Malvertising and Ad Quality Index

The Foremost Benchmark Report on
Digital Ad Quality, Security, and Privacy.

2023

January 1st - December 31st

INTRODUCTION

Confiant's **Malvertising and Ad Quality (MAQ) Index** is a view into creative quality and security in digital advertising. Using a sample of more than one trillion impressions monitored in real time, 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. The MAQ was the industry's first and is still the leading systematic study 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 issues facing the industry.

In 2018, Confiant released the industry's first benchmark report. This report, the 19th in the series, covers the entirety of 2023.

METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of more than **1.1 trillion advertising impressions** monitored from January 1 to December 31st, 2023, across tens of thousands of premium websites and apps from top publishers.

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.

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. In H1 2022, we refactored our Quality score to remove an issue that was largely outside of the SSP's control. As a result, some historical metrics in this report may not match those in prior reports.

DEFINITIONS

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]

Quality Violations

Non-security issues related to **ad behavior, technical characteristics,** or **content**.

Top issues include:

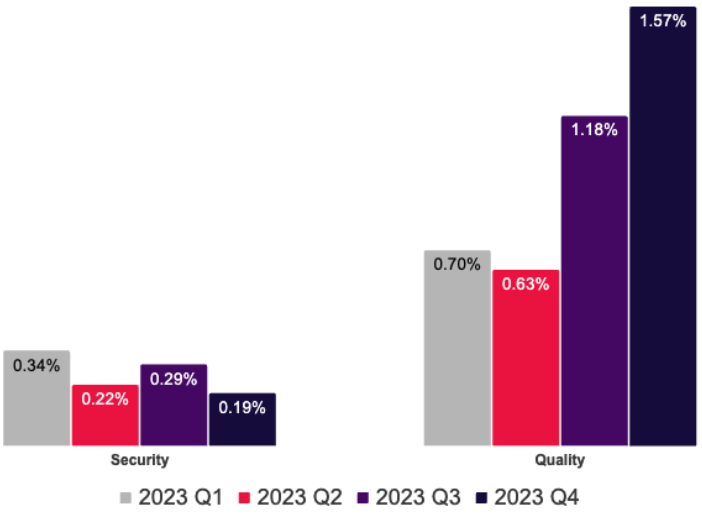
- **Heavy Ads (including Chrome Heavy Ad Intervention)**
- **Misleading Claims**
- **Video Arbitrage (formerly In-Banner Video)**
- **Undesired Audio**
- **Undesired Video**
- **Undesired Expansion**

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

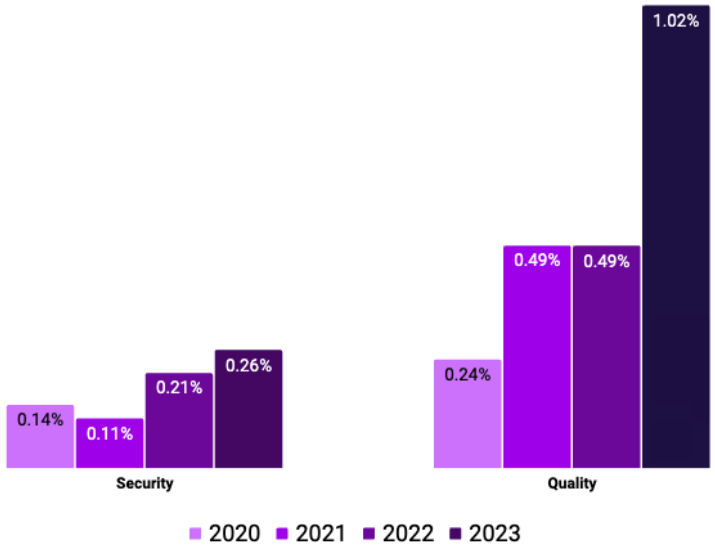

CONFIANT
Industry View
2023

In 2023,
one in every 79
impressions was
dangerous or
highly disruptive
to the end user.

Quarterly View



Annual View

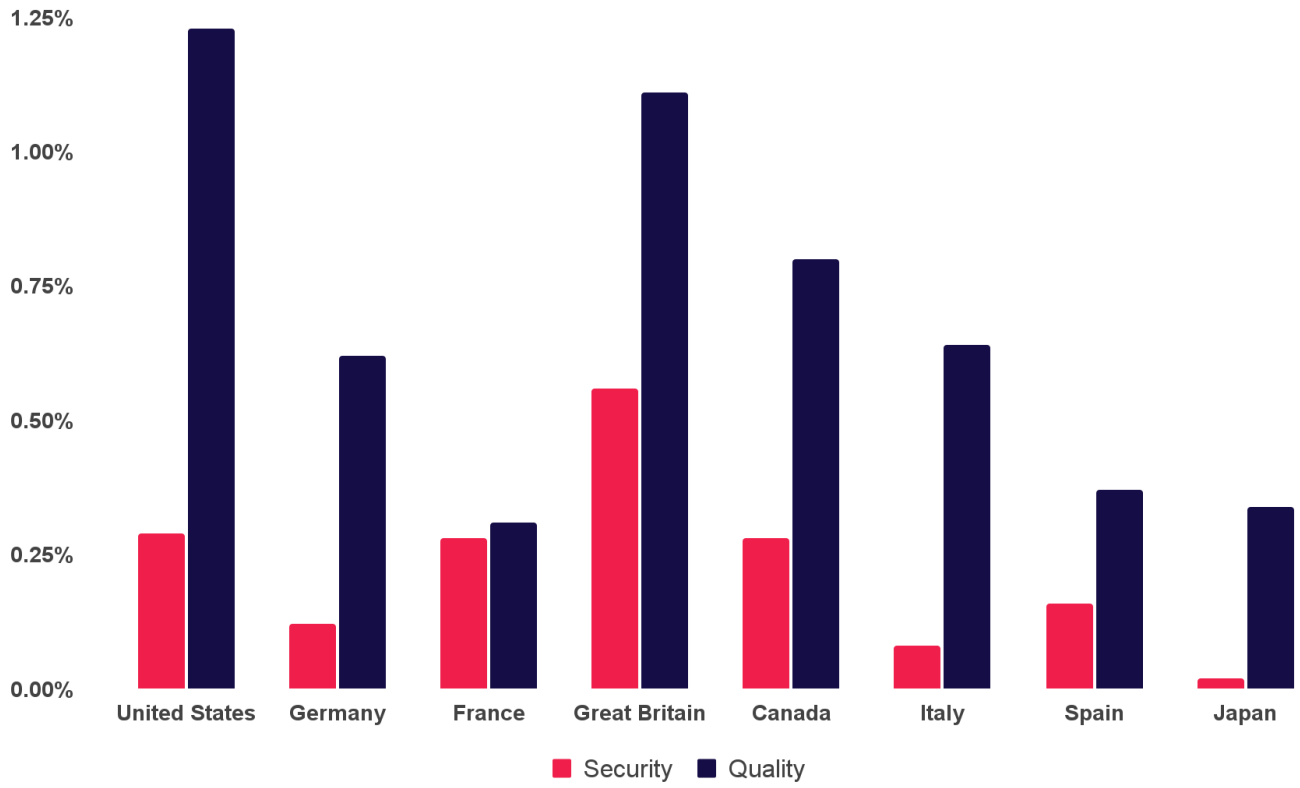


How did the industry fare?

The industry-wide security violation rate rose for the third straight year, averaging 0.26% for 2023. Only Q4's security violation rate was lower than the previous year's overall security violation rate. The beginning of 2023 saw intense attacks from cloaked ads.

In only half a year, the industry-wide ad quality violation rate more than doubled from 0.63% to 1.57%. This uplift was fueled by Heavy Ads.

The quality violation rate in Q4 2023 was the highest level since 2018.

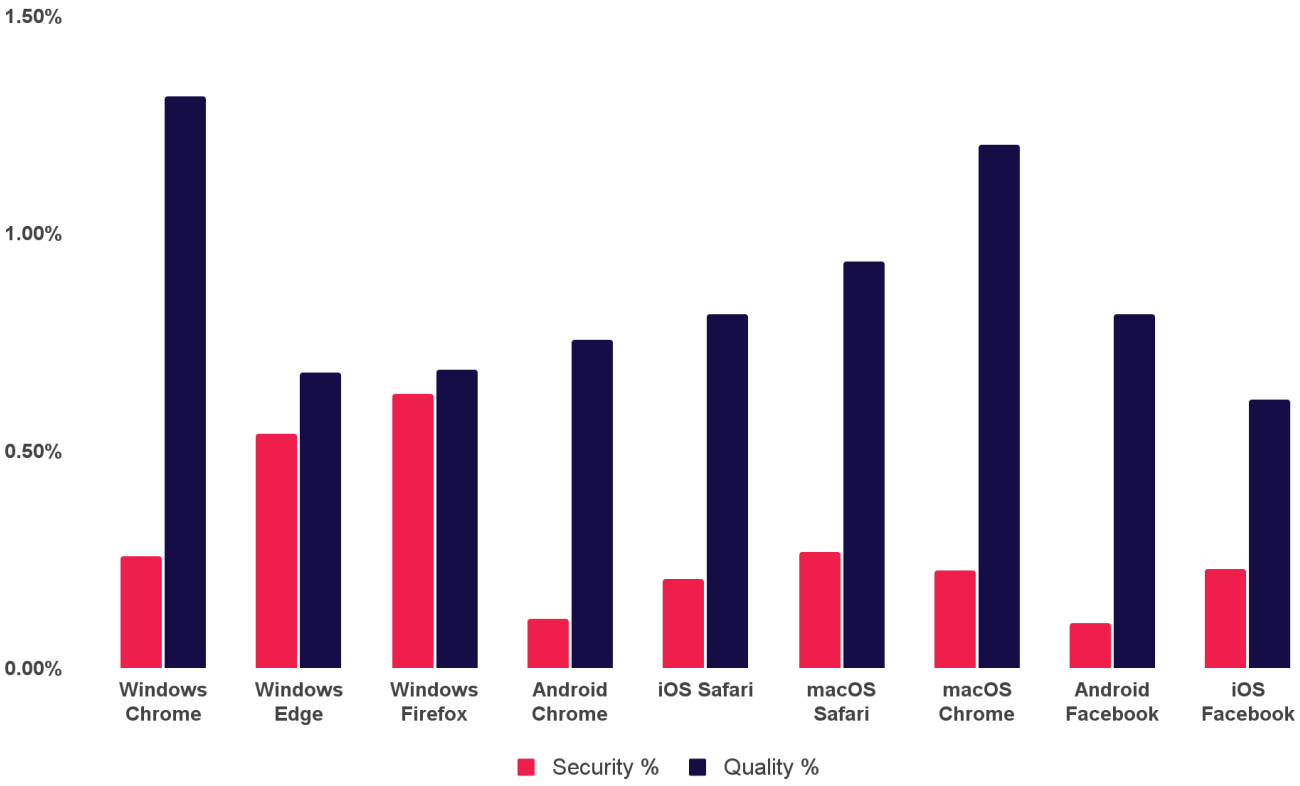


2023 Violation Rates by Country

Compared to 2022 averages, **almost every country had significant increases in quality issues in 2023, with the USA, France, Italy, and Spain seeing their rates double.** Only Japan bucked this trend with a declining quality violation rate.

Great Britain had the highest rate of Security issues for 2023, coming in at 0.56%, nearly double the USA - the second highest. **Italy and Japan were the safest markets.**

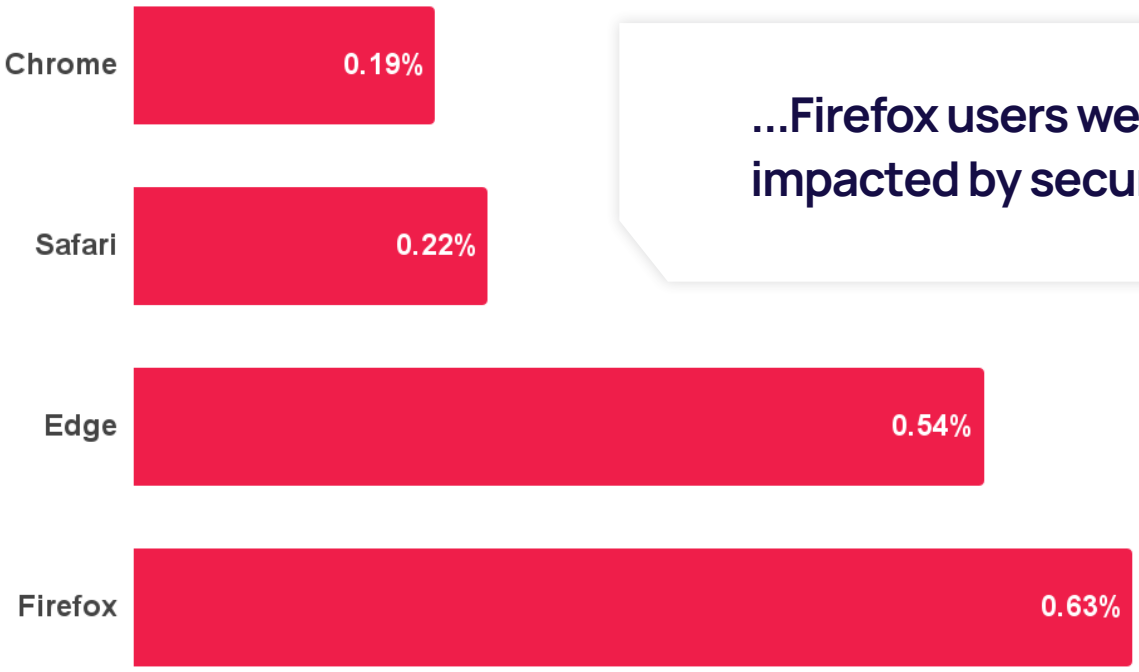
The Quality violation rate was highest in the USA, Great Britain, and Canada. Great Britain had both the highest Security and Quality violation rates in H1 2023, and nearly so for 2023 overall.



2023 Violation Rates by Browser

Throughout all of 2023 (in both H1 and H2) **users of Firefox for Windows experienced the highest rate of security issues**, with Windows Edge users in a close second place.

Conversely, **Chrome performed well for security issues across all platforms, but relatively poorly for quality issues**, being 1st, 2nd, and 5th worst overall.



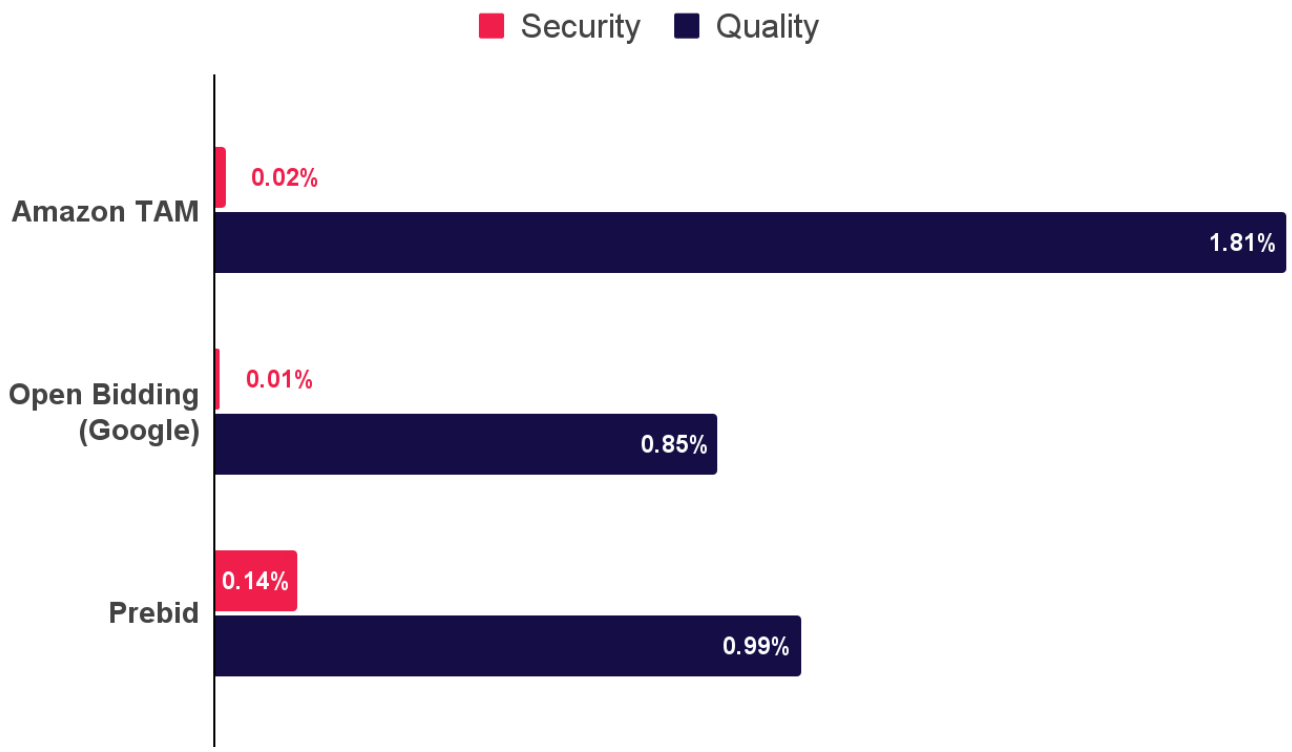
...Firefox users were the most impacted by security issues...

2023 Security Violation Rates by Browser Family

When browsers were grouped as a family across all operating systems and devices, interesting patterns emerged.

In 2023, Firefox users were the most impacted by security issues, continuing the trend it took over from Edge in H1 2023. Safari, and especially Chrome users, were less than half as likely to experience ads with security issues. **Firefox's 2023 security violation average is 0.63%, an increase of over 50% from its 2022 average.**

Of all browsers, only Safari saw a decrease in its security violation rate, at 0.22% compared to 0.26% in 2022.

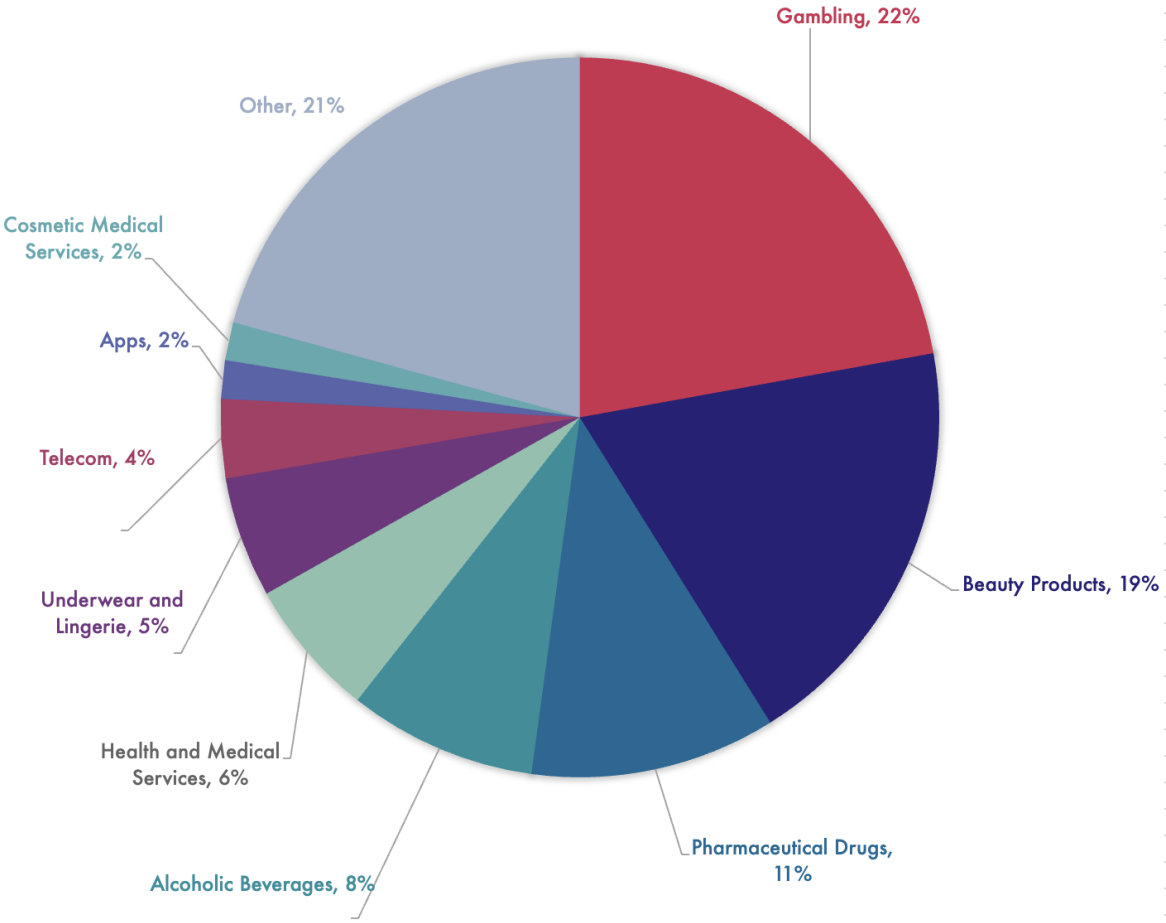


2023 Violation Rates by Bidding Framework

Publishers use frameworks like **Prebid** and **Open Bidding** to manage bidding from multiple SSPs. In both cases, demand from a diverse set of SSPs flows through the framework, exposing publishers to security and quality issues.

In 2023, Google outperformed Prebid and Amazon TAM on both security and quality issues.

All frameworks saw a significant decrease in their security violation rates, but massive increases to their quality violation rates compared to 2022.



"Other" includes over 100 other categories

2023 Most Blocked Ad Categories

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

In 2023, Gambling was the most blocked category, followed by Beauty Products, a category that skyrocketed out of the Other category in 2023. Alcohol and Pharmaceutical Drugs still remain top categories that are blocked. These four categories represent 66% of all blocks in 2023. **Gambling fell from 42% of all category blocks in 2022 to just 22% in 2023.**

Cryptocurrency, Tobacco & Smoking, Sexual Health, and Political Advertising have lost the top spots they held in 2022. The cryptocurrency craze has dissipated, and 2022 included a midterm election in the USA which affected category blocks for political ads. The Other category increased its share from 17% to 21%.


CONFIANT
SSP Rankings
2023

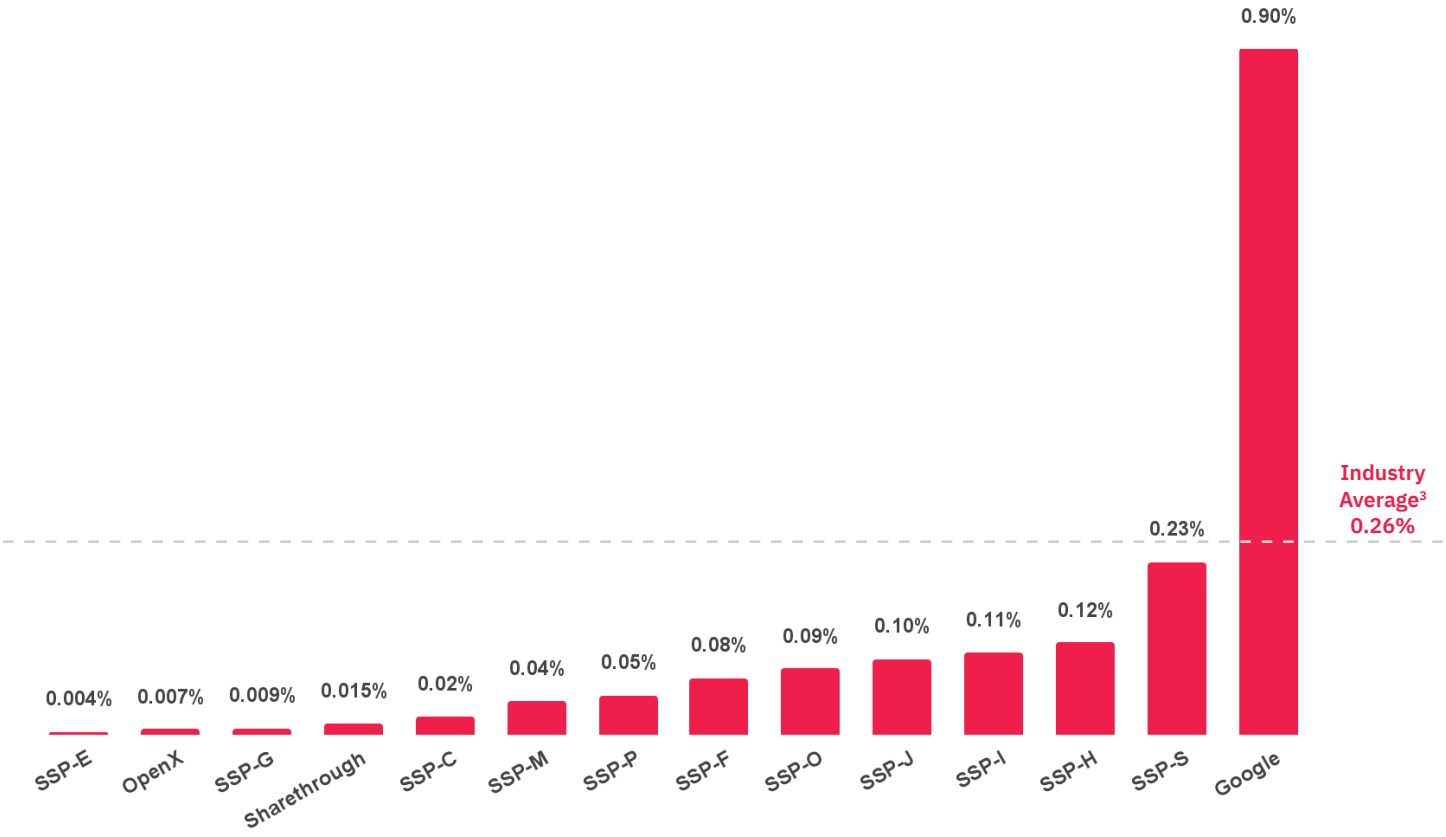
2023 SSP Rankings

In 2023, Confiant tracked impressions from over **100 SSPs and demand sources**. However, the majority of **global impressions originated from only 14 providers**[1] that are commonly used by publishers. These 14 providers[1] 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 per quarter** across a cross-section of publishers in our global sample.

We identify three SSPs in these rankings: **Google, OpenX,** and **Sharethrough**. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. **OpenX** and **Sharethrough** have consented to have their names and their data included in our reports without obfuscation, which is an option we offer to any SSP upon request.

[1] Google, Magnite, TripleLift, OpenX, Xandr, Index Exchange, Pubmatic, Sharethrough, Sovrn, Yahoo, GumGum, Sonobi, Media.net, and YieldMo



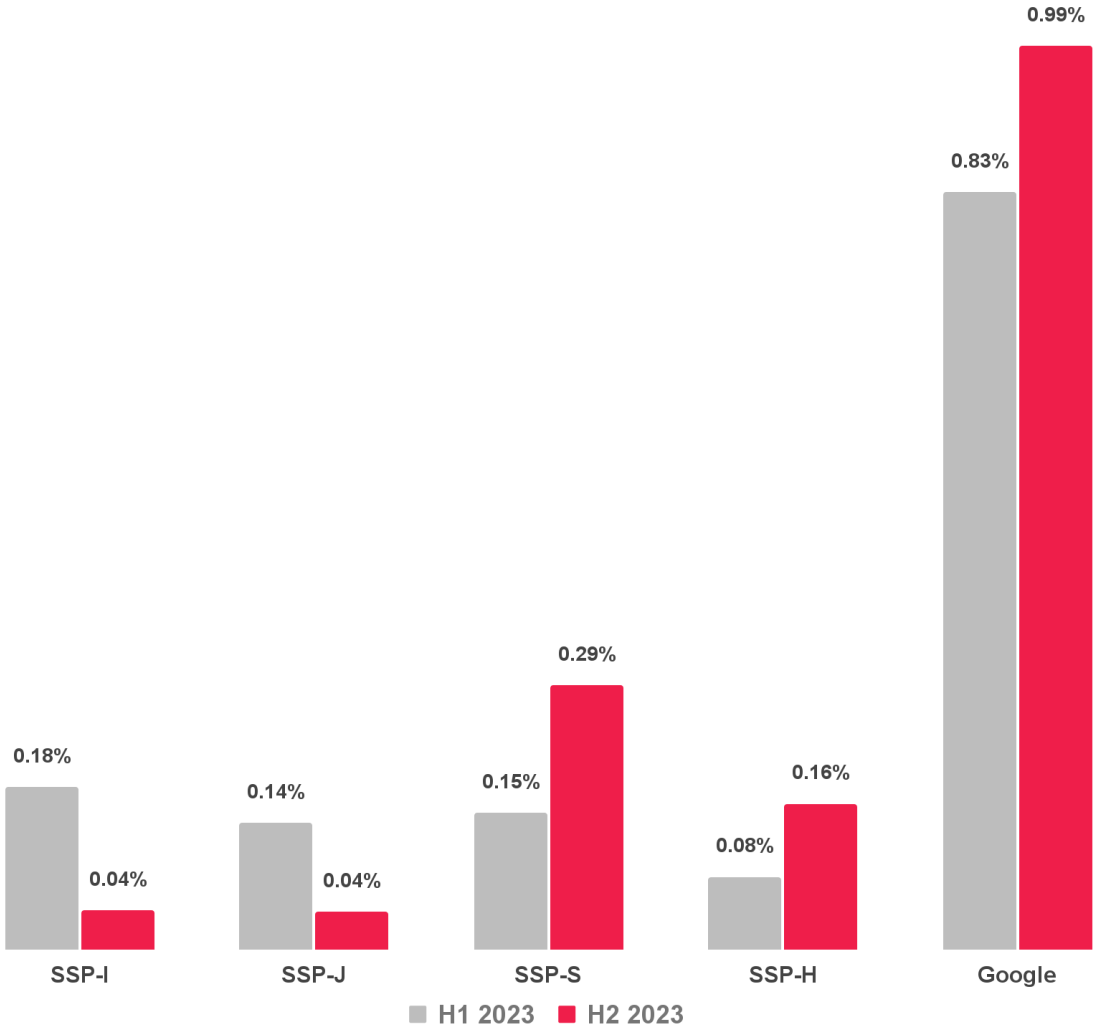
[3] The weighted average across all SSPs based on impression volume.

Security Violation Rate by SSP

In 2023, **Google and SSP-S struggled with high security violation rates**, with Google's rate being almost 4x worse than SSP-S. **Google's security rate dramatically increased from 0.48% in 2022 to 0.90% in 2023**. SSP-S, newly added in our H1 2023 report, saw an increase from 0.15% in H1 2023 to 0.23% overall in 2023.

The SSPs with the lowest rate of security violations for the year were **SSP-E**, **SSP-G**, and **OpenX**, each achieving a rate of less than 0.01%, with **Sharethrough** right behind them.

SSP-E remains the frontrunner.



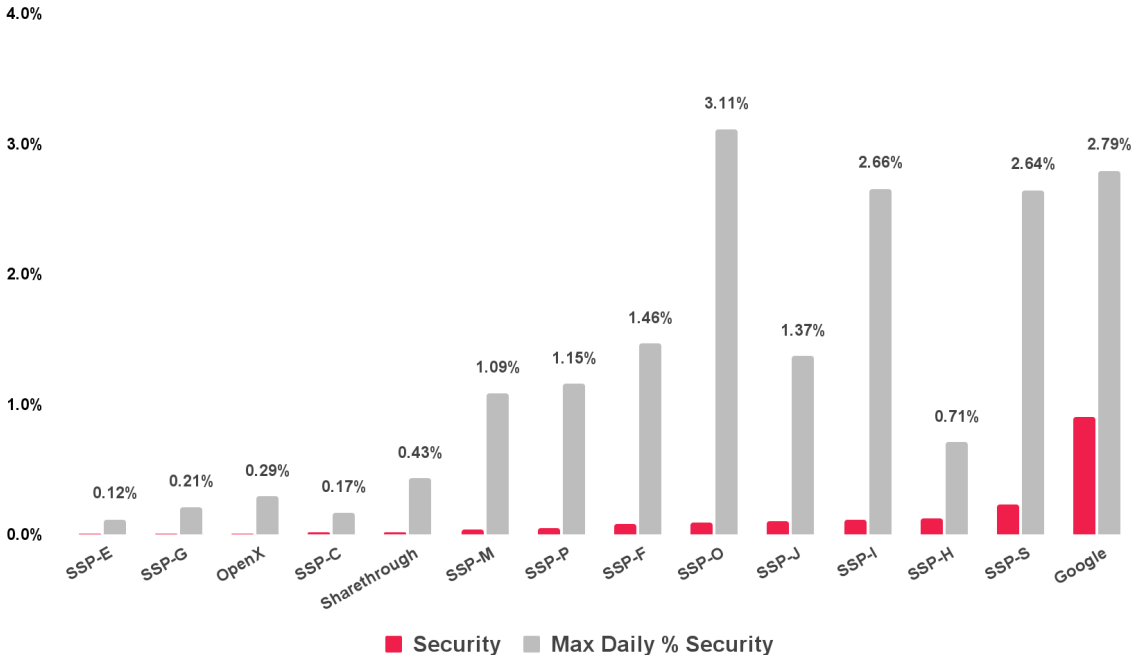
Security Violation Rate: H1 2023 vs. H2 2023

Google's security violation rate reached 1% in H2 2023, continuing its escalation. In H2 2022, its rate was 0.42%. This increase is largely driven by Fake Software Updates and malicious downloads. These malicious campaigns optimize to stay within Ad Platform policies, and as a consequence are very prevalent, especially in Google Ads.

SSP-I and SSP-J saw significant drops in their security rates in H2 2023. Both SSPs have matched their lowest 2022 rates after seeing a spike in H1 2023.

Conversely, **SSP-H and SSP-S** saw significant increases to their security rates in H2 2023.

Peak Date	
SSP-E	7/5
SSP-G	7/27
OpenX	10/4
SSP-C	3/19
Sharethrough	10/5
SSP-M	1/13
SSP-P	8/8
SSP-F	4/30
SSP-O	2/17
SSP-J	3/19
SSP-I	2/1
SSP-H	7/17
SSP-S	2/1
Google	10/2



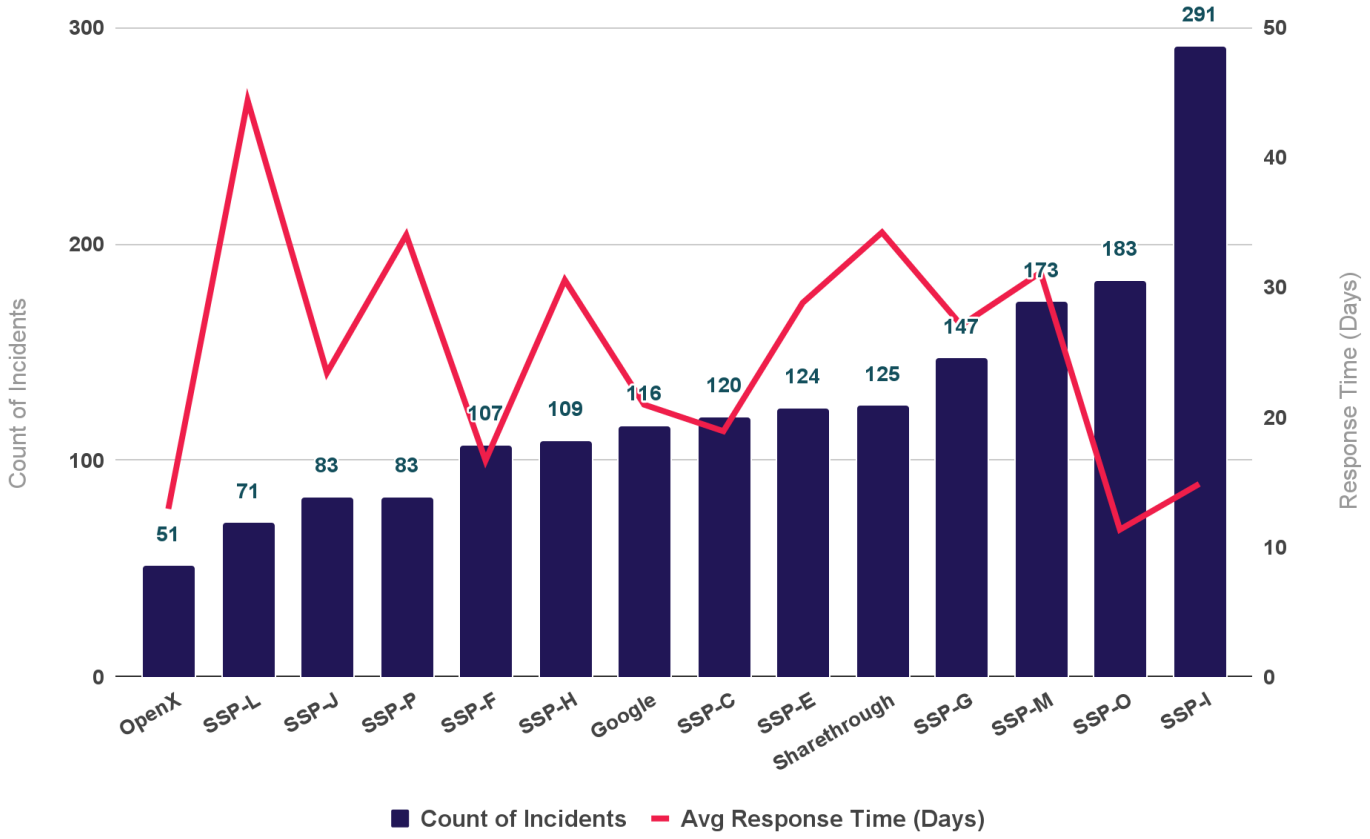
Daily Maximum Security Rate by SSP

Averages can mask significant variation in day-to-day performance, so it's important to note the **upper bound of the security violation rate** for each SSP to get a sense of overall risk.

In 2023, **Google and SSP-O recorded the highest daily security rates for the year at 2.79% and 3.11% respectively.** This means that during one day during 2023, more than one in 36 impressions from Google had security issues, and one in 32 for SSP-O.

SSP-E had both the lowest average security rate and the lowest daily security rate in 2023.

SSP-G, SSP-C, SSP-I, Sharethrough, and **OpenX** saw significant decreases in their highest daily security rates compared to 2022.



Incidents and Average Response Time

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.

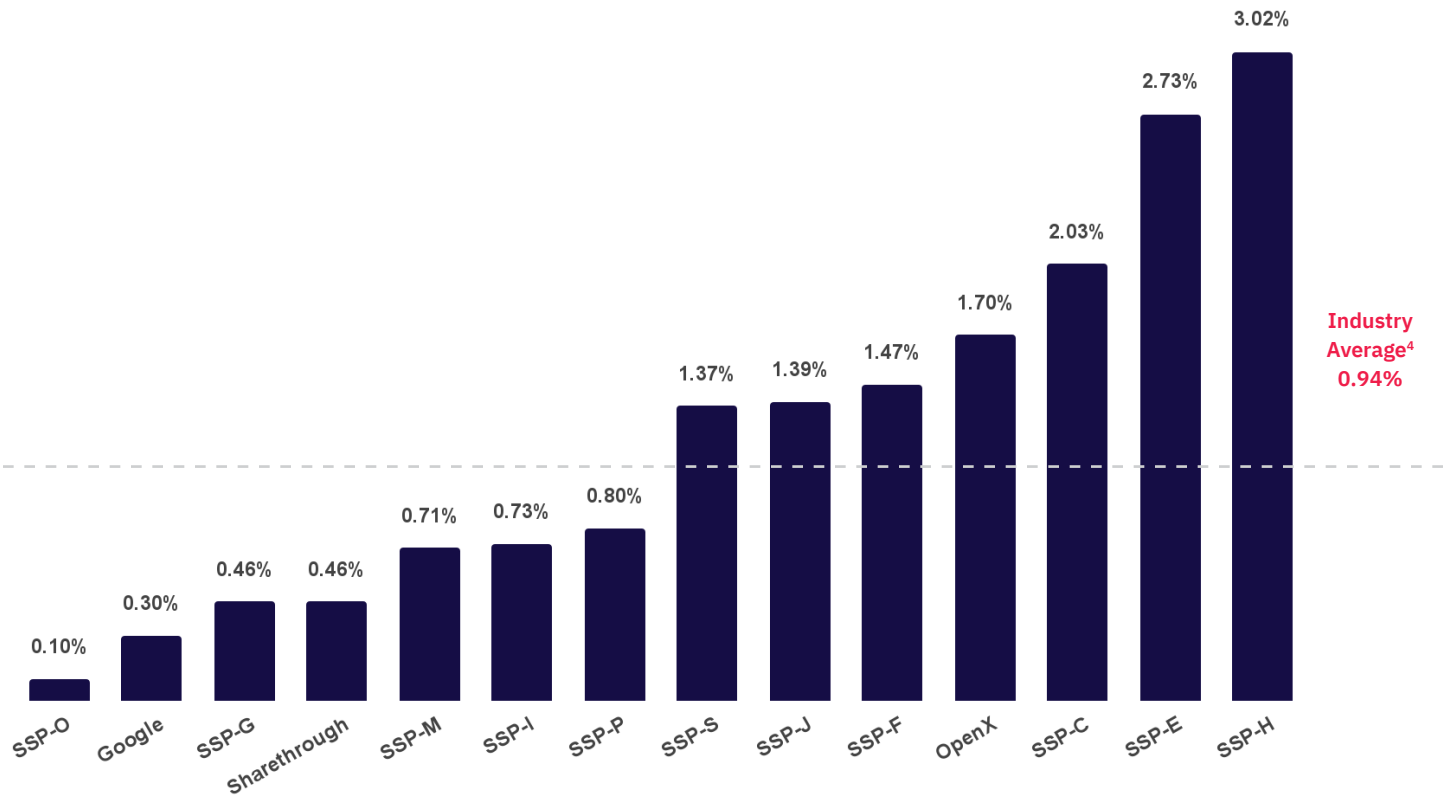
The elevated security rate in 2023 resulted in a higher number of incidents for all SSPs compared to 2022, except for Google and SSP-P, who both saw significant improvements.

Google cut its number of incidents and response time by 44% each when compared to its 2022 performance.

SSP-I, while holding the title of most incidents as it did in 2022 with 219 incidents, dramatically reduced its response time from 53 days to just 15, the 3rd best.

SSP-E, while boasting the best security rate in 2023, performed in the bottom half in terms of response time. Average response times increased dramatically in H2, increasing the average response times for all of 2023.

The number of incidents and average response times usually have matching trends, but response time trends varied in 2023.



[4] The weighted average across all SSPs based on impression volume.

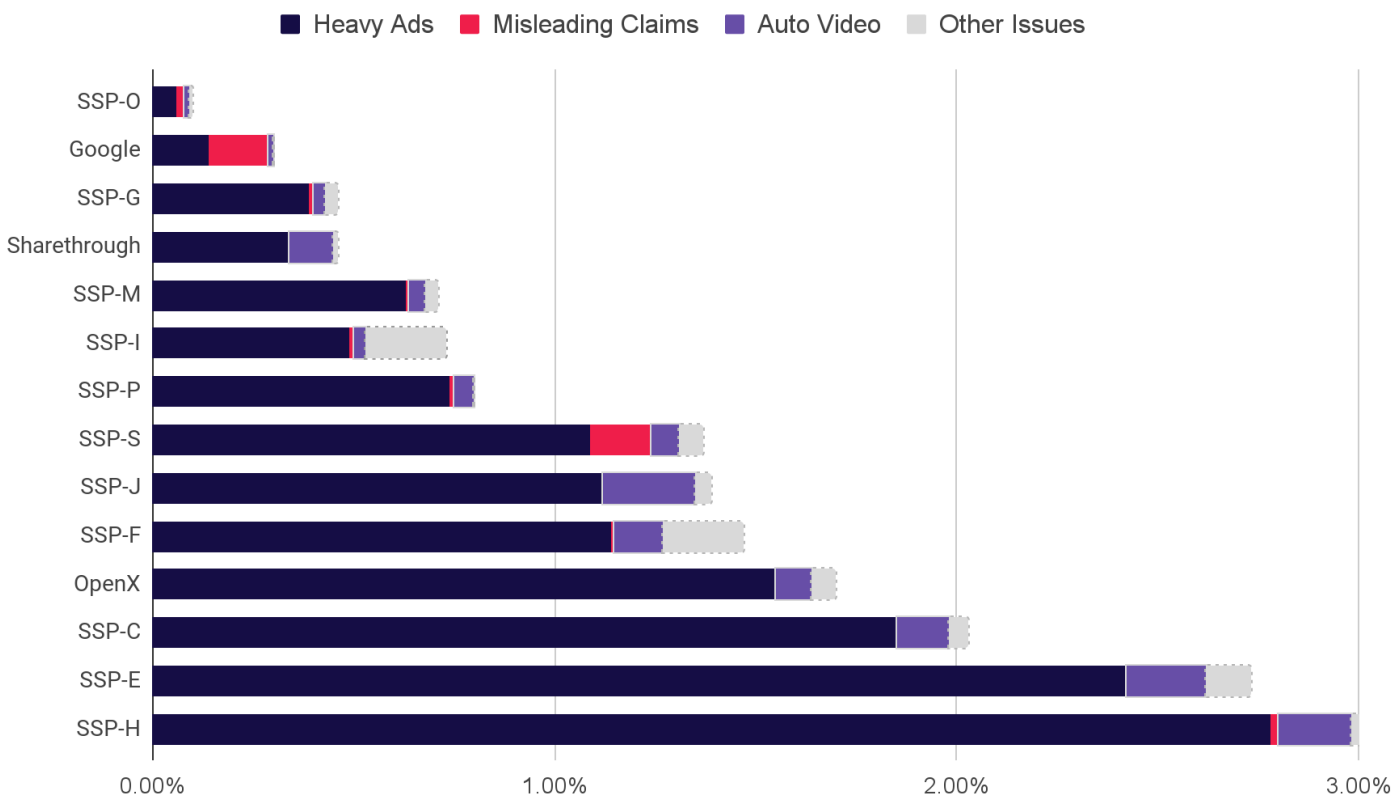
Quality Violation Rate by SSP

Quality violations cover a diverse array of non-security issues that publishers can monitor on the Confiant platform. Examples include **Auto Video, Heavy Ads, and Misleading Claims.** These controls correspond to ad behaviors that disrupt or impair the user experience.

SSP-O and Google were the only SSPs to improve their quality performance compared to 2022. **SSP-P**, the previous year's best at 0.16%, now sits at 0.80%.

SSP-J coincidentally averaged the same quality rate as it did in last year at 1.39%. However, while that performance placed it last in 2022, it now finds itself in the middle of the pack in 2023.

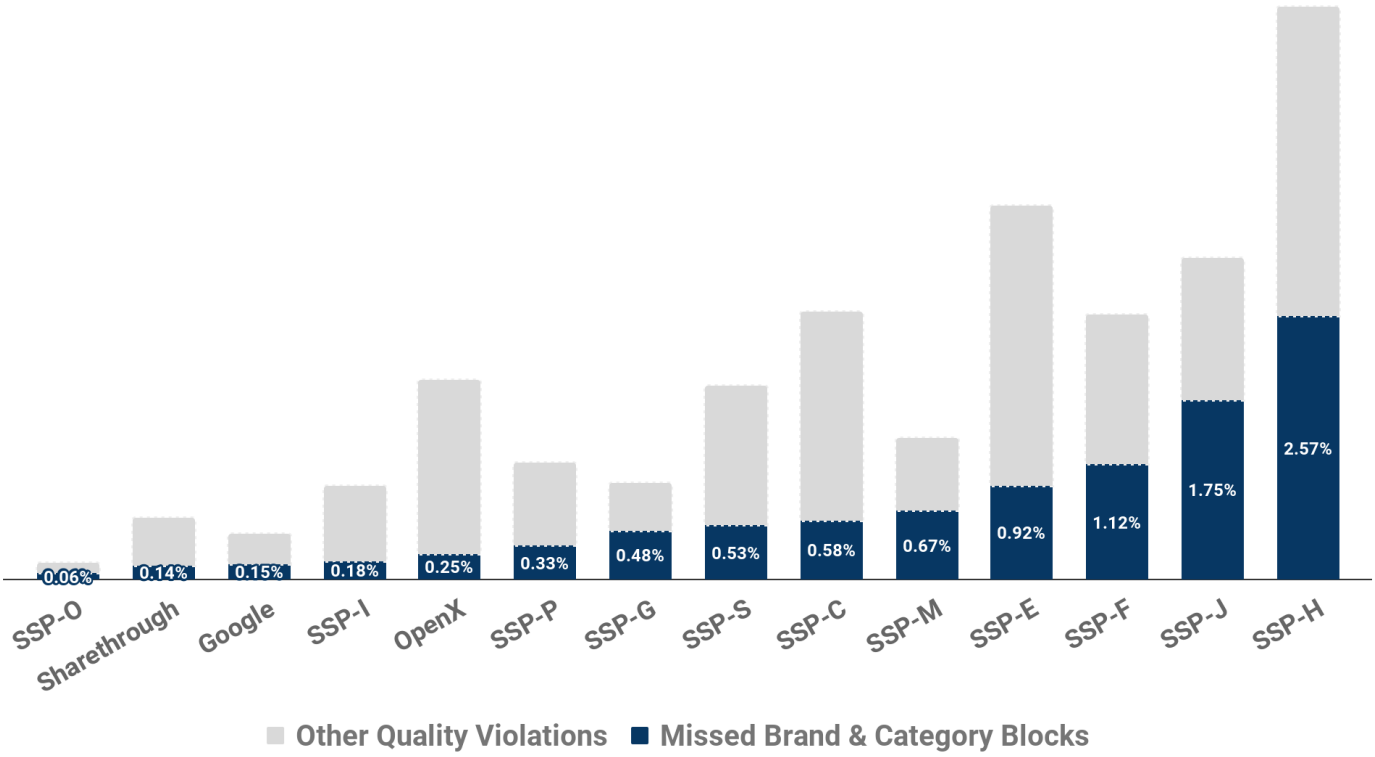
During 2023, 1 in 34 ads from SSP-H had quality violations.



Quality Violation Detail

For nearly all SSPs, **Heavy Ads** — ads with characteristics like high network load, large number of unique hosts, or Chrome Heavy Ad Intervention — were consistently the most common quality issue. Display ads that **auto-play video** without any user interaction were also quite common.

Misleading Claims — ads that use misleading language or imagery to garner clicks or sell products and services of dubious quality — was still the largest issue for Google, although they represent only half of their quality violations, down from 80% in 2022.



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.

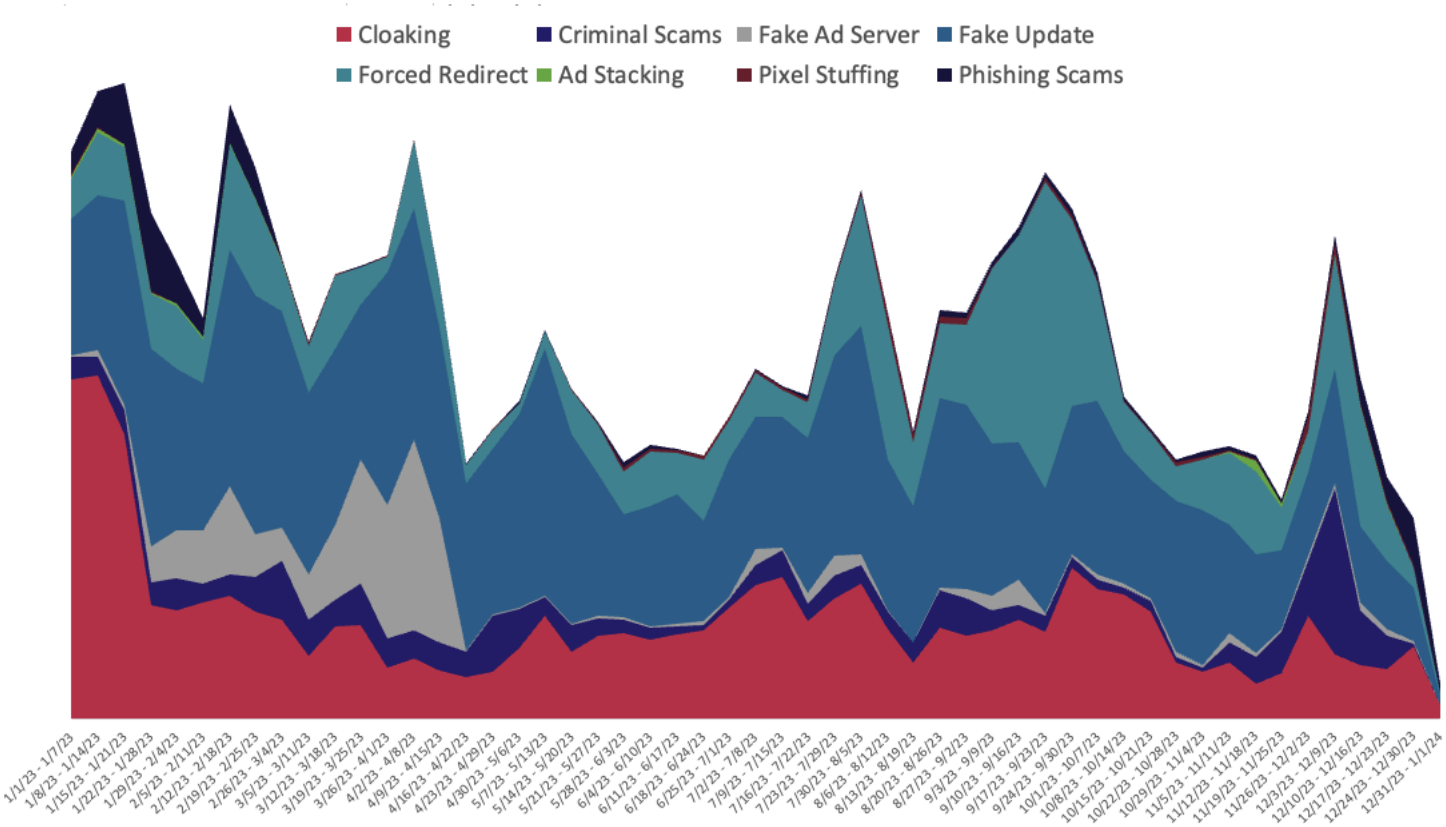
SSP-H not only had the highest Quality Violation Rate in 2023, but also the highest rate of blocks for brands and categories requested by Confiant publishers. SSPs O, I, Sharethrough, OpenX, and Google consistently performed well on this measure.

Violation Rates by SSP

Six SSPs had better-than-average performance for both security and quality: Sharethrough, SSP-G, SSP-M, SSP-P, SSP-O, and SSP-I. These were the same SSPs who ranked highly in 2022, with SSP-M being the newest member.

All other SSPs performed well on one measure but not the other. No major SSPs have underperformed in both categories simultaneously since 2021.


CONFIANT
Major Threat Activity
2023



Threat Detail

The nature of security threats shift constantly as attack techniques fall in and out of favor.

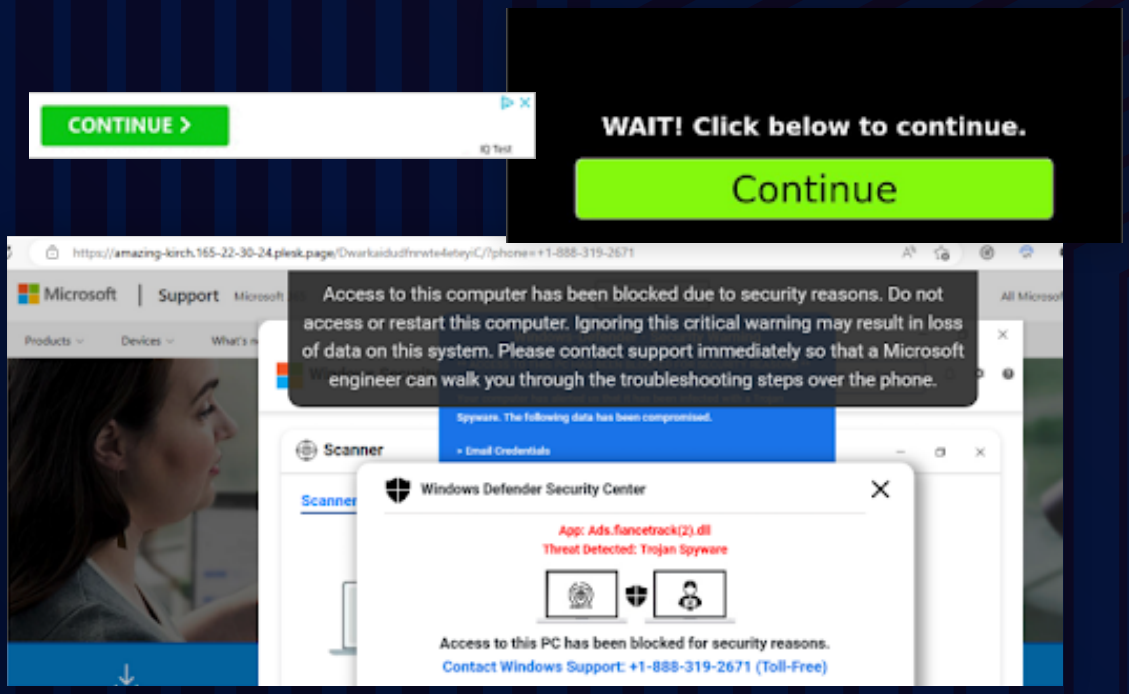
For three weeks in January 2023, **Cloaked Ads** accounted for half of the threats. There was a small bump in attacks in Q3.

Fake Updates/Downloads was the most consistent threat in 2023.

There was a surge of **Forced Redirect** attacks from late August to the end of September.

QUIZTSS

The top threat actor in 2023 was QuizTSS with total volumes that we estimate accounted for 20% of all malicious impressions....



Peak activity: **Continuous**

The Tech Support Scam (TSS) scene continues to evolve. The top threat actor in 2023 was QuizTSS with total volumes that we estimate accounted for 20% of all malicious impressions.

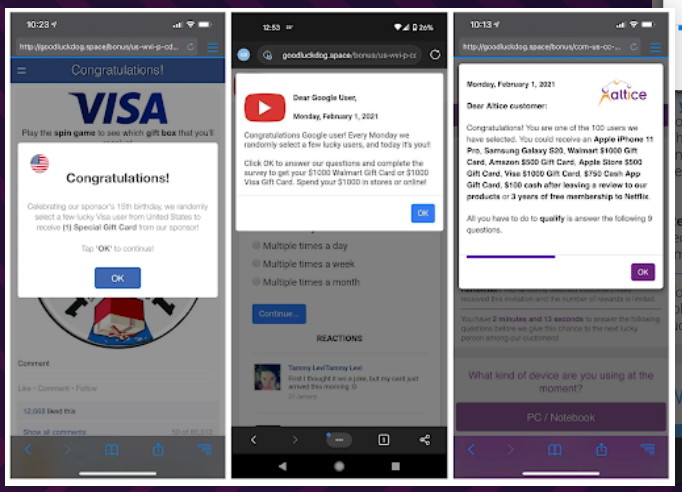
QuizTSS uses seemingly innocuous “Start” and “Continue” buttons on cloaked AI generated or quiz landing pages as a conduit for malicious activities. These buttons, designed to blend seamlessly with legitimate quiz content, mislead users into clicking them under the guise of continuing their engagement.

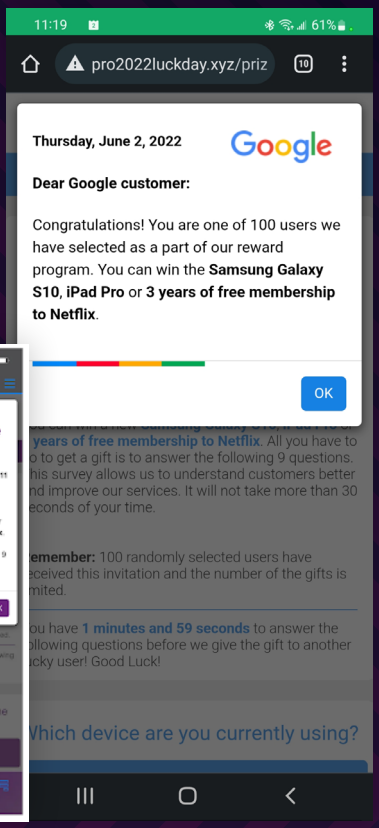
However, instead of progressing through the quiz, users are redirected to fraudulent tech support websites. These sites often employ aggressive tactics, such as fake virus alerts or system warnings, to deceive users into believing their devices are compromised and coercing them into purchasing unnecessary technical support services.

SCAMCLUB

ScamClub's primary method involves using Forceful redirects, subtly guiding users to harmful websites...

Take-Down Target





Peak activity: **Continuous**

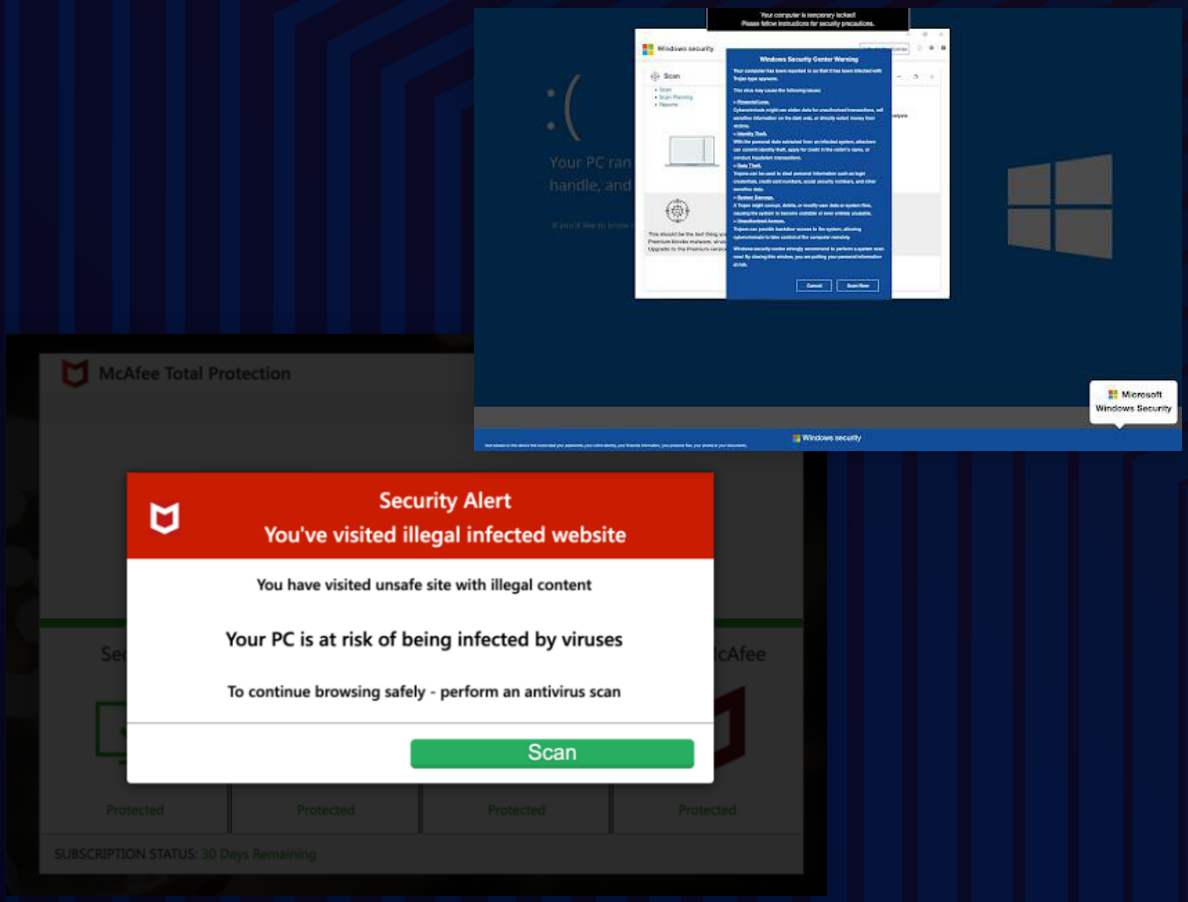
ScamClub's primary method involves using Forceful redirects, subtly guiding users to harmful websites, often hosting Scareware or fraudulent Gift-Card Scams, Carrier Branded Scams, Giveaway Scams. They skillfully penetrate established advertising networks, circumventing regular security measures to impact a broader audience.

ScamClub recent integration into video ads marks an evolution in their strategy to ensnare more victims, and suggests a focus on amplifying their revenue streams. By injecting malicious JavaScript into conventional VPAID (Video Player-Ad Interface Definition), they employ a straightforward yet potent technique to manipulate video ad content for malicious purposes.

In September 2023 Confiant threat intel and take-down report on ScamClub provided the threat intelligence that allowed an organized action to dismantle ScamClub supply chain links. Previously, ScamClub was abusing a browser vulnerability that Confiant had reported (CVE-2021-1801).

DCCBOOST

DCCBoost has deployed counterfeit McAfee scareware attacks on desktop users since late 2021...



Peak activity: **March, April, June and October**

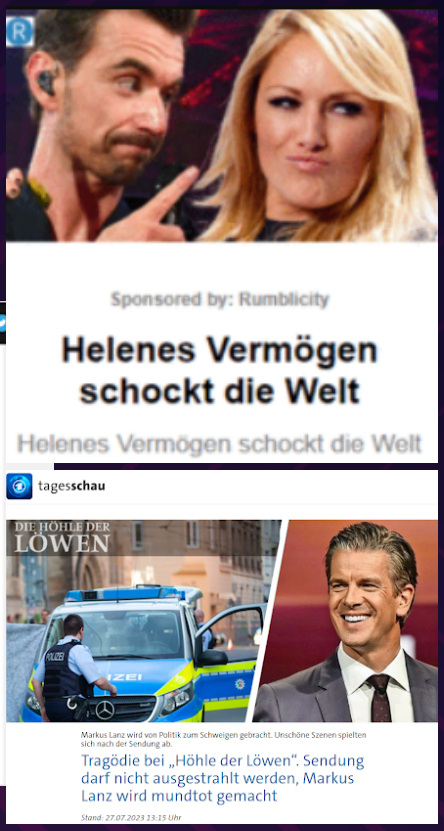
DCCBoost has deployed counterfeit McAfee scareware attacks on desktop users since late 2021, transitioning from their prior mobile device focus. Their scareware attacks forcefully redirect users to a site that poses as McAfee and executes a fake antivirus scan.

They employ refined detection evasion techniques, including a five-second delay before activation identified as Time-based technique and user interaction-based redirections (e.g., scrolling, clicking, or pressing keys on the page) identified as Click-jacking.

DCCBoost targets users in the United States, Canada, Europe, and other regions. Various Supply Side Platforms (SSPs) have been impacted.

FIZZCORE

FizzCore, a malvertising threat actor primarily targeting Europe, who is focused on cryptocurrency scams...



Peak activity:
August, November, December

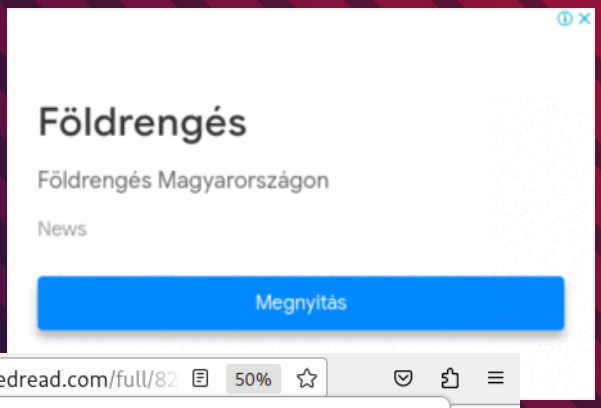
FizzCore, a malvertising threat actor primarily targeting Europe, who is focused on cryptocurrency scams via deceptive ads as lead magnets.

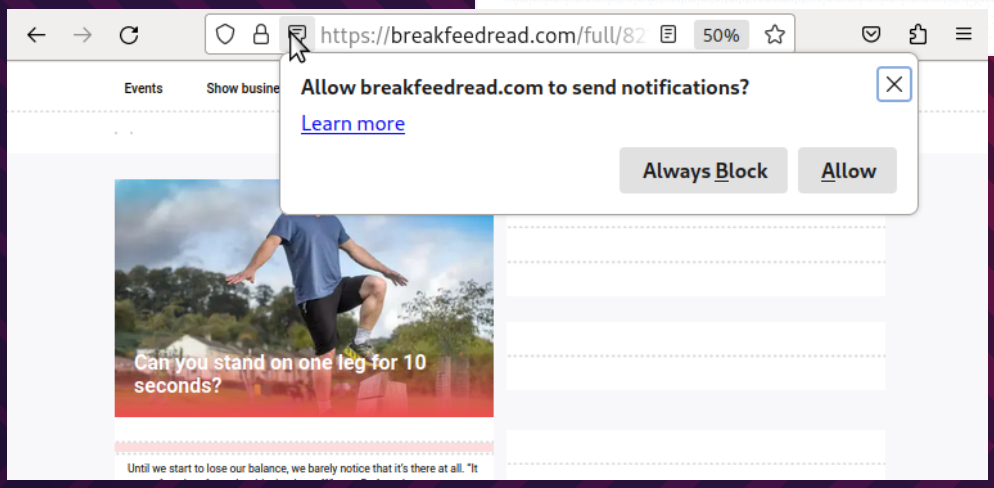
They publish deceptive ads with shocking images, like injured celebrities. Clicking on ad leads users to fake articles with misleading content that promotes Bitcoin investments, seemingly endorsed by celebrities. Unsuspecting individuals, especially retirees, are often tricked into investing large sums, resulting in substantial financial losses through the Fizzcore financial traps.

FizzCore's concern lies in its rapid and aggressive strategy of launching, getting detected, then rebuilding and relaunching, coupled with its advanced cloaking techniques that evade standard detection methods on advertising platforms.

THENOVOSTI

TheNovosti ad copy is generally themed around pensions or health-related clickbait factoids (e.g. garlic or sugar) and targeting elderlies...





Peak activity:
Continuous

Tricks people into opting into malicious push notifications, sometimes by using page templates that look “half loaded”.

Notifications escalate to a broad variety of malvertising chains
Very quick churn of domains.

Ad copy is generally themed around pensions or health-related clickbait factoids (e.g. garlic or sugar) and targeting elderlies.

The campaign is mostly active in Eastern Europe but has expanded to many countries.

2023

HIGHLIGHTS

- **One in every 79 impressions revealed significant security or quality issues, marking the highest rate observed since the previous peak in 2018.**
- The **quality violation rate in Q4 2023 also hit its highest level since 2018.**
- In the second half of 2023, **the industry-wide ad quality violation rate more than doubled from 0.63% to 1.57%.**
- On average, **one in every 384 impressions delivered in 2023 was a security risk to the user.**
- **For two years in a row, SSP-E had the lowest security violation rate, and daily maximum security rate.**
- The number of incidents and average response times usually have matching trends, but response time trends varied in 2023.
- **Forced Redirect attacks surged in September of 2023.**

About CONFIANT

Confiant is the cybersecurity leader in detecting and stopping Malvertising attacks. Having built hundreds of integrations directly into the web's ad tech infrastructure, Confiant has unparalleled visibility to the malware, scams and fraud serving through ads today. Leveraging our security expertise, we deliver complete control over ads to publishers and ad platforms, also remediating quality issues, privacy violations, and mis-categorized ads.

In publishing the industry's leading ad quality benchmark report and mapping the threat actors that use ads-as-an-attack-vector at matrix.confiant.com, Confiant is leading the charge in protecting users from criminals hijacking the ad tech supply chain. Trusted by customers like Microsoft, Paramount, and Magnite, we celebrate more than a decade supporting our ad tech partners.

LEARN MORE

Malvertising and Ad Quality Index

Please visit our website at:

www.confiant.com

2023 Report

January 1st - December 31st