INSIDE SECURE ADVERTISING PROTECTION SOLUTION

Defeat fraud and safeguard your advertising revenue. Get paid for showing ads and prevent ad signaling from being blocked or altered.

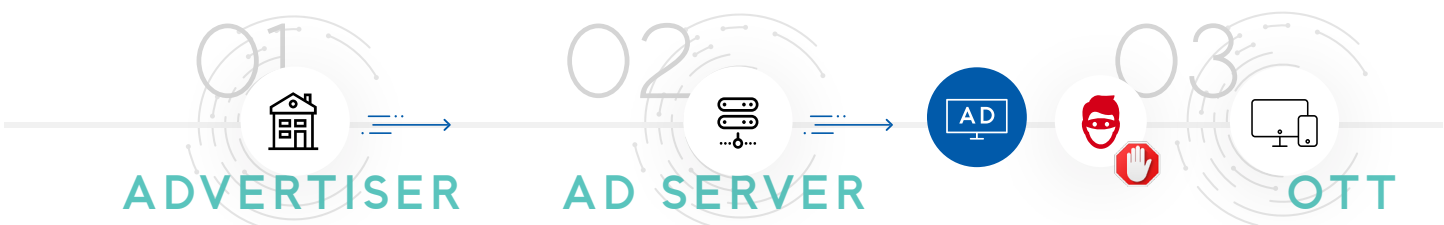
Without a solution to significantly thwart ad blocking, it is estimated that publishers alone will lose **$75 billion by 2020**, according to research published by Ovum. Another research by Statista estimates that the cost of **online ad fraud will grow worldwide from $19 billion on 2018 to $44 billion in 2022**, mostly from ad bots and domain spoofing.

Inside Secure ensures that Ad blockers and Ad fraud sources are prevented from affecting or tampering ad-display information coming to end user devices or being reported back to servers, ensuring reliable distribution and receipt of ad display revenue share. Inside Secure Advertising Protection Solution protects the delivery channel of the advertisement and secures the ad tracking pixel reporting.

Advertisement display is ensured through **bypassing ad blockers and hacking sources** (**bots, pre-bid and post-bid spoofing, domain and cookie spoofing, pixel stuffing, malicious apps...**). Inside Secures Advertising Protection Solution also has the capability, when required, to ensure that users are notified that ad blocker apps must be removed before being allowed to continue viewing content. Inside Secure Advertising Protection Solution is future-proof and can evolve based on new attacks by updating the technology based on Ad block and fraud detection heuristics and app algorithms.

Inside Secure Advertising Protection Solution prevents the add being:

- **blocked or unreported**
- **replaced or its metadata altered**
- **reported and recounted several times, while it has only been viewed once**

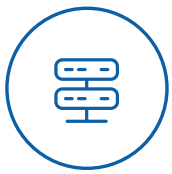


Inside Secure Advertising Protection solution is made up of three components:

• Advertising Protection Client

Protects ad bidding, display and tracking information against ad blockers, as well as hacker replay, replacement and spoofing attacks.

This is an SDK that integrates with mobile applications (iOS, Android) and websites. It is superset of HTTP calls therefore is very easy to integrate with existing applications. It adds a layer of authentication and secure communications between the media distributor's application or website and the ad servers so that all data flowing in this communication are encrypted and cannot be intercepted or manipulated by ad blockers, ad bots or malicious hackers trying to impersonate legitimate ads metadata. The code manipulating ad related data locally on the end user device is obfuscated and protected against tampering by Inside Secure code and data anti-tampering technologies so that they also cannot be misused by bots and hackers.



• Advertising Protection Server

Runs on a server and secures the communication between a client device displaying ads and the ad server.

This is a JAVA based product that runs on distributor's premises and which channels the communication between the Advertising Protection Client and the Ad servers of the distributor.

• Advertising Protection Service

Tracks the communication between a client device displaying ads and the ad server.

This is dashboard-based monitoring service that allows the distributors or the agencies or the advertisers to track fraudulent activities on their end user devices (ad blockers installed, ad bots...), as well as measuring the impact of piracy on their service (percentage of illegal calls versus legal calls). These information would allow each of those companies to measure how much money there are losing out of illegal activities on their service.

For further details on all of Inside's security solutions, visit www.insidesecure.com

inside secure