AD Secure

Malvertising Prevention & Ad Quality Solution

Media Kit



Elevating Compliance & Brand Safety Through Advanced Technical Innovation

Introduction

The global push for better and more compliant ads through initiatives like the Coalition for Better Ads or the Google Ad Experience, combined with the European regulatory environment—encompassing GDPR, the ePrivacy Directive and future ePrivacy Regulation, the IAB TCF framework, and the Digital Services Act—continues to push AdTech platforms toward more robust compliance measures. AdSecure stands out as a highly technical, crawler-based platform that excels at real-time ad scanning and automated risk mitigation. Our solution emulates genuine user behavior, leveraging proxies and real browser testing to catch even the most sophisticated threats—securing both compliance and brand integrity at scale.

AdSecure

Why monitor your Ads?

Malicious and non-compliant ads negatively impact:

+ Brand reputation
+ Google ranking
+ Partner trust
+ Revenue growth

What is AdSecure?

We provide constant monitoring and protection of your ad supply chain by automating your ad verification process before ads go live & while they are running.

+ Eliminate malicious ads
+ Detect non-compliant & low quality ads
+ Identify unsafe & offensive ad content
+ Measure ad performance against industry standards



AdSecure

What is AdSecure?

AdSecure is a software based on a crawler technology that is designed to emulate real user behavior while systematically scanning and analyzing advertisements, redirects and landing pages and also publisher’s web pages for blacklisted keywords. This ensures that ads comply with industry standards and do not contain security risks, non-compliant content, or deceptive practices.



Advanced Technical Capabilities

Real Browser Testing

Where many solutions rely on simple script-based checks, AdSecure deploys real browser sessions—mirroring an authentic end-user environment. This allows us to detect hidden or dynamically injected content that ordinary crawlers often miss. By replicating multiple user scenarios, AdSecure ensures that no malicious code or deceptive practice slips through undetected.

Extensive Proxy Network

AdSecure offers multi-GEO coverage through an extensive proxy network, including 93 datacenter locations, 154 residential ISP connections, and 745 mobile ISP providers. This is crucial for detecting geo-targeted threats and region-specific compliance violations. Our proxies deliver reliable, high-fidelity scans, ensuring that content is reviewed from the precise vantage point of local users.

AdSecure

Near Real-Time Analysis at Scale

Powered by an advanced distributed architecture, AdSecure processes high volumes of ad scans in near real-time. We routinely handle surges in ad traffic—ensuring that ad reviews remain both continuous and highly responsive. As soon as a potential violation is detected, instant alerts and automated blocking mechanisms can be triggered, thwarting threats before they disrupt our clients inventories.

Exceptional User Emulation

Our industry-leading user emulation environment simulates everything from click interactions to extended browsing sessions, capturing highly accurate data on how a genuine user would experience each ad. This not only highlights malicious behaviors such as cloaking and forced redirects, but it also detects subtle compliance lapses such as cookie drops before consent or IAB ad spot violations.

Flexible and Adaptive to Client Requirements

AdSecure's platform is built to adapt seamlessly to any workflow or policy environment. Whether you need bespoke scanning rules, specialized reporting formats, or specific partner integrations, our system can be fine-tuned to meet our client's exact requirements. The result is a scalable, future-proof solution that evolves with your business and the ever-changing regulatory landscape.

AdSecure

Why monitor your ads?

- Brand reputation.
- Google ranking (Google Safe Browsing/Webrisk).
- Partner trust.
- Revenue growth.
- Eliminate malicious ads (integrated into the platform AdSecure can trigger webhooks to initiate certain actions such as creative, campaign stop/pause. Advertiser’s account suspension etc.).
- Decline of Publisher’s website (Brand Safety) to stop traffic from web pages with blacklisted keywords.
- Detects non-compliant & low quality ads (IAB ad spots standards).
- Measure ad performance against industry standards (IAB ad spots standards).



AD Secure

Who we help?

1

Publishers

Protecting users from malicious attacks and negative browsing experiences.

2

Ad Platforms

Automating compliance tasks and assisting teams to drive high quality ad delivery, meet industry standards and be free of malvertising

3

Brands

Avoiding placing ads next to inappropriate or irrelevant web content in order to reinforce online brand safety strategy and maintain positive brand image.

When we help?

1

Pre-Flight Verification

Perform deep analysis of your ad campaigns before they launch.

2

Active Monitoring

Keep analysing your ad campaigns while they are active.

3

Real Blocking

Perform real-time verifications before displaying the ads.

How do we protect?

Key Features Supporting Regulatory Compliance

Pre-Approval & Ongoing Scans

Analyze campaigns before launch and continuously throughout their lifecycle to account for geo-variations, domain changes, and content updates.

Technical Threat Intelligence

Harness deep insights into malicious code, forced redirects, and unauthorized tracking to minimize reputational risks and improve user trust.

Multi-Device Coverage

Scan ads across desktop, tablet, and mobile device profiles, detecting usage-specific compliance issues, from bandwidth consumption to ad dimension standards.

Brand Safety & IAB Standards

Identify banned keywords, ensure ad weight limits are respected, and monitor every step in the redirection path for potential compliance breaches.



How do we protect?

Strategic Benefits

Regulatory Alignment: Effortlessly meet GDPR, ePrivacy, and future requirements like the Digital Services Act with consistent, automated oversight.

Reduced Compliance Overheads: Shrink manual review loads and free your experienced compliance team to focus on more strategic tasks.

Secured Brand Reputation: Shield your partners, publishers, and audience from malicious or low-quality ads, fortifying trust and brand goodwill.

Scalable Architecture: Respond seamlessly to traffic spikes or shifting campaign volumes, maintaining inspection integrity at all times.

Future-Proof Approach: With an adaptable platform and real-time detection, AdSecure ensures you stay ahead of emerging threats and new regulations.





User Security

- Adware
- Browser Locker
- Drive-by mining
- Malicious URL: Google Webrisk
- Malicious URL: Sucuri
- Malicious URL: Virustotal
- Malware
- Phishing URL: Google Webrisk
- Ransomware
- Scareware
- SSL-non-compliant
- Unwanted Programs: Google Webrisk
- VAST Cookie Detection

User Experience

- Auto-download
- Auto-pop
- Auto-redirect
- Auto-redirect App Store
- Auto-vibrate
- Back button hijack
- JS Alert on entry
- JS Alert on exit
- Landing page error
- Permission: Cameral
- Permission: Clipboard
- Permission: Geolocation
- Permission: Microphone
- Permission: Notification
- Uncommon Protocols

User Advisory

- IAB: Ad Dimension
- IAB: Ad file compression
- IAB: Ad request count
- IAB: Ad weight
- Suspicious TLD
- Threat Intelligence
- Unsafe content: Adult
- Heavy Ad
- Keyword Violation / Brand Safety

AD Secure

Our Solutions & Key Features

+ Ad Safety
+ Brand Safety



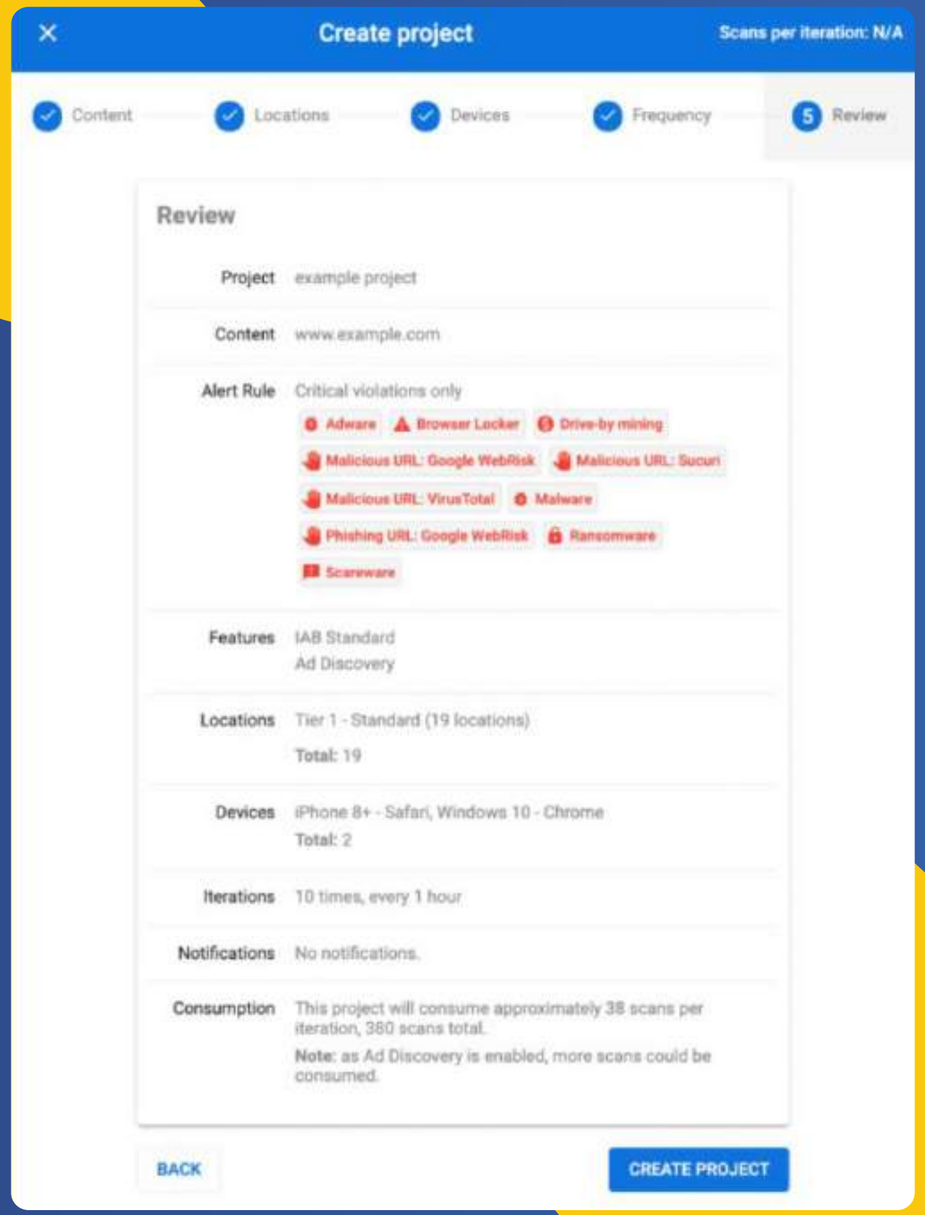
Ad Safety

Active Monitoring

- After the ad is launched, our crawler allows you to perform detailed analysis while the ad is running.
- An exhaustive set of devices and locations (residential and mobile IPs) are available to perform those analysis.
- Detects all digital malvertising threats and obfuscated code hidden deep within redirection chains.
- Notifies you in real-time of detections, providing a detailed report and enabling webhook execution via notifications, including:

  + **Email Notification:** Sent **on alert**
  + **Trigger Actions:** Executed **on alert, on violation, on completion, or on error**

Webhook triggers can be configured for various notification types.



Ad Safety

Active Monitoring *Rules that can be applied to Analysis and Project:*

Alert Rules

Alert Rule lets you define the conditions that must occur to trigger an alert based on AdSecure detections. By default every detection made by AdSecure will get flagged as a violation. Alert Rules allow you to define alert conditions that would highlight the violations in the reports, but would also allow you to generate notifications (emails, callbacks).

Allowlist Rules

An Allowlist provides the option to explicitly allow some exceptions when dealing with alerts.

On some occasions, you might want to make an exception for a certain domain and/or alert violations, to temporarily not be taken into account when you check the compliance of ads or site pages within AdSecure. A good example of this would be when you are in the process of resolving a known threat or quality issue detected on a project that scans frequently. Applying an Allowlist Rule in such a case will allow you to save time to focus on new alert violations that may occur on the project, rather than having to repeatedly check alerts on the known issue you are in the process of resolving.

You can whitelist Virus Total as a one Violation or whitelist the exact antivirus companies by name.

AdSecure

Ad Safety

Active Monitoring *Rules that can be applied to Analysis and Project:*

Notifications

AdSecure notification’s system will allow you to receive information about the status of your scans through several options (email, HTTP callback, AWS Simple Notification Service).

Referrer

Referring Domain & Custom Referrer
A referring domain is the website that directs users to your page via a backlink. It's key for SEO and tracking traffic sources.

Why Use a Custom Referrer?
A custom referrer allows publishers to scan websites exposed to traffic from specific sources. This is useful when partners set custom parameters for advertising. AdSecure enables users to add a custom referrer to scans, analyzing traffic from specific domains instead of just general traffic.

It also supports A/B testing, helping marketers assess campaign performance and ad content quality for referrer vs. non-referrer traffic.

AdSecure

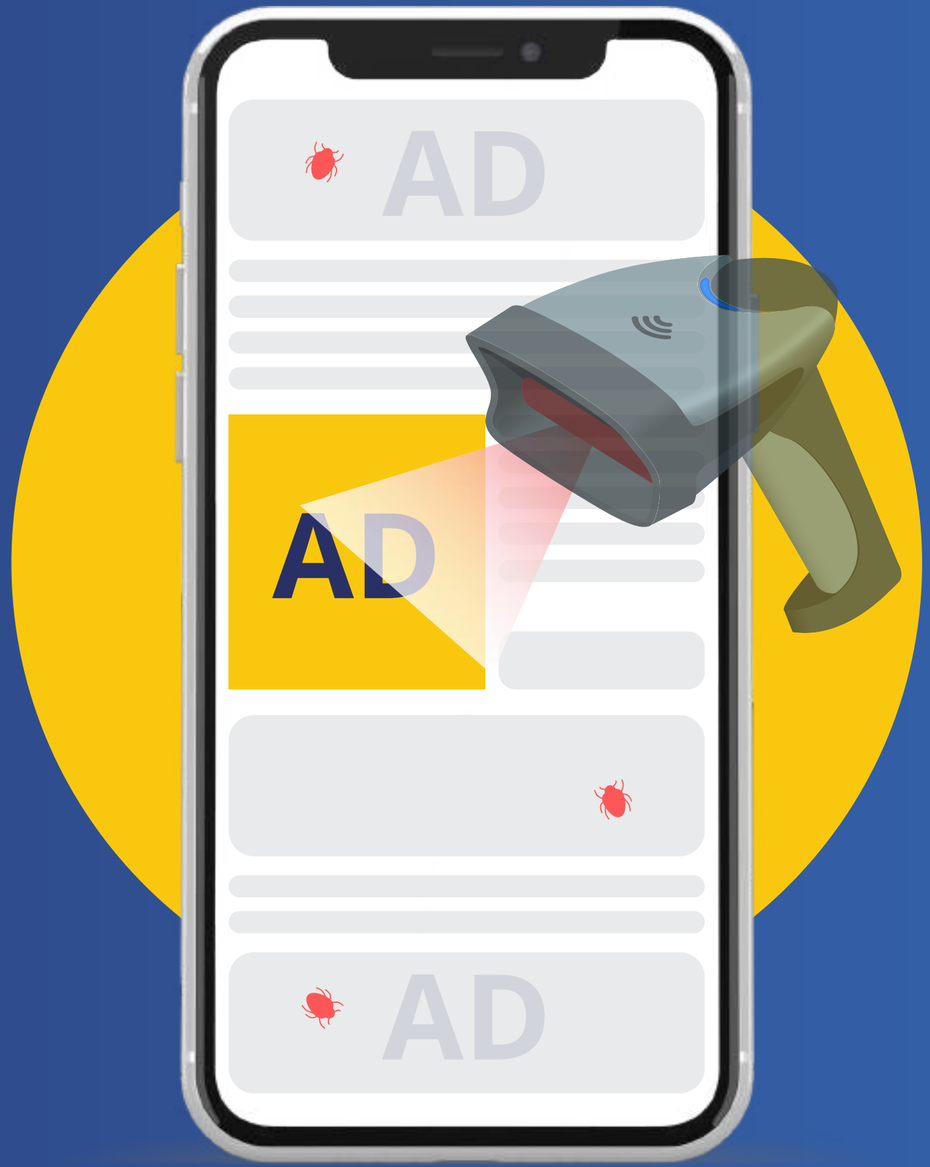
Ad Safety

Ad Discovery

Automatic detection and analysis of all ads while they are running.

Ad discovery using crawler involves a process where crawler visits a publisher's website to identify ad spots and then interact with those ads in a way that mimics human behavior, such as clicking on them. This process lead to the crawler being redirected to the advertiser's landing pages.

- Support most of the ad formats (incl. iFrames).
- Analyses the main site page.
- Engages with the ad campaign like an end user would.
- Detects any malicious activity on the campaign's redirects and landing pages.



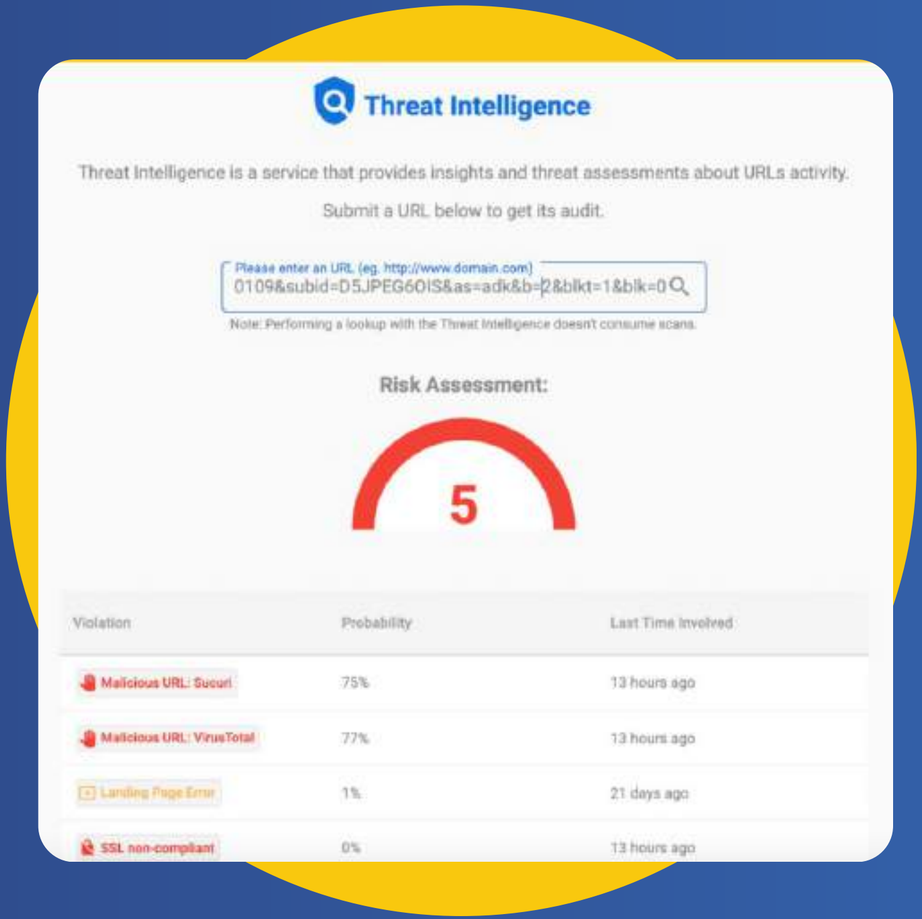
AD Secure

Ad Safety

Threat Intelligence

What is Threat Intelligence?
Threat Intelligence provides insights regarding a specific URL's ongoing violation activity revealing the potential presence of threats within the URL. The URL could be a website, pre lander/landing page or link related to an ad creative/ad campaign throughout the redirection path.

- Provides an indication on a scale from 0 to 5 of how risky we consider a URL to be.
- Lists previous violations detected for that URL.
- Threat Intelligence is an excellent way to perform a pre-flight check and to enhance and optimise your live daily monitoring.



AD Secure

Ad Safety

IAB Standards Compliance

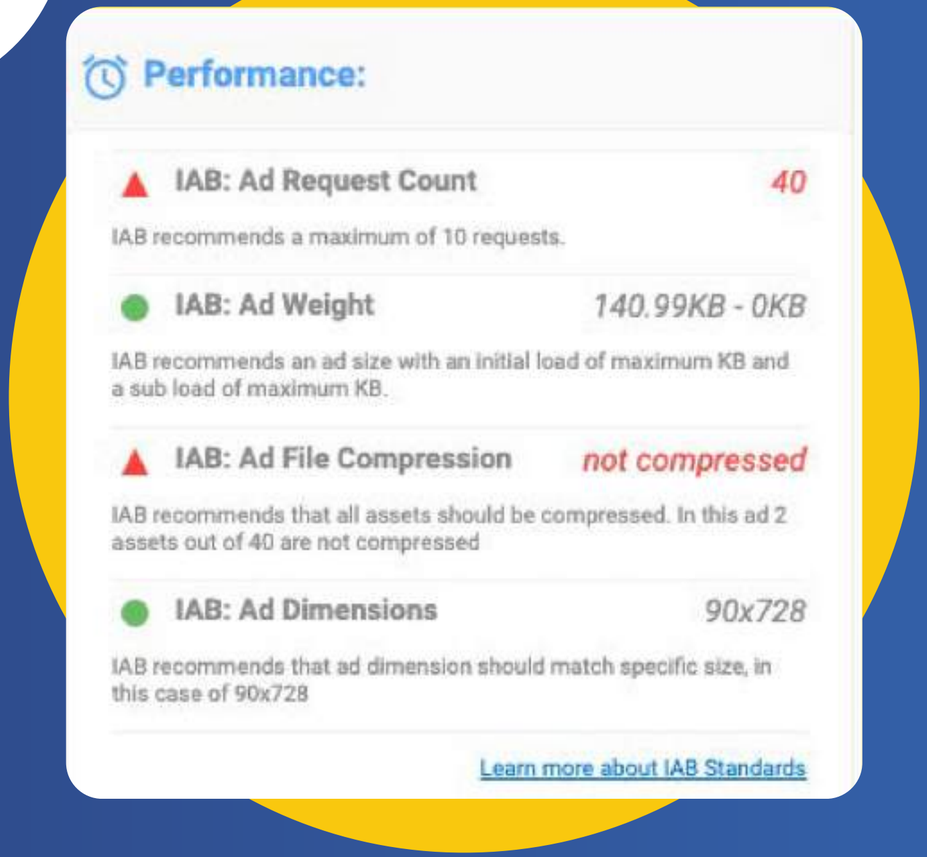
- Measure the performance of ads against the Industry IAB standars to stay Google compliant.

Ad Dimension:
Flags ads that don’t meet IAB’s recommended size range (100x200 - 150x300).

Ad Weight:
Ensures ads follow IAB limits—max 50KB initial load and 100KB sub-load.

Ad Request Count:
Detects ads exceeding 10 requests, which impact load performance.

Ad File Compression:
Identifies ads not using gzip or other compression formats for optimization.



Ad Safety

VAST Cookie Detection

AdSecure now supports the processing of VAST XML files to ensure compliance with resource guidelines. VAST (Video Ad Serving Template) is an XML-based format used to load advertisements into video players. These ads can take the form of images, videos, or other media types. AdSecure analyzes the content within the VAST XML to verify that all resources adhere to the specified guidelines, including checking for unauthorized cookie drops or other compliance issues.

What We Check For:

The primary goal of processing VAST XML files is to detect if cookies are being set before user consent is obtained. We specifically search for the presence of the Set-Cookie header within the HTTP responses of all resources referenced in the VAST XML. By analyzing these headers, AdSecure ensures that no cookies are being dropped in violation of consent guidelines.

AdSecure

Ad Safety

Hosted Ad Network
The crawler is interacting with a dedicated ad zone. We will need the code for this ad zone to host it independently.

RTB Analyses
RTB analyses are regular analyses, the difference being that they will scan the AD inside the RTB URL instead of the URL itself.

AD Secure

Brand Safety

A pixel tracker embedded in the banner triggers the crawler upon loading (impression) to collect data and check for predefined rule keywords found on the webpage of the Publisher

- Advertise in a safe and compliant environment of high-quality content
- Avoid placing ads next to inappropriate, unsavory, or irrelevant web content
- Select a list of pre-defined keywords or define your own keyword lists
- Support API integration



AD Secure

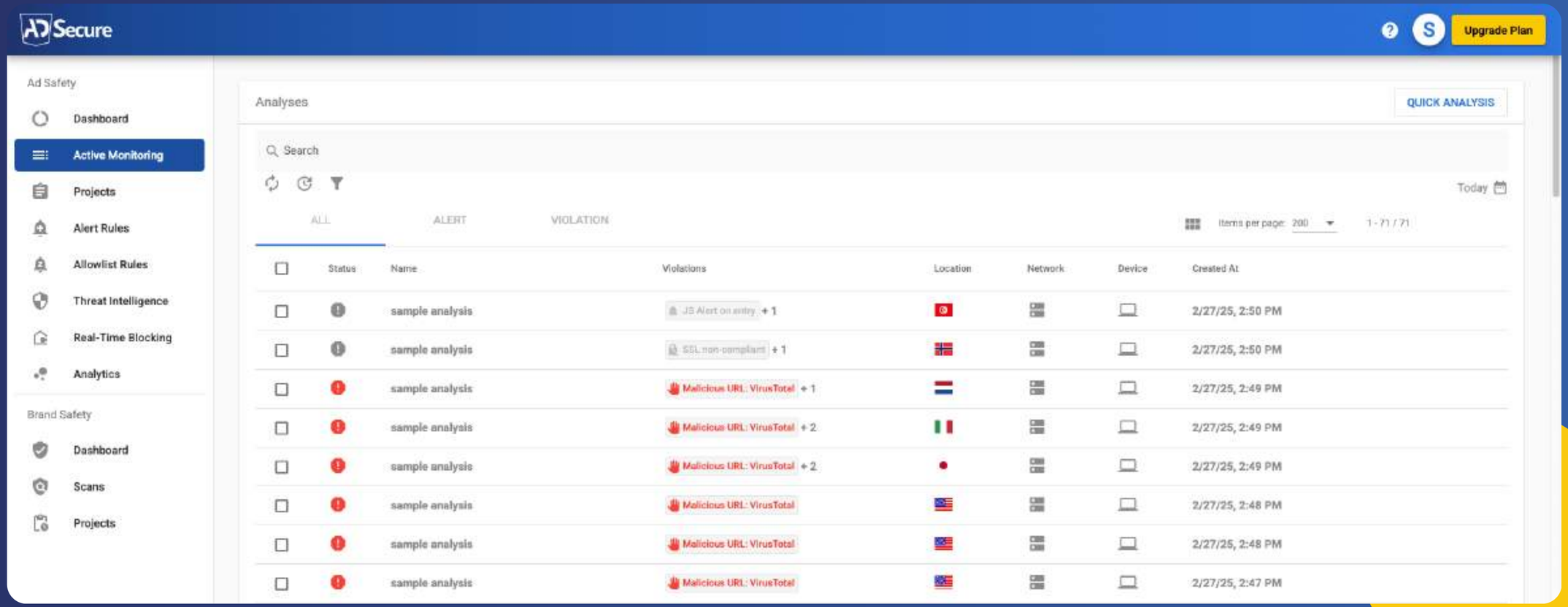
AD Secure

What’s inside?



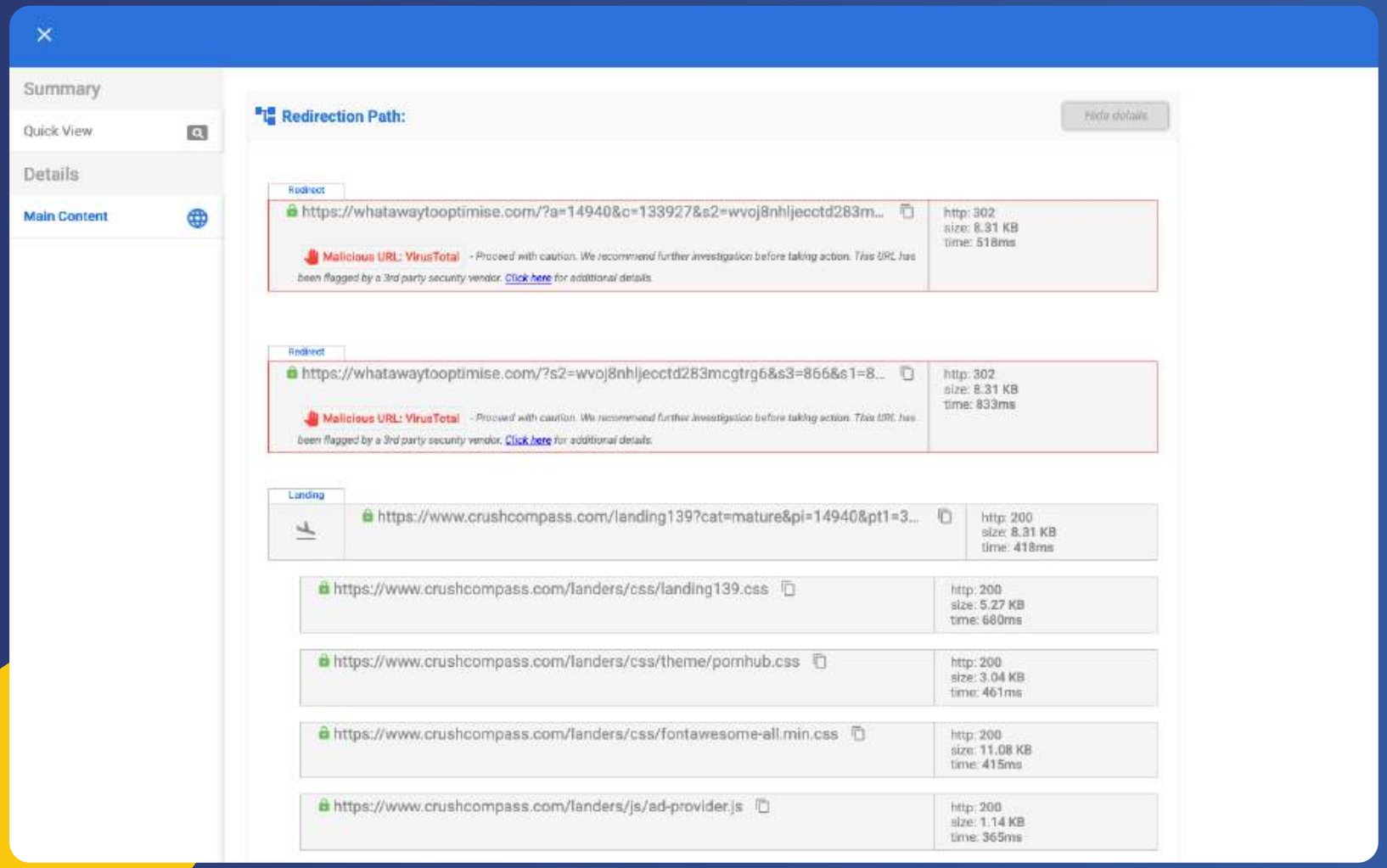
User Interface

Fast, Intuitive and Easy



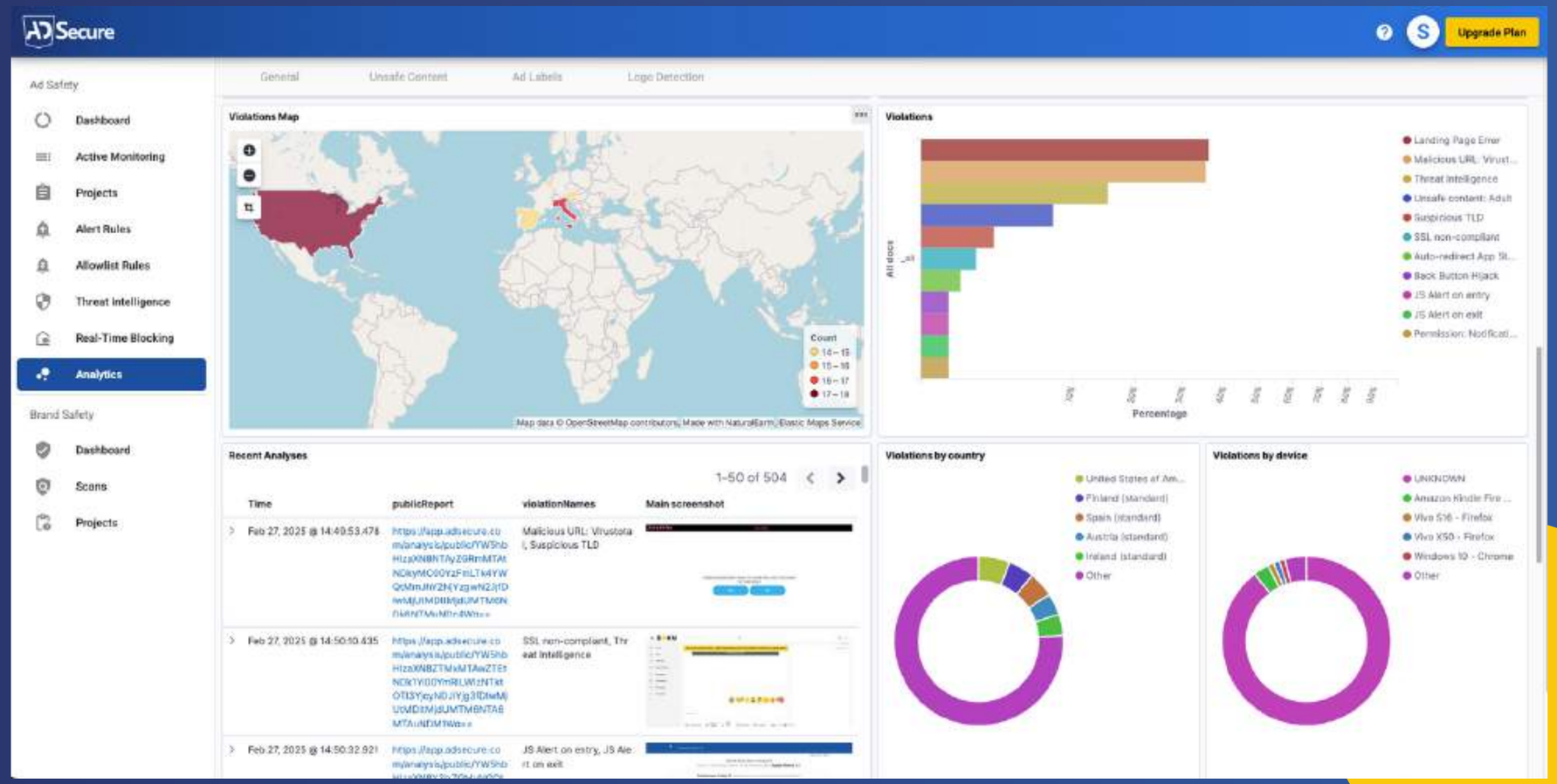
Forensic-level Reporting

Exhaustive report of all digital threats & obfuscated code hidden in the redirection chains



Actionable Analytics

Data drives strong decision making



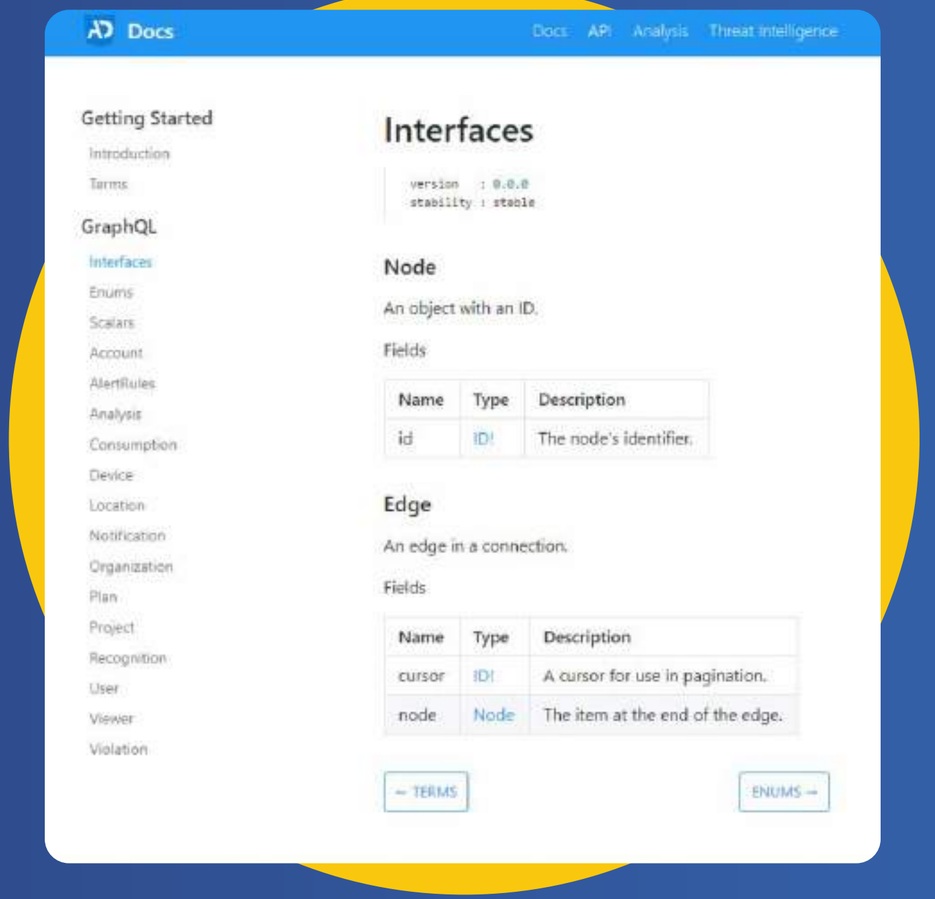
For Developers

Simplified API automation

Our API is built by developers, for developers.

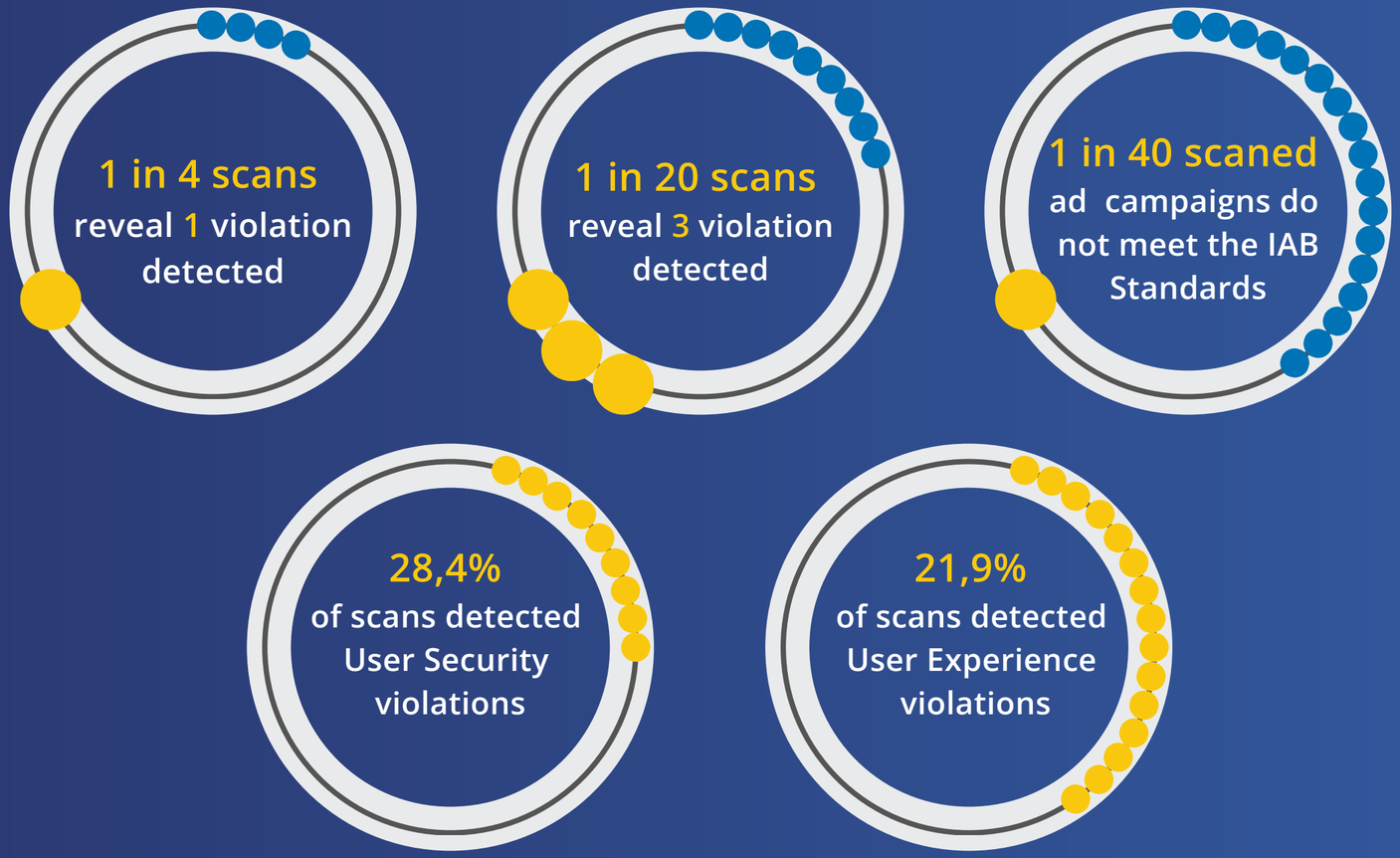
Any action you can perform through the interface, can be implemented through the API.

This allows you to automate any action you need, like stopping campaigns on your platform when AdSecure detects a bad ad.



AdSecure

Some Statistics from our Violations Report



AD Secure

Client Testimonials

"AdSecure has lifted our ad serving SaaS platform way ahead of our competitors."

Barry O'Sullivan,
Product Director EXADS ad server

"Since its integration into our platform andnetwork, AdSecure has become a key'go-to' tool in maintaining Traffic Factory's high quality in advertising standards."

Takanori Kanto,
Sales Director, Traffic Factory

"AdSecure enabled us to detect 475,618 violations in one quarter"

Ross Allan,
Advertising & Marketing Executive, TrafficForce

Read our Client Case Studies

Why choose AdSecure?

Automatic detection and analysis of ads before ads go live & while they are running.

- 360° ad security protection
- Uses the latest crawler technology
- Consistent threat monitoring and blocking
- Detailed analysis reports in real-time
- User friendly and advanced interface
- Comprehensive API
- Efficient customer support

AD Secure



Start a Free Trial

Stop bad ads. Deliver high quality experiences.
Maximise your revenue!

Start 14 day trial

AD Secure





www.adsecure.com
email us: contact@adsecure.com



Member of TAG Malware Working Group