CONFIANT

Demand Quality Report

2020 Year in Review

Introduction

Confiant's **Demand Quality Report** is a quarterly look into the quality of demand in digital advertising. Using a sample of over 650 billion impressions monitored in real time in 2020, 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 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 Demand Quality Report, 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 eleventh in the series, covers Q4 2020 and full-year 2020.

Methodology

To compile the research contained in this report, Confiant analyzed a normalized sample of **more than 650 billion advertising impressions** monitored from January 1 to December 31, 2020, from over **40,000 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.

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.

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

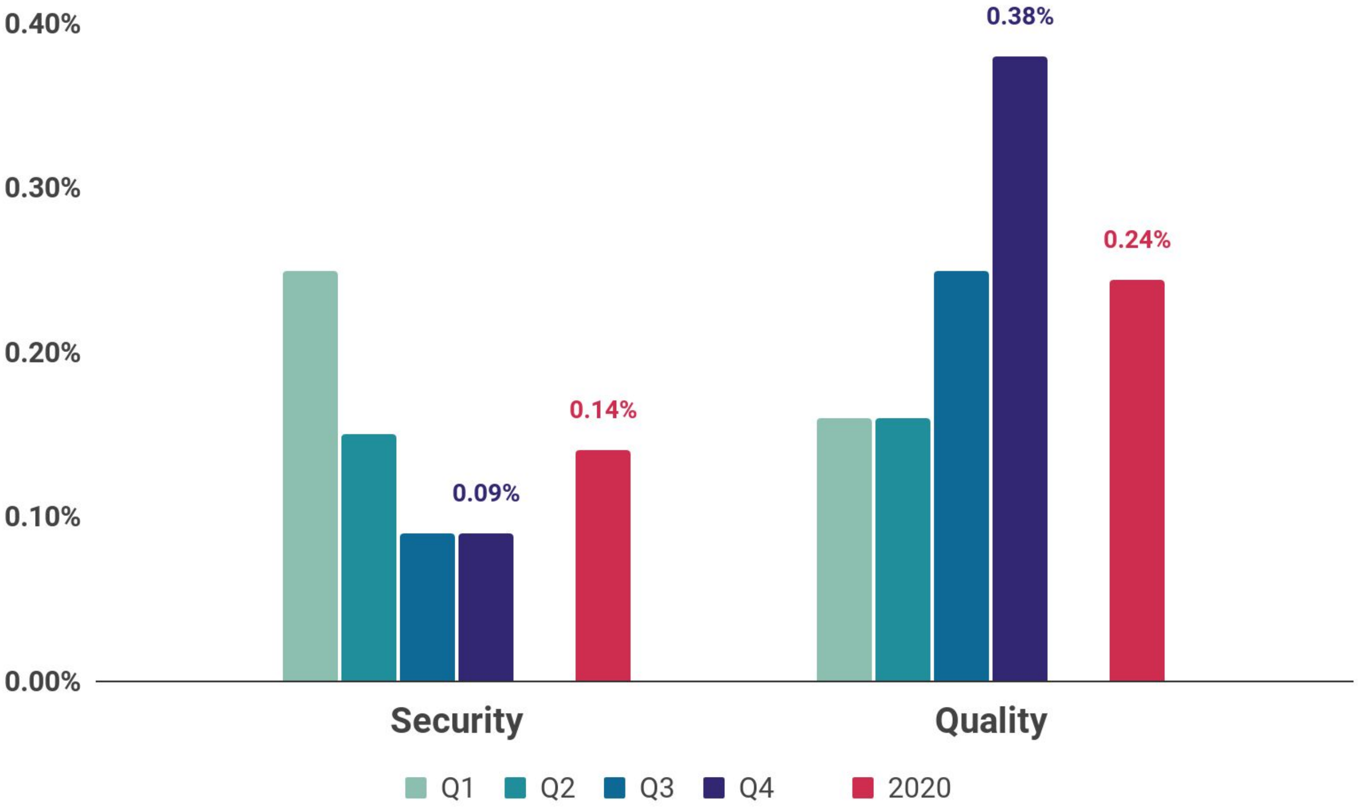
Non-security issues related to **ad behavior**, **technical characteristics**, or **content**. Top issues include:

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

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

Industry View: 2020

How did the industry fare in 2020?

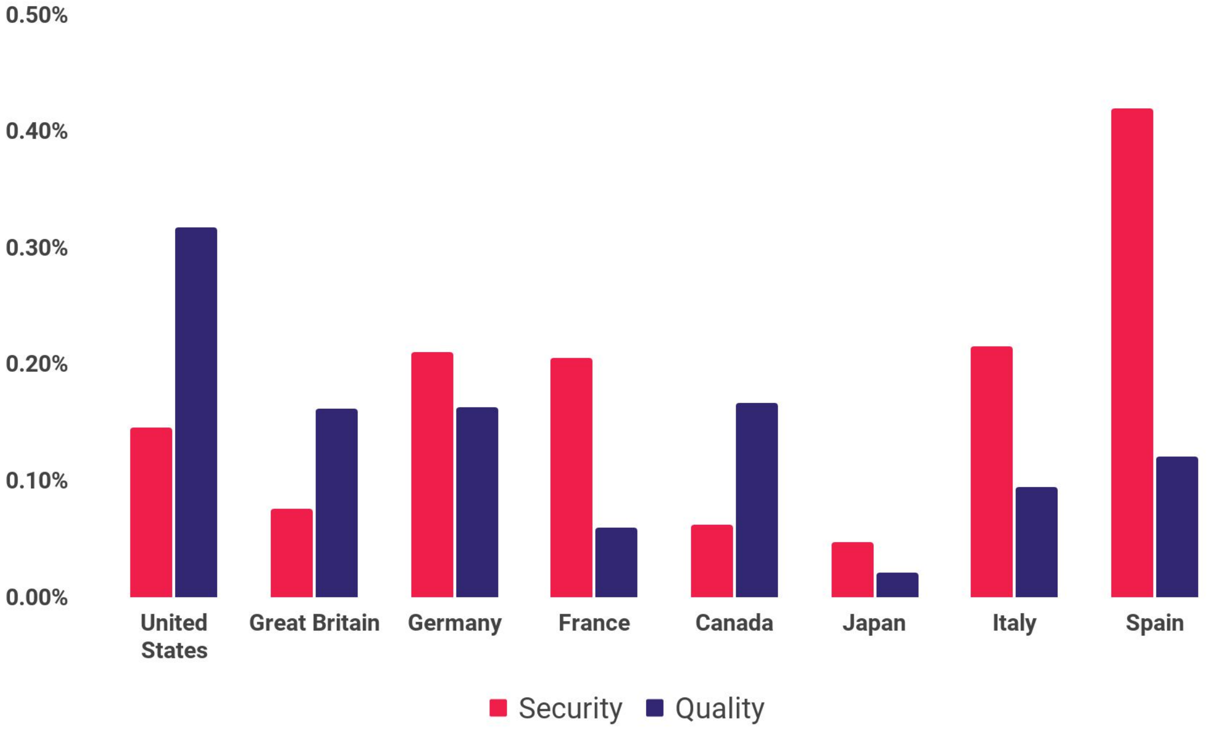


The **Security violation rate** for 2020 was 0.14%. The rate fell significantly from Q2 to Q3, then remained flat at just under 0.10% for the remainder of the year. This improvement was largely driven by better quality control at two of the largest SSPs.

Conversely, the **Quality violation rate** increased from 0.25% in Q3 to 0.38% in Q4, an **increase of over 50%**. The Quality violation rate for the full year was 0.24%.

In 2020, **1 in every 260** impressions was **dangerous** or **highly disruptive** to the user.

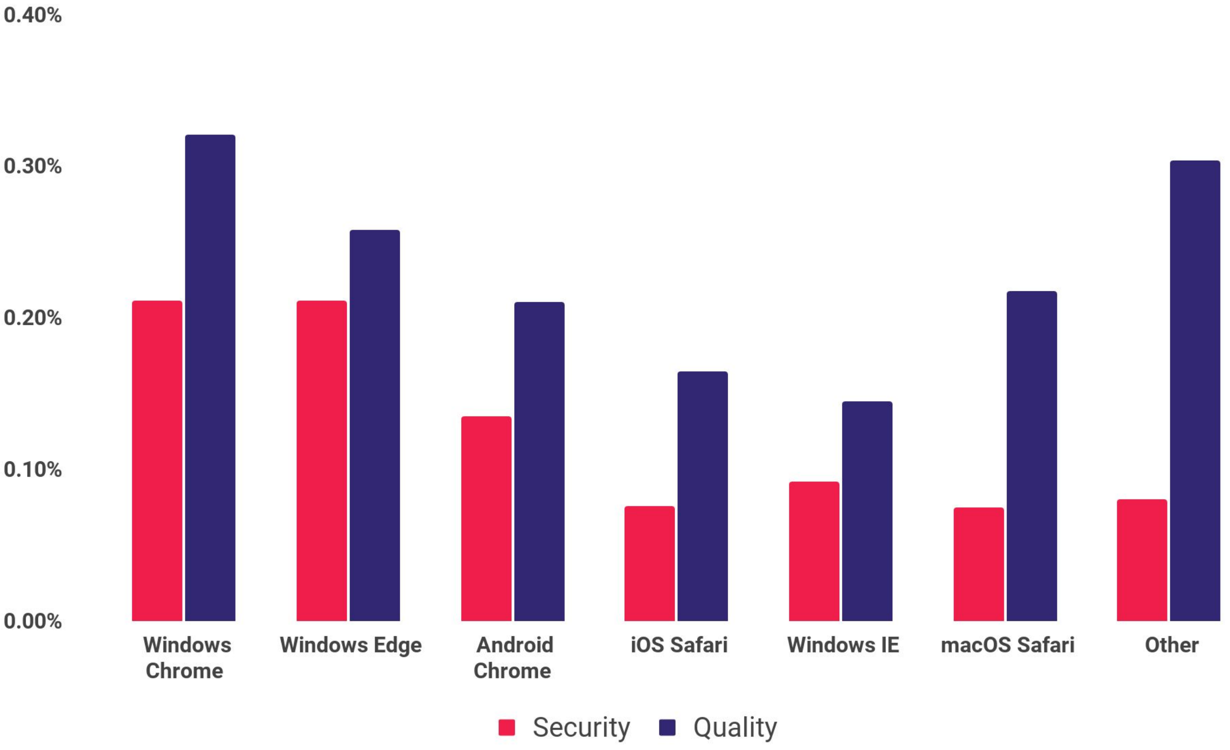
2020 Violation Rates by Country



Continuing a trend from past years, **European markets in 2020 tended to have higher rates of Security violations** than the U.S. or Canada. However, the gap between the U.S. and Europe closed over the year, with the U.S. Security rate finally exceeding all major European markets by Q4.

Quality violations remained more prevalent in the U.S. than elsewhere in 2020, including in Q4.

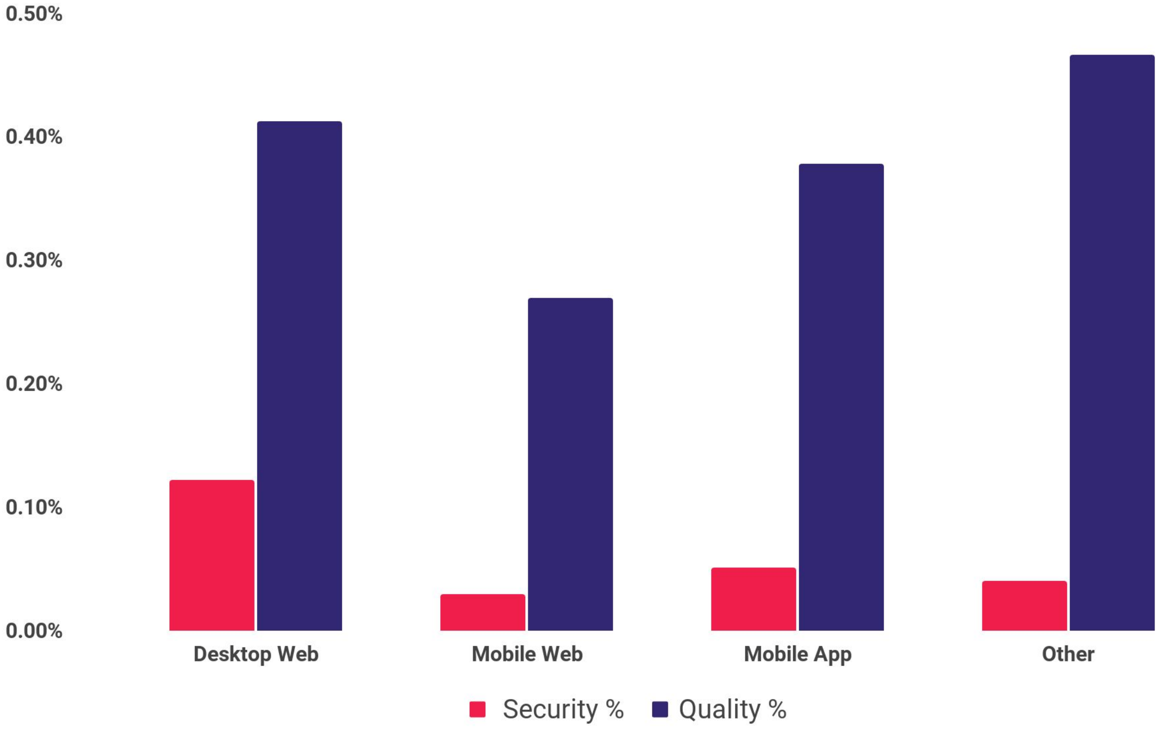
2020 Violation Rates by User Agent



Chrome for Windows was the **top source of Security issues in 2020**, with a violation rate more than twice that of iOS Safari. This reverses the trend from 2019, when Safari had the highest rate of Security violations.

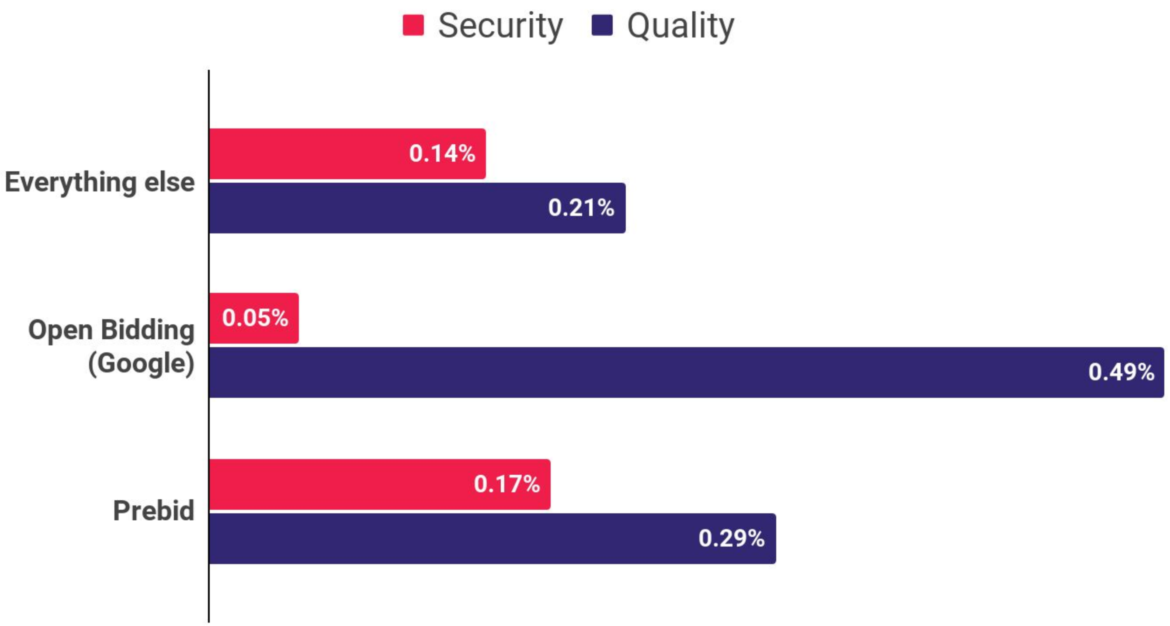
Chrome for Windows also had the **highest rate of Quality violations** in 2020, a repeat of their 2019 performance.

2020 Violation Rates by Environment



In a reversal of previous years, **Desktop computers were the most vulnerable target for threat actors in 2020**, with Security violation rates far in excess of those for Mobile Web or Mobile App. With **COVID-19 leaving many users (and workers) stuck at home**, it's not surprising that threat actors shifted to desktop as their primary target.

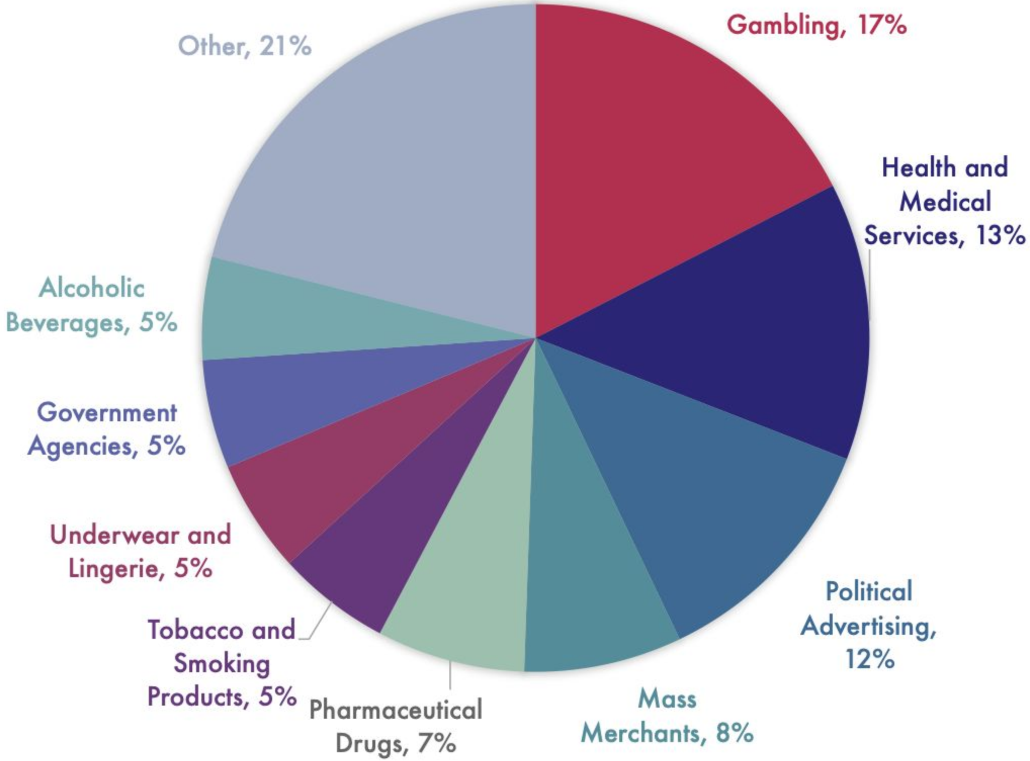
2020 Violation Rates by Header Bidding Framework



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 2020, we found that demand flowing through **Open Bidding performed significantly better than other sources for Security, but lagged on Quality issues**.

Most Blocked Ad Categories



"Other" includes over 100 other categories

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

In Q4, **almost 80% of category blocks were tied to just 9 categories**. While most of these categories related to perennial areas of sensitivity like Gambling, others likely rose to prominence due to seasonal factors (Mass Merchant in the lead-up to the holidays) or specific events (Health and Medical Services due to COVID-19).

SSP Rankings

Q4 2020 US SSP Rankings

In Q4, Confiant tracked impressions from over **100 SSPs**. However, **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 impressions** a quarter.

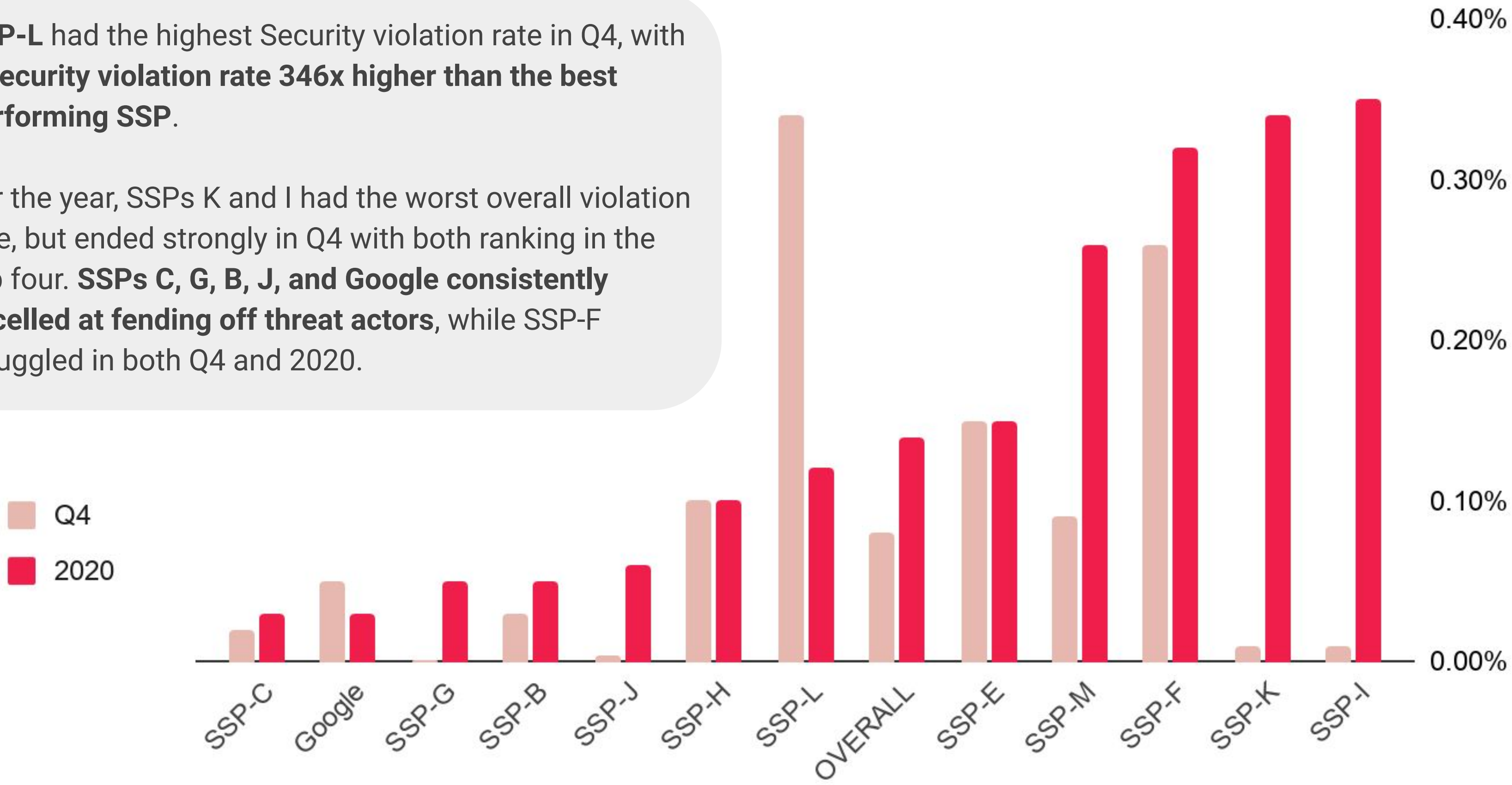
We identify Google Ad Exchange within these rankings. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges, which one could reasonably expect to translate into higher efficacy when it comes to catching issues. Our data confirms this assumption, with Google Ad Exchange consistently placing among the top performers.

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

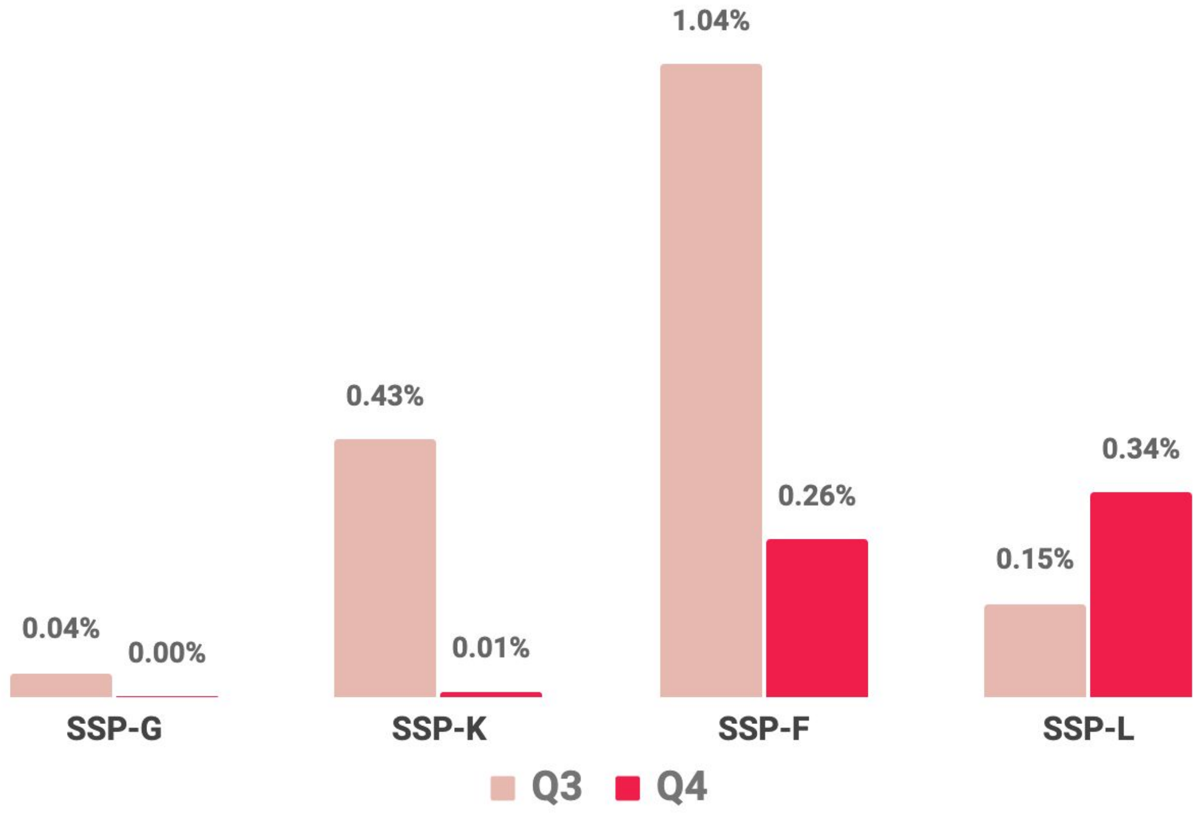
Q4 and 2020 Security Violation Rate by SSP

SSP-L had the highest Security violation rate in Q4, with a **security violation rate 346x higher than the best performing SSP**.

For the year, SSPs K and I had the worst overall violation rate, but ended strongly in Q4 with both ranking in the top four. **SSPs C, G, B, J, and Google consistently excelled at fending off threat actors**, while SSP-F struggled in both Q4 and 2020.



Security Violation Rate: Q3 vs. Q4

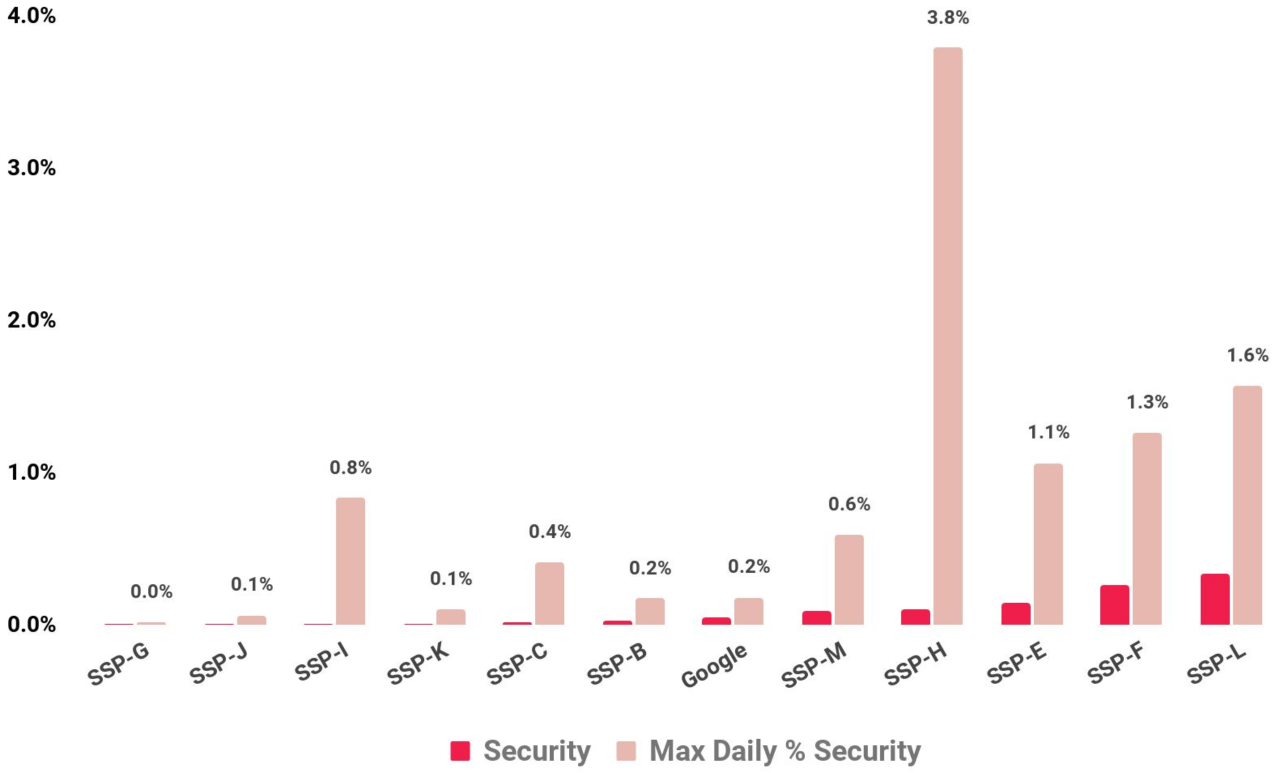


Last quarter’s worst performer, **SSP-F, made strong progress in Q4, reducing their Security violation rate by 75%**. However, they still ended the quarter with the 2nd-to-worst violation rate.

SSP-L’s Security violation rate more than doubled in Q4, dropping them to last place.

On the other end of the spectrum, **SSP-K reduced their violation rate by a whopping 98%**.

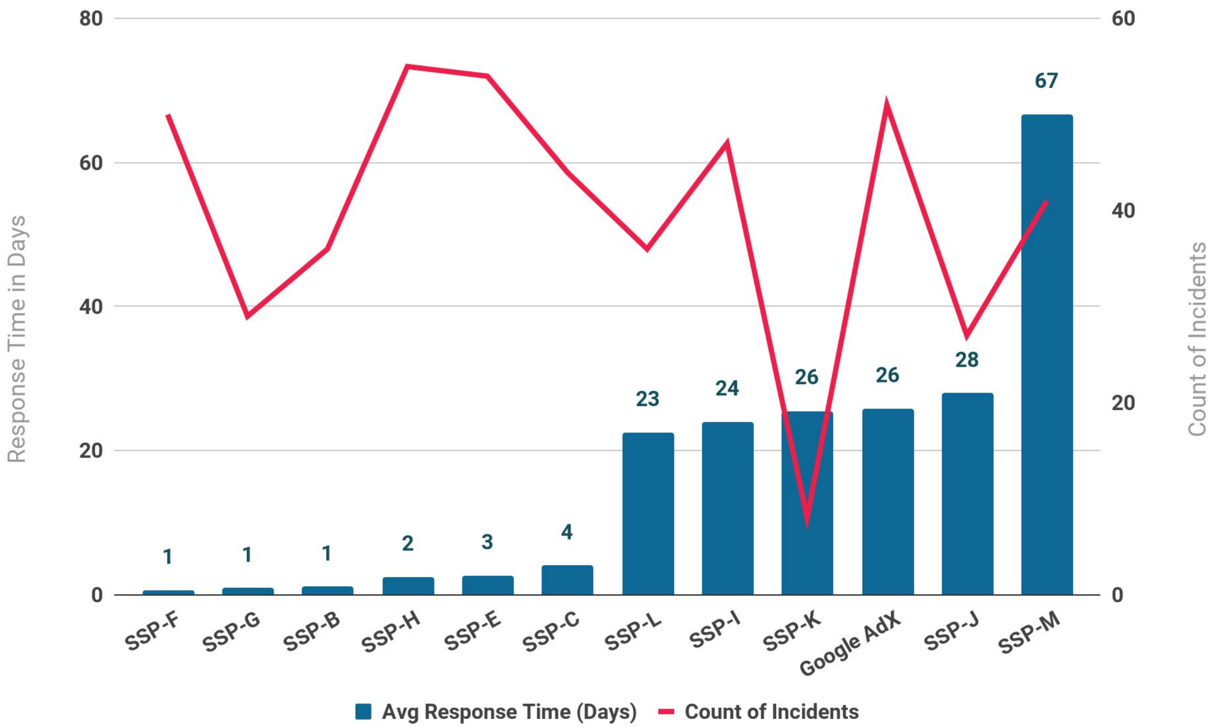
Q4 Daily Maximum Malicious Rate by SSP



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, even good performing **SSPs 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 Q4



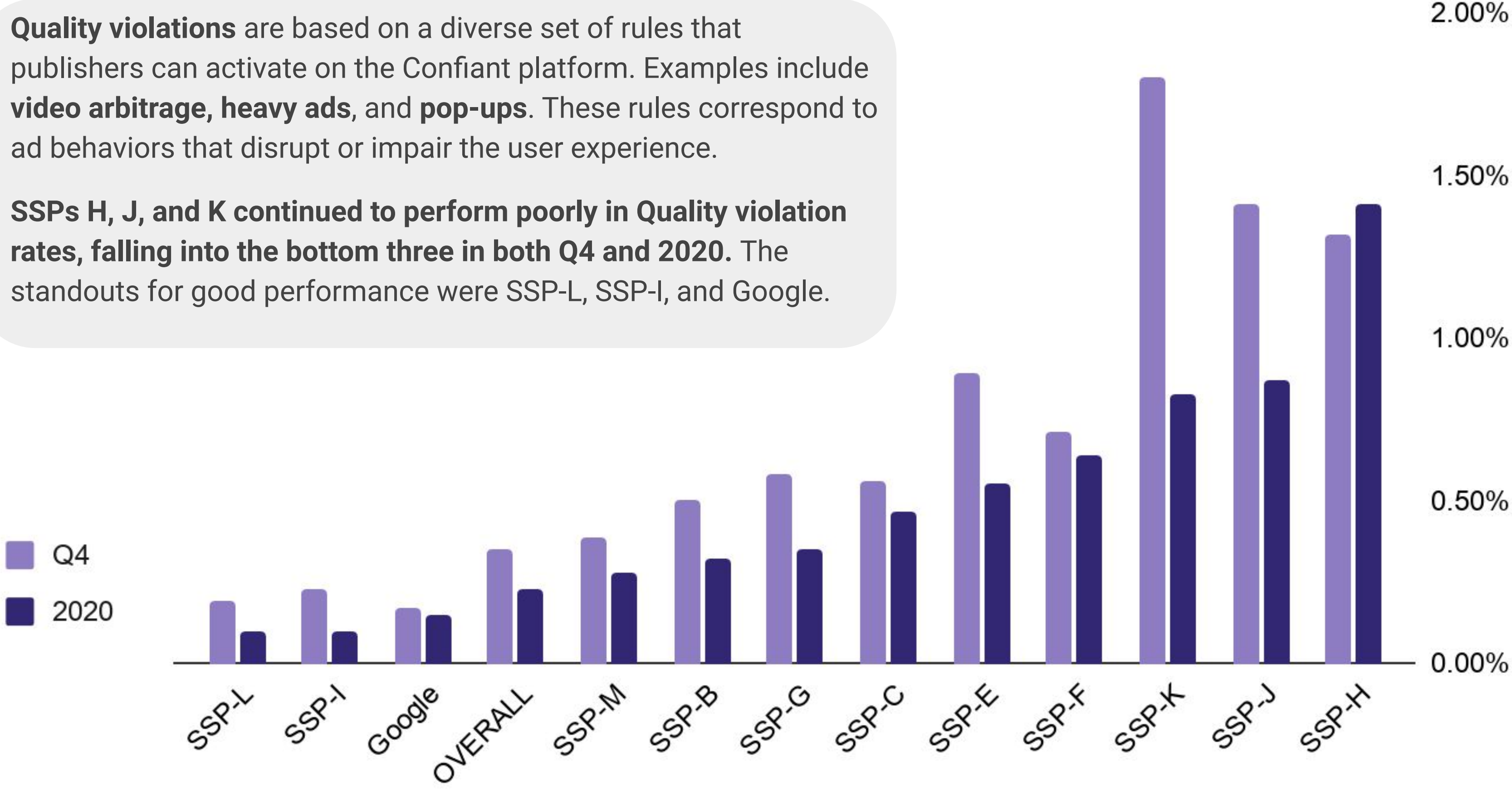
It's important to understand **how long threats persist on an SSP** once an attack is underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. On this measure, we see huge differences among the major SSPs.

In Q4, SSP-M's average response time increased from 14 to 67 days, dropping them into last place. **Notably, three SSPs achieved average response times of 1 day or less**, with SSPs F and G maintaining that outstanding level of performance over the past two quarters.

Quality Violation Rate by SSP

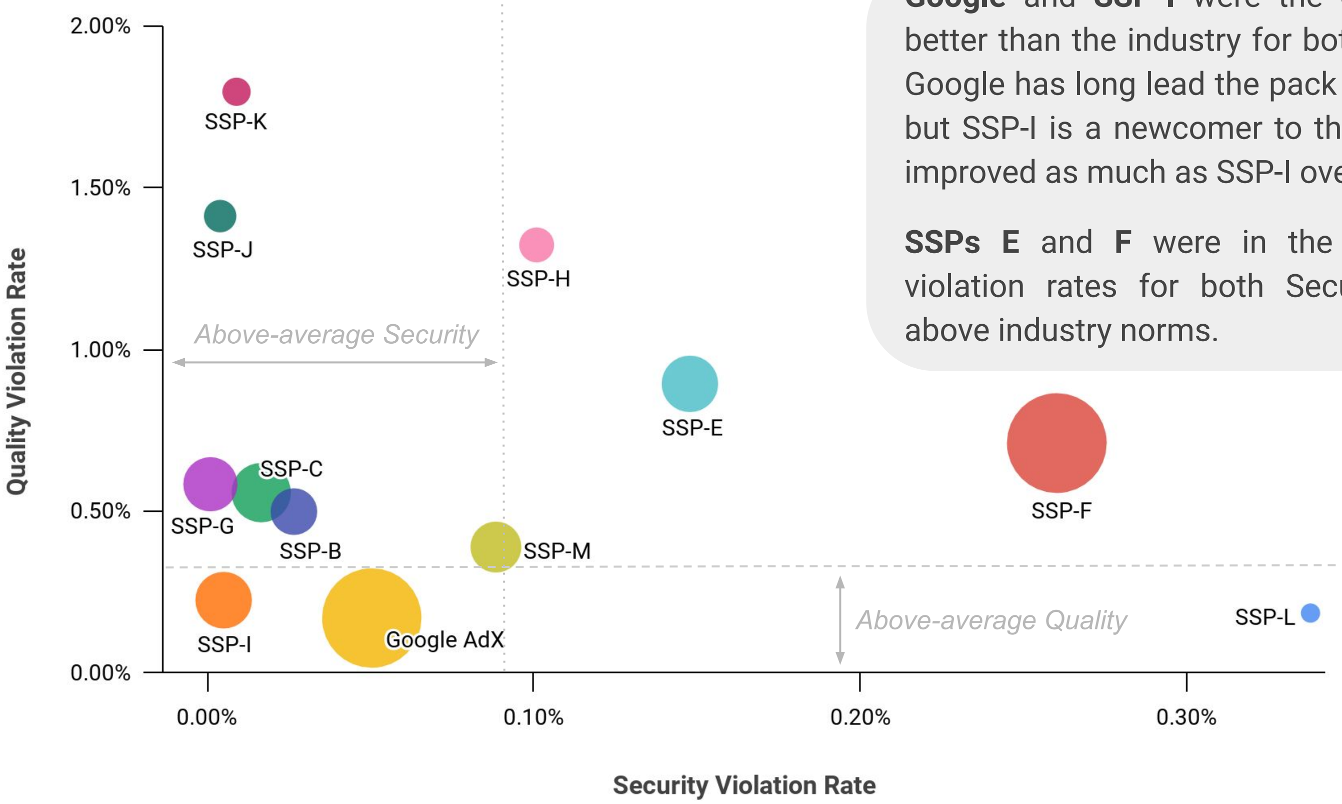
Quality violations are based on a diverse set of rules that publishers can activate on the Confiant platform. Examples include **video arbitrage, heavy ads**, and **pop-ups**. These rules correspond to ad behaviors that disrupt or impair the user experience.

SSPs H, J, and K continued to perform poorly in Quality violation rates, falling into the bottom three in both Q4 and 2020. The standouts for good performance were SSP-L, SSP-I, and Google.



The worst performing SSP delivered security issues at **346x the rate** of the best

Q4 Violation Rates by SSP Size



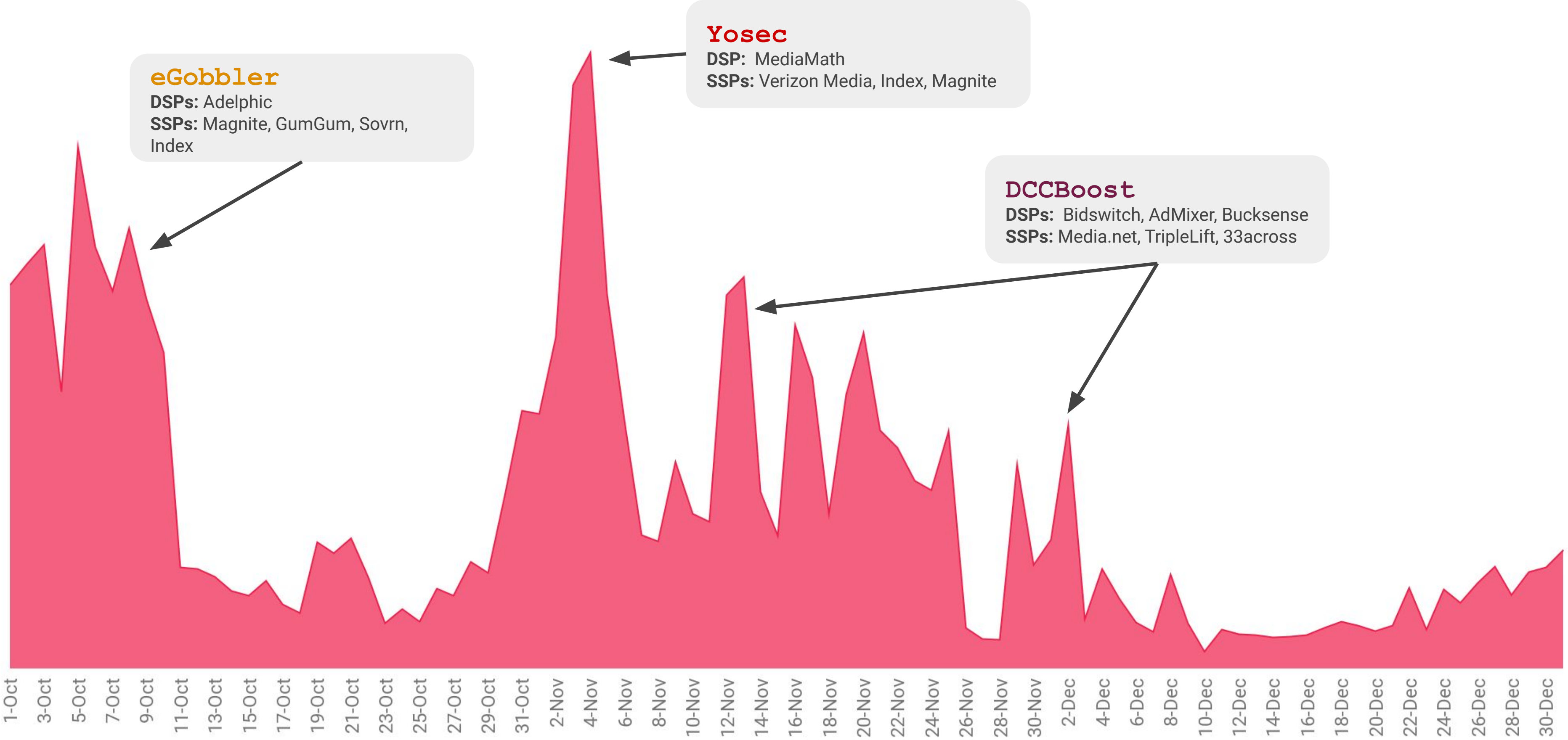
Google and **SSP-I** were the only SSPs to perform better than the industry for both Security and Quality. Google has long lead the pack across both measures, but SSP-I is a newcomer to the leaderboard. No SSP improved as much as SSP-I over the course of 2020.

SSPs E and **F** were in the opposite camp, with violation rates for both Security and Quality well above industry norms.

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

Major Threat Groups Active in Q4

Notable Threat Activity



eGobbler

DSPs: Adelphic

SSPs: Magnite, GumGum, Sovrn, Index

Yosec

DSP: MediaMath

SSPs: Verizon Media, Index, Magnite

DCCBoost

DSPs: Bidswitch, AdMixer, Bucksense

SSPs: Media.net, TripleLift, 33across

eGobbler

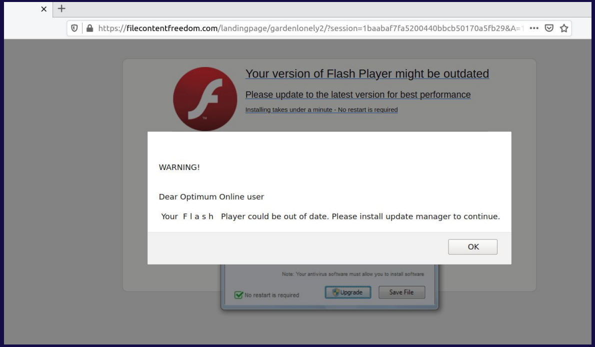
Peak activity: early October

Notable characteristics: eGobbler runs their campaigns in big waves that usually gravitate around the weekends.

The majority of their recent activity has been centered primarily around the United States and Europe, where they deliver disruptive, highly targeted drive-by downloads and carrier-branded scams.

This is a sophisticated attacker that has been observed to exploit sandbox bypasses in both Chrome and Safari in order to maximize the impact of their campaigns.

We believe there to be a close relationship between Nephos7 and eGobbler based on certain shared tactics, techniques, and timing.



https://filecontentfreedom.com/landingpage/gardenlonely2/?session=1baabaf7fa5200440bbcb50170a5fb29&A=1

Your version of Flash Player might be outdated

Please update to the latest version for best performance

Installing takes under a minute - No restart is required

WARNING!

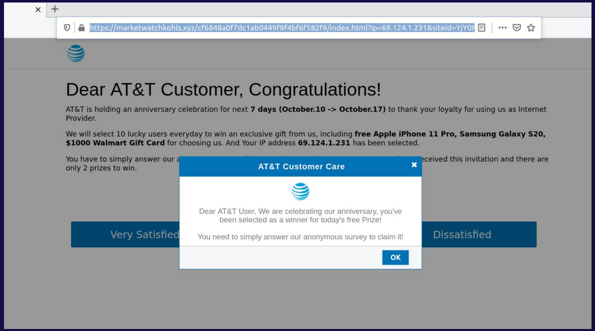
Dear Optimum Online user

Your Flash Player could be out of date. Please install update manager to continue.

OK

Note: Your antivirus software must allow you to install software

☑ No restart is required



https://marketwatchkohls.xyz/cf6848a0f7dc1ab0449f9f4bf6f582f9/index.html?ip=69.124.1.231&siteid=YjY0N

Dear AT&T Customer, Congratulations!

AT&T is holding an anniversary celebration for next **7 days (October.10 -> October.17)** to thank your loyalty for using us as Internet Provider.

We will select 10 lucky users everyday to win an exclusive gift from us, including **free Apple iPhone 11 Pro, Samsung Galaxy S20, $1000 Walmart Gift Card** for choosing us. And Your IP address **69.124.1.231** has been selected.

You have to simply answer our a eceived this invitation and there are only 2 prizes to win.

AT&T Customer Care

Dear AT&T User, We are celebrating our anniversary, you've been selected as a winner for today's free Prize!

You need to simply answer our anonymous survey to claim it!

OK

Yosec

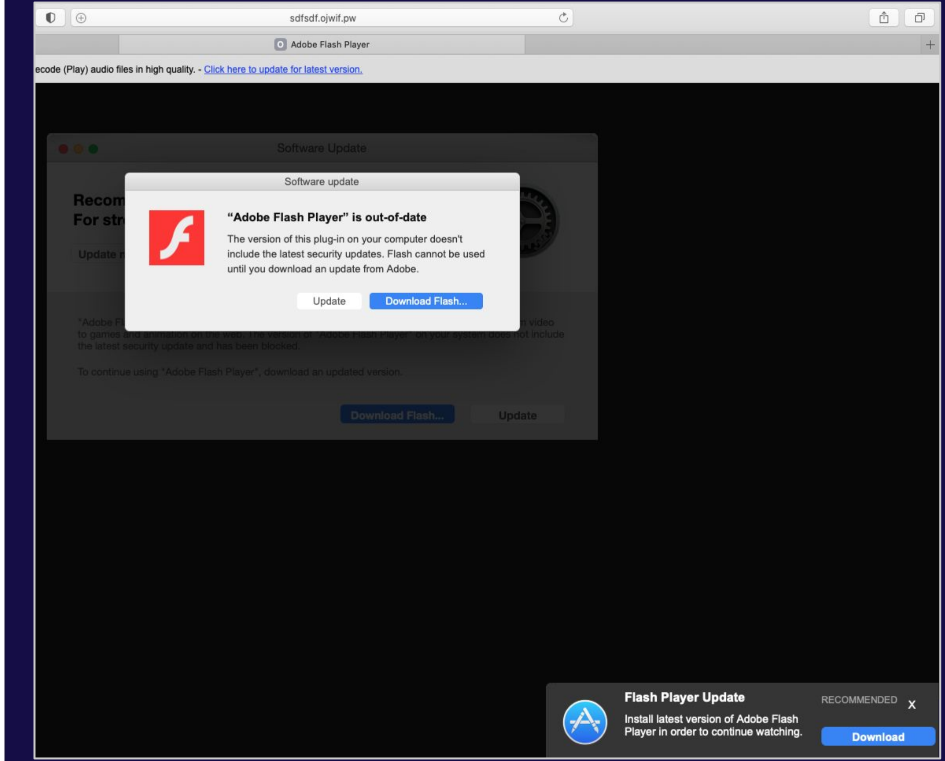
Peak activity:early November

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

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 observed up them to 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 in order to bypass built-in security mitigations in Safari.



sdfsdf.ojwif.pw

Adobe Flash Player

ecode (Play) audio files in high quality. - Click here to update for latest version.

Software Update

Recom
For str

Software update

“Adobe Flash Player” is out-of-date

The version of this plug-in on your computer doesn't include the latest security updates. Flash cannot be used until you download an update from Adobe.

"Adobe F… …n video to games and animation on the web. The version of "Adobe Flash Player" on your system does not include the latest security update and has been blocked.

To continue using "Adobe Flash Player", download an updated version.

Flash Player Update

RECOMMENDED

Install latest version of Adobe Flash Player in order to continue watching.

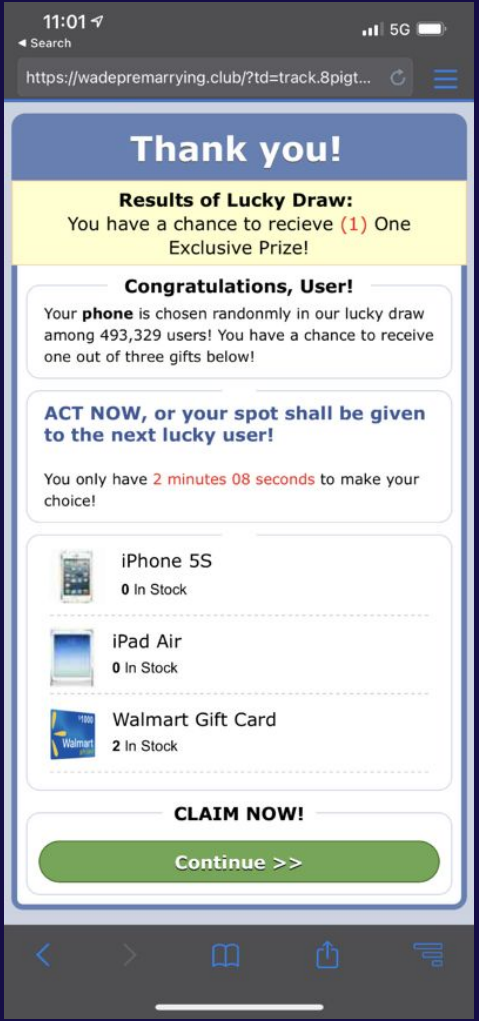
DCCBoost

Peak activity: early November and early December

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.

The Confiant Security Team recently published a detailed analysis of DCCBoost’s end of year attack on our blog:



Thank you!

Results of Lucky Draw:
You have a chance to recieve (1) One Exclusive Prize!

Congratulations, User!

Your **phone** is chosen randonmly in our lucky draw among 493,329 users! You have a chance to receive one out of three gifts below!

ACT NOW, or your spot shall be given to the next lucky user!

You only have 2 minutes 08 seconds to make your choice!

iPhone 5S
0 In Stock

iPad Air
0 In Stock

Walmart Gift Card
2 In Stock

CLAIM NOW!

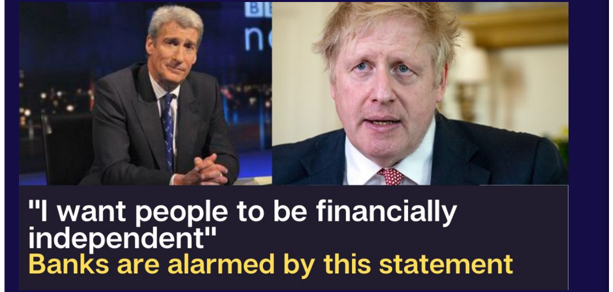
Fizzcore-style attackers

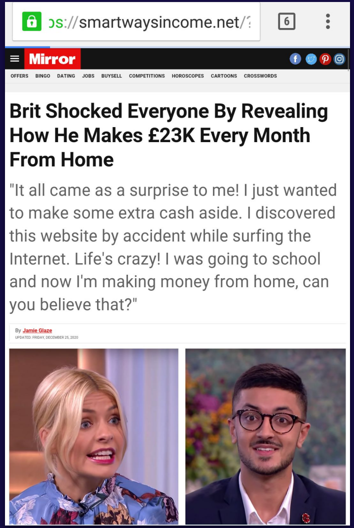
Peak activity: throughout the quarter

Notable characteristics: In Q3, Confiant witnessed an explosion of new threat actors leveraging Fizzcore-style attacks, as well as a growing sophistication in text and image manipulation. Q4 saw a relative normalization.

While Germany and the UK continue to be prime targets, interest in other geographies spiked and faded, as seen in Australia (very active until October). Eastern Europe is becoming a strong focus of interest since November (e.g. Poland, Hungary, Romania).

Additionally, some attackers have gained persistence by aiming at ad platforms (tier-2, native) that do not police against investment scams and provide demand to large SSPs.


"I want people to be financially independent"
Banks are alarmed by this statement


ɔs://smartwaysincome.net/

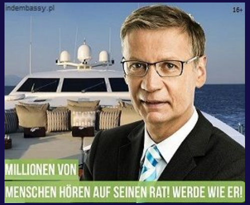
Mirror

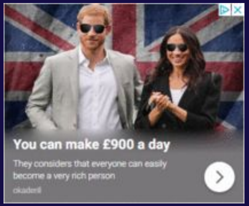
OFFERS BINGO DATING JOBS BUYSELL COMPETITIONS HOROSCOPES CARTOONS CROSSWORDS

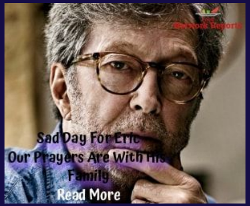
Brit Shocked Everyone By Revealing How He Makes £23K Every Month From Home

"It all came as a surprise to me! I just wanted to make some extra cash aside. I discovered this website by accident while surfing the Internet. Life's crazy! I was going to school and now I'm making money from home, can you believe that?"

By Jamie Glaze
UPDATED: FRIDAY, DECEMBER 25, 2020




You can make £900 a day
They considers that everyone can easily become a very rich person
okadenl



Conclusion

2020

For 2020 as a whole, we detected **serious security or quality issues with 1 in every 260 impressions**.

With COVID-19 leaving many users stuck at home, **threat actors shifted back to desktop** as a primary target. Security violation rates for desktop exceeded those for mobile web and app.

Threat actors are employing more **sophisticated cloaking techniques** in an escalating battle with ad-quality scanners.

Q4

The **worst-performing SSP** of the top 12 was over **300x** as likely to deliver a **malicious ad** compared to the best.

Almost 80% of category blocks were tied to just 9 categories, with **Gambling**, **Health**, and **Political being the three most blocked**.

About Confiant

Confiant's mission is to make the digital world safe for everyone.

Confiant is a cybersecurity ad tech and malware prevention services provider. We help publishers and ad platforms take back control of the user ad experience. Our solution protects reputation, revenue, and resources by providing real-time verification of digital advertisements. Confiant's technology actively blocks and detects malicious activity and low-quality ads. Our platform provides 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 detect and protect billions of ad impressions per month for our clients, which include CBSi, Magnite, Gannett, and Politico.

Learn More