



MALVERTISING + AD QUALITY INDEX

MAQ INDEX

CONFIENT'S MALVERTISING AND AD QUALITY (MAQ) INDEX IS A QUARTERLY LOOK INTO CREATIVE QUALITY IN DIGITAL ADVERTISING. USING A SAMPLE OF OVER 156 BILLION IMPRESSIONS MONITORED IN REAL TIME.

Q2 2021



INTRO

INTRODUCTION

Confiant's Malvertising and Ad Quality (MAQ) Index (formerly known as the Demand Quality Report) is a quarterly look into creative quality in digital advertising. **Using a sample of over 156 billion impressions monitored in real time in Q2 2021, Confiant is able to answer fundamental questions about the state of creative quality.**

Digital advertising delivers significant value to publishers but also introduces myriad risks related to **security, privacy, and user experience. Malicious, disruptive, and annoying ads degrade user experience and drive adoption of ad blockers.** However, few if any systematic studies have been conducted on the frequency and severity of ad quality issues as experienced by the real victims: end users.

Part of this is due to data issues: it had historically been challenging to estimate impact without client-side instrumentation in place on a large and diverse set of publishers. The advent of Confiant's real-time creative-verification solution in 2017 created a view into the problem and some of the underlying causes for the first time. The MAQ Index, which leverages Confiant's position as the vendor of choice to monitor ad security, quality, and privacy issues, aims to provide a comprehensive view into the creative-quality issues facing the industry.

In September 2018, Confiant released the industry's first benchmark report. This report, the thirteenth in the series, covers Q2 2021.



DEFINITIONS

QUALITY VIOLATIONS

Non-security issues related to ad behavior, technical characteristics, or content. Top issues include:

- Heavy ads
- Misleading claims
- Video arbitrage (formerly In-Banner Video)
- Undesired audio
- Undesired video
- Undesired expansion

SECURITY VIOLATIONS

Attempts to compromise the user through the use of malicious code, trickery, and other techniques. Top issues include:

- Forced redirects
- Criminal scams
- Fake ad servers
- Fake software updates
- High-Risk Ad Platforms (HRAPs)¹

¹Ad platforms that consistently serve abnormal levels of malicious ads and are the preferred vector for malicious actors.



Want to know more about these topics? Head to our popular research section on our website

<https://www.confiant.com/resources#research>



To compile the research contained in this report, Confiant analyzed a normalized sample of more than 156 billion advertising impressions monitored from April 1 to June 30, 2021, from over 22,000 premium websites and apps.

The data was captured by Confiant's real-time creative verification solution, which allows us to measure ad security and quality on live impressions (not sandbox scans) across devices and channels.

The violation rate is calculated by dividing the number of impressions exhibiting a particular issue by the total number of impressions monitored by Confiant.

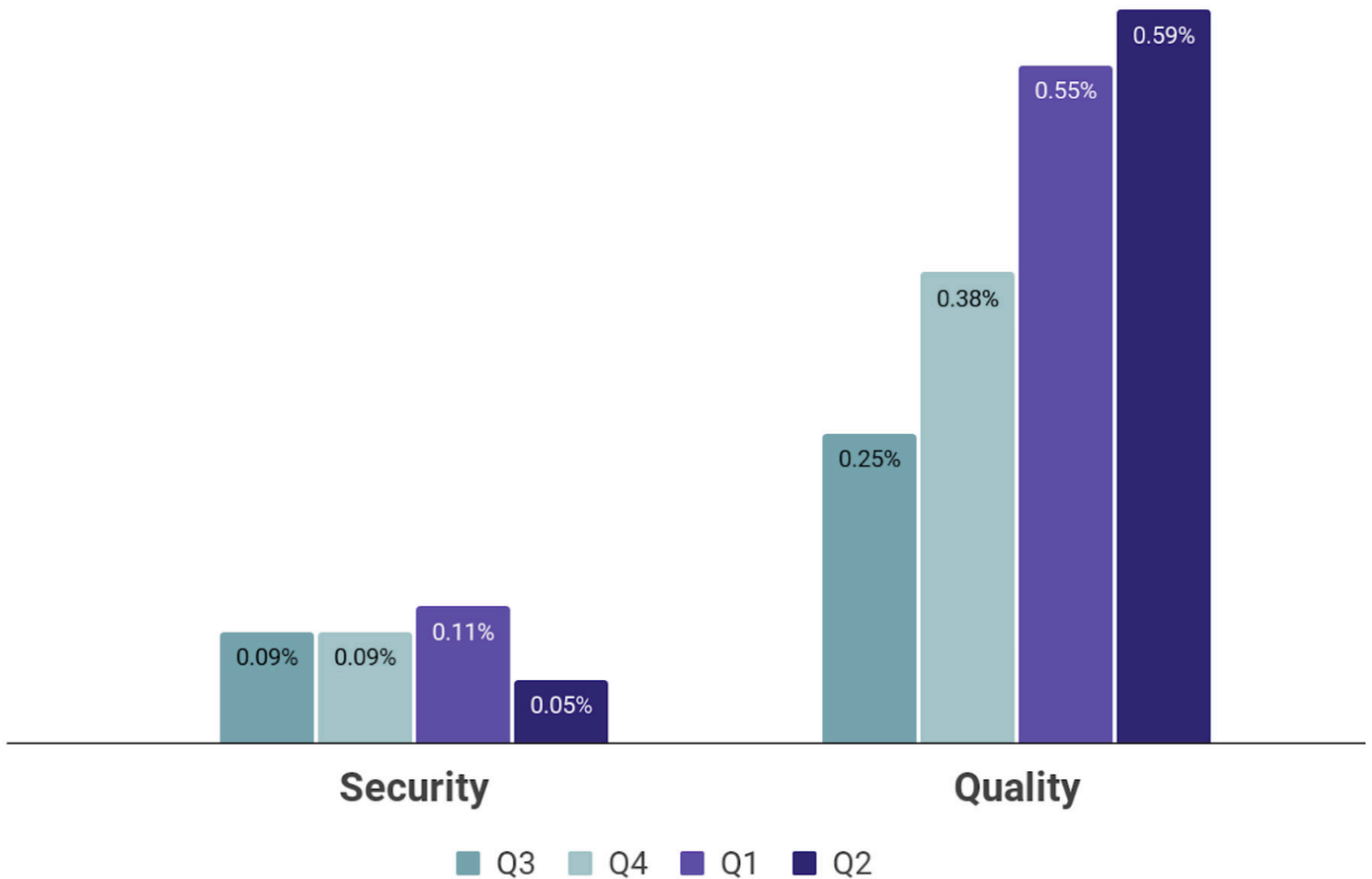
METHODOLOGY

Please note that in Q3 2020, we shifted from using U.S. to global data, necessitating a restatement of our results to allow quarter-to-quarter comparison. As a result, some metrics in this report may not match those in prior quarters.



INDUSTRY VIEW

Q2 2021



HOW DID THE INDUSTRY FARE IN Q1 2021?

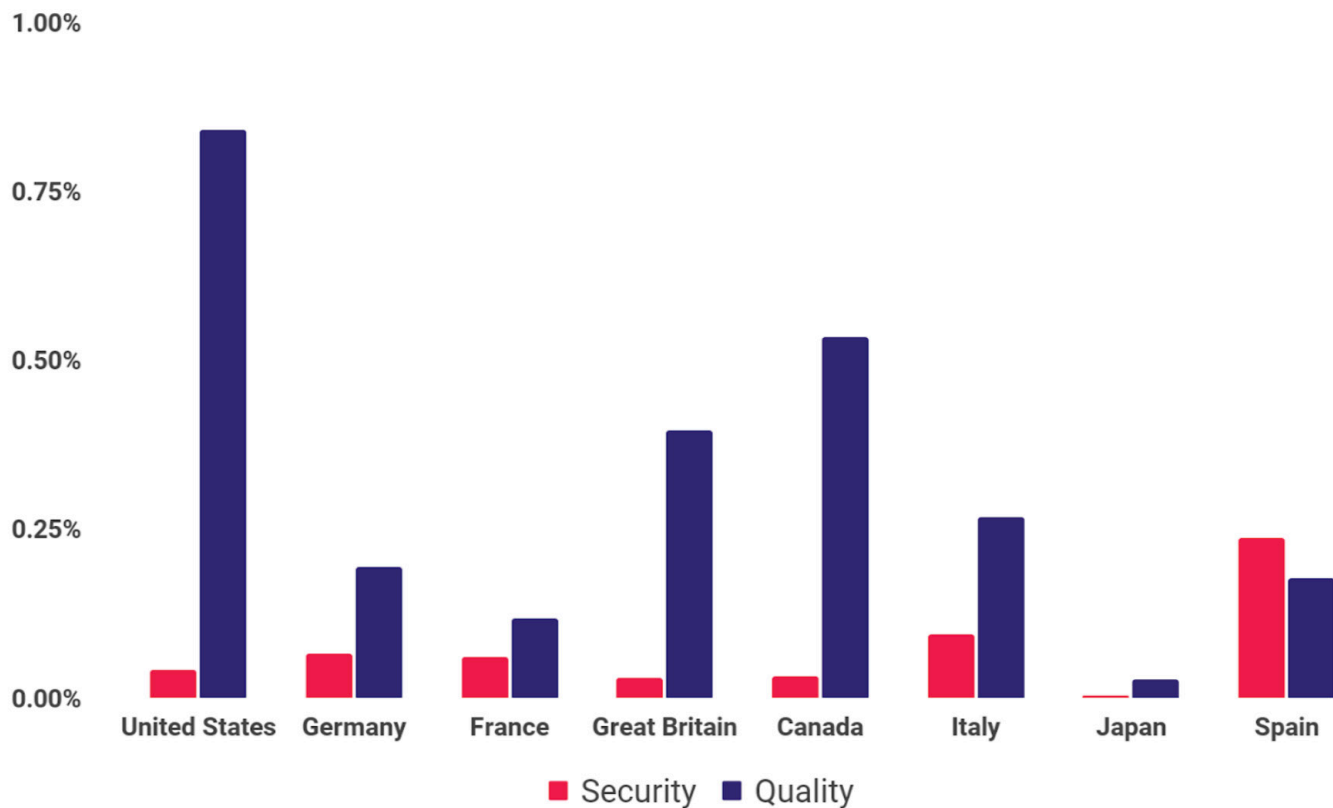
In Q2 2021, the **Security violation rate decreased by 0.06 percentage points from Q1 2021**. We caution that data so far in Q3 shows that the decline was just a temporary respite and that vigilant protections should be kept in place.

Conversely, the Quality violation rate continued its steady rise, increasing by more than 7 percentage points to 0.59 percent. This is the fourth consecutive quarter that the Quality violation has increased, driven by the increased prevalence of Heavy Ads and Misleading Ads.



In Q2 2021,
1 in every 156
ad impressions
was dangerous or
highly disruptive
to users





Q2 2021 VIOLATION RATES BY COUNTRY

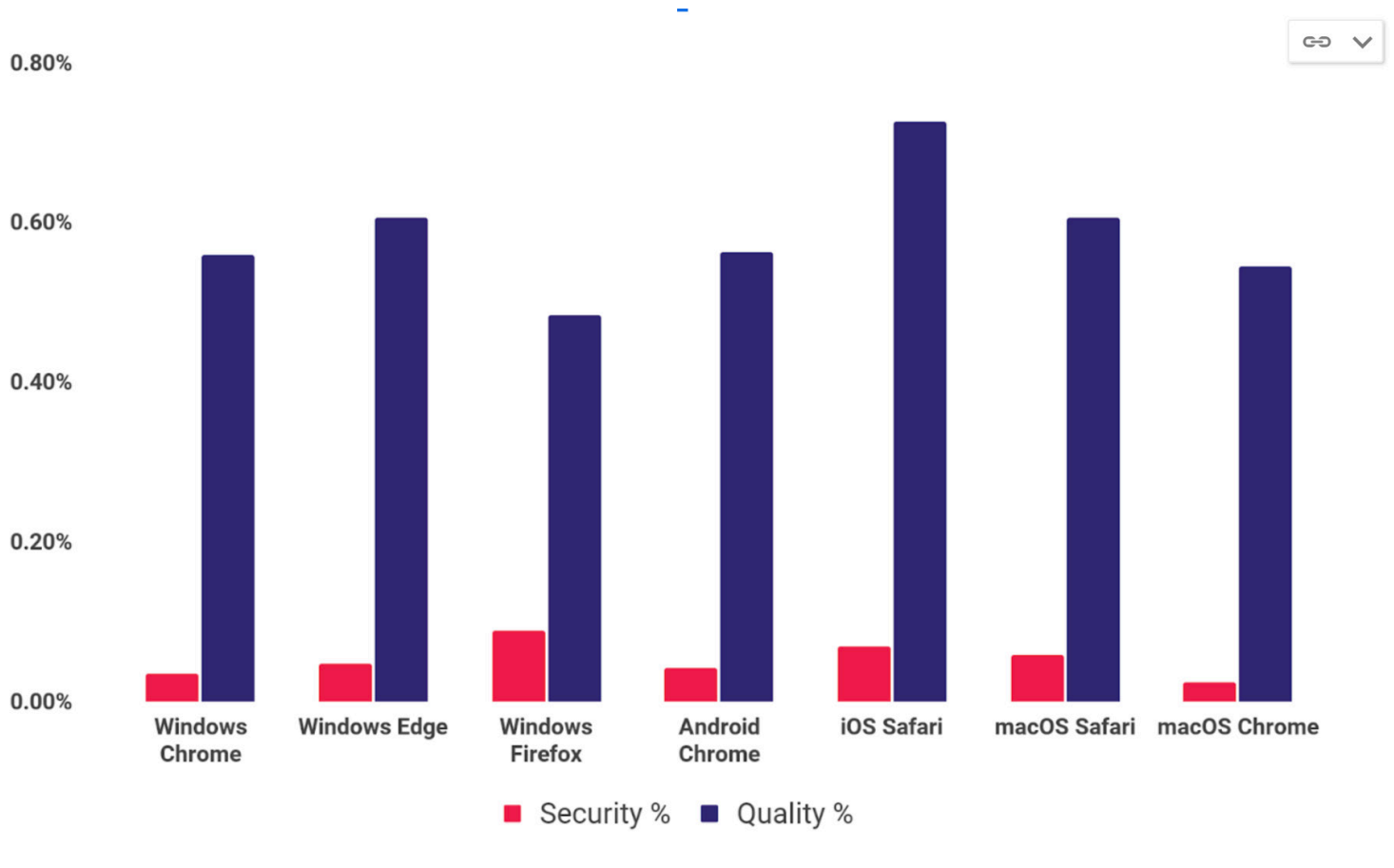
European markets have historically had higher rates of Security violations than the U.S., a trend that continues in Q2.

The **Great Britain was the lone exception, with a Security violation rate 29% below the U.S. rate. Spain was a hotbed for Security issues, coming in at 5x the U.S. level.**

Quality violations remained far more prevalent in the U.S. than elsewhere in Q2, a trend that's held through several reports.



Safari for iOS had the highest rate of Quality violations among major browsers in Q2

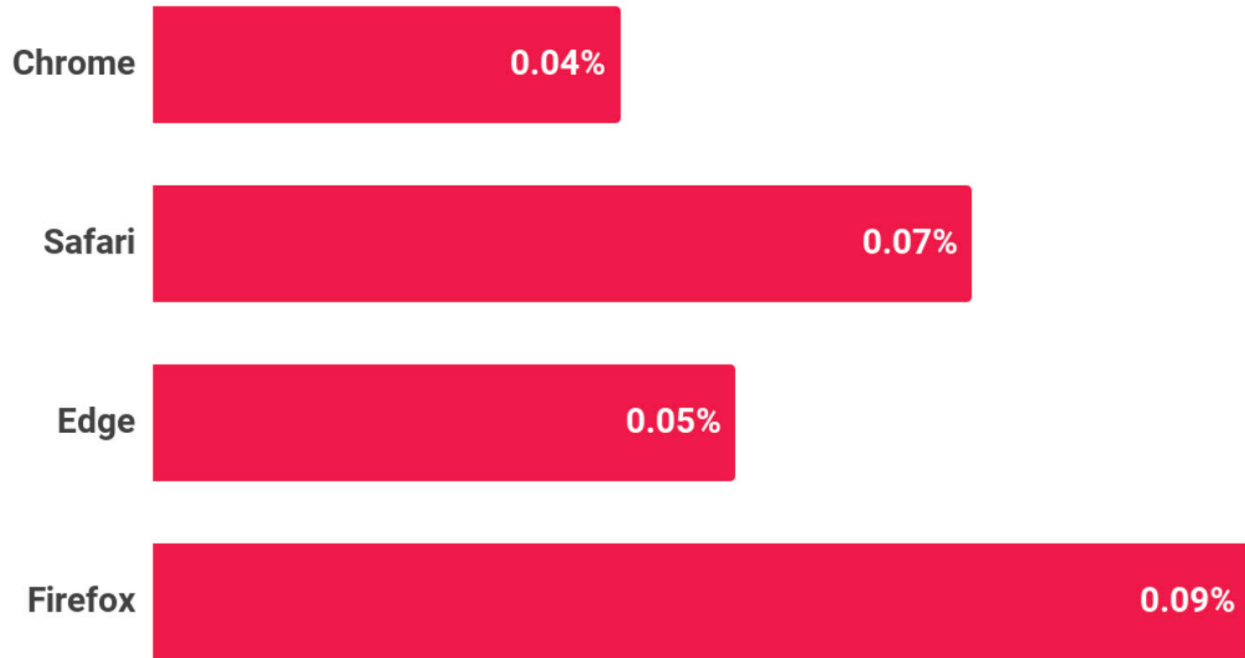


Q2 2021 VIOLATION RATES BY BROWSER

Firefox for Windows was the top source of Security issues in Q2, with a violation rate twice that of Chrome for Windows. On mobile devices, Chrome surpassed Safari as the safest browser.

Safari for iOS had the highest rate of Quality violations among major browsers in Q2, driven by a far higher rate of ads containing misleading claims.





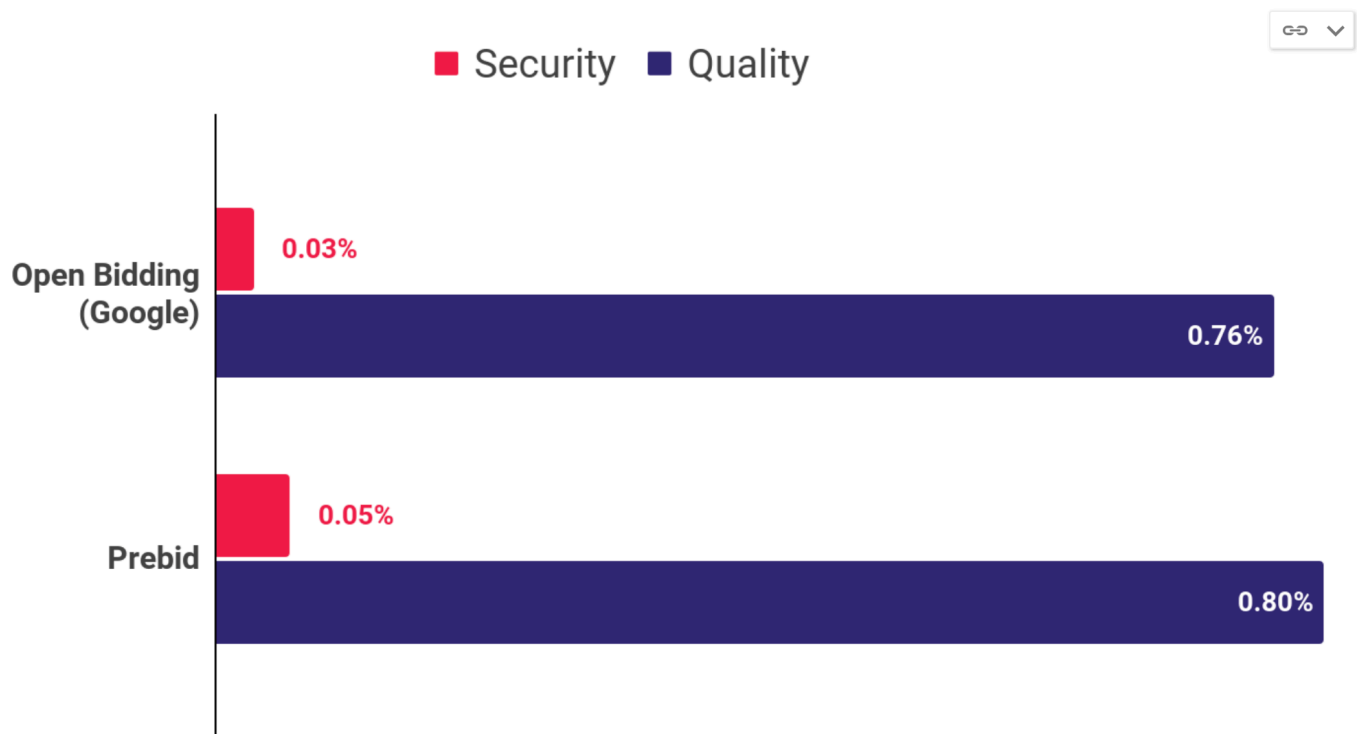
Q2 2021 SECURITY VIOLATION RATES BY BROWSER FAMILY

Most browsers are available for multiple operating systems and devices. When browsers are grouped as a family, interesting patterns emerge.

In Q2, we found that, compared to **Chrome**, **Firefox** was more than twice as susceptible to security issues and **Safari** was 75% more susceptible.

...And Safari was 75% More Susceptible to security issues.

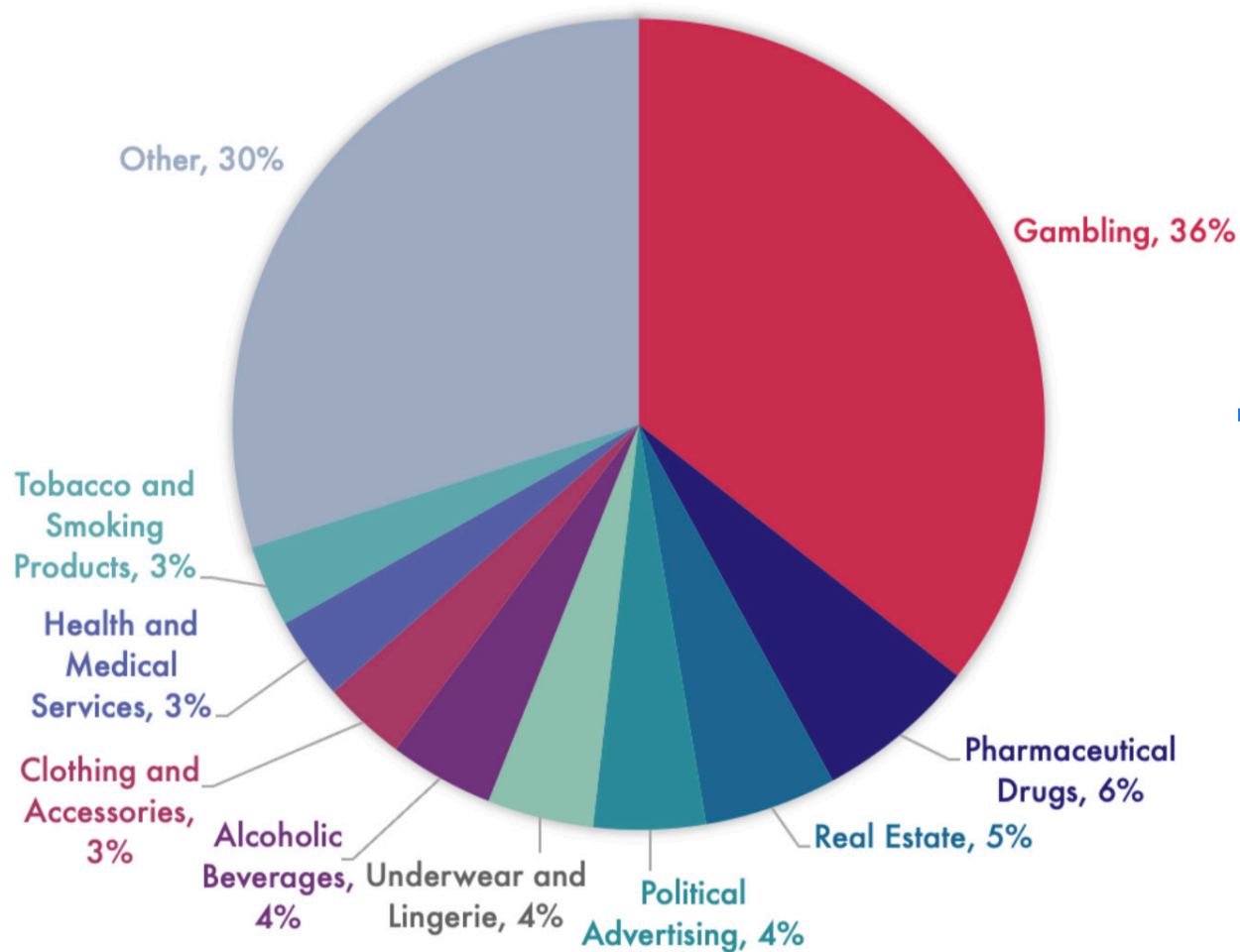




Q2 2021 VIOLATION RATES BY HEADER BIDDING FRAMEWORK

Publishers use frameworks like Prebid to manage bidding from multiple SSPs. Google offers a similar feature within Ad Manager called Open Bidding. In both cases, demand from a diverse set of SSPs flows through the framework, putting the publisher at risk of Security and Quality issues. In some cases, these frameworks can apply malware checks over and above those of the SSPs present.

In Q2, Open Bidding continued its strong performance on Security and Quality relative to Prebid.



MOST BLOCKED AD CATEGORIES

Confiant allows publishers to block creatives across 100+ different categories, including common verticals like Automotive and sensitive topics like Alcoholic Beverages.

Having seen a rise in ads for gambling during 2020 and as the pandemic has progressed, we suspect the results are COVID related. Gambling surpassed Pharmaceutical Drugs to become the most blocked ad category, representing over a third of all category blocks. Blocks for Political advertising continued to fall as we moved further from 2020's contentious election cycle. Two new categories, Real Estate and Underwear/Lingerie, entered the top 5 blocked categories for the first time.


"Other" includes over 100 other categories



INSITES

Why Gambling?

Among the Most Blocked Ad Categories that increased during Q2 2021 was Online Gambling, leading with one-third of the blocked ads in the category, which surpassed Pharmaceutical Drugs to become the most blocked ad category. That is not surprising and is most likely linked to the effects of the COVID Virus on our world. Research and Markets reported that "The online gambling market is expected to register a CAGR of 11.94% during the forecast period, 2021-2026. The COVID-19 pandemic positively impacted the market, as consumers turned more toward the online platform to bridge their financial, social, and psychological crisis during lockdowns. Online betting is expected to be the fastest-growing segment during the forecast period." Apparently, consumers are using online gambling sites to replace their attendance at in-person sports events during

lockdowns due to COVID restrictions. Sports betting was legalized in the United States by the Supreme Court in 2018, adding sites with legal authority to appear in ads as well as an opportunity for threat actors to take advantage of the appearance of legal online gambling for malvertising. Pharmaceutical ads continue to be a largely blocked category because Publishers realized that consumers are overwhelmed with COVID ads during the prior 18 months and current period. Real Estate also entered the top 5 blocked ad categories in Q2. In February 2021 Reuters notes "Last year, most of the world's largest economies were brought to their knees by the pandemic but record low interest rates and pent-up demand for homes pushed U.S. house prices to levels not seen in more than half a decade." 





CONFIANT

SSP RANKINGS

Q2 2021

Q2 2021 US SSP RANKINGS

In Q2, Confiant tracked impressions from over 100 SSPs.

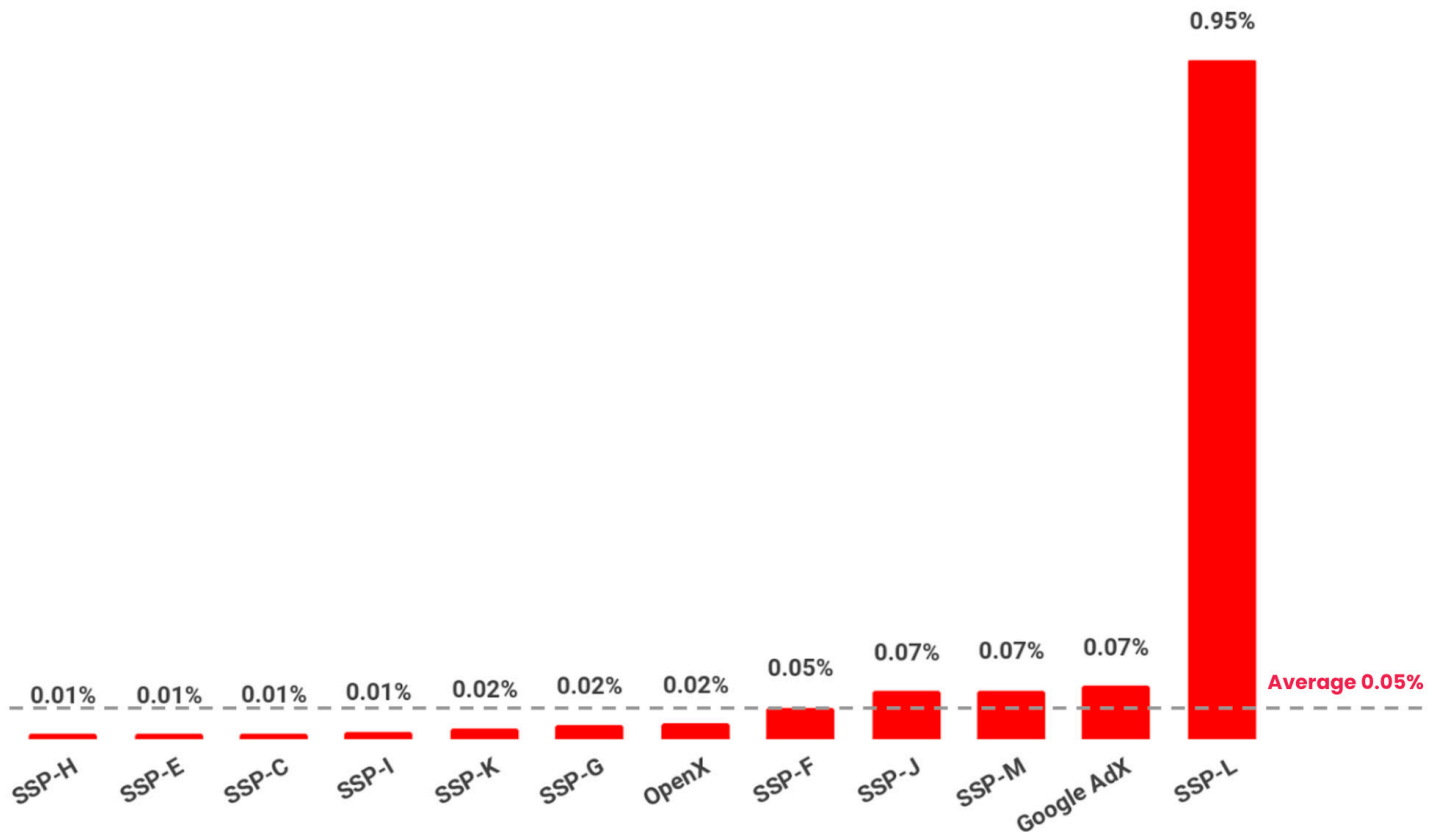
However, the vast majority of global impressions originated from just 12 providers¹ commonly used by publishers. These 12 providers are noted in the charts that follow using a coding system that carries over from one quarter to the next to allow comparisons over time.

To qualify for inclusion, a provider had to have been a consistent source of at least One billion Confiant-monitored impressions a quarter across our global sample.

We identify two SSPs in these rankings: Google AdX and OpenX. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. OpenX has opted to be listed in our reports without obfuscation, an option we offer to any SSP that requests it. We encourage other leading SSPs to request full disclosure so that we may provide the publisher community with a complete view into relative quality of their partners.

¹ Google AdX, Magnite, OpenX, Xandr, Verizon Media, Index Exchange, PubMatic, Sonobi, TripleLift, District M, 33Across, and Sovrn





SECURITY VIOLATION RATE BY SSP

After years of strong performance, Google has underperformed the market for two quarters in a row.

Google's Security violation rate exceeded the industry average by 47%. SSP-L turned in a last-place performance for the third straight quarter, with their Security violation rate coming in at 132x that of the best performing SSP.

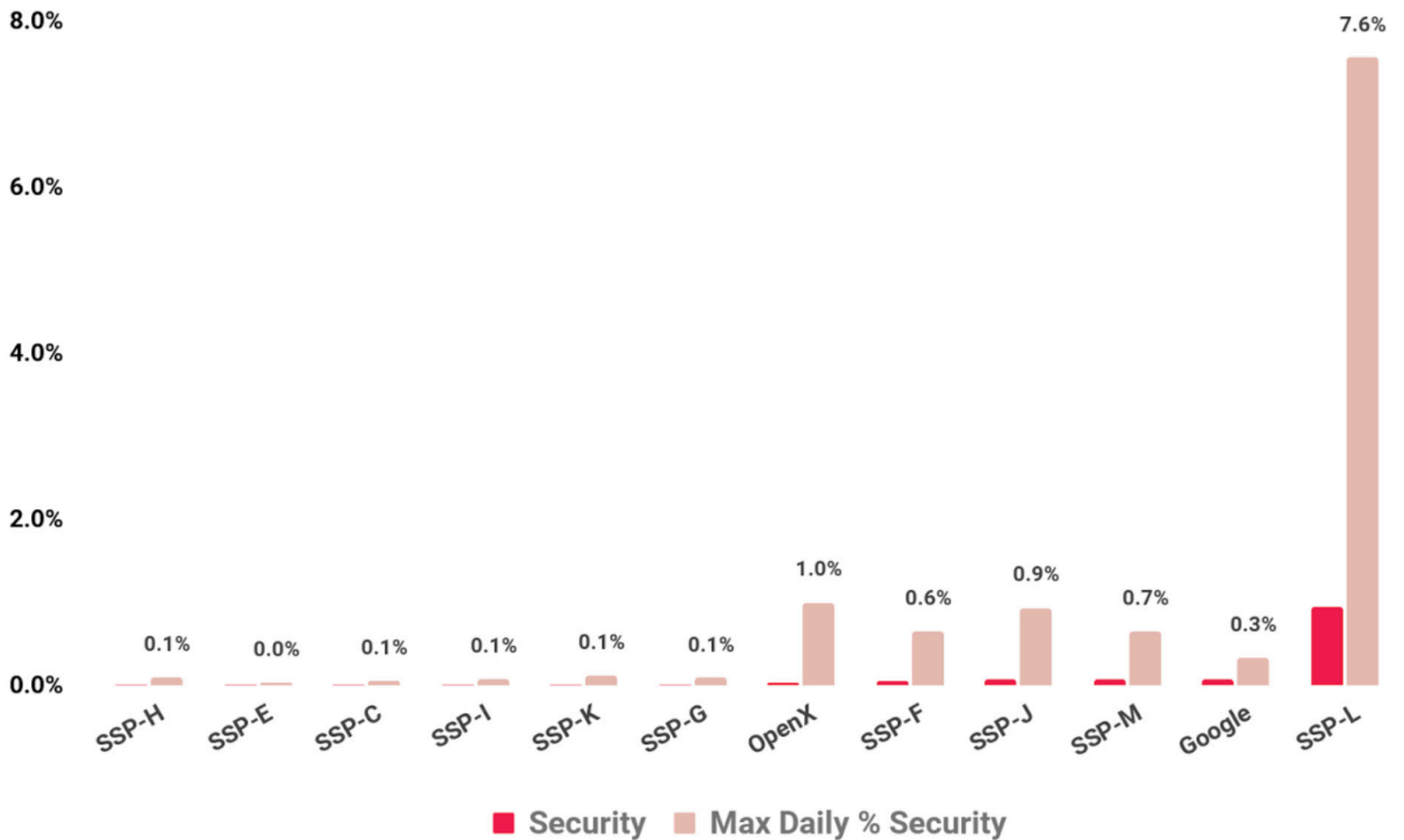
A record 7 of the 12 SSPs were able to reduce malvertising to minimal levels, demonstrating the significant progress the industry has made against the scourge of malvertising.



500,000+

Since launching our privacy product
in May Confiant's Security Team
has seen **more than half a million**
GDPR violations per day





DAILY MAXIMUM MALICIOUS RATE BY SSP

Quarterly averages can mask significant variation in day-to-day performance, so it's important to measure the upper bound of the Security violation rate for each SSP to get a sense of overall risk.

When under sustained attack, SSPs L had days where an incredible 1 in 13 impressions was a Security violation, putting publishers and users at considerable risk.



BREAKDOWN

How a 7% increase in Quality issues and continued decrease in Security issues has Impact

As shown in this report, this is the fourth consecutive quarter that the Quality violation rate has increased, driven by the overwhelming prevalence of Heavy Ads and Misleading Ads.

As we know, Heavy Ads can lead to page latency, lower interaction and engagement rates, higher bounce rates, and lost revenues. Rising bounce rates mean decreased time on page. These factors can lead to brands and agencies questioning the quality of publications.

If your ads are seen as misleading or "scammy", it reflects on the quality of your site, your reputation, and its content. Native ads are favored by scammers and can present the largest challenge for publishers to control. Misleading ads next to legitimate brand ads, threaten advertiser dollars if the legitimate ads are seen to have an adjacency issue, i.e being next to "bad ads". This may be perceived as a negative reflection on your brand and quality level, as well those ads contributing to the advertiser brand looking cheap.

WHAT DOES THAT MEAN FOR PUBLISHERS?

As Simon Hearne points out in his article on the topic of page speed:

- *Slow pages lead to higher bounce rates*
- *Slow pages lead to lower interaction rates*
- *Slow pages lead to poorer organic SEO rankings*
- *Slow pages lead to higher ad costs*
- *Slow pages lead to lost users*
- *User loss leads to revenue loss*

Hearne Continued, "At the most basic level, we know that faster pages lead to an increase in page views. This increase comes from a number of factors: reducing bounce rate (Is this page ever going to load?), increasing session length (I've only got a minute to catch up on the news) and favourable rankings from search engines which include speed as a ranking factor. Session length and time on page contribute to rank score. Blocking bad ads improves authoritative ranking on Google. Assuming that there is a near-linear relationship between page views and ad revenue, there is an obvious benefit to improving site speed." It may be obvious but, this is where revenue is lost due to heavy ads.

In their article, [Are Slow Site Load Times Crippling Your Digital Marketing Programs?](#) Synapse SEM points out that: Slow load times are a major driver behind user bounces and exits. **"58% of shoppers will leave a website if it takes more than 3 seconds to load."** For Amazon, for example, **"a 100 millisecond improvement in load time [is equivalent to] a 1% revenue increase."** These stats demonstrate a clear connection between page speed and conversions and ultimately ROI. Misleading ads are bad for brand safety and publisher brand integrity.

As a top-tier Publisher, with stellar content on your site, is it worth 1% or more of your audience being upset with your ad content? Threat actors are working overtime to hijack user data, and steal from users while they are engaged with publisher content. Confiant's previous investigations estimated the [financial cost of malicious ads to users and publishers into cost billions of dollars per year](#). In the case of FizzCore, the financial scam threat group Confiant discovered and named, we know they netted one million dollars in one day.




BREAKDOWN

Continued...

Aside from the clear negative user experience and negative impacts to your business from ads with heavy and misleading ads, is the rapidly increasing potential of this type of Malvertising to cause your business to be out of compliance with the latest privacy regulations (GDPR, CCPA, CPRA, CPA, PIPEDA, CPPA and many others worldwide), leaving your organization exposed to significant financial losses due to fines and penalties by government enforcement authorities. Recently, [Le Figaro's parent company was fined 50,000 euros \(nearly \\$59,000 US\), Google was fined \\$121 million, and Amazon Europe was fined 35 million euros \(over \\$41 million US\).](#)

It may not be the fault of the publisher, however Malvertisers

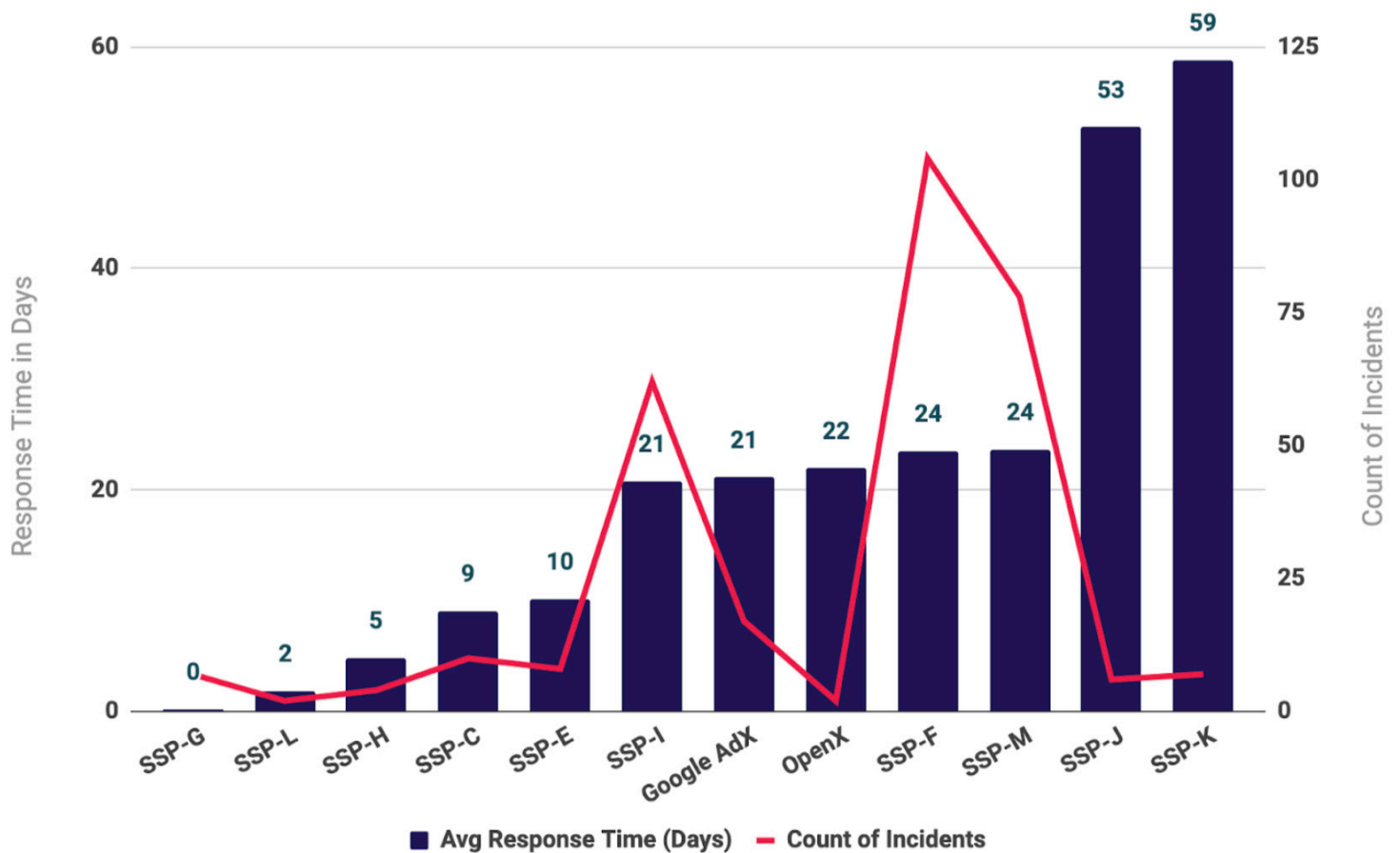
use publisher sites and the Adtech ecosystem to deliver bad ads, leaving you partially or wholly responsible for the

repercussions: Loss of impressions, loss of viewers, negative corporate reputation, loss of revenue, and exposure to significant fines and penalties by regulatory agencies. In short, you should continue to implement your controls for Security, Quality, Privacy and Compliance, or buckle-up and expect a bumpy ride. 

"Optimizely added artificial latency to the Telegraph and saw page views plummet: by 11% for a 4 second delay and 44% for a 20 second delay." while this was in 2019 heavy ads have only exacerbated the issue of latency.

¹Source: <https://simonhearme.com/2019/site-speed-for-publishers/>



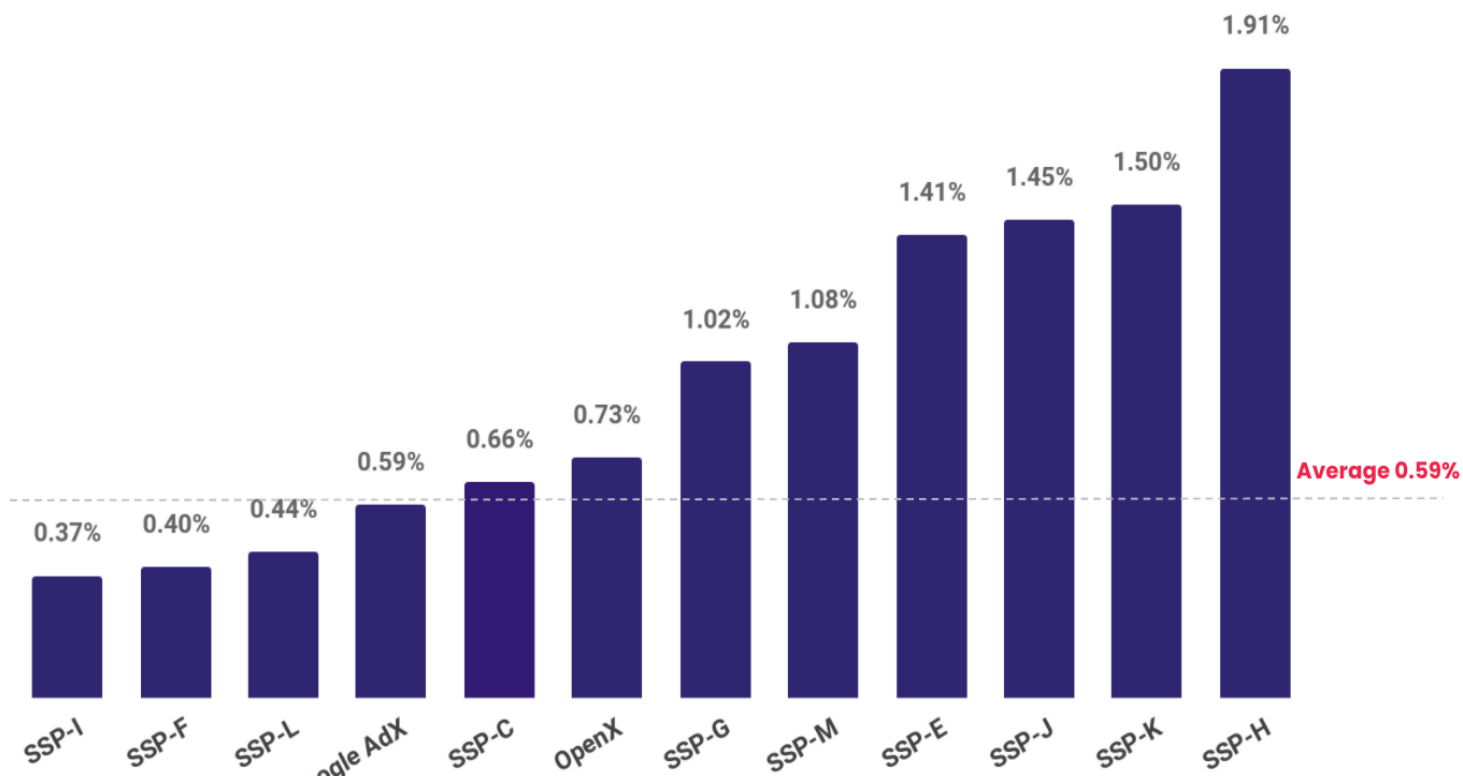


AVG DURATION OF ATTACK BY SSP IN Q2

SSPs differ in their ability to respond to attacks once they are underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. **On this measure, we see huge differences among the major SSPs.**

In Q2, SSPs J and K were the outliers, taking an average of over 50 days to fully resolve an attack. Conversely, SSP G took less than a day to resolve attacks.



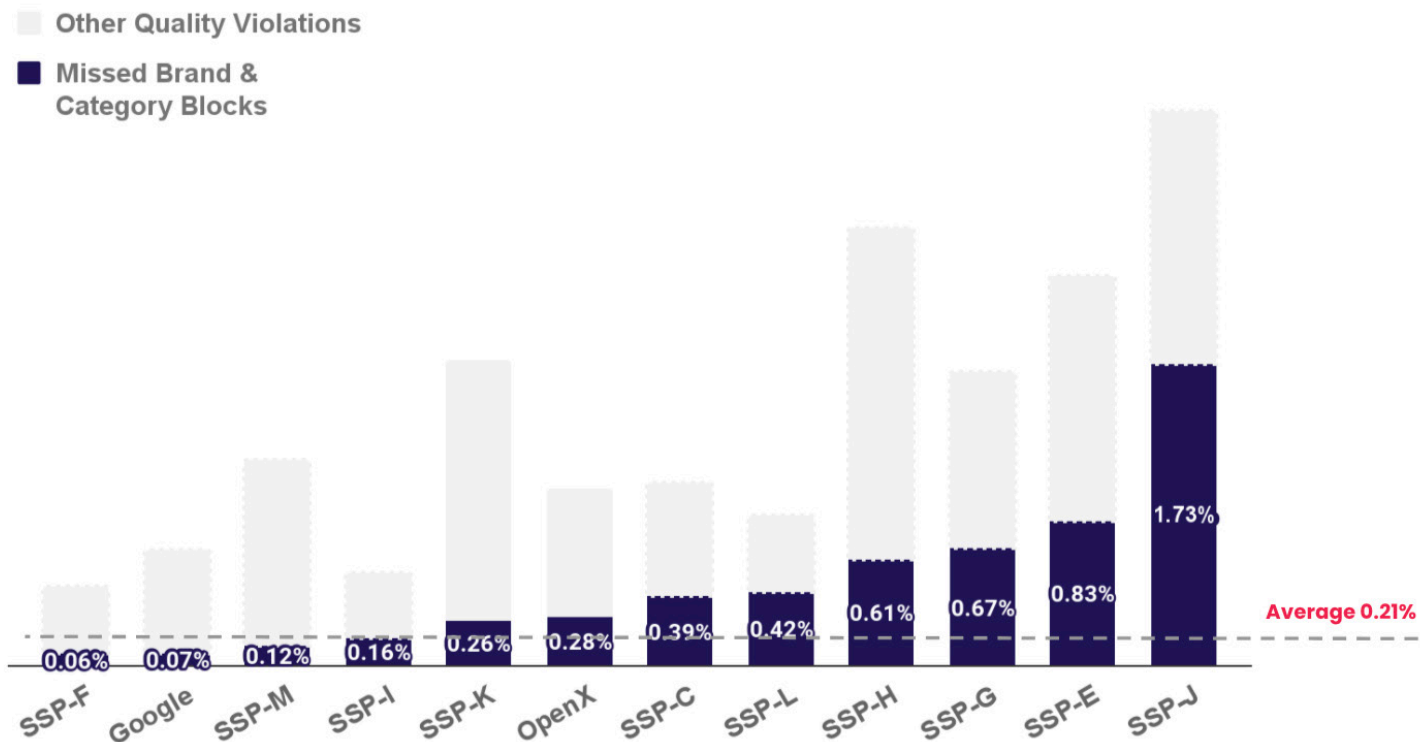


QUALITY VIOLATION RATE BY SSP

Quality violations are based on a diverse set of controls that publishers can activate on the Confiant platform. Examples include misleading claims, heavy ads, and pop-ups. These rules correspond to ad behaviors that disrupt or impair the user experience.

SSP H fell to last place, driven by an increase in Misleading Ads. SSPs I, F, and L had the lowest Quality violation rate, with SSP-I taking the top spot for the 2nd quarter in a row.



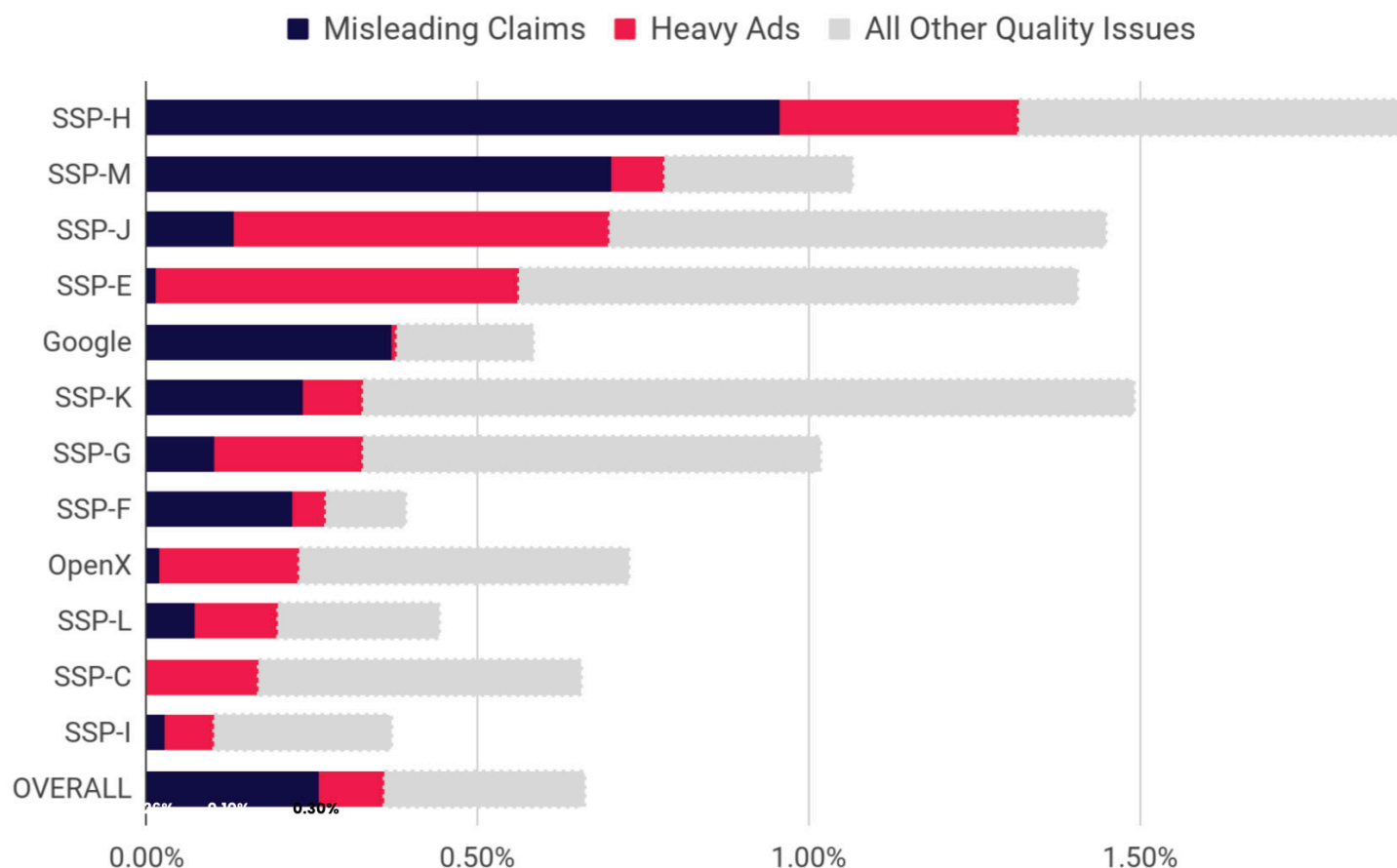


MISSED BRAND/CATEGORY BLOCKS

Publishers rely on SSPs as their first line of defense against ads associated with unsuitable brands and categories. However, these controls are not always effective.

SSP J once again struggled to block the brands and categories requested by Confiant publishers, while SSPs M, F, and Google consistently performed well on this measure.



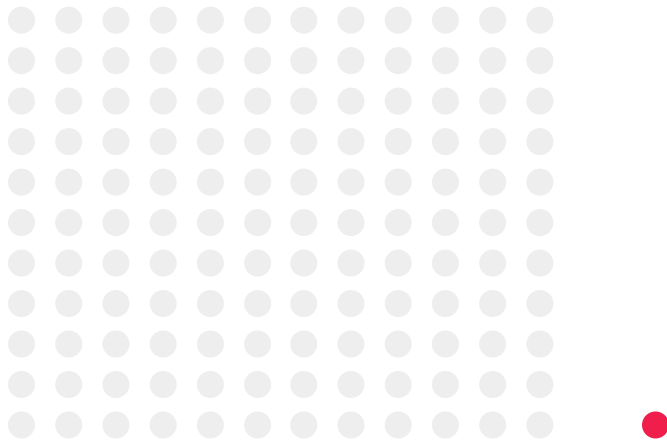


QUALITY ISSUES DEEPDIVE

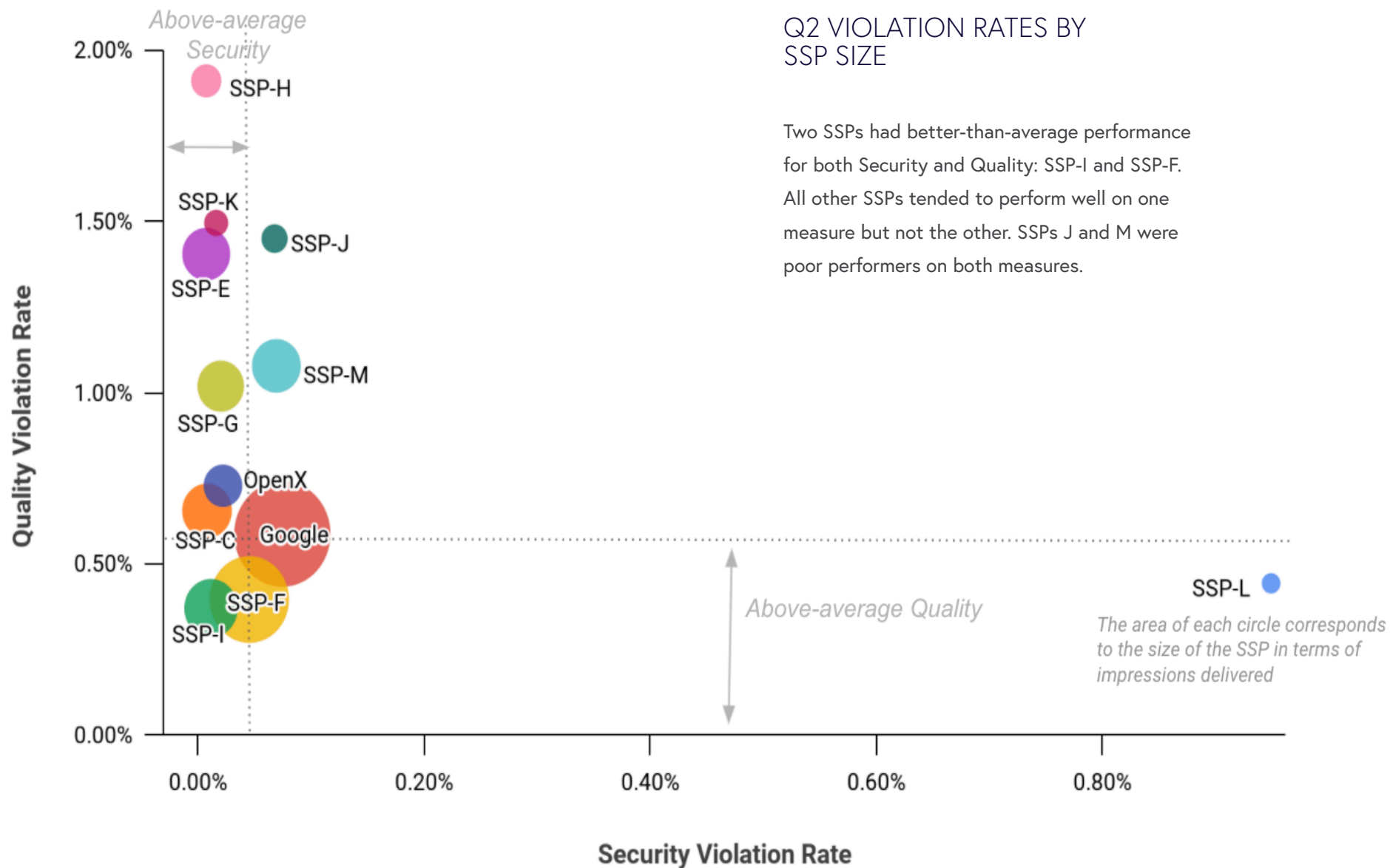
Of the myriad quality issues we monitor, publishers are often most concerned about Misleading Claims, which covers legally fraught issues like fake celebrity endorsements and bogus health claims, and Heavy Ads, which can affect the perceived performance of a site and risk being blocked by Chrome.

Almost 1 in every 100 ads delivered by SSP-H was misleading. SSPs H and M had the highest rate of misleading ads, while SSPs-J and E struggled with heavy ads. SSP-I's great overall performance for quality is based in part on their mastery over these two threats.





The worst
performing SSP
had a **violation
rate 132x that
of the best**





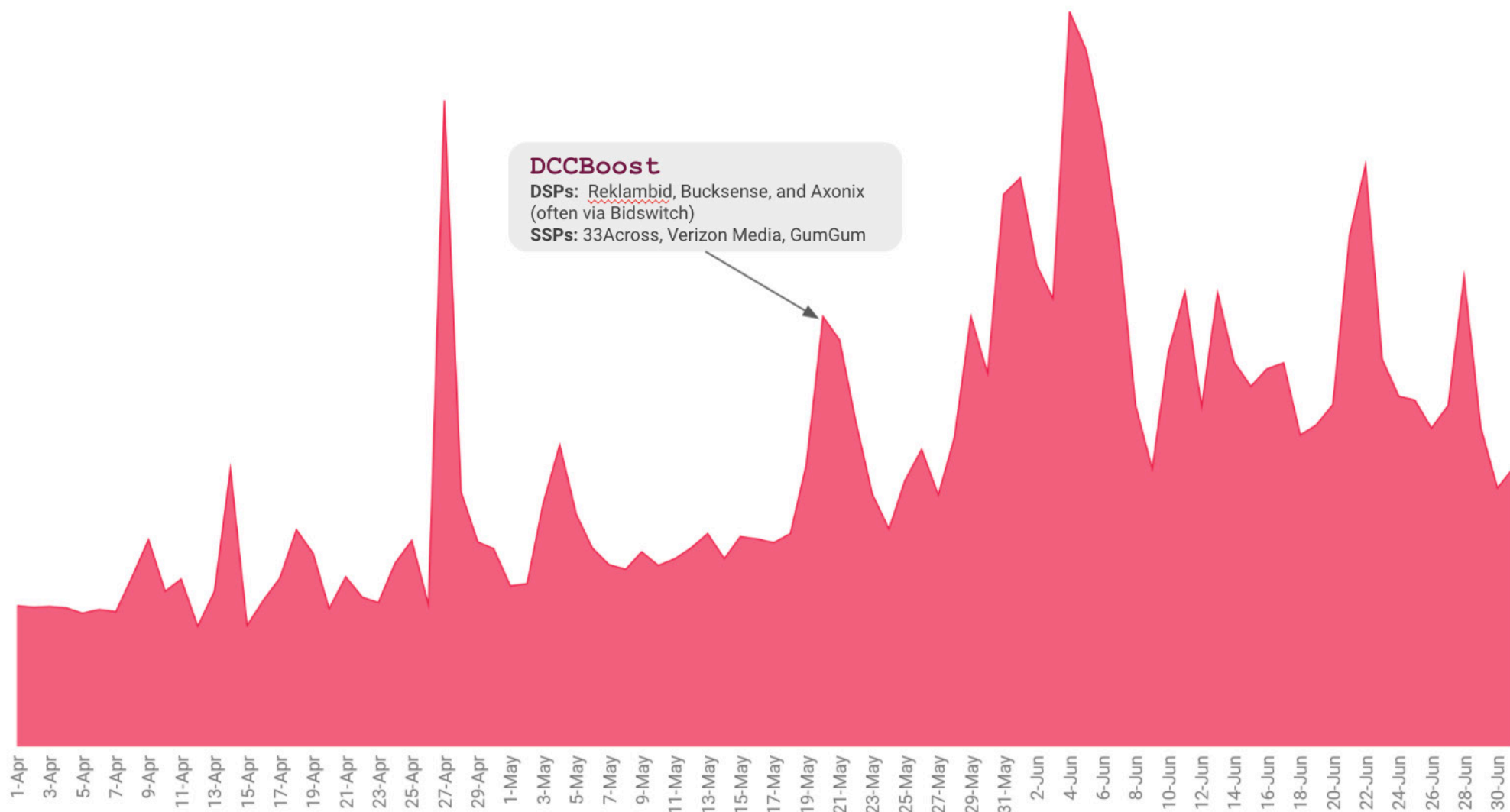
CONFIAANT

MAJOR THREAT GROUPS ACTIVE IN Q2

Q2 2021

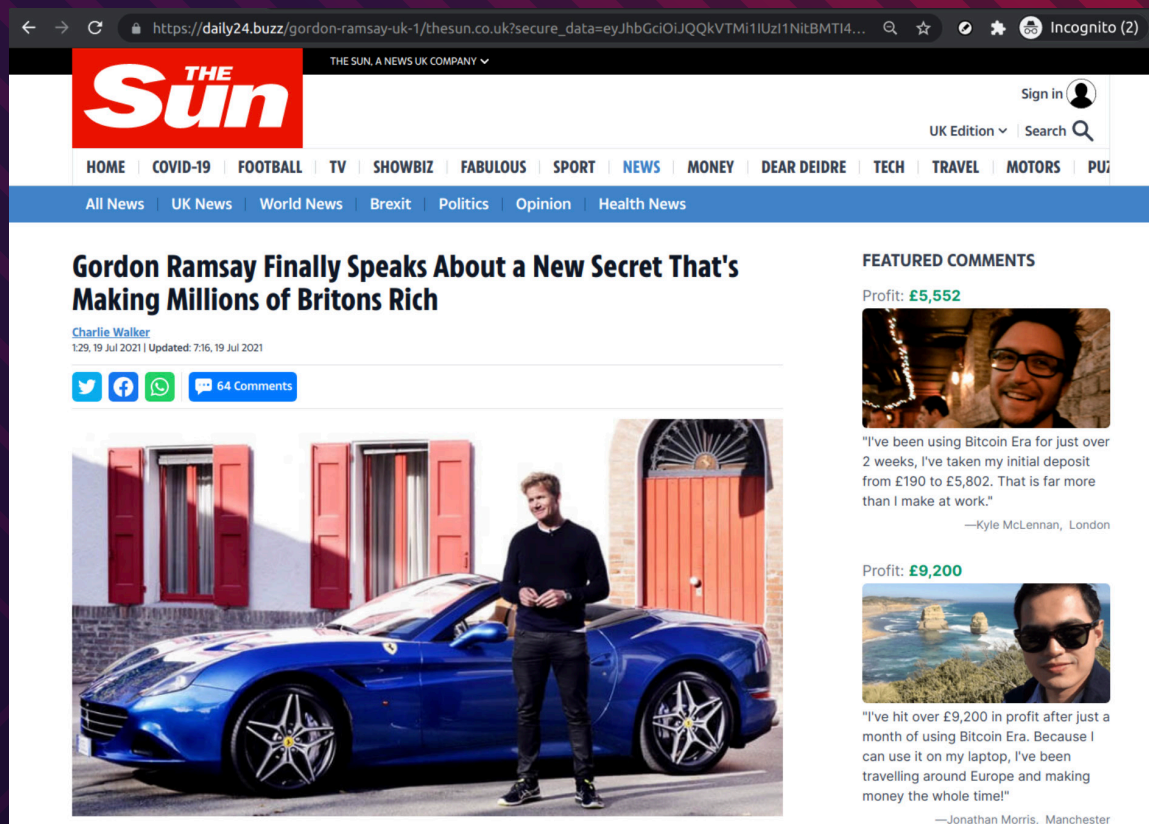


Notable Threat Activity



ZIRCONIUM

Zirconium is notable for their persistence, technical prowess, and ability to adapt in a changing environment.



PEAK ACTIVITY: FEBRUARY

For years, Zirconium have used their understanding of Ad Tech in order to form dozens of convincing business entities to gain seats on major buying platforms.

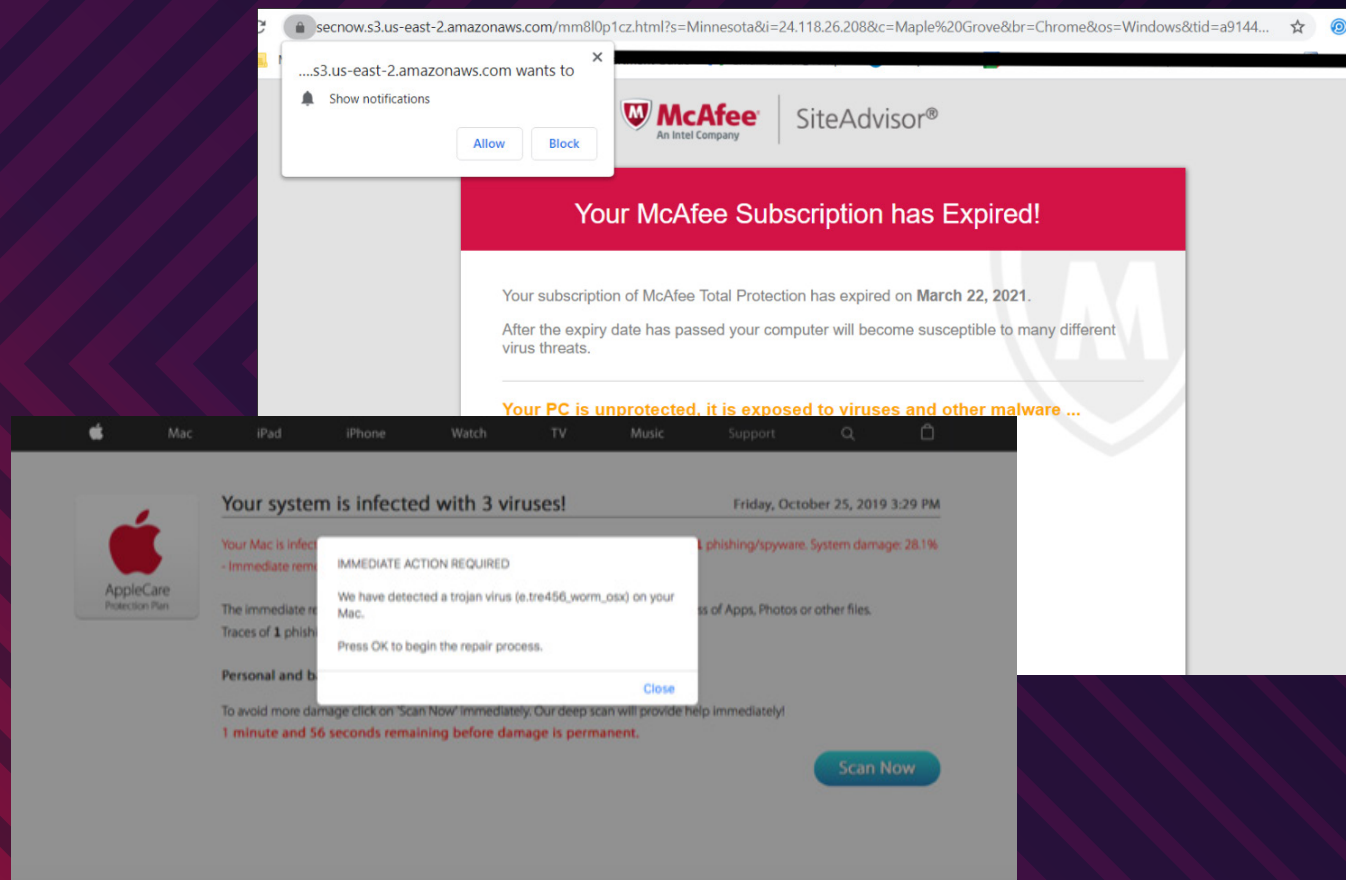
Recently, the group has hopped on the investment scam bandwagon to serve up cloaked ads that promote dubious money-making opportunities, almost exclusively targeting UK audiences.

The group is known for their technical wizardry on the client-side, and they continue to bring these same skills to the task of promoting these new payloads.



YOSSEC

Yosec is a threat actor that pushes fake Flash drive-by downloads and tech support scams via forced redirects.



PEAK ACTIVITY:
APRIL/MAY

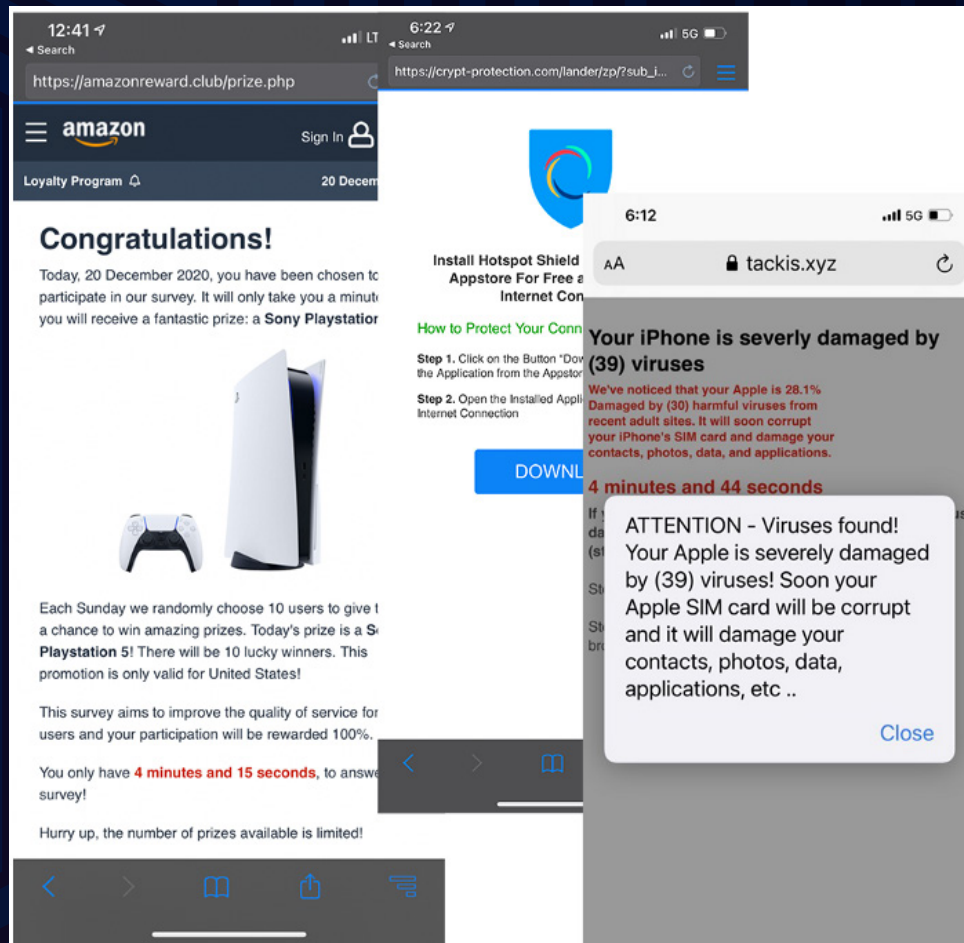
The bulk of their activity targets Mac devices, particularly the Safari browser. Yosec malvertising activities are characterized by short, targeted bursts, but at times we have seen them ramp up to large volumes over the course of several hours.

In February of 2021, Confiant was credited with [CVE-2021-1765](#) for reporting an exploit leveraged by Yosec to bypass built-in security mitigations in Safari, and CVE-2021-30533 more recently for their abuse of the same bug in Chromium. The full disclosure will soon be available on the Confiant Security Blog.



DCCBoost

DCCBoost campaigns consistently include interesting malvertising innovations from a technical standpoint.



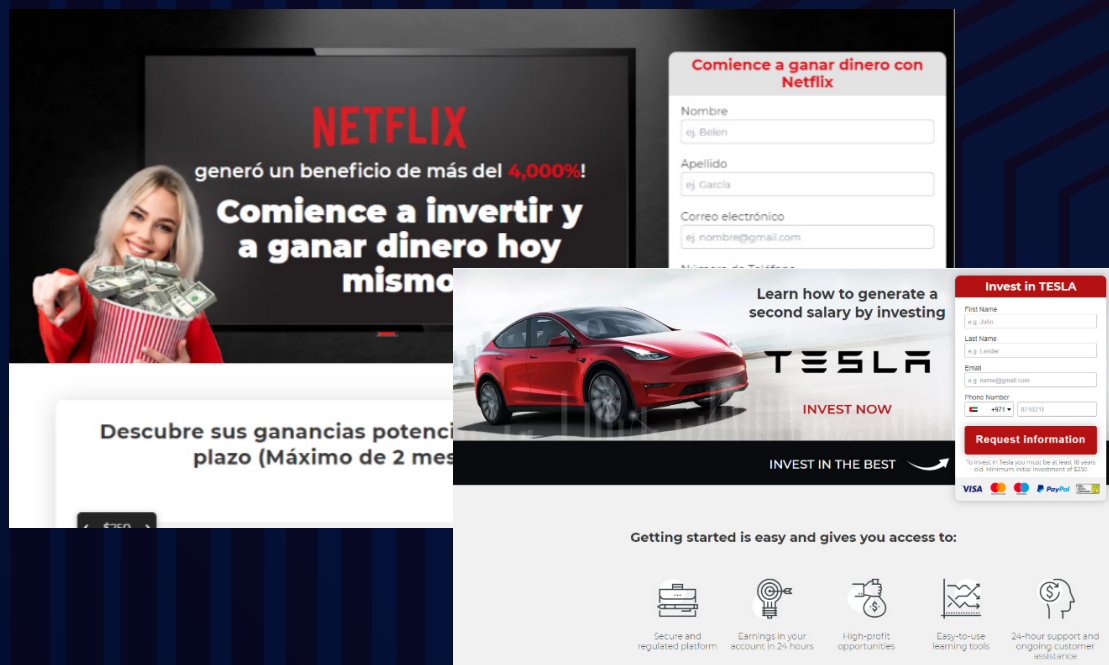
PEAK ACTIVITY:
MAY
and **ONGOING**

They use a combination of server-side targeting combined with a compartmentalized client-side payload in order to deliver the malicious ad in stages.

We estimate that this malvertiser routinely impacts tens of millions of ad impressions when they run their campaigns at full scale, with a particular focus on the United States

HircusPircus

Fully licensed to operate as investment brokers across Europe, these companies accumulate victims' complaints and regulatory friction for their unsavory practices.



PEAK ACTIVITY:
ONGOING

While not a specific malvertising threat actor, we wanted to highlight a cluster of investment firms primarily based in Cyprus that sit at the end of the kill chain for a large amount of malvertising scams.

Fully licensed to operate as investment brokers across Europe, these companies accumulate victims' complaints and regulatory friction for their unsavory practices.

HircusPircus' savvy in defrauding investors is evidenced by their carefully crafted sales funnels that often start with affiliates offering investment opportunities in known well performing brands. Initial payments are typical limited to \$250 to qualify real victims.

The campaigns have a huge presence in Native advertising and often sneak onto publisher sites via lesser known platforms.



PEAK ACTIVITY: ONGOING

These days, most malvertising falls under the category of "Malicious Clickbait". The attackers will launch a display ad campaign for a benign looking brand and then "flip" the creative to some clickbait messaging — usually a celebrity-endorsed investment opportunity.

The landing page will typically be cloaked so that the scam is revealed only to the specific audiences and devices targeted by the attackers. These attacks mostly impact Europe, Canada, and the US.

The campaigns have a huge presence in Native advertising and often sneak onto publisher sites via lesser known platforms.

KEY TAKEAWAYS



Violation rates for Quality issues rose 7% in Q2 vs. Q1, while Security saw its first substantial decline in several quarters.



For the second quarter in a row, Google underperformed the industry average for Security, coming in at 47% above the average violation rate and ranking 11th of 12.



Misleading Claims and Heavy Ads loomed large as the top quality issues for publishers. Nearly 1 in every 100 ads delivered by a major SSP was misleading.



Gambling was the most-blocked ad category, representing over one-third of all category blocks.



1 in every 156 impressions was dangerous or highly disruptive to the user.



Compared to Chrome, Firefox was more than twice as susceptible to security issues and Safari was 75% more susceptible.





MALVERTISING + AD QUALITY INDEX

MAQ INDEX

[CONFIENT.COM/MAQ-INDEX](https://confiant.com/maq-index)

For more information on our entire suite of Security, Quality and Privacy protection products please visit our website or

email us at:

MARKETING@CONFIENT.COM

Q2 2021