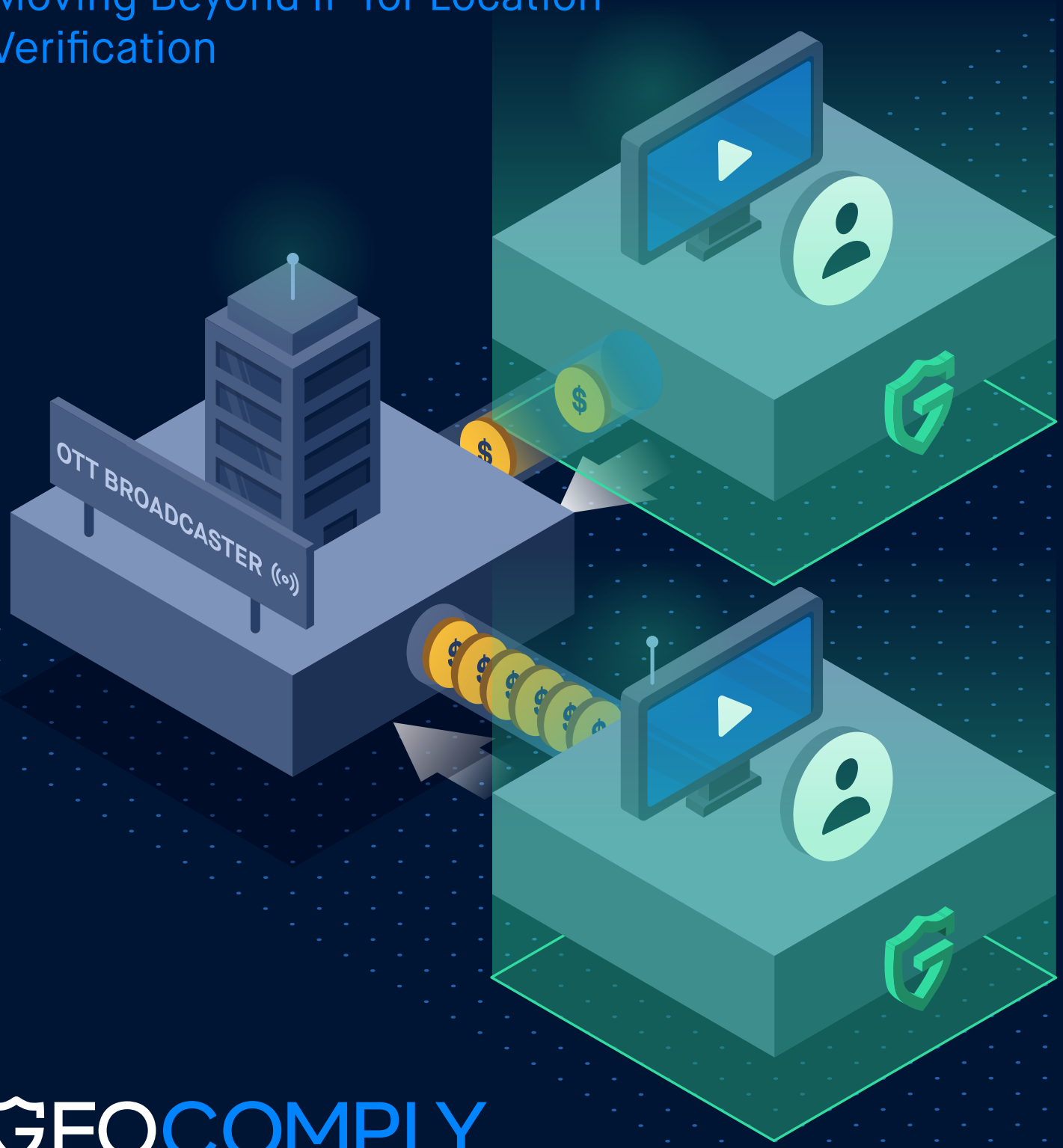
The Next Generation of Content Protection

Moving Beyond IP for Location Verification



GEOCOMPLY

Executive Summary

This white paper discusses the importance of protecting territorially restricted content from ever-evolving geolocation fraud threats. It also highlights how IP addresses alone are becoming increasingly insufficient for location verification and why in the not-so-distant future, OTTs may need to move toward a multi-source location data solution in order to safeguard their high-value, premium content.

From current threats such as using VPNs and DNS proxies to new threats like hijacked residential IP addresses and Proxy-Over-VPN attacks, the white paper shows how advanced geolocation technology can help OTT broadcasters, sports leagues and streaming video providers protect the value of their content and better enforce their rights contracts requirements to ensure compliance with territorial restrictions.

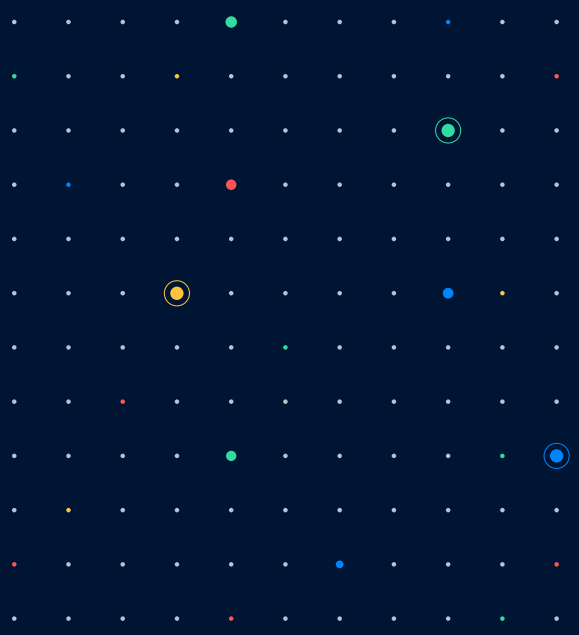


Table Of Contents

Introduction

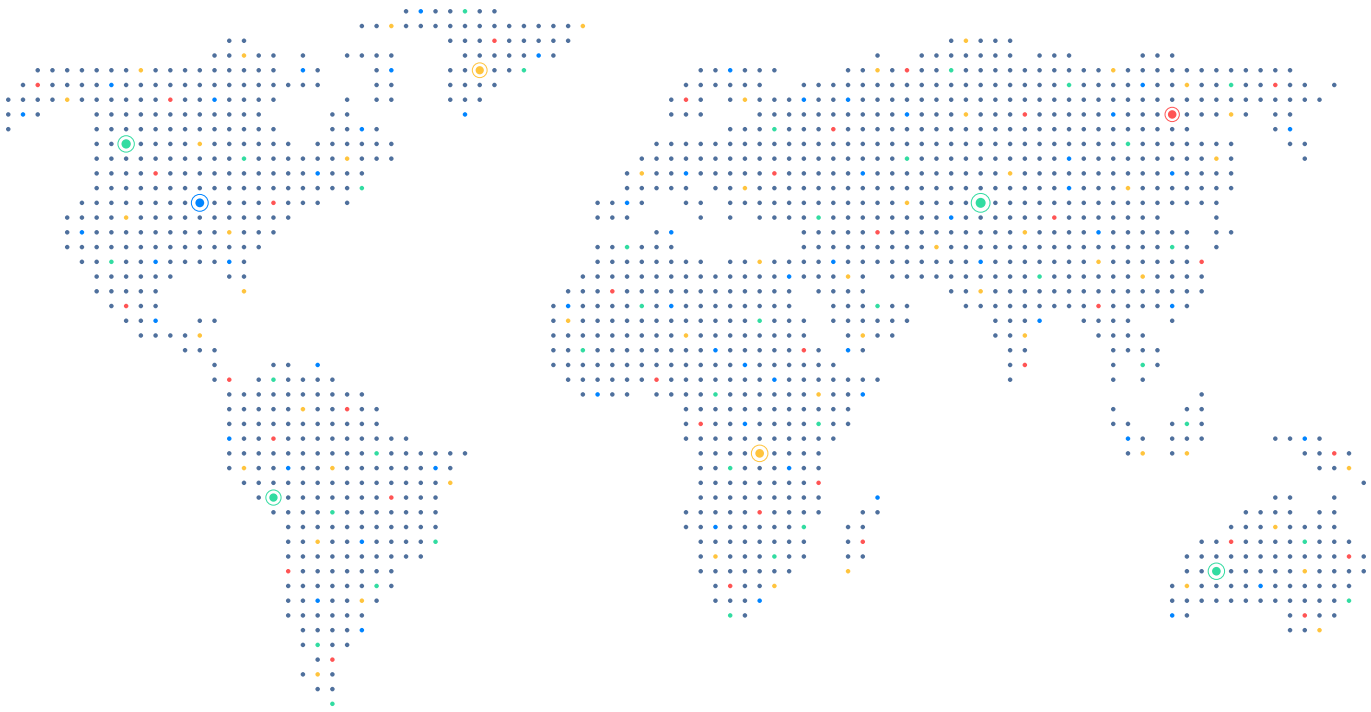
Territorial Exclusivity in Rights Contracts

Territorial exclusivity is a critical part of any content rights contract. Virtually every contract will specify the territory in which viewers are permitted to access the content as well as specify the requirements for the OTT broadcaster to implement geo-blocking technology to stop the content from leaking outside of the contracted territory.

To uphold territorial exclusivity requires a strong geo-fencing and geolocation fraud detection solution. Without it, content is vulnerable to leakage, which quickly erodes content value and negatively impacts the relationship between rights owners and OTT broadcasters.

As the piracy tools and techniques grow in sophistication, rights owners are making stronger anti-piracy measures a contractual requirement. For example, FIFA's broadcaster servicing manager, Eva Norroy, urges sports broadcasters to treat pirates like competitors and to, "do their utmost to protect themselves and ensure their feeds aren't being circumnavigated."

And these aren't just idle threats. Just ask Serie A. The football league was recently penalized around $200 million during contract negotiations when Qatar-based broadcaster, beIN Sport, deemed Serie A's content "non-exclusive" due to rampant geo-piracy. Moving forward, we can expect the demand for exclusivity and increasing levels of content protection to become the industry norm.

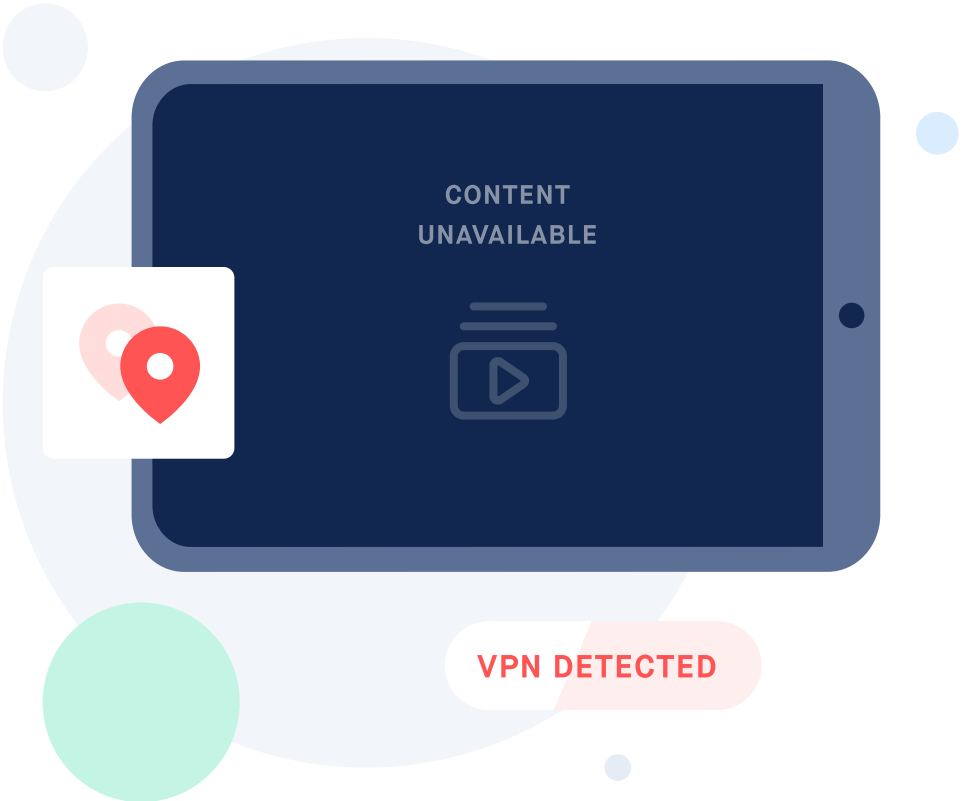


Traditional IP Spoofing Via VPNs and Proxies

Currently, the most common way for users to access geo-restricted content is to simply spoof their IP address using a VPN or DNS proxy. There are a number of “free” or subscription-based VPNs/proxies that enable users to change their IP address to appear to be located in a different country or territory. This technique to circumvent territorial restrictions works very well when the OTT broadcaster has only implemented basic geo-IP checks on their platform.

Fortunately, this type of widespread geolocation fraud or geo-piracy is totally preventable. All an OTT broadcaster needs to do is to implement an industry-standard geolocation fraud tool to detect when someone is masking their true location via a VPN or DNS proxy. The most efficient and cost-effective way to do so is with our “Hollywood Studio Approved” solution, GeoGuard.

When a user visits the OTT broadcaster website via a VPN or proxy, their IP address is checked against a highly accurate and up-to-date database of known IP addresses used by anonymizing services – updated several times a day. If the IP address is recognized as belonging to a VPN, an error message is displayed informing the viewer their location cannot be confirmed and access to the content is denied.



Hijacked Residential IPs – A New Tactic by VPN Providers

Millions of users who downloaded “free” VPN software to bypass territorial restrictions have unwittingly had their residential IPs hijacked by these VPN providers (through the terms of service) and then sold to the highest bidder – usually other VPNs who in turn sell these residential IPs as a premium-priced option to by-pass existing VPN detection. Since these residential IPs are not included in a VPN IP database (as they are essentially people’s home IP addresses), users of these premium VPN services are able to circumvent traditional VPN detection methods.

Because residential IPs are expensive to use for the actual content delivery, they are only employed at the website level to grant access to the content. When a broadcaster is utilizing a CDN that’s integrated with GeoGuard (such as Akamai), once the actual video starts streaming, the VPN switches to a cheaper non-residential IP address (a datacenter IP). The CDN (running GeoGuard) detects this switch and the illegal stream can be immediately stopped.

By integrating GeoGuard at the CDN level, residential IP addresses can be easily detected, and the illegal stream stopped. In fact, that’s why rights holders and content owners are increasingly requiring their streaming services and OTT broadcasters to use a CDN and check for a changed IP during the video stream, at the CDN level.

GeoGuard is fully integrated with leading CDNs, including Akamai and Amazon AWS CloudFront. This makes turning on VPN and proxy detection as easy as flipping a switch. GeoGuard is the only solution fully integrated with Akamai, the world’s largest CDN for the streaming industry, powering their Enhanced Proxy Detection (EPD) service.

Combating New and Emerging Geo-Fraud Threats

VPN providers are always devising new ways to enable users to spoof their location. GeoComply is constantly adding new features and enhancements to GeoGuard to ensure that rights holders, including studios and sports leagues, who rely on territorial restrictions to maintain the value of their content rights, and OTT broadcasters, who are contractually obliged to combat this form of content leakage, can benefit from an advanced level of geolocation fraud protection.

Recent important enhancements to GeoGuard include:

GeoGuard has been third-party tested by Kingsmead Security and found to be 99.6% effective in detecting VPNs and Proxies.

Proxy-Over-VPN

As the only solution in the industry with this functionality, GeoGuard's advanced logic can now identify attempts by premium VPN providers to target high-value video streaming services using proxy over VPN techniques that effectively double-spoof the streaming provider in an attempt to go undetected. GeoGuard's advanced logic now identifies such attacks to prevent content leakage.

IPv6

With VPN providers adding IPv6 ranges that allow users to spoof their location, GeoComply has added IPv6 detection to GeoGuard. This allows OTT broadcasters to remain fully compliant with their contractual obligations and business rules while continuing to allow users to access their services on IPv6-only connections.

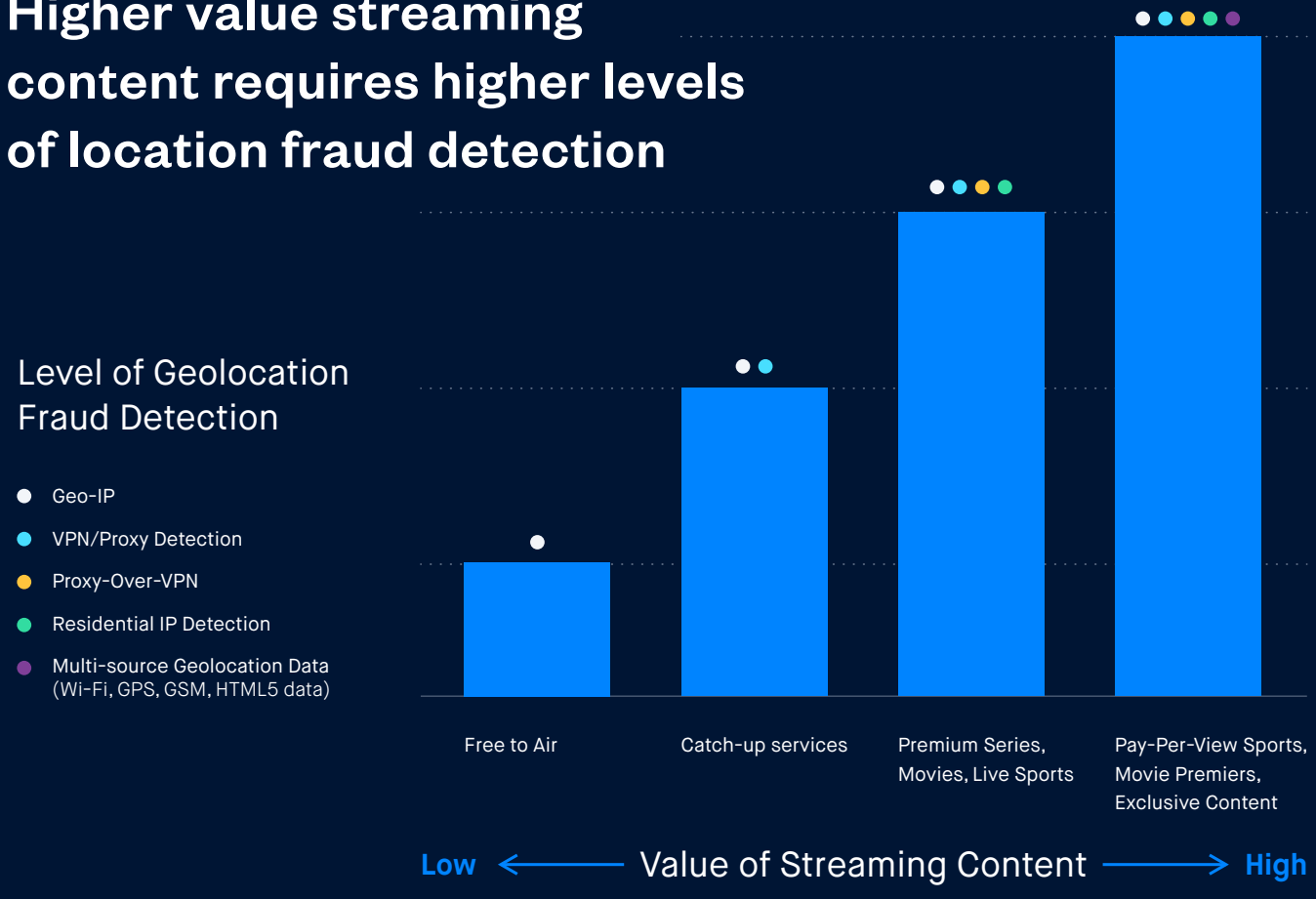
Moving Beyond IP – The Next Generation of Geolocation Technology

As outlined in the Streaming Video Alliance's (SVA) report Securing Streaming Video, "Determining geographical location requires more than just checking the geographical IP of the end-user. Addresses cannot be solely relied upon to make decisions as IP databases are often inaccurate and IP addresses can be masked with virtual private networks (VPNs)."

The report recommends the best way to prevent geo-piracy is to go beyond IP and incorporate HTML5, Wi-Fi, GPS and cellular data for viewer location validation. "Poorly implemented restrictions allow consumers to access content outside the permitted territories for free and/or at a reduced price than the licensed distributor price (e.g., a boxing match in Ireland costs $25 vs. $80 for the same match in the US)."

While this approach may seem a little heavy-handed for low-value content, as the SVA points out, when it comes to big-ticket sporting events and highly anticipated movie releases, not adopting stronger geolocation verification methods could cost studios, sports leagues, rights holders and premium OTTs billions in lost revenue.

Higher value streaming content requires higher levels of location fraud detection



The More Valuable the Content, the More Sophisticated the Fraudster

When it comes to protecting high-value, premium content, such as high-profile live sports events or movie premiers, streaming broadcasters need to deploy a much higher level of geolocation and fraud detection technology, since the more valuable the content, the more sophisticated the fraudster.

As the SVA recommends, protecting high-value content requires going beyond IP and GeoComply has the proven tools, technology and expertise to help the entire streaming ecosystem to tackle geolocation fraud now and in the future.

GEOGUARD

GeoGuard is an easy to implement solution, consisting of a locally or cloud hosted database of IPs associated with location spoofing applications. Unlike mainstream IP databases, GeoGuard provides multi-layered fraud protection against VPNs, DNS proxies, peer-to-peer networks and other types of data manipulation. Our solution is continuously updated as new threats and data centers are identified and mitigation methods are developed.

- A continuously updated database of IP addresses associated with location fraud
- An up-to-date database of IP addresses associated with location fraud
- Detects VPNs, proxies and other forms of IP data manipulation
- Integrated directly with leading Content Delivery Networks (CDNs) including Akamai and Amazon CloudFront
- Other integration options are available

RISKGUARD

RiskGuard provides a frictionless, configurable and low-touch solution that helps OTT broadcasters identify and prevent a wide variety of fraud including content piracy, account sharing, chargeback fraud and account takeovers. RiskGuard uses a number of location signals including Wi-Fi, GSM, GPS, HTML5 and IP data to determine a user's true location and detect fraud.

- Utilizes both a real-time and a historical risk engine to identify and flag potential fraudulent activity
- Processes all location data and cross-checks against pre-existing patterns of fraud
- Detects whether a user/device jumps a long distance in a short period of time
- Configurable for the amount of user data shared, the types of flags generated and the fraudulent activities identified and stopped
- Provides a fast return on investment using an API-based, easy-to-implement solution

About GeoComply

99.6%
Accuracy in VPN detection

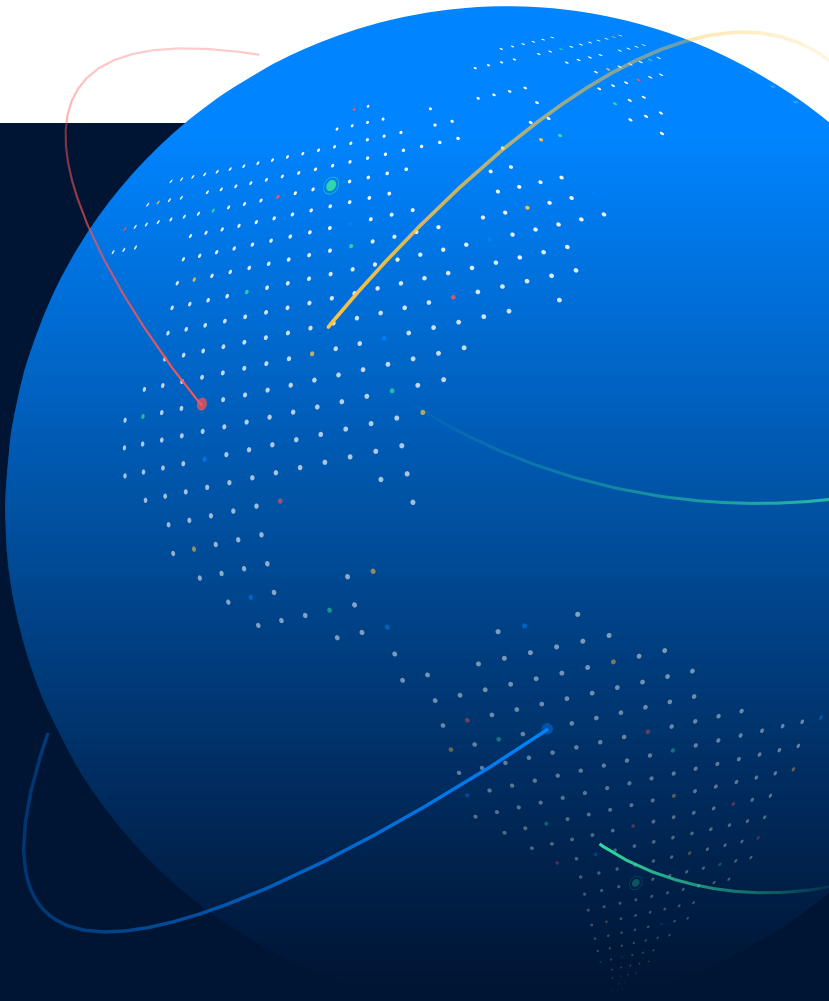
Highest-rated solution, backed by third-party testing

+/- 5 Meters
Location accuracy

Geofencing, reverse-geocoding, and granular location analysis

10 B+
Streaming requests per month

Scalable infrastructure with various integration options



Founded in 2011, GeoComply is the digital industry's trusted provider of proven, secure and accurate geolocation compliance and fraud detection solutions. Our products are based on the award-winning technologies that GeoComply developed for the highly regulated and complex U.S. online gaming and sports betting market. Beyond iGaming, GeoComply provides geolocation fraud detection solutions for streaming video broadcasters and the online banking, payments and cryptocurrency industries, building an impressive list of global customers including Amazon Prime Video, BBC, Akamai, Sightline, DraftKings, FanDuel and MGM.

The company's software is installed on over 400 million devices worldwide and analyzes over 3 billion transactions a year, placing GeoComply in a unique position to identify and counter both current and newly emerging geolocation fraud threats.

To learn more, contact us at

solutions@geocomply.com | geocomply.com

GEOCOMPLY