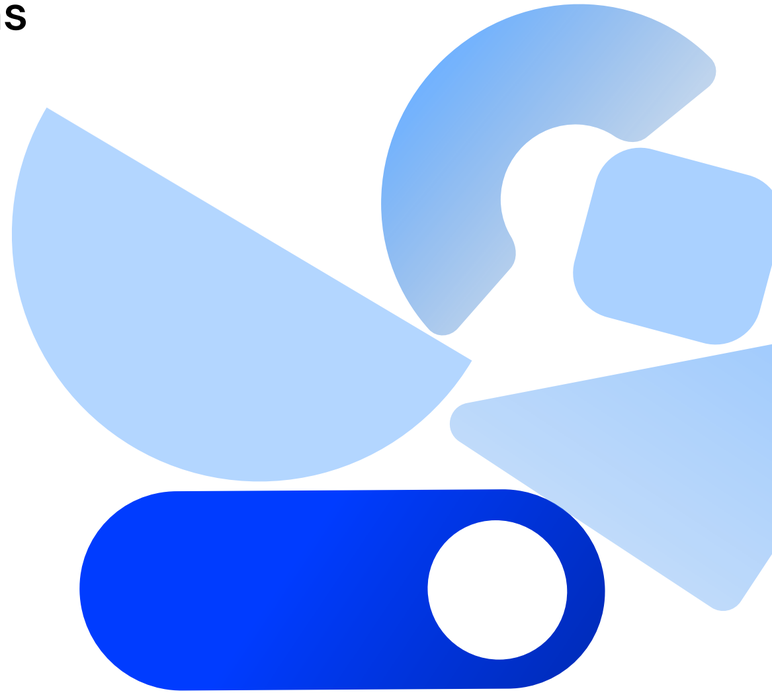
Q3 2024 Ad Quality Report

Ad Quality and Malvertising Trends

GeoEdge's Ad Quality Report examines the prevalence and origins of malvertising attacks on global devices across programmatic advertising channels. Here's how AdTech fared in Q3 2024:

- Auto-redirects surged to 61% of all malvertising in Q3, doubling from H1
- Video-driven redirects doubled in Q3, with 1 in every 460 video ads compromised
- Mobile attacks spiked to 76% in Q3, with 68% driven by auto-redirects

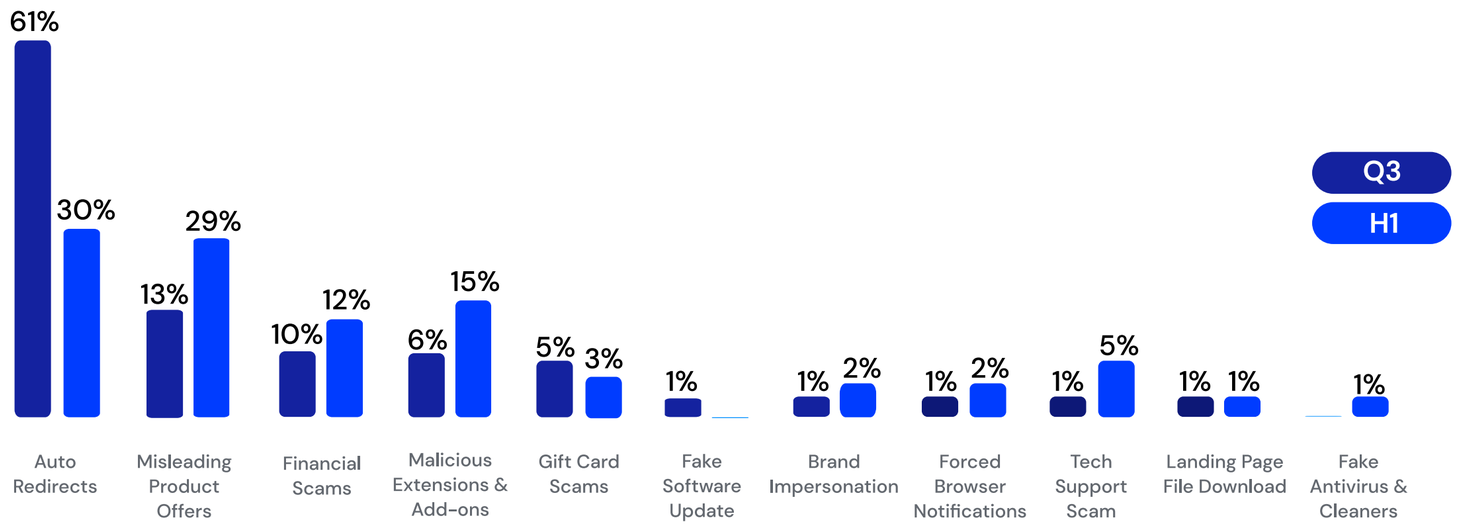


GeoEdge monitored and analyzed billions of advertising impressions across premium websites, apps, and SSPs to compile the research presented in this report. The data was collected using GeoEdge's real-time ad security solution, which assesses ad quality and malvertising blocking on live impressions across devices and channels.

Top Malvertising Attack Vectors in Q3 2024

Auto-Redirects account for 61% of all malvertising

Malvertising Attack Vectors - Q3 Vs H1 Average



AdTech Vs Auto-Redirects

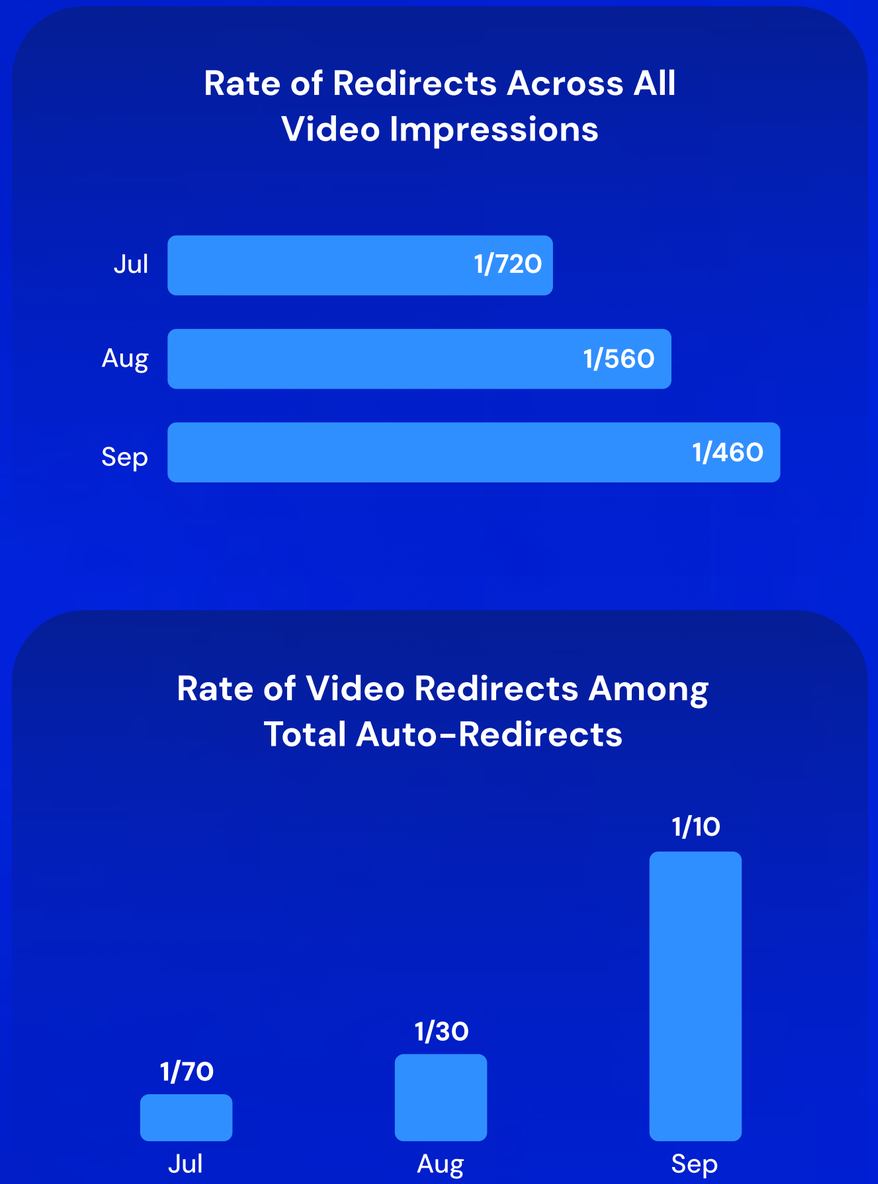
Auto-redirects have more than doubled this quarter compared to the H1 average. In contrast, misleading product offers have decreased by half, largely due to the significant rise in redirects.

The State of Video Malvertising

As vulnerabilities in video ads are increasingly exploited by cybercriminals, there is a noticeable rise in video-driven redirects. This quarter, the share of video redirects has doubled, signaling an alarming trend. In September alone, 1 in every 10 redirects originated from a video ad, while 1 in every 460 video ads was compromised by a malicious redirect.

Learn More

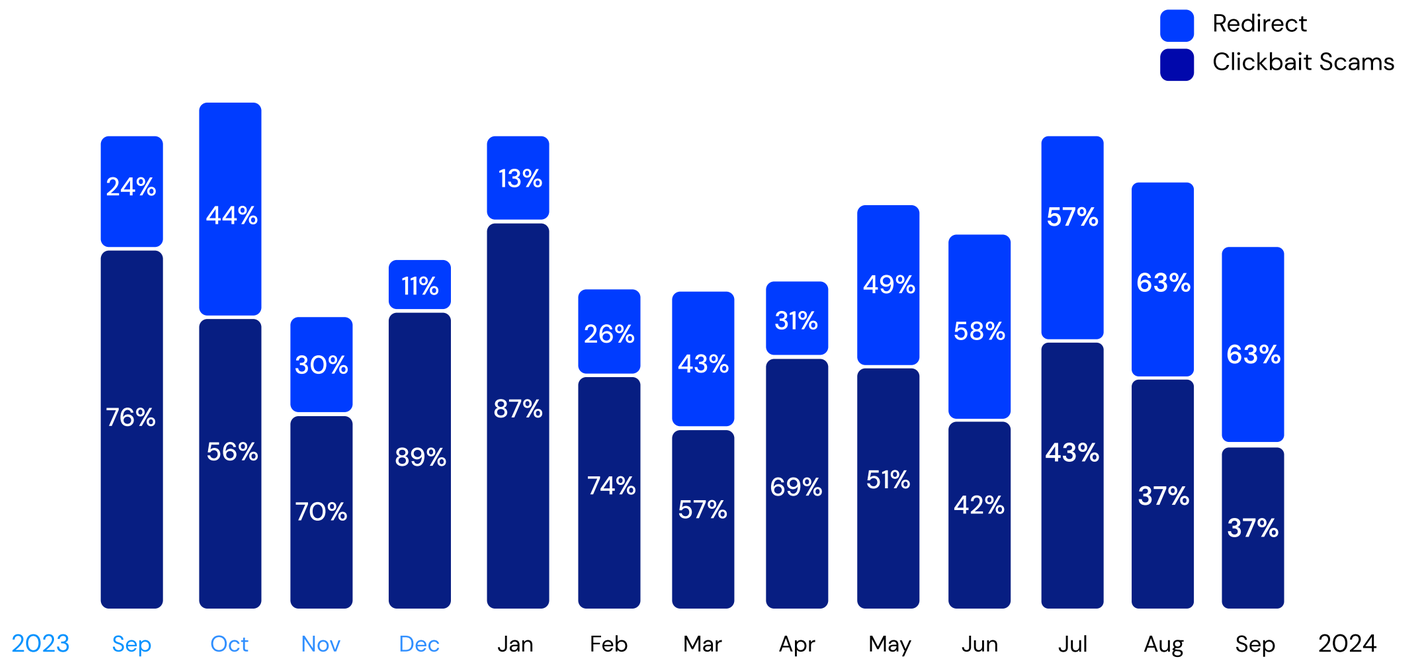
1 in 10 malicious redirects originates from a video ad

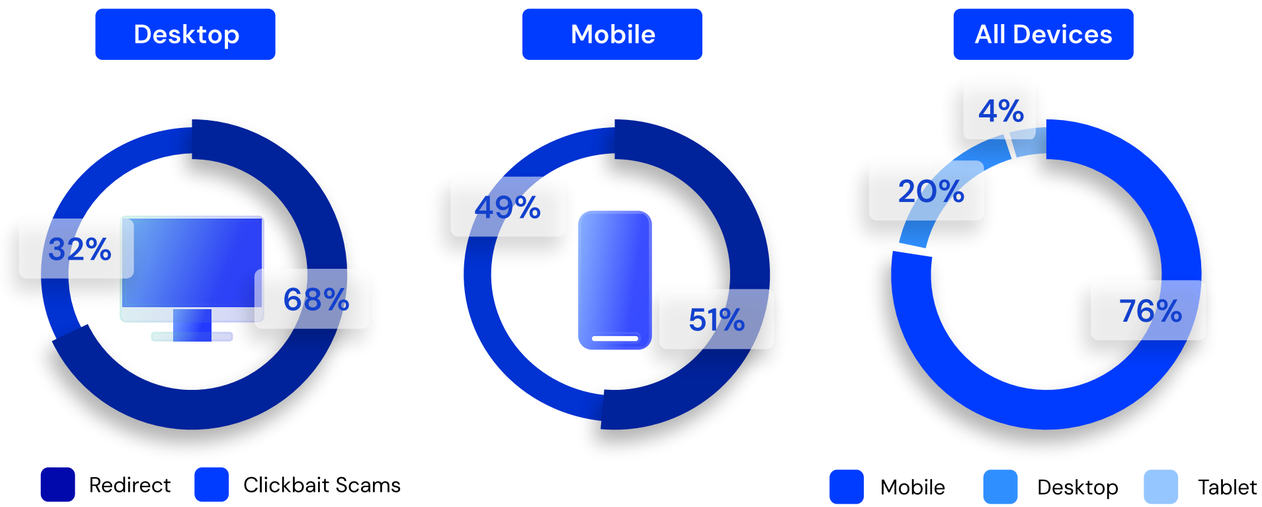


Redirect vs Clickbait Scams

Redirect vs Clickbait Scams:

Over the past 12 months, the expansion of redirects has steadily escalated. Even as the overall volume of malicious ads slightly decreased in August and September, forced redirects continued to be the primary tactic for scammers, now accounting for 63% of all scams.

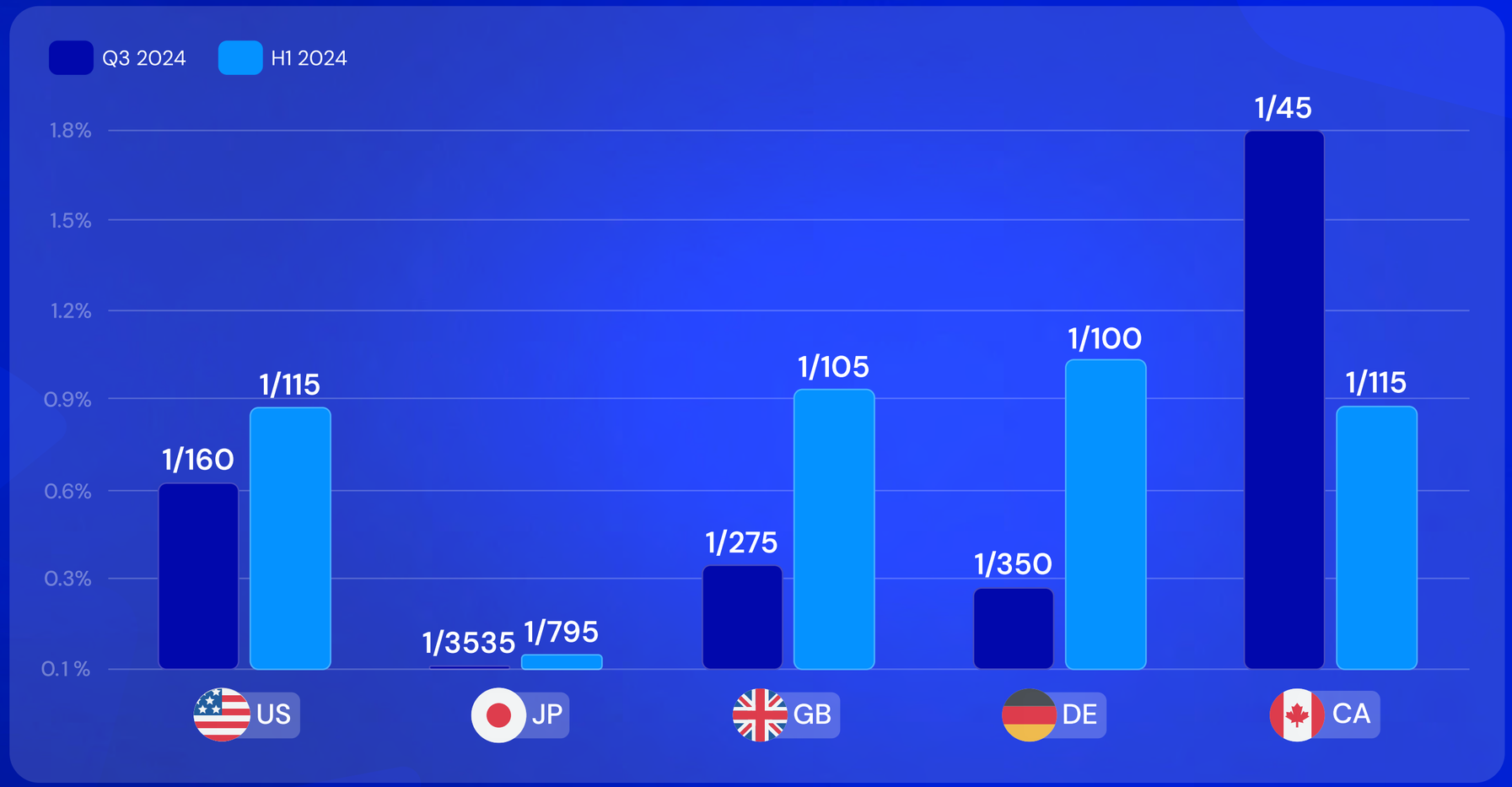




Device Targeting

Malvertising attacks shifted to mobile in Q3, with 76% now targeting mobile devices-68% involving redirects, and 32% clickbait scams. Desktop attacks saw an increase in redirects, which now account for 51% of incidents, up from the usual 80-90% clickbait focus.

Regional Malicious Activity



In Q3, 1 in 45 impressions in Canada was affected by malvertising, primarily due to a mobile auto redirect attack that began in late July and continued through the first week of September. In contrast, Japan is experiencing the lowest levels of malvertising we've seen in the past year, with incidents dropping to 3.5 times lower than the first half average.

Global SSP Rankings: Malvertising Rates and Malicious Activity

The top three most infected SSPs have shown significant improvement in Q3. Google, SSP06, and SSP12 have lowered infection rates down to the industry's average, now sitting below 0.5%.

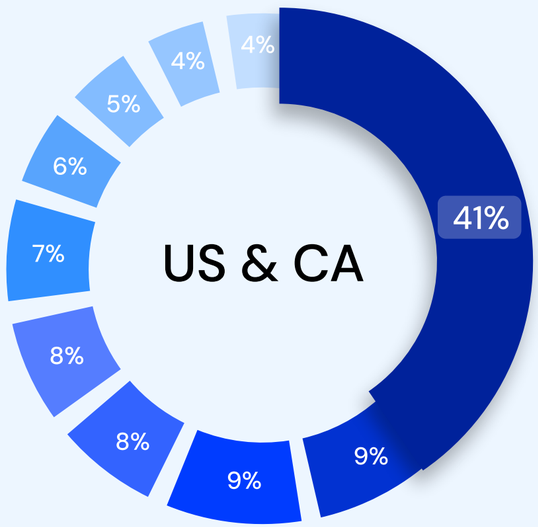
However, two trends stand out: SSP11, a midsized player, experienced a surge in clickbait attacks this quarter, pushing its infection rate to nearly 0.8%. Additionally, SSP13, known for its clean record, was notably impacted by financial scams and misleading product offers, particularly targeting readers of top U.S. news sites.

Learn More

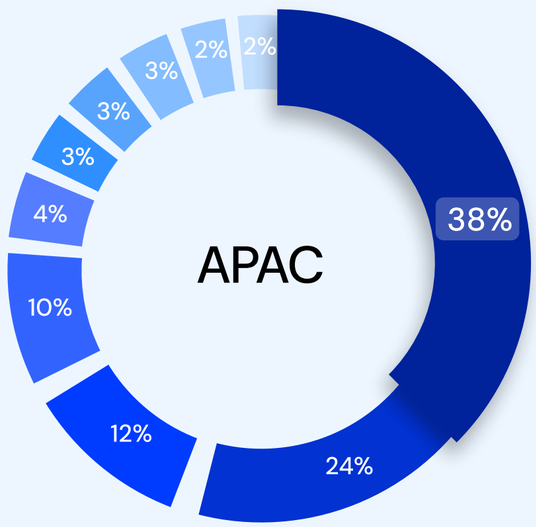
Ad Content Filtering Trends

In the U.S. and Canada, political and election ads, along with weapon-related content, remain key categories. Gambling remains the top blocked category, accounting for 54% of all content blocking by EU publishers. However, there's a notable rise in blocked mobile app categories, with health-related ads, app store games, and social networking ads steadily claiming more space in the blocking charts.

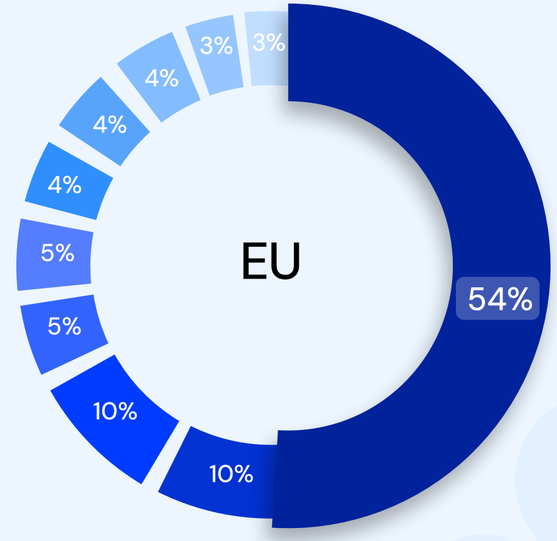
For the first time, App Store-related ads have climbed to third place across all regions, hitting a record high. In APAC, 33% of content blocking is tied to App Store/Play Store categories. It's clear that publishers are increasingly recognizing the value of filtering mobile app ads, particularly within certain categories.



- Gambling
- Weapons
- App Store Category - Games
- Law, Government & Politics
- Marijuana
- Election
- Tobacco
- News and Media
- Pharmaceuticals
- Alcohol



- Gambling
- Tobacco
- App Store Category - Social Networking
- Google Play Category - Comics
- Google Play Category - Weather
- Pharmaceuticals
- Religion
- App Store Category - Games
- App Store Category - Finance
- App Store Category - Books



- Gambling
- News and Media
- App Store Category - Social Networking
- Weight Loss
- Google Play Category - Shopping
- App Store Category - Health & Fitness
- Swimwear and Intimate Apparel
- App Store Category - Games
- Weapons
- Health

Ensure User Protection and Immersive Ad Experiences with GeoEdge's Ad Quality Control

GeoEdge's robust ad security and user protection solutions empower publishers and platforms across web, CTV, and in-app environments to proactively block malicious actors and harmful ads. With GeoEdge, you can ensure that every ad is malware-free and meets the highest technical and content quality standards before it reaches your users. By identifying threats at the pre-impression level, we help you maintain clean campaigns and safeguard the user experience.

Trusted worldwide, GeoEdge provides real-time protection that upholds integrity and fosters trust across the AdTech ecosystem. Safeguard your audience with real-time defenses that prevent malvertising and unwanted content from disrupting the user experience.

Learn More: www.geoedge.com