
CONFIANT
MALVERTISING + AD QUALITY INDEX
MAQ INDEX
Q1 2021

INTRODUCTION

Confiant's Malvertising and Ad Quality (MAQ) Index (formerly known as our Demand Quality Report) is a quarterly look into the quality of demand in digital advertising. Using a sample of over 180 billion impressions monitored in real time in Q1 2021, Confiant is able to answer fundamental questions about the state of ad quality in the industry at large.

Digital advertising delivers significant value to publishers but 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 has historically been challenging to estimate impact without client-side instrumentation in place on a large and diverse set of publishers. The MAQ Index, which leverages Confiant's position as the vendor of choice for real-time creative verification, aims to change that.

In September 2018, Confiant released the industry's first benchmark report. This report, the twelfth in the series, covers Q1 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]

[1]*Ad 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 181 billion advertising impressions monitored from January 1 to March 31, 2021, from over 29,000 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.

METHODOLOGY

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

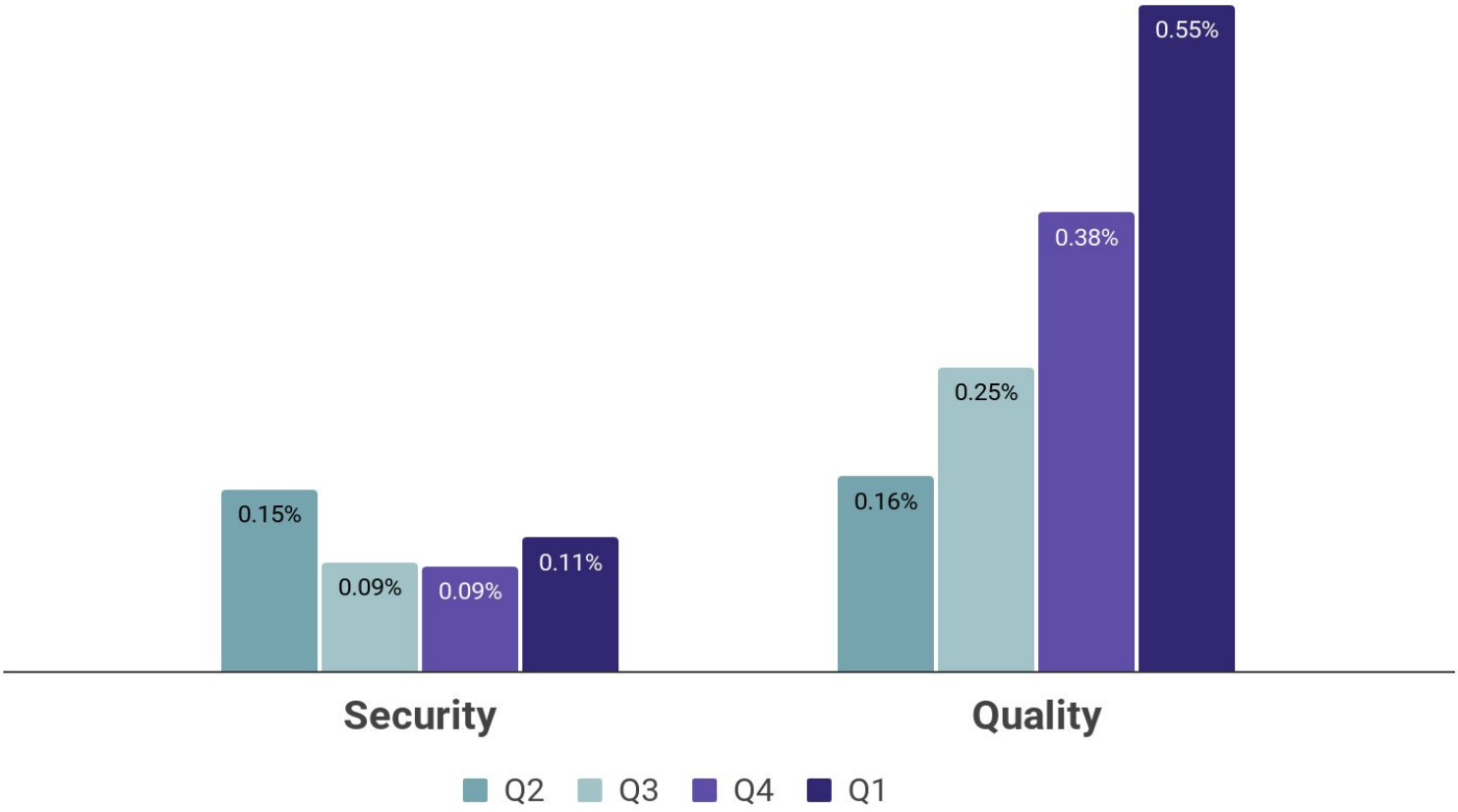
Please note that in Q3 2020, we shifted from using U.S. to global data, necessitating a restatement of our results to allow quarter-to-quarter comparison. As a result, some metrics in this report may not match those in prior quarters.

Q1 2021 VIOLATION RATES BY COUNTRY

While European markets have historically had higher rates of Security violations than the U.S., the picture was more mixed for Q1. The UK and Italy both saw violation rates well in excess of the U.S., while Germany, France, and Spain saw much lower activity than in past reports.

Quality violations remained more prevalent in the U.S. than elsewhere in Q1, a trend that's held through several reports.


CONFIANT
INDUSTRY
VIEW
Q1 2021

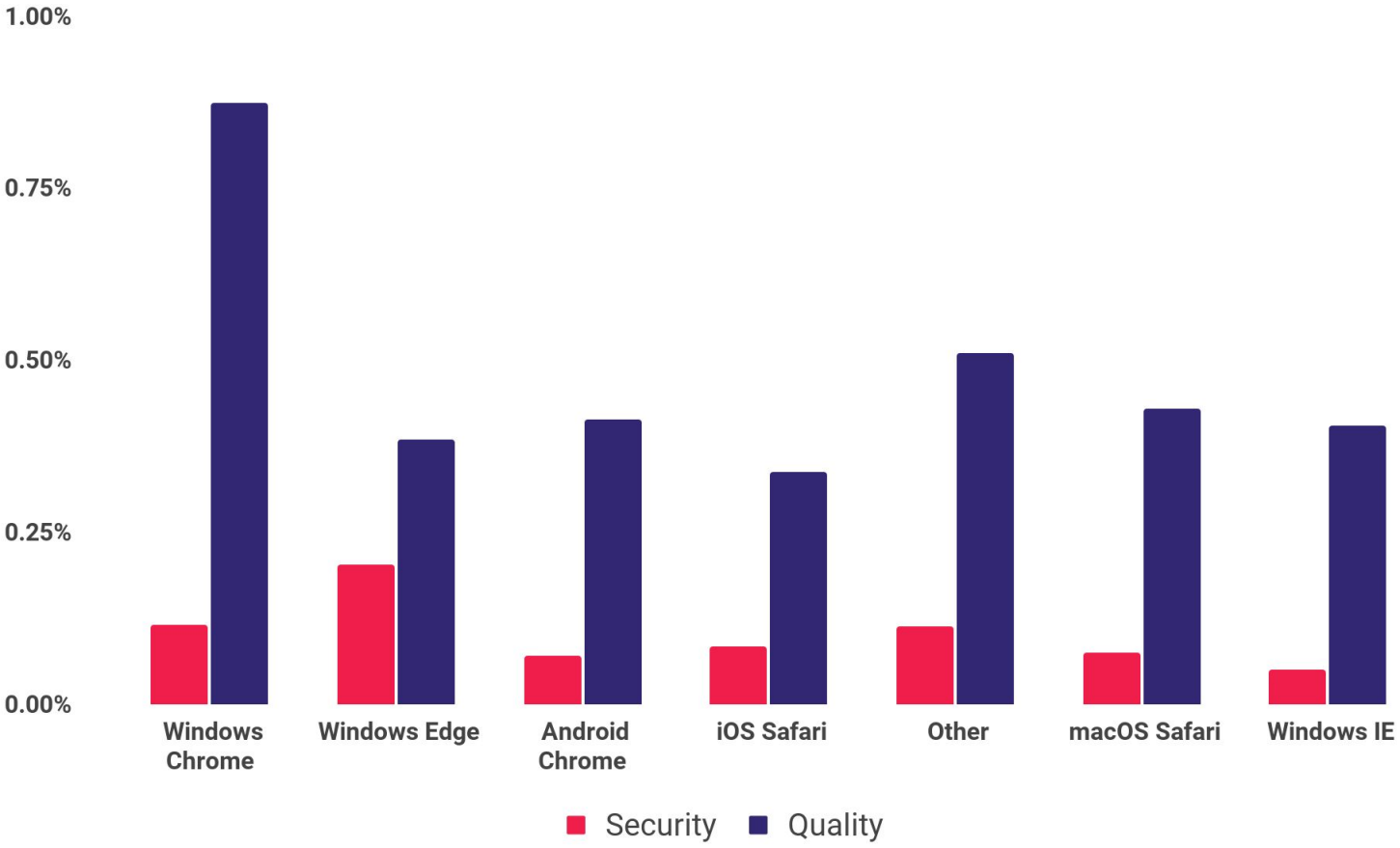


HOW DID THE INDUSTRY FARE IN Q1 2021?

The **Security violation rate** for Q1 2021 was 0.11%, an increase of 0.02 percentage points over Q4 and the highest level we've seen since Q2 2020.

The **Quality violation rate** increased from 0.38% in Q4 to 0.55% in Q1, an **increase of almost 45%**. The Quality violation rate has climbed for three straight quarters driven by increased rates of Heavy Ads and Video Arbitrage.

In Q1 2021
1 in every 150
impressions was dangerous or highly disruptive.



Q1 2021 VIOLATION RATES BY USER AGENT

Edge for Windows was the top source of Security issues in Q1, with a violation rate 76% higher than Chrome. Rates for the main mobile browsers—Android, Chrome, and iOS Safari—were comparable to one another, both falling in the 0.07% - 0.08% range.

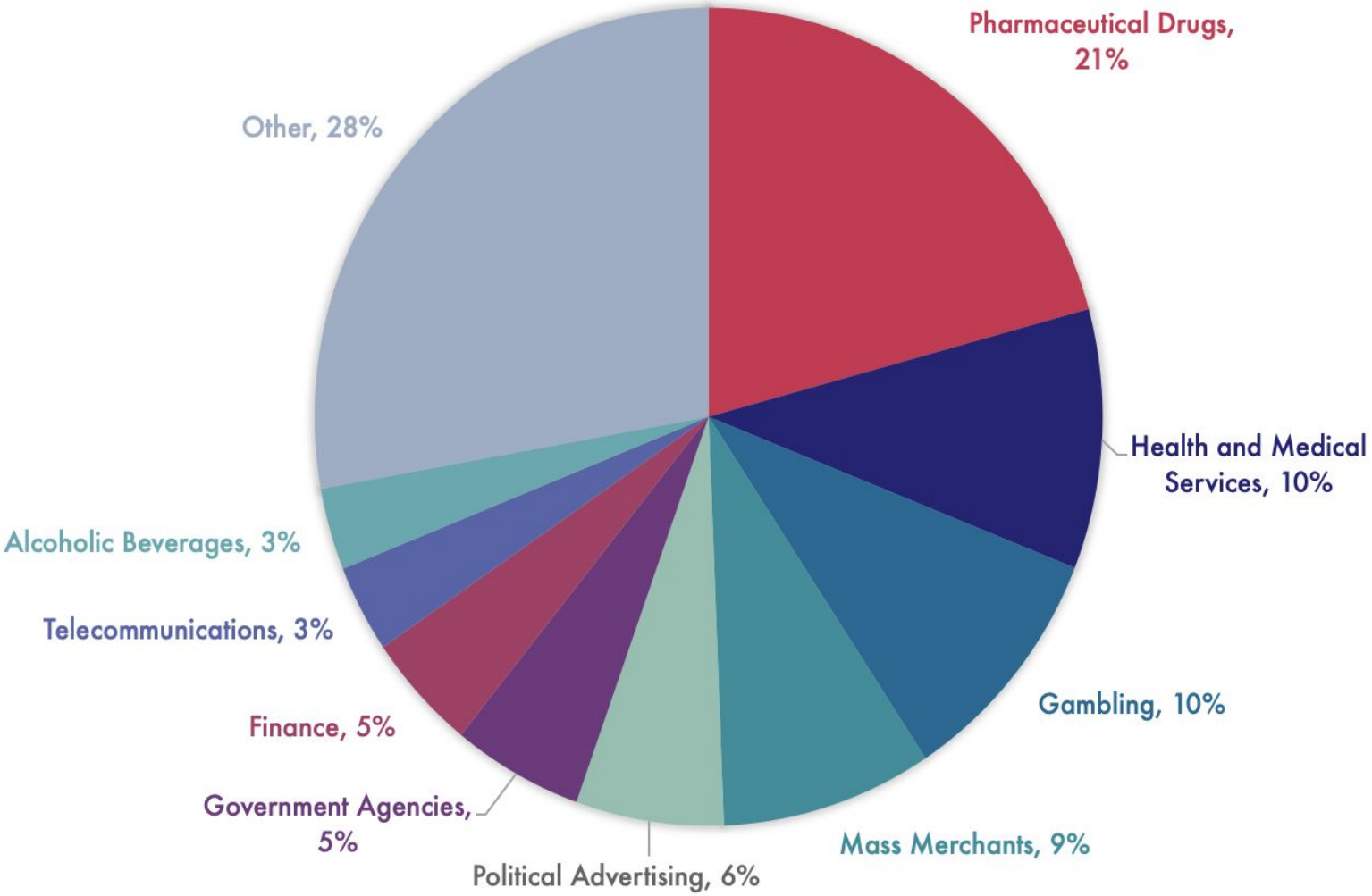
Chrome for Windows had the highest rate of Quality violations in Q1, an unfortunate repeat of its poor performance on this measure in 2020.

Q1 2021 VIOLATION RATES BY HEADER BIDDING FRAMEWORK

Publishers increasingly 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 Q1, Open Bidding continued its strong performance on Security relative to other sources, while also beating Prebid on Quality violation rate.

MOST BLOCKED AD CATEGORIES



"Other" includes over 100 other categories

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

In Q1, Pharmaceutical Drugs was the most blocked ad category, rocketing from 5th place in Q4. Even more striking, health-related topics represented close to one-third of all category blocks, likely reflecting sensitivities stemming from COVID-19. With the 2020 presidential election now well in the rearview mirror, Political Advertising fell from 12% of total blocks to just 6%.


CONFIANT
SSP RANKINGS
Q1 2021

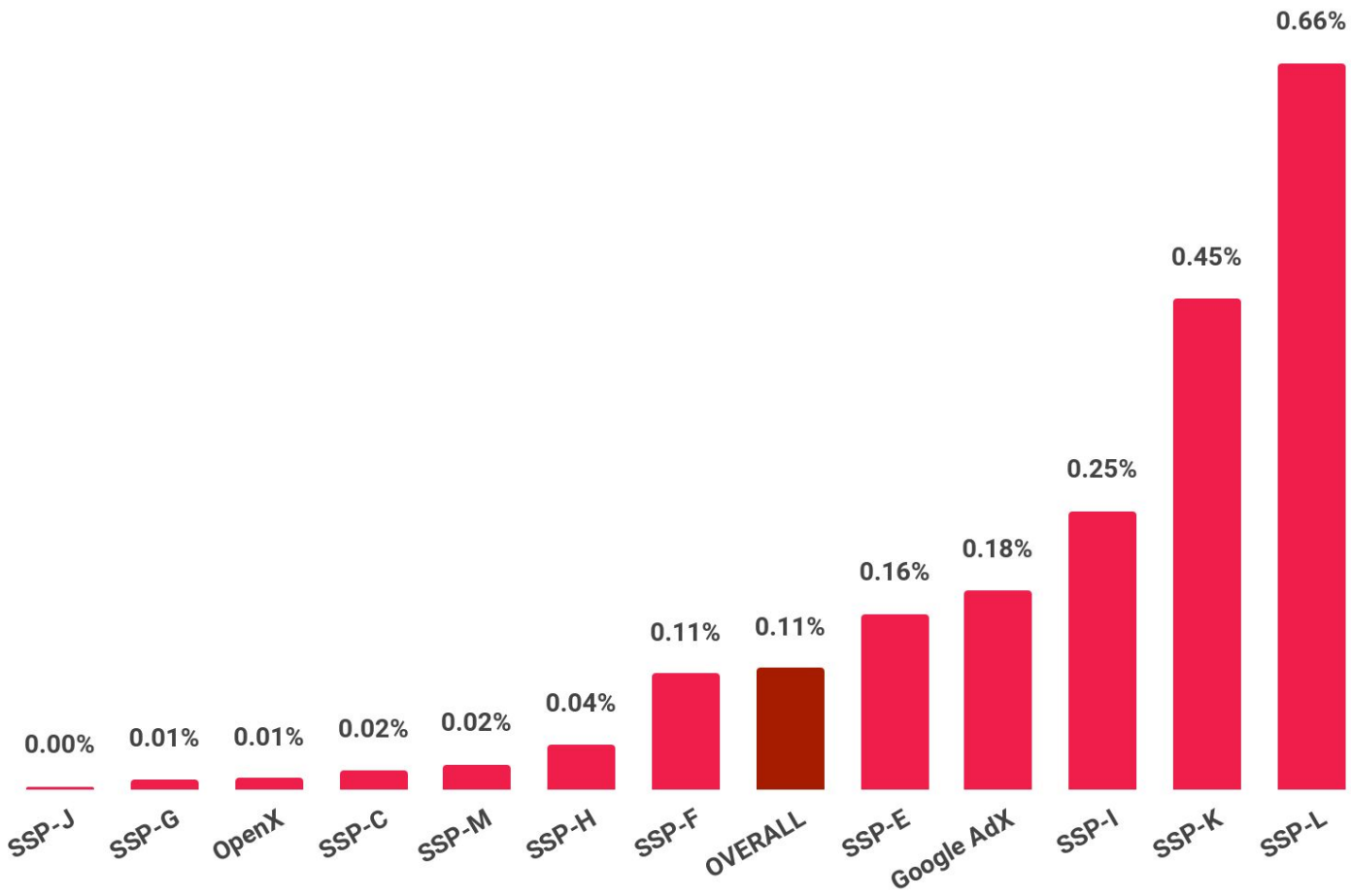
Q1 2021 US SSP RANKINGS

In Q1, Confiant tracked impressions from over 100 SSPs. However, more than 75% of global impressions originated from just 12 providers[1] 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.

We identify Google Ad Exchange within these rankings. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. For the first time, we identify another SSP in the rankings. OpenX has opted to be listed in our reports without obfuscation, an option we offer to any SSP that requests it.

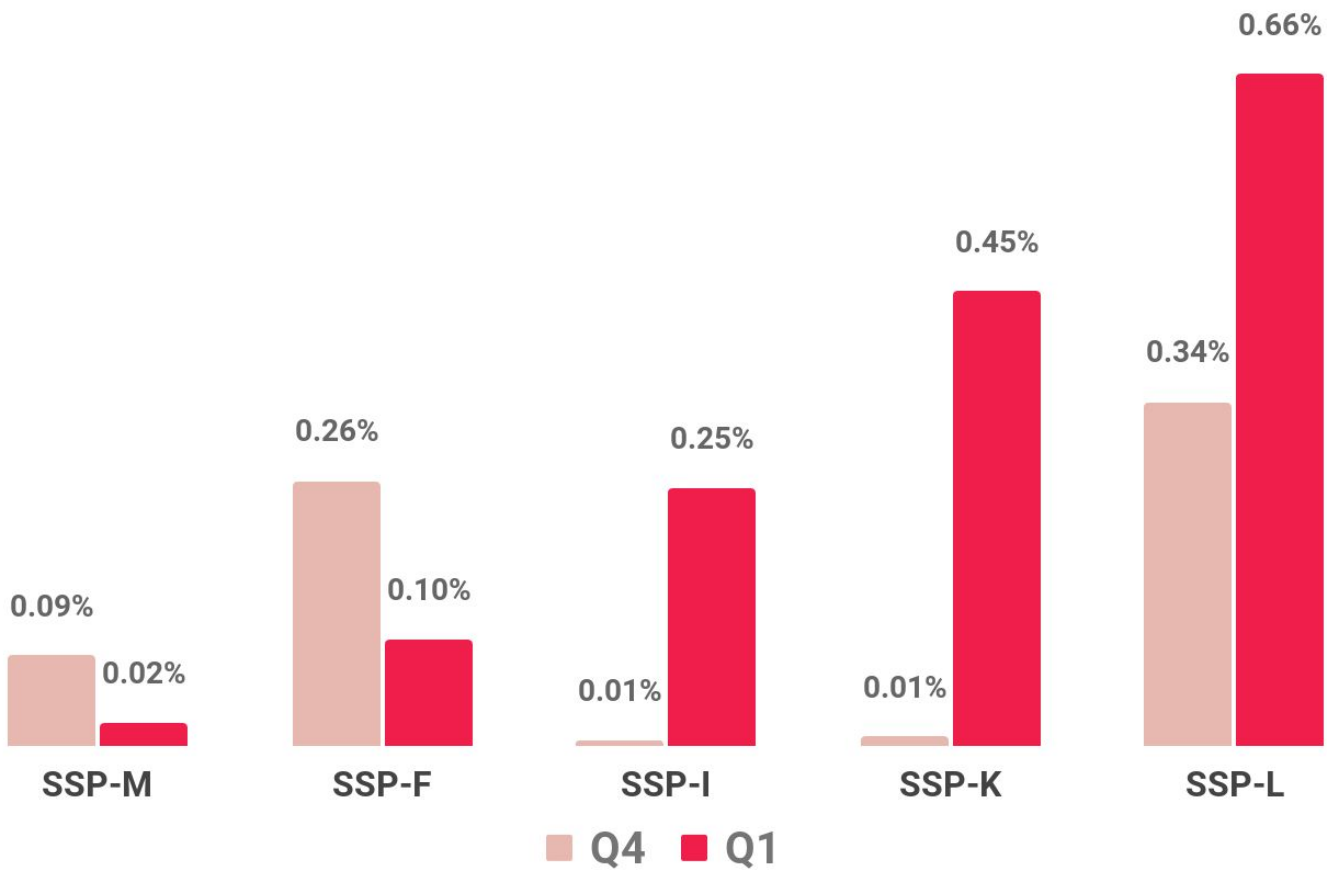
[1] *Google AdX, Magnite, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, Sonobi, TripleLift, District M, 33Across, and Sovrn*



SECURITY VIOLATION RATE BY SSP

A perennial strong performer, **Google experienced an uncharacteristic setback** this quarter. Their Security violation rate increased from 0.05% in Q4 to 0.18% in Q1 and exceeded the industry average for the first time. SSP-L had the highest Security violation rate, coming in at **213x the rate of the best performing SSP**. SSP-L was also the worst performer in Q4.

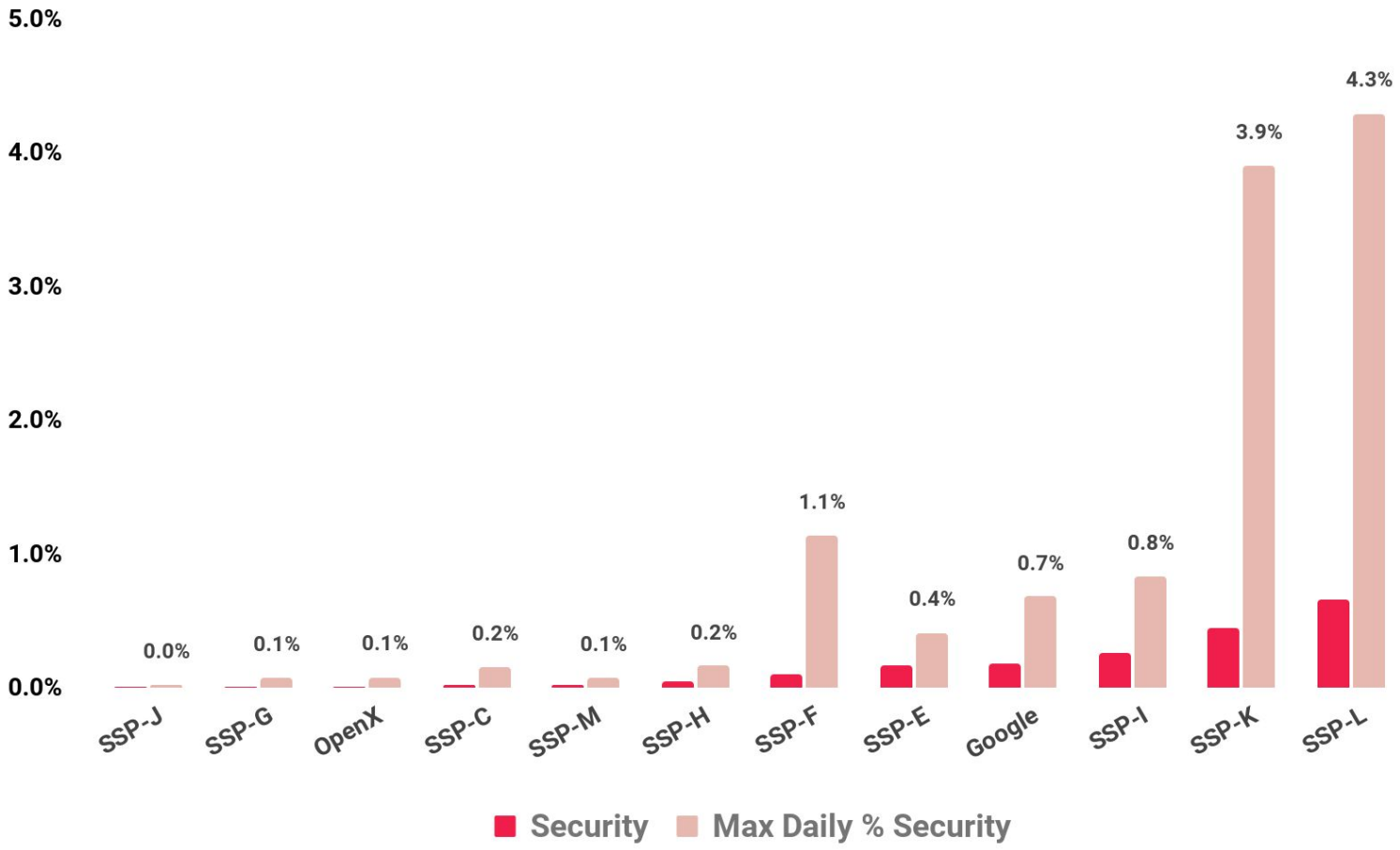
SSPs J, G, and OpenX were the quarter's top performers, each with a Security violation rate coming in at 0.01% or below.



SECURITY VIOLATION RATE: Q4 VS. Q1

SSP-F continued to improve quarter over quarter and has now reduced their Security violation from a high of 1.0% back in Q3 to just 0.10% in Q1.

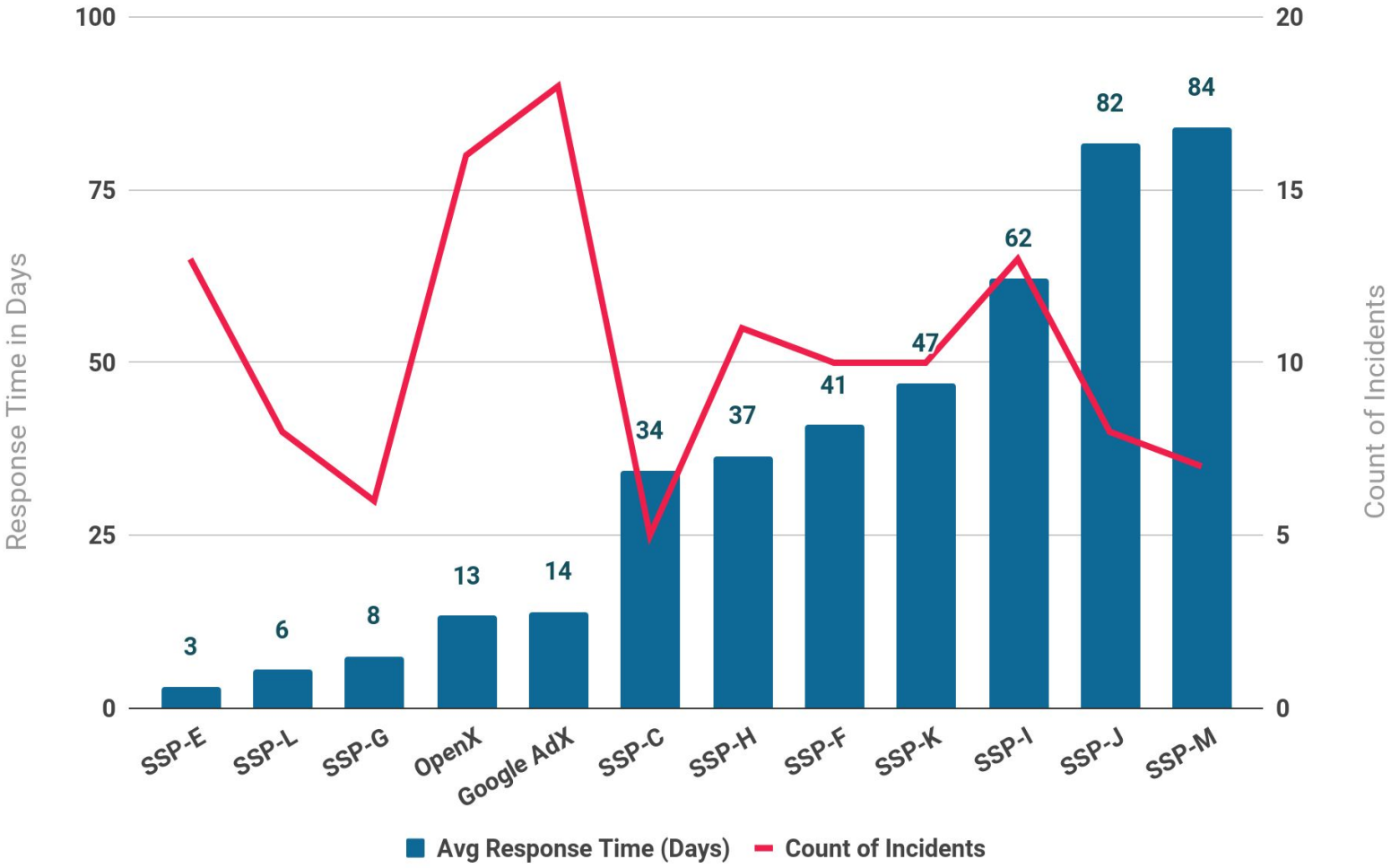
On the opposite side of the ledger, SSPs I, K, and L all saw big increases in their Security violation rate. SSP L's rate has now doubled two quarters in row. SSP-K has been extremely volatile, alternating between the best and worst in each of the past 3 quarters.



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.

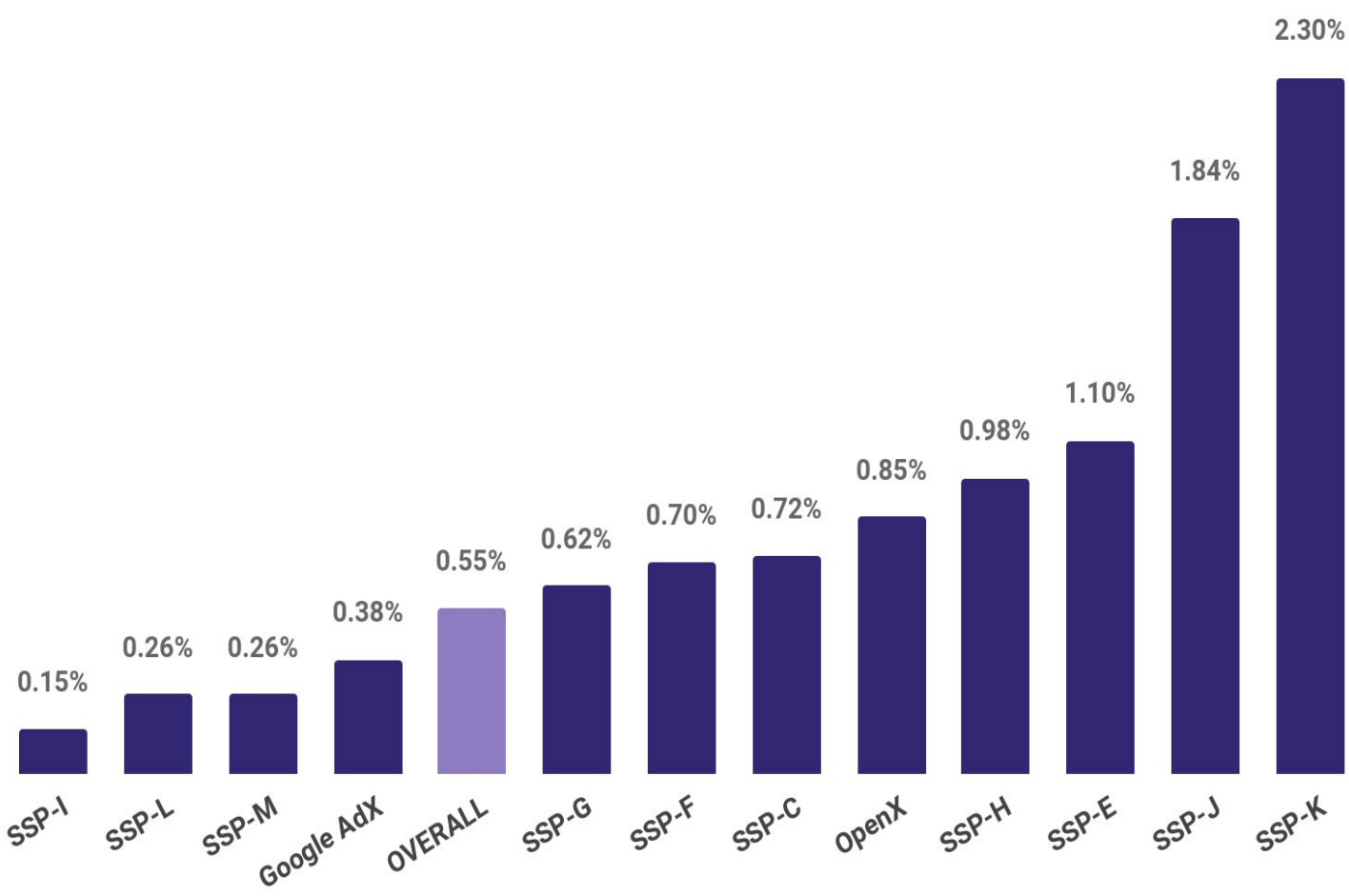
When under sustained attack, SSPs K and L had days where 1 in 25 impressions was a Security violation, putting publishers and users at considerable risk.



AVG DURATION OF ATTACK BY SSP IN Q1

It's also crucial to understand how long threats persist on an SSP once an attack is 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.

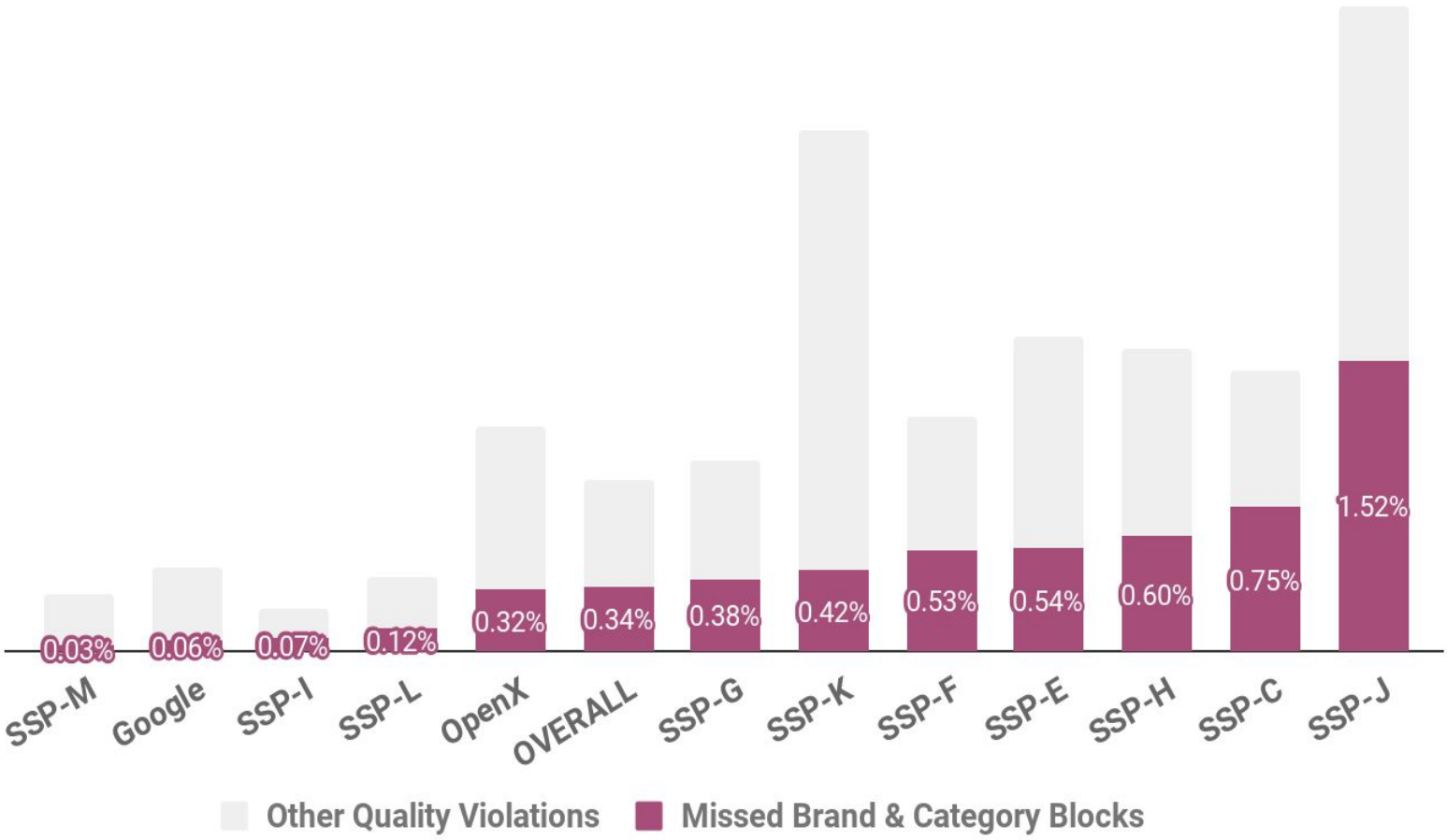
In Q1, SSP-M's average response time remained quite elevated at 84 days. Unlike last quarter, no SSP achieved average response times of 1 day or less, and many issues persisted for multiple weeks before being resolved.



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 video arbitrage, heavy ads, and pop-ups. These rules correspond to ad behaviors that disrupt or impair the user experience.

SSPs J and K continued to perform poorly in Quality violation rates, falling into the bottom three in both Q4 and Q1. The standouts for good performance were SSPs I, L, and M.



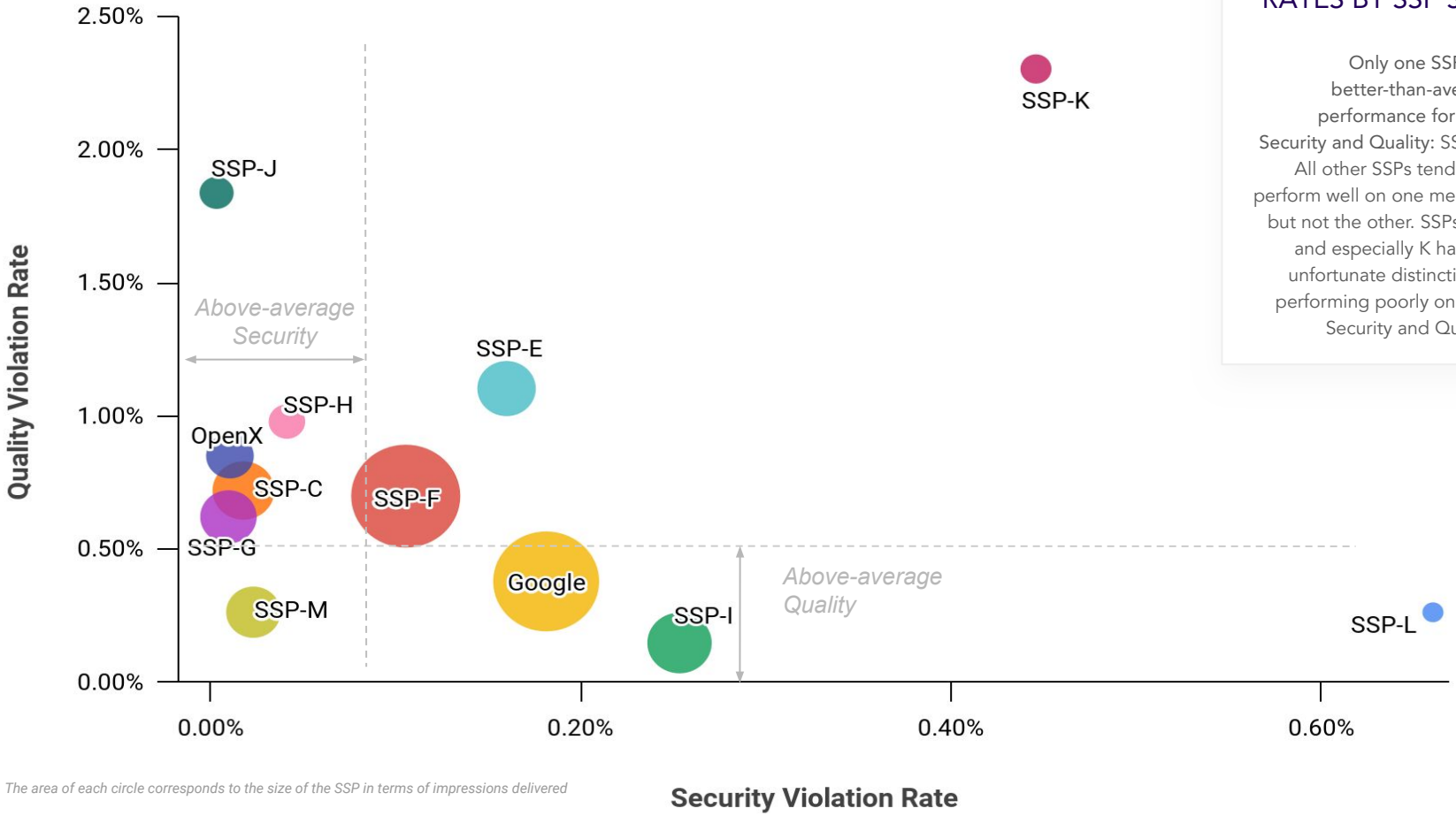
MISSED BRAND/CATEGORY BLOCKS

Publishers rely on SSPs as the first line of defense against ads associated with unacceptable brands and categories. Publishers use brand and category blocks to exclude ads that feature competitors, are inappropriate for their audience, or create channel conflicts.

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

The worst performing SSP delivered security issues at **213x the rate** of the best

Q1 VIOLATION RATES BY SSP SIZE



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

Q1 VIOLATION RATES BY SSP SIZE

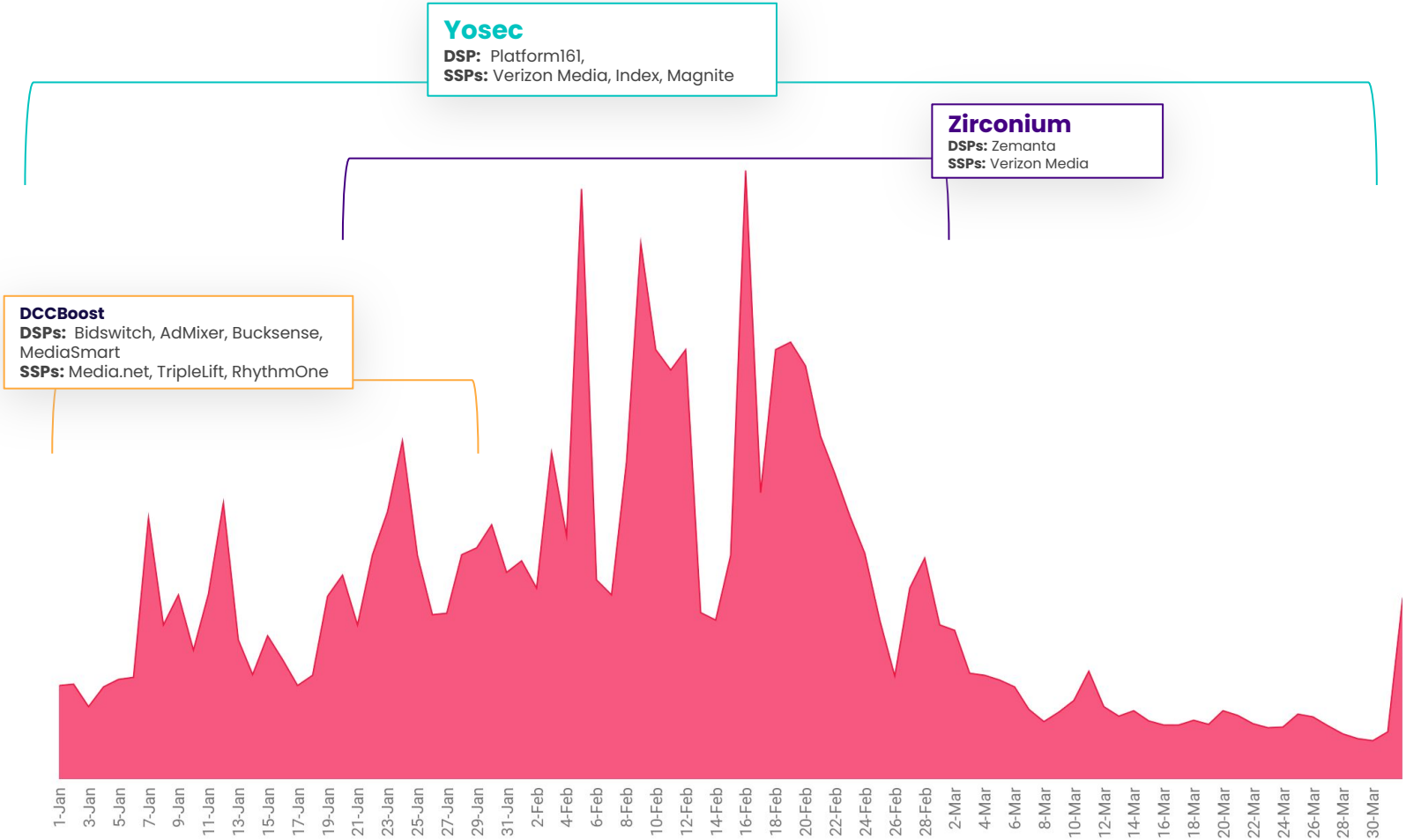
Only one SSP had better-than-average performance for both Security and Quality: SSP-M. All other SSPs tended to perform well on one measure but not the other. SSPs F, E, and especially K had the unfortunate distinction of performing poorly on both Security and Quality.

CONFIANT

MAJOR THREAT GROUPS ACTIVE IN Q1

Q1 2021

NOTABLE THREAT ACTIVITY



ZIRCONIUM

On a rolling basis, the gang would run redirects to tech support scams that are cloaked in multiple layers of sophisticated Javascript obfuscation.

SPECIAL REPORT: UK's Top Celebrity Chef Comes Out with New Secret That's Making Millions of Brits Rich

AS SEEN ON

ten 60 MINUTES smh.com.au sunrise THE PROJECT

https://platform.ed-onlinepartners.com/u/b/2958085/hcwDEB1w4GmC?MPC_4=1612901777&MPC_3=mbq&so=bitcoinrevolutionen&sub=bitcoinrevolutionen

(https://platform. 4GmC?MPC_4=1612901777&MPC_3=mbq&so=bitcoinrevolutionen&sub=bitcoinrevolutionen)

(https://platform.ed-onlinepartners.com/u/b/2958085/hcwDEB1w4GmC?MPC_4=1612901777&MPC_3=mbq&so=bitcoinrevolutionen&sub=bitcoinrevolutionen) *(Tuesday, February 9, 2021) - UK's top celebrity chef comes out with new secret that's making millions of Brits rich*

(BBC) - Multi-Michelin star celebrity chef Gordon Ramsay just bought his ninth Ferrari using money he earned not from his TV shows or restaurants - but from a new controversial investment he revealed on live television. **"Due to the Virus epidemic that has hit our Country, the market is changing rapidly. Everybody should stay at home and build massive wealth by using this**

ZIRCONIUM
PEAK ACTIVITY:

FEBRUARY

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

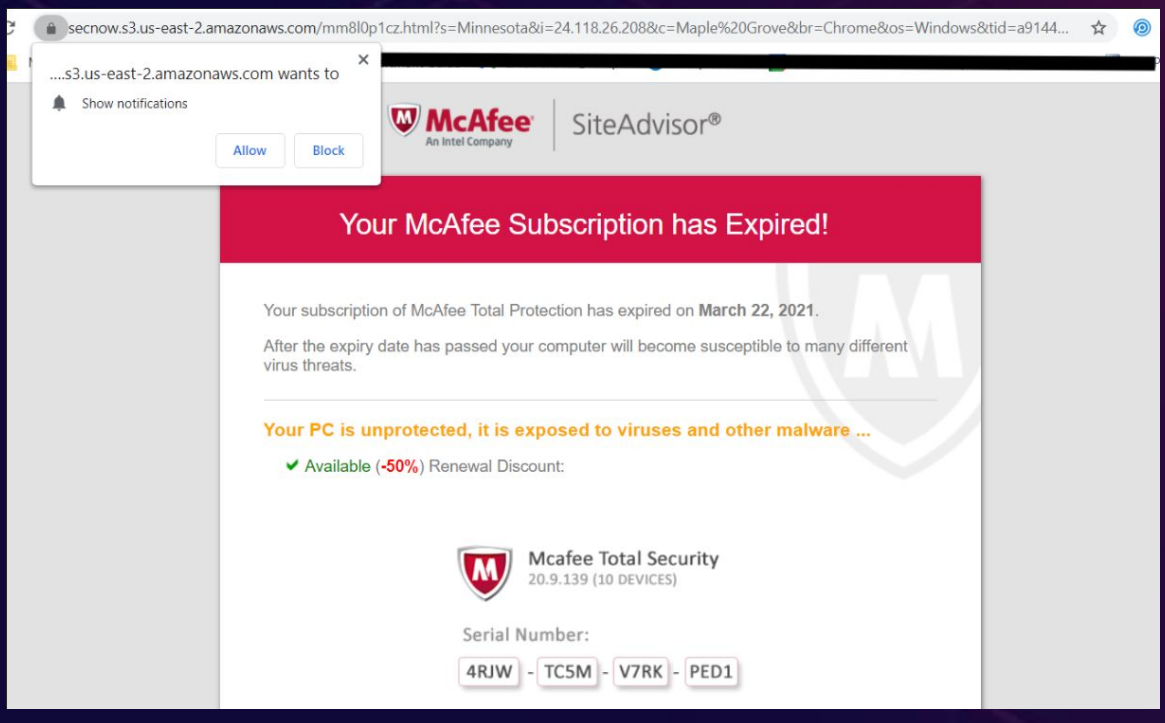
For years, Zirconium have used their understanding of Ad Tech in order to form dozens of convincing business entities to gain seats on major buying platforms.

On a rolling basis, the gang would run redirects to tech support scams that are cloaked in multiple layers of sophisticated Javascript obfuscation.

As of last quarter, they've re-emerged with several large scale cloaking campaigns that push Bitcoin scams in a Fizzcore-style manner.

YOSEC

The bulk of their activity targets Mac devices, particularly the Safari browser.



YOSEC
PEAK ACTIVITY:

ONGOING

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

The bulk of their activity targets Mac devices, particularly the Safari browser.

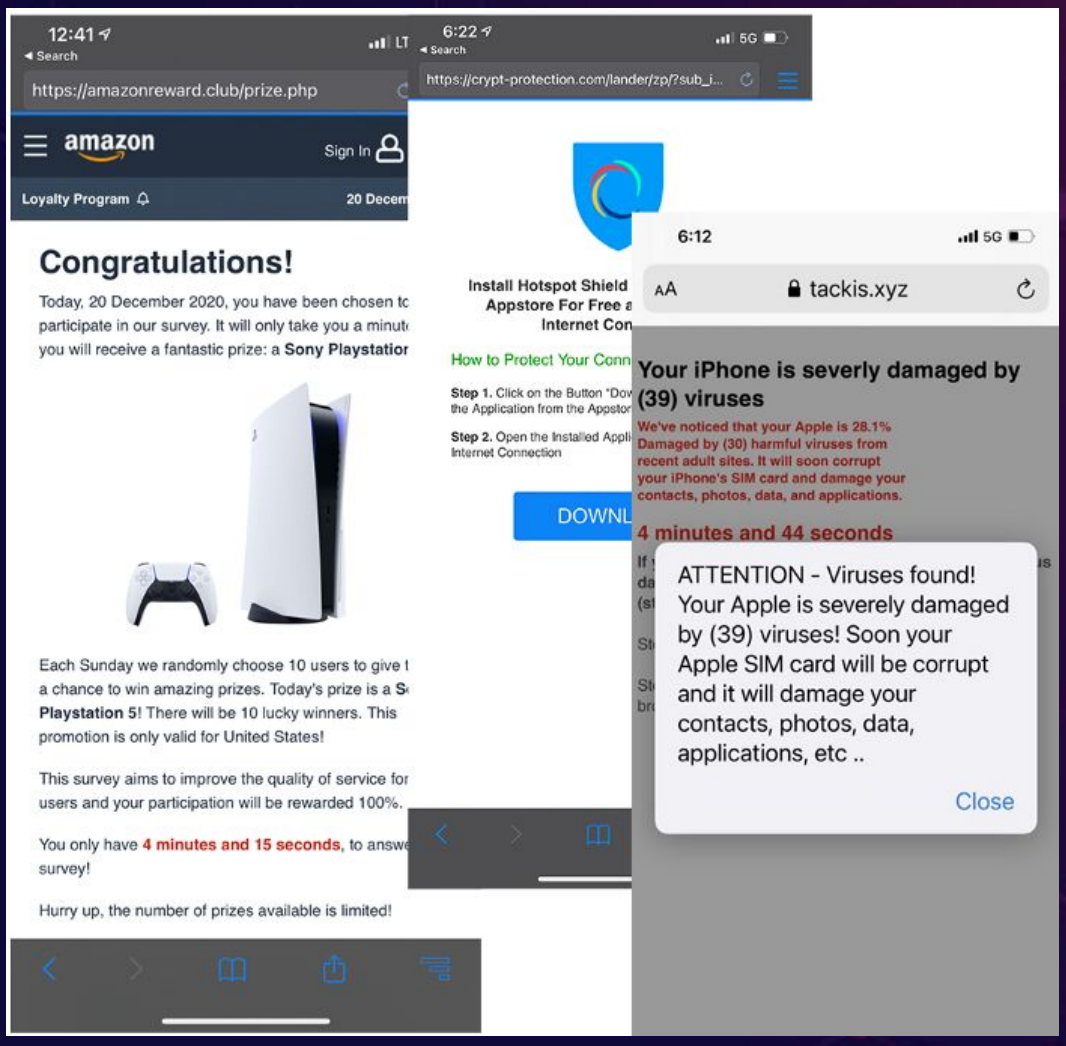
Yosec malvertising activities are categorized by short, targeted bursts, but at times we have seen them ramp up to large volumes over the course of several hours.

In February of 2021, Confiant was awarded CVE-2021-1765 for reporting an exploit leveraged by Yosec to bypass built-in security mitigations in Safari.

.

DCCBOOST

We estimate that this malvertiser routinely impacts tens of millions of ad impressions



DCCBOOST
PEAK ACTIVITY:

JANUARY

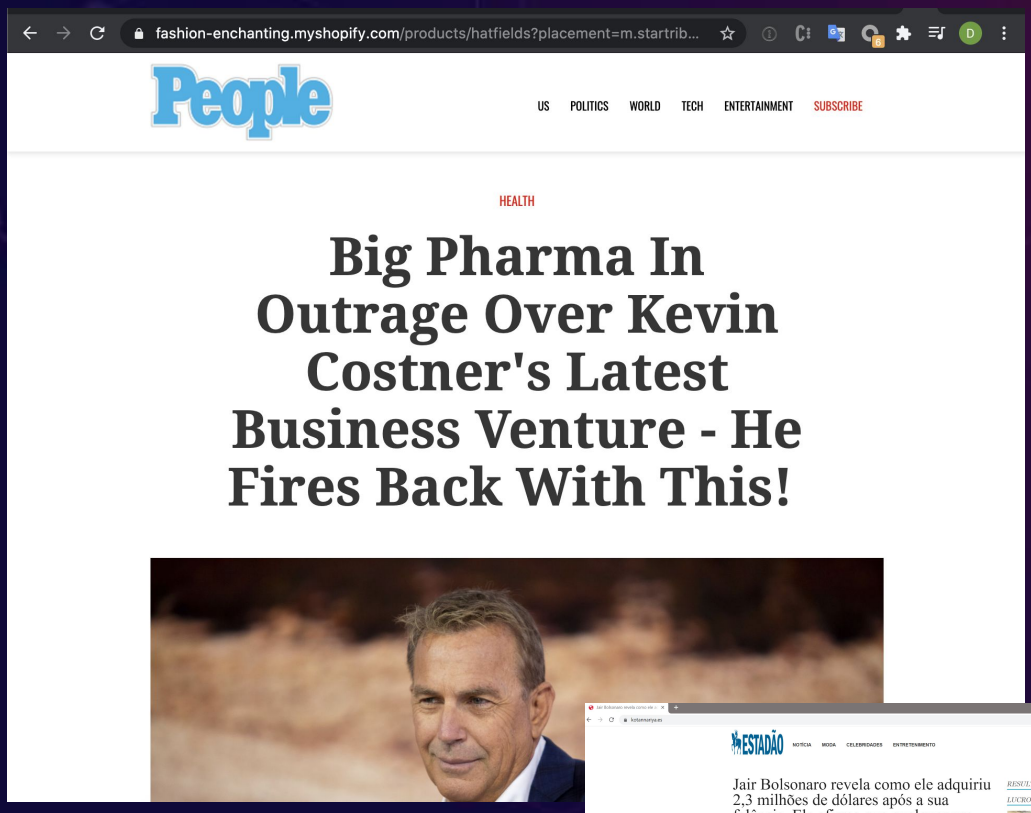
Notable characteristics: DCCBoost campaigns consistently include interesting malvertising innovations from a technical standpoint.

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.

MALICIOUS CLICKBAIT ATTACKS

The attackers will launch a display ad campaign for a benign looking brand and then "flip" the creative to some clickbait messaging



MALICIOUS CLICKBAIT

PEAK ACTIVITY:

ONGOING

Notable characteristics: 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 European countries and Canada at larger scale, but there is significant activity in the US as well. This is a fundamental shift compared to one or two short years ago when forced redirections were the preferred flavor of ad-based malware.

Violation rates for both Security and Quality issues rose significantly in Q1 vs. Q4.

For the first time, Google's Security violation rate exceeded the industry average.

KEY TAKEAWAYS

SSPs struggled to meet publisher's expectations when it came to brand and category blocks. One in every 30 impressions flagged by Confiant was due to a missed brand or category exclusion.

Health was the most-blocked ad category, representing close to one-third of all category blocks.

1 in every 150 impressions was dangerous or highly disruptive to the user.

CONFIANT

MALVERTISING + AD QUALITY INDEX

MAQ INDEX

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

Q1 2021