



MALVERTISING + AD QUALITY INDEX

# MAQ INDEX

---

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 150 BILLION IMPRESSIONS MONITORED IN REAL TIME EACH QUARTER, CONFIANT IS ABLE TO ANSWER FUNDAMENTAL QUESTIONS ABOUT THE STATE OF CREATIVE QUALITY.

**Q3 2021**



# INTRODUCTION

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 new way to examine the problem, revealing the underlying causes for the first time. The MAQ Index, which leverages Confiant's position as the vendor of choice for ad security, quality, and privacy monitoring, aims to provide a comprehensive view into the creative-quality issues facing the industry.

In 2018, Confiant released the industry's first benchmark report. This report, the fourteenth in the series, covers Q3 2021.



To compile the research contained in this report, Confiant analyzed a normalized sample of more than 150 billion advertising impressions monitored from July 1 to September 30, 2021, from tens of thousands of 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.*



## SECURITY VIOLATIONS

Attempts to **compromise the user** through the use of malicious code, trickery, and other techniques.

Top issues include:

- Malicious clickbait
- Forced redirects
- Criminal scams
- Fake ad servers
- Fake software updates
- High-Risk Ad Platforms (HRAPs)<sup>1</sup>

## 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

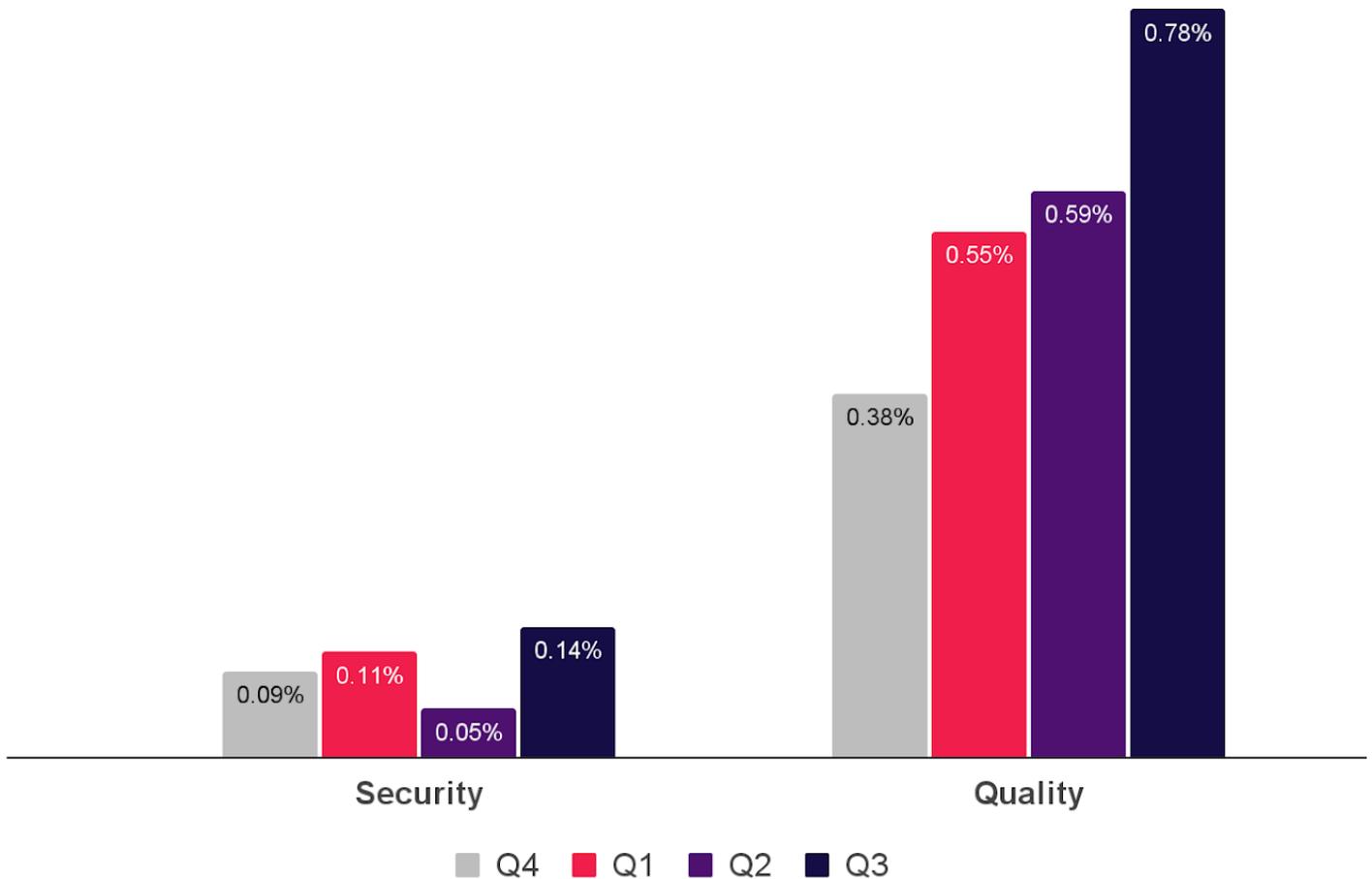
---

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



# INDUSTRY VIEW

**Q3 2021**



## HOW DID THE INDUSTRY FARE IN Q3 2021?



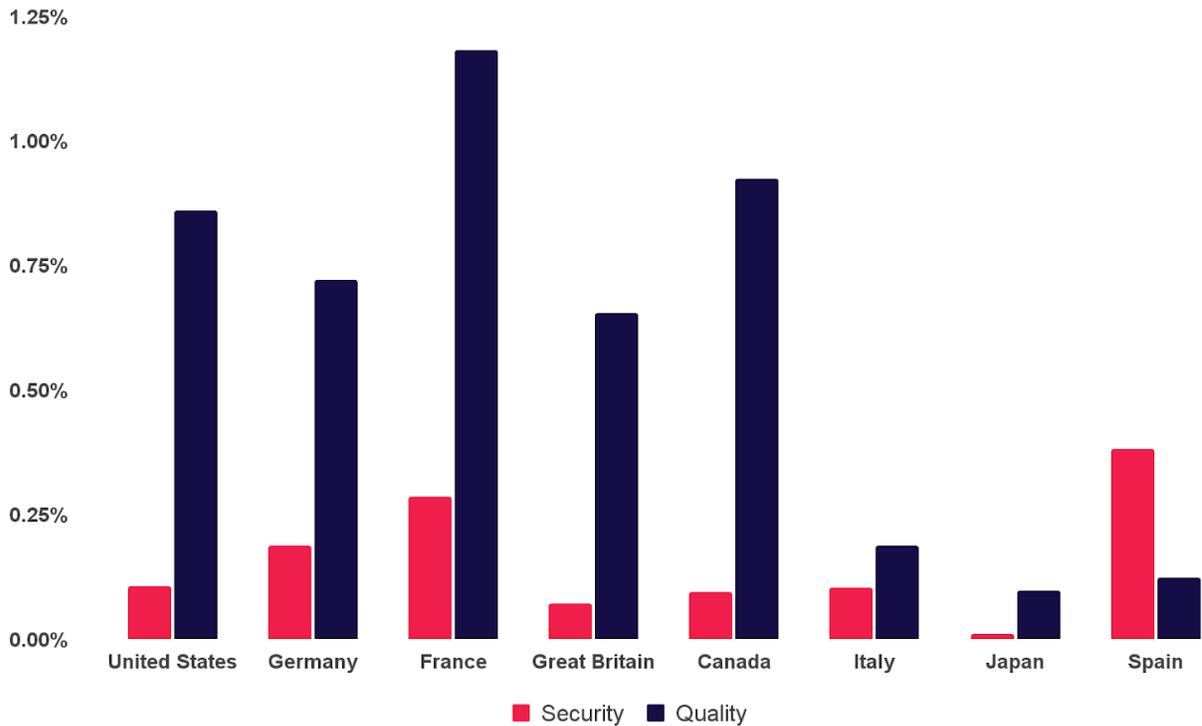
The industry struggled to deal with both Security and Quality issues in Q3, turning in its **worst overall performance in over a year.**

The **Security violation rate nearly tripled** from Q2 to Q3, rising to 0.14%, the **highest level in over a year.**

The **Quality violation rate increased a whopping 0.19 percentage points** to 0.78%. This is the **fifth consecutive quarter that the Quality violation has increased**, driven by the increased prevalence of Heavy Ads and Misleading Ads.



In Q3 2021,  
**1 in every 108**  
ad impressions  
was dangerous or  
highly disruptive  
to users



## Q3 2021 VIOLATION RATES BY COUNTRY

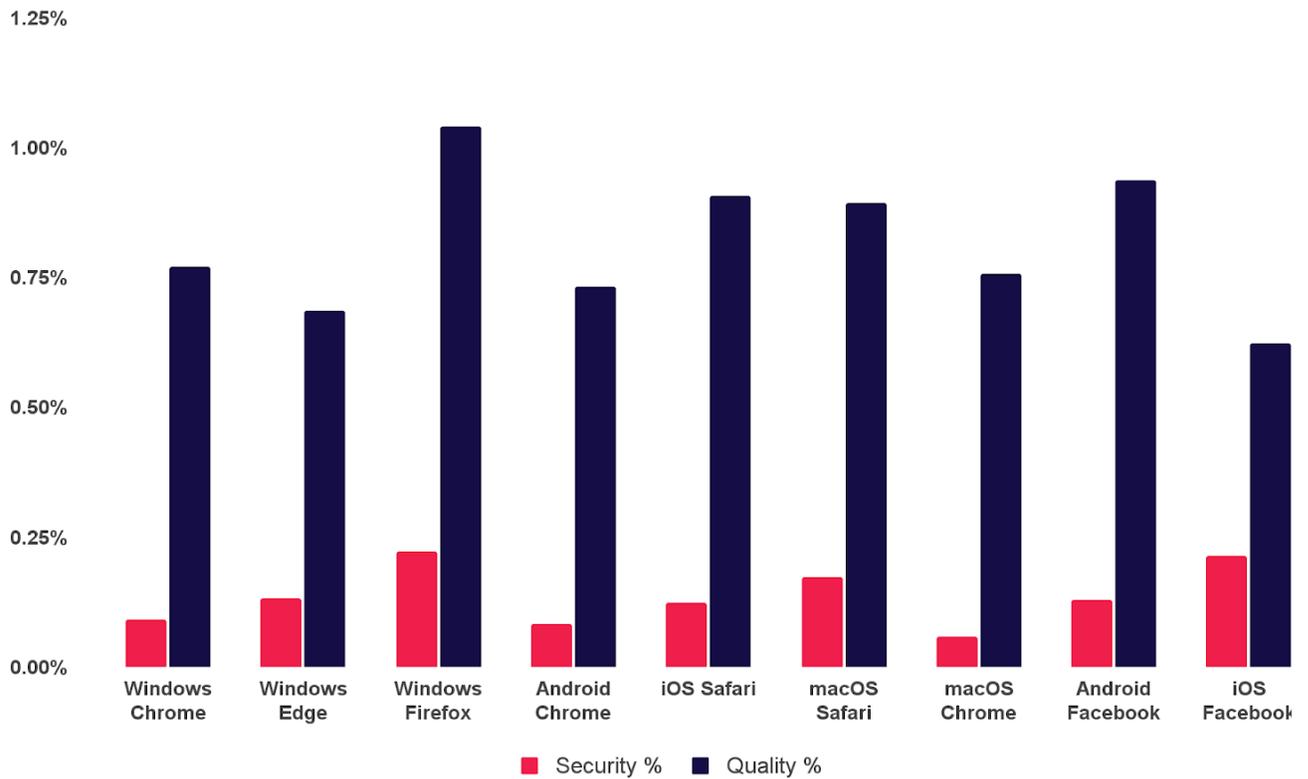


### European markets remained a hotbed for Security

**issues in Q3**, with large increases above Q2 2021 in Germany (168%), Spain (60%), France (478%), and Great Britain (236%).

In a departure from previous quarters, **Q3 Quality violations** outside the U.S. often came close to, or exceeded U.S. levels. **France and Canada in particular saw high rates of Quality issues.**



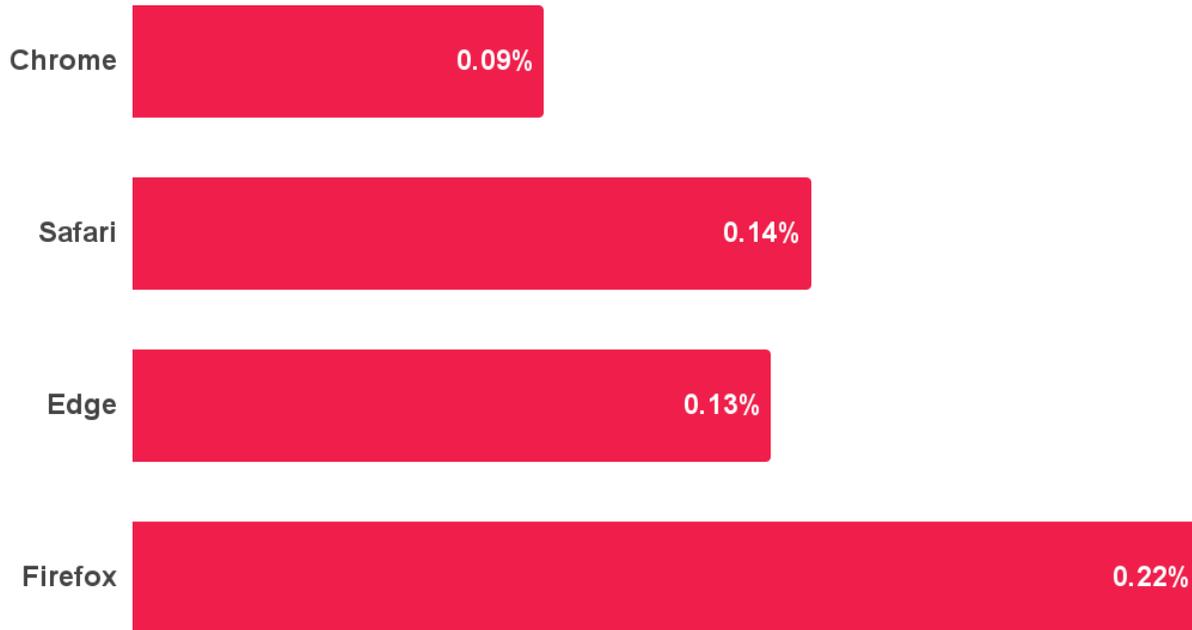


### Q3 2021 VIOLATION RATES BY BROWSER



**Firefox for Windows had the highest rate of Security issues in Q3**, repeating its poor performance from Q2. On mobile devices, the browser integrated into **Facebook for iOS** was the worst performer.

On the other hand, the various versions of **Chrome** generally had the lowest **Security violation rates**.

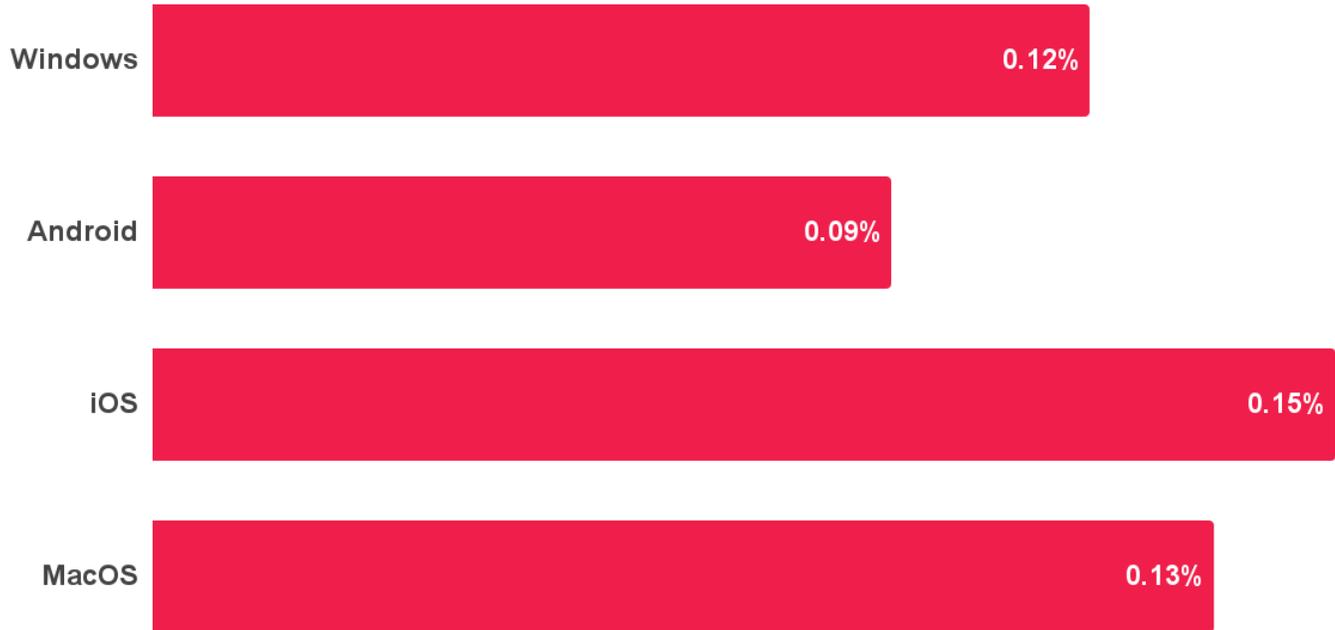


## Q3 2021 SECURITY VIOLATION RATES BY BROWSER FAMILY



Most browsers are available for multiple operating systems and devices. When browsers are grouped as a family, interesting patterns emerge. In Q3, we found that, **compared to Chrome, Firefox was more than twice as susceptible to security issues** and **Safari was 64% more susceptible**. That said, we saw significant increases in violations across all browser families.

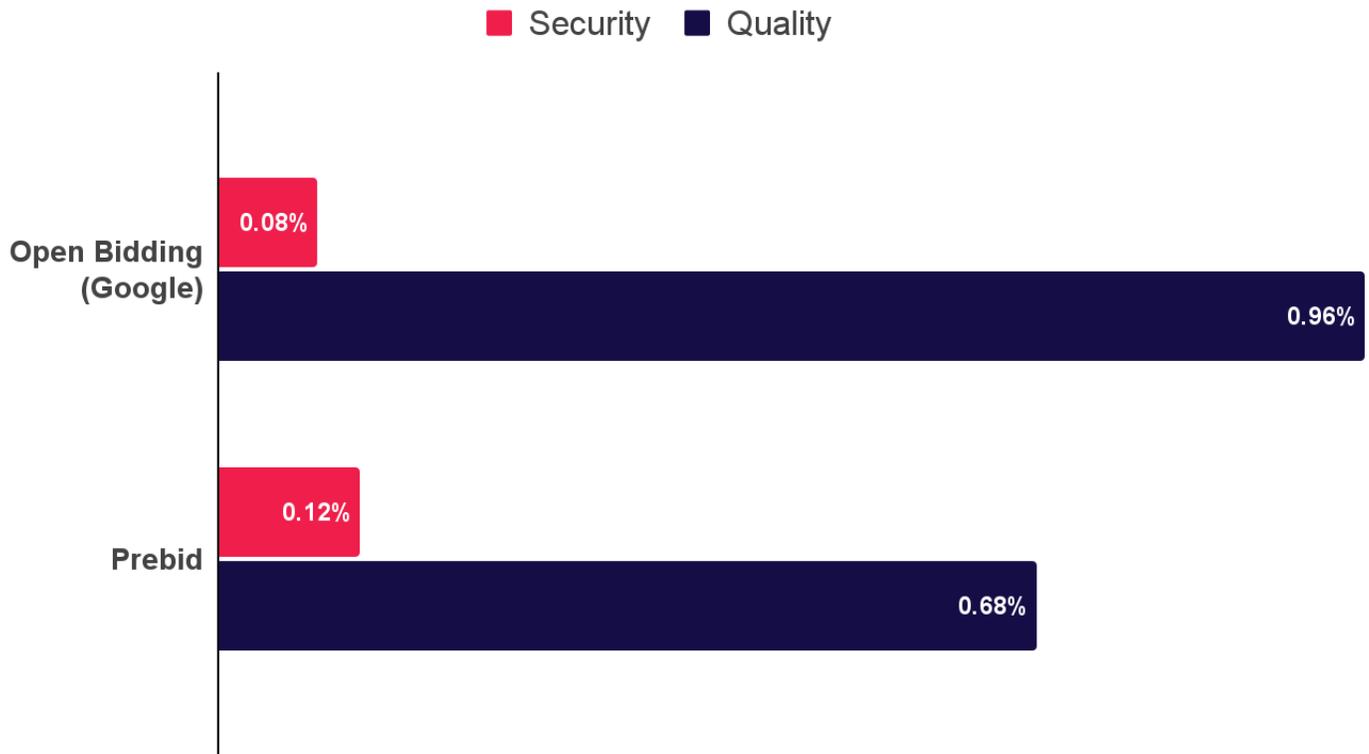
**...Safari was 64% more susceptible to security issues.**



## Q3 2021 SECURITY VIOLATION RATES BY OPERATING SYSTEM



Security rates also vary by operating systems sometimes significantly. In Q3, we found that **Apple's operating systems, iOS and MacOS, were more susceptible to Security issues** than either Windows or Android, going against conventional wisdom. In the most extreme example, **iOS's security violation rate was 60% higher than Android's.**

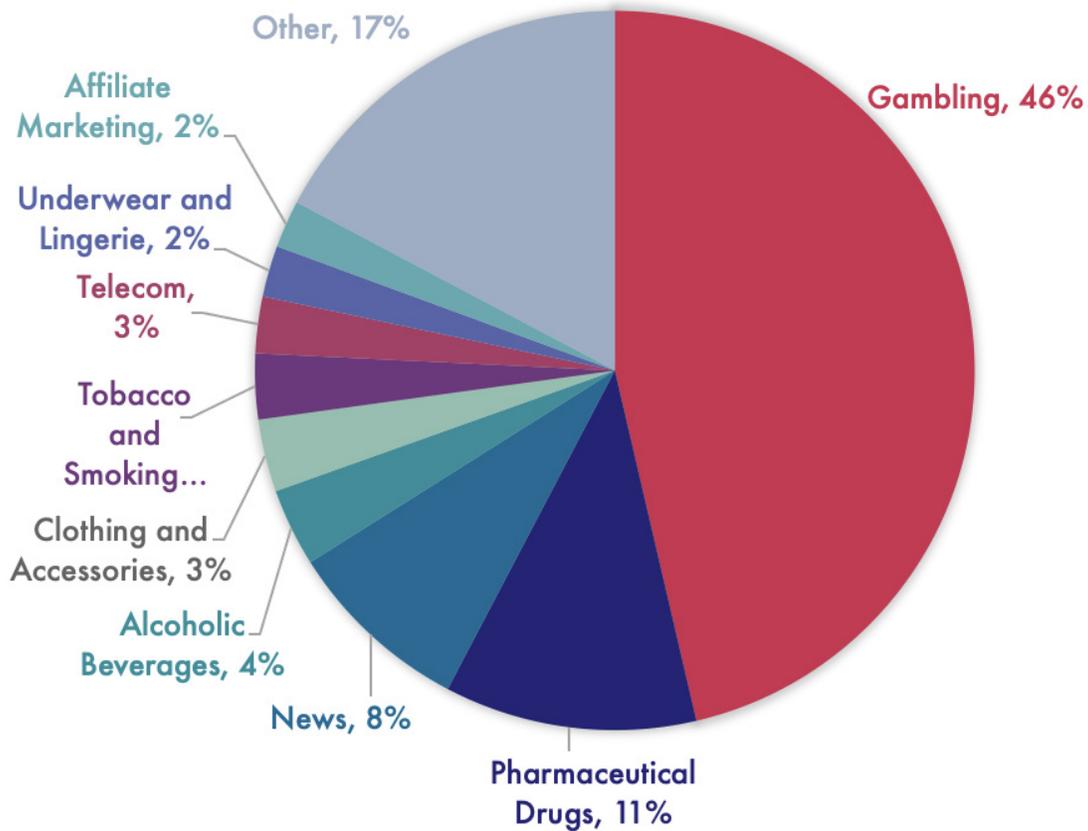


### Q3 2021 VIOLATION RATES BY HEADER BIDDING FRAMEWORK



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.

**Google Open Bidding outperformed Prebid on Security issues in Q3**, but the gap has narrowed considerably over the past few quarters. In addition, Open Bidding fell behind Prebid on Quality issues for the first time in 2021.



"Other" includes over 100 other categories

## 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.

In Q3, **Gambling and Pharmaceutical Drugs** repeated as the most blocked ad categories, collectively representing over 50% of all blocking activity. Meanwhile, blocks for Political Advertising and Real Estate fell off the map and were replaced with **News and Clothing and Accessories** in the top 5. **Alcoholic Beverages** rose two spots to become the 4th most blocked category.



# SSP RANKINGS

**Q3 2021**



## Q3 2021 US SSP RANKINGS

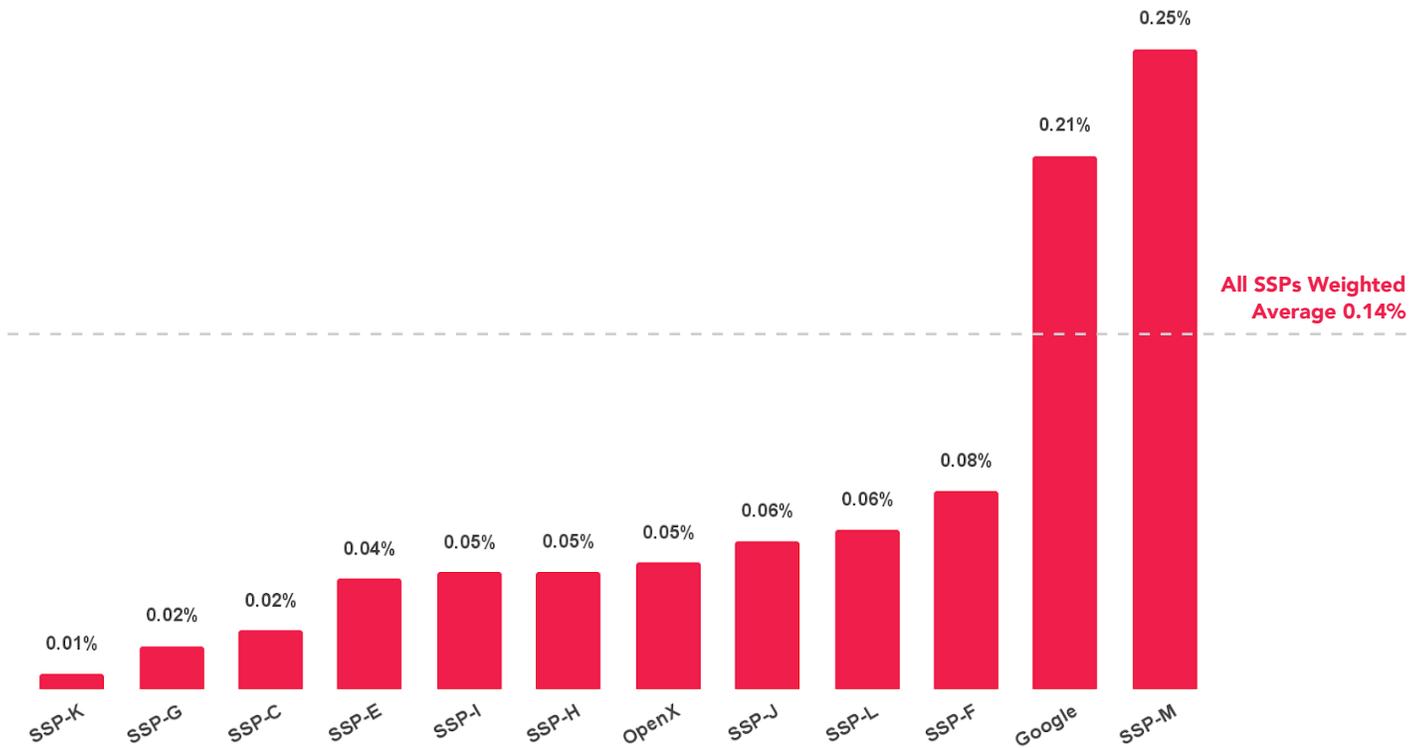
In Q3, Confiant tracked impressions from over **100 SSPs**. However, the vast majority of **global impressions originated from just 12 providers**<sup>1</sup> commonly used by publishers. These 12 providers are noted in the charts that follow using a coding system that carries over from one quarter to the next to allow comparisons over time.

To qualify for inclusion, a provider had to have been a consistent source of **at least 1 billion Confiant-monitored impressions** a quarter across our global sample.

We identify two SSPs in these rankings: **Google** 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.

---

<sup>1</sup> Google, Magnite, OpenX, Xandr, Yahoo, Index Exchange, Pubmatic, Sonobi, TripleLift, Sharthrough/DistrictM, 33Across, and Sovrn

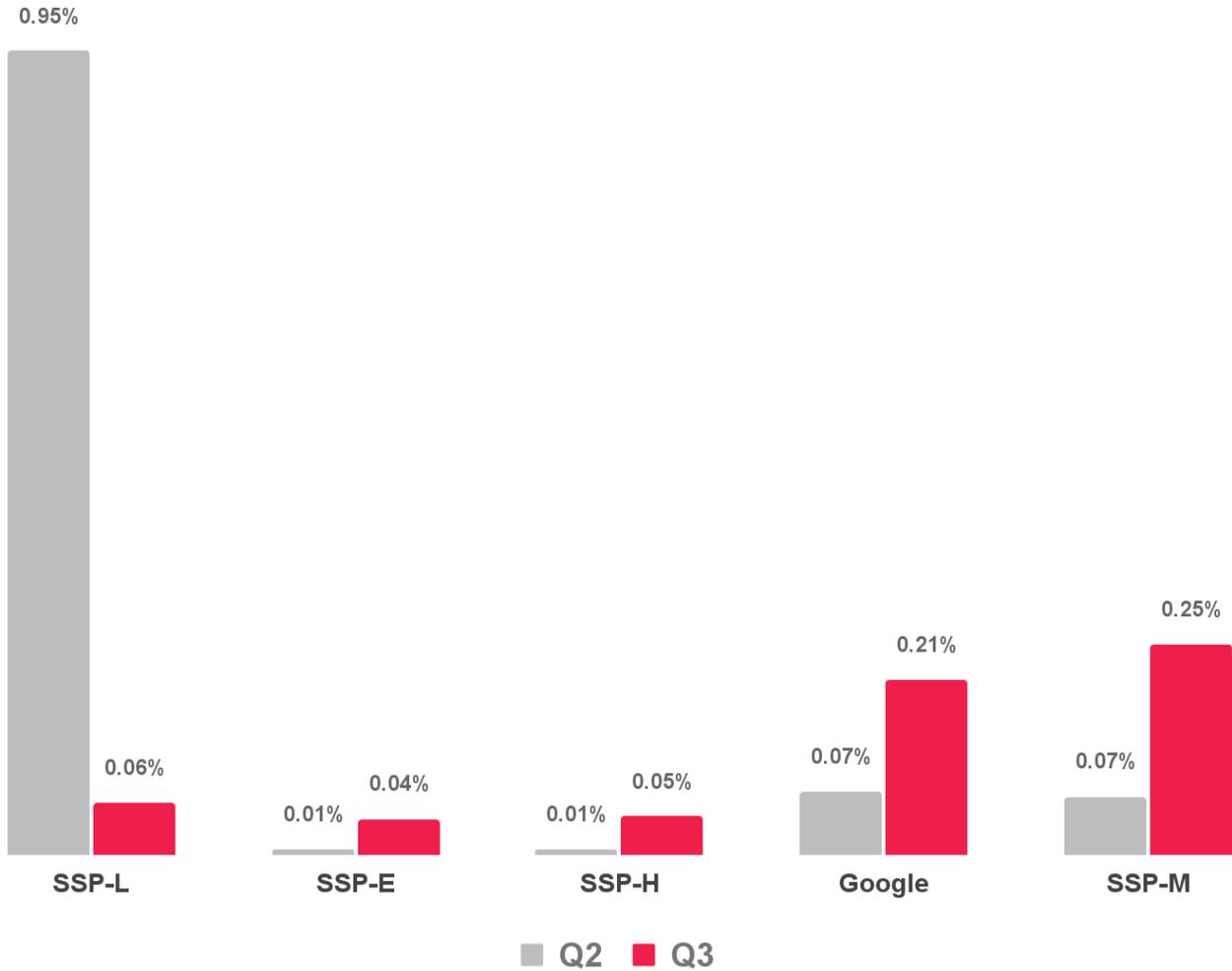


## SECURITY VIOLATION RATE BY SSP



**Google's performance on Security continued to deteriorate after two previous quarters of struggles.** Google's Security violation rate exceeded the industry average by 48% and they ranked 2nd to last among all top SSPs. **SSP-M's Security violation rate more than tripled from Q2 to Q3, moving them from 10th place to dead last.**

**SSP-K took the top spot**, with a Security violation rate of only 0.01%.

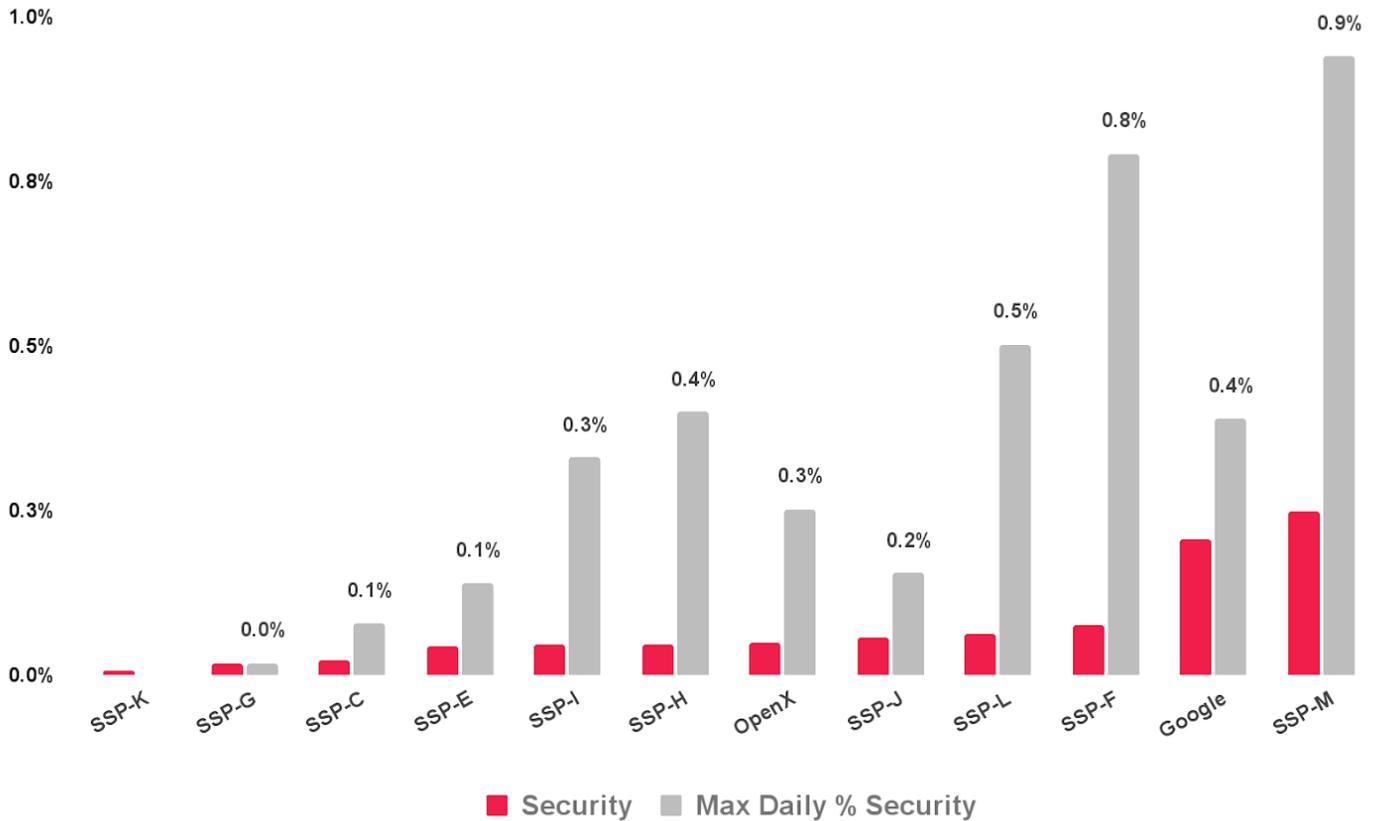


## SECURITY VIOLATION RATE: Q2 VS. Q3



**SSP-L reduced their Security violation rate by over 90%**, making them the quarter's most improved SSP.

Meanwhile, SSPs E and H had large increases in violation rate (but from low levels), while **Google and SSP-M saw their violation rates more than triple from already high levels.**

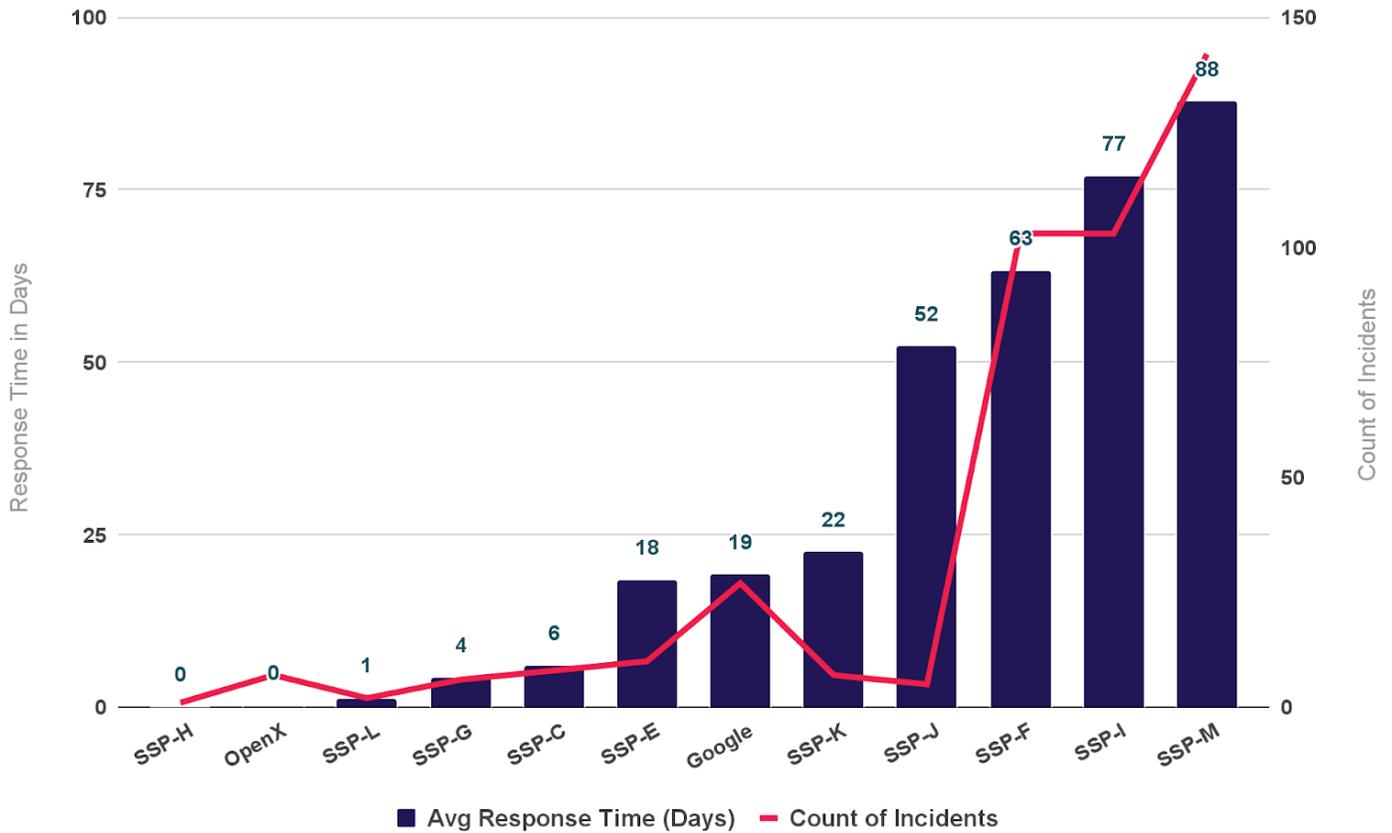


## DAILY MAXIMUM MALICIOUS RATE BY SSP



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.

Matching their poor performance in overall Security rate, **SSP-M had the highest maximum violation rate among the top SSPs, nearing 1%.**

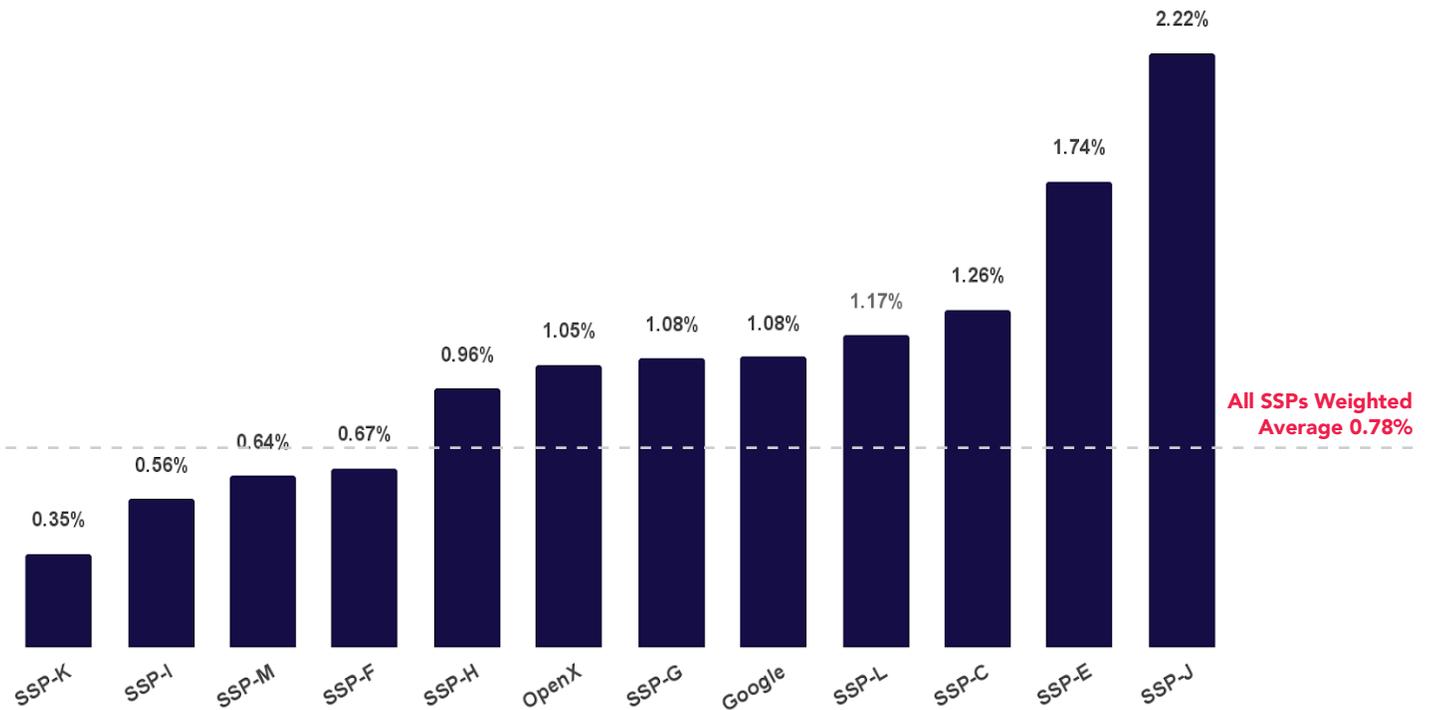


## AVG DURATION OF ATTACK BY SSP IN Q3



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 Q3, **OpenX reduced their average response time from 22 days to less than a day**, and SSP-H reduced theirs from 5 days to less than a day. On the other end of the spectrum, **SSP-M had the slowest response rate and the highest number of incidents**, perhaps no surprise given their last-place showing in Security.



## QUALITY VIOLATION RATE BY SSP

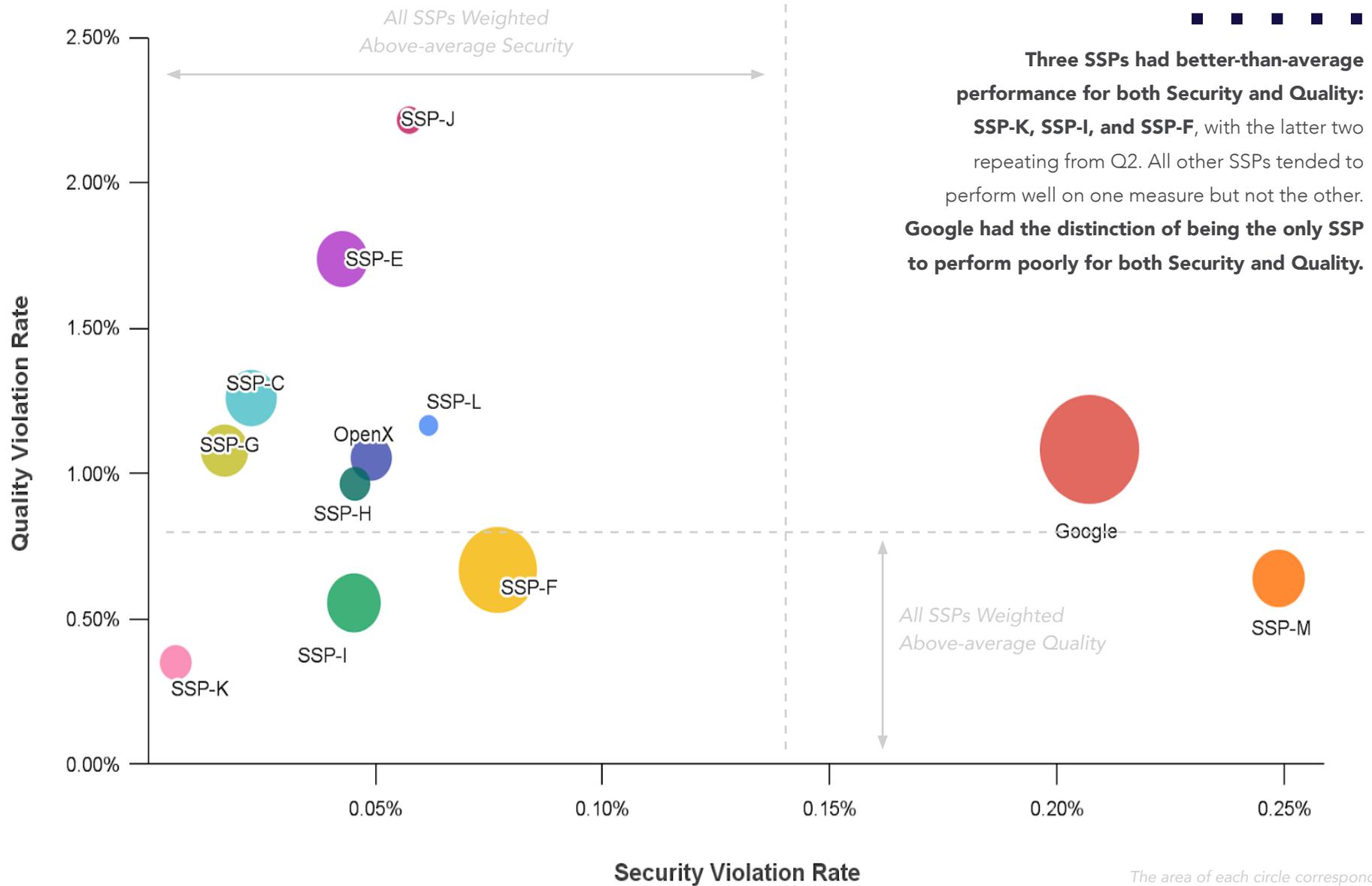


**Quality violations** are based on a diverse set of controls that publishers can activate on the Confiant platform. Examples include **misleading ads, heavy ads, and pop-ups**. These rules correspond to ad behaviors that disrupt or impair the user experience.

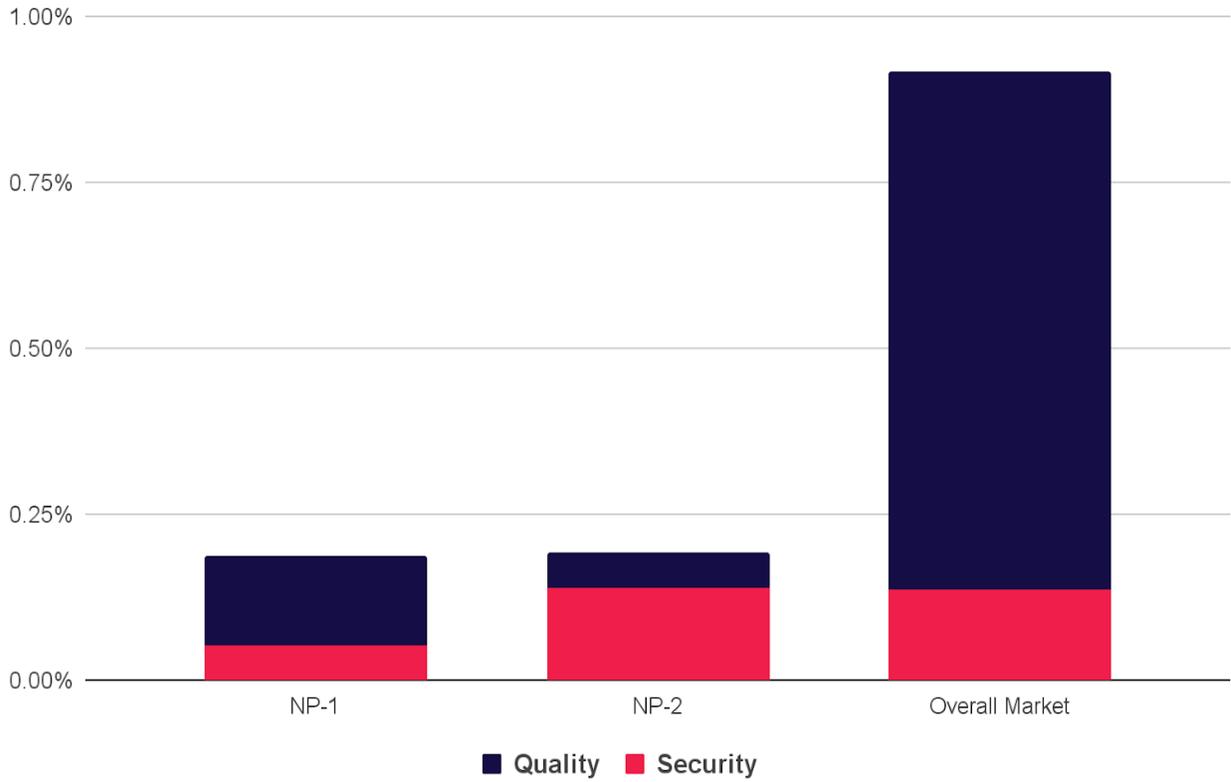
**SSP-J continued to suffer from quality issues, finishing in last place** after a poor showing in each of the last five quarters. **SSP-K vaulted to the top spot**, followed by last quarter's leader, SSP-I.



## Q3 VIOLATION RATES BY SSP SIZE



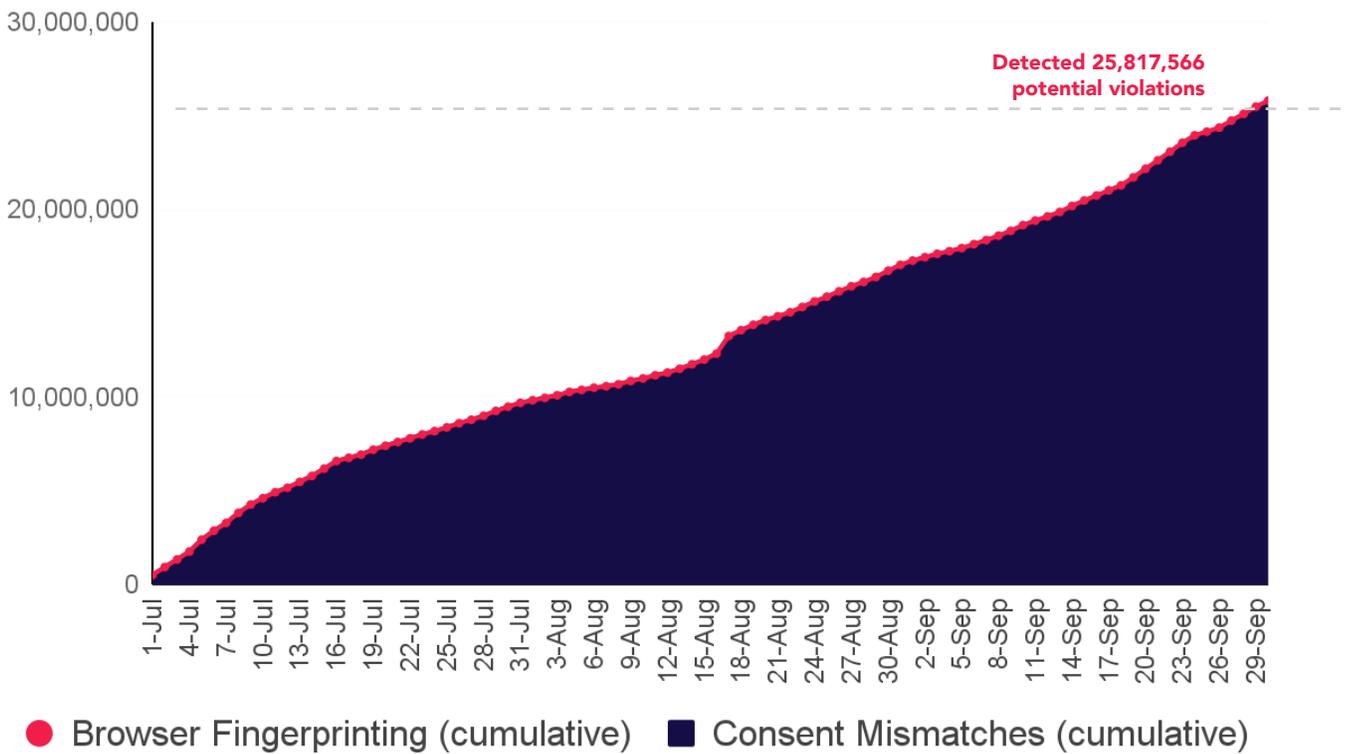
*The area of each circle corresponds to the size of the SSP in terms of impressions delivered*



## SPECIAL REPORT: NATIVE ADVERTISING



Confiant covers dedicated on-page Native ad units in addition to both banner and native demand served into standard display ad units. **The two largest providers of on-page Native ad units compare well to the overall market**, showing much lower rates of Quality issues (primarily Misleading Ads) and equal or better rates of Security issues (primarily Criminal Scams).

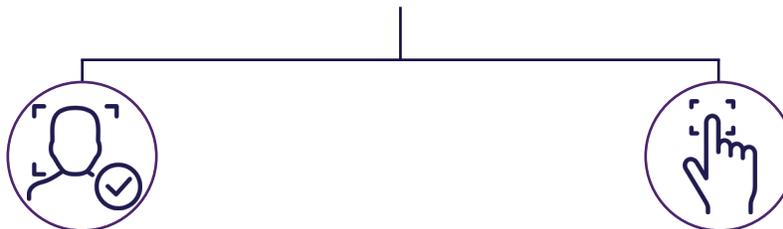


## SPECIAL REPORT: PRIVACY COMPLIANCE VIOLATIONS



Over the course of Q3, **Confiant detected nearly 26 million probable GDPR and CCPA violations.**

Detections fell into one of two buckets:



### **Consent mismatch**

A mismatch detected between the tracking behavior of an ad and the consent given by a user.

### **Browser fingerprinting**

Detection of attempts to use various browser and device parameters to create a unique fingerprint of a user.

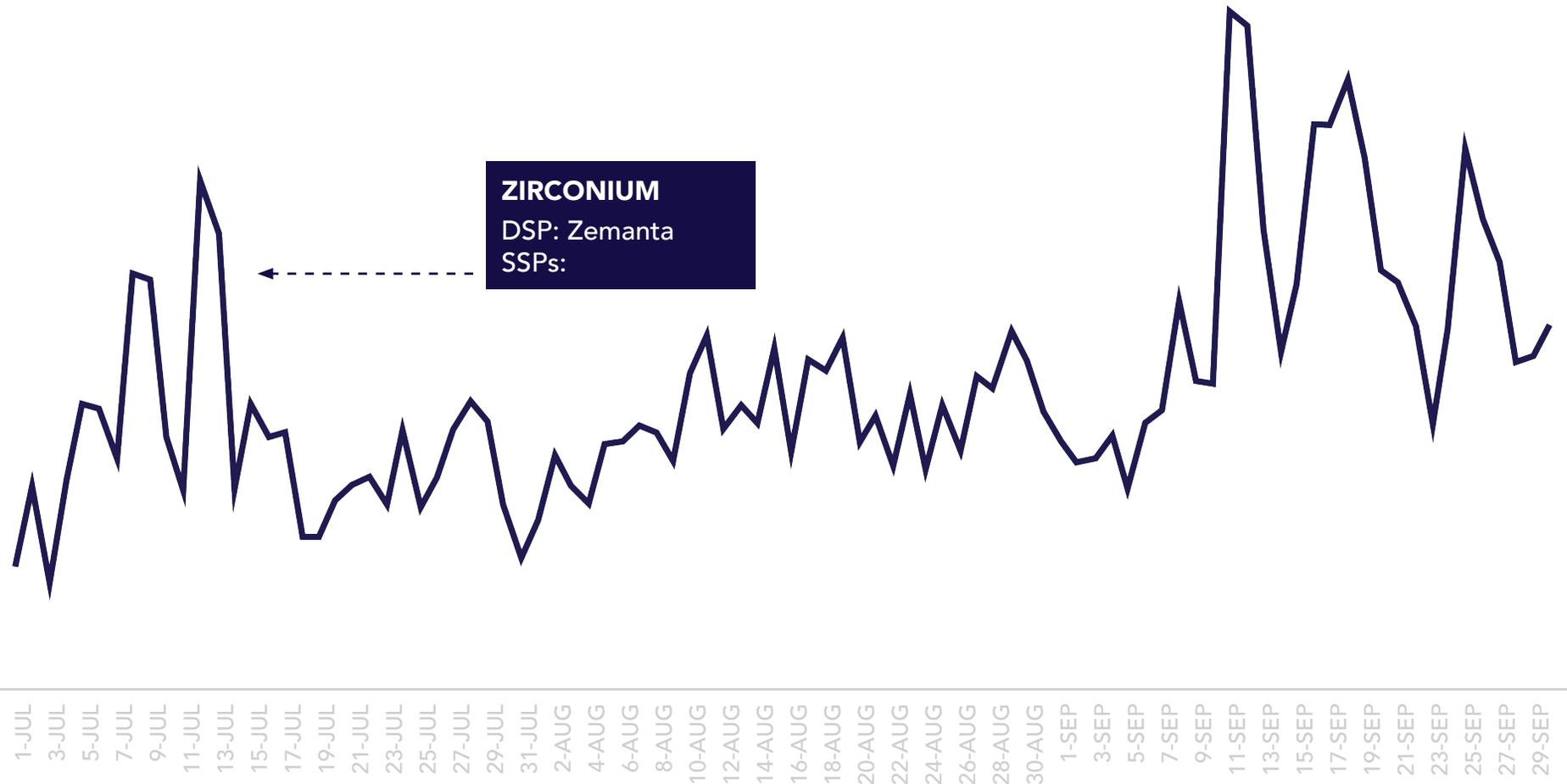


# MAJOR THREAT GROUPS ACTIVE IN Q3

**Q3 2021**

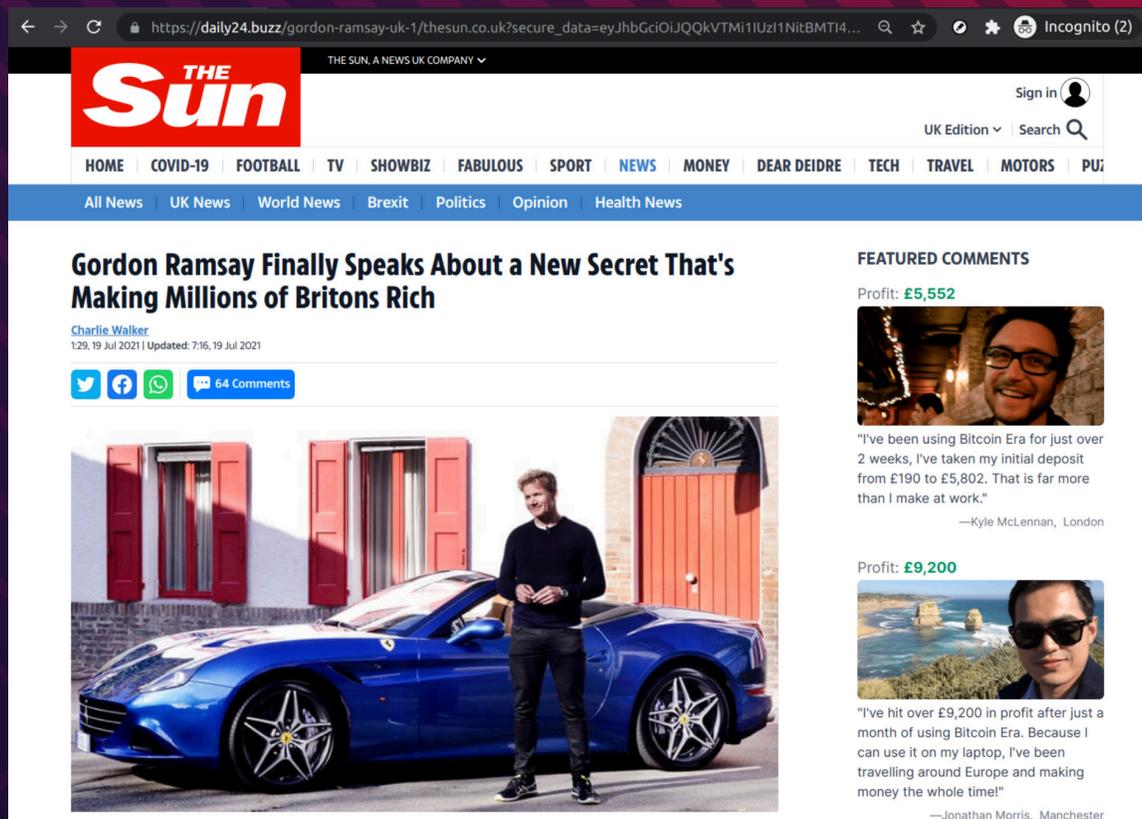


# NOTABLE THREAT ACTIVITY



# ZIRCONIUM

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



## PEAK ACTIVITY: JULY

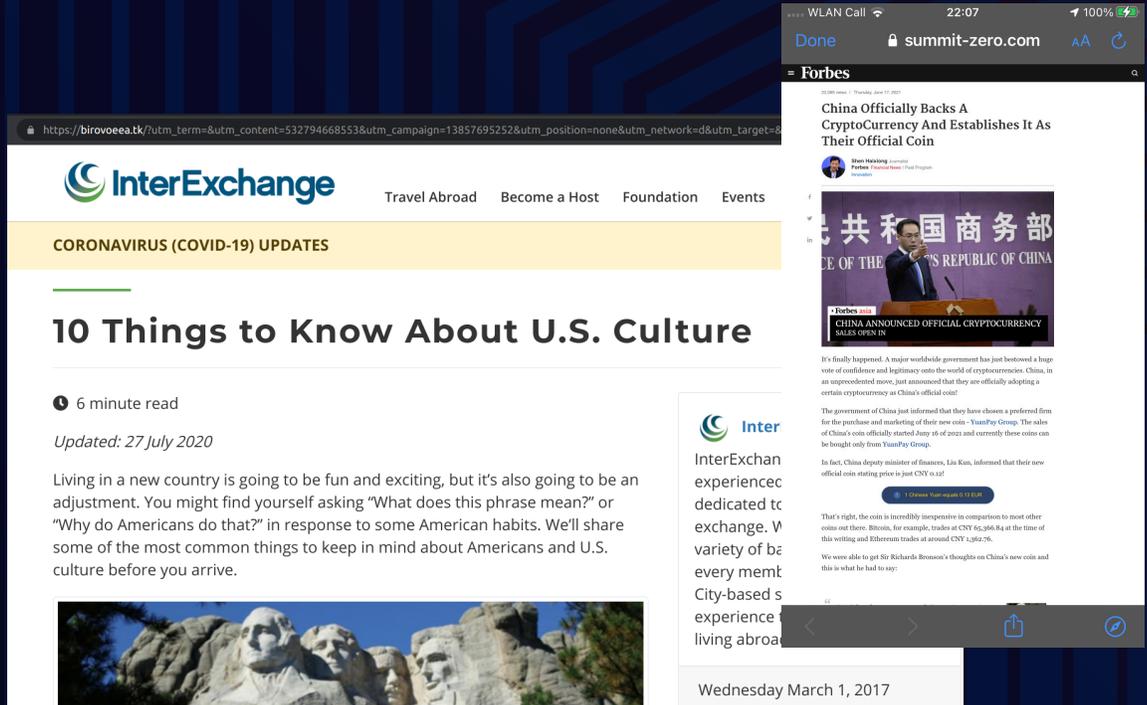
For years, Zirconium have used their understanding of Ad Tech in order to form dozens of convincing business entities to gain seats on major buying platforms.

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.

# MALICIOUS CLICKBAIT ATTACKS

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



PEAK ACTIVITY:  
**ONGOING**

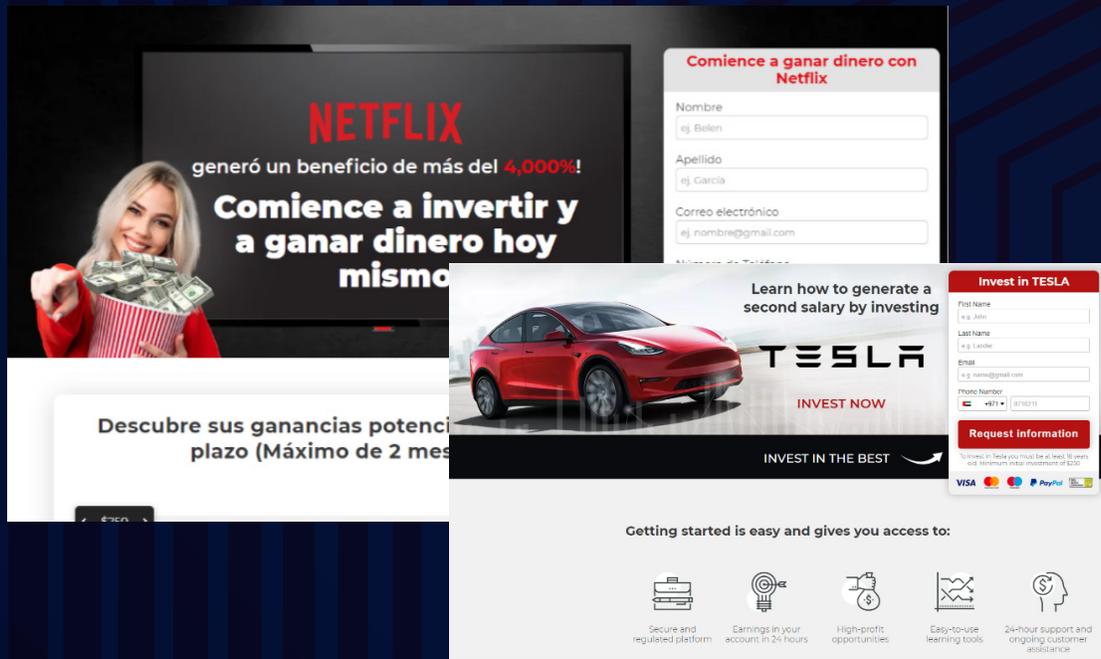
These days, most malvertising falls under the category of "Malicious Clickbait". The attackers will launch a display ad campaign for a benign looking brand and then "flip" the creative to some clickbait messaging — usually a celebrity-endorsed investment opportunity.

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.

# 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

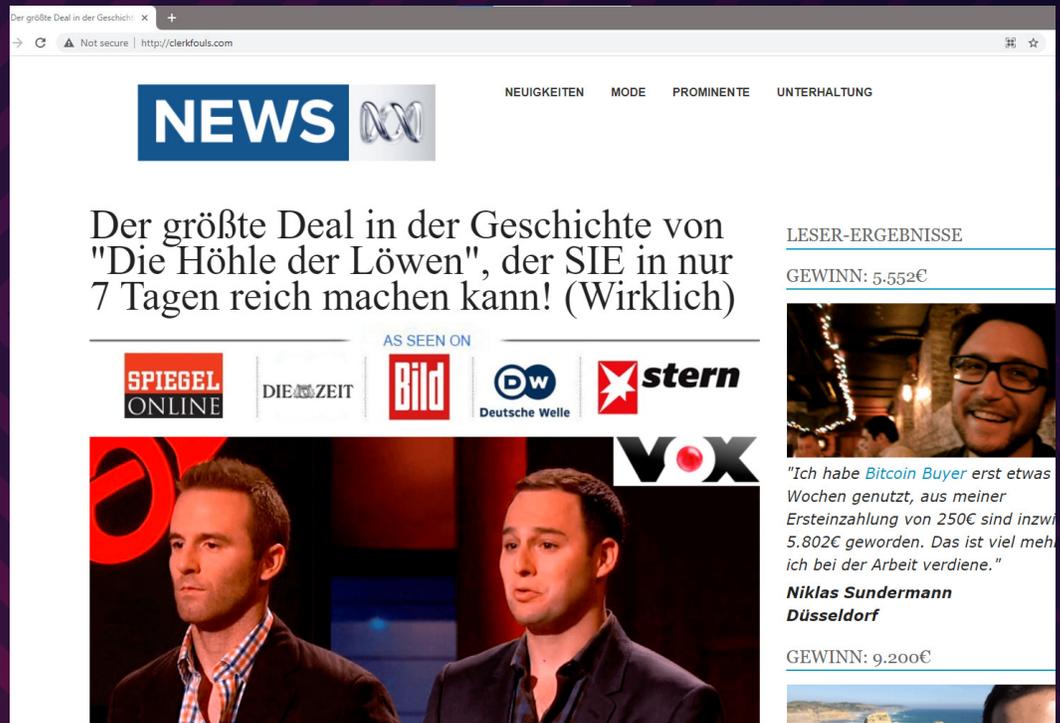
While not a specific malvertising threat actor, we wanted to highlight a cluster of investment firms primarily based in Cyprus that sit at the end of the kill chain for a large amount of malvertising scams.

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.

BRS

The group is very adept at establishing a broad media buying presence, running obscure campaigns that evade scrutiny, employ cloaking, and utilize a thorough sales funnel.



PEAK ACTIVITY:  
ONGOING

While cloaked clickbait might be the name of the game for most of the dominant malvertisers in 2021, they are certainly not all created equal.

The BRS group, for example, specializes specifically in promoting dubious Bitcoin investment opportunities via convincing fake news websites, and of course fugazi celebrity endorsements.

The group is very adept at establishing a broad media buying presence, running obscure campaigns that evade scrutiny, employ cloaking, and utilize a thorough sales funnel.



## CONCLUSION

-  **Violation rates for both Security and Quality jumped significantly in Q3** compared to Q2, with the **Security violation rate nearly tripling** and the **Quality violation rate rising for the fifth consecutive quarter**.
-  **Google once again underperformed the industry for Security**, coming in at nearly 50% above the industry average. Google's Security violation rate tripled from Q2 to Q3.
-  Misleading Claims and Heavy Ads remained top Quality issues, with **Heavy Ads increasing nearly 50% in prevalence**.
-  **Gambling remained the most-blocked ad category by a wide margin**, but it was joined by **News** in the top three.
-  **1 in every 108 impressions was dangerous or disruptive** to the user.

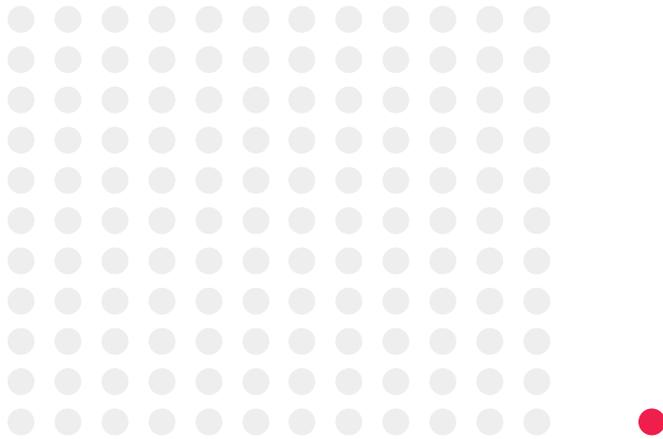


# ABOUT CONFIANT

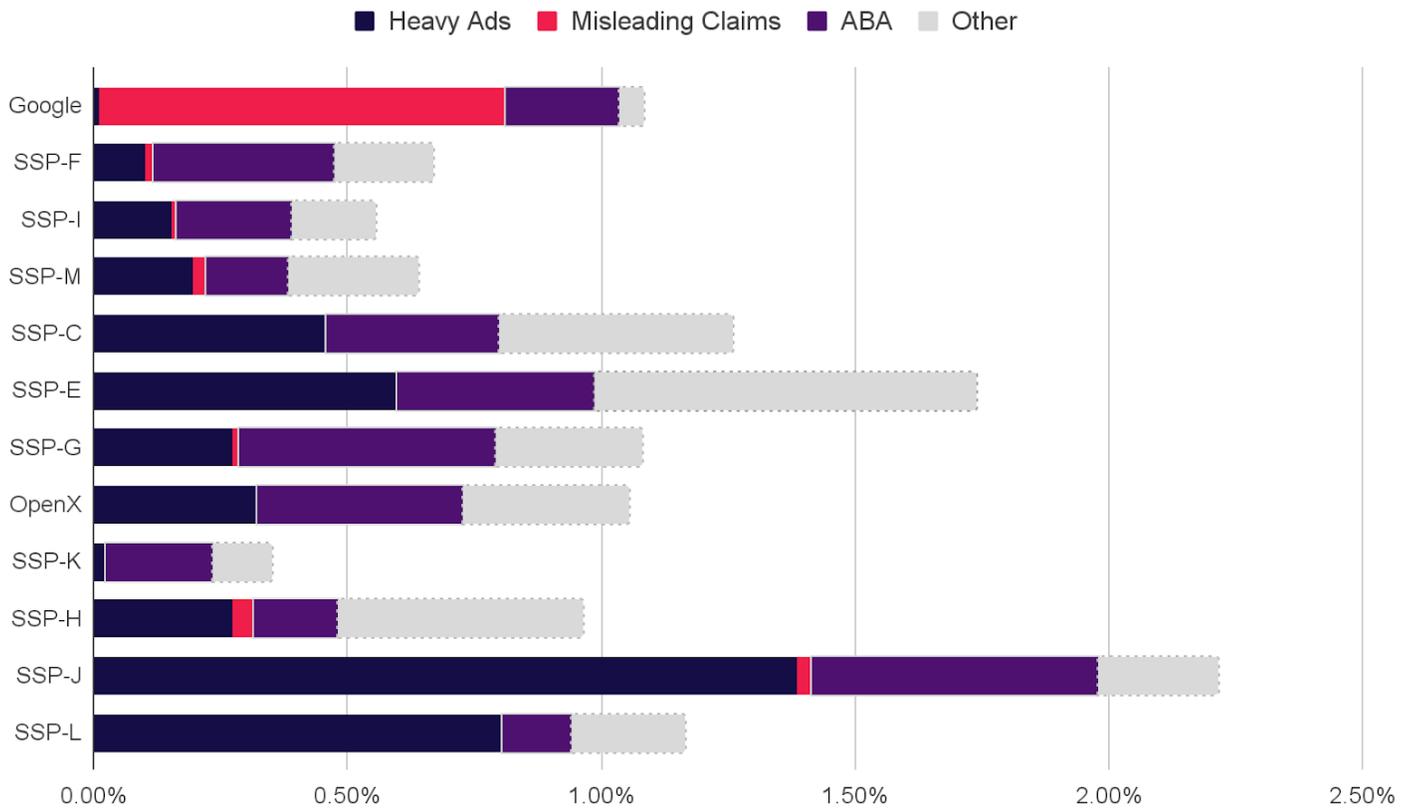
Confiant's mission is to make the digital world safe for everyone. We defend the digital ad industry by helping publishers and ad platforms protect their users and take back control of the ad experience from rogue actors. Our solution protects reputation, revenue, and resources by providing real-time verification of digital advertisements.

By providing industry-leading protection from malvertising, disruptive ads, and privacy risks, Confiant empowers premium ad platforms and publishers with actionable data to ensure the digital ad ecosystem is safe and secure for everyone. We protect hundreds of billions of impressions per month for our clients, which include CBSi, Magnite, Gannett, and Politico.

[LEARN MORE](#)



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

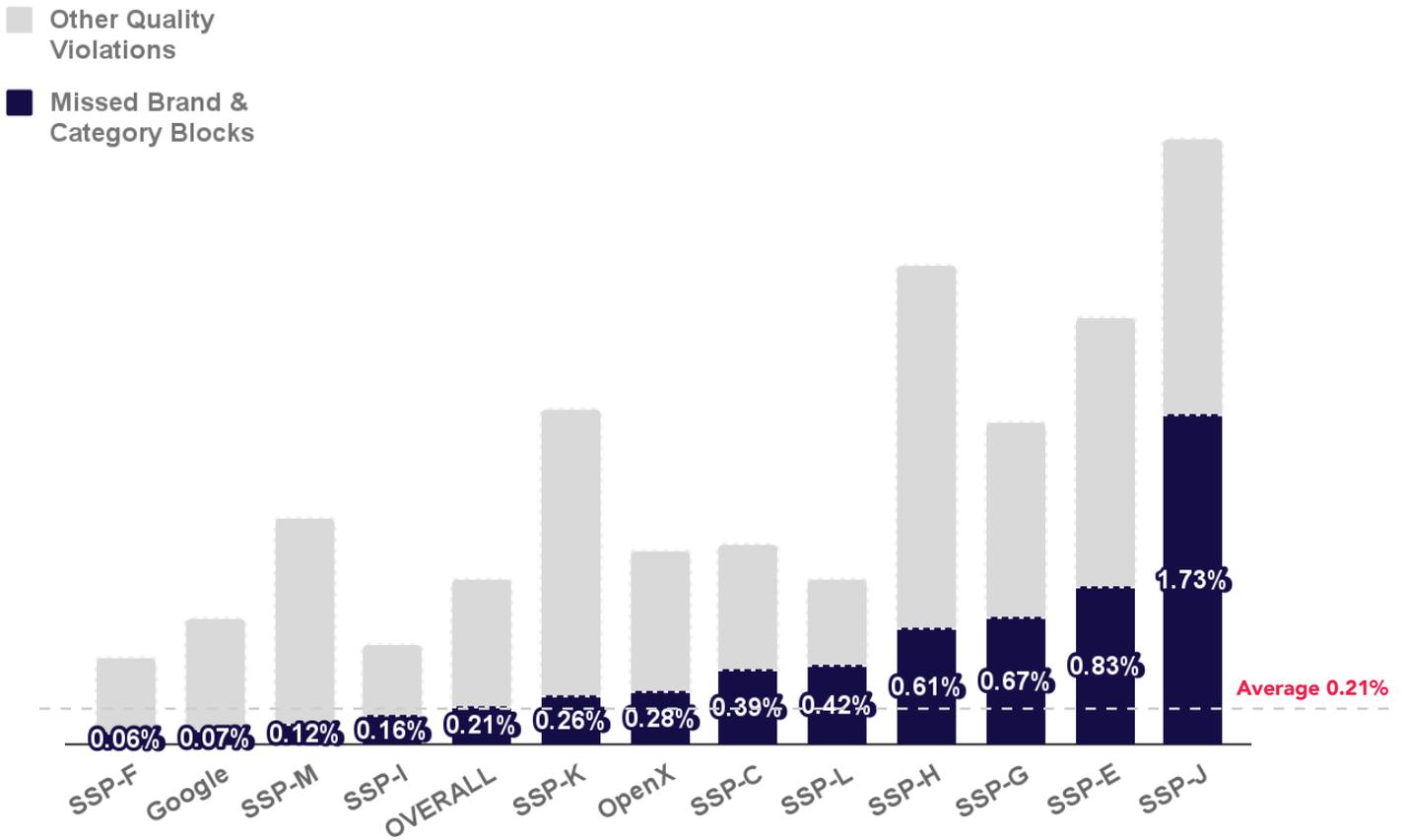


## QUALITY ISSUES DEEPAIVE



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.



## 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.



MALVERTISING + AD QUALITY INDEX

# MAQ INDEX

---

[CONFIANT.COM/MAQINDEX](https://confiant.com/maqindex)

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

email us at:

[MARKETING@CONFIANT.COM](mailto:MARKETING@CONFIANT.COM)

**Q3 2021**