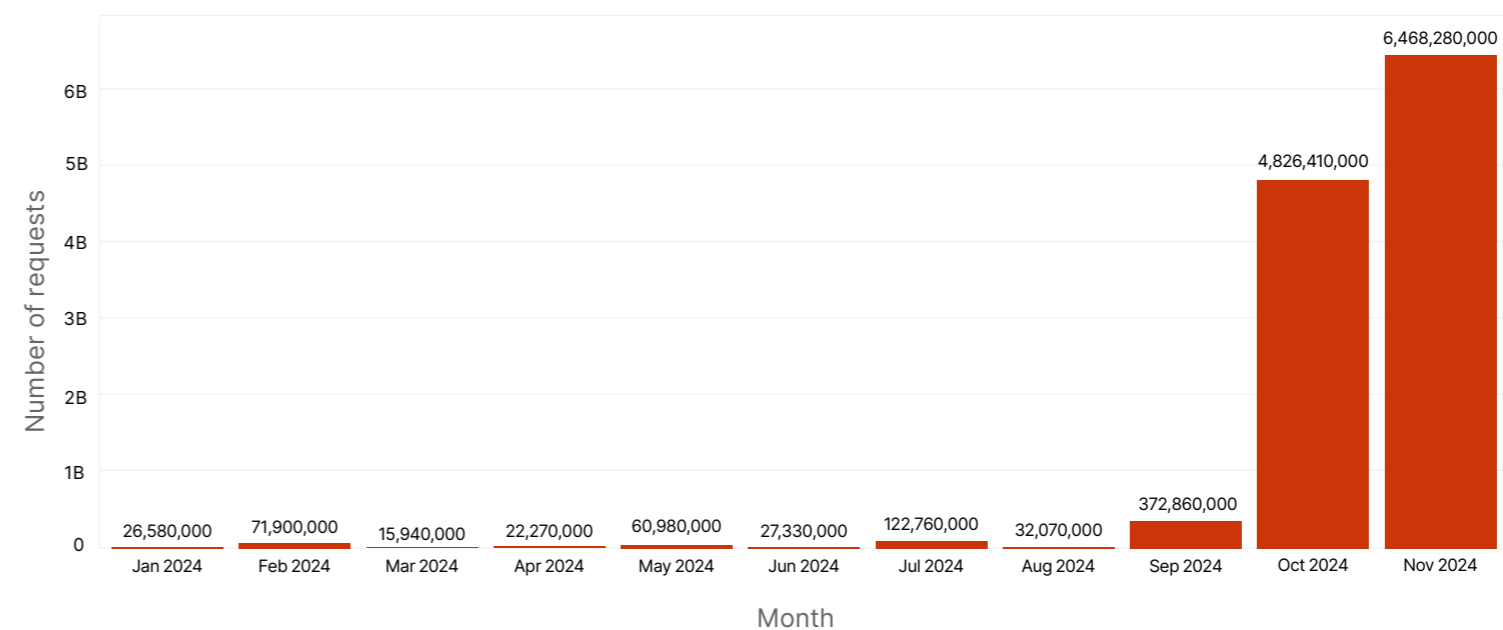
Held
50+
support calls with state and local governments

Onboarded
90+
political campaigns and related entities to Cloudflare for Campaigns

Onboarded
60+
local media sites to Project Galileo



DDoS requests mitigated — US political or election-related websites

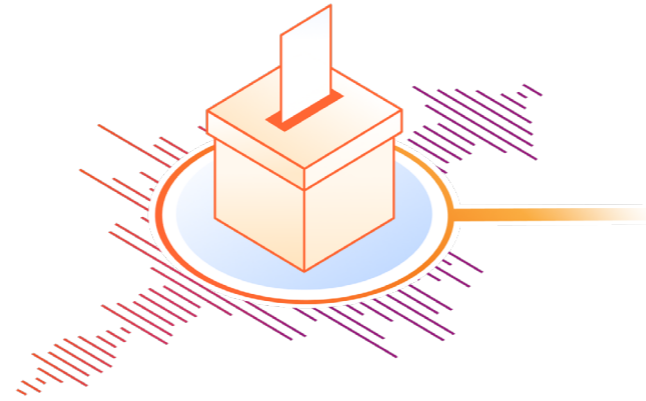


<< Cloudflare detected a notable increase in DDoS attacks targeting political entities prior to the election; we are proud that those attacks did not cause any significant disruption.

Protecting the democratic process in the year of elections

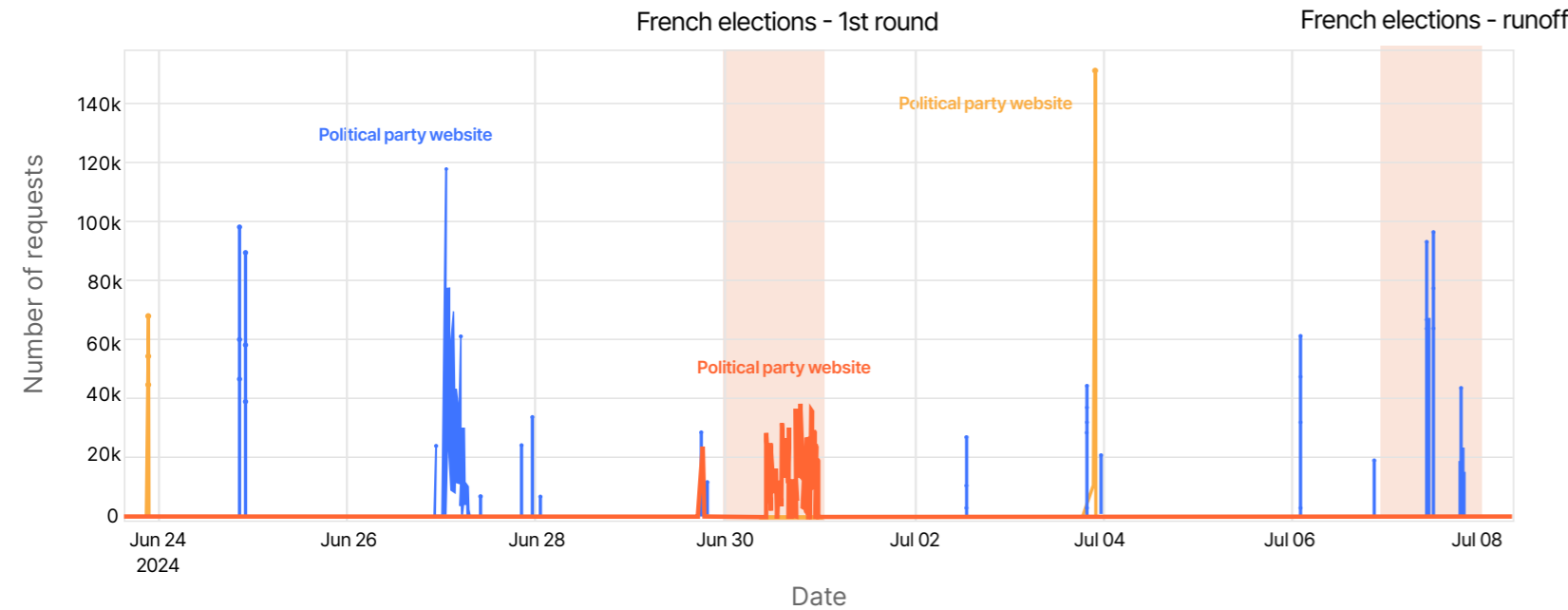
Reporting on global elections

Cloudflare monitors Internet traffic, attacks, and potential shutdowns during elections around the world through our free public resource Cloudflare Radar. We publish those results to help our civil society partners and the public better understand what is happening online throughout the electoral process.

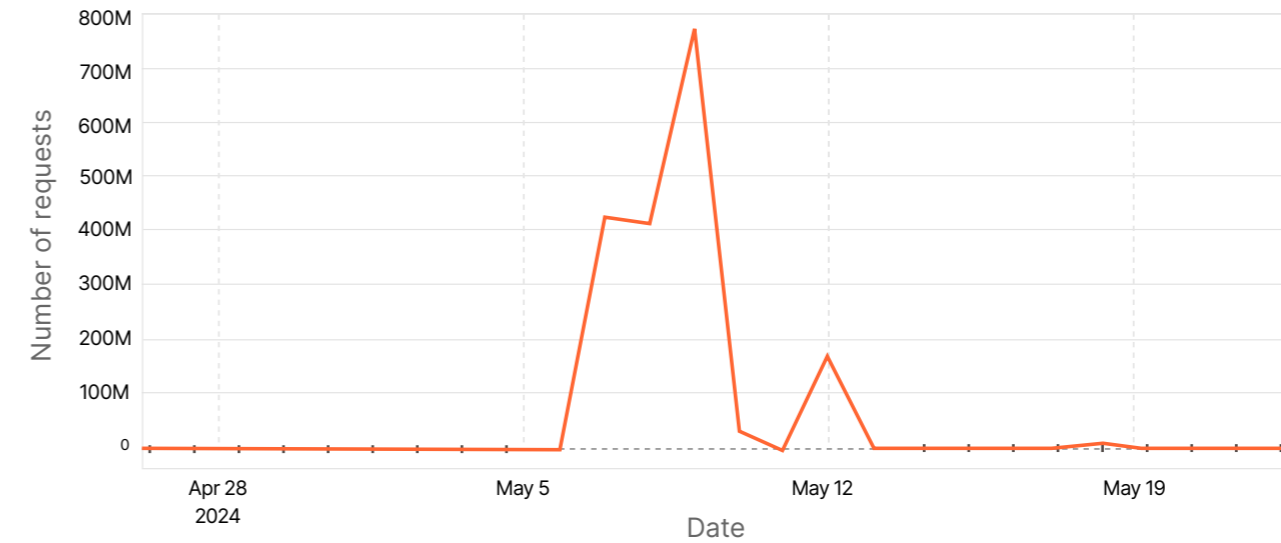


Application-layer DDoS attacks targeting politics-related websites in France

15-06-2024 to 08-07-2024 (UTC)



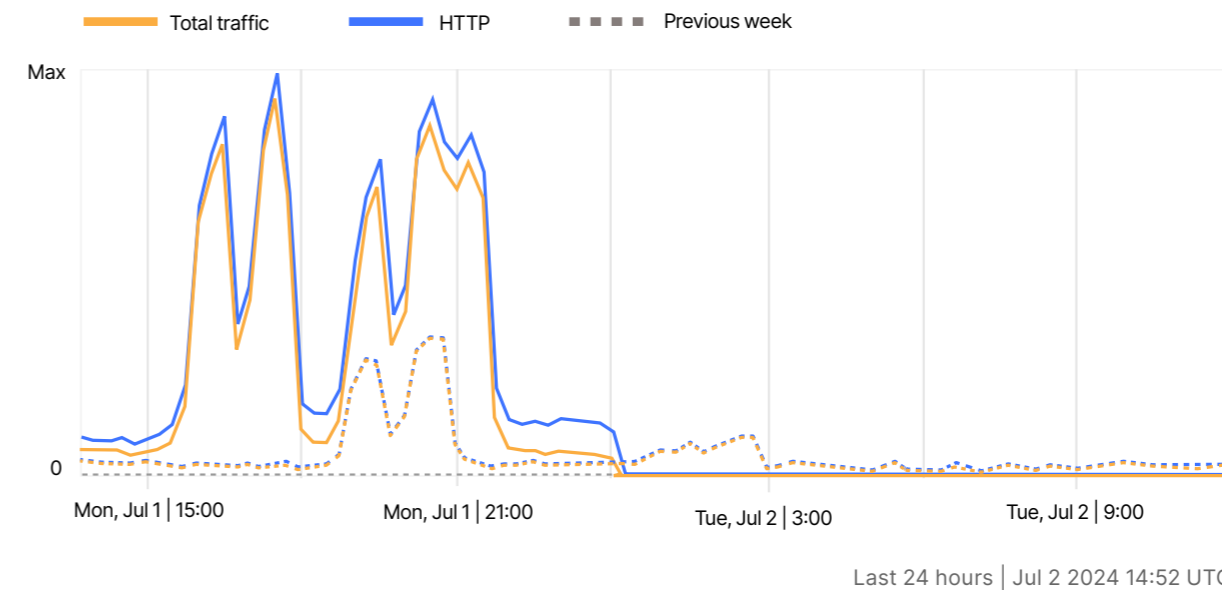
HTTP DDoS attacks toward a South African news Internet property



<< Prior to elections in South Africa, Cloudflare detected a significant DDoS attack against a major South African news site, with more than 773 million daily requests.

Internet traffic trends for AS37508 (MATTEL)

Traffic volume over the selected time period



<< Following elections, the Mauritanian government announced increased security because of protests in the capital city, Nouakchott. Cloudflare observed Internet disruptions that coincided with reports that the government suspended mobile Internet connectivity.

Athenian Project

EST. 2017

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.



Election security at a glance

426

Internet properties protected

6

countries

33 US states

receive free Cloudflare services through the Athenian Project

317 million

threats to government election websites mitigated between January 1, 2024, and November 14, 2024, an average of 1 million threats per day

“

We want to maintain public trust, especially in regards to our election process, by making our web presence as secure as financially possible. And thanks to this project, we were able to add another layer of protection to our website. Our website is critical for sharing information and results for all of our elections and Cloudflare is now part of keeping that information available to Sioux County citizens and interested observers.”

Micah Van Maanen, Information Technology Director, Sioux County, Iowa

“

There are so many things to do in the world of IT, and there’s only so much money, time, and manpower that you have to resolve complex cyber security issues. We’ve been able to enhance our security in a very meaningful and substantial way with the Athenian Project.”

Ryan J. Tiano, CIO, Columbia County, New York

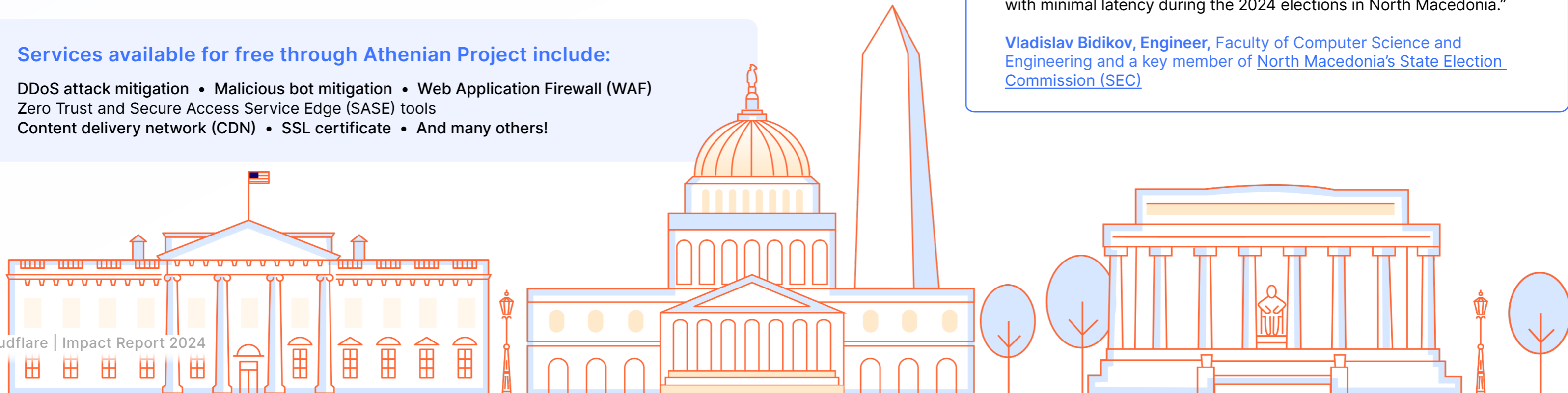
“

By utilizing Cloudflare Workers and implementing smart caching rules, we significantly reduced the load on their backend systems while ensuring that voters and media outlets received up-to-date information with minimal latency during the 2024 elections in North Macedonia.”

Vladislav Bidikov, Engineer, Faculty of Computer Science and Engineering and a key member of [North Macedonia’s State Election Commission \(SEC\)](#)

Services available for free through Athenian Project include:

- DDoS attack mitigation
- Malicious bot mitigation
- Web Application Firewall (WAF)
- Zero Trust and Secure Access Service Edge (SASE) tools
- Content delivery network (CDN)
- SSL certificate
- And many others!



Project Galileo

EST. 2014

Human rights defenders, journalists, and humanitarian organizations are often vulnerable to cyber attacks. In collaboration with 54 civil society partners, Cloudflare protects public interest groups from attacks intended to silence them online.

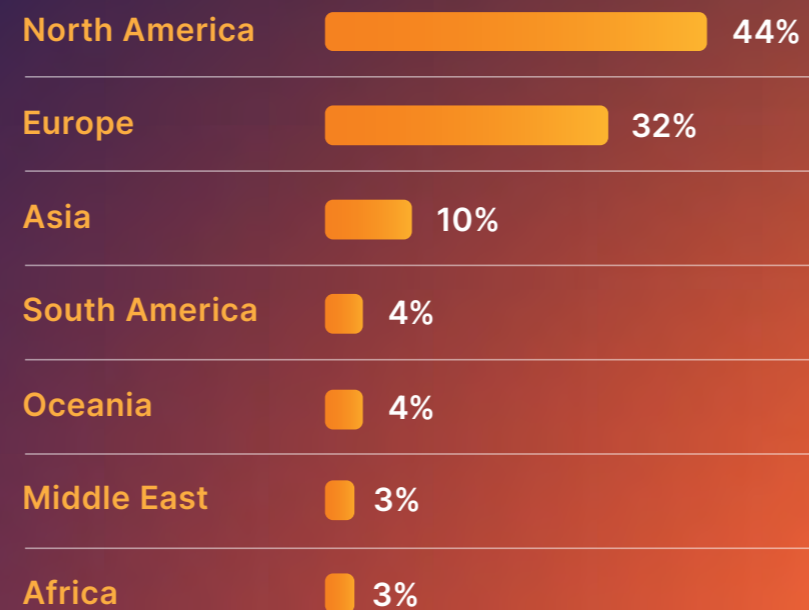
Learn more and apply at cloudflare.com/galileo.



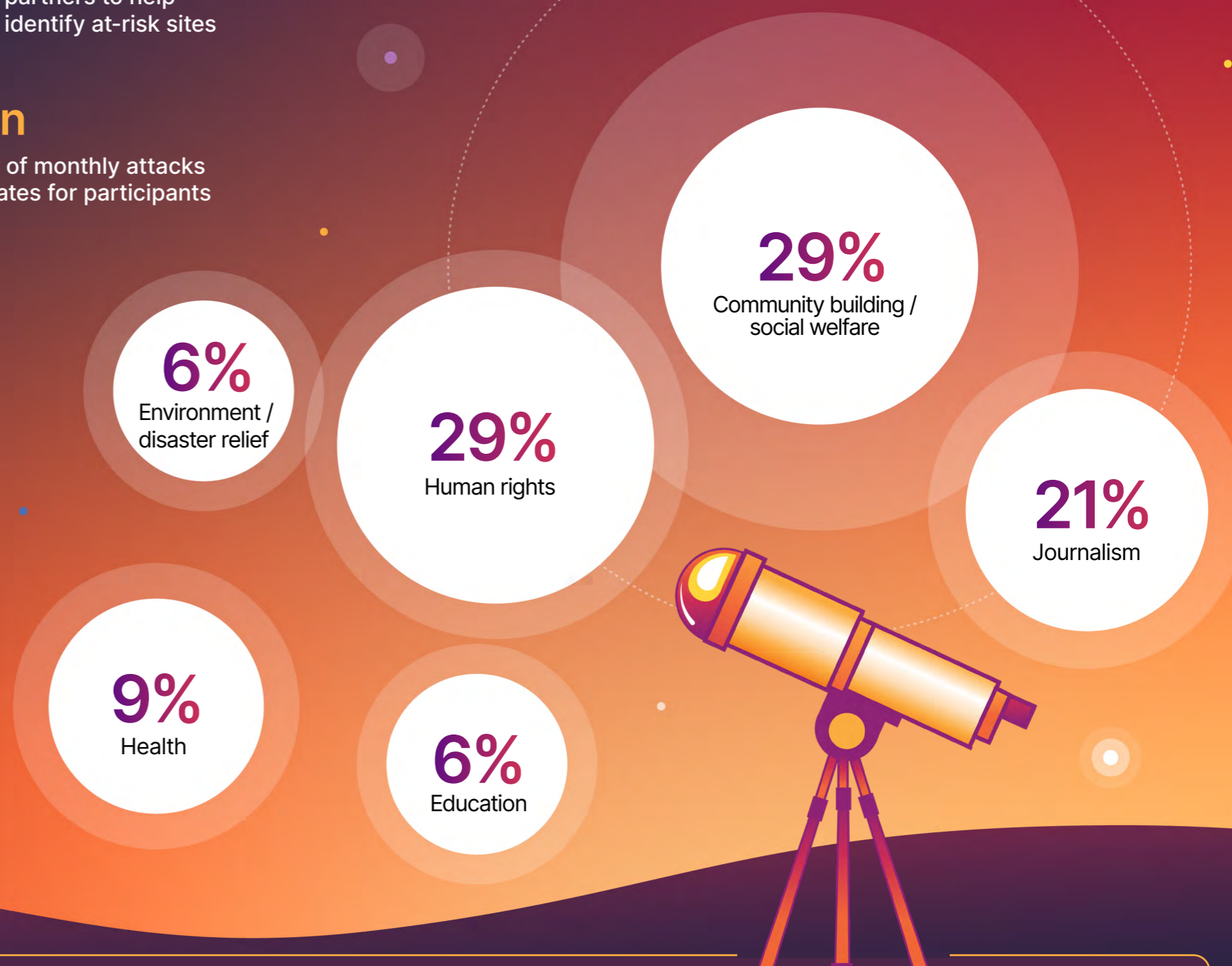
2,900+ Internet properties
111+ countries
54 partners to help identify at-risk sites

95.8 million average number of daily attacks Cloudflare mitigates for participants
3 billion average number of monthly attacks Cloudflare mitigates for participants

Project Galileo participants



Participants by organizational type



Services available for free through Project Galileo include:

DDoS mitigation • Web Application Firewall (WAF) • DNS • Content delivery network (CDN) • Zero Trust tools • SSL certificate • Among many others!

Protecting and engaging with civil society

Civil society is a building block of democracy, the free and open Internet, and open global markets. Cloudflare’s partnerships with civil society organizations are an important part of our mission, and essential to our business.

Advocating for civil society’s role in Internet governance

This multistakeholder governance model, which anticipates a diverse array of voices getting to consensus, has allowed the Internet to grow into the miracle it is today. Part of Cloudflare’s advocacy on behalf of the free and open Internet is supporting civil society’s role in Internet governance, including at venues like the World Summit on the Information Society and the Internet Governance Forum.

Hacking together new applications for our partners

Cloudflare has partnered with Nuxt, an open source framework and developer community, to volunteer to design and build new websites or apps for nonprofit organizations. The new program will launch at the upcoming Nuxt Winter Hack 25. The first partner organization selected is the CyberPeace Institute. Developers from Cloudflare and Nuxt will work with CyberPeace Institute on a new application that will help streamline reporting and managing cyber attacks against nonprofit organizations.

Cyber security tools to support reproductive health advocates

The Gateway Coalition offers resources, support, and outreach for abortion access groups that advocate for patients and reproductive rights. Cloudflare supports their efforts by delivering free cyber security services and training to help organizations advocating for reproductive care to protect their operations and data.



<< Cloudflare attended the WSIS+20 Forum to advocate for protecting civil society’s role in Internet governance

Welcoming NetHope as a Project Galileo partner!

NetHope is a global nonprofit uniting over 60 leading humanitarian organizations with technology companies and funding partners to solve challenges and expand their impact. NetHope is one of 54 leading civil society organizations that work with Cloudflare to vet and approve Project Galileo applications.



We need more tech companies to realize that civil society needs [programs like Project Galileo], and not software at a discount, that was not built with their needs in mind that gives them the illusion of security. No, we need more. . . value-driven companies that are realizing the critical role that civil society plays in their business model.”

Adrien Ogée, Chief Operations Officer, CyberPeace Institute

At the 5th Congress of Portuguese Journalists, Cloudflare >> presented on tools available to support journalists



Engineering privacy into the Internet

Cloudflare collaborates on Internet standards to make the Internet more private.

The next frontier of encryption: transparency (with WhatsApp)

End-to-end encrypted messaging apps like WhatsApp rely on public key cryptography to encrypt messages. But it can be challenging to ensure that a user has the intended recipient's correct key. Cloudflare is partnering with WhatsApp, using Cloudflare Workers, to independently audit and vouch for WhatsApp's key distribution. This allows users to verify that their encryption keys are valid and unique from anywhere.

A faster, more secure way to manage Internet traffic

Building MASQUE into WARP allows Cloudflare to provide faster, more secure, and more reliable privacy-enhancing VPN solutions to the public for free. MASQUE is a new protocol that builds on performance improvements like packet coalescing and multiplexing, while also supporting NIST-recommended encryption standards. MASQUE also helps WARP more closely resemble ordinary HTTPS traffic, which will help prevent inadvertent blocking.



⚡ Timestamping service architecture (Cloudflare Workers in Rust, using a Durable Object for storage).

Learn more about Cloudflare's work on privacy-enabling technologies

- ✓ Code Auditability
- ✓ Privacy Gateway
- ✓ Privacy Proxy
- ✓ Cooperative Analytics
- ✓ [Cloudflare Privacy Edge](#)



Working together to secure the Internet

Collaboration and information sharing are essential to cyber security. Cloudflare supports a number of public-private partnerships and initiatives that help us better protect our customers and critical infrastructure.

Pledging to secure by design

Cloudflare helps build products that make world-class cyber security and privacy tools simple and affordable enough for anyone to use. Cloudflare welcomed the US CISA's new guidelines and recommendations that encourage all technology companies to integrate secure by design principles. We were proud to commit to the Secure by Design pledge, and encourage others to do the same.

Customized threat intelligence and information sharing

Cloudflare formed a strategic partnership with the US Department of the Treasury and the Department of Energy's Pacific Northwest National Laboratory to create custom threat intelligence feeds for our customers. The new partnership will allow the government to share information about malicious websites, phishing attacks, and other cyber security threats more efficiently with Cloudflare customers, particularly financial institutions.

Learn more about Cloudflare's work with public-private partnerships

[Joint Cyber Defense Collaborative \(JCDC\)](#)

[JCDC Free Cybersecurity Services and Tools](#)

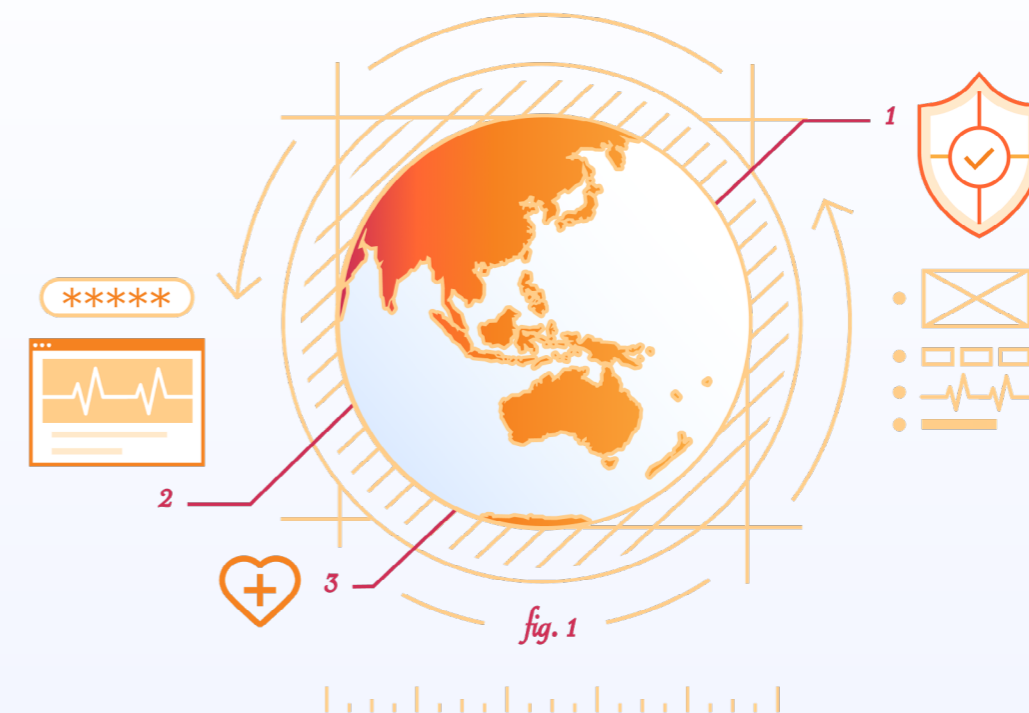
[National Cybersecurity Center of Excellence](#)

[Alliance for Cybersecurity \(BSI\)](#)

[Digital Partnership of the Council of Europe](#)

[White House Internet Routing Security Working Group](#)

[IT Sector Coordinating Council](#)



Announcing Project Secure Health

General practitioner clinics are the backbone of community healthcare in Australia. Cloudflare is helping improve these clinics' cyber security practices by providing free access to our Zero Trust security tools for free. We are also partnering with the Critical Infrastructure Information Sharing and Analysis Centre (CI-ISAC) in Australia, which is a nonprofit organization that builds collective defenses of Australia's critical infrastructure through sharing cyber threat intelligence.

Building trust through transparency

Trust is the foundation of our business. We earn trust by respecting the sanctity of personal data transiting our network, and by being transparent about how we handle and secure that data.

Trust Hub

Cloudflare's Trust Hub is a publicly available resource that includes our policies, technologies, and certifications that help us earn customer trust. Our Trust Hub includes details on our approach to abuse, compliance with privacy laws like GDPR, and compliance resources, among other things.

Transparency Report

Cloudflare publishes detailed information on legal requests we receive regarding our customers, restricting access to content on our network, and responding to abuse claims. Our Transparency Report also provides information to help our customers understand the types of government or law enforcement requests we may receive, what they require, and how they might apply to data stored on or transiting our network.

Warrant Canaries are a 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. This list is kept up to date on cloudflare.com/transparency.



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 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.

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.

ISO 27018:2019

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

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.

FedRAMP Moderate

Cloudflare maintains FedRAMP Moderate authorization, allowing federal agencies to adopt Cloudflare’s performance, security, and Zero Trust solutions.

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.

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).

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.



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

[Trust Hub](#)

[Privacy Policy](#)



[GDPR Compliance](#)

[US Privacy Law Compliance](#)

Implementing our human rights principles

Cloudflare is committed to respecting human rights under the United Nations Guiding Principles on Business and Human Rights (UNGPs) and protecting and advancing privacy and freedom of expression as part of the Global Network Initiative (GNI).

How we implement our human rights commitments

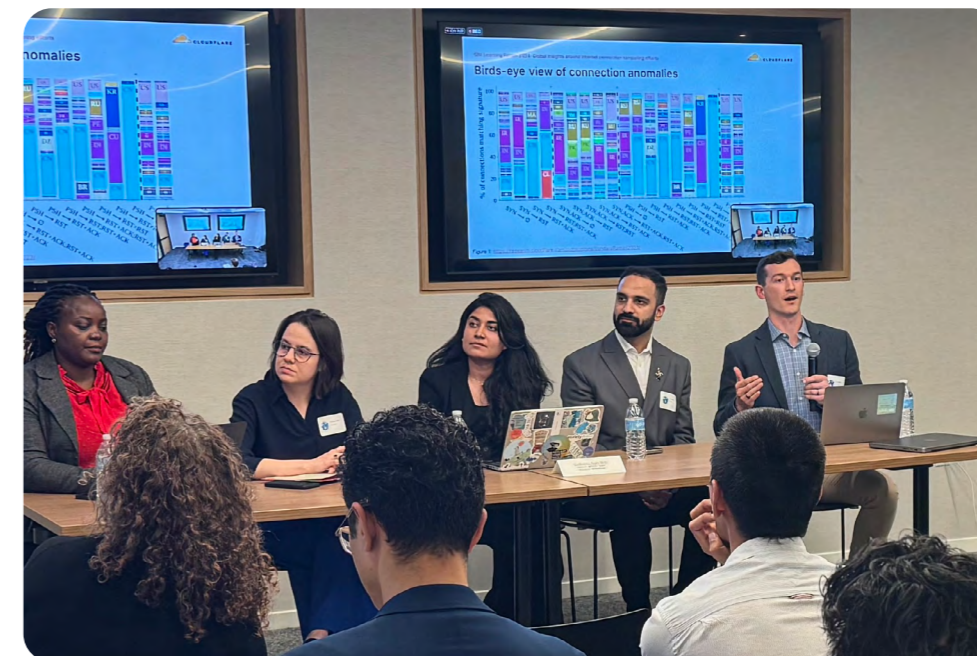
-  Due diligence
-  Respecting the privacy of personal data
-  Respecting our employees
-  Addressing abuse
-  Being transparent
-  Assessing our supply chain
-  Supporting human rights defenders

Assessment and accountability

Cloudflare applies the same transparent approach to implementing our human rights commitments as we do to any other part of our business. We work with academic, civil society, and independent experts to evaluate our policies, processes, and human rights impacts. Cloudflare is preparing for its second GNI assessment, which will be independently reviewed and subject to approval by the multistakeholder GNI board of directors. We also commissioned an independent human rights advisory firm to evaluate the human rights impacts of certain Cloudflare products.

An Internet built on human rights

Cloudflare works with civil society experts around the world to advocate for regulations and policies that are based on human rights principles. We support protection of user data, access to privacy-enhancing technologies, multistakeholder governance, and access to information. We help raise awareness and share data regarding government practices that appear to violate human rights like Internet shutdowns, blocking, and connection tampering.



<< Cloudflare presented new research on Internet connection tampering to civil society and human rights advocates at the GNI Annual Learning Forum

Learn more about Cloudflare's human rights commitments and work

- [Cloudflare Human Rights Policy](#)
- [Cloudflare's Approach to Law Enforcement](#)
- [Privacy & Data Protection](#)
- [Cloudflare Transparency Report](#)
- [Our Approach to Abuse](#)
- [Reporting Abuse](#)
- [Applying Human Rights Frameworks to Our Approach to Abuse](#)



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.

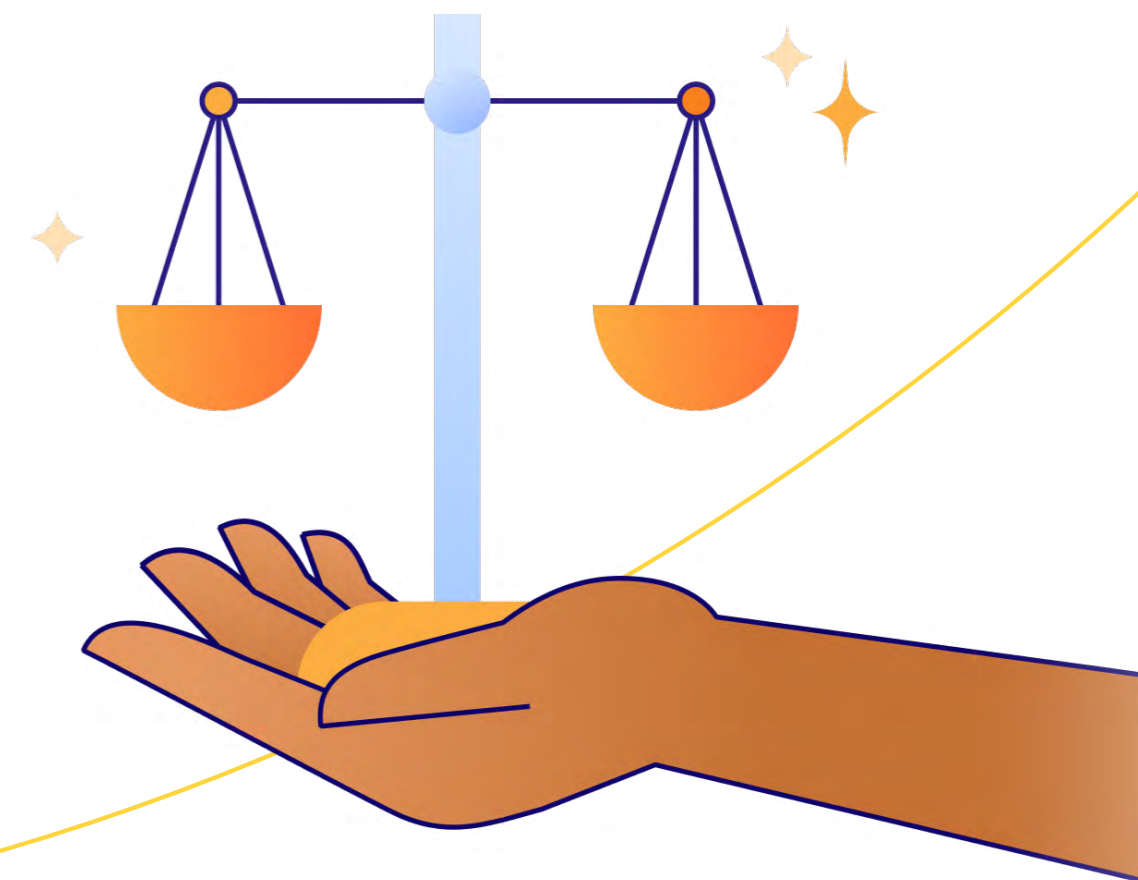
Fair labor and modern slavery

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 2023.

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.





A better Internet is for everyone.

Reaffirming our commitment to free

We offer a Free plan out of more than goodwill — it is a core business differentiator that helps us build better products, drive growth, and keep costs low. And it helps us advance our mission.

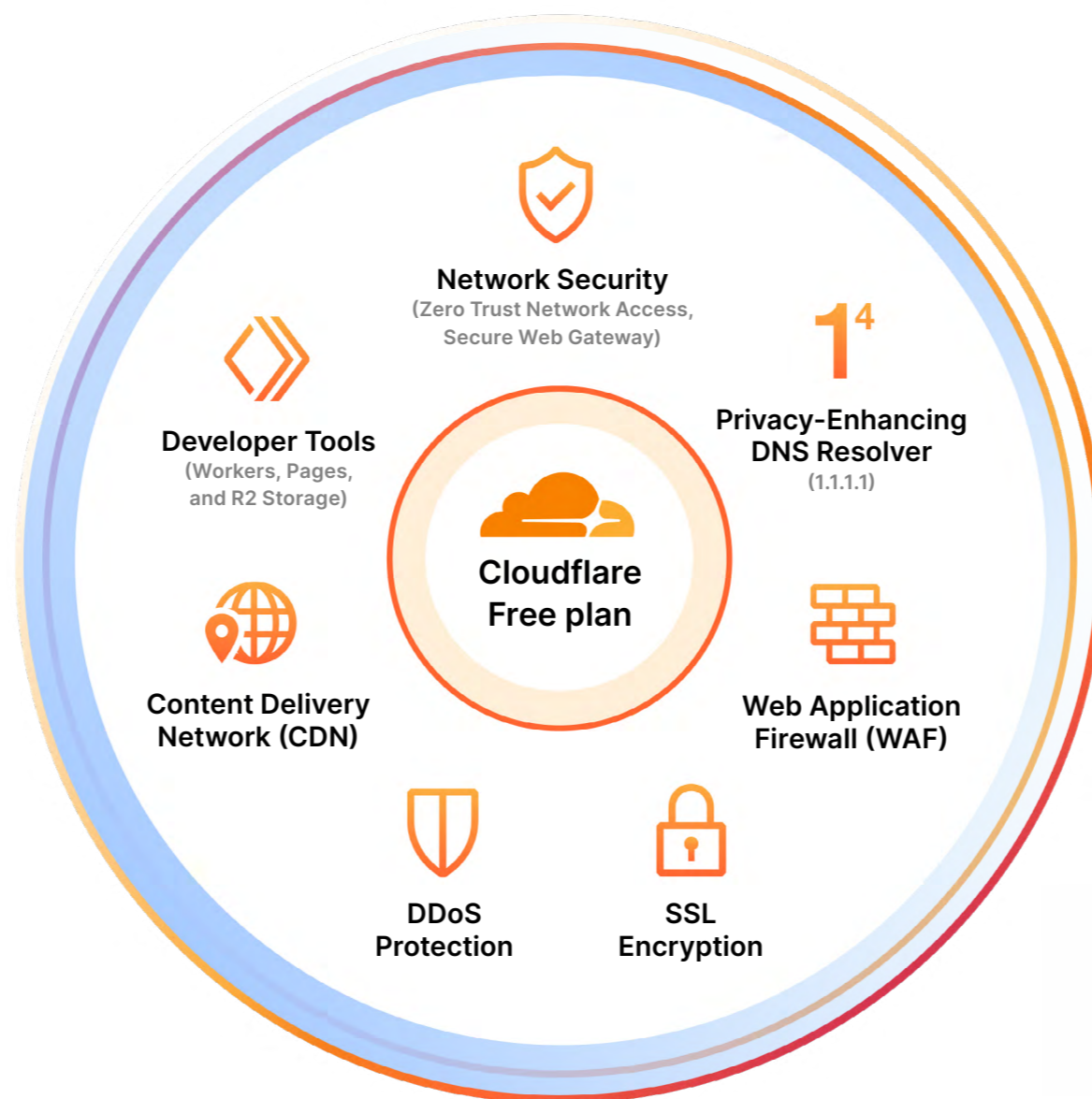
Supporting our mission

Building a better Internet is a collective effort. Today, more than 30 million Internet properties, making up some 20% of the web, sit behind Cloudflare. Our Free plan makes that portion of the web faster, more secure, and more efficient. Free is not just a commitment — it's a cornerstone of our strategy. Cloudflare's goal has always been to make world-class security and performance tools free and easy enough for anyone to use.

Today, more than **30M** Internet properties, making up some **20%** of the web, sit behind Cloudflare.

Better, more secure products

Our Free plan gives Cloudflare access to unique threat intelligence. A wide surface area exposes our network to diverse traffic and attacks that we would not otherwise see, often allowing us to identify potential security and reliability issues at the earliest stage. Like an immune system, we learn from these attacks and adapt to improve our products for all customers.



“Cloudflare always has, and always will, offer a generous free version for public-facing applications, internal private networks and people, and developer tools.”

[Cloudflare blog, September 2024](#)

New free services in 2024

Cloudflare pays back the benefits we receive from our Free plan by constantly improving our free offerings. This year we added 16 updates to our Free plan, including Turnstile, Cloudflare's privacy-focused CAPTCHA replacement that is now free for unlimited use by any website owner on any platform. We also released a new feature that automatically checks whether a customer's password has been leaked somewhere online and is known to potential attackers.

To see the complete list of new products and features added to our Free plan in 2024, please visit the [Cloudflare blog](#).

Empowering the open source community

We believe in the power of open source. It's more than code, it's the spirit of collaboration, innovation, and shared knowledge that drives the Internet forward.

Expanding our support for open source with Project Alexandria

Open source projects are vital to the continued health of the Internet. Cloudflare uses open source software (OSS) in our own products, and we provide free services to support other nonprofit OSS projects like Git and the Linux Foundation. Project Alexandria is a dramatic expansion of our previous open source support program that provides more flexibility, more choice, and new free Cloudflare services to help every OSS project not only survive, but thrive.

Open sourcing Pingora

Cloudflare released our custom-built framework for managing Internet traffic on our network to the open source community for free. Pingora is a faster, more efficient, more flexible, more secure system, built on a memory safe programming language. Early [deployment](#) has shown that Pingora uses roughly 70% less CPU and 67% less memory compared to our old service, and saves our customers and users 434 years of TLS handshake time every day.

“

Partnering with Cloudflare marks a significant milestone in our mission to support and sustain vital JavaScript and web technologies. Cloudflare's expertise in security and performance will be invaluable in ensuring the health and resilience of our open source projects.”

Robin Bender Ginn, Executive Director,
OpenJS Foundation

Want to join Project Alexandria?

If you're 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](#)

Sponsorships

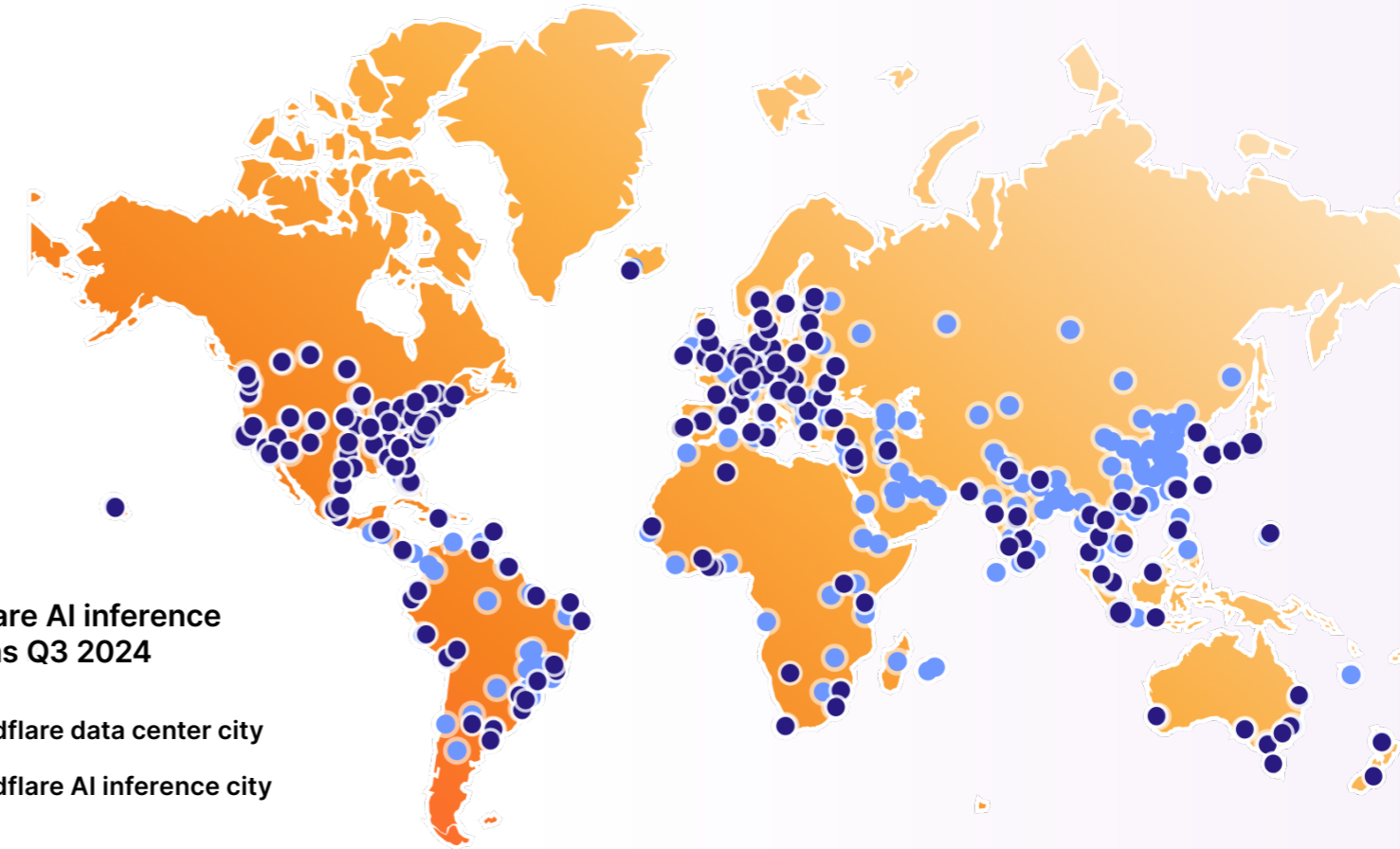


Responsible AI for everyone

Cloudflare is providing tools that bring affordable, powerful, and responsible AI inference to anyone, anywhere on Earth.

AI inference-as-a-service

Cloudflare wants to make it easier and more affordable for anyone to build and deploy AI applications. Our full-stack AI building blocks are designed to allow engineers to go from zero to production in minutes. Because AI applications built on Cloudflare are created directly on our edge network, they are instantly available and nearly infinitely scalable all over the world. Cloudflare AI tools are serverless, which means developers can spend less time on infrastructure and more time on their ideas.



AI everywhere

Cloudflare is obsessed with improving the performance of applications. We now have GPUs at more than 180 cities across our network, doubling our capacity over the past year. We are also deploying more powerful GPUs, which give our customers access to significantly larger models. Deploying AI-capable GPUs closer to users reduces latency and speeds up AI applications.

More choice and control

Cloudflare's AI developer tools are compatible with nearly any major AI model. Building AI applications on Cloudflare also allows developers to monitor, control, and optimize their applications' interactions with commercial AI models. This helps our customers control costs and avoid being locked into one provider.

Investing in technical standards efforts

Standards have allowed the Internet to grow from a collection of discrete networks to the miracle it is today. They allow anyone to connect, exchange data, and create new ideas.

Standards are the common technical language that allow hardware and software from all over the world to connect and work together. Standards like Transmission Control Protocol/Internet Protocol (TCP/IP) and HyperText Transfer Protocol (HTTP) helped found the Internet because they allowed millions of machines and developers to connect and share data. Standards development is an open and collaborative process, based on technical viability and consensus.

Why we participate in standards development

Cloudflare invests significant resources in tracking, participating in, and leading technical standards efforts in venues like the IETF and W3C. An open and transparent standards process helps our customers interoperate with other services or technologies on the Internet and enables everyone to build new products and try new ideas without getting locked into a single provider's ecosystem.

Helping encrypt web traffic

Encrypted Client Hello (ECH) is a protocol extension that makes it harder for third parties to see what websites you are visiting online, expanding user privacy. Cloudflare has enabled ECH by default for all of its customers using the Free plan.

“

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 2024



Learn more about Cloudflare's work with on privacy and security standards

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

Anatomy of a DDoS attack

Distributed denial-of-service (DDoS) attacks are used by powerful actors online to attack freedom of expression, disrupt economies, and compromise critical infrastructure. We believe DDoS attacks can be made obsolete.

Cloudflare provides access to unmetered and unlimited DDoS protection to the public, for free — no matter the size, duration, and frequency of attacks.

What is a DDoS attack?

A DDoS attack is a cyber attack that overloads Internet properties with traffic to make them inaccessible to legitimate users. It is considered a low-cost, high-impact attack method with a low barrier of entry. DDoS attacks are like traffic jams, preventing commuters from reaching their destination.

DDoS attacks on the rise

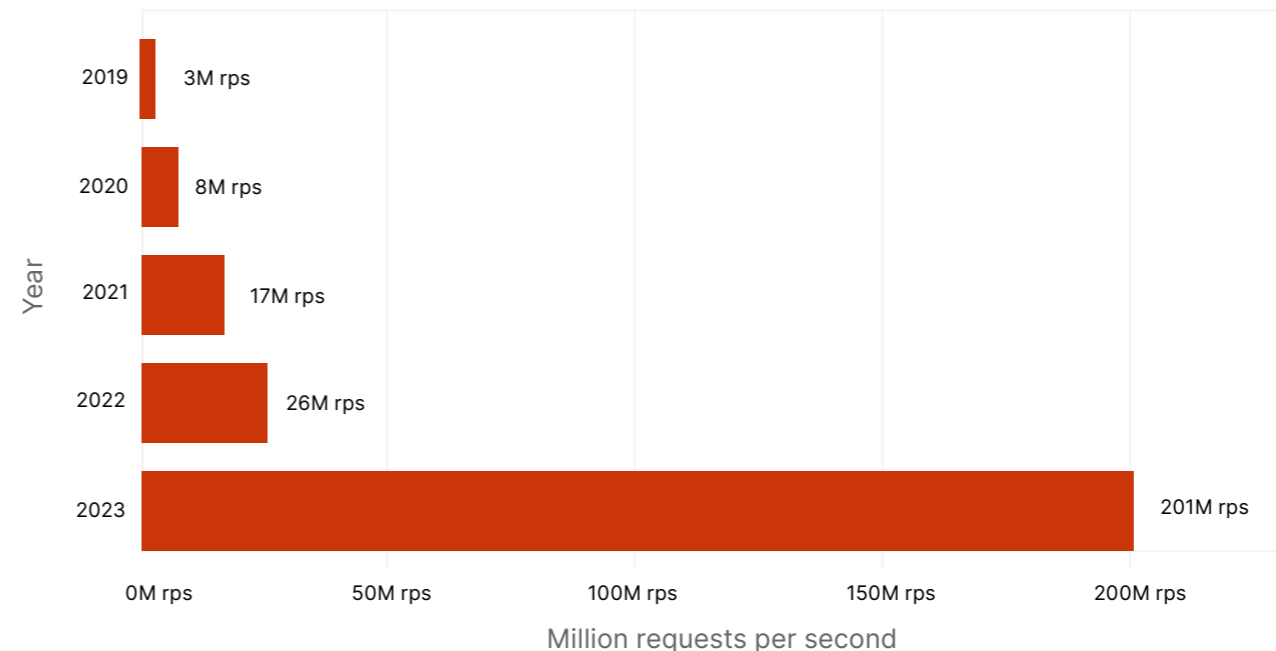
In the third quarter of 2024, DDoS attacks increased by 49% from the previous quarter and 55% over the same period in 2023. This year, Cloudflare mitigated over 14.5 million DDoS attacks, which is an average of 2,200 attacks every hour. The largest attacks peaked at 5.6 terabits per second (Tbps) and 2.1 billion packets per second. To date, 5.6 Tbps is the largest attack publicly reported by any organization. DDoS attacks have also increased against civil society organizations. For example, in 2024 Cloudflare reported blocking an attack on Meduza, an independent journalism site covering Russia, that peaked at 7 million requests per second.

14.5 million

DDoS attacks mitigated by Cloudflare this year

Largest HTTP DDoS attacks

As seen by Cloudflare by year



Want more up-to-date information on DDoS attacks and trends? Visit the [Cloudflare blog](#).

Learn more about DDoS attacks in the [Cloudflare Learning Center](#)

[What is a DDoS attack?](#)

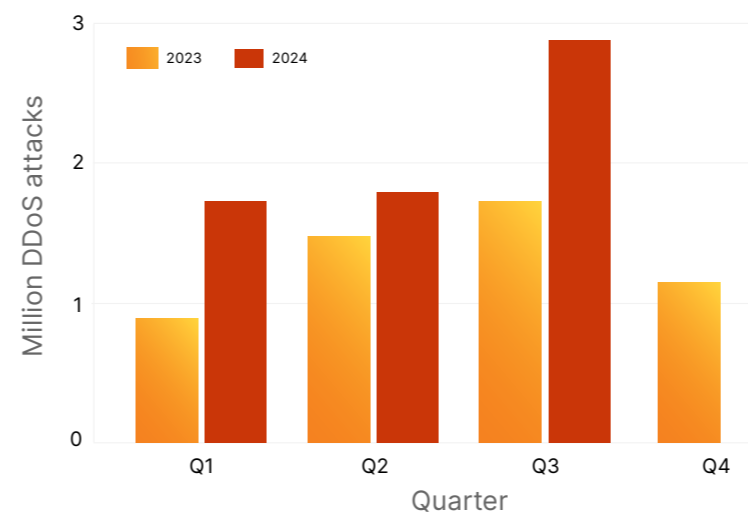
[What is a DDoS botnet?](#)

[What is a DNS flood?](#)

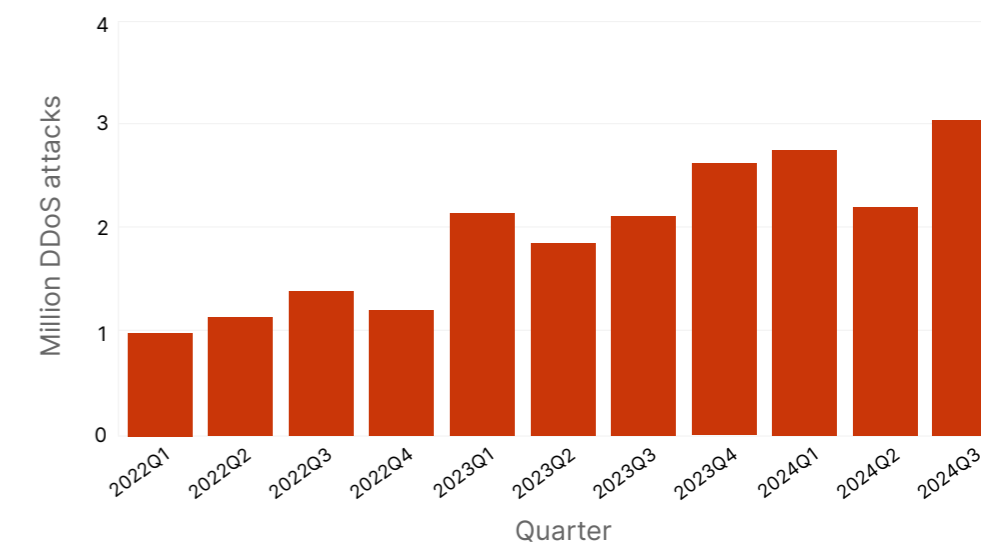
[How are DDoS attacks mitigated?](#)



HTTP DDoS attacks by quarter



L3/4 DDoS attacks by quarter



Cloudflare Radar

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, attacks, shutdowns, and anomalies around the world.

EST. 2020

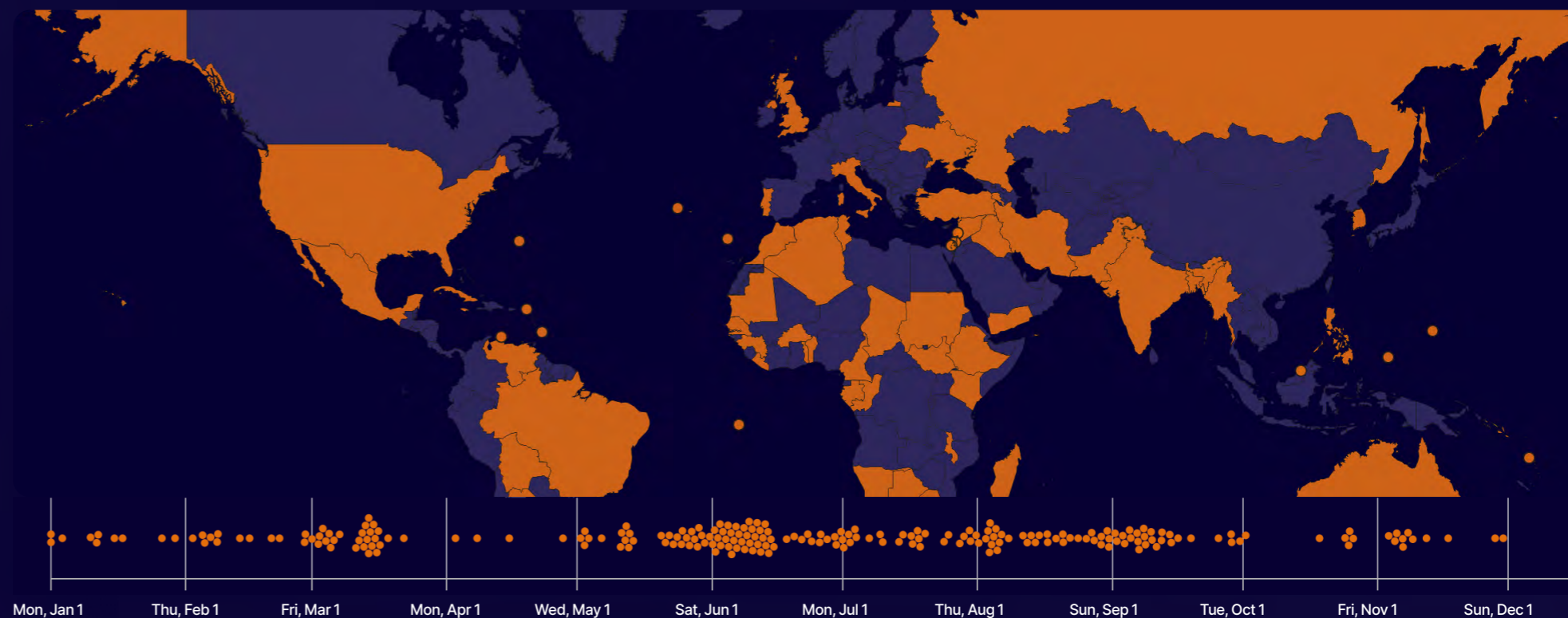
Most attacked industries



Gambling/games organizations were the most targeted in 2024

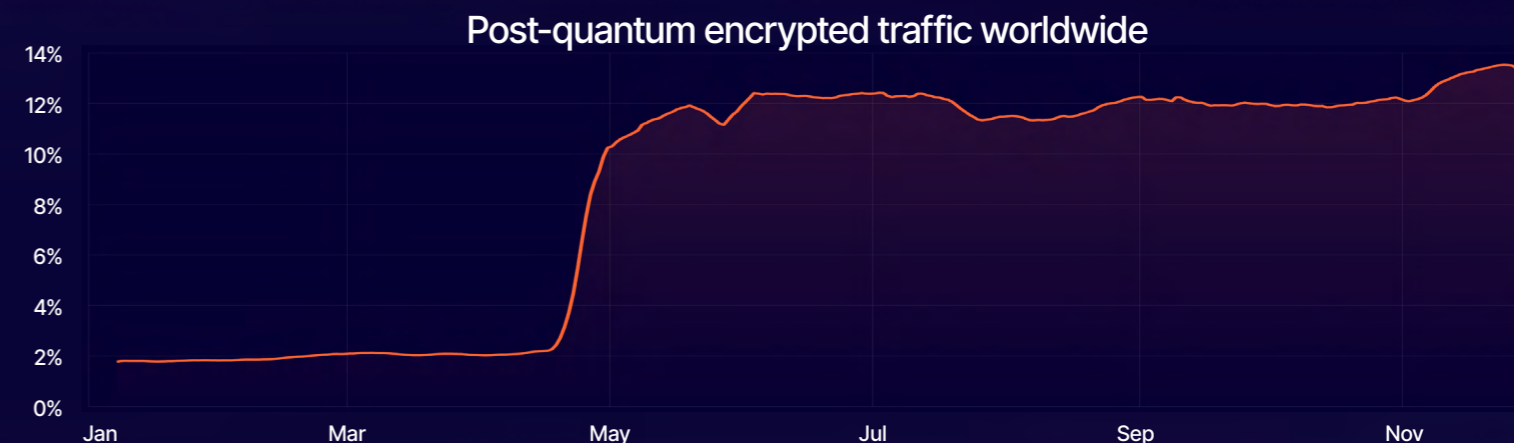
Internet outages

225 major Internet disruptions observed globally



Post-quantum encryption

13.0% of TLS 1.3 traffic is using post-quantum encryption

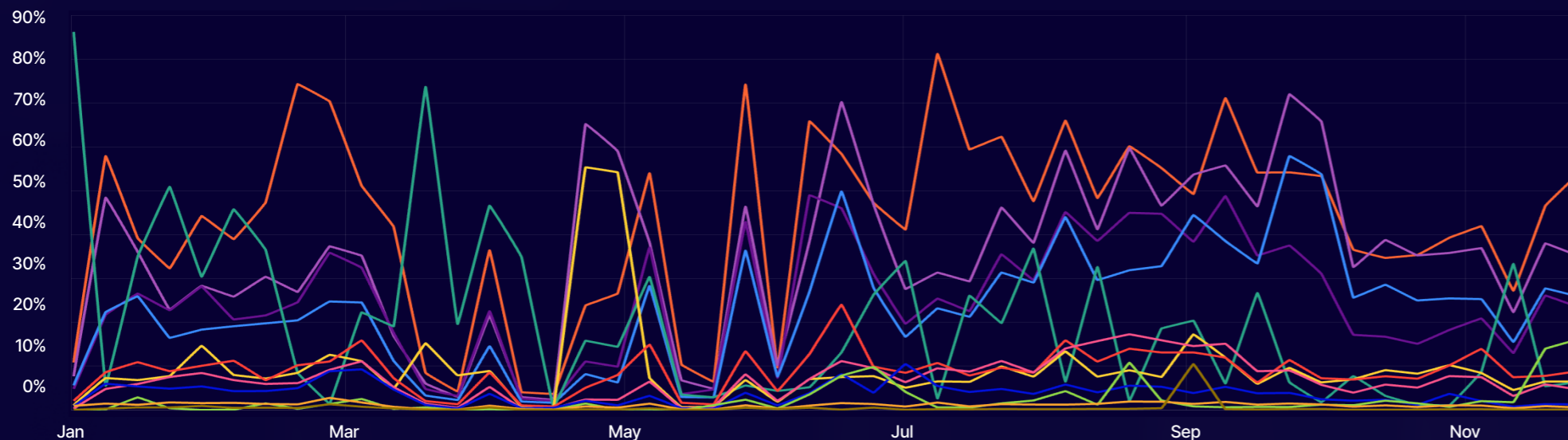


Top email threats

42.9% of malicious emails contained a deceptive link

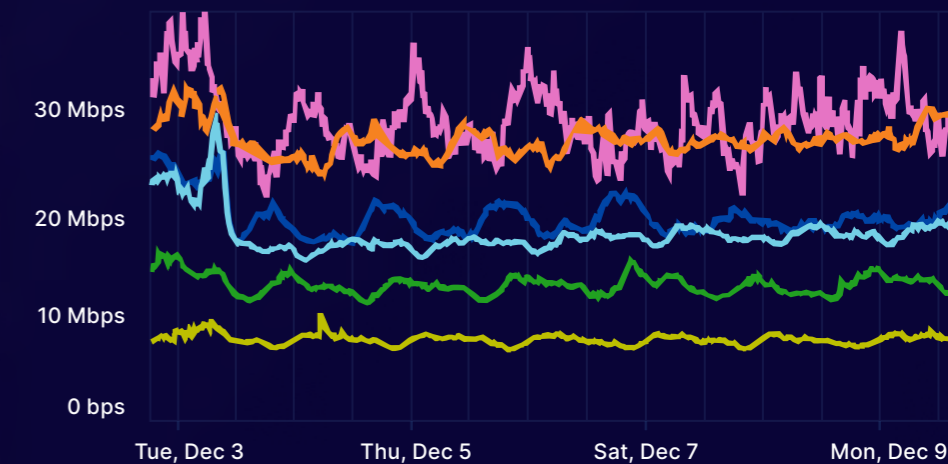
Threat category percentage

- Deceptive Link 42.9%
- Identity Deception 35.1%
- Credential Harvester 24.6%
- Brand Impersonation 23.3%
- Extortion 19.7%
- Attachment 9.5%
- ASN Reputation 9.0%
- Account Compromise 7.0%
- Scam 3.7%
- Domain Age 2.2%
- BEC 1.1%
- Voice Phishing 0.5%

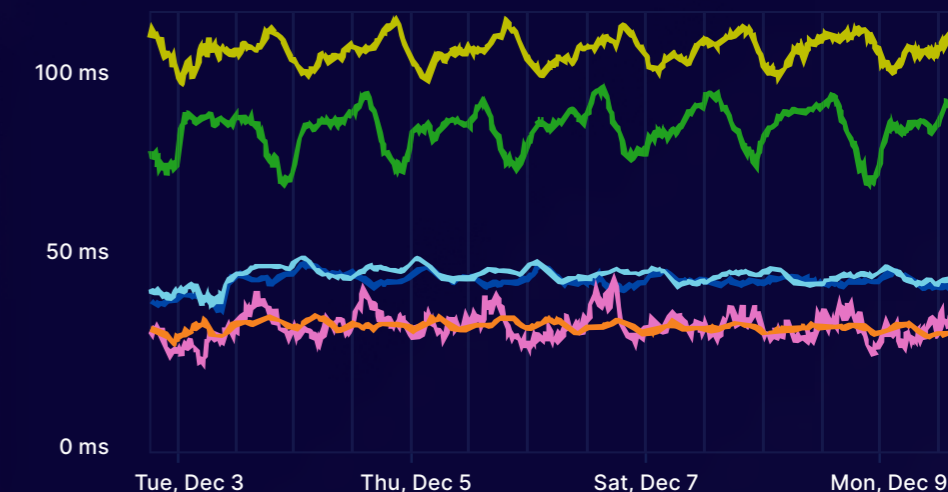


Internet quality

Bandwidth by continent



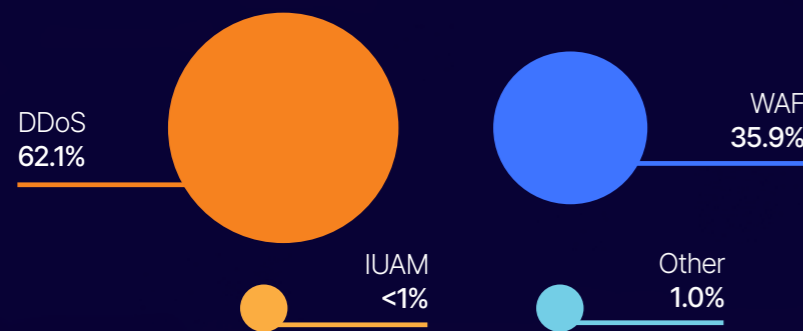
Latency by continent



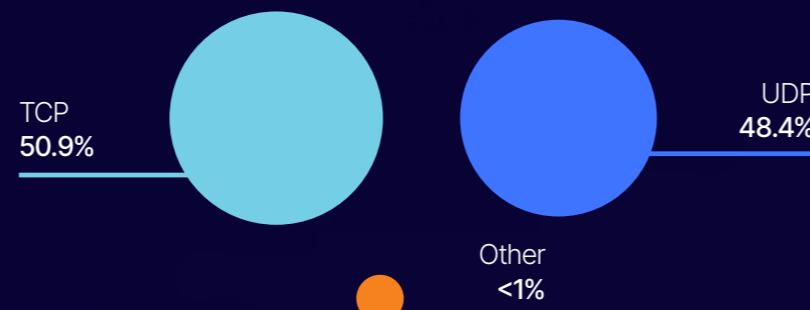
- North America
- South America
- Europe
- Africa
- Asia
- Oceania

Security and attacks

Layer 7 attacks | Top mitigation techniques



Layer 3 & 4 attacks | DDoS attack type



Radar in focus: connection tampering

Connection tampering allows third parties to block access to information online by disrupting an Internet connection. Cloudflare published a groundbreaking peer-reviewed study documenting the use of connection tampering at scale and around the world.

Connection tampering is a way for a third party to block access to content online by disrupting an Internet connection. There are two primary methods for a third party to force a connection to close: dropping packets to induce timeouts, or injecting forged reset packets into an existing message.

To identify potential connection tampering, Cloudflare researchers examined a variety of connection anomalies, which are unexpected drops in an established Internet connection before any useful data is exchanged. One explanation for repeated connection anomalies is intentional connection tampering. Across the company's network, about 20% of all connections to Cloudflare closed unexpectedly. Although some low rates of connection anomalies are expected, higher rates, particularly those consistent with known tampering observed in other reporting, suggest intentional disruption.

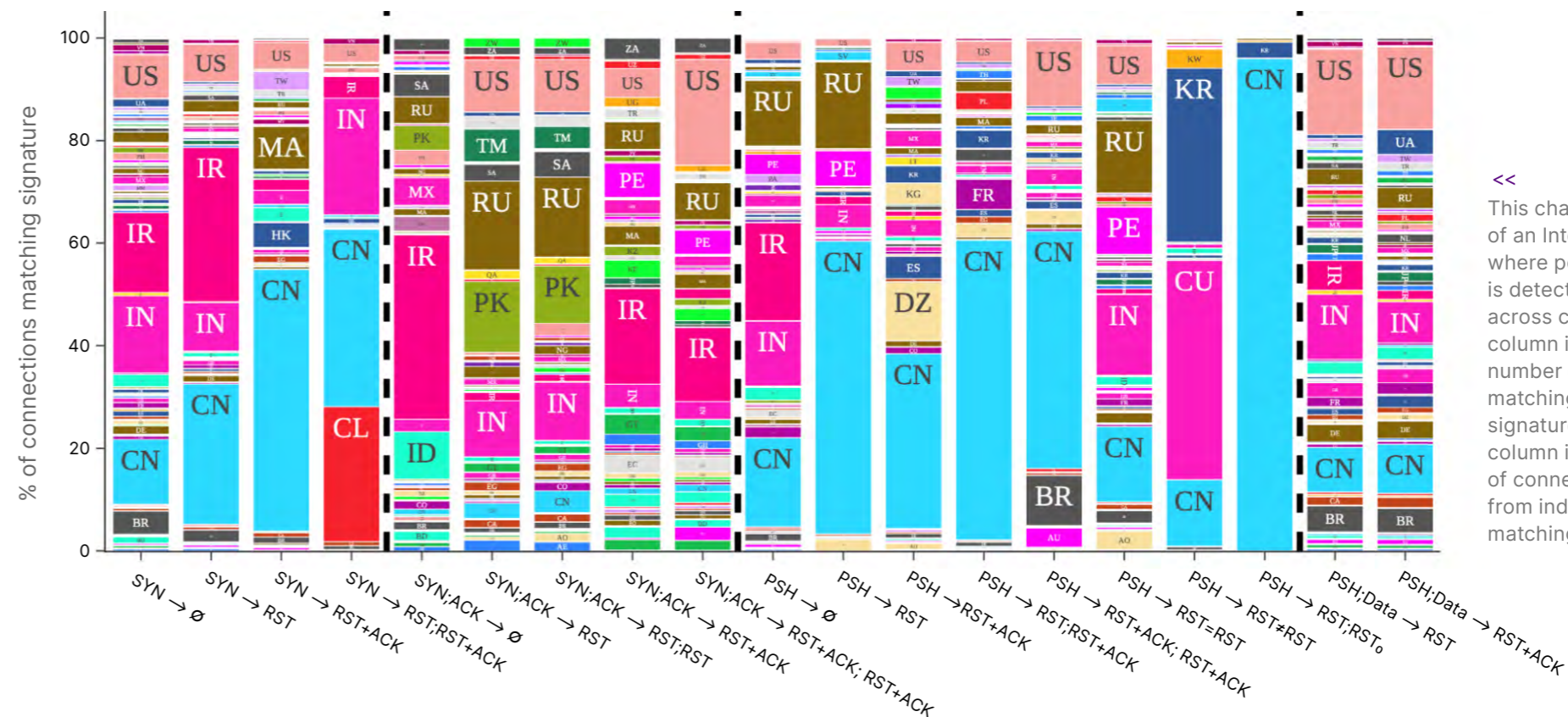
Among all connections from Turkmenistan (TM), Russia (RU), Iran (IR), and China (CN), roughly 80%, 30%, 40%, and 30%, respectively, were classified as anomalous. By comparison, about 10% of connections from Great Britain (GB), the United States (US), and Germany (DE), respectively, were classified as anomalous.

[Learn more about Cloudflare's work on connection tampering](#)

[A global assessment of third-party connection tampering](#)

[Global, passive detection of connection tampering](#)

[Cloudflare Radar TCP resets and timeouts dashboard](#)

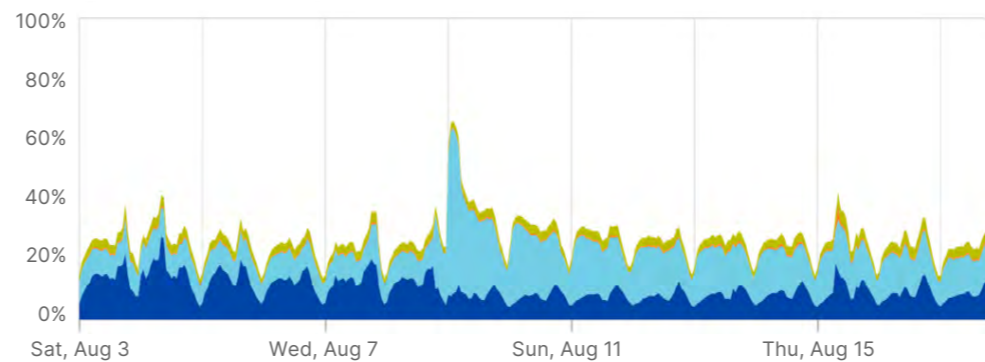


<< This chart shows the stage of an Internet connection where potential tampering is detected, organized across countries. Each column is the total global number of connections matching a specific signature. Within each column is the proportion of connections initiations from individual countries matching that signature.

TCP resets and timeouts in Pakistan

Percentage of TCP connections terminated within the first 10 packets by a reset or timeout

Post SYN: 10.3% | Post ACK: 13.2% | Post PSH: 0.5% | Later: 2.7%

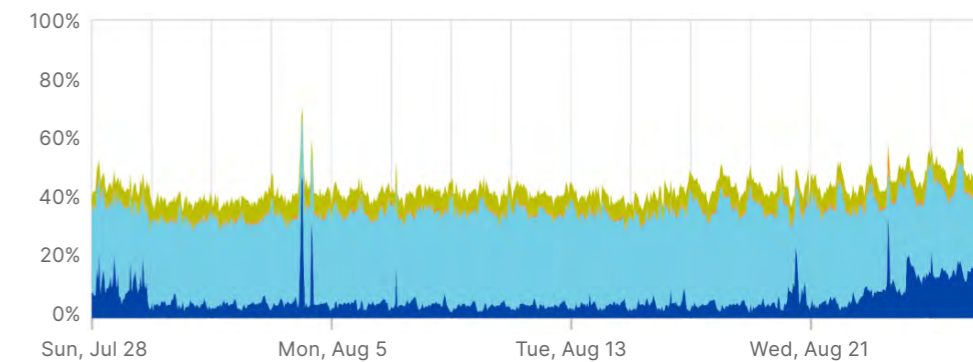


Aug 3 2024 00:00 UTC → Aug 17 2024 23:45 UTC

TCP resets and timeouts in Tanzania

Percentage of TCP connections terminated within the first 10 packets by a reset or timeout

Post SYN: 6.7% | Post ACK: 30.1% | Post PSH: 0.6% | Later: 6.0%



Jul 28 2024 00:00 UTC → Aug 26 2024 23:45 UTC

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 Cybersecurity & Infrastructure Security Agency (CISA) at the Department of Homeland Security, and the Department of Education.

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

Eligibility requirements

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

Types of threats mitigated

- ✓ Social engineering attacks via email
- ✓ Multichannel phishing
- ✓ Credential harvesting
- ✓ Unwanted and harmful online content

“Where other options would cost us somewhere in the thousands, we are now able to secure devices for free using one of the simplest and scalable platforms, featuring one of the easiest learning curves I’ve worked with.”

Wyatt Determan, Technology Specialist, HLWW Public School District, Minnesota

“Since implementing the Cybersafe Schools program as our secure email gateway, we’ve saved over \$5,000 per year compared to similar solutions. The program has effectively filtered out numerous malicious emails, greatly enhancing our security posture.”

Paul Strout, Network Manager, Regional School Unit 71, Belfast, Maine

“We expect school districts to go toe-to-toe with transnational criminal organizations largely by themselves. This isn’t just unfair; it’s ineffective.”

Kemba Walden, Acting US National Cyber Director

131 school districts

210K+ students and staff members protected

30 states across the country

1.1.1.1

Fast. Free. Private.

EST. 2018

1.1.1.1 is Cloudflare’s free public DNS resolver that makes DNS queries faster and more secure. Unlike most resolvers, 1.1.1.1 does not track users and sell their data to advertisers, and helps make DNS queries more secure by incorporating features like strong encryption, the DNSSEC security protocol, and query name minimization.

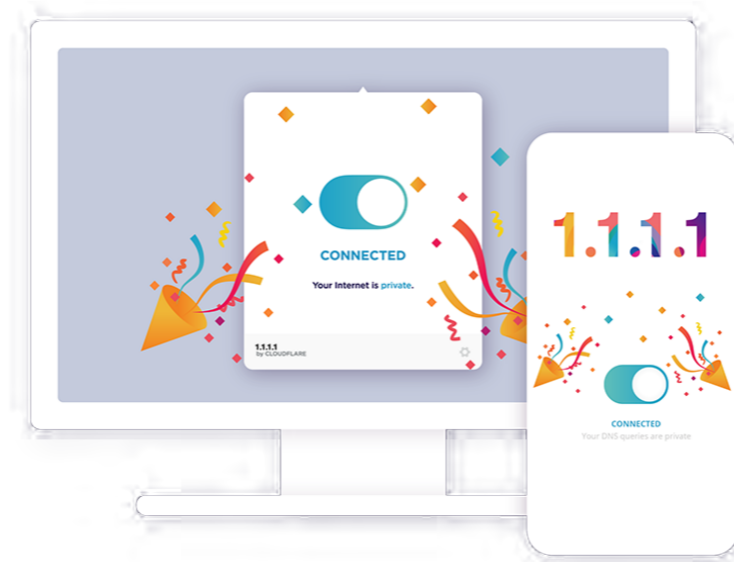
Learn more at one.one.one.one.

1.8 trillion

queries per day on average

~16 ms

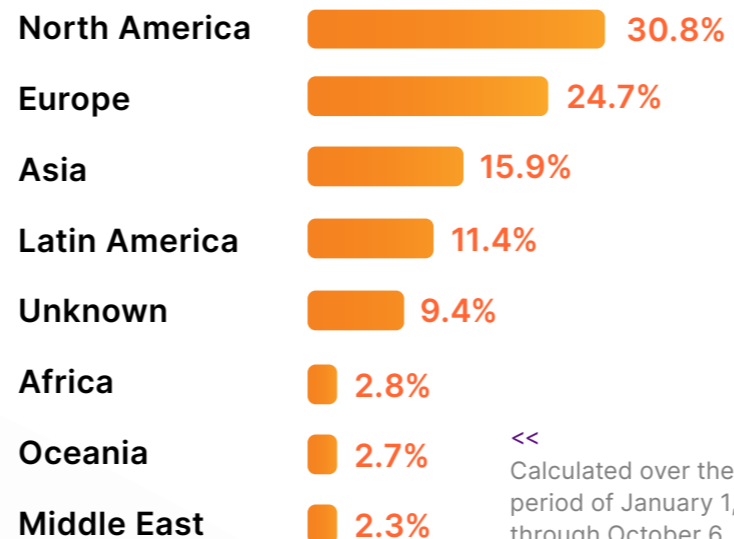
average latency
(October 2024, dnsperf.com)



What is DNS?

The [Domain Name System \(DNS\)](#) is the phonebook of the Internet. DNS translates domain names (example.com) to IP addresses so that users can access websites more easily. A DNS resolver is a type of server that manages the “name to address” translation, in which an IP address is matched to a domain name and sent back to the computer that requested it.

Distribution of 1.1.1.1 queries by region



<<
Calculated over the time period of January 1, 2024, through October 6, 2024.

Learn more about DNS in the Cloudflare Learning Center

[What is DNS?](#)

[DNS security](#)

[DNS server types](#)

[DNS records](#)



Exploring life @ Cloudflare

Cloudflare is an organization that strives to make sure our entire team feels safe and empowered to bring their whole selves to work.

Interns with impact

Through the Cloudflare intern program, we give students a chance to develop their skills by working on complex and meaningful problems, and it is rewarding to help them build their careers. This summer, Cloudflare welcomed a new cohort of interns. The dozens of interns, some of whom were returning for their second internship with the company, joined teams including software engineering, internal audit, business development, product management, research, and security analytics.

Learn more about the Cloudflare intern program at cloudflare.com/careers/early-talent.



Intern-ets!

“

This is a special program because it offers first-hand exposure to some of the most complex and challenging problems on the Internet.”

Matthew Prince, Co-Founder & CEO, Cloudflare

<< Summer interns volunteered at the Central Texas Food Bank

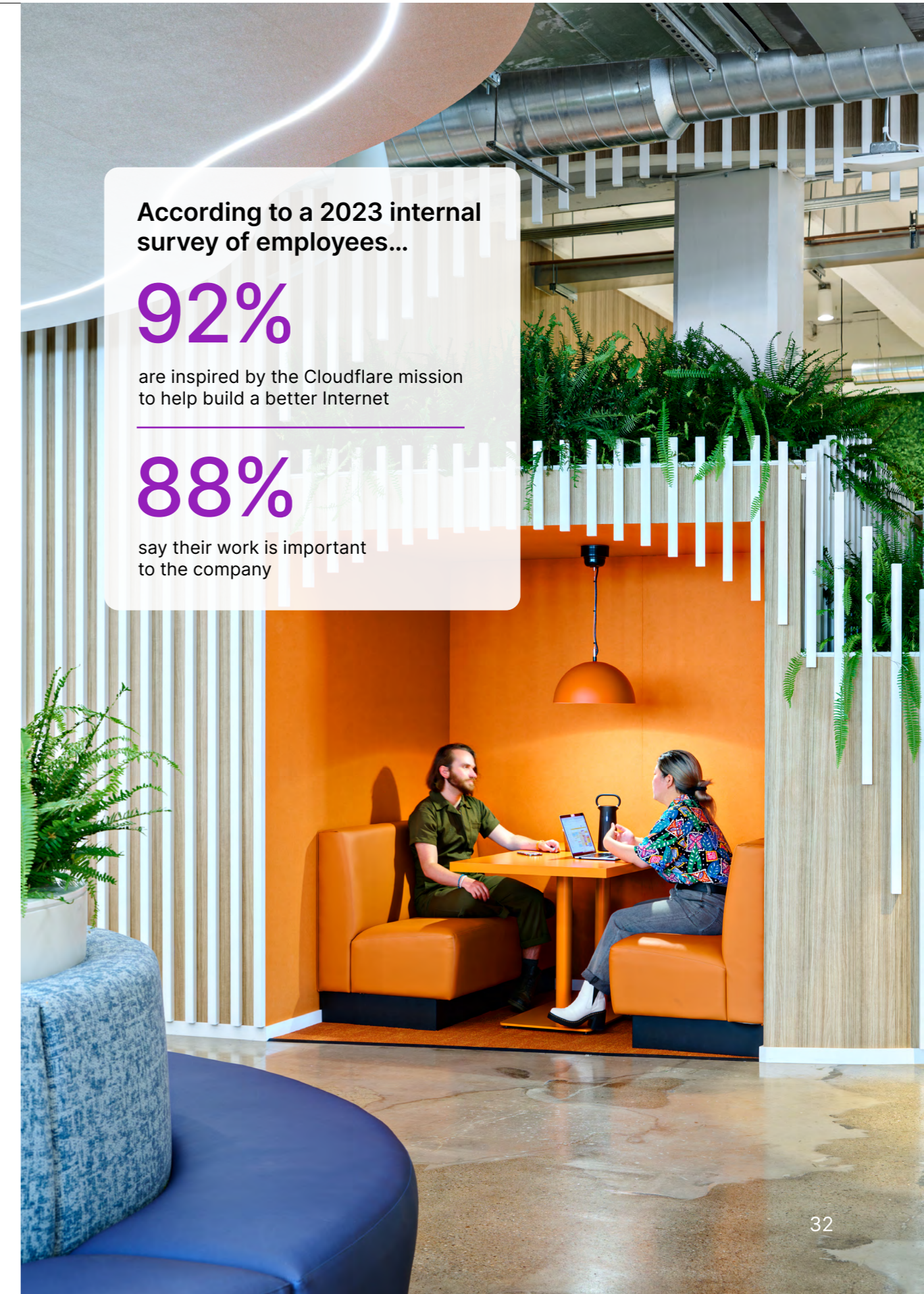
According to a 2023 internal survey of employees...

92%

are inspired by the Cloudflare mission to help build a better Internet

88%

say their work is important to the company



Creating a sense of belonging

Employee resource groups (ERGs) are just one of the ways that Cloudflarians build a community. These groups are centered on essential aspects of identity such as heritage, interests, gender, and life experience.

Learning, growing, and coming together

ERG initiatives this year included:

- Proudflare and Careflare collaborated on a volunteering event in Austin — the group helped individuals with HIV/AIDS get settled into new housing.
- At our Austin office, Afroflare held a panel discussion on Black in Tech, in which Cloudflare colleagues provided insight into their career paths and how they have navigated the dynamic landscape of the tech industry.
- Womenflare hosted a session on breaking through gender barriers, practicing self-advocacy, and honing negotiation skills — featuring Anne Doepner, senior director of diversity, equity, and inclusion for the Minnesota Vikings.



Afroflare



Arabflare



Asianflare



Careflare



Cloudflarents



Crossflare



Desiflare



Flarability



Greencloud



Judeoflare



Latinflare



Mindflare



Nativeflare



Persianflare



Proudflare



Soberflare



Turkflare



Vetflare



Womenflare

Recruiting @ Cloudflare

Year after year, we are fine-tuning our strategy for finding exceptional talent with the diverse perspectives and experiences we need to help deliver on the promise of what the Internet can truly be.

A direct line to leadership

Before receiving an offer, every candidate in the final stage connects with one of our executive leaders, including our co-founders. This has been part of our interview process for many years, and it is designed to ensure candidates truly understand what they are signing up for in their role as part of joining the Cloudflare team. It also makes our executive team accessible to everyone starting on day one, creating an open door for employees to share ideas and raise concerns.



Grace Hopper Celebration

At the Grace Hopper Celebration in Philadelphia, our team engaged with thousands of women and nonbinary people in tech. Highlights include leading a session on building inclusive and accessible web applications, conducting 30 on-site interviews, and hosting a luncheon featuring a women in tech panel.

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

RenderATL

Cloudflare colleagues collaborated with tech enthusiasts interested in developing on our Workers platform and delivered talks on getting better output from large language models, automating browser tasks, and protecting modern cloud workloads.

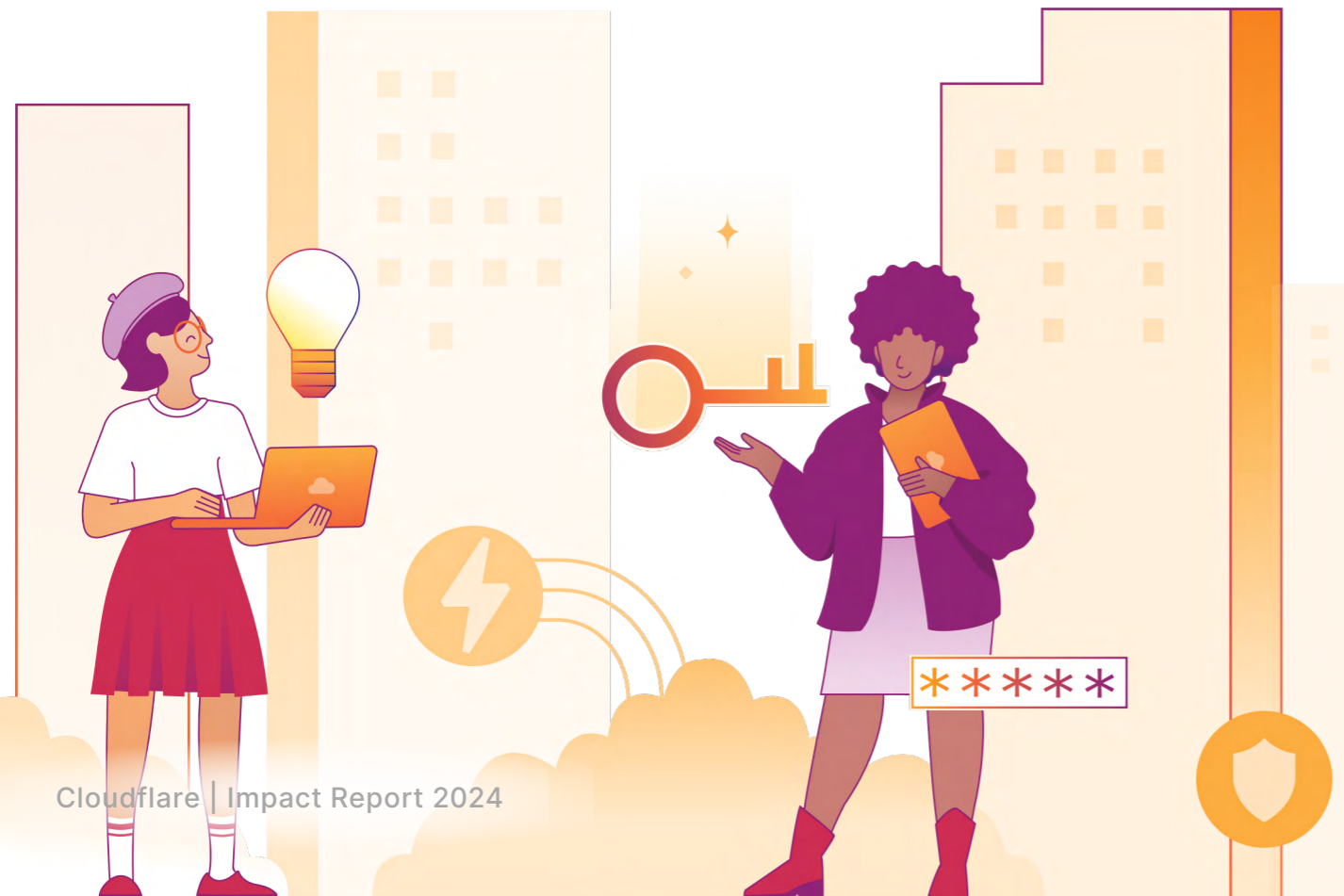
RenderATL is a continuing education >> conference for people working in tech



Mums@Work

In 2024, we partnered for the second time with Mums@Work, a group in Singapore that collaborates with employers to help support working mothers and women returning to the workplace after having children. At the #wegotyouback career convention, returnees received guidance on their resumes, advice on interviewing skills, and information about roles at the 18 partner companies participating in the event.

<< In Singapore, Cloudflare and other companies gathered with the objective of giving back to women in the local talent community









Measuring diversity at Cloudflare

Tracking data is just one small piece of our efforts to build a diverse team that thrives in an inclusive culture — and one where people are empowered to do their best work. However, it is an important part of being transparent about our progress and continued efforts.

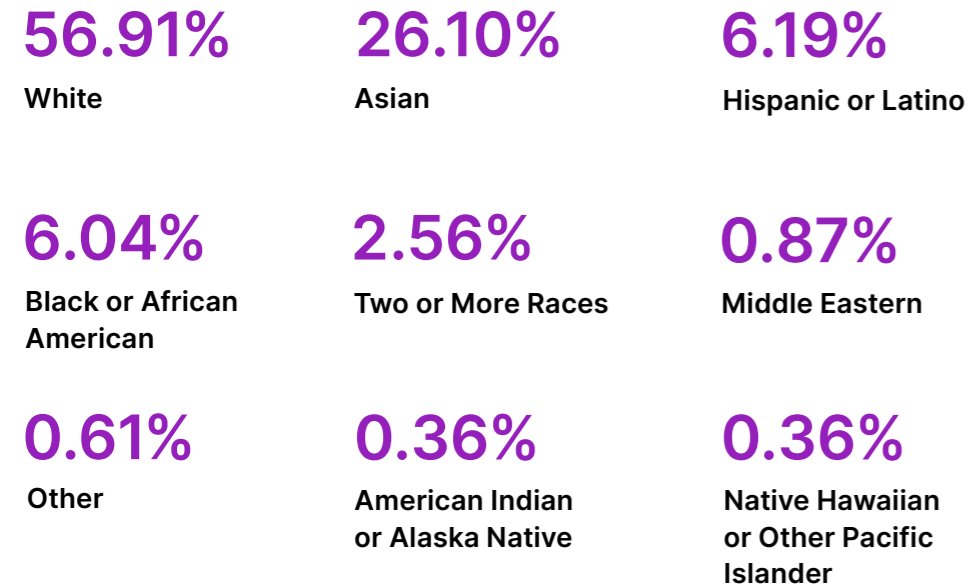
Throughout the hiring process, we evaluate applicants using the Cloudflare Capabilities, which are the values that we believe drive our culture. No matter the team, role, or seniority, all employees are expected to exhibit all six behaviors, since they are an essential part of our success. As such, our training and performance review processes are centered on ensuring these capabilities stay at the forefront of our priorities.

Get more details about our efforts on diversity, equity, inclusion education, and recruiting at cloudflare.com/diversity-equity-and-inclusion.

Cloudflare Capabilities

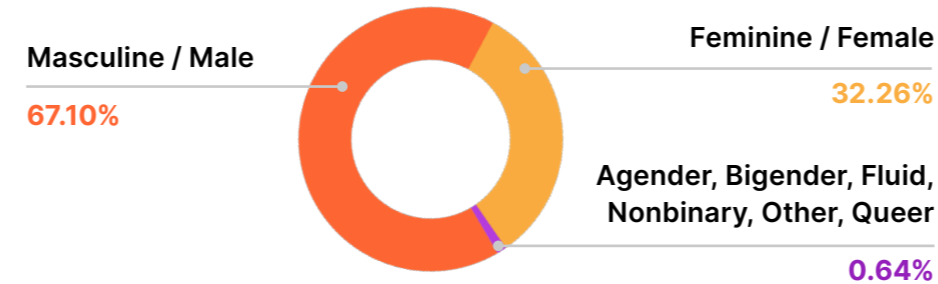
-  Be curious to learn and grow
-  Communicate clearly, directly, and transparently
-  Do the right thing
-  Embrace diversity to make Cloudflare better
-  Get your work across the finish line
-  Lead with empathy and assume good intentions

US Overall Race/Ethnicity

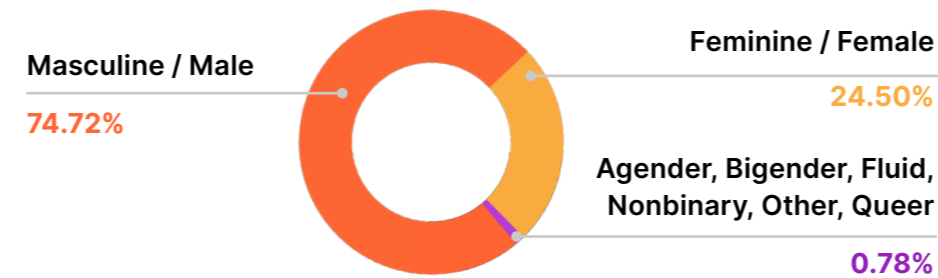


Data presented here reflects only the information shared by employees who volunteer to disclose their representation data.

Overall gender identity



Leadership gender identity



An aerial photograph of a forest. The left side of the image is dominated by a dense, vibrant green forest. On the right side, a road curves through a forest with trees in various shades of autumn, including yellow, orange, and red. A small dark car is visible on the road. The overall scene is captured from a high angle, looking down on the landscape.

A better Internet is **sustainable.**

Next-generation hardware

We are obsessed with efficiency. Every watt of energy saved is good for the planet and our business.

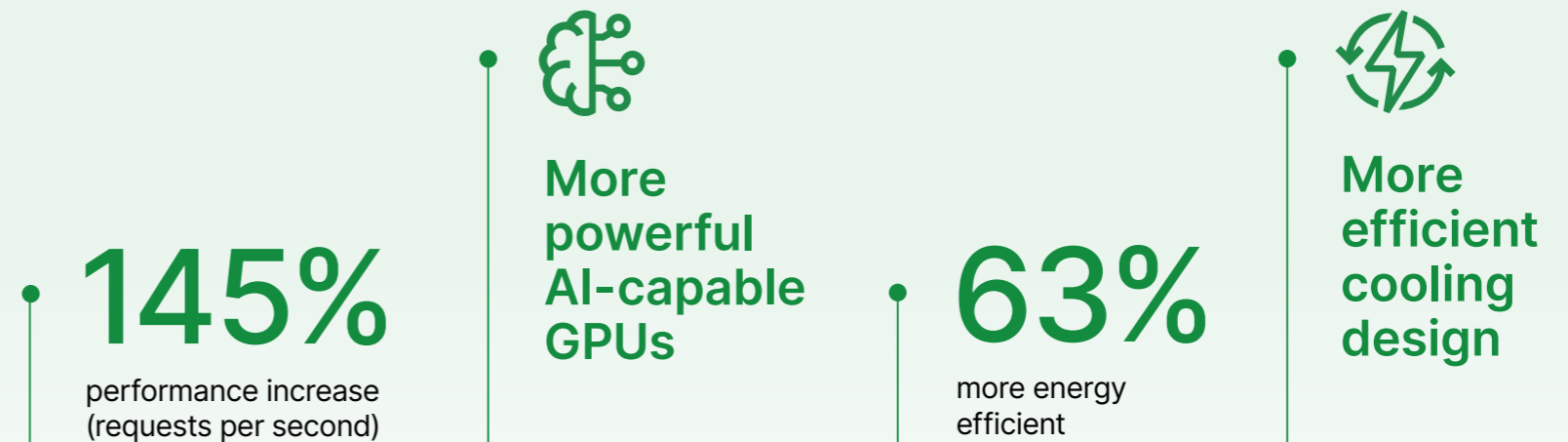
Serving Internet traffic more efficiently

Cloudflare’s 12th-generation servers are the most powerful and power-efficient servers we have ever deployed. Supporting the latest generation of AMD processors, they were designed in close cooperation with our suppliers to simultaneously process more requests per second while using less energy and supporting more powerful GPUs.

Modular design and open standards

Modular design and open standards reduce waste and encourage recycling and reuse. Modular design decouples server functions such as management and security from CPU and memory. This allows network administrators to upgrade individual parts rather than replacing an entire system or server. Open standards ensure that component modules are compatible across hardware types and leveraged by multiple vendors, which allows more parts to be resold and reused rather than being sent to landfills. Cloudflare’s 12th-generation servers incorporate modular design and open standards to help reduce embodied carbon across our network.

Cloudflare 12th-generation servers

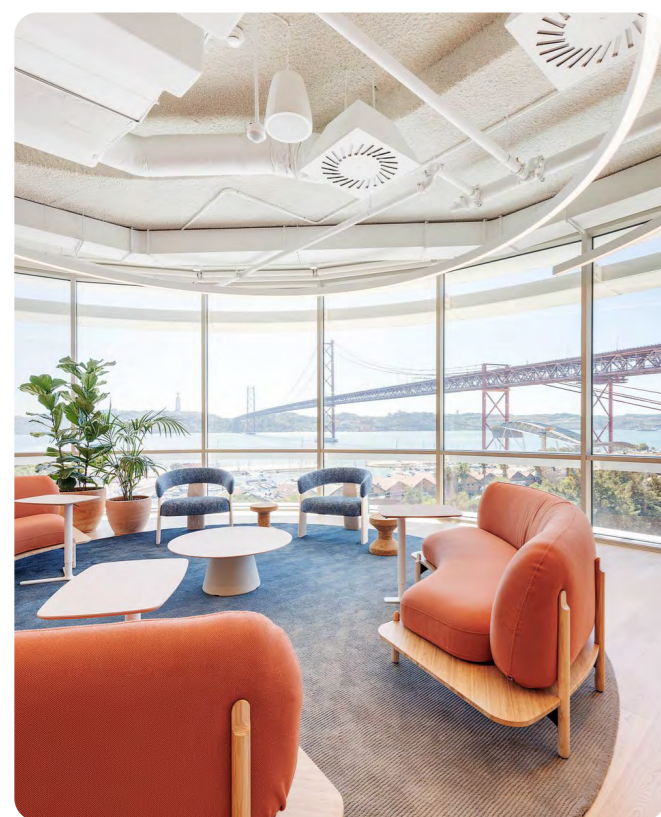
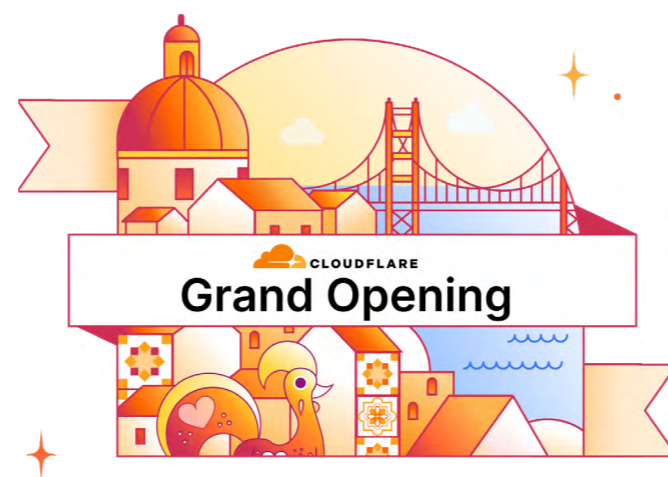


Reimagining how and where we work

Cloudflare is investing in communities and facilities that reflect how we work: creatively, collaboratively, and sustainably.

Our new Lisbon home

Cloudflare’s Lisbon office is now our largest European hub. It represents our ongoing commitment to the Lisbon community, which continues to provide a beautiful and dynamic city in which to grow our European team. To ensure we are making a positive impact on the surrounding environment, we focused on incorporating sustainable materials and accessibility features throughout the design, construction, and operation of our new space.



Cloudflare Lisbon certifications

- ✓ **LEED Gold** - According to the US Green Building Council, this rating system “provides a framework for healthy, highly efficient, and cost-saving green buildings”
- ✓ **WELL Gold** - The WELL building standard prioritizes occupants’ health and well-being
- ✓ **WiredScore Platinum** - WiredScore’s highest level of certification for our wired infrastructure, resilience, and wireless network

Sustainability from ceiling to floor

- All newly purchased private workspaces are 100% recyclable
- Open areas and meeting rooms use carpet made from 100% recyclable materials
- In our boardroom-style space, wall coverings are made of cork, a rapidly renewable and naturally antimicrobial material

Designing with everyone in mind

Our efforts to help ensure accessibility in the office include:

- Inclusive seating options
- Automatic doors
- Height-adjustable tables

Top and bottom photos courtesy of Vector Mais >>



Tracking greenhouse gas emissions

Greenhouse gas emissions

As part of our environmental commitments, Cloudflare publishes our companywide direct (Scope 1) and indirect (Scope 2) greenhouse gas (GHG) emissions on an annual basis. In September, we published our 2023 emissions inventory.

Our [emissions analysis](#), as described in our annual emissions inventory, 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.

To account for these Scope 1 and Scope 2 emissions, each year we purchase the same amount of zero-emissions energy, such as wind and solar, as we consume in all of our data centers and facilities around the world.

Emissions Category		Carbon Dioxide Equivalent (CO2e) in Metric Tons (MT)	Percent of Calculated Total
Scope 1		259	100%
Scope 2 (Location-based)			
	Facilities	1,110	2%
	Network	55,940	98%
Scope 2 (Market-based)		0	100%
Total (Market-based) ¹		0	100%

¹Total (market-based) emissions include Cloudflare’s 2023 verified offsets and renewable energy purchases.



Fighting back against bad bots

30% of traffic Cloudflare sees on the Internet is related to bots. Excessive bot traffic can slow service for legitimate users and in some cases be quite dangerous.

Bot Fight Mode and Super Bot Fight Mode are tools that help detect and mitigate bot traffic on a domain. They identify traffic matching the patterns of known bots and issue computationally expensive challenges in response to those bots.

Since those challenges may result in higher CPU usage by attackers, Cloudflare donates to reforestation projects each year to help account for this activity. To prioritize efficiency, our team also identifies where blocking bots is a better strategy to avoid their energy-wasting behavior.

While bad actors will keep trying to evade bot detection, we will continue to keep watch, refine our bot detection strategies, and evolve our machine learning models to help keep the Internet a place where everyone has a voice.

Good bots vs. bad bots

A bot is a computer program that automates interactions with web properties over the Internet. A good bot is any bot that performs useful or helpful tasks that aren't detrimental to a user's experience on the Internet.

Bad bots can steal data, break into user accounts, submit junk data through online forms, and perform other malicious activities. Types of bad bots include credential stuffing, content-scraping, spam, and click fraud bots.

11,740

The number of trees Cloudflare will plant to account for 2024 bot-fighting activities

98,812

Trees donated to date



A look back at recent projects

For our 2023 usage, we arranged for 28,812 trees to be planted, split between projects in Mexico and Indonesia.

In and around Mexico's Monarch Butterfly Biosphere Reserve, new trees will provide a more supportive habitat for monarch butterflies and assist with mitigating droughts and flooding, recharging aquifers, and maintaining soil humidity.

Meanwhile, in the Kubu Raya Regency in Indonesia, mangrove restoration will help stabilize fisheries and protect the essential habitat of several endangered species.

Photos of Mexico and Indonesia 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 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) 2024, 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. See GRI 305. No other section of this report was externally verified. See Shift Advantage verification letter, page 52.
	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 Filing
	2-23 Policy commitments	ESG resources: <ul style="list-style-type: none"> • 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, i2c, CCIA, TechUK, Eco, Bitkom, Germany Secure Online (Deutschland sicher im Netz), ISPA, American Chamber of Commerce Japan, Communications Alliance, Australian Information Industry Association, US-India Business Council, US-ASEAN Business Council, and US-China Business Council.

GRI Standards

SASB

GRI Standard	Disclosure	Answer
GRI 201: Economic Performance	201-2 Financial implications and other risks and opportunities due to climate change	10-K Filing
GRI 205: Anti-corruption	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>
	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>
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	<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>
GRI 302: Energy	302-1 Energy consumption within the organization	<p>Cloudflare consumed no non-renewable energy as defined under GRI 302 in CY2023.</p> <p>Cloudflare consumed 165.77 gigawatt hours (GWh) total energy in CY2023. 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 2023.</p> <p>Emissions Inventory 2023</p>

GRI Standards

SASB

GRI Standard	Disclosure	Answer
GRI 302: Energy <i>(continued)</i>	302-3 Energy intensity	Based on 2023 total revenue and energy data, Cloudflare consumed .000128 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	<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>
GRI 305: Emissions	305-1 Direct (Scope 1) GHG emissions	<p>See emissions data, page 39.</p> <p>Cloudflare recorded Scope 1 location-based emissions of 259 metric tons (MT) carbon dioxide equivalent (CO2e) in 2023. Cloudflare used the operational control consolidation approach, under the GHG Protocol.</p> <p>Emissions Inventory 2023</p>
	305-2 Energy indirect (Scope 2) GHG emissions	<p>See emissions data, page 39.</p> <p>Cloudflare recorded the following Scope 2 emissions in 2023:</p> <p>Location-based emissions: 57,050 metric tons (MT) carbon dioxide equivalent (CO2e).</p> <p>Market-based emissions: 0 MT CO2e.</p> <p>Emissions Inventory 2023</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 CY2023 location-based emissions, Cloudflare emitted .000044 MT (CO2e) per dollar of revenue generated.</p> <p>Cloudflare emitted 0 market-based emissions in CY2023.</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
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 401: Employment	401-1 New employee hires and employee turnover	In 2024 (as of October 1, 2024), Cloudflare hired 1,037 employees and experienced a turnover rate of 14.7% (as of October 1, 2024).
	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.
GRI 403: Occupational Health and Safety	403-1 Occupational health and safety management system	<p>Cloudflare’s global Safe & 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>
	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
GRI 403: Occupational Health and Safety <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. In addition, in October 2024, we began rolling out global workplace violence prevention training.
	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, family forming benefits, caregiving resources, fitness program access through a healthcare provider, 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 2024. Cloudflare experienced no high-consequence work-related injuries in 2024.
	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: Training and Education	404-1 Average hours of training per year per employee	Of the employees who participated in development training for 2024, they completed a total of 41,458 hours. On average, each employee completed 8.19 hours of training.
GRI 405: Diversity and Equal Opportunity	405-1 Diversity of governance bodies and employees	Diversity, Equity, and Inclusion at Cloudflare
	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. Diversity, Equity, and Inclusion at Cloudflare
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 2024 in which the rights of employees to freely associate or collectively bargain were at risk.

GRI Standards

SASB

GRI Standard	Disclosure	Answer
GRI 408: Child Labor	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>Human Rights Policy Third Party Code of Conduct</p>
GRI 409: Forced or Compulsory Labor	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>Modern Slavery Act Statement</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>
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 2023 that will enable the company to screen suppliers against risks, including environmental, social, and governance criteria.
GRI 415: Public Policy	415-1 Political contributions	<p>Cloudflare made no political contributions in 2024, 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>
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

SASB - Technology & Communications Sector

Software & 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 165.77 gigawatt hours (GWh) total energy in CY2023. 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 2023. Emissions Inventory 2023
	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 & 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. Transparency Report

GRI Standards

SASB

SASB - Technology & Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Answer
Data privacy & freedom of expression <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 includes 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, 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>Transparency Report</p>
	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.
Data security	TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	<p>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; FedRAMP Moderate; and C5; and has been evaluated by third-party assessors against the requirements.</p> <p>Cloudflare Trust Hub</p>

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"> • US 10% • UK 49% • Portugal 30% • Singapore 57% • Germany 31% • Australia 13% • Canada 15% • Netherlands 57% • France 23% • Japan 16% • Mexico 8% • India 0% • UAE 0% • China 0% • Korea 0% • Malaysia 0% • Belgium 100% 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	Diversity, Equity, and Inclusion at Cloudflare
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
Managing systemic risks from technology disruptions	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>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.</p>
	TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	10-Q Filing

Emissions verification letter

Cloudflare
101 Townsend St
San Francisco, CA 94107

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

6/20/2024

Dear Patrick,

Shift Advantage is pleased to provide consulting and advisory services to Cloudflare to support the calculation of Cloudflare's 2023 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 2023 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 GHG emissions. Scope 3 GHG emissions are excluded from both the footprint and from this verification. Cloudflare's total reported 2023 emissions are 57,308 MT CO₂e. Verified emissions by scope are shown below:

- Scope 1 Emissions: Direct emissions associated with natural gas used to heat offices - 259 MT CO₂e
- Scope 2 Emissions: Indirect emissions associated with purchased electricity in offices and co-located data centers – 57,049 MT CO₂e (location based)



Daniel Tremblay – Lead Verifier
Shift Advantage



This document is for informational purposes only and is the property of Cloudflare. This document does not create any commitments or assurances from Cloudflare or its affiliates to you. You are responsible for making your own independent assessment of the information in this document. The information in this document is subject to change and does not purport to be all inclusive or to contain all the information that you may need. The responsibilities and liabilities of Cloudflare to its customers are controlled by separate agreements, and this document is not part of, nor does it modify, any agreement between Cloudflare and its customers. Cloudflare services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied.

© 2024 Cloudflare, Inc. All rights reserved. CLOUDFLARE® and the Cloudflare logo are trademarks of Cloudflare. All other company and product names and logos may be trademarks of the respective companies with which they are associated.