



Cloudflare 2023 Year in Review

12-12-2023



David Belson









28 min read





The 2023 Cloudflare Radar Year in Review is our fourth annual review of Internet trends and patterns observed throughout the year at both a global and country/region level across a variety of metrics. Below, we present a summary of key findings, and then explore them in more detail in subsequent sections.

Key findings

[Traffic Insights & Trends](#)

-
- Global Internet traffic grew 25%, in line with peak 2022 growth. Major holidays, severe weather, and intentional shutdowns clearly impacted Internet traffic. 
 - Google was again the most popular general Internet service, with 2021 leader TikTok falling to fourth place. OpenAI was the most popular service in the emerging Generative AI category, and Binance remained the most popular Cryptocurrency service. 
 - Globally, over two-thirds of mobile device traffic was from Android devices. Android had a >90% share of mobile device traffic in over 25 countries/regions; peak iOS mobile device traffic share was 66%. 
 - Global traffic from Starlink nearly tripled in 2023. After initiating service in Brazil in mid-2022, Starlink traffic from that country was up over 17x in 2023. 
 - Google Analytics, React, and HubSpot were among the most popular technologies found on top websites. 
 - Globally, nearly half of web requests used HTTP/2, with 20% using HTTP/3. 
 - NodeJS was the most popular language used for making automated API requests. 
 - Googlebot was responsible for the highest volume of request traffic to Cloudflare in 2023. 








Connectivity & Speed

- Over 180 Internet outages were observed around the world in 2023, with many due to government-directed regional and national shutdowns of Internet connectivity. 
- Aggregated across 2023, only a third of IPv6-capable requests worldwide were made over IPv6. In India, however, that share reached 70%. 

-
- The top 10 countries all had measured average download speeds above 200 Mbps, with Iceland showing the best results across all four measured Internet quality metrics. 
 - Over 40% of global traffic comes from mobile devices. In more than 80 countries/regions, the majority of traffic comes from mobile devices.



Security

- Just under 6% of global traffic was mitigated by Cloudflare's systems as being potentially malicious or for customer-defined reasons. In the United States, 3.65% of traffic was mitigated, while in South Korea, it was 8.36%. 
- A third of global bot traffic comes from the United States, and over 11% of global bot traffic comes from Amazon Web Services. 
- Globally, Finance was the most attacked industry, but the timing of spikes in mitigated traffic and the target industries varied widely throughout the year and around the world. 
- Even as an older vulnerability, Log4j remained a top target for attacks during 2023. However, HTTP/2 Rapid Reset emerged as a significant new vulnerability, beginning with a flurry of record-breaking attacks. 
- 1.7% of TLS 1.3 traffic is using post-quantum encryption. 
- Deceptive links and extortion attempts were two of the most common types of threats found in malicious email messages. 
- Routing security, measured as the share of RPKI valid routes, improved globally during 2023. Significant growth was observed in countries including Saudi Arabia, the United Arab Emirates, and Vietnam. 

Introduction

[Cloudflare Radar](#) launched in September 2020, and in the [blog post that announced its availability](#), we talked about how its intent was to “shine a light on the Internet’s patterns”. Cloudflare’s network currently spans more than 310 cities in over 120 countries/regions, serving an average of over 50 million HTTP(S) requests per second for millions of Internet properties, in addition to handling over 70 million DNS requests per second on average. The data generated by this massive global footprint and scale, combined with data from complementary Cloudflare tools, enables Radar to provide unique near-real time perspectives on the patterns and trends we observe across the Internet. For the last several years ([2020](#), [2021](#), [2022](#)), we’ve been aggregating these insights into an annual Year In Review, shining a light on the Internet’s patterns over the course of that year. The new [Cloudflare Radar 2023 Year In Review](#) continues that tradition, featuring interactive charts, graphs, and maps you can use to explore notable Internet trends observed throughout this past year.

The 2023 Year In Review is organized into three sections: [Traffic Insights & Trends](#), [Connectivity & Speed](#), and [Security](#). We have incorporated several new metrics this year, and have endeavored to keep underlying methodologies consistent with last year wherever possible. Website visualizations shown at a weekly granularity cover the period from January 2 through November 26, 2023. Trends for over 180 countries/regions are available on the website, with some smaller or less populated locations excluded due to insufficient data. Note that some of the metrics are presented only as a worldwide view, and will not be shown if a country/region is selected. Because of the [control plane and analytics outage](#) that occurred November 2-4, traffic data for relevant metrics has been interpolated for that three-day period.

Below, we provide an overview of the content contained within the major Year In Review sections ([Traffic Insights & Trends](#), [Connectivity & Speed](#), and [Security](#)), along with notable observations and key findings. In addition, we

have also published a companion blog post that specifically explores trends seen across [Top Internet Services](#).

However, the notable observations and key findings contained within this post only skim the surface of the unique insights that can be found in the [Year in Review website](#), which we strongly encourage you to visit to explore the data in more detail and look at trends for your country/region. As you do so, we encourage you to consider how the trends presented within these blog posts and the website's various sections impact your business or organization, and to think about how these insights can inform actions that you can take to improve user experience or enhance your security posture in the future.

Traffic Insights & Trends



Global Internet traffic grew 25%, in line with peak 2022 growth. Major holidays, severe weather, and intentional shutdowns clearly impacted Internet traffic.

Twenty-five years ago, Worldcom executives claimed that [Internet traffic was doubling](#) every 100 days (3.5 months). A quarter-century later, we know that these claims were unrealistically aggressive, but it is clear that the Internet is growing quickly as more and more devices are connected, consuming content from a growing universe of websites, applications, and services.

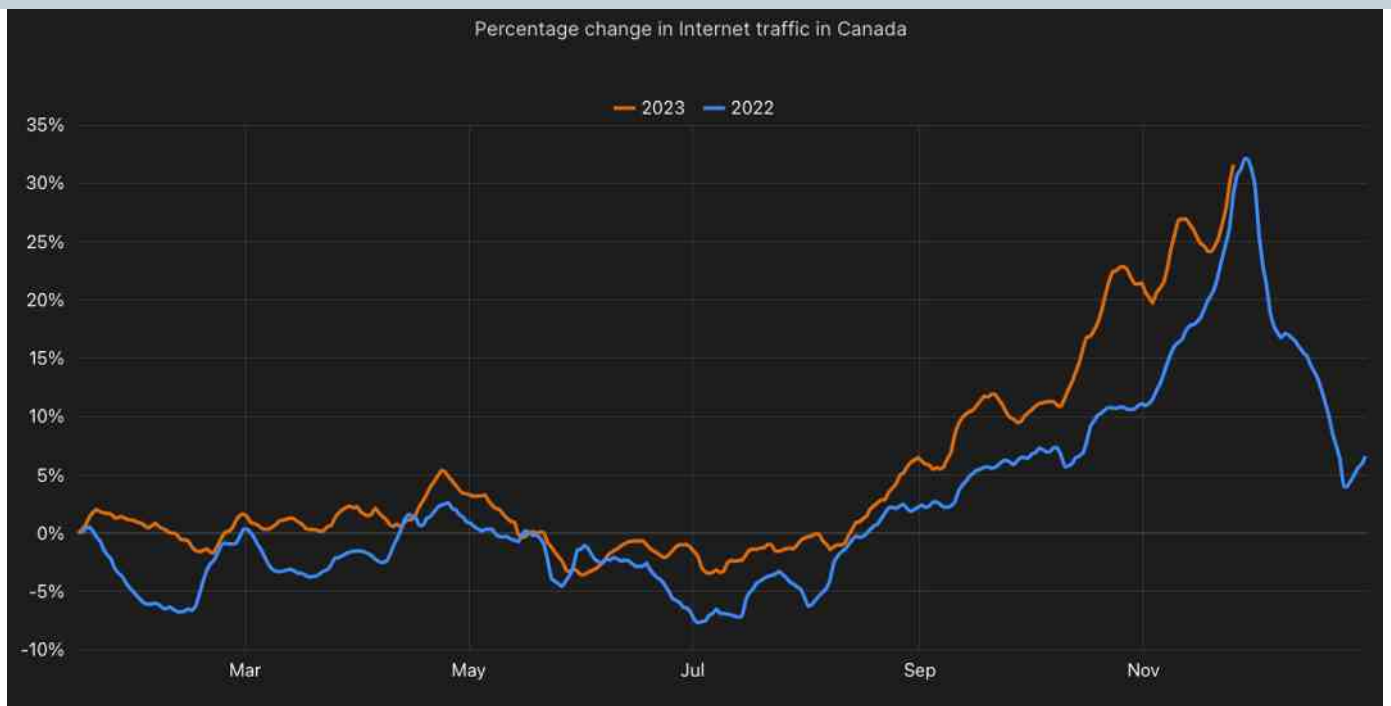
To determine the traffic trends over time, we first established a baseline, calculated as the average daily traffic volume (excluding bot traffic) over the second full calendar week (January 8-14) of 2023. We chose the second calendar week to allow time for people to get back into their “normal” routines

(school, work, etc.) after the winter holidays and New Year's Day. The percent change shown in our traffic trends chart is calculated relative to the baseline value, and represents a seven-day trailing average — it does not represent absolute traffic volume for a country/region. The seven-day averaging is done to smooth the sharp changes seen with a daily granularity. A trend line for 2022 is shown for comparison purposes.

Our data shows that [globally](#), Internet traffic grew 25% in 2023, with nominal initial growth accelerating during the second half of the year. Overall, the pattern is similar to that observed in 2022 (excepting last year's late February spike), and peak growth for the year is just slightly above the peak growth level seen in 2022. Traffic patterns in [Canada](#) were also rather consistent year-over-year, exhibiting similar seasonality, and peak growth above 30% in both 2022 and 2023. In many countries, the 2022 trend line shows a clear drop in traffic heading into the Christmas holiday, with a slight rebound ahead of New Year's Day. It will be interesting to see if traffic follows this pattern in 2023 as well.



Global Internet traffic growth in 2023, compared with 2022



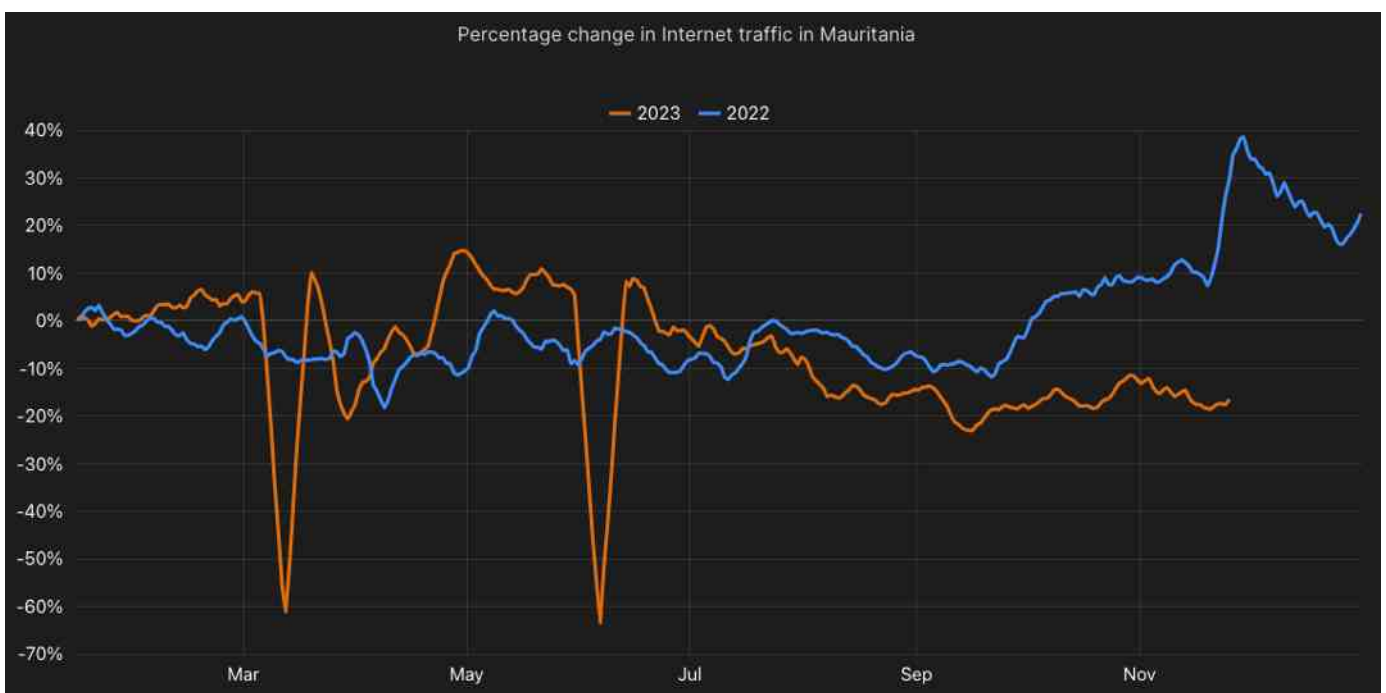
Internet traffic growth in Canada in 2023, compared with 2022

Comparisons with 2022 traffic trends helps make the [impact of major holidays on Internet traffic](#) more visible. For example, in Muslim countries including [Indonesia](#), [Turkey](#), and the [United Arab Emirates](#), the celebration of Eid-UI-Fitr, the festival marking the end of the fast of Ramadan, is visible as a noticeable drop in traffic around April 21-23, 2023, just before a similar drop visible in the 2022 trend line during last year's celebration on May 2-3. In [Italy](#), a drop in traffic is clearly visible around Pasqua di Resurrezione and Lunedì dell'Angelo (Easter Sunday and Monday) on April 9-10, one week ahead of a similar drop in traffic in 2022

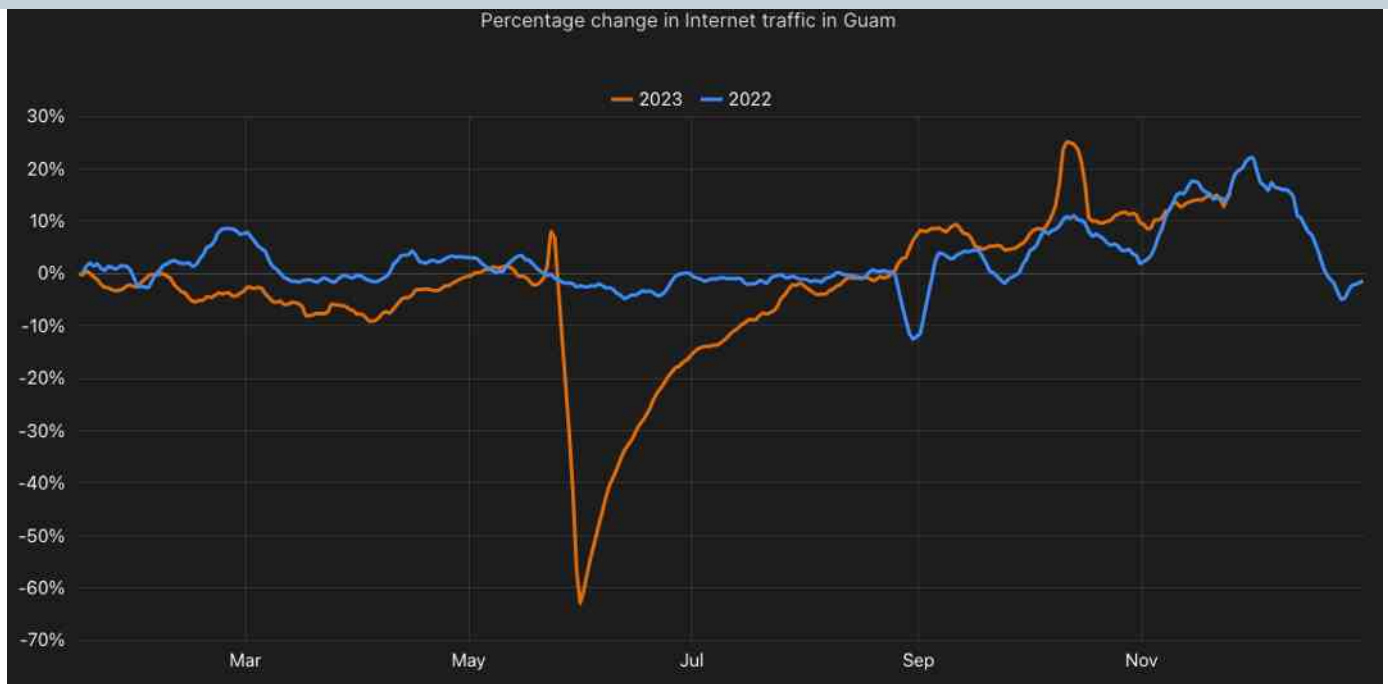


Internet traffic growth in Indonesia in 2023, compared with 2022

In addition, extended disruptions to Internet connectivity are also clearly visible within the traffic trend charts. Examples include [Mauritania](#), where government-directed shutdowns occurred from [March 6-12](#) and [May 30 - June 6](#), and [Gabon](#), where a [shutdown](#) was in place from August 26-30, as well as [Guam](#), where [Super Typhoon Mawar](#) caused a multi-week drop in traffic starting on May 24.



Internet traffic growth in Mauritania in 2023, compared with 2022



Internet traffic growth in Guam in 2023, compared with 2022

Google was again the most popular general Internet service, with 2021 leader TikTok falling to fourth place. OpenAI was the most popular service in the emerging Generative AI category, and Binance remained the most popular Cryptocurrency service.

One of the most popular sections of the Year In Review over the last several years has been the exploration of the most popular Internet services, both generally and across a number of categories. These rankings of service popularity are based on analysis of anonymized query data of traffic to our [1.1.1.1 public DNS resolver](#) from millions of users around the world. Although DNS resolution operates at a domain level, domains that belong to a single Internet service are grouped together for the purposes of these rankings.

In the overall category, [Google](#) once again held the top spot, owing in part to its broad portfolio of services as well as the popularity of the Android mobile operating system. In addition to perennial categories like e-commerce, video streaming, and messaging, this year we also looked at Generative AI, which has been on a meteoric rise in 2023. In this category, [OpenAI](#) held the top

spot, building on the success and popularity of [ChatGPT](#), which it launched only a year ago. And despite the turmoil seen in the cryptocurrency space this year, [Binance](#) remained the most popular service in that category.

We explore these categorical rankings, as well as trends seen by specific services, in more detail in a [separate blog post](#).

Overall	Rank	Service
Generative AI	#1	Google
Social Media	#2	Facebook
Video Streaming	#3	Apple
News	#4	TikTok
E-Commerce	#5	Microsoft
Messaging	#6	YouTube
Metaverse & Gaming	#7	AWS
Financial Services	#8	Instagram
Cryptocurrency Services	#9	Amazon
	#10	iCloud

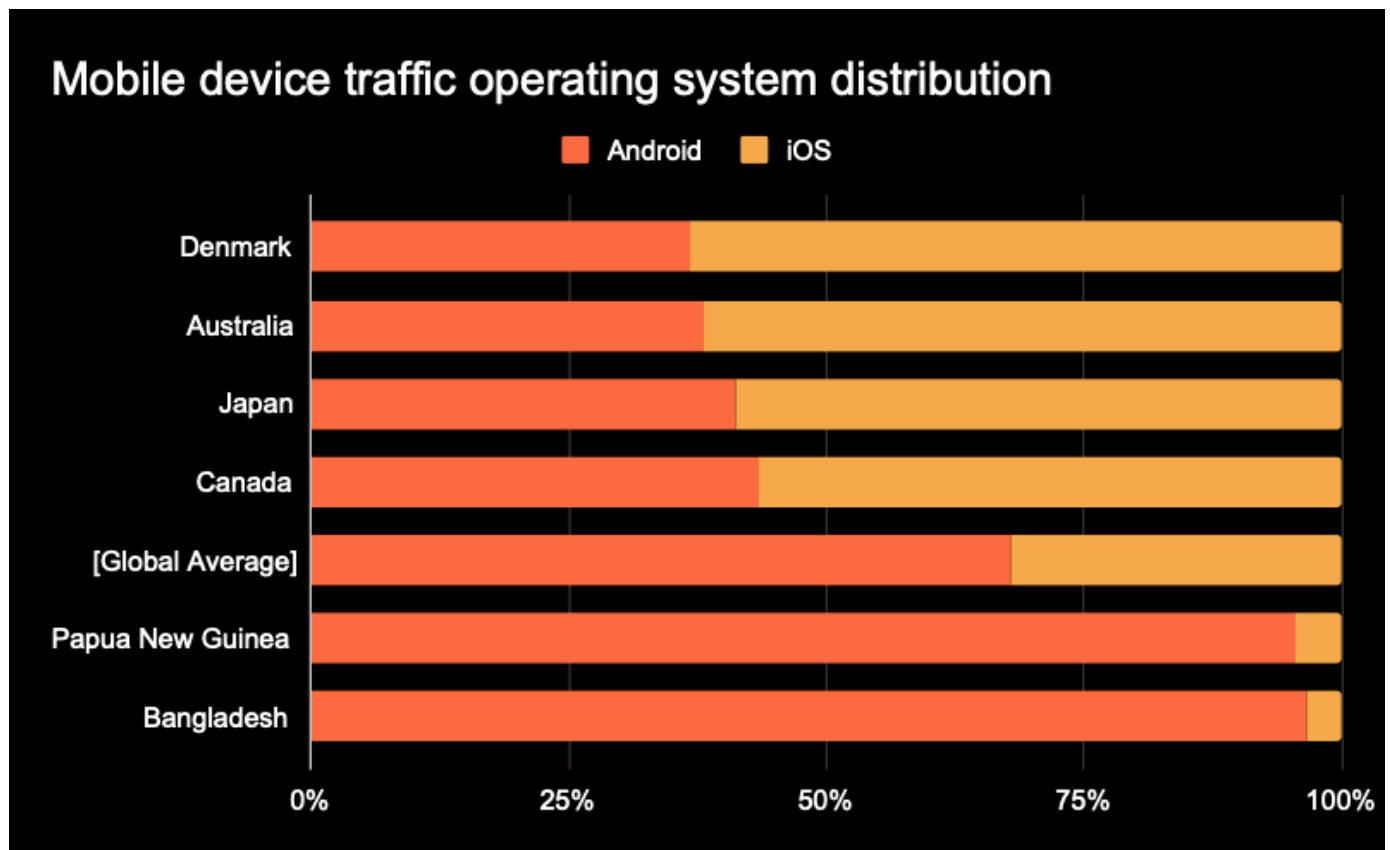
Globally, over two-thirds of mobile device traffic was from Android devices. Android had a >90% share of mobile device traffic in over 25 countries/regions; peak iOS mobile device traffic share was 66%.

[Apple's iOS](#) and [Google's Android](#) are the two leading operating systems used on mobile devices, and analysis of information in the user agent reported with each request allows us to gain insight into the distribution of traffic by client operating system throughout the year. Given the wide range of both devices and price points for Android devices, it is not surprising that Android is responsible for the majority of mobile device traffic when aggregated globally.

[Globally](#), over two-thirds of mobile device traffic was from Android devices. The split is in line with Android/iOS usage observed in 2022. When looking at the countries/regions with the highest levels of Android usage, we find [Bangladesh](#) and [Papua New Guinea](#) at the top of the list, both with over 95%

of mobile device traffic coming from Android devices. Looking more closely at other countries that see particularly high levels of Android usage, it is interesting to note that they are largely in Africa, Oceania/Asia, and South America, and that many have lower levels of [gross national income per capita](#). This is presumably where the availability of lower priced “budget” phones plays to Android’s advantage from an adoption perspective.

In contrast, while the share of mobile device traffic from iOS at a country/region level never tops 70%, many of the countries with an iOS share over 50%, including [Denmark](#), [Australia](#), [Japan](#), and [Canada](#), have comparatively higher gross national income per capita, which likely speaks to a greater ability to afford higher priced devices.



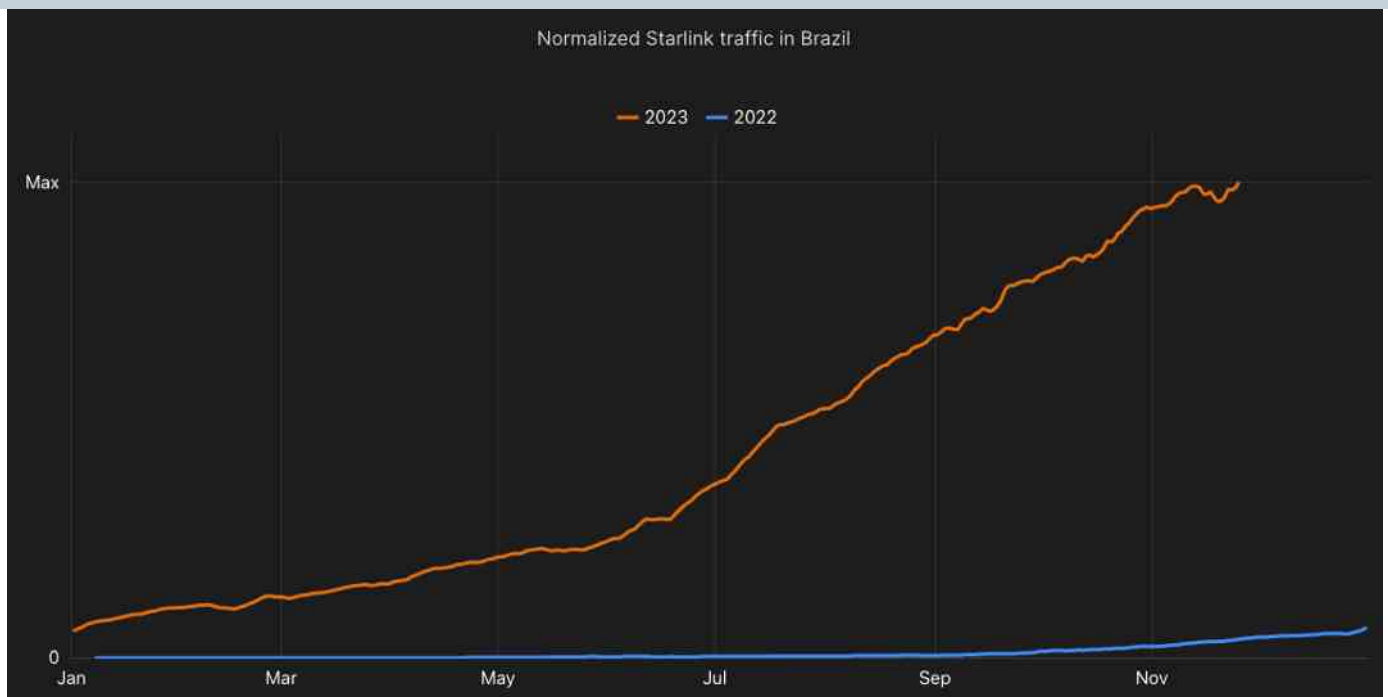
Mobile device traffic operating system distribution across selected countries

Global traffic from Starlink nearly tripled in 2023. After initiating service in Brazil in mid-2022, Starlink traffic from that country was up over 17x in 2023.

SpaceX's [Starlink](#) high-speed satellite Internet service has continued to rapidly grow its footprint since launching in 2019, making high performance Internet connections available in many countries/regions that were previously unserved or underserved by traditional wired or wireless broadband. The current leader in the space, in the future it will be joined by Amazon's [Project Kuiper](#) service, which [launched its first two test satellites this year](#), as well as [Eutelsat OneWeb](#), which [grew its satellite constellation](#) in 2023 as well.

To track the growth in usage and availability of Starlink's service, we analyzed aggregate Cloudflare traffic volumes associated with the service's autonomous system ([AS14593](#)) throughout 2023. Although Starlink is not yet available globally, we did see traffic growth across a number of countries/regions. The request volume shown on the trend line in the chart represents a seven-day trailing average. A trend line for 2022 is shown for comparison purposes, and is scaled to the maximum value across 2022 and 2023.

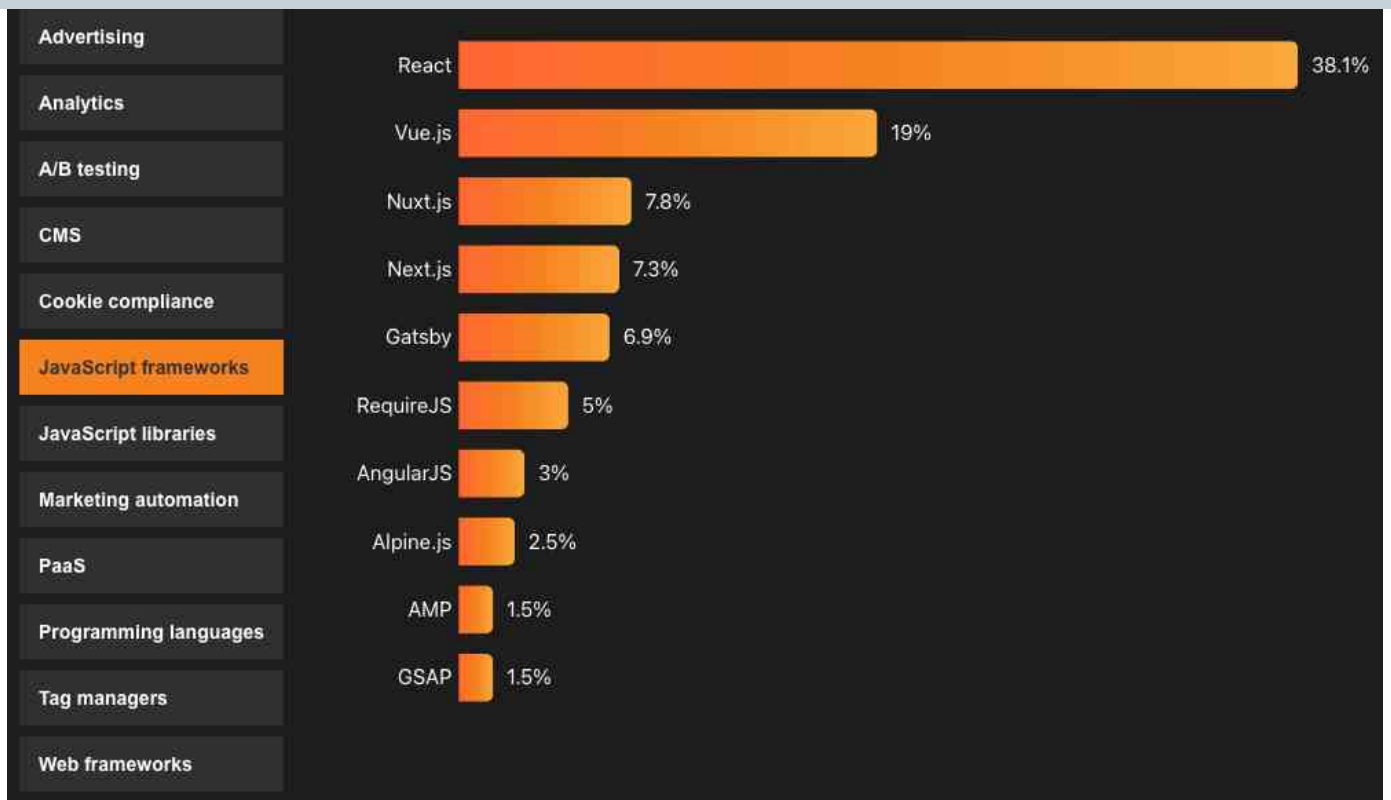
[Globally](#), we saw Starlink traffic more than triple this year. In the [United States](#), traffic from Starlink was up over 2.5x, and grew over 17x in [Brazil](#). In countries where Starlink turned up service in 2023, including [Kenya](#), [the Philippines](#), and [Zambia](#), we saw traffic grow rapidly once the service became available.



Starlink traffic growth in Brazil, compared with 2022

Google Analytics, React, and HubSpot were among the most popular technologies found on top websites.

Modern websites are complex productions, relying on a mix of frameworks, platforms, services, and tools, and the developer community is responsible for making them coexist with one another to deliver a seamless experience. Using the [Cloudflare Radar URL Scanner](#), which we [launched in March 2023](#), we scanned websites associated with the [top 5000 domains](#) to identify the [most popular technologies and services](#) used across a dozen different categories, including (but not limited to) Analytics, where [Google Analytics](#) was by far the most widely used; JavaScript Frameworks, where [React](#) had a commanding lead; and Marketing Automation providers, where leader [HubSpot](#) was closely followed by several competitors.



Top website technologies, JavaScript frameworks category

Globally, nearly half of web requests used HTTP/2, with 20% using HTTP/3.

HTTP (HyperText Transfer Protocol) is the core protocol that the web relies upon. [HTTP/1.0](#) was first standardized in 1996, [HTTP/1.1](#) in 1999, and [HTTP/2](#) in 2015. The most recent version, [HTTP/3](#), was completed in 2022, and runs on top of QUIC, a new transport protocol. On the client side, HTTP/3 support is [enabled](#) by default in the latest versions of desktop and mobile Google Chrome and Mozilla Firefox, and for a portion of Apple Safari users. HTTP/3 is [available for free](#) for all Cloudflare customers, though not every customer chooses to enable it.

[Using QUIC](#) allows HTTP/3 to deliver improved performance by mitigating the effects of packet loss and network changes, as well as establishing connections more quickly. It also provides encryption by default, mitigating the risk of attacks. Websites and applications that remain on older versions of HTTP miss out on these benefits.

Analysis of the HTTP version negotiated for each request allows us to gain insight into the distribution of traffic by the various versions of the protocol aggregated throughout the year. (“HTTP/1.x” aggregates requests made over HTTP/1.0 and HTTP/1.1.) At a [global](#) level, 20% of requests were made over the latest version, HTTP/3. Another third of requests were made over the comparatively ancient HTTP/1.x versions, while HTTP/2 remained dominant, and accounted for the 47% balance.



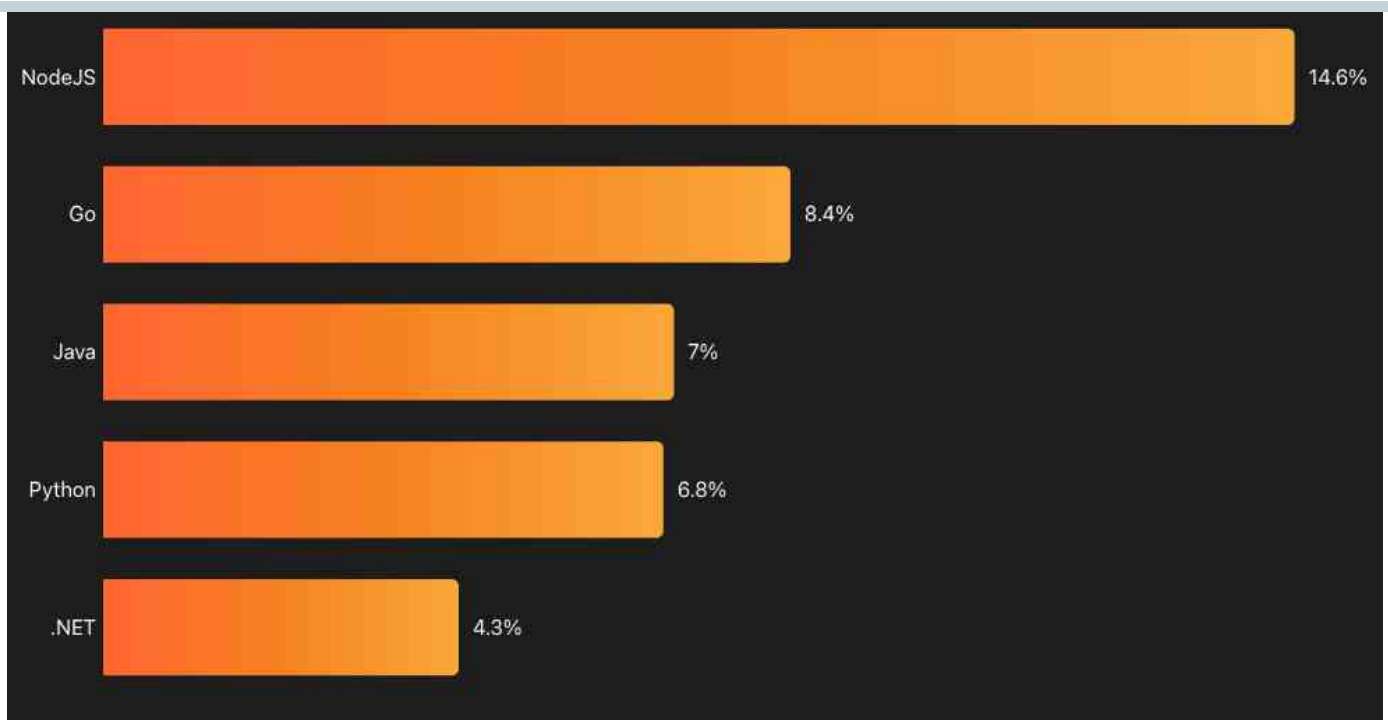
Global HTTP version traffic distribution

Looking at the version distribution geographically, we found a number of Asian countries, including [Nepal](#), [Thailand](#), [Malaysia](#), and [Sri Lanka](#) among those with highest rates of HTTP/3 usage, although these rates did not exceed 35%. In contrast, more than half of the requests from ten countries, including [Ireland](#), [Albania](#), [Finland](#), and [China](#), were made over HTTP/1.x during 2023.

NodeJS was the most popular language used for making automated API requests.

In addition, as developers increasingly use [automated API calls](#) to power dynamic websites and applications, we can use our unique visibility into Web traffic to identify the top languages these API clients are written in. Looking at API-related requests determined to not be coming from a person using a browser or native mobile application, we applied heuristics to help identify the language used to build the client.

[Our analysis](#) found that almost 15% of automated API requests are made by [NodeJS](#) clients, with [Go](#), [Java](#), [Python](#), and [.NET](#) holding smaller shares.



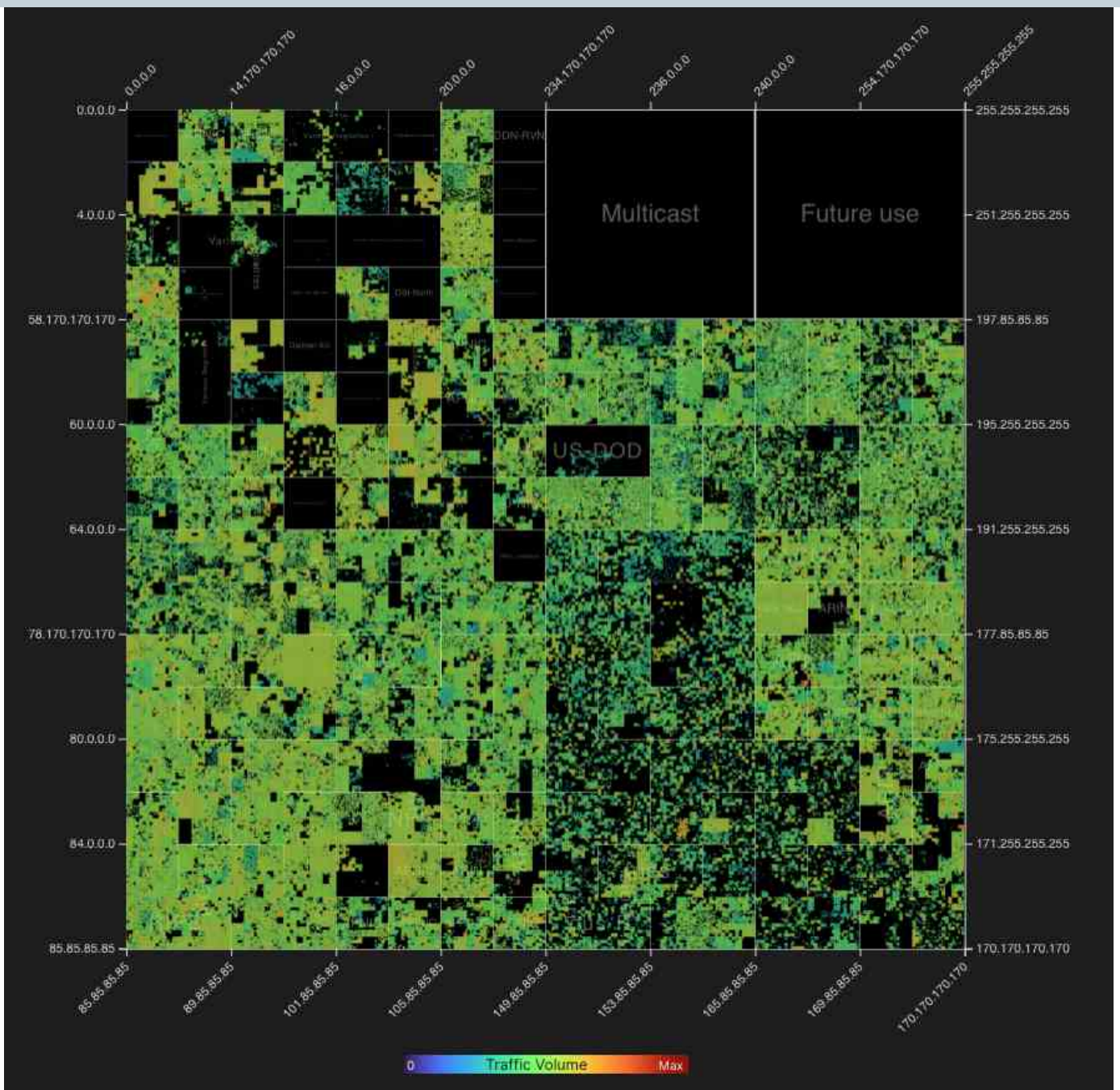
Top languages used to make automated API calls

Googlebot was responsible for the highest volume of request traffic to Cloudflare in 2023.

Cloudflare Radar enables users to see Internet traffic trends at a country/region or network level over a selected period of time. However, we wanted to zoom out a bit, and look at the traffic Cloudflare saw from the entire IPv4 Internet over the course of the entire year. [Hilbert curves](#), as “continuous space-filling curves”, have properties that are useful for [visualizing the Internet's IPv4 address space](#).

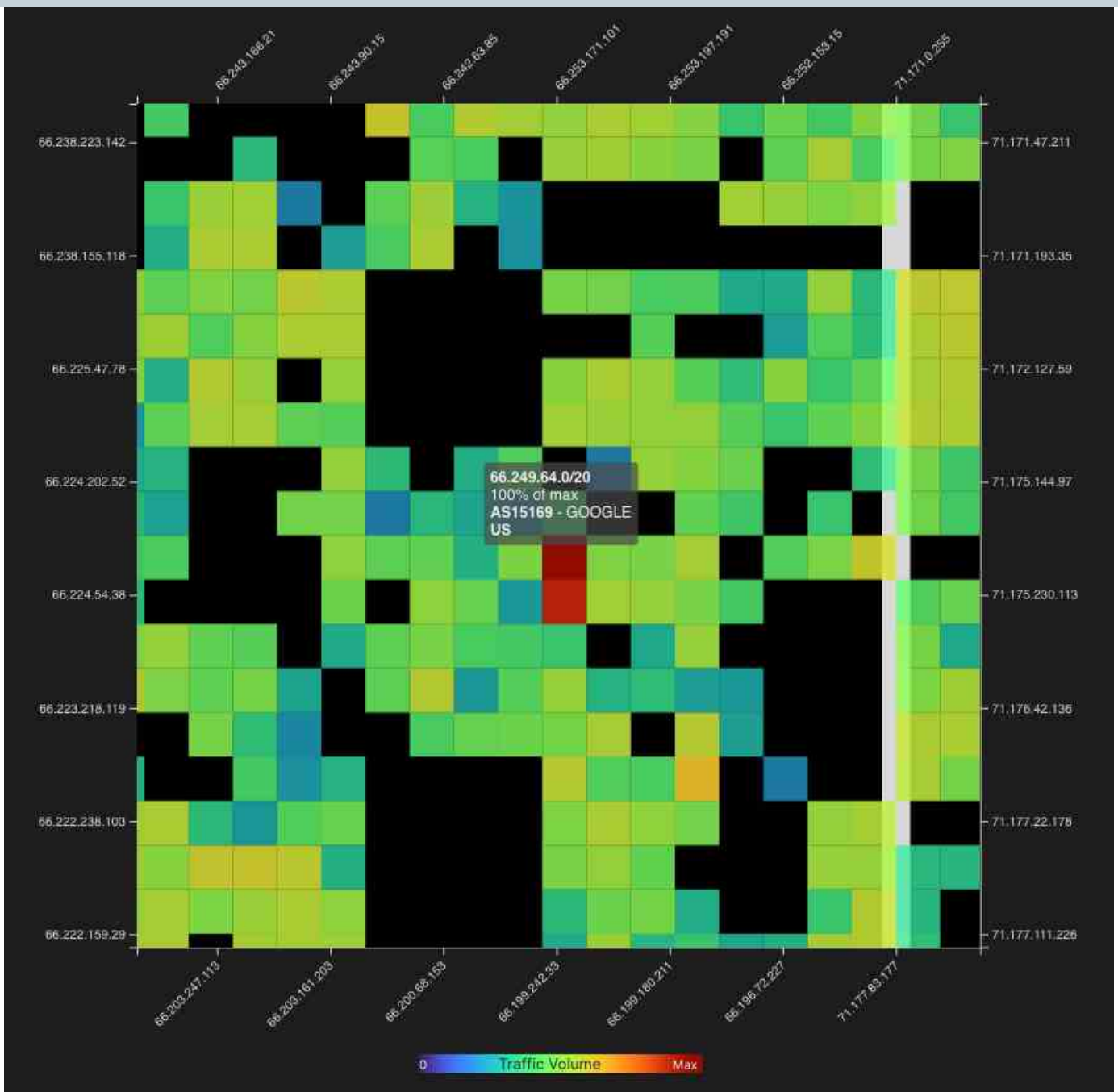
Using a Hilbert curve visualization, we can visualize aggregated request traffic (over IPv4) to Cloudflare from January 1st through November 26th, 2023. In order to make the amount of data used for the visualization manageable, IP addresses are aggregated at a [/20](#) level, meaning that at the highest zoom level, each cell represents traffic from 4096 IPv4 addresses. (The sheer size of the IPv6 address space would make associated traffic very [hard to see](#) in such a visualization, especially as such a small amount has been [allocated for assignment by the Regional Internet Registries](#).)

Within the visualization, IP addresses are grouped by ownership, and for much of the IP address space shown there, a mouseover at the default zoom level will show the [Regional Internet Registry \(RIR\)](#) that the address block belongs to. However, there are also a number of blocks that were assigned prior to the existence of the RIR system, and for these, they are labeled with the name of the organization that owns them. Progressive zooming ultimately shows the autonomous system and country/region that the IP address block is associated with, as well as its share of traffic relative to the maximum. (If a country/region is selected, only the IP address blocks associated with that location are visible.) Overall traffic shares are indicated by shading based on a color scale, and although a number of large unshaded blocks are visible, this does not necessarily mean that the associated address space is unused, but rather that it may be used in a way that does not generate traffic to Cloudflare.



Hilbert curve showing aggregated 2023 traffic to Cloudflare across the IPv4 Internet

Areas of higher request volume, indicated by warmer orange/red shading, are visibly scattered throughout the plot, but the IP address block that had the maximum request volume to Cloudflare during 2023 was 66.249.64.0/20, which belongs to Google. This IP address block is [one of several](#) used by the [Googlebot](#) web crawler, which is a likely explanation for the high request volume, given the number of web properties on Cloudflare's network.



Zoomed view of the Hilbert curve showing the IPv4 address block that generated the highest volume of requests

It is hard to do this visualization justice with a short summary and static screenshot. To explore it in more detail, we encourage you to go to [the Year in Review website](#) and explore it by dragging and zooming to move around the IPv4 Internet.

Connectivity & Speed

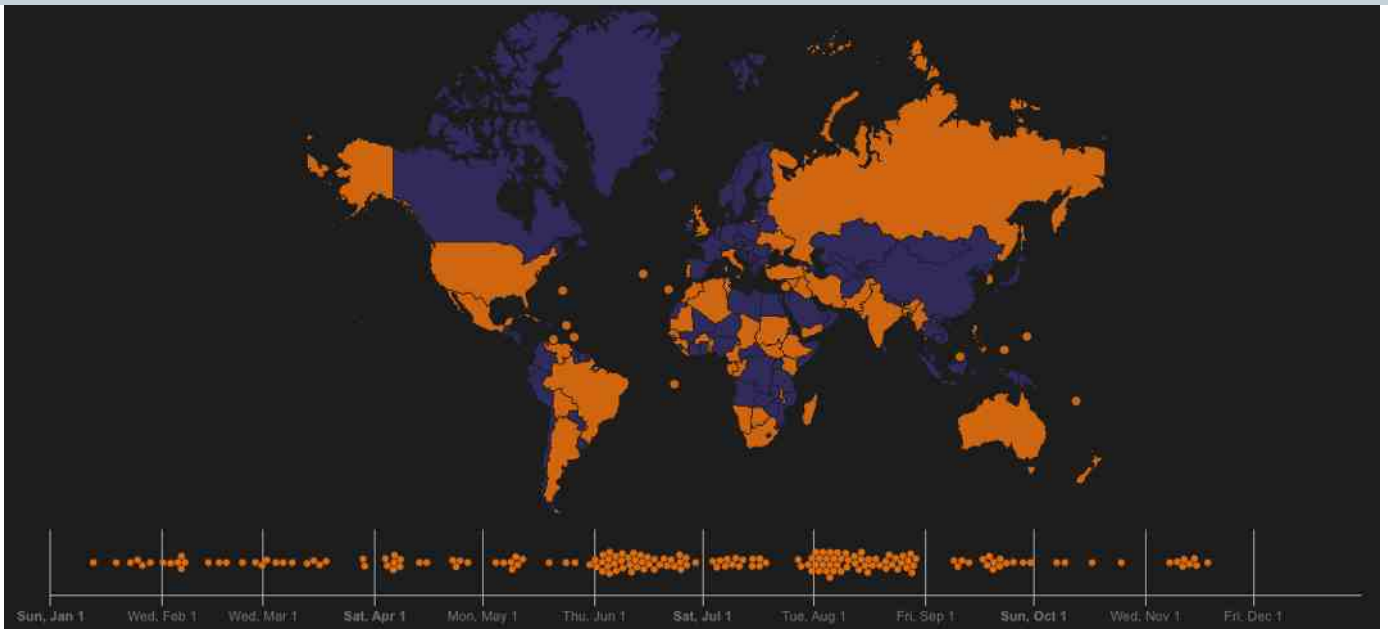


Over 180 Internet outages were observed around the world in 2023, with many due to government-directed regional and national shutdowns of Internet connectivity.

During 2023, we have written frequently about Internet outages, whether due to [technical issues](#), [government-directed shutdowns](#), or [geopolitical conflict](#), as well as infrastructure resilience issues (including fiber cuts, power outages, and severe weather) highlighted in our [quarterly summaries](#). The impacts of these outages can be significant, including significant economic losses and severely limited communications. The [Cloudflare Radar Outage Center](#) tracks these Internet outages, and uses Cloudflare traffic data for insights into their scope and duration.

Some of these outages seen through the year were short-lived, lasting just a couple of hours, while others have stretched on for multiple months. In the latter category, localized government-directed shutdowns in Manipur, [India](#) and Amhara, [Ethiopia](#) have lasted over seven and four months respectively (as of early December). In the former category, [Iraq](#) frequently experienced multi-hour nationwide Internet shutdowns intended to prevent cheating on academic exams — these contribute to the clustering visible in the timeline during June, July, and August.

Within the [timeline](#) on the Year in Review website, mousing over a dot will display metadata about that outage, and clicking on it will open a page with additional information. If a country/region is selected, only outages for that country will be displayed.



Internet outages were observed around the world during 2023

Aggregated across 2023, only a third of IPv6-capable requests worldwide were made over IPv6. In India, however, that share reached 70%.

IPv6 has been around in some fashion since 1998, with an expanded address space that better supports the universe of Internet-connected devices that has grown exponentially over the last quarter-century. And over that time, available IPv4 space has been [exhausted](#), leading connectivity providers to resort to solutions like [Network Address Translation](#), and cloud and hosting providers to acquire blocks of IPv4 address space for as much as [\\$50 per address](#). IPv6 also brings a number of other [benefits](#) to network providers, and if implemented correctly, adoption should be transparent from an end user perspective.

Cloudflare has been a vocal and active advocate for IPv6 stretching all the way back to our first birthday in 2011, when we announced our [Automatic IPv6 Gateway](#), which enabled free IPv6 support for all of our customers. Just a few years later, we enabled [IPv6 support by default for all of our customers](#). (Although it is enabled by default, not all customers choose to keep it enabled for a variety of reasons.) However, this support is only half of the equation for

driving IPv6 adoption, as end user connections need to support it as well. (Technically, it is a bit more complex than that, but those are the two foundational requirements.) Analysis of the IP version used for each request made to Cloudflare allows us to gain insight into the distribution of traffic by the various versions of the protocol, aggregated throughout the year.

Thanks to [near-complete IPv6 adoption by Indian telecommunications provider Reliance Jio](#), 70% of [dual-stacked](#) requests from Indian users were made via IPv6. [India](#) was followed closely by [Malaysia](#), where 66% of dual-stacked requests were made over IPv6 during 2023, thanks to strong IPv6 adoption rates across [leading Internet providers](#) within the country. Other countries that saw more than half of dual-stacked requests, on average, made over IPv6 include [Saudi Arabia](#), [Vietnam](#), [Greece](#), [France](#), [Uruguay](#), and [Thailand](#). In contrast, there were on the order of 40 countries/regions where less than 1% of dual-stacked requests were made over IPv6 during 2023. Lagging adoption across such a large cohort of countries/regions 25 years after IPv6 was first published as a [draft standard](#) is quite surprising.



IPv4/IPv6 traffic distribution in India

The top 10 countries all had measured average download speeds above 200 Mbps, with Iceland showing the best results across all four measured Internet quality metrics.

Even when they are not facing Internet outages, users around the world are often contending with poor performance on their Internet connections, whether due to low speeds, high latency, or a combination of these factors. Although Internet providers continue to evolve their service portfolios to offer increased connection speeds and reduced latency in order to support growth in use cases like online gaming and videoconferencing, consumer adoption is often mixed due to cost, availability, or other issues. By aggregating the

results of speed.cloudflare.com tests taken during 2023, we can get a geographic perspective on [connection quality](#) metrics including average download and upload speeds, and average idle and loaded latencies, as well as the distribution of the measurements.

In [Iceland](#), [over 85% of all Internet connections are over fiber](#), and this is reflected in its ranking as the country with the best overall Internet quality metrics, as speed test results show that providers there deliver the highest average speeds (282.5 Mbps download, 179.9 Mbps upload) and lowest average latencies (9.6 ms idle, 77.1 ms loaded). The histogram below shows that while there is a large cluster of download speeds between 0–100 Mbps, there were also a significant number of tests that measured even higher speeds, including some in excess of 1 Gbps.

Western European countries including [Spain](#), [Portugal](#), and [Denmark](#) also ranked among the top 10 across multiple Internet quality metrics.



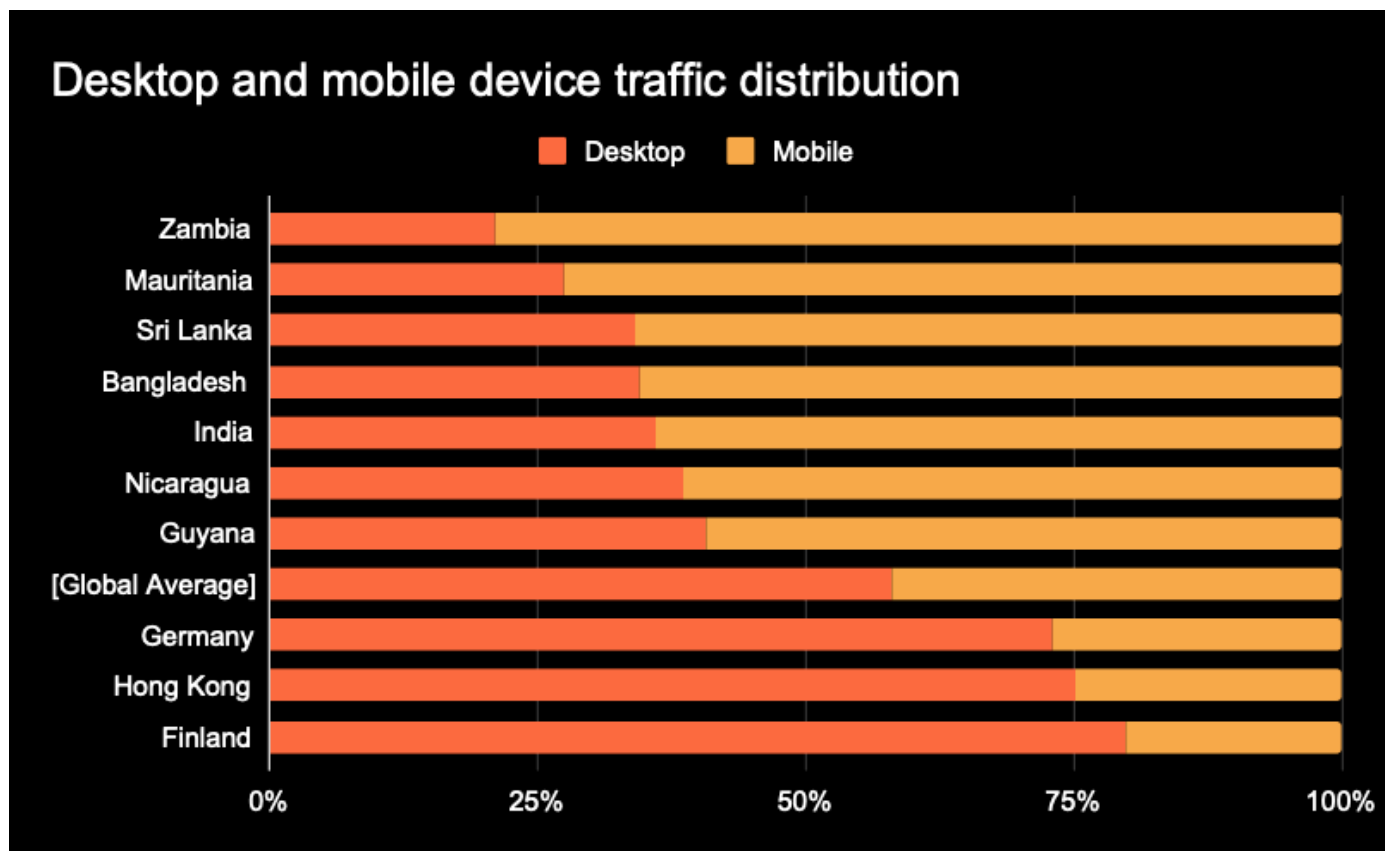
Download and upload speed test result distribution in Iceland

Over 40% of global traffic comes from mobile devices. In more than 80 countries/regions, the majority of traffic comes from mobile devices.

Over the last 15 years or so, mobile devices have become increasingly ubiquitous, becoming indispensable in both our personal and professional lives, thanks in large part to their ability to enable us to access the Internet from nearly anywhere at any time. In some countries/regions, mobile devices

primarily connect to the Internet via Wi-Fi, while others are “mobile first”, where Internet access is primarily through 4G/5G services.

Analysis of information contained with the user agent reported with each request to Cloudflare enables us to categorize it as coming from a mobile, desktop, or other type of device. Aggregating this categorization throughout the year at a global level, we found that 42% of traffic came from mobile devices, with 58% coming from desktop devices such as laptops and “classic” PCs. These traffic shares were in line with those measured in 2022. 79% of traffic came from mobile devices in [Zambia](#), making it the country with the largest mobile device traffic share in 2023. Other countries/regions that had more than 50% of traffic come from mobile devices were concentrated in the Middle East/Africa, the Asia Pacific Region, and South/Central America. In contrast, [Finland](#) had one of the highest shares of desktop device traffic, at 80%.



Desktop and mobile device traffic distribution across selected countries

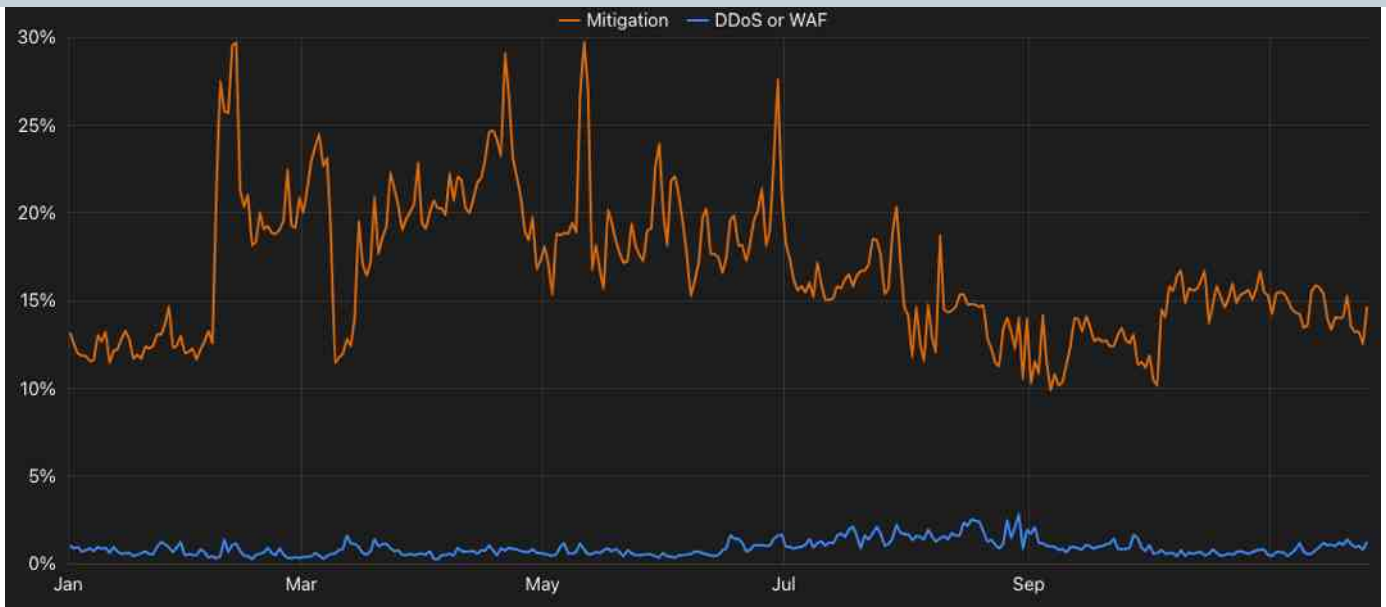
Security



Just under 6% of global traffic was mitigated by Cloudflare's systems as being potentially malicious or for customer-defined reasons. In the United States, 3.65% of traffic was mitigated, while in South Korea, it was 8.36%.

Malicious bots are often used to attack websites and applications. To protect customers from these threats, Cloudflare mitigates (blocks) this attack traffic using [DDoS](#) mitigation techniques or [Web Application Firewall \(WAF\) Managed Rules](#). However, customers may also choose to have Cloudflare mitigate traffic using other techniques for a variety of other reasons, such as [rate-limiting](#) requests, or [blocking all traffic from a given location](#), even if it isn't malicious. Analyzing traffic to Cloudflare's network seen throughout 2023, we looked at the overall share that was mitigated (for any reason), as well as the share that was mitigated as a DDoS attack or by WAF Managed Rules.

[Overall](#), just under 6% of global traffic was mitigated by Cloudflare's systems as being potentially malicious or for customer-defined reasons, while only around 2% of it saw DDoS/Managed WAF mitigations. Some countries, such as [Bermuda](#), saw the percentages for the two metrics track very closely, while other countries, like [Pakistan](#) and [South Africa](#) showed much larger gaps between their trend lines.



Mitigated traffic trends in Pakistan

A third of global bot traffic comes from the United States, and over 11% of global bot traffic comes from Amazon Web Services.

[Bot](#) traffic describes any non-human Internet traffic, and monitoring bot traffic levels can help site and application owners spot potentially malicious activity. Of course, bots can be helpful too, and Cloudflare maintains a list of [verified bots](#) to help keep the Internet healthy. Verified bots include those used for things like search engine indexing, performance testing, and availability monitoring. Regardless of intent, we wanted to look at where bot traffic was coming from, and we can use the IP address of a request to identify the network ([autonomous system](#)) and country/region associated with the bot making the request. Perhaps unsurprisingly, we found that cloud platforms were among the leading sources of bot traffic. This is likely due to the ease of automating the provisioning/teardown of compute resources and the relatively low cost of doing so, the distributed geographic footprint of cloud platforms, and the availability of high-bandwidth connections.

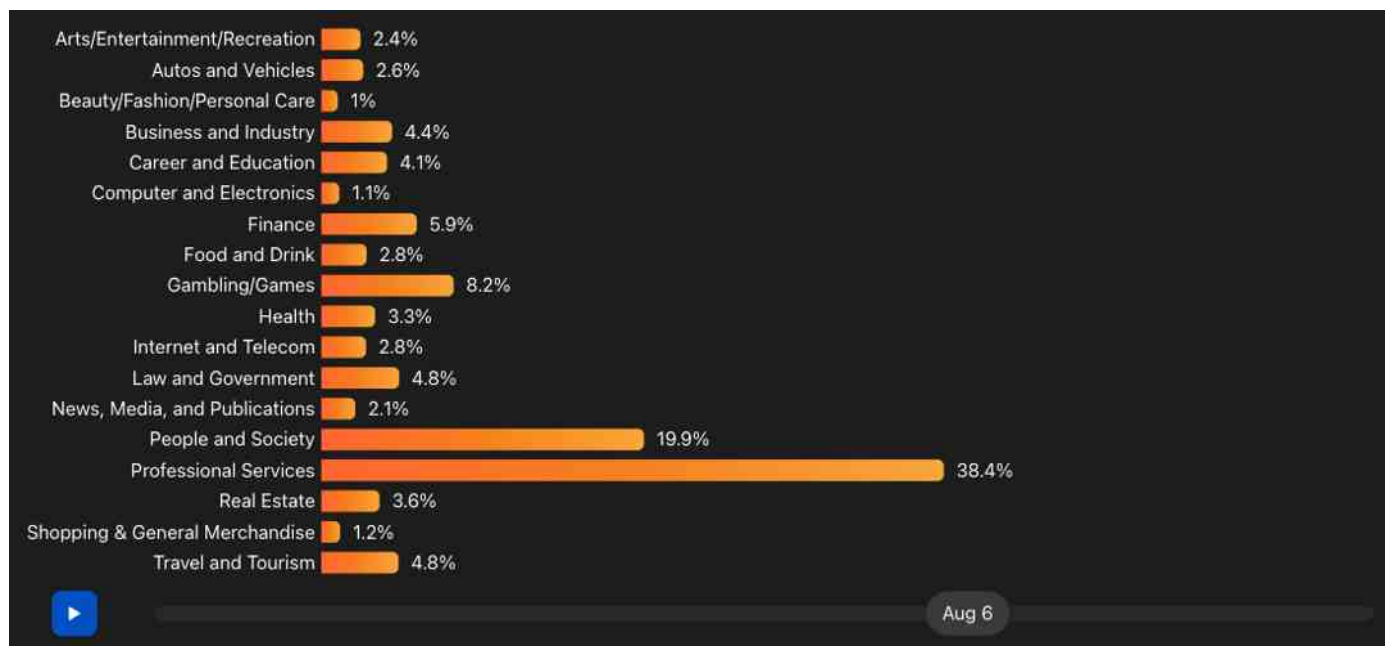
[Globally](#), nearly 12% of bot traffic comes from Amazon Web Services, and over 7% from Google. Some of it comes from consumer ISPs as well, with U.S. broadband provider Comcast originating over 1.5% of global bot traffic. A disproportionate amount of bot traffic originates from the United States,

The industries targeted by attacks often shift over time, depending on the intent of the attackers. They may be trying to cause financial harm by attacking ecommerce sites during a busy shopping period, or they may be trying to make a political statement by attacking government-related sites. To identify industry-targeted attack activity during 2023, we analyzed mitigated traffic for customers that had an associated industry and vertical within their customer record. Mitigated traffic was aggregated weekly by source country/region across 18 target industries.

At a [global level](#), Finance organizations were the most attacked over the course of the year, though we saw a significant amount of volatility from week-to-week. Interestingly, some clustering was evident, as Finance, which includes organizations that provide websites and applications for mobile payments, investments/trading, and cryptocurrency, was also a top target for a number of European countries, including [Austria](#), [Switzerland](#), [France](#), [the United Kingdom](#), [Ireland](#), [Italy](#), and [the Netherlands](#), as well as in North America, for [Canada](#), [the United States](#), and [Mexico](#). The Health industry, which includes companies that make exercise equipment, as well medical testing device manufacturers, was a top target across multiple African countries, including [Benin](#), [Côte d'Ivoire](#), [Cameroon](#), [Ethiopia](#), [Senegal](#), and [Somalia](#).

Overall, however, the year started slowly, with no industry seeing more than 8% of traffic being mitigated. As the first quarter progressed, Professional Services and News/Media/Publications organizations saw spikes in the share of mitigated traffic later in January, with Health jumping in mid-February and Law & Government organizations seeing a sharp increase in mitigated traffic in early March. Customers in the Arts/Entertainment/Recreation industry classification were apparently targeted by a multi-week attack campaign, with more than 20% of traffic mitigated during the weeks of March 26, April 2, and April 9. The overall peak during the year was experienced by the Professional Services industry, which saw a mitigated traffic share of 38.4% for the week

of August 6, nearly twice its January spike. The timing of spikes and the industries experiencing those spikes varied widely across countries/regions.



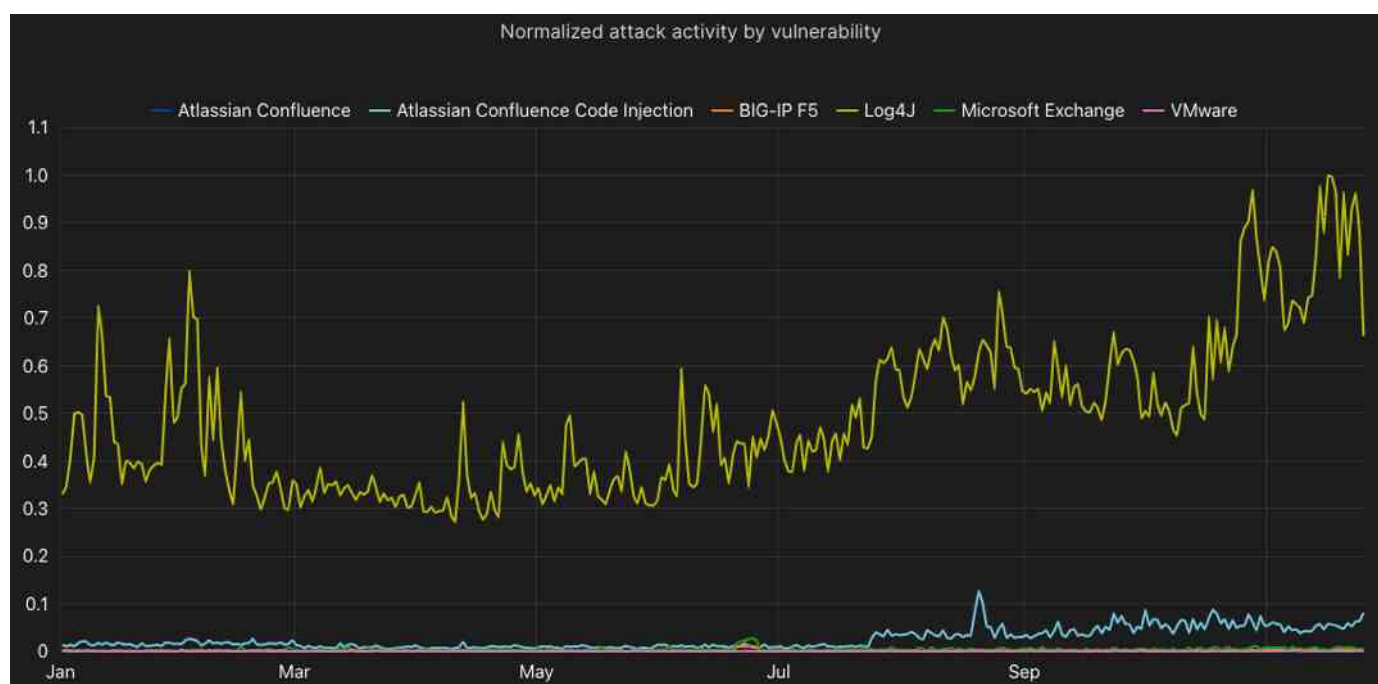
Global mitigated traffic share by industry, week of August 6, 2023

Even as an older vulnerability, Log4j remained a top target for attacks during 2023. However, HTTP/2 Rapid Reset emerged as a significant new vulnerability, beginning with a flurry of record-breaking attacks.

In August 2023, we published a [blog post](#) that explored traffic seen by Cloudflare for the most commonly exploited vulnerabilities of 2022, as listed in a [joint Cybersecurity Advisory](#). These included vulnerabilities in the Log4j Java-based logging utility, Microsoft Exchange, Atlassian's Confluence platform, VMWare, and F5's BIG-IP traffic management system. Although these are older vulnerabilities, attackers continued to actively target and exploit them throughout 2023, in part because organizations are frequently slow to follow the recommendations outlined in the Cybersecurity Advisory. We updated the analysis done for our blog post to include just the attack activity seen in 2023.

Attack activity by vulnerability varied by location, and in some, attacks targeted only a subset of the vulnerabilities. [Aggregated worldwide](#), attack

volume targeting Log4j consistently dwarfed that seen for the other vulnerabilities, and saw spikes during the last week of October and mid-late November; attack activity targeting Atlassian vulnerabilities increased in late July and trended slowly higher through the rest of the year. At a country/region level, Log4j was generally the most targeted vulnerability. In countries including [France](#), [Germany](#), [India](#), and the [United States](#), associated attack volume remained at a significant level throughout the year, while in other countries/regions, these attacks are most visible as infrequent, short-lived spikes within a country/region's graphs, punctuating otherwise low levels of attack volume.

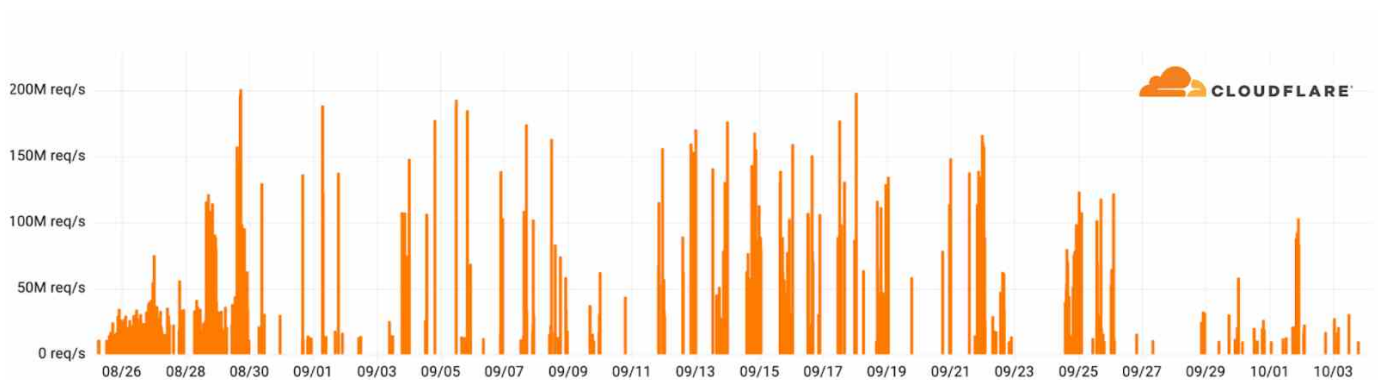


Global attack activity trends for commonly exploited vulnerabilities

We also expect that through 2024, attackers will continue to target the [HTTP/2 Rapid Reset](#) vulnerability disclosed in October. The vulnerability (see [CVE-2023-44487](#) for details) abuses an underlying weakness in the request cancellation feature of the HTTP/2 protocol, leading to resource exhaustion on the target web/proxy server. Between the end of August and the beginning of October, we saw a number of attacks targeting this vulnerability. Across this set of attacks, the average attack rate was 30M requests per second (rps), with nearly 90 peaking above 100M rps, and the largest one hitting

201M rps. This largest attack was nearly 3x bigger than our [previous biggest attack on record](#).

One notable concern about this vulnerability is that the attacker was able to generate such a large attack with a botnet consisting of just 20,000 compromised systems. This is much smaller than some of the largest botnets today, which comprise hundreds of thousands or millions of hosts. With average web traffic estimated to be between 1–3 billion requests per second, attacks using this method could conceivably focus an entire web's worth of requests on a few unsuspecting targets.



HTTP/2 Rapid Reset campaign of hyper-volumetric DDoS attacks

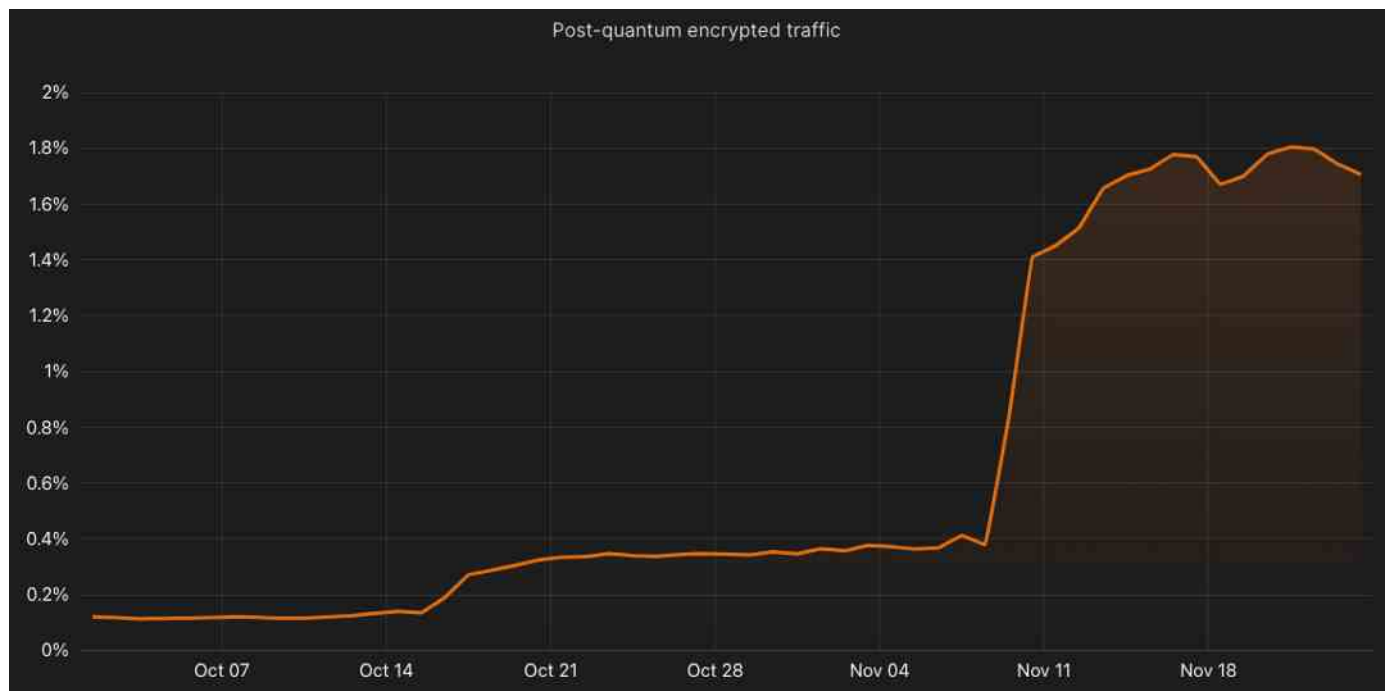
1.7% of TLS 1.3 traffic is using post-quantum encryption

[Post-quantum](#) refers to a new set of cryptographic techniques that can protect data from adversaries with the ability to capture and store today's data for decryption by sufficiently powerful quantum computers in the future. The Cloudflare Research team has been [exploring post-quantum cryptography since 2017](#).

In October 2022, we enabled [post-quantum key agreement](#) at our edge by default, but use of it requires that the browser support it as well. Google's Chrome browser started to slowly enable support in August 2023, and we expect its support will continue to grow in 2024, and that other browsers will add support over time as well. In September 2023, we announced [general](#)

[availability of post-quantum cryptography](#) for both inbound and outbound connections and for many internal services, and expect to finish upgrading all internal services by the end of 2024.

After first enabling support in August, Chrome began ramping the number of browsers (version 116 and later) that use post-quantum cryptography, resulting in gradual growth leading to the significant increase seen on November 8. These actions helped [push the share](#) of TLS 1.3 traffic using post-quantum encryption to 1.7% at the end of November. As this ramp continues with future Chrome updates, and as other browsers add support for post-quantum encryption, we expect this share to continue to grow rapidly in 2024.

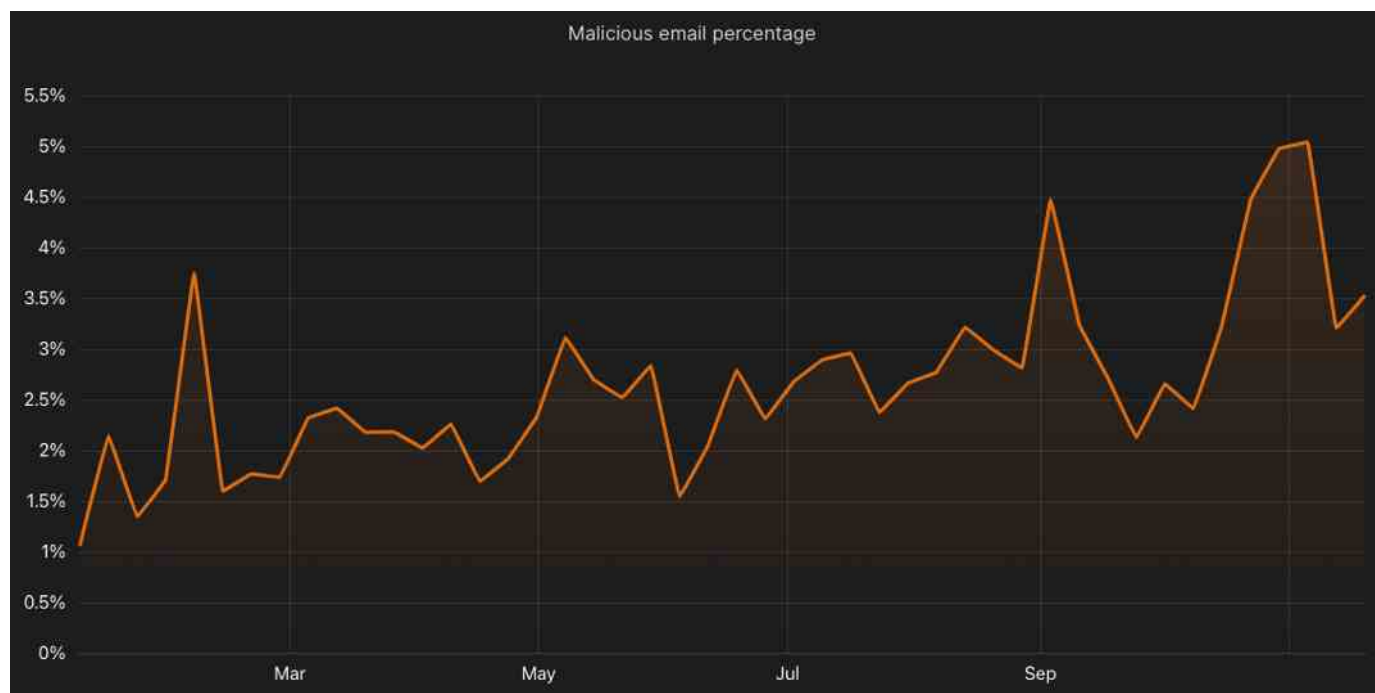


Growth trends in post-quantum encrypted TLS 1.3 traffic

Deceptive links and extortion attempts were two of the most common types of threats found in malicious email messages.

As the #1 business application, email represents a very attractive entry point into enterprise networks for attackers. Targeted malicious emails may attempt to impersonate an otherwise legitimate sender, try to get the user to click on a deceptive link, or contain a dangerous attachment, among other types of

threats. [Cloudflare Area 1 Email Security](#) protects customers from email-based attacks, including those carried out through targeted malicious email messages. [Over the course of 2023](#), an average of 2.65% of emails analyzed by Cloudflare Area 1 were found to be malicious. Aggregated at a weekly level, spikes to over 3.5%, 4.5%, and over 5% were seen in early February, early September, and late October respectively.

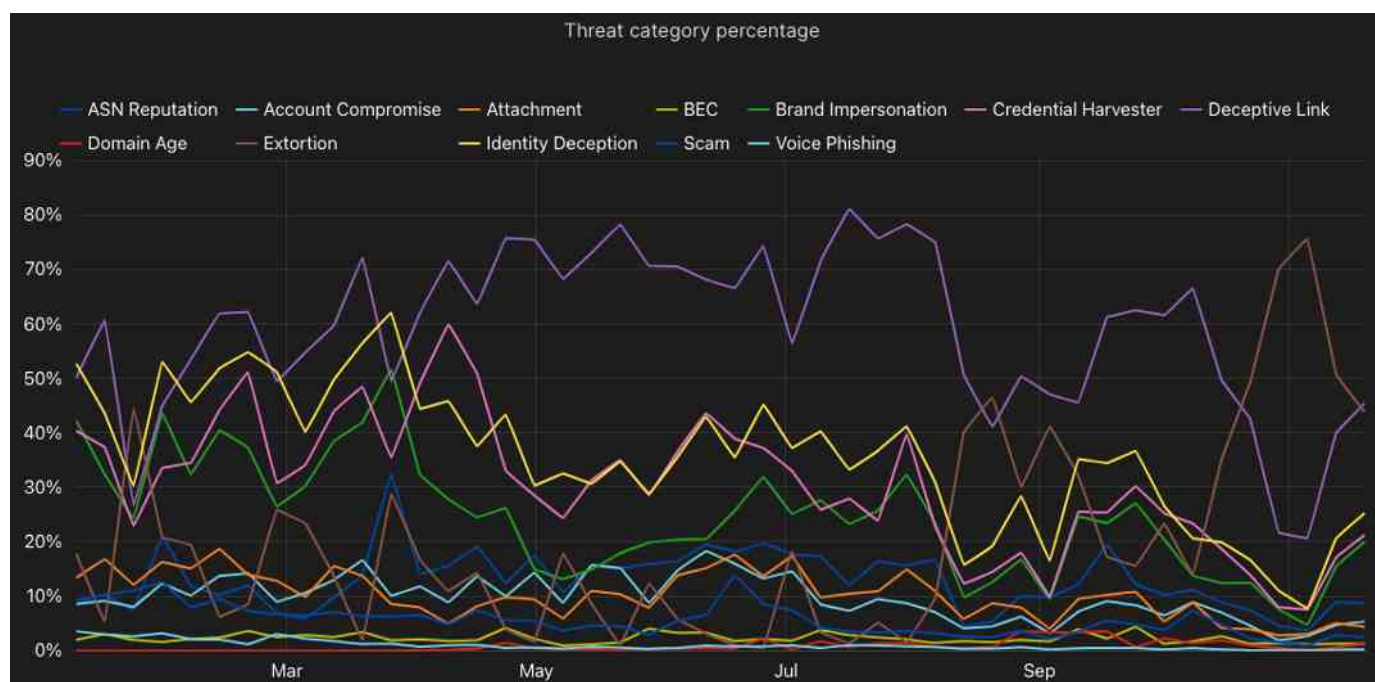


Global malicious email share trends

When carrying out attacks using malicious email messages, attackers use a variety of techniques, which we refer to as threat categories. These categories are defined and explored in detail in Cloudflare's [2023 phishing threats report](#). Analysis of malicious emails shows that messages may contain multiple types of threats, highlighting the need for a comprehensive email security solution. [Exploring threat activity trends for these categories](#), aggregated weekly across the year, we found that as much as 80% of them contained deceptive links.

However, it appears that attackers may have started to shift strategies in August, as the percentage of emails containing deceptive links began to fall while the share proposing to extort the recipient began to increase. By the end of October, and into November, the two threat categories had traded

places, with nearly 80% of analyzed malicious emails containing an extortion threat, while only 20% contained deceptive links, as seen towards the right side of the graph below. However, this extortion campaign may have been short-lived, as its percentage fell almost as quickly as it rose. Identity deception and credential harvesting were also commonly identified threats, though the share of emails they were found in gradually declined over the course of the year.



Global threat category trends for malicious emails

Routing security, measured as the share of RPKI valid routes, improved globally during 2023. Significant growth was observed in countries including Saudi Arabia, the United Arab Emirates, and Vietnam.

[Border Gateway Protocol \(BGP\)](#) is the routing protocol for the Internet, communicating routes between networks, enabling traffic to flow between source and destination. However, because it relies on trust between networks, incorrect information shared between peers, whether done so intentionally or not, can send traffic to the wrong place, potentially with [malicious results](#). [Resource Public Key Infrastructure \(RPKI\)](#) is a cryptographic method of signing records that associate a BGP route

announcement with the correct originating AS number. In simple terms, it provides a way of ensuring that the information being shared originally came from a network that is allowed to do so. (Note that this is only half of the challenge of implementing routing security, as network providers also need to validate these signatures and filter out invalid announcements.) In the United States, the federal government recognizes the importance of routing security, with the Federal Communications Commission holding a [“Border Gateway Protocol Security Workshop”](#) on July 31.

Cloudflare has been a strong proponent of routing security, from being a founding participant in the [MANRS CDN and Cloud Programme](#), to releasing an [RPKI toolkit](#) for network operators, to providing a [public tool](#) that enables users to test whether their Internet provider has implemented BGP safely, to presenting at this summer’s FCC workshop.

Building on the [July release](#) of the new [Routing page](#) on Cloudflare Radar, we analyzed data from [RIPE NCC's RPKI daily archive](#) to determine the share of RPKI valid routes (as opposed to those route announcements that are invalid or whose status is unknown) and how that share has changed over the course of 2023. Since the start of the year, the [global share of RPKI valid routes](#) grew to nearly 45%, up six percentage points from the end of 2022. At a country/region level, we are looking at routes announced by autonomous systems associated with the given country/region. In the [United States](#), the increased FCC attention on routing security is arguably warranted, as less than a third of the routes are RPKI valid. Although this is significantly better than [South Korea](#), where less than 1% of announced routes are RPKI valid, it trails [Vietnam](#) significantly, where the share increased 35 percentage points during the first half of the year to 90%.



RPKI valid route growth in Vietnam

Conclusion

In the [Cloudflare Radar 2023 Year In Review](#), we have attempted to provide a snapshot of the Internet, as dynamic as it is, through trend graphs and summary statistics, providing unique perspectives on Internet traffic, Internet quality, and Internet security, and how key metrics across these areas vary around the world.

As we said in the introduction, we strongly encourage you to visit the [Cloudflare Radar 2023 Year In Review website](#) and explore the trends relevant to metrics, countries/regions, and industries of interest, and to consider how they impact your organization so that you are appropriately prepared for 2024.

If you have any questions, you can contact the Cloudflare Radar team at radar@cloudflare.com or on social media at [@CloudflareRadar](#) (X/Twitter), [cloudflare.social/@radar](#) (Mastodon), and radar.cloudflare.com (Bluesky).

Acknowledgements

As we noted last year, it truly is a team effort to produce the data, website, and content for our annual Year in Review, and I'd like to acknowledge those

team members that contributed to this year's effort. Thank you to: Sabina Zejnilovic, Jorge Pacheco, Carlos Azevedo (Data Science); Arun Chintalapati, Reza Mohammady (Design); Vasco Asturiano, Nuno Pereira, Tiago Dias (Front End Development); João Tomé (Most popular Internet services); and Davide Marquês, Paula Tavares, Celso Martinho (Project/Engineering Management) as well as countless other colleagues for their answers, edits, and ideas.

We protect [entire corporate networks](#), help customers build [Internet-scale applications efficiently](#), accelerate any [website or Internet application](#), [ward off DDoS attacks](#), keep [hackers at bay](#), and can help you on [your journey to Zero Trust](#).

Visit [1.1.1.1](#) from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, [start here](#). If you're looking for a new career direction, check out [our open positions](#).

ON AIR | **CLOUDFLARE TV**

Radar Bulletin: 2023 Year in Review

Tune In



Year in Review

Cloudflare Radar

Trends

Internet Traffic

Outage

Follow on X

David Belson | [@dbelson](#)