2025 Report

Ad-Shield

Adblocking:
The Rise of Dark Traffic

Introduction

Welcome to adblocking 2.0

Ad-Shield

Need to know

A new generation of adblockers has cut off nearly 1 billion users from publishers and advertisers. Their visits go unmeasured. Their content consumption, unmonetized.

This marks a dramatic shift from legacy adblockers, which allowed measurement and monetization. Today's new-gen users outnumber them 3.8X, growing 13% year-on-year — posing a direct threat to publisher business models.

This ecosystem shake-up has gone unnoticed by the industry. Blocked measurement tools have concealed its users from view in dashboards. Until now.

We call this hidden audience **dark traffic**.

Dustin Cha
Co-founder and Co-CEO

Ad-Shield

Dark traffic — key insights

- **976M Internet users are dark traffic.** This represents 18% of total web traffic. 49% growth in 3 years.
- **57% did not choose to adblock.** It's activated by a third-party, such as workplace IT departments, security software, public WiFi, and enterprise security providers.
- **It's revenue blocking, not just adblocking.** Analytics, adblock walls, cookie banners, regwalls, paywalls, affiliate links, and subscribe pop ups also get blocked.
- **Dark traffic is 53% mobile.** Attracting mainstream audiences in US, UK, Germany, France, and Canada.
- **Traditional adblock recovery tools fail.** Acceptable Ads & adblock walls are not compatible.

What is dark traffic?

Ad-Shield

There are two types of adblocking traffic: “gray” and “dark”

Not all adblocking traffic is the same. We have identified two distinct categories, based upon the effects they have on open web publishers.

Adblocking traffic

	Gray traffic	Dark traffic
On-site analytics *(e.g. Google Analytics)*	✓	✗
Whitelisted ads *(e.g. Acceptable Ads)*	✓	✗
Adblock walls *(e.g. Funding Choices)*	✓	✗
Cookie consent *(e.g. OneTrust)*	✓	✗
Regwalls & paywalls	✓	✗

✓ Allowed ✗ Blocked

Brutal adblockers are the cause of dark traffic

Ad-Shield

They represent a new generation of adblockers — redefining the terms with publishers

Adblockers fall into two distinct categories: **“soft adblockers”** and **“brutal adblockers”.**

Soft adblockers

Cause gray traffic

Soft adblockers were first to introduce adblocking to a mainstream audience. Examples are AdBlock and Adblock Plus.

They are “soft” because they allow publishers measurement and monetization capabilities:

- ✓ On-site analytics
- ✓ Whitelisted ads
- ✓ Adblock walls
- ✓ Cookie consent
- ✓ Regwalls & paywalls

Brutal adblockers

Cause dark traffic

Brutal adblockers emerged after soft adblockers had already gained popularity. Their usage grew through bundling with other products, default opt-ins via networks and IT security setups, and aggressive ‘block-everything’ philosophies.

They are “brutal” because they deny publishers measurement and monetization capabilities:

- ✕ On-site analytics
- ✕ Whitelisted ads
- ✕ Adblock walls
- ✕ Cookie consent
- ✕ Regwalls & paywalls

Surfshark®

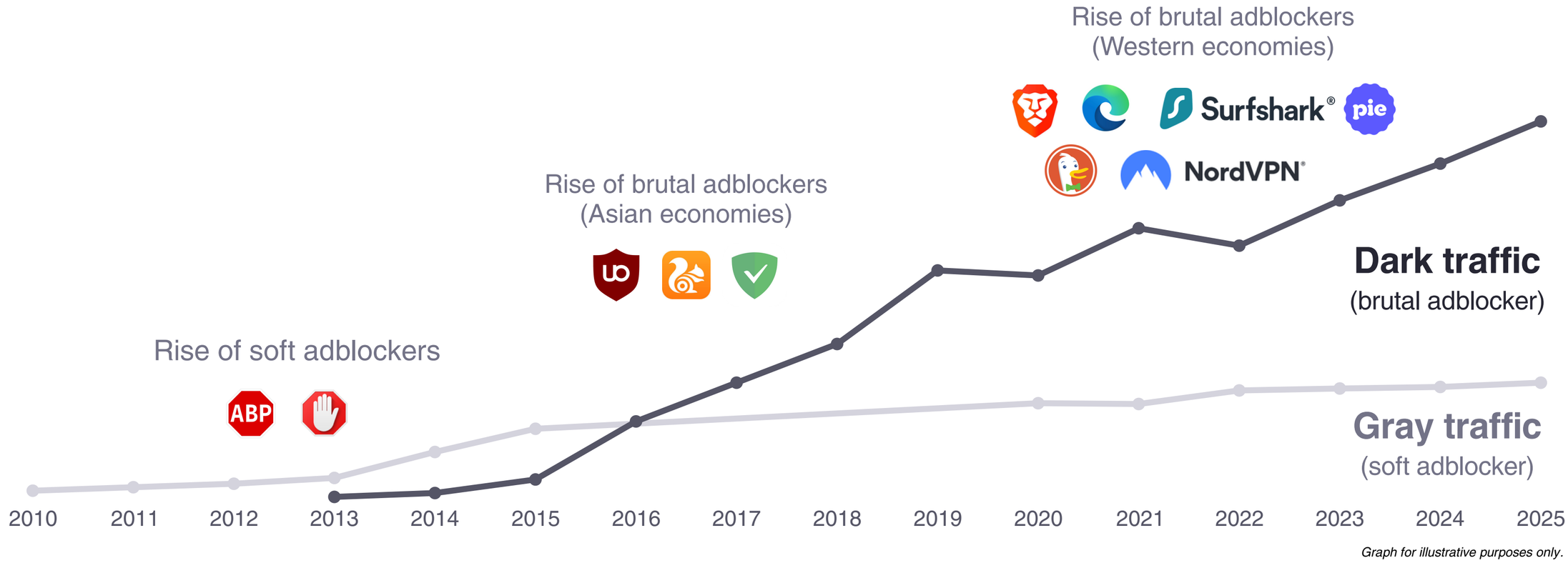
NordVPN®

The rise of brutal adblockers

Ad-Shield

It has gone unnoticed, because it doesn’t show up in dashboards

Adblocker user growth



Graph for illustrative purposes only.

💡 Between 2015 and 2020, uptake of brutal adblockers was strongest in mobile-first, high-population markets across Asia. Since 2020, growth has shifted to Western economies — introducing new challenges for publisher monetization, user visibility, and engagement strategies.

Defining dark traffic

Ad-Shield

Dark traffic used to mean “no referrer”. Now it means “no audience”.

2012: The origin of dark traffic

“Traffic with no clear referral source”

Back in 2012, the term “dark traffic” was adopted by webmasters and analytics professionals to describe visits to websites with no attributed referral source. This audience segment appeared as “direct” traffic in analytics dashboards, which masked their origin.

Fast forward to 2025, and that definition is no longer sufficient. Publishers face something worse: traffic that isn’t just unattributed — it’s undetectable and unmonetizeable.

This is a blind spot at the core of the digital publishing model, created by the spread of a new generation of adblockers.

2025: Dark traffic today

“Undetectable and unmonetizeable traffic”

We believe the definition of dark traffic must evolve to match the circumstances presently facing publishers.

Therefore, we are using the following working definition:

Definition of “dark traffic”

When a user visits a website and any of the below occur:

- ✕ Site analytics is blocked (not measured in dashboard)
- ✕ Ads are blocked without option to replace with whitelisted ads (e.g. Acceptable Ads)
- ✕ Adblock wall or user messaging is blocked

Dark traffic is costing publishers 18% of their revenue

The new adblocking landscape

Ad-Shield

Publishers face a fragmented ecosystem of brutal adblockers

Adblocking is no longer primarily driven by browser extensions on Chrome and Firefox.

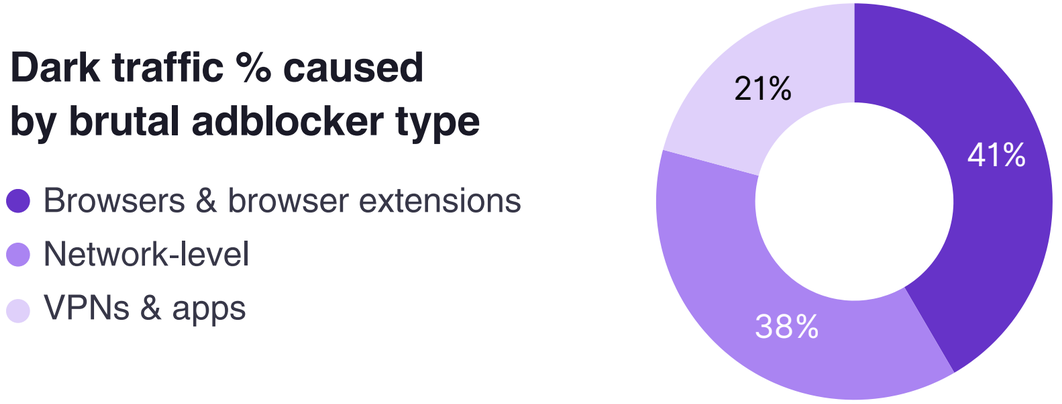
It has expanded across a wide range of products and services, which have proven highly effective distribution channels for brutal adblockers.

Key examples include:

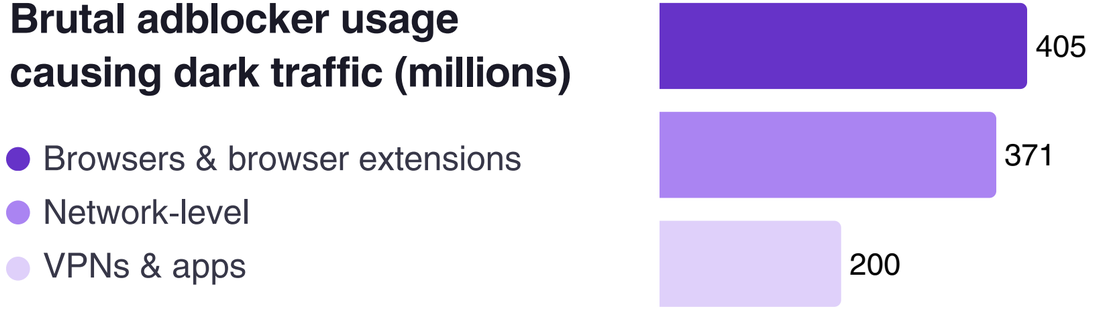
- Apps
- Bundled with VPNs
- Built into browsers
- Network-level integration
  - Workplaces, organizations, and public WiFi

The rise of these new adblocking technologies has exposed a weakness in traditional adblock recovery solutions: they are incompatible with them. To address dark traffic, publishers need a new approach.

Dark traffic % caused by brutal adblocker type



Brutal adblocker usage causing dark traffic (millions)



59% of dark traffic isn’t caused by browsers

Brutal adblocker marketplace

Ad-Shield

Products that cause dark traffic

Cross-platform

GHOSTERY
ADGUARD
AdBlocker ULTIMATE
BLOKADA
AdLock

Browsers (built-in)

brave
Aloha
VIVALDI
DuckDuckGo
Microsoft Edge
NAVER whale
vivo
Gener8 Browser

VPNs

NordVPN
Surfshark
Proton VPN
CyberGhost
ExpressVPN

Browser extensions

Poper Blocker
uBlock Origin
Stands FREE ADBLOCKER
pie
uBlock
Malwarebytes
TOTAL Adblock

Apps

AdBlock Pro
SEVEN AdClear
norton

Network-level

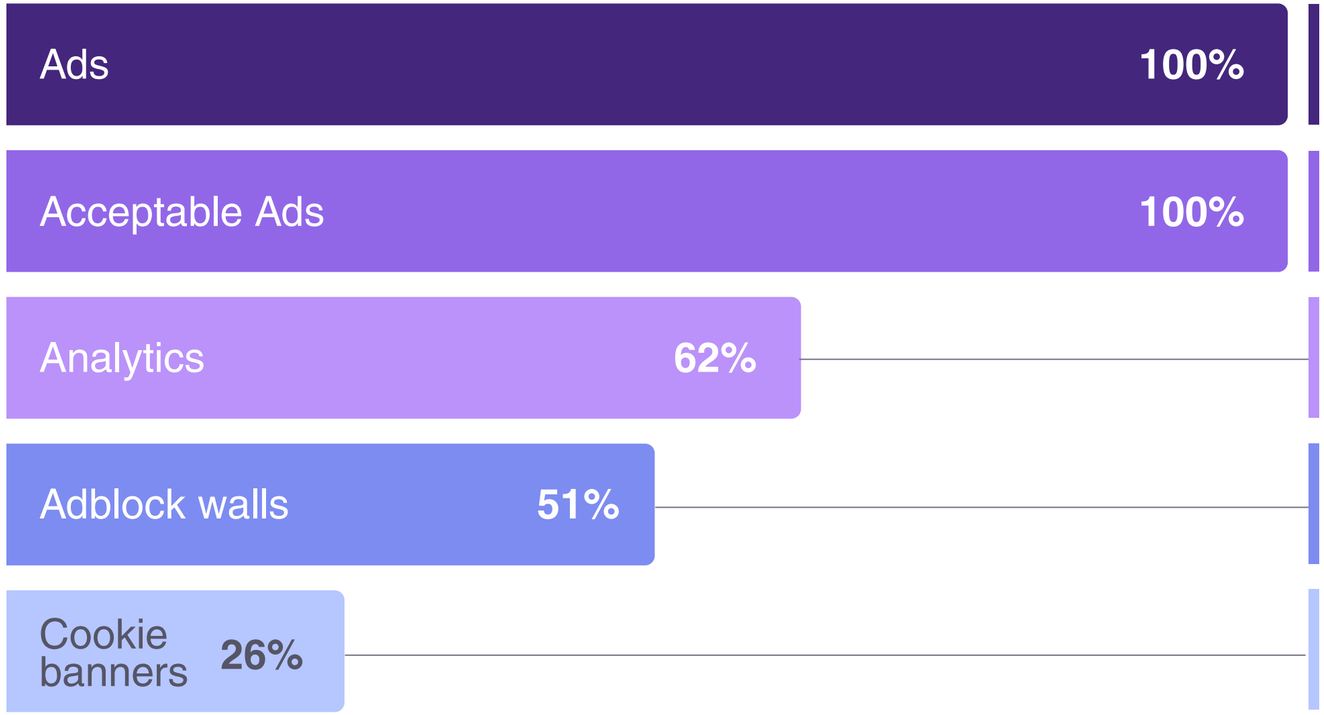
NextDNS
Pi-hole
ADGUARD DNS
CONTROL D

What’s getting blocked

Revenue-linked features are the primary target

Brutal adblockers cut off the entire measurement and monetization stack. This includes removing traditional adblock recovery mechanisms.

% of dark traffic page views that blocked each type



Ads, and their associated 3rd-party tracking, are consistently blocked.

Brutal adblockers do not participate in whitelisted ads programs. The most prominent, Acceptable Ads, receives 0% ad impressions from dark traffic.

The majority of dark traffic blocks analytics tools, such as Google Analytics. It does not show up in dashboards.

Attempts to detect or convert adblock users with messaging are disabled, deactivating this recovery mechanism.

CMPs (consent-management platforms) are blocked or auto-filled with minimal permissions given (‘reject all cookies’).

💡 Regwalls, paywalls, affiliate links, and subscribe pop ups also get blocked. Measuring the prevalence of this fell outside the defined scope of this study, but it is worthy of future investigation.

Note: We used a representative proxy to measure the blocking rate of analytics, adblock walls, and cookie banners (see methodology).

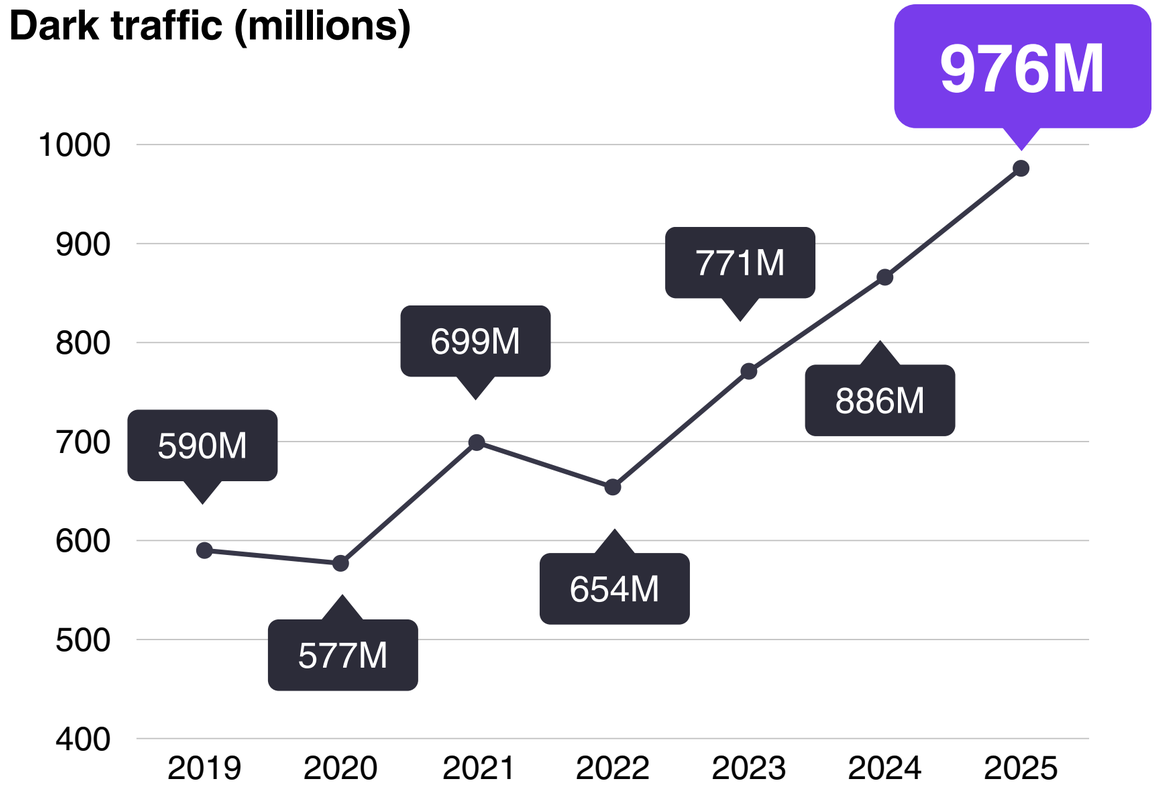
Dark traffic growth

It’s grown 49% in the past 3 years, out of view

There are now **976M brutal adblocker** users that cause dark traffic — growing **14% per year.**

- **79% of adblocking traffic is dark traffic**
- **18% of total traffic is dark traffic**

This growth has largely gone unnoticed, due to the fact it blocks existing measurement technologies.



💡 Brutal adblocker usage started within the developer community around 2014. As the products became more appealing and accessible (auto opt-in) to mainstream audiences, it has experienced an explosion in growth.

Dark traffic will hit 1.1BN in 2026

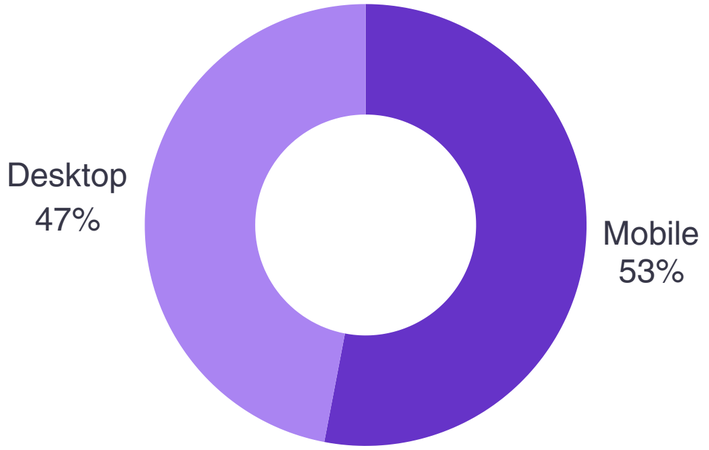
Users by device type

Dark traffic is 53% mobile

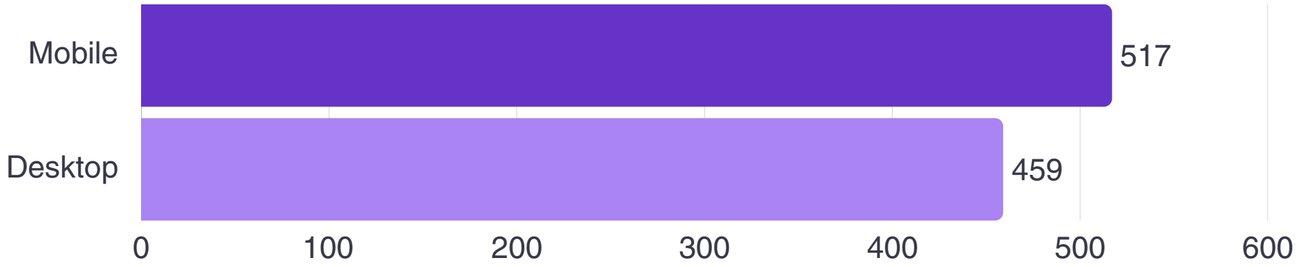
- **Key drivers of dark traffic growth:** mobile web browsers that block ads by default, network-level adblocking, extensions, apps, and VPNs that block ads
- Brave’s mobile browser has been downloaded 100M+ times. DuckDuckGo’s mobile browser has been dowloaded 50M+ times
- Network-level adblocking has 370m+ users
  - Connected mobile devices auto-block ads
  - Affects workplaces, public WiFi, etc

💡 Dark traffic began as a desktop phenomenon with tech-minded early adopters (e.g. uBlock Origin). It has transformed to become mobile-dominant.

Dark traffic by device (%)



Dark traffic by device (millions)



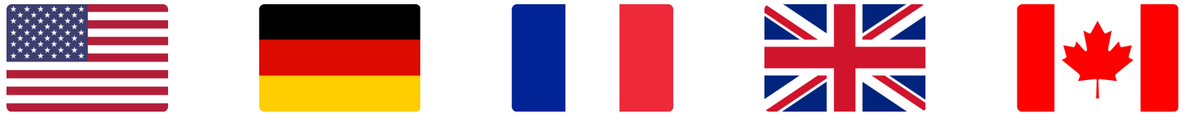
Countries affected

Dark traffic is prevalant in Western economies

- **Around 1 in 5 Internet users in the US, UK, and Canada use brutal adblockers. In France and Germany, it's higher – closer to 1 in 3**
- Cybersecurity policies within organizations and networks is accelerating adoption. The US has been particularly impacted by this.
- GDPR has created a frictional user experience. To remove cookie banners, consumers have responded by seeking out evermore aggressive forms of adblocking.

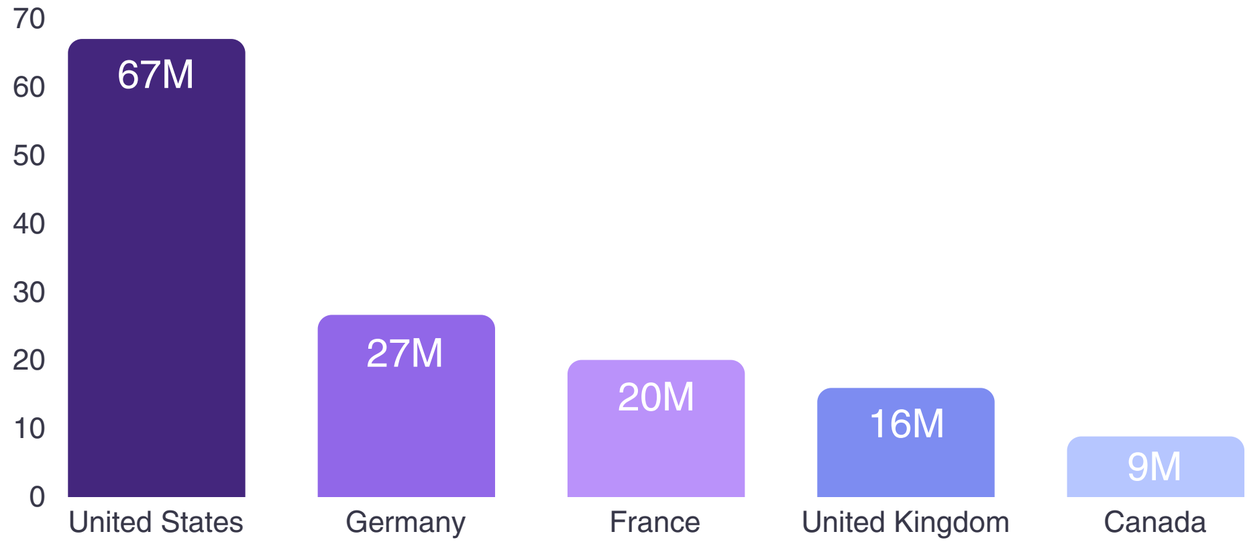
💡 Dark traffic has grown 2–3× faster in Western markets since 2023 — a trend likely fuelled by a news story claiming that the "FBI recommends installing an adblocker."*

% of total traffic that is dark traffic



21%	34%	32%	23%	23%

Dark traffic by country (millions)



*https://www.securityweek.com/fbi-recommends-ad-blockers-cybercriminals-impersonate-brands-search-engine-ads/

Content categories affected

All content categories are impacted, some more than others

The average dark traffic rate across all categories is 18%. Gaming and tech sites face the highest dark traffic exposure, with average rates of 34% and 30%, respectively.

This aligns with historical adblock adoption trends and is influenced by users who actively seek out and install brutal adblockers — typically younger, more technically literate audiences.

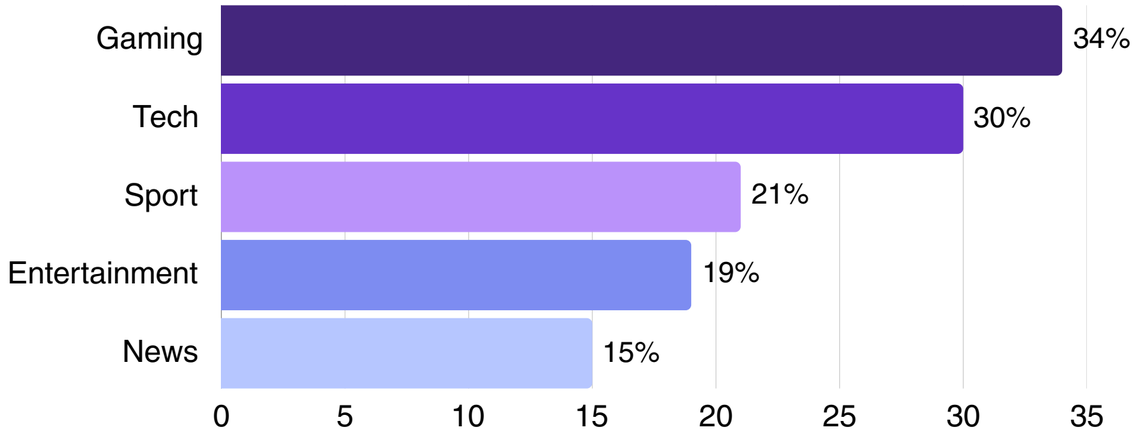
However, this imbalance is restrained by a broader truth: most dark traffic does not stem from conscious user choice.

The majority of users were opted-in without their awareness or decision to do so, suggesting these category differences are significant but not completely reflective of underlying user demographics.

% dark traffic across 5 major categories

18%

Avg. dark traffic (all categories)



Most users don’t know they’re blocking ads

Only 43% made a conscious decision to use a brutal adblocker

Up until now, the adblock recovery narrative has centered on user intent. Respecting the user’s preference to block ads has come first. Dark traffic requires a new perspective. Our research reveals the majority of this traffic had their adblocker activated without their awareness or active consent.

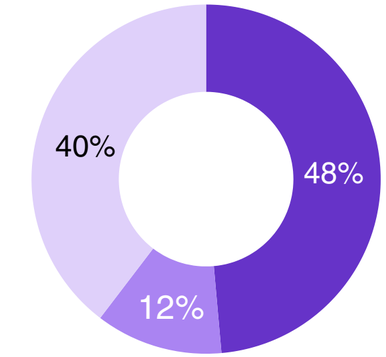
57%

never made the decision to block ads

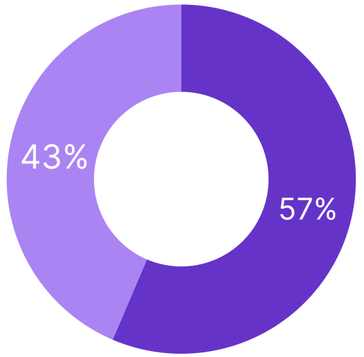
52%

had limited or no awareness they were blocking ads

User awareness they were adblocking



If the user made the decision to adblock



💡 IT managers and cybersecurity products have caused a surge in users being unaware they are using an adblocker (see next slide).

Note: “Didn’t make decision” reflects inferred status. “Made decision” was explicity provided (see methodology)

Why organizations use brutal adblockers

Ad-Shield

They’re converting hundreds of millions of Internet users into dark traffic

As cybersecurity threats from digital advertising increase, organizations are responding by deploying adblocking tools to protect their networks, devices, and users.

This includes companies, government departments, educational institutions, and public WiFi providers — all aiming to reduce exposure to malware, spyware, phishing attempts, and data leakage.

Public endorsements by U.S. government agencies such as the FBI have helped standardize adblocking across both the public and private sectors. What began as a consumer behavior is now becoming ‘best practice’ among IT and security professionals.

In these cases, brutal adblockers are typically preferred over softer alternatives because they’re more effective. These are activated at both the network-level and device-level.

Why people use brutal adblockers

Ad-Shield

Hardline blocking all ads is not the main reason

It’s natural to assume that anyone using a brutal adblocker is a hardline anti-ad fanatic with zero tolerance for ads.
The data from our survey highlights why that assumption is false:

57%

57% didn’t choose to block ads.

It was activated without their awareness or consent. Therefore, they can’t be labelled “anti-ad”.

23%

23% prefer not to see ads.

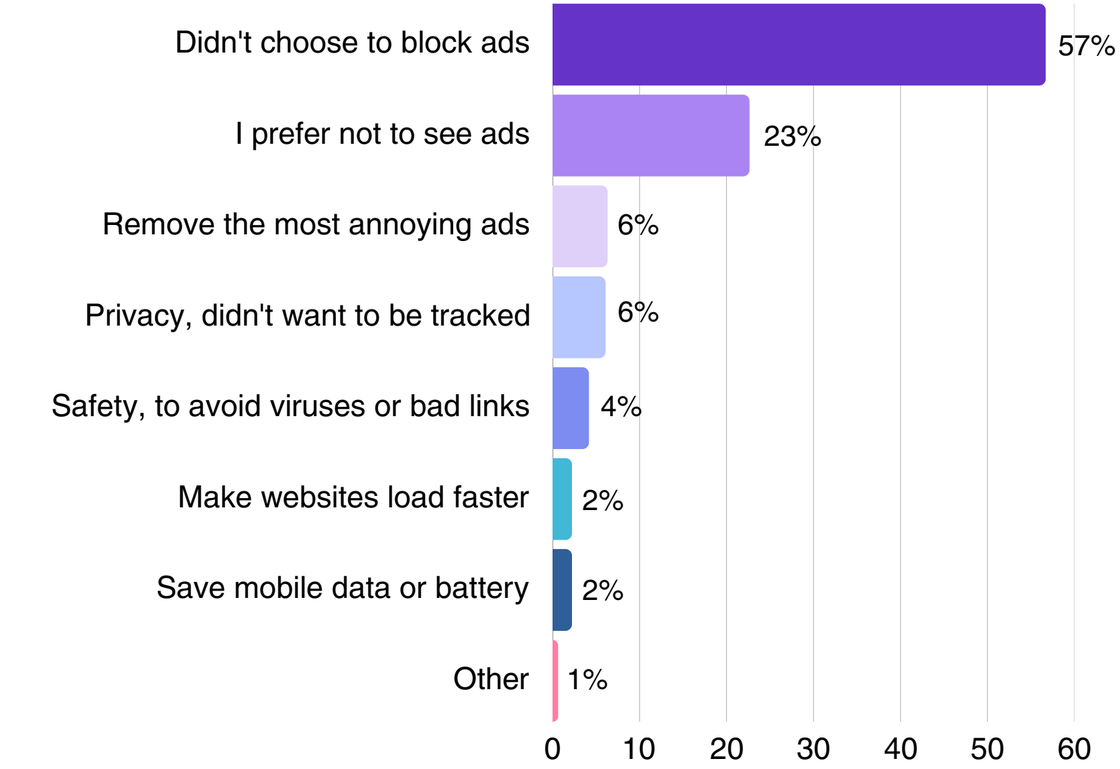
1 in 5 said they would “prefer” not to see ads, which does not mean zero tolerance for all ads in all contexts.

6%

6% to remove the most annoying ads.

1 in 20 want to remove the most annoying ads, signalling they are OK to view certain forms of ads that match their preferences.

Reasons to adblock



Note: “Didn’t choose to block ads” reflects inferred status. All other categories are based on explicit motivations selected by users (see methodology)

Motivating factors for self-activation

Pre-roll ads are a major trigger for seeking out brutal adblockers

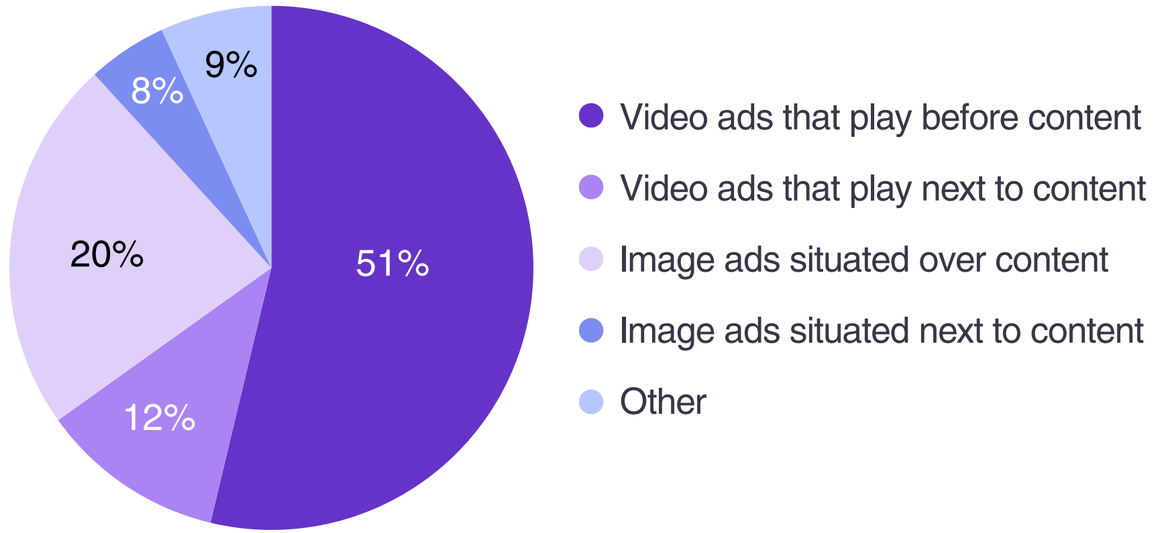
Among the 43% who made the decision to use a brutal adblocker, one adoption trigger stands out: pre-roll video ads.

In our consumer survey:

- 51% of respondents identified pre-roll ads as the most frustrating ad format
- Other disruptive formats included image ad overlays (20%) and video ads alongside content (12%)

💡 Although broad reasons like “I prefer not to see ads” and “Remove the most annoying ads” are cited (which represented 67% of responses in the self-activation segment), the trigger point for action is often a specific frustration — like pre-roll ads.

Question asked: Which of the following types of ads do you find the most disruptive or frustrating?



Avoiding YouTube Ads is a key motivator

How consumers discover brutal adblockers

The most common method is via ads

For the 43% of users who self-activated a brutal adblocker, those who remembered how they found it most often cited:

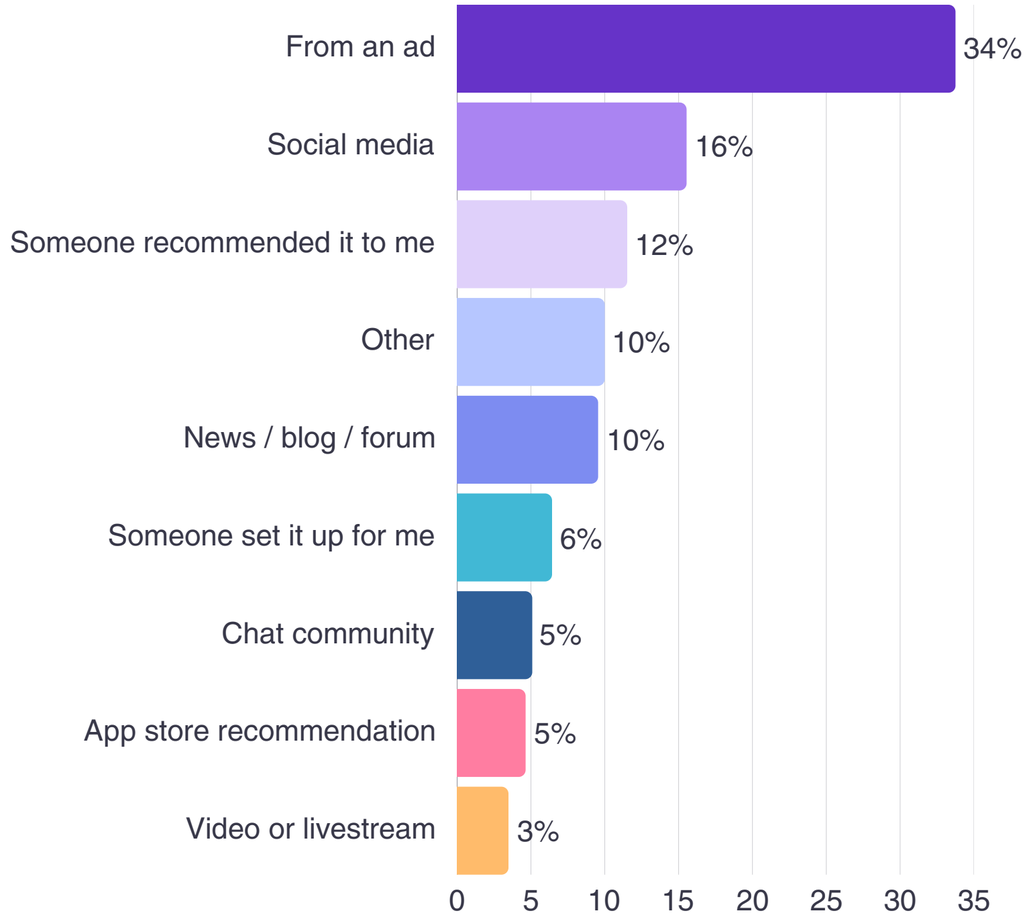
- **34% advertising**
- **31% word of mouth**
- **16% media (including social media)**

These insights align with our ecosystem observations: many adblock developers now market their products aggressively via Google Ads and programmatic placements, reaching users at scale.

For publishers, this underlines the importance of awareness — brutal adblockers are no longer fringe tools. They're mainstream products with real marketing budgets.

Note: 31% of respondents couldn't recall how they found their adblocker. Typically because they've been using it long-term.

Those who could remember



User sentiment towards ads

85% either expect to see ads or find certain types of ads tolerable

What brutal adblockers do — and what their users expect and feel — are two different things.

59%

59% expect to see ads. These users are unaware that adblocking is active, or, they didn't make the choice to block. They therefore expect to see ads.

26%

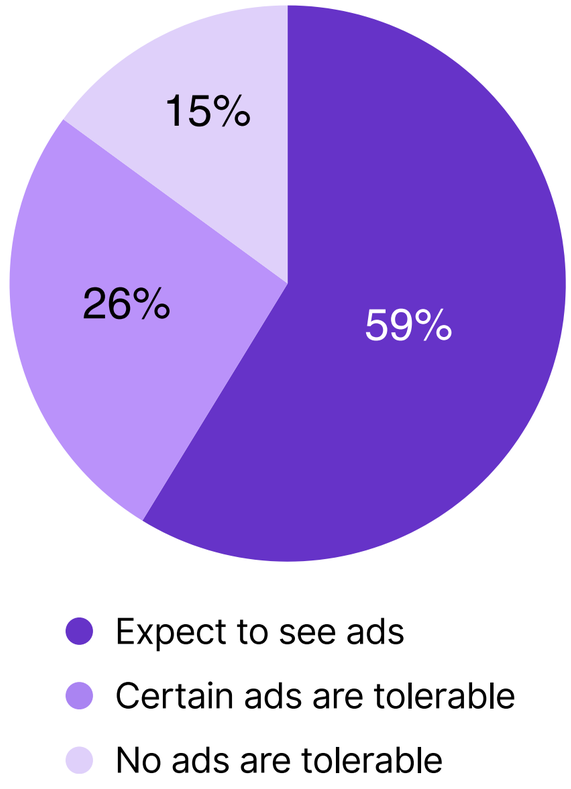
26% find certain ad formats tolerable. 1 in 4 users find certain types of ads tolerable. They are not categorically opposed to ads, just those they deem intolerable.

15%

15% find no ad formats tolerable. A minority of users do not find any advertising experiences tolerable.

💡 Users who self-activate a brutal adbocker often do so with the primary intention of removing YouTube video ads. Brutal adblockers block all ads by default, including ads they may find tolerable.

Attitudes towards ads



Note: The 85% figure includes respondents who were unaware they were blocking ads, from which it was inferred they expect to see ads. Other answers were directly provided by respondents (see methodology)

Who are the end users?

Ad-Shield

Dark traffic skews male and is broadly distributed across age groups

Dark traffic is spread across age groups, unlike traditional adblock users — who are typically younger and more tech-aware.

This reflects a key distinction: most dark traffic didn't actively install a brutal adblocker. It was done for them.

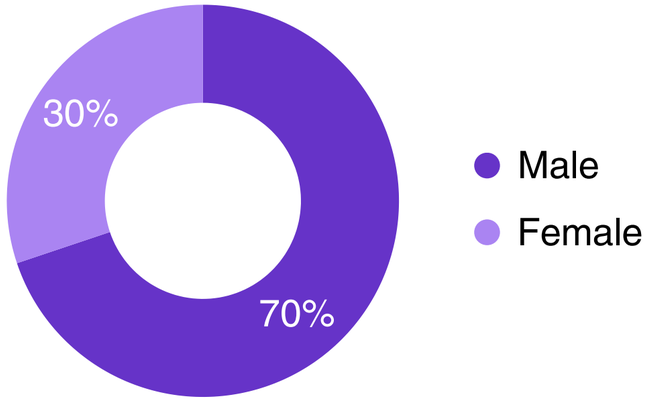
In contrast, users who self-activate a brutal adblocker tend to be younger, reinforcing the divide between active and passive adoption.

However, a skew remains: nearly 70% are male, hinting that brutal adblockers may be more common in male-heavy organizations with active adblocking cybersecurity policies. This warrants further investigation.

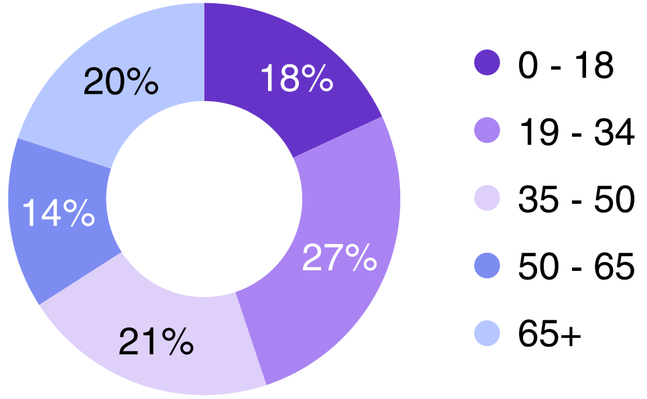
Key findings:

- 70% male
- 45% are under the age of 35
- Age distribution is more balanced than with soft adblockers

Sex



Age group



45% under age 35

Analysis

Ad-Shield

“

Dark traffic represents one of those industry shifts that's been happening quietly while we've all been focused elsewhere.

What's clear is the causes behind ad blocking have become fragmented. It’s no longer purely user driven. This requires a fresh and thoughtful approach.

Given the scale of what this report presents, even solving parts of this puzzle could meaningfully impact publisher economics.

Paul Bannister

CSO, Raptive

“

Brutal ad blockers don’t just cut into publisher ad revenue; they can also degrade the consumer experience by blocking important functionality like analytics and consent tools.

Publishers should have the ability to build trusted, informed relationships with their audiences.

Partners like Ad-Shield help restore these critical insights, enabling publishers to better understand their audiences and improve their properties over time.

Jason Cicchetti

General Counsel and Head of Exchange Quality, Index Exchange

Analysis

Ad-Shield

“

As an industry, we’ve known about ad blocking for a long time. This report changes how we should think about it.

The growth of dark traffic undermines the ability of publishers to fund the production of quality content, or even operate as a business. We must recognize users are not the main driver causing this.

At Freestar, these findings are informing our approach to restoring both audience visibility and revenue recovery for this table-stakes segment.

Heather Carver
CRO, Freestar

“

Dark traffic is unlike anything we have seen before. It’s demonetizing publisher content – at scale – without user consent.

Publishers already face an existential-level threat in the face of AI reducing referral traffic. This is another slice that publishers cannot afford to lose.

Recovering dark traffic is now a meaningful option withn a publisher’s return-to-growth playbook.

Detecting and measuring is the first step.

Scott Messer
Principal & Founder, Messer Media

Closing Thoughts

Dustin Cha

Co-founder & Co-CEO, Ad-Shield

Email dustin@ad-shield.io
Website www.ad-shield.io

In 2015 the digital industry was taken by surprise. The sudden explosion in adblocker adoption caused widespread panic. “*Is this the end of digital ads!?*”

Fortunately, that didn’t happen. In the years that followed, adblocking growth in Western economies tailed off. It didn’t make the jump to mobile.

But now, things have changed. Adblockers are back in a new aggressive form. They’re stronger and more numerous than they ever were. They’re mobile. And, it’s all happening under the radar, in the form of dark traffic.

The purpose of this report is not to scaremonger. It’s a wake up call. Very soon, 1 billion users will be dark to measurement and monetization. We invite you to join us in bringing this audience back into the light. To discuss how we can do this together, please feel free to get in touch.

Dustin Cha

Methodology

Data sources and approach

This report draws on a multi-method research framework combining direct measurement, consumer insights, and third-party data to present a comprehensive view of dark traffic and adblocking trends.

- **On-site measurement**: Ad-Shield's proprietary adblocker detection technology was deployed across a diverse network of publisher sites, capturing anonymized visitor data from 5BN+ page views.

- **Consumer survey:** To complement on-site data, we conducted an independent survey with 2,616 respondents who were using brutal adblockers at the time, and therefore constituted dark traffic.

- **Third-party datasets:** Where historical or global baseline figures were required, we integrated data from credible external sources — including industry reports from Eyeo, Blockthrough, and PageFair, as well as publicly available datasets from Statista, GWI, and the ITU. These were adjusted using Ad-Shield's observed ratios and multipliers to reflect current realities more accurately.

Together, these data sources provide both breadth and depth: measuring the scale of the problem and diagnosing its underlying drivers.

Dark traffic users

Ad-Shield began testing its adblocker detection technology in 2023. While we started capturing data that year, the volume collected during the beta phase was not large enough to serve as a statistically reliable foundation for historical modelling.

Therefore, to estimate the number of dark traffic users from 2019 to 2023, we used a hybrid approach that combined publicly available industry data with Ad-Shield's internal detection insights from 2024 and 2025.

For baseline figures between 2019 and 2023, we used adblock user estimates from the PageFair Adblock Reports (2020, 2021, 2022) and the 2023 Eyeo Ad-Filtering Report. These sources reflect the most widely referenced and reputed data available at the time. However, these reports primarily focused on traditional adblockers that rely on the EasyList filter and did not fully account for newer forms of blocking that do not. These methods are harder to detect, but make up a significant portion of what we classify as "dark traffic." This fact was acknowledged in the 2021 PageFair report: "*These estimates omit users of adblockers not reliant on the EasyList blocklist; i.e. they do not account for the "dark matter of adblocking"*

In 2023, Eyeo introduced a 20% multiplier to their user estimates in an attempt to account for content blockers, DNS-based tools, and VPN-level adblocking (i.e. dark traffic). However, based on what Ad-Shield observed in the early deployment of our detection technology, particularly in North America and Europe, this adjustment underrepresented the real scale of dark traffic. As a result, we replaced Eyeo's 20% multiplier with a 39% adjustment in our model for 2023, to better reflect the unexpected growth in network-level adblocking and the adoption of more aggressive, harder-to-measure tools during that time period.

For the years 2019 through 2022, we applied lower adjustments, increasing incrementally each year to reflect the gradual rise of brutal adblockers. These adjustments were informed by backward extrapolation from our more complete data set in 2024 and 2025.

Methodology

For example, we applied modest increases in 2019 and 2020, when the prevalence of network-level adblocking was still limited, with progressively larger adjustments in 2021 and 2022 as adoption accelerated. To estimate the actual number of dark traffic users for each year, we applied a dark traffic ratio to the adjusted total number of adblock users. These ratios were derived from anonymized data captured by Ad-Shield's detection technology that was live across a range of publisher websites during 2024 and 2025, extrapolating backwards. In the case of 2023, based on Ad-Shield's extrapolated measurements, we adjusted the total number of adblock users from the 912 million originally reported by Eyeo to 1.056 billion. Applying a dark traffic ratio of 73% to this figure yielded an estimate of 771 million users of brutal adblockers.

This estimate aligns with an independent lens on the same data: subtracting the 307 million users opted into Acceptable Ads (as reported by Eyeo in 2023) from the adjusted total also suggests approximately 749 million users were using brutal adblockers that cause dark traffic.

For 2024, we used consumer research from GlobalWebIndex (GWI) as the base reference, which reported that 21% of users across 60 countries regularly use an adblocker. This figure closely matched what we observed through Ad-Shield's publisher network. We applied the 21% usage rate to the 2024 Internet population figure published by the International Telecommunication Union, which estimated 5.5 billion people online globally. This yielded a total of 1.155 billion adblock users in 2024. Based on measurement data from our detection tools live on our publisher network, we applied a dark traffic ratio of 75%, resulting in an estimate of 866 million dark traffic users for that year.

For 2025, GlobalWebIndex (GWI) was not available. Instead, we used a combination of forward projection through extrapolation, third-party data, and the data collected through Ad-Shield's detection technology. Based on this, we applied a dark traffic ratio of 79% to the 2025 internet population figure published by Statista (a figure from the International Telecommunication Union was not available), which estimated 5.56 billion people online globally. This calculated 976 million brutal adblocker users that cause dark traffic.

Adblocking landscape

To better understand the distribution of brutal adblockers across different implementation types, Ad-Shield conducted an analysis of anonymized dark traffic across 187m page views in our publisher network.

Using our proprietary detection technology, we fingerprinted how adblocking occurred on each page request — not at the level of individual users, but based on observable patterns in how page content was being modified or suppressed. This allowed us to infer the likely type of adblocking tool in use without collecting any personally identifiable information.

We then grouped each instance of adblocking into one of the following categories:

- Browser-based
- Network-level
- VPNs and apps

Methodology

This methodology allowed us to estimate the relative share of each adblocking category with a high degree of confidence across a large, global sample of web traffic. It also highlighted a key structural trend: that dark traffic is no longer dominated by traditional browser extensions, but increasingly driven by infrastructure-level or bundled adblocking tools that fall outside the scope of conventional detection and recovery technologies.

What's getting blocked

To determine which monetization and measurement features are being blocked by brutal adblockers, we analyzed a representative sample of 55.5 million anonymized dark traffic pageviews across Ad-Shield's publisher network. For each pageview, we tested whether a commonly in-use representative proxy for each type of feature was blocked or not.

The following tools were used as representative proxies:

- **Analytics:** Google Analytics
- **Adblock walls:** Funding Choices
- **Cookie banners:** OneTrust
- **Acceptable Ads:** This is not technically "blocked". Instead, brutal adblockers do not subscribe to the Acceptable Ads whitelist, which has the same outcome. As a result, no Acceptable Ads are rendered or monetized, and we categorize this traffic as fully excluded.
- **Ads:** This figure is not a direct measurement but a known behavioral constant: brutal adblockers block all ads and associated third-party tracking by default. Based on established functionality and observed implementation, we treat adblocking on dark traffic as universal. There are a few exceptions — for example, AdGuard allows search ads on Google — but these are outliers that do not materially affect the overall picture for the publishers that are the target of this report.

All figures reflect the percentage of measured dark traffic pageviews where blocking was detected. Further, less than 2% of pageviews were excluded from the sample due to scripts not finishing the request successfully.

Users by device type

To determine the breakdown of dark traffic users by device type, we analyzed anonymized internal data from Ad-Shield's publisher network. This was based on a sample of just under one billion page views recorded across a diverse set of sites using Ad-Shield's adblocker detection technology. For each adblocked visit, we identified the device type — mobile or desktop — using user agent signals and page rendering characteristics. This allowed us to calculate a reliable device ratio specifically for users of brutal adblockers, i.e. those generating dark traffic. We then applied this ratio to our 2025 estimate of total dark traffic users, previously calculated at 976 million.

Users by country

To estimate dark traffic penetration by country, we first measured the percentage of total page views identified as dark traffic across the Ad-Shield network — segmented by country of origin. This was based on anonymized traffic data from publishers using Ad-Shield's detection technology, allowing us to observe the relative share of adblocked traffic on a per-country basis.

We then applied these percentages to each country's total Internet user population to estimate the absolute number of users generating dark traffic.

Methodology

For Internet user counts: We used Statista data for the United States and United Kingdom. For France, Germany, and Spain, we referenced figures published by DataReportal. All figures represent the most recent estimates available at the time of writing, generally reflecting 2024–2025 data.

Categories affected by dark traffic

To analyze dark traffic rates across different content verticals, we grouped publisher domains into five cleaned content categories: Entertainment, Tech, News, Gaming, and Sports.

For each category, we measured the total dark traffic ratio across both desktop and mobile using Ad-Shield's detection technology present on its publisher partner websites. To avoid skewing the results toward high-traffic publishers, we used a flat site-level average. This means each website in a given category was treated equally, regardless of its traffic volume. In effect, every site contributed one data point to the category average, whether it reached 100,000 users or 10 million. This approach helped reduce the influence of large outlier domains and more accurately reflects the *average* dark traffic rate per site within each vertical.

Awareness of blocking ads

To assess how many users knowingly block ads, we conducted a consumer survey that included a series of branching questions across four sequences (A, B1, B2, and C). Each sequence was designed to assess both the user's awareness of adblocking and whether they had personally made the decision to use a brutal adblocker.

For the awareness data shown in this slide, we asked all respondents whether they were aware that ads may not be showing on websites they visit due to adblocking activity. Results showed that:

- 1,312 said they were aware
- 318 were only somewhat aware
- 1,070 said they were not aware at all

To determine how many users had actively chosen to install or use a brutal adblocker, we drew from responses in Sequence B2 — where users explicitly indicated whether they made the decision themselves. 1,097 respondents in B2 said they had made the decision to use an adblocker.

For the remaining groups — A (1,034), C (203), and B1 (187) — we made the determination they did not make the decision to block ads. This combination of 1,424 users either lacked awareness they were blocking ads, or, stated that someone else set it up.

In total, there were 2,521 usable responses.

- Didn't make decision (1,424)
- Made decision (1,097)

Motivating factors for self-activation

To understand what motivates users to actively install brutal adblockers, we asked a targeted subset of respondents to identify the types of ads they found most disruptive or frustrating. This question was posed in Sequence B2 of our consumer survey — the only branch where respondents demonstrated full awareness of adblocking and had made the decision to use a blocker themselves.

Methodology

By isolating this group of 1,086 respondents, we ensured that the responses reflected the preferences and frustrations of users who consciously opted out of ad-supported experiences, rather than those who inherited blockers by default.

How consumers discover brutal adblockers

To understand how users first discovered brutal adblockers, we asked a direct question within our consumer survey: “How did you find out about adblockers?”

This question was presented to respondents in Sequences B1, B2, and C — the only groups that demonstrated awareness of adblocking. In total, 1,616 respondents. We excluded responses from Sequence A, as participants in that group indicated they did not know what an adblocker was and therefore could not reliably answer the discovery question.

Why people use brutal adblockers

To explore the reasons why users block ads, we asked respondents in Sequence B2 — the only group that actively chose to install a brutal adblocker — to identify the most important factor in their decision to block ads. This ensured that we captured the motivations of users who had consciously opted out of advertising, rather than those who inherited blockers passively.

However, since Sequence B2 represents only around 40% of total respondents (1,089 for this question), focusing solely on their answers would present an incomplete view of why brutal adblocking occurs.

To provide a comprehensive picture, we incorporated response data from the remaining sequences (A, B1, and C) — who did not actively choose to block ads — and grouped them under a new category: “Didn’t choose to block ads.” This included users whose blockers were installed by someone else, included by default, or added via network or device settings without their knowledge (1,424 respondents). By combining both segments — those who opted in and those who didn’t — we were able to quantify the broader breakdown of dark traffic motivations across all respondents. In total, there were 2,513 useable responses.

Note: While “Didn’t choose to block ads” is presented alongside explicit user motivations, it is not based on a direct response. Instead, it reflects an inferred status derived from respondents in Sequences A, B1, and C — users who either lacked awareness that adblocking was active, or indicated someone else made the decision for them. This category is included to contextualize the broader drivers of dark traffic, but should not be interpreted as a self-declared reason.

User sentiment towards ads

To assess how brutal adblocker users feel about advertising, we combined data from two parts of our survey.

First, we analysed responses from Sequence B2, which included only those users who were fully aware of adblocking and had made the decision to use a brutal adblocker.

Methodology

In this sequence, we asked: “Which of these ad types do you find tolerable when they show up on websites you like?” Because this question allowed for multiple responses, we treated the 393 users who selected “no ads are tolerable” as a distinct group, assuming that they would not have also marked other formats as tolerable. We then subtracted that figure from the total responses to the question (1,085), resulting in 692 users who found at least some ad formats tolerable.

Second, we aggregated the total number of respondents across Sequences A, B1, and C — those who either did not make the decision to install a brutal adblocker or were unaware one was active. This group, totalling 1,545 users, was determined to expect ads to appear during their web experience. Their unawareness and indecisiveness suggests they had not chosen to block ads and therefore had not explicitly opted out of advertising. In total, there were 2,630 respondents.

Demographics

To understand the demographic profile of users generating dark traffic, we asked all respondents to identify their age bracket and gender as part of the survey.

These questions were posed consistently across all sequences (A, B1, B2, and C), providing a complete sample of 2,621 respondents. Age responses were grouped into five brackets (0–18, 19–34, 35–50, 50–65, and 65+), while gender responses included the options: “Man,” “Woman,” and “Prefer not to say.” All percentages shown in the report are based on respondents who selected either "Man" or "Woman", excluding those who preferred not to say.

Notes

- For the purposes of clarity, we used the “common rounding” convention on all figures. Therefore, if the fractional part is .5 or greater, we rounded up. If it was less than .5, we rounded down. There were a couple of exceptions due to the need to total 100%.

- The figures “Didn’t make decision” (57%), “Didn’t choose to block ads (57%), and “Expect to see ads” (59%) are derived from different sections of the survey, but reflect the same behavioural insight: that the majority of brutal adblocker users did not explicitly opt out of ads. The very small variance between them results from the different sections in the survey where these responses were gathered from.