CLOUDFLARE

Impact Report 2021

We are proud to share our first Cloudflare Impact Report.
It is a collection of the work we have done over the years,
but especially the past year, to give back to the Internet, protect
important causes and voices online, and promote sustainability.

In short, it describes how we are helping build a better Internet.

Cloudflare did not start as a mission-driven company. We launched in 2010 by offering free security services to individual developers and small businesses while we built our network and developed products we could sell. However, working with our free customers, including some doing incredibly important work like reporting on corruption in Africa, helped illustrate how small organizations often struggle to operate online in the face of powerful and persistent cyber attacks.

We started to understand that making world-class security services accessible to everyone, regardless of their ability to pay or their technical acumen, was something vitally important. It inspired us to continue to make versions of our newest privacy, security, and reliability products available to everyone for free. It also inspired us to launch Project Galileo, which allows journalists, humanitarian groups, and civil rights organizations around the world to access our highest level cyber security services for free.

Eleven years after our founding, we still strive to live that mission in everything that we do.

To that end, 2021 was an exciting year. We officially launched Cloudflare Impact, our first comprehensive corporate responsibility and environmental, social, and governance (ESG) initiative.

We also held our first Impact Week, a companywide effort dedicated to finding new ways to use our network to do good in the world. Over the course of the week, we announced 16 new initiatives, including:

• A program to help underserved communities connect to the global Internet

• New commitments on renewable energy and eliminating our historic emissions

• A tool enabling customers to automatically schedule computing tasks at the greenest parts of our network

• A product allowing customers to understand and improve their own carbon emissions

• A tool to help human rights defenders monitor Internet shutdowns

This inaugural Impact Report not only describes how we are working toward our mission but also includes our first environmental, social, and governance (ESG) disclosures to make sure we are accountable for our commitments.

We are thrilled to share the progress we made over the past year. More importantly, we are just getting started.

Matthew Prince
Co-Founder & CEO, Cloudflare

Michelle Zatlyn
President & COO, Cloudflare

Introduction

A better Internet is principled

A better Internet is for everyone

A better Internet is sustainable

Appendix

Impact @ Cloudflare

Cloudflare Impact launched in 2021 with a simple mission: help Cloudflare and the Internet do good in the world. As part of the Pledge 1% initiative, Cloudflare is committed to donating 1% of our product and our time back to our local communities and the communities we support online.

$24.4M
in donated services since 2017

2,094
Internet properties protected under Cloudflare Impact programs

100M+
COVID-19 vaccine appointments scheduled, using Cloudflare Waiting Room

2021 Spotlight: COVID-19 and Project Fair Shot

In February 2021, Cloudflare launched Project Fair Shot to provide free access to our Waiting Room service to any government, hospital, or pharmacy that is helping distribute COVID-19 vaccines.

To date, we have helped more than 100 organizations in 10 countries schedule approximately 100 million vaccinations.

In July 2021, we extended the program for an additional 12 months. To learn more, please visit **www.cloudflare.com/fair-shot**.

Waiting Room
Our service is designed for organizations with high demand for any resource — be it concert tickets, sneakers, or vaccines. By allowing individuals to queue and then allocating access, organizations can avoid frustrating site crashes. Waiting Rooms can be deployed in front of any existing registration website without requiring code changes.

"Cloudflare Waiting Room allowed us to plan for a steady load instead of having a large investment in the infrastructure for the launch. And it helped with communication because it was considered a good service to the public."

— **Maris Dreimanis, Vaccination Project Office IT Coordinator, Ministry of Health, Republic of Latvia**

"Bottom line is Cloudflare saved lives today. Our county will be forever grateful for your participation in getting the vaccine to those that need it most in an elegant, efficient, and ethical manner."

— **Tyler Penney, Web Services Administrator, County of San Luis Obispo, California, United States**
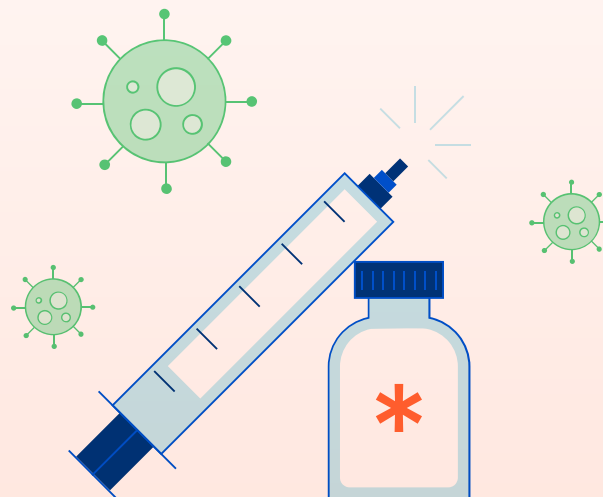
2021 Spotlight: Birthday Week 11!

Birthday Week is special at Cloudflare. It is the time that we try to give back to the Internet with new free products and services to help make a better Internet for everyone.

As we turned 11 on September 27, we celebrated by launching several new features and products that we hope will help make email and the Internet faster, safer, and more reliable.

For more information on Birthday Week 11, visit www.cloudflare.com/birthday-week.

Solving Email Challenges
In response to customer requests, we are taking on email security. With the Email Security DNS Wizard, we guide website owners through the process of creating the required DNS records to ensure their domain is safe — preventing spoofing and phishing.

A One-Inbox Approach to Email
Cloudflare Email Routing simplifies the process of creating and managing email addresses without the necessity of checking multiple inboxes. It takes a privacy-first approach — we do not look into, queue, or store emails at any point.
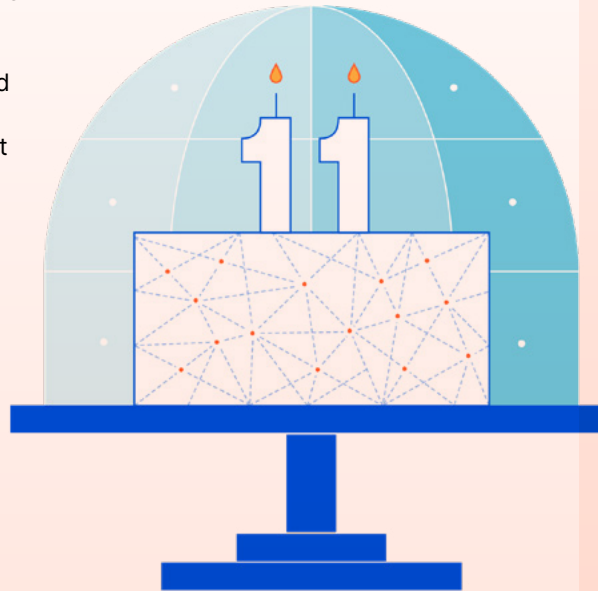
Highlights From Past Birthday Weeks

2020
— **Free, Privacy-First Analytics**
Cloudflare Radar

2019
— **WARP Available to All**

2018
— **The Bandwidth Alliance**

2017
— **Unmetered DDoS Protection**

2016
— **Dedicated SSL Certificates**

2015
— **Expansion to China**

2014
— **Universal SSL**

2011
— **Free Automatic IPv6**

A better Internet is principled.

Being principled means thinking long term and doing the right thing even if it is not in our short-term interest.

It means proving our commitment to individual privacy not only by minimizing our collection and use of personal data but also by updating and securing the Internet's legacy protocols to protect personal data.

It means demonstrating our respect for international human rights and promoting the work of human rights defenders.

It means being transparent about how we approach and address challenges, and holding ourselves accountable for our mistakes.

More Private, More Secure

Cloudflare is helping to build privacy and security into the Internet. We believe we should empower entities and individuals by providing tools that reduce the amount of personal data available.

Fixing Protocols That Leak Data
Internet protocols that connect users with information online also expose personal information, like IP addresses, location, and device information. A variety of actors can use this information to observe and track users without their consent.

Cloudflare is working with partners to address these leaks and secure the web. For example, through Oblivious DNS over HTTPS (ODoH), we are helping make the source of DNS queries invisible to DNS resolvers. We also recently announced work on Encrypted Client Hello (ECH), a standard that will ensure all TLS handshakes are fully encrypted.

Password Protection
OPAQUE is a new cryptographic technique that keeps passwords hidden even from servers. Utilizing a construction called an Oblivious Pseudorandom Function (as seen in Privacy Pass), a server does not learn passwords — it learns only whether the user knows the password.

Privacy-First Web Analytics
Cloudflare has created website analytics tools that allow website owners to understand traffic to their sites without sacrificing privacy. Rather than using IP addresses, user agents, or other digital fingerprinting to track customer behavior across the web, Cloudflare Web Analytics enables tracking anonymous page views and website visits. These tools are free and available for anyone to use.

1.1.1.1 Privacy-First DNS
Cloudflare believes that customers should have a fast, private way to browse the Internet. Our free public DNS resolver is one of the fastest public DNS resolvers on Earth, employs privacy- and security-enhancing protocols, and unlike most resolvers, does not mine customer data or sell data to advertisers. WARP is an optional app built on top of 1.1.1.1 that creates a secure connection between personal devices and Internet services. To help those looking to protect themselves from cyber attack and parents seeking parental controls for their children, we launched 1.1.1.1 for Families, a filtered DNS resolver that restricts access to malware and/or adult content.

Privacy @ Cloudflare

Privacy is at the heart of everything we do. We will never sell, lease, rent, or give away personal information without consent.

Policies

Our overriding privacy principle is that any personal information customers provide to us is just that: private. Our Privacy by Design policy sets out the high standards and evaluations that must be undertaken if products and services are to collect and process personal data, and we are transparent about how we collect and use data. To read our full Privacy Policy, visit www.cloudflare.com/privacy.

Independent Verification

We use best-in-class standards and certifications to help demonstrate our commitment to privacy. Earlier this year, Cloudflare became one of the first organizations in our industry to achieve the new ISO/IEC 27701:2019 privacy certification, and the first web performance and security company to be certified to the new ISO privacy standard as both a data processor and controller. Our newest certification builds on our previous privacy certifications and audits, including:

ISO 27701:2013

PCI DSS 3.2.1

Information Security Management System (ISMS)

1.1.1.1 Public DNS Resolver Privacy Examination

SOC 2 Type II

BSI Qualification

For information on compliance resources, visit www.cloudflare.com/trust-hub.

Personal Data Control

Countries around the world are enacting new regulations to give individuals greater control over their personal data.

The Cloudflare network and all of our products are built with data protection in mind. We do not use personal data for any purpose other than to provide our services to our customers.

We give customers the ability to access, correct, and delete their personal information — in all countries, not just where it is legally required. Further, we give our customers control over the information that passes through our network.

For more information on Cloudflare's GDPR compliance, visit www.cloudflare.com/gdpr/introduction.

Human Rights @ Cloudflare

Cloudflare respects human rights under the UN Guiding Principles on Business and Human Rights. We are also helping protect and advance freedom of expression and privacy online as part of the Global Network Initiative.

Commitment and Policy
Cloudflare published our first comprehensive international human rights policy in 2021. Our new policy describes our commitment to international human rights and how we implement those commitments in our operations, products, and policies.

Beginning in 2022, all Cloudflare employees will receive annual training on our human rights policy and as part of new hire onboarding.

Global Network Initiative (GNI)
GNI is a multistakeholder initiative composed of information and communications technology companies, human rights and press freedom organizations, academics, and investors. Its goal is to protect and advance freedom of expression and privacy rights by setting a global standard for responsible company decision-making as well as advocating against government restrictions and demands.

Cloudflare joined GNI as an observer member in 2020, and was approved to serve as a full term member in 2021.

United Nations B-Tech Community of Practice
The B-Tech Project is a multi stakeholder initiative that provides authoritative guidance and resources for implementing the UN Guiding Principles on Business and Human Rights in the technology space. Cloudflare is one of twelve companies that participates in the B-Tech company Community of Practice, which regularly meets to discuss best practices on applying concepts like human rights due diligence to emerging technology issues.

In December 2021, Cloudflare CEO Matthew Prince participated in the UN B-Tech Leadership Dialogue with the UN High Commissioner for Human Rights to discuss the role of business leaders in advancing corporate respect for human rights.

Project Galileo

Cloudflare provides free security services to artistic groups, journalists, humanitarian organizations, and social activists to ensure these vulnerable groups are not taken offline through denial-of-service and other cyber attacks.

For more information on Project Galileo, visit www.cloudflare.com/galileo.

1,600
civil society organizations in 111 countries.

53M
cyber threats per day on average.

$3M+
in services donated in 2021.

Galileo Partners

Electronic Frontier Foundation
Free Press
Fourth Estate
Sontusdatos.org
AccessNow
Front Line Defenders
Mozilla
Open Technology Fund
Committee to Protect Journalists
Amnesty International
ACLU
Anti-Defamation League
Centre for Policy Alternatives
Meedan
SMEX
Lion Publishers
Xlab.org
NDI
Tech Against Terrorism
Business & Human Rights Resource Centre
World Wide Web Foundation
Council of Europe
IRI
The Carter Center
Freedom House
Open Briefing
National Endowment for Democracy
Center for International Media Assistance
Defend Defenders
Alliance of Democracies
National Coalition Against Censorship
Civil Rights Defenders
Engine
Reporters Sans Frontieres
New America
Center for Democracy & Technology
Institute for War & Peace Reporting
Derechos Digitales

Project Galileo 7th Anniversary

Earlier this year, we celebrated the 7th anniversary of Project Galileo. To mark the occasion, our Cloudflare Radar team launched the Galileo Dashboard, which helps visualize some of the cyber security trends we see affecting civil society organizations around the world. For example, from August 2020 to March 2021, Galileo participants experienced over 13 billion cyber threats — more than 53 million threats per day on average. The most common attacks used by hackers included exploiting SQL injection vulnerabilities, user agent anomaly, and fake search engine bots.

For more information, see https://radar.cloudflare.com/notebooks/project-galileo-7th-anniv.

Top 12 attack types

Attack Type	Percentage
External Entity Attack (XXE)	0.2%
Method Anomalies	1.4%
Information Disclosure	1.8%
Code Injection	1.9%
Attacks on WordPress Sites	2.8%
Other	5.7%
Other Header Anomalies	6.2%
File Inclusion	6.3%
Cross Site Scripting (XSS)	6.9%
Faking Search Engine Bots	18.9%
User-Agent Anomaly	23.1%
SQL Injection	24.7%
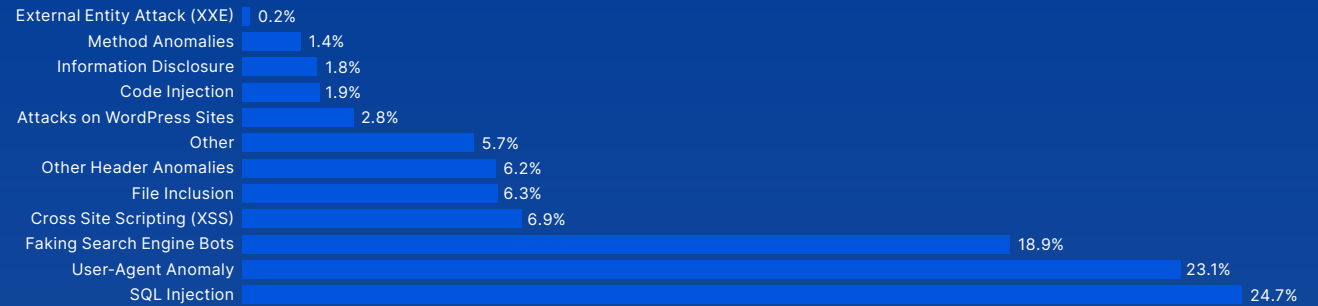
Protecting more than 1,600 organizations in 111 countries

North America 44%

South America 5%

Europe 28%

Africa 4%

Middle East 3%

Asia 12%

Oceania 4%
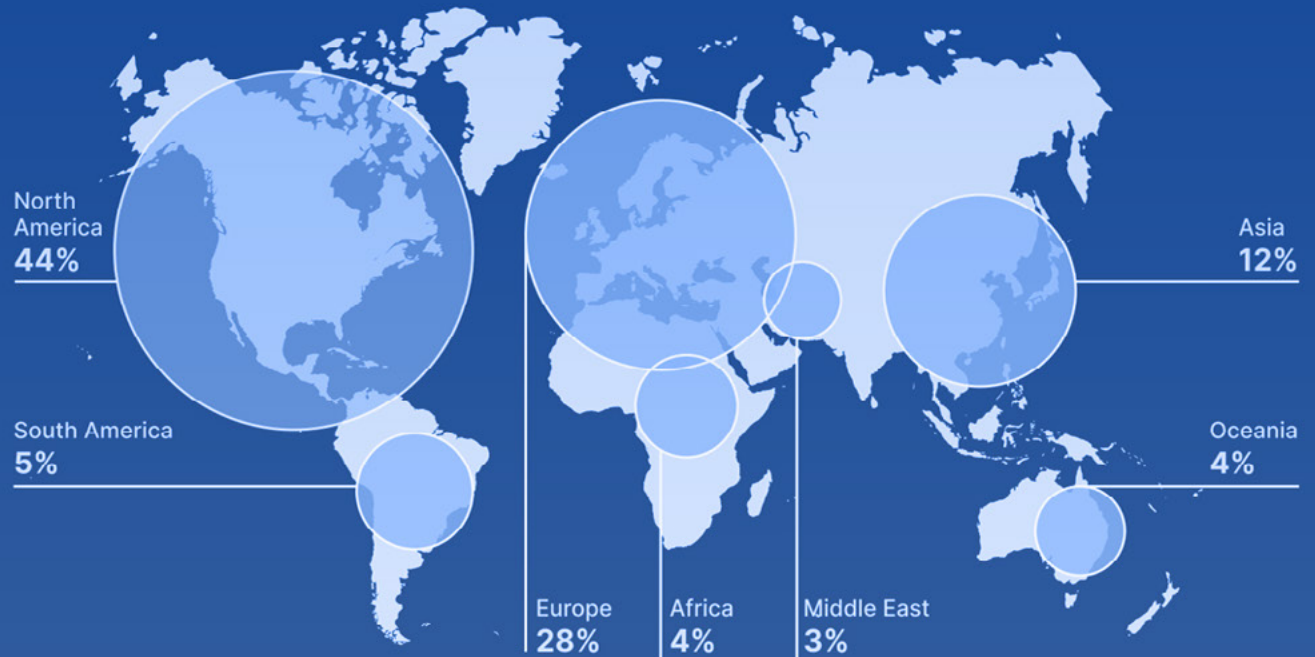
Protecting Elections and Campaigns

Cloudflare provides free services to state and local governments to make sure voters have access to election information. Working with a nonprofit partner, we provide free services to political campaigns, so that all candidates have access to the same tools to effectively campaign online.

Athenian Project

Started in 2017, the Athenian Project provides free enterprise-level Cloudflare services to state and local governments in the United States to help protect their election websites.

Earlier this year, we announced that the Athenian Project is now available to help governments outside of the United States. In partnership with the International Foundation for Electoral Systems (IFES), National Democratic Institute (NDI), and International Republican Institute (IRI), we have identified locations Cloudflare can donate free services to regional, state, and municipal governments consistent with local laws.

Cloudflare for Campaigns

In partnership with Defending Digital Campaigns, Cloudflare provides state and federal political candidates in the US with access to free security and performance tools. Cloudflare also provides a free website security guide to help campaigns protect against common security threats.

$5M+

in services donated in 2021.

292+

state and local government websites in 30 US states have received free Cloudflare services through the Athenian Project.

"The idea of our election websites being inaccessible due to a distributed denial of service (DDoS) attack was a concern for us, especially in the election space where trust and access to authoritative voting information is crucial. There is only so much you can plan and test in terms of preparedness on the security side and after implementing Cloudflare and many other security precautions, we felt confident we had a security platform in place where we could adjust and respond to threats and high demand in real-time."

— **Stacy Mahaney, Chief Information Officer, Missouri Secretary of State, Oregon, United States**

"It's easy for the public to see a lock and know that they have extra protection. It's really important that people understand that we have that lock on our door. And Cloudflare is that lock."

— **Roxanna Moritz, Auditor and Commissioner of Elections, Scott County, Iowa, United States**

Impact Spotlight: Internet Shutdown Alerts

In June, Cloudflare launched a service to support human rights organizations that monitor Internet shutdowns. Using Cloudflare Radar, our free platform that tracks traffic and insights across our network, Cloudflare provides real-time alerts to partner organizations regarding suspicious drops in Internet traffic.

These alerts deliver data to organizations like Access Now, the Carter Center, and Internews that are working to quickly and reliably identify and diagnose Internet shutdowns, particularly those associated with important social or political events.

For more information on Cloudflare Radar Alerts, please visit radar.cloudflare.com.

Radar partners

Change in Internet traffic in Burkina Faso (last 7 days)
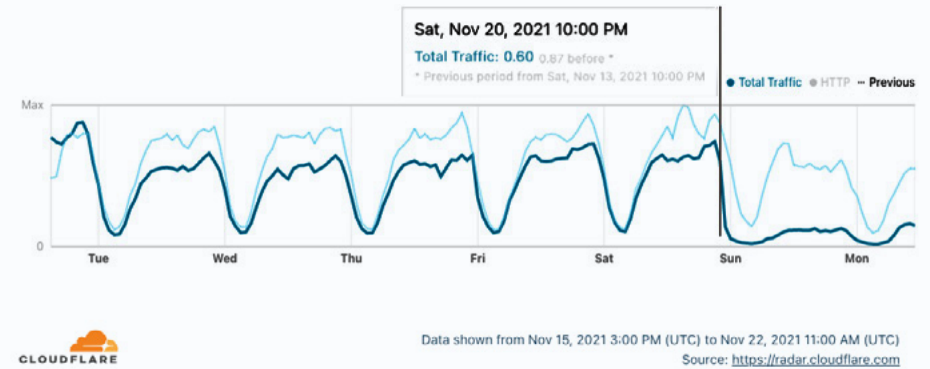
"In the fight to end Internet shutdowns, our community needs accurate reports on Internet disruptions at a global scale. When leading companies like Cloudflare share their data and insights, we can make more timely interventions. Together with civil society, Cloudflare will help #KeepItOn."

— Peter Micek, General Counsel, Access Now

Transparency @ Cloudflare

Transparency is one of our core values.
We strive to communicate clearly and openly how we manage our network, the challenges we see, and the actions we take.

Abuse
We are transparent and principled in how we address reports of abuse on our network. Our approach to addressing abuse is based on three guiding principles:

Service specific:
We believe responses to abuse should reflect the nature of the services at issue and the ability to address the harm, while minimizing the possibility of unintended consequences.

Access to process:
We believe complainants should have a mechanism to present their grievances to the party best positioned to address them.

Transparency:
We believe in being transparent about when and how we take actions to address abuse.

To learn more, please visit
www.cloudflare.com/trust-hub/abuse-approach.

Requests for Customer Information
Our approach to law enforcement, government, or other lawful requests for customer information is based on three principles:

Due process:
Any law enforcement requests that we receive must strictly adhere to the due process of law and be subject to judicial oversight.

Privacy:
Our respect for our customers' privacy applies with equal force to government or law enforcement requests.

Notice:
Our policy is to notify customers of a subpoena or other legal process requesting their information prior to disclosure.

To read our most recent Transparency Report, please visit
www.cloudflare.com/transparency.

Transparency Spotlight: Warrant Canaries

Cloudflare maintains a public list of things we have never done on behalf of any government, law enforcement, or authority. We started the list in 2013, expanded and modified it in 2019, and are pleased to report no changes in 2021.

Why Do We Have Warrant Canaries?
Keeping a public list of actions we have never taken does a few things. It helps our customers understand how we have acted in the past, and how we intend to act in the future. It is a useful way to keep customers informed about potential law enforcement or other legal orders that prevent us from disclosing them publicly (sometimes called "gag orders"). For example, if we received a secret order that required us to act in conflict with one of our commitments, although we could not disclose the order itself, we could still remove the commitment from our list.

Finally, we hope that keeping this list clearly demonstrates to those that may ask us to do something contrary to our values that we take these issues seriously, and doing so would not be easy.

Some things we have never done

1
Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone.

2
Cloudflare has never installed any law enforcement software or equipment anywhere on our network.

3
Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network.

4
Cloudflare has never modified customer content at the request of law enforcement or another third party.

5
Cloudflare has never modified the intended destination of DNS responses at the request of law enforcement or another third party.

6
Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party.

Operating With Integrity:
Ethics and Compliance

At Cloudflare, we are committed to operating with the highest level of ethics and integrity in everything we do, including conducting business in full compliance with all applicable laws and regulations.

Anti-Corruption

Corruption undermines legitimate business and governance. 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 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.

WE SUPPORT

UN GLOBAL COMPACT

Ethical Conduct

Our commitment to business ethics and responsibilities is described in our Code of Business Conduct and Ethics, which 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

Fair competition

Fair Labor and Modern Slavery

Cloudflare is 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, the use of involuntary labor, and child labor. These policies are reflected in our Modern Slavery Act Statement for Fiscal Year 2020.

Compliance

Cloudflare's commitment to compliance includes programs that prohibit us from doing business with sanctioned parties, those that restrict the export of certain technology, and those that govern the reporting and restriction of child sexual abuse material (CSAM). Our robust compliance program includes safeguards designed to prevent sanctioned parties from signing up for service and ensure that all Cloudflare products are properly classified and authorized for export. We actively screen our customers, resellers, vendors, and partners to identify links to sanctioned or restricted parties and countries. Our contracts include commitments from our customers, resellers, vendors, and partners that they will comply with all US export controls 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.

Helping build an Internet for everyone means making products and services that were previously available only to large companies easy and affordable for everyone.

It means promoting online access by helping more communities safely and securely connect to the global Internet.

It also means investing in diversity, equity, and inclusivity to develop more innovative teams and products.

Democratizing Access to New Technologies

Cloudflare believes that everyone — not only the largest businesses — should have access to new technologies and tools to make the Internet faster, more reliable, and more secure.

Democratizing access to cyber security tools and making complicated and technical solutions accessible opens doors for the next generation's inventors and improves the security of the Internet ecosystem and the experience for everyone online.

Free Cyber Security Services
Cloudflare makes security and optimization services accessible, for free, to organizations that would otherwise not have access to them, from online blogs, to small businesses, to non-governmental organizations. Cloudflare's free plan includes unmetered distributed denial-of-service attack (DDoS) mitigation, a content delivery network (CDN), and universal SSL encryption, helping protect millions of web properties from being taken offline by cyber attack.

Zero Trust Services
Because we believe even the smallest organizations should have access to tools to secure their employees and apps, we launched a free version of Zero Trust browsing and application access. These services can help even organizations without significant resources protect themselves from data loss, malware, and phishing.

Supporting Tomorrow's Innovators
At Cloudflare, we believe innovators can come from anywhere. To help developers looking to build new applications without configuring or maintaining infrastructure, we have provided free access to our Workers platform. This year, Cloudflare added free access to Cron Triggers, which allows developers to schedule workloads and manage development workflow.

520,205+

unique DDoS attacks against Cloudflare free customers were detected and mitigated by our network in 2021, including 160 billion attack requests.

200K+

accounts using the Workers free plan in 2021.

22M+

SSL certificates provided for free in 2021.

Impact Spotlight:
Helping More Communities
Access the Internet

Half of the world's population has no access to the Internet. Even in communities that are able to invest in WiFi antennas or fiber cables, connection to the global Internet remains prohibitively expensive.

Project Pangea

In July 2021, Cloudflare launched Project Pangea to provide free connection services to the Internet for rural, nonprofit, and local community networks, particularly in underserved areas.

Cloudflare can help communities solve the network challenges of routing traffic to and from the Internet on behalf of the local or community network, while also providing state-of-the-art security, privacy, and performance.

Participants gain access to our suite of network services — Cloudflare Network Interconnect, Magic Transit, and Magic Firewall — which will collectively reduce the cost for communities to connect to the Internet, with industry-leading security and performance functions built-in.

To learn more, visit www.cloudflare.com/pangea.
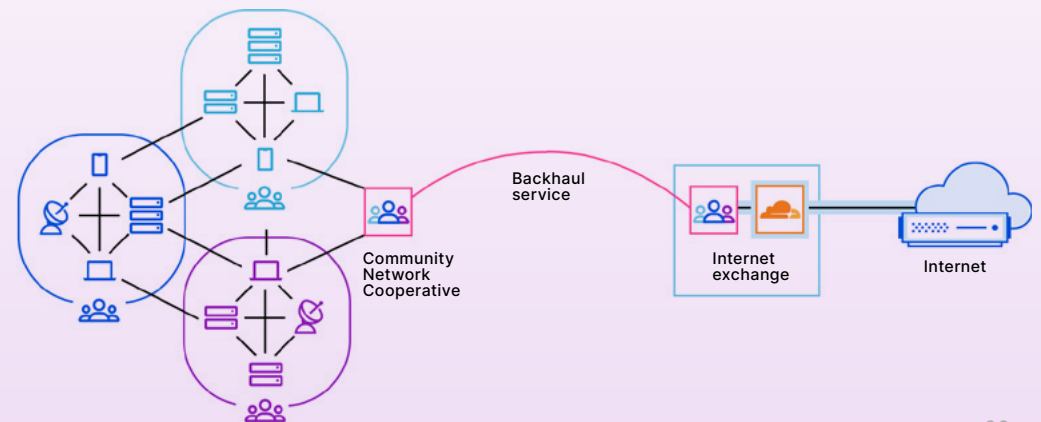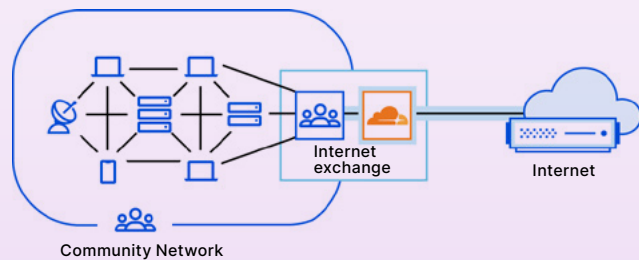
"My research on Internet performance in developing regions makes me believe that community networks — and their end users — will benefit tremendously from Project Pangea. It is so exciting to be part of such an amazing journey."

— Roderick Fanou, Systems Engineer, Cloudflare, Austin, Texas

Community Network

Internet exchange

Internet

Community Network Cooperative

Backhaul service

Internet exchange

Internet

We Invest in Diversity, Equity, and Inclusivity (DEI)

At Cloudflare, we believe that diverse teams make better decisions, are more innovative, and produce better results. DEI is part of our mission, and imperative to our business.

To learn more about DEI at Cloudflare, visit www.cloudflare.com/diversity-equity-and-inclusion.

Recruiting
An important component of our DEI strategy is to grow a diverse talent pool. We have recruiting partnership programs with organizations to reach underrepresented groups, including the AnitaB.org Grace Hopper Celebration, National Sales Network, and PowerToFly. We also support returnships that allow caregivers to return to the workforce through our partnerships with Mums@Work and Path Forward.

Building Skills
We define an inclusive culture as one where everyone feels safe, welcome, and respected with a sense of belonging. We do not leave this to chance. We invest in training and programs to develop and deepen the skills needed to nurture and preserve inclusive communities at Cloudflare, including through partnerships with tEQuitable (a resource for mitigating bias, discrimination, and harassment) and Paradigm (a platform for advancing and benchmarking DEI programs).

Accountability
We hold ourselves accountable by analyzing data, setting goals, and measuring progress objectively. We set annual companywide goals around our diversity, and for the last few years we have added individual goals for managers — one focused on building a more diverse team, and one focused on building an inclusive team culture. We also place a high value on behaviors. We believe that culture is defined by the behaviors we reward. Our Cloudflare Capabilities are the behaviors we have deemed essential for a healthy and inclusive culture.

📖	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

Equity
Working toward reducing and ultimately eliminating the gender pay gap is just part of our mission. To hold ourselves accountable, Cloudflare has signed several equity charters, including the EU Charter, UK Tech Talent Charter, and German Diversity Charter.

Inclusivity
Without inclusive teams and a collaborative culture, the positive impacts of diversity will not be attained. We have fostered an inclusive culture through the development of employee-led communities, educational offerings, incorporating behaviors into performance, and reviews of our processes and policies for fairness and inclusion. We are proud to be one of Human Rights Campaign's 2021 Best Places to Work for LGBTQ Equality.

HUMAN RIGHTS CAMPAIGN FOUNDATION — BEST PLACES TO WORK — 2021 — for LGBTQ Equality — 100% CORPORATE EQUALITY INDEX

Communities @ Cloudflare

Employee resource groups (ERGs) are important to our success. They foster community and a sense of belonging, help drive organizational change, and improve the overall quality of an organization's culture. Most essentially, they help organizations become more diverse, equitable, and inclusive.

Afroflare

Asianflare

Cloudflarents

Desiflare

Flarability

Greencloud

Judeoflare

Latinflare

Mindflare

Nativeflare

Proudflare

Soberflare

Vetflare

Womenflare

Diversity @ Cloudflare

We are working hard to understand the makeup of our teams and increase our diversity. We are proud to publish our 2021 employee diversity data and share our progress.

To review our diversity data, visit www.cloudflare.com/diversity-equity-and-inclusion.

Overall Gender Identity

- Masculine / Male: 68.04%
- Feminine / Female: 31.61%
- Agender, Bigender, Non-Binary, Queer, and Other: 0.35%

US Overall Race/Ethnicity
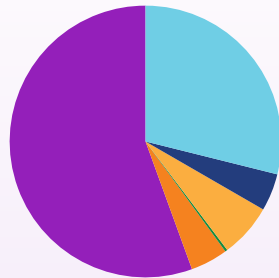
- White: 55.45%
- Asian: 28.74%
- Hispanic or Latino: 6.52%
- Black or African American: 4.49%
- Two or More Races: 4.49%
- American Indian or Alaska Native: 0.21%

Leadership Gender Identity

- Masculine / Male: 75.60%
- Feminine / Female: 24.40%

Project Galileo Spotlight:

Switchboard joined Project Galileo in 2019 to gain visibility into HTTP traffic, including threats targeting their site. They are a telephone helpline in the United Kingdom that provides support and information to people of all kinds, but especially those who identify as LGBT+.

As of 2021, the organization averages 1,500 unique service users a month, connecting with volunteers who are available seven days a week.

"We have people that call in to talk about things such as seeking help in navigating their gender identity, looking for resources on mental health in the UK, or to discuss issues in their community when it comes to LGBT+ rights," explains Switchboard's Pete Hannam.

"We had no visibility into our traffic or threats before Cloudflare," says Pete. After the site was hacked because of a vulnerability in a WordPress plug-in, the team did not realize they had been compromised. "As an organization that provides a platform for those sharing sensitive information... trust is essential for us and presenting an insecure platform is a huge breach of respect and professionalism."

To learn more about Project Galileo, visit www.cloudflare.com/galileo.

"We have the exact same issues as large companies, possibly even more targeted due to the sensitivity of our work, with significantly fewer resources. So it is important for organizations such as ours to have the opportunity to use advanced security tools, and Cloudflare's Project Galileo allows us access to these tools to keep our site reliable, secure, and trustworthy."

— Pete Hannam, Switchboard UK

A better Internet is sustainable.

Helping build a sustainable Internet means systems, networks, and protocols that are more energy efficient.

It means reducing carbon emissions by transitioning to renewable energy and removing existing carbon from the atmosphere.

It also means helping others understand and reduce their own emissions footprint.

Making the Internet More Efficient

The fastest way to reduce greenhouse gas emissions (GHG) is to use less energy. Cloudflare is helping build an Internet that is more efficient at every level: design, hardware, systems, and protocols.

Shifting the Network to the Cloud
Cloudflare is helping its customers migrate from a patchwork of legacy on-premise network security, performance, and reliability solutions to more efficient cloud-based services.

Efficiency at the Edge
Cloudflare customers are able to serve web content (images, videos, or webpages) directly from our distributed network, located in 250 cities in 100 countries, rather than wherever that content is actually hosted. Serving content locally reduces transit, and alleviates congestion on finite resources like undersea cables.

Additionally, because the Cloudflare edge network is designed to process large volumes of traffic, including distributed denial-of-service (DDoS) attacks, our customers do not need to maintain their own excess server capacity to handle unexpected traffic spikes.

Next-Generation Hardware
In July, Cloudflare deployed our first edge servers featuring ARM-based CPUs. This new generation of servers processes 57% more Internet requests per watt of energy. Overall, the Cloudflare network is now securely processing 10x as many Internet requests for every watt consumed as we did in 2013.

Cloudflare Network Performance (Internet Requests) Per Watt, Indexed
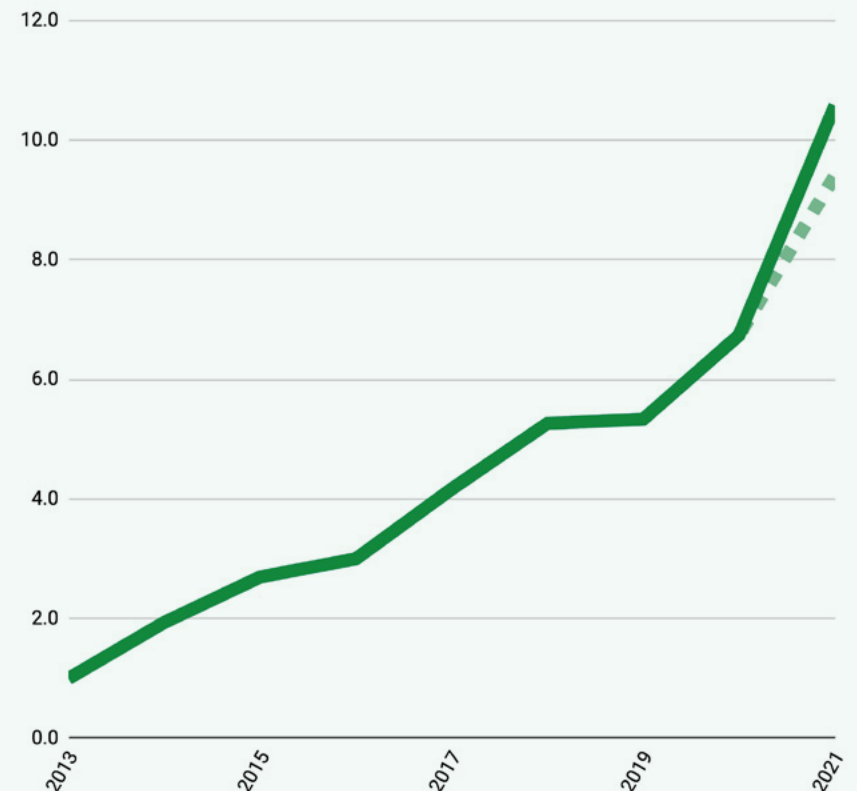
Solid green line represents the performance of ARM-based CPUs over other Cloudflare servers.

Tackling Wasted Web Crawler Traffic
In order to return fast and accurate results, search engines use web crawlers — automated bots that constantly scour the Internet looking for website updates. Unfortunately, crawlers often visit the same sites over and over, even when no changes have been made. Based on analysis of traffic on our network, we estimate as much as 53% of web crawler traffic is wasted.

Working with Microsoft and Yandex, Cloudflare recently announced a new protocol to help improve the efficiency of search engines. Under this system, our network proactively notifies search engines when a website has changed, rather than requiring search engines to constantly check for updates.

Carbon Impact Reports
Cloudflare provides all customers with customized and free GHG emissions data based on their use of our network. Our Carbon Impact Reports highlight recommendations on adjusting settings to further improve efficiency.
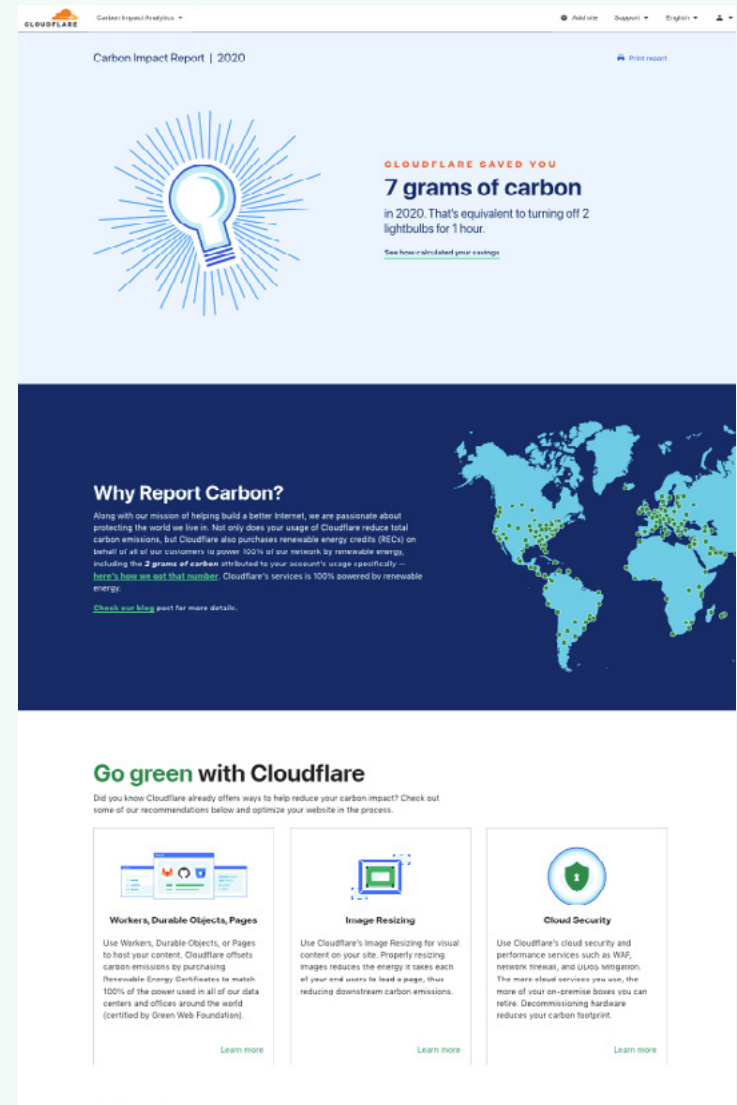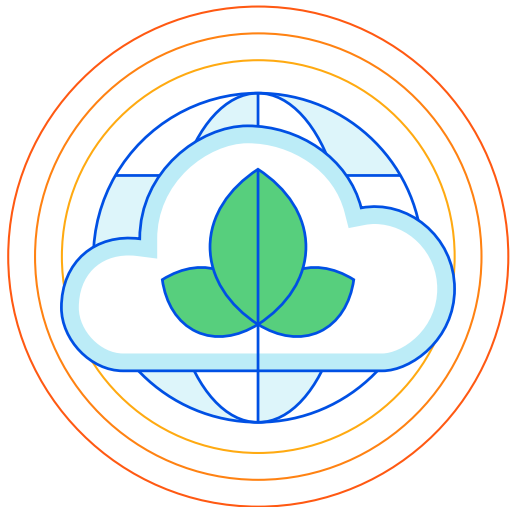
Transition to Zero Emissions

Cloudflare is helping build a sustainable Internet that is powered by renewable energy and engineered to drive better climate outcomes.

100% Renewable Energy

Earlier this year, we announced our commitment to using 100% renewable energy for our operations indefinitely. In practice, that means we purchase the same amount of energy from renewable sources as we actually consume from electrical grids.

This builds on work we started in 2018, when we made our first renewable energy purchase to account for all of our US operations that year. In 2019 and 2020, we expanded our purchases to cover 100% of the energy used in all of our global operations.

For more information on our renewable energy purchases, see our 2020 Emissions Inventory report.
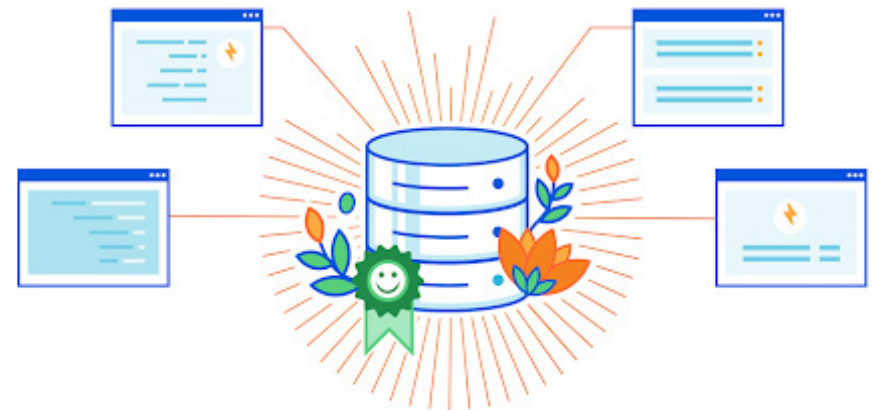
Zero Historic Carbon Emissions

Taking our sustainability efforts one step further, we are also committed to removing or offsetting all historic GHG emissions resulting from powering our network by 2025. As we move toward an Internet powered by renewables, we think it is important to be accountable for all emissions resulting from operating our network.

Product Spotlight: Green Compute With Cloudflare Workers

Cloudflare Workers allows customers to schedule computing tasks to run exclusively at our data centers that are located in third-party-owned facilities — also powered by 100% renewable energy.

To sign up for Green Compute, visit
www.cloudflare.com/green-compute-cloudflare-workers.

Doubling Our Support for Renewable Energy
All Cloudflare machines are powered by 100% renewable energy. However, our renewable energy purchases only cover energy used by our machines.

Many of our data centers are located in facilities owned by third parties. Because of emissions accounting rules, we typically do not include other energy used by those facilities in our renewable energy or emissions calculations, including heating, cooling, lights, and other equipment.

Using our Cron Triggered Workers platform, Cloudflare customers can schedule computing tasks to run at these green facilities automatically — with no code changes!
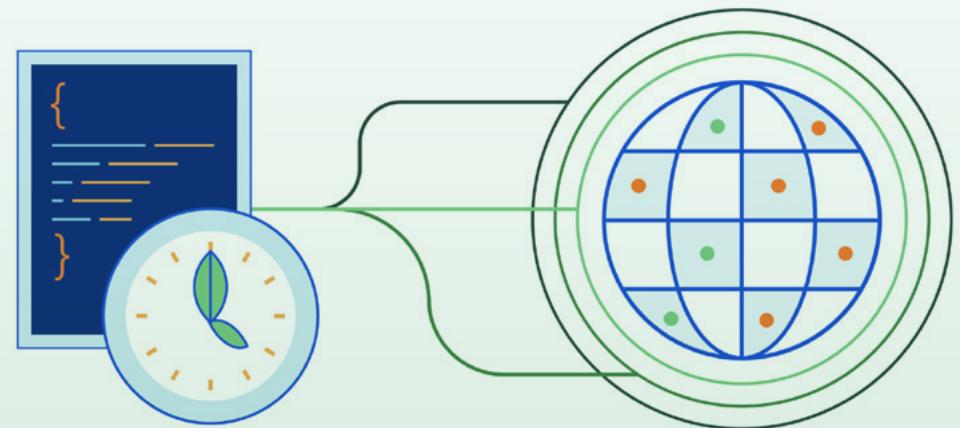
Emissions @ Cloudflare[1]

Emissions Category		Metric Tons (MT) Carbon Dioxide Equivalent (CO2e)	Percent of Calculated Total
Scope 1		0	0%
Scope 2 (Location-based)		13,955.15	100%
	Facilities	754.27	5.4%
	Network	13,200.88	94.6%
Scope 2 (Market-based)		0	100%
Total (Market-based)		0	100%

Greenhouse Gas (GHG) Emissions

In July, we released our first Emissions Inventory. Based on the GHG Protocol, we separated our calculations into two categories of emissions: Scope 1 and Scope 2.

Cloudflare also recorded two values within our Scope 2 emissions: location-based and market-based.

Scope 1 emissions capture activities that emit GHGs directly into the atmosphere, like coal-fired power stations, furnaces, and gas-powered vehicles.

Scope 2 emissions are indirect, capturing emissions resulting from energy purchased through the electrical grid.

Location-based is a calculation of the amount of energy used multiplied by the emissions factor of the electrical grid where the energy was consumed.

Market-based emissions incorporates the environmental benefits of voluntary purchases like renewable energy, carbon offsets, and carbon removals.

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

Product Spotlight:
Bot Fight Mode

For every bad bot we stop online, we donate to support tree planting projects.

Malicious bots are a common problem on the Internet. They carry out harmful attacks, slow down applications, and waste computing resources.

In 2019, Cloudflare launched Bot Fight Mode to detect bad bots and stop them in their tracks. The tool is completely free and is already used by over 370,000 sites.

Bot Fight Mode uses a technique known as "tarpitting" to exhaust bots, redirecting them to meaningless challenges so they cannot spend their time attacking sites. **To date, bots have spent more than 3,000 years on these challenges.**

Unfortunately, tarpitting also consumes resources and likely generates emissions. To help address this impact, Cloudflare supports tree planting projects through One Tree Planted based on the number of bad bots we defeat.

In 2021, we donated 50,000 trees that were divided among three projects:

Fruit tree planting in Haryana and Rajasthan, India

Forest fire recovery in British Columbia, Canada

Municipal dump conversion through reforestation in Nova Scotia, Canada

Bot Fight Mode continues to issue **millions of challenges** each day.

Appendix

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Organization profile	102-1	Name of the organization	Cloudflare, Inc.			
	102-2	Activities, brands, products, and services	10-K Filing			
	102-3	Location of headquarters	101 Townsend Street, San Francisco, CA			
	102-4	Location of operations	Cloudflare Office Locations			
	102-5	Ownership and legal form	10-K Filing			
	102-6	Markets served	10-Q Filing 10-K Filing			
	102-7	Scale of the organization	10-Q Filing 10-K Filing			
	102-8	Information on employees and other workers	Cloudflare.com/diversity-equity-and-inclusion Cloudflare does not have a significant portion of activities performed by workers who are not employees.			
	102-9	Supply chain	10-K Filing			
	102-10	Significant changes to the organization and its supply chain		Entire disclosure	Not applicable	
	102-11	Precautionary principle or approach	See Making the Internet More Efficient, page 26. See Transition to Zero Emissions, page 28. See Emissions @ Cloudflare, page 30.			
	102-12	External initiatives	Cloudflare is a signatory of the UN Global Compact, and a member of the Global Networking Initiative. Cloudflare also participates in the Pledge 1% Initiative.			
	102-13	Membership of associations	Cloudflare participates in the following trade associations: BSA, i2c, CCIA, BSA, TechUK, Eco, Asia Internet Association, and Bitkom. Cloudflare also regularly participates and engages with additional organizations focused on cyber security, Internet governance, and Internet safety, including: Technology Coalition, Cybersecurity Tech Accord, Internet Watch Foundation, and Global Cyber Alliance.			

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Strategy	102-14	Statement from senior decision-maker	See statement from Cloudflare founders, page 2.			
	102-15	Key impacts, risks, and opportunities	10-Q Filing 10-K Filing See statement from Cloudflare founders, page 2. See More Private, More Secure, page 8. See Human Rights @ Cloudflare, page 10. See We Invest in Diversity, Equity, and Inclusivity, page 21. 2021 Cloudflare Communication on Progress			
Ethics and integrity	102-16	Values, principles, standards, and norms of behavior	Code of Business Conduct and Ethics			
	102-17	Mechanisms for advice and concerns about ethics	See Operating With Integrity, page 17. Code of Business Conduct and Ethics			
Governance	102-18	Governance structure	Proxy Statement Filing			
	102-19	Delegating authority	Reporting on environmental, social, and governance topics is generally conducted by the Legal, Policy, and Trust and Safety team and is overseen by the General Counsel.			
	102-20	Executive-level responsibility for economic, environmental, and social topics	Cloudflare's CEO has executive responsibility for implementation of environmental, social, and governance topics.			
	102-21	Consulting stakeholders on economic, environmental, and social topics	See 102-31. Proxy Statement Filing			
	102-22	Composition of the highest governance body and its committees	Proxy Statement Filing			
	102-23	Highest governance body's role in sustainable reporting	Proxy Statement Filing The Nominating and Governance Committee was briefed on sustainability issues in 2021.			
	102-24	Nominating and selecting the highest governance body	Proxy Statement Filing Nominating and Corporate Governance Committee Charter			
	102-25	Conflicts of interest	Corporate Governance Guidelines Audit Committee Charter Proxy Statement Filing Code of Business Conduct and Ethics			

| General Disclosures | Economic | Environmental | Social | SASB |

				Omission		
GRI Standard	**Reference**	**Disclosure**	**Answer**	Part Omitted	Reason for Omission	Explanation of Omission
Governance *(continued)*	102-26	Role of highest governance body in setting purpose, values, and strategy	Corporate Governance Guidelines Proxy Statement Filing			
	102-27	Collective knowledge of highest governance body	The Nominating and Governance Committee was briefed on sustainability issues in 2021.			
	102-28	Evaluating highest governance body's performance	Cloudflare's Board of Directors was not evaluated with respect to sustainability in 2021.			
	102-29	Identifying and managing economic, environmental, and social impacts	The Nominating and Governance Committee was briefed on sustainability issues in 2021.			
	102-30	Effectiveness of risk management processes	Proxy Statement Filing			
	102-31	Review of economic, environmental, and social topics	The Nominating and Governance Committee was briefed on sustainability issues in 2021.			
	102-32	Highest governance body's role in sustainable reporting	Cloudflare's Impact Report is reviewed by its General Counsel and CEO.			
	102-33	Communicating critical concerns	Proxy Statement Filing			
	102-34	Nature and total number of critical concerns	In 2021, there were no critical concerns as defined by 102-34 associated with this report that required reporting to the Board of Directors.			
	102-35	Remuneration policies	Proxy Statement Filing			
	102-36	Process for determining remuneration	Proxy Statement Filing			
	102-37	Stakeholders' involvement in remuneration	Proxy Statement Filing			
	102-38	Annual total compensation ratio		Entire disclosure	Insufficient data	
	102-39	Percentage increase in annual total compensation ratio		Entire disclosure	Insufficient data	

| General Disclosures | Economic | Environmental | Social | SASB |

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Governance *(continued)*	102-36	Process for determining remuneration	Proxy Statement Filing			
	102-37	Stakeholders' involvement in remuneration	Proxy Statement Filing			
	102-38	Annual total compensation ratio		Entire disclosure	Insufficient data	
	102-39	Percentage increase in annual total compensation ratio		Entire disclosure	Insufficient data	
Stakeholder engagement	102-40	List of stakeholder groups	Cloudflare stakeholders include its customers, users, employees, investors, partners, or any other groups that are materially affected by Cloudflare's business or the decisions it makes. As part of its mission to help build a better Internet, Cloudflare also includes the Internet and Internet community generally among its stakeholder groups.			
	102-41	Collective bargaining agreements	10-K Filing			
	102-42	Identifying and selecting stakeholders	See 102-13 and 102-40. See also Privacy @ Cloudflare, page 9. See Project Galileo, page 11. See Human Rights @ Cloudflare, page 10. See Impact Spotlight: Internet Shutdown Alerts, page 14.			
	102-43	Approach to stakeholder engagement	Examples of engagement with stakeholders can be found throughout Cloudflare's 2021 Sustainability Report. Internally, all employees have the opportunity to engage in open dialogue through internal communication platforms, as well as through Employee Resource Groups (ERG) and the Cloudflare Inclusion Council. Externally, Cloudflare's Legal, Policy, and Trust and Safety teams regularly engage in industry dialogue regarding Internet governance. Cloudflare also participates in a number of multistakeholder organizations as described in 102-13. Finally, Cloudflare regularly engages in multistakeholder consultation through programs like Project Galileo, which includes over 40 civil society partner organizations. See Project Galileo, page 11.			

| General Disclosures | Economic | Environmental | Social | SASB |

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Reporting practice	102-44	Key topics and concerns raised	Cloudflare gathers input on its key topics and concerns from stakeholders through a variety multistakeholder organizations including those described in 102-13 and 102-43. Human Rights Policy			
	102-45	Entities included in the consolidated financial statements	10-Q Filing 10-K Filing			
	102-46	Defining report content and topic Boundaries	The report covers all of Cloudflare's global operations. The reporting period is calendar year (CY) 2021, unless otherwise stated.			
	102-48	Restatements of information		Entire disclosure	Insufficient data	This report is Cloudflare's first GRI content index.
	102-49	Changes in reporting		Entire disclosure	Insufficient data	This report is Cloudflare's first GRI content index.
	102-50	Reporting period	CY2021			
	102-51	Date of most recent report		Entire disclosure	Insufficient data	This report is Cloudflare's first GRI content index.
	102-52	Reporting cycle	Annual			
	102-53	Contact point for questions regarding the report	Impact@cloudflare.com			
	102-54	Claims of reporting in accordance with the GRI standards	This report is intended to align with the GRI Standards: Core option.			
	102-55	GRI content index	Cloudflare 2021 GRI Content: Index (this document).			
	102-56	External assurance	Cloudflare's greenhouse gas emissions were externally verified. See GRI-305. No other section of this report was externally verified. See SBC Verification, page 55.			

| General Disclosures | **Economic** | Environmental | Social | SASB |

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Economic Performance	103-1	Explanation of material topic and its Boundary	Economic performance is material to Cloudflare's continued growth and long-term sustainability. 10-K Filing Cloudflare's management teams and CEO are responsible for economic performance as defined under 201-1.			
	103-2	The management approach and its components	10-Q Filing 10-K Filing			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines Audit Committee Charter			
	201-1	Direct economic value generated and distributed	10-Q Filing 10-K Filing			
Indirect Economic Impacts	203-2	Significant indirect economic impacts	A fundamental part of Cloudflare's mission is to make world-class security, performance, and reliability services easy to use and affordable for everyone. Cloudflare secures millions of websites through its free service plan. See Democratizing Access to New Technologies, page 19. Cloudflare also provides free access to its highest-level services for important civil society and humanitarian organizations as well as state and local governments and candidates for political office. See Project Galileo, page 11. See Protecting Elections and Campaigns, page 13.			
Anti-corruption	103-1	Explanation of material topic and its Boundary	Cloudflare is committed to conducting its business with integrity, as well as partnering with companies that share its same values against corruption. See Operating With Integrity: Ethics and Compliance, page 17. See Code of Business Conduct and Ethics.			
	103-2	The management approach and its components	Cloudflare manages corruption and bribery issues through its policies prohibiting such conduct, and through its annual training and certification. Compliance with Cloudflare's policy on anti-corruption as well as its training requirements are overseen by the Head of Legal Compliance and the General Counsel.			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines Audit Committee Charter			

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Anti-corruption *(continued)*	205-2	Communication and training about anti-corruption policies and procedures	All employees, including senior managers, complete training on bribery and corruption at onboarding, and as part of annual training and certification. Cloudflare conducts a thorough screening of each supplier, reseller, and partner at onboarding and with real-time monitoring to ensure the company is not partnering with companies that pose a high risk of corruption. Cloudflare will begin anti-bribery and anti-corruption training for its third parties for 2022.			
	205-3	Confirmed incidents of corruption and actions taken	Cloudflare is aware of no incidents of corruption as described in 205-3 among its employees. As a result, no employee was dismissed or disciplined for corruption. Cloudflare is aware of no incidents of corruption among its contracted business partners. As a result, no related contract was terminated or discontinued on that basis. Cloudflare is aware of no associated legal cases brought against Cloudflare or its employees.			
Anti-competitive behavior	103-1	Explanation of material topic and its Boundary	Cloudflare believes that competition laws and regulations throughout the world are designed to foster a competitive marketplace and prohibit activities that restrain trade. Cloudflare is dedicated to compliance with laws governing fair competition in all of its activities. Any activity that undermines this commitment is unacceptable. Code of Business Conduct and Ethics			
	103-2	The management approach and its components	Cloudflare's policy and training on anti-competitive behavior is led by its Head of Legal Compliance, and overseen by its General Counsel. The purpose of Cloudflare's policy on anti-competitive behavior is to ensure that all Cloudflare operations are conducted in accordance with relevant legal requirements and the highest ethical standards.			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines Audit Committee Charter			
	206-1	Legal actions for anti-competitive behavior, anti-trust, and monopoly practices	Cloudflare was involved in no legal actions regarding anti-competitive behavior, anti-trust, or monopoly practices.			

| General Disclosures | Economic | Environmental | Social | SASB |

GRI Standard	Reference	Disclosure	Answer	**Omission** Part Omitted	Reason for Omission	Explanation of Omission
Tax	103-1	Explanation of material topic and its Boundary	Cloudflare's global tax policy is to comply with the applicable tax laws, rules, regulations, and reporting requirements within the jurisdictions in which it operates, as supplemented with advice from external advisors. Cloudflare is committed to paying all taxes that are legally due and in line with the spirit of the tax legislation as enacted by the governing authorities within each jurisdiction in which it operates.			
	103-2	The management approach and its components	Cloudflare's tax policy is led by its Global Head of Tax and overseen by the Chief Financial Officer.			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines Audit Committee Charter			
	207-1	Approach to tax	Cloudflare's tax strategy and decisions are evaluated by internal tax professionals and are supplemented by the advice of outside advisors. The executive finance organization as a whole plays a role in all tax decisions and tax planning opportunities. Cloudflare's approach to compliance is conservative and disciplined. Its internal tax team monitors the activities of the business, ensuring that appropriate care is applied in relation to all processes that could materially affect its compliance with its tax obligations. Cloudflare is committed to accurately filing its tax returns and remitting tax payments on a timely basis. Furthermore, Cloudflare actively monitors changes in tax laws, regulations, rules, and reporting requirements as part of its routine procedures in financial and tax reporting.			
	207-3	Stakeholder engagement and management of concerns related to tax	Cloudflare's global tax function engages with tax authorities as part of its routine tax compliance process and where deemed necessary to appropriately apply the tax statutes and regulations to its facts and circumstances. Additionally, it engages with tax authorities in connection with requests for additional information and audits over open return years as necessary. Cloudflare does not engage in public policy advocacy on tax issues. Cloudflare's global tax function engages with internal and external stakeholders to facilitate strategic initiatives, growth, and development of its multinational enterprise.			

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Materials	301	Materials		Entire disclosure	Not material	As a cloud-based SaaS provider, materials as described in GRI 301-1, 301-2, and 301-3 are not a material issue as defined in GRI103-1 for Cloudflare. Cloudflare is not aware of any facilities in which Cloudflare operates that have had a regulatory or compliance issue.
Energy	103-1	Explanation of the material topic and its Boundaries	Cloudflare uses purchased electricity to operate its global network as well as its facilities. The Cloudflare Network includes data centers located in over 100 countries and 250 cities around the world. Cloudflare also leases space in 16 facilities globally. All energy data included in this section is based on CY2020. Emissions Inventory 2020			
	103-2	The management approach and its components	The Cloudflare Network is managed by the Head of Infrastructure. Cloudflare facilities are managed by the Head of Places.			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines 10-K Filing			
	302-1	Energy consumption within the organization	Cloudflare consumed no non-renewable energy as defined under GRI-302 in CY2020. Cloudflare consumed 41.3 gigawatt hours (GWh) total energy in CY2020. 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 2020. Emissions Inventory 2020			

General Disclosures	Economic	**Environmental**	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Energy *(continued)*	302-2	Energy consumption outside the organization	Cloudflare compiles energy data from each of its data centers. In locations where Cloudflare colocates data center equipment in a facility owned and controlled by a third party, Cloudflare does not record any energy used by that facility that is unrelated to Cloudflare-owned and -controlled equipment.			
	302-3	Energy intensity	Based on 2020 total revenue and energy data, Cloudflare consumed .000096 megawatt hours (Mwh) of energy for every dollar of revenue generated.			
	302-4	Reduction of energy consumption		Entire disclosure	Not applicable	CY2020 was the first reporting year for Cloudflare.
	302-5	Reduction in energy products and services		Entire disclosure	Not applicable	CY2020 was the first reporting year for Cloudflare.
Water	303	Water and effluents		Entire disclosure	Entire material	As a cloud-based SaaS provider, water and effluents as described in 303-1 through 303-5 are not a material issue as defined in GRI103-1 for Cloudflare. The UN CEO Global Water Mandate does not classify Cloudflare as either a medium- or high-risk enterprise for water usage. Cloudflare is not aware of any facilities that it operates that have had a regulatory or compliance issue. Cloudflare is working to better understand and reduce water usage at each of its facilities, though it does not anticipate that those efforts will result in a material disclosure.

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Emissions	103-1	Explanation of the material topic and its Boundaries	Greenhouse gas (GHG) emissions associated with Cloudflare operations are the result of energy consumed by powering its network and facilities. Cloudflare emissions data included in this section describes Cloudflare's calendar year 2020 activities.			
	103-2	The management approach and its components	GHG emissions are managed by the Infrastructure, Places, and Policy teams.			
	103-3	Evaluation of the management approach	Corporate Governance Guidelines 10-K Filing			
	305-1	Direct (Scope 1) GHG emissions	See Emissions @ Cloudflare, page 30. Cloudflare recorded 0 Scope 1 location-based emissions in 2020. Cloudflare used the operational control consolidation approach, under the GHG Protocol. Emissions Inventory			
	305-2	Energy indirect (Scope 2) GHG emissions	See Emissions @ Cloudflare, page 30. Cloudflare recorded the following Scope 2 emissions in 2020: Location-based emissions: 13,955 Metric Tons (MT) Carbon Dioxide Equivalent (CO2e) Market-based emissions: 0 MT CO2e Emissions Inventory			
	305-3	Other indirect (Scope 3) GHG emissions		Entire disclosure	Insufficient data	Cloudflare does not currently collect Scope 3 emissions data. Cloudflare defines energy consumed by all of the hardware and network scaffolding associated with its data centers as Scope 2 emissions.

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
Emissions *(continued)*	305-4	GHG emissions intensity	Based on its CY2020 location-based emissions, Cloudflare emitted .000032 MT (CO2e) per dollar of revenue generated. Cloudflare emitted 0 market-based emissions in CY2020.			
	305-5	Reduction of GHG emissions		Entire disclosure	Insufficient data	CY2020 was Cloudflare's first GHG emissions reporting year.
	305-6	Emissions of ozone-depleting substances (ODS)		Entire disclosure	Not applicable	Cloudflare is not aware of any ODS in its products, processes, or services.
	305-7	Nitrogen oxides (NOx), sulfur oxides (SOx), and other significant air emissions		Entire disclosure	Not applicable	Cloudflare is not aware of any of its activities that result in emission of nitrogen oxides, sulfur oxides, or other significant air emissions identified in 305-7.
Effluents and waste	306	Effluents and waste		Entire disclosure	Not material	As a cloud-based SaaS provider, waste as described in 306-1 is not a material issue for Cloudflare as defined in GRI103-1. Cloudflare is working with local providers to better understand waste and recycling impacts at each of its facilities, though it does not anticipate that data will result in a material disclosure.
Environmental compliance	307-1	Non-compliance with environmental laws and regulations	Cloudflare is not aware of any non-compliance with environmental laws or regulations.			
Supplier environmental assessment	308-1	New suppliers that were screened using environmental criteria	Cloudflare intends to screen suppliers using environmental criteria beginning in 2022.			

| General Disclosures | Economic | Environmental | **Social** | SASB |

| GRI Standard | Reference | Disclosure | Answer | Omission | | |
				Part Omitted	Reason for Omission	Explanation of Omission
GRI 401: Employment	103-1	Explanation of material topic and its Boundary	Cloudflare provides employees with a variety of voluntary programs to promote worker health. Cloudflare provides access to an Employee Assistance Program (EAP), which includes licensed professional counseling services, including work/life balance assistance. In addition, Cloudflare employees have access to an on-demand digital mental health and well-being platform. Cloudflare provides access to a fertility benefit that covers a variety of family planning services, including fertility treatment, adoption, and gestational carrier support — also referred to as surrogacy. During the COVID-19 pandemic, Cloudflare provided access to free online yoga and Pilates classes, as well as free digital membership to a fitness application through its health care provider.			
	103-2	The management approach and its components	Employment at Cloudflare is overseen by the Head of People and the COO.			
	103-2	Evaluation of the management approach	10-K Filing Compensation Committee Charter			
	401-1	New employee hires and employee turnover	In 2020, Cloudflare hired 907 employees and experienced a turnover rate of 11.5%.			
	401-3	Parental leave	Cloudflare's global parental leave policy allows a minimum of 10 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. Cloudflare also provides 6 paid weeks Pregnancy Health Leave (PHL) to recover from childbirth, unless more is required by local law. PHL leave and bonding leave can be taken consecutively for a total of 16 weeks paid leave.			

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
GRI 403: Occupational Health and Safety	403-1	Occupational health and safety management system	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. Cloudflare is in the process of developing a new comprehensive health and safety program, which will include employee training and site risk assessments as well as accident reporting, monitoring, and reviewing. The new program is expected to be in place in 2022. Code of Business Conduct and Ethics			
	403-6	Promotion of worker health	Cloudflare provides employees with a variety of voluntary programs to promote worker health. Cloudflare provides access to an Employee Assistance Program (EAP), which includes licensed professional counseling services, including work/life balance assistance. In addition, Cloudflare employees have access to an on-demand digital mental health and well-being platform. Cloudflare provides access to a fertility benefit that covers a variety of family planning services, including fertility treatment, adoption, and gestational carrier support — also referred to as surrogacy. During the COVID-19 pandemic, Cloudflare provided access to free online yoga and Pilates classes, as well as free digital memberships to a fitness application through its health care provider.			
	403-9	Work-related injuries	Cloudflare experienced no fatalities as a result of work-related injury. Cloudflare experienced no high-consequence work-related injuries.			

General Disclosures	Economic	Environmental	**Social**	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
GRI 404: Training and Education	103-1	Explanation of material topic and its Boundary	Learning and development at Cloudflare provides the tools and resources for all Cloudflare employees to grow and develop skills critical for success (Cloudflare Capabilities) and build an empathetic and inclusive community.			
	103-2	The management approach and its components	Learning and development at Cloudflare is overseen by the Head of People and the COO.			
	404-1	Average hours of training per year per employee	Cloudflare employees participated in approximately 5,752 hours of voluntary, developmental training. Cloudflare estimates that to be approximately 2.88 hours of training per employee.			
GRI 405: Diversity and Equal Opportunity	103-1	Explanation of material topic and its Boundary	See We Invest in Diversity, Equity, and Inclusivity, page 21. See Communities @ Cloudflare, page 22. Cloudflare Diversity, Equity, and Inclusion			
	103-2	The management approach and its components	Cloudflare diversity initiatives are overseen by the Head of People and the COO. Cloudflare diversity initiatives are also advanced by the Cloudflare Diversity and Inclusion Council as well as its Employee Resource Groups. Cloudflare Diversity, Equity, and Inclusion			
	103-3	Evaluation of the management approach	10-K Filing			
	405-1	Diversity of governance bodies and employees	See Diversity @ Cloudflare, page 23. Cloudflare Diversity, Equity, and Inclusion Corporate Governance Guidelines Proxy Statement Filing			
	405-2	Ratio of basic salary and remuneration of women to men	Cloudflare does not currently publish data on salary remuneration between men and women. However, Cloudflare is committed to achieving pay equity. Cloudflare has committed to the EU Charter, the UK Tech Talent Charter, and the German Diversity Charter. Cloudflare Diversity, Equity, and Inclusion			

General Disclosures	Economic	Environmental	Social	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
GRI 407: Freedom of Association and Collective Bargaining	103-1	Explanation of material topic and its Boundary	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 of the Fundamental Principles at Work. Human Rights Policy			
	103-2	The management approach and its components	10-K Filing			
	103-3	Evaluation of the management approach	10-K Filing			
	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 of the Fundamental Principles and Rights at Work. Human Rights Policy Cloudflare is not aware of any operations in 2021 in which the rights of employees to freely associate or collectively bargain were at risk.			
GRI 408: Child Labor	103-1	Explanation of material topic and its Boundary	Cloudflare expressly prohibits the use of child labor in its operations or among its suppliers. Human Rights Policy Modern Slavery Act Statement			
	103-2	The management approach and its components	All Cloudflare employees are required to complete mandatory compliance training, including regarding Cloudflare's prohibition on child labor. Business partners, resellers, suppliers, and vendors are regularly reviewed by legal, compliance, security, and senior leadership teams at Cloudflare. Evaluations of suppliers and vendors begin during the onboarding process and are periodically assessed for any material changes.			
	103-3	Evaluation of the management approach	Cloudflare's Modern Slavery Act Statement and associated policies, including prohibition on child labor, are overseen by its Head of Legal Compliance and General Counsel.			

General Disclosures	Economic	Environmental	Social	SASB

| GRI Standard | Reference | Disclosure | Answer | Omission | | |
				Part Omitted	Reason for Omission	Explanation of Omission
GRI 408: Child Labor *(continued)*	408-1	Operations and suppliers at significant risk for incidents of child labor	Cloudflare is not aware of any of its operations or suppliers that have significant risks for incidents of child labor or young workers exposed to hazardous work. In 2021, as in previous years, Cloudflare continues to explicitly prohibit child labor in its operations and among its suppliers. Although Cloudflare has identified no significant risk of child labor, it continues to regularly review its partners, resellers, suppliers, and vendors to ensure compliance with its policy.			
GRI 409: Forced or Compulsory Labor	103-1	Explanation of material topic and its Boundary	Cloudflare is committed to the ILO Declaration on Fundamental Principles and Rights at Work. To that end, Cloudflare expressly prohibits forced or compulsory labor. Human Rights Policy Modern Slavery Act Statement			
	103-2	The management approach and its components	All Cloudflare employees are required to complete mandatory compliance training, including regarding Cloudflare's prohibition on forced or compulsory labor. Business partners, resellers, suppliers, and vendors are regularly reviewed by legal, compliance, security, and senior leadership teams at Cloudflare. Evaluations of suppliers and vendors begin during the onboarding process and are periodically assessed for any material changes.			
	103-3	Evaluation of the management approach	Cloudflare's Modern Slavery Act Statement and associated policies, including prohibition on forced or compulsory labor are overseen by its Head of Legal Compliance and General Counsel.			
	409-1	Operations and suppliers at significant risk for incidents of forced or compulsory labor	Cloudflare is not aware of any of its operations or suppliers that have significant risks for incidents of forced or compulsory labor. In 2021, as in previous years, Cloudflare continues to explicitly prohibit forced or compulsory labor in its operations and among its suppliers. 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.			

General Disclosures   Economic   Environmental   **Social**   SASB

GRI Standard	Reference	Disclosure	Answer	Omission		
				Part Omitted	Reason for Omission	Explanation of Omission
GRI 412: Human Rights Assessments	103-1	Explanation of material topic and its Boundary	Human Rights Policy			
	103-2	The management approach and its components	Human Rights Policy			
	103-3	Evaluation of the management approach	Human Rights Policy			
	412-1	Operations that have been subject to human rights reviews or impact assessments	See Human Rights @ Cloudflare, page 10. Cloudflare published its first human rights policy in 2021. Cloudflare's Public Policy team regularly engages in multistakeholder dialogue on human rights issues, including as part of the Global Network Initiative and UN B-Tech Project Community of Practice.			
	412-2	Employee training on human rights policies or procedures	Cloudflare employees were not subject to human rights training in 2021. However, Cloudflare intends to implement annual human rights training for 100% of its employees beginning in 2022.			
GRI 414: Supplier Social Assessment	414-1	Supplier social assessment	Cloudflare intends to screen suppliers using social criteria beginning in 2022.			
GRI 415: Public Policy	103-1	Explanation of material topic and its Boundary	Cloudflare's Public Policy team serves as a conduit between the company and regulators, policy makers, civil society, and the public on policy issues relevant to Cloudflare's mission to help build a better Internet.			
	103-2	The management approach and its components	The Public Policy team is overseen by the Vice President and Global Head of Public Policy and the General Counsel.			
	415-1	Political contributions	Cloudflare made no political contributions in 2021, and does not operate a Political Action Committee. 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 102-13.			

General Disclosures	Economic	Environmental	**Social**	SASB

GRI Standard	Reference	Disclosure	Answer	Omission Part Omitted	Reason for Omission	Explanation of Omission
GRI 418: Customer Privacy	103-1	Explanation of material topic and its Boundary	See Privacy @ Cloudflare, page 9. See More Private, More Secure, page 8. Cloudflare Privacy Policy Cloudflare GDPR Cloudflare Privacy and Compliance Week			
	103-2	The management approach and its components	Cloudflare's Privacy and associated policies are overseen by its Data Protection Officer and General Counsel.			
	418-1	Substantiated complaints concerning breaches of customer privacy and losses of customer data	Cloudflare has not experienced any breaches or intrusions of its information technology systems resulting in inadvertent or unauthorized disclosure of personal data. See also SASB.			
GRI 419: Socioeconomic Compliance	419-1	Non-compliance with laws and regulations in the economic or social area	Cloudflare has not aware of any non-compliance with laws or regulations in the social area.			

General Disclosures	Economic	Environmental	Social	SASB

SASB - Technology
& Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Category	Answers
Environmental Footprint of Hardware Infrastructure	TC-S1-130a.1	1) Total energy consumed, 2) percentage grid electricity, 3) percentage renewable	Quantitative	Cloudflare consumed 41.3 GWh in 2020. 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 2020. Emissions Inventory 2020
	TC-S1-130a.1	1) Total water withdrawn, (2) total water consumed, percentage of regions with High or Extremely High Baseline Water Stress	Quantitative	See GRI 303.
	TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	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. See Making the Internet More Efficient, page 26.
Data Privacy & Freedom of Expression	TC-SI-220a.1	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	See Privacy @ Cloudflare, page 9. Cloudflare Privacy Policy Cloudflare Cookie Policy
	TC-SI-220a.2	Number of users whose information is used for secondary purposes	Quantitative	Cloudflare only processes personal information 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. See Privacy @ Cloudflare, page 9.
	TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Quantitative	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	Quantitative	See Transparency @ Cloudflare, page 15. See Transparency Spotlight: Warrant Canaries, page 16. Transparency Report

General Disclosures	Economic	Environmental	Social	SASB

SASB - Technology
& Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Category	Answers
Data Privacy & Freedom of Expression *(continued)*	TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Discussion and Analysis	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 January 2020, a German court issued an order directing Cloudflare to block access to a website it had concluded was violating copyright law. Pending further litigation, and to the extent the website uses Cloudflare's services, Cloudflare took steps in February 2020 to disable access to the website for customers in Germany or from Cloudflare equipment in Germany. In July 2020 and October 2020, Italian courts issued orders directing Cloudflare to block access to websites the courts concluded were violating copyright law. Consistent with those orders, Cloudflare took steps following the issuance of each order to disable access to those websites for customers in Italy or from Cloudflare equipment in Italy, to the extent those websites continue to use Cloudflare's services. Cloudflare took action to geoblock all 6 domains that were addressed by the court orders and were using our service at the time the orders were issued. To provide additional transparency, Cloudflare maintains a list of warrant canaries on its website, which list actions Cloudflare has never taken: • Cloudflare has never turned over our encryption or authentication keys or our customers' encryption or authentication keys to anyone. • Cloudflare has never installed any law enforcement software or equipment anywhere on our network. • Cloudflare has never provided any law enforcement organization a feed of our customers' content transiting our network. • Cloudflare has never modified customer content at the request of law enforcement or another third party. • Cloudflare has never modified the intended destination of DNS responses at the request of law enforcement or another third party. • Cloudflare has never weakened, compromised, or subverted any of its encryption at the request of law enforcement or another third party. See Transparency Spotlight: Warrant Canaries, page 16.

General Disclosures	Economic	Environmental	Social	SASB

SASB - Technology
& Communications Sector

Software & IT Services

Topic	Code	Accounting Metric	Category	Answers
Data Security	TC-SI-230a.1	1) Number of data breaches, 2) percentage involving personally identifiable information (PII), 3) number of users affected	Quantitative	Cloudflare did not experience any data breaches involving personally identifiable information (PII).
	TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cyber security standards	Discussion and Analysis	Cloudflare has implemented a formal security risk program that adheres to industry standards such as ISO 27000, 27701, PCI DSS, and SOC 2 Type II and has been evaluated by third-party assessors against the requirements.
Recruiting & Managing a Global, Diverse & Skilled Workforce	TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and 2) located offshore	Quantitative	Cloudflare Diversity, Equity, and Inclusion
	TC-SI330a.2	Employee engagement as a percentage	Quantitative	Omitted; insufficient data.
	TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for 1) management, 2) technical staff, and 3) all other employees	Quantitative	Cloudflare Diversity, Equity, and Inclusion
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	Quantitative	Cloudflare incurred no monetary losses resulting from anti-competitive behavior regulations.
Managing Systemic Risks from Technology Disruptions	TC-SI-550a.1	Number of 1) performance issues, and 2) service disruptions; 3) total customer downtime	Quantitative	Cloudflare modified its disclosure consistent with the SASB Standards Application Guidance. In April 2020, Cloudflare's core co-location facility in the US Pacific Northwest experienced an outage of approximately 4-1/2 hours as a result of an error that occurred during planned maintenance activities at that facility and, during the outage, customers lost access to certain features included in Cloudflare products.
	TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	Discussion and Analysis	10-Q Filing

SBC VERIFICATION LETTER

Cloudflare
101 Townsend St
San Francisco, CA 94107

Sustainable Business Consulting
3409 California Ave SW Unit C
Seattle, WA 98116

June 25, 2021

Dear Patrick,

Sustainable Business Consulting (SBC) is pleased to provide an independent and impartial validation of Cloudflare's 2019 and 2020 Greenhouse Gas (GHG) footprint. This report provides Cloudflare with an independent third-party limited assurance that the 2019 and 2020 GHG Emissions reported are correct. In this report, the detailed verification framework and associated activities conducted to reach an assurance conclusion are discussed. The findings from this verification are reported here, along with a verification statement attesting to the accuracy of the Cloudflare's GHG emissions reporting. The verification statement is signed by the Lead Verifier and the Peer Reviewer.

This verified emissions report encompassed all of Cloudflare's operations for the 2019 and 2020 calendar years. This includes global network and facilities leased by Cloudflare. Cloudflare reports emissions in the two reporting scopes: Scope 1, direct emissions, Scope 2, indirect emissions. This successful third-party verification confirms the accuracy and completeness of the information provided to substantiate the 2019 and 2020 Cloudflare's GHG emissions reporting.

In providing this limited assurance, SBC has found no evidence that the Cloudflare's 2019 and 2020 GHG emissions reports are not correct, and not presented fairly in accordance with stated criteria.

Nidhi Singh

Nidhi Singh

June 25, 2021

For more information, please visit www.cloudflare.com/impact.