GeoEdge Malvertising Protection

Display | in App | Native | Video

The current state of programmatic advertising can be characterized as a loss of control as cyber attackers usher in a new era of bad ads. Malicious actors hijack publishers' traffic to inject malware, spyware, and ransomware into users' devices in order to collect personal and financial information. Malvertising subjects digital publishers to users' complaints, leading to frustration, brand damage, low retention, and revenue loss. GeoEdge's Real-Time Bad Ad Blocking solution goes beyond mere technology by eliminating the problem.

Real-Time Protection

Rely on AI-powered models to check each ad and ensures high ad quality. Automatically blocks all bad ads and replaces unwanted ads with safe ads.

Security

Defend against malvertising, whether injected through the creative or the landing page.

User Experience

Filter out low-quality ads that harm the user experience. Eliminates pop-ups, auto-audio, landing page alerts, and more.

Content Management

Manage ad content with proprietary content classification for creatives and landing pages with GeoEdge's ad review center and customized lists.

Complete Threat Map Protection

1 Pre-Click Issues

After bidding, as an ad renders on a publisher's page, the code it runs may exploit users' privacy & security. Malvertisers inject malicious code to serve ransomware or malware to collect users' private information or traffic hijacking by automatically redirecting users to malicious landing pages.

2 Deceptive Sites

Cyber attackers find it easier to run their malicious schemes on their own landing pages. Using clickbait ads with deceptive or fake messaging, malvertisers lure users to phishing scams to collect credit card details and additional personal information.

3 Post-Click Scams

Users are exposed to a myriad of threats after clicking on an ad. Threats include cloaked landing pages running phishing scams, fake tech support scams luring users to install PC cleaners, fake antivirus software, and PDF converters that monitor and log user activity on and offline.

GEOEDGE FEATURES		WHAT'S IN IT FOR YOU?
Multi-Layered Detection Engine	Our team of security researchers are constantly hunting bad actors who attempt to conceal their activity and escape detection. To root out malicious actors, GeoEdge's Detection Engine consists of multiple layers. Each layer identifies different aspects of the attackers' activity, from cloaking detection mechanisms to extensive landing page analysis. While each layer performs as a stand-alone unit, our algorithms match data points across these layers to form our single forensic insight.	The Multi-Layer approach ensures that GeoEdge will detect even the most sophisticated and well-hidden attacks. The frustration of fighting bad ads is gone, allowing your team to focus on monetization.
Zero-Day Detection	When GeoEdge blocks a scam, the attacker often attempts to pivot the attack through various vectors by changing domains or rewriting parts of their scripts. Occasionally, attackers launch new attacks by trying to slip below the radar. To detect new attacks at "Zero-Day," we harness the power of AI. Our real-time algorithms identify ads that behave suspiciously and require further analysis. Suspicious ads are automatically blocked until investigated by an analyst.	20%-25% of the bad ads blocked by GeoEdge are blocked for behavioral aspects detected by our AI logic. Our clients know that GeoEdge will always protect them, even from future threats.
Pinpoint Detection	Malvertisers exploit AdTech's infrastructure and supply chain to conceal their activity. When a scam is detected, traditional ad security solutions often block the entire channel, which in turn blocks many safe ads and advertisers. GeoEdge's Pinpoint Detection goes a step further to identify the bad creatives associated with a scam. Only malicious ads are blocked, allowing the channel to stay active and continue serving clean ads.	Blocking clean ads directly impacts publishers' monetization. Advertisers who are blocked without reason allocate less of their budget to publishers with whom they see a lower ROI.
Automated Demand Notifications	Blocking bad ads on the client-side is just the first step in our quest to make the internet a cleaner, safer place. GeoEdge's Ad Integrity Network (GAIN) automatically notifies your SSPs and demand partners about bad ads blocked on your site to ensure that bad ads are not served across your digital properties.	GAIN notifications streamline communication with your SSPs. We provide your partners with the data required to eliminate the problem at its source.
Monetizing Blocked Ads	When GeoEdge blocks a malicious ad, the ad unit is refreshed to fetch a new creative, ensuring that revenue is not lost. If the new creative is also blocked, we provide fallback options, allowing you to call up any ad from your server.	Ensures that users are not exposed to blank ad units and that blocked ads never harm your monetization efforts.

GEOEDGE OFFERS MORE THAN TECHNOLOGY. WE OFFER TRUE PARTNERSHIP.

We believe it's not enough to have a powerful detection engine and a vast network of publishers and platforms. You need a partner you can trust who will have your back even when things go south. GeoEdge assigns our partners a dedicated success manager who will proactively make sure you're getting the most out of your account. We pledge to provide the best protection and data for you, as well as for your team and your users.