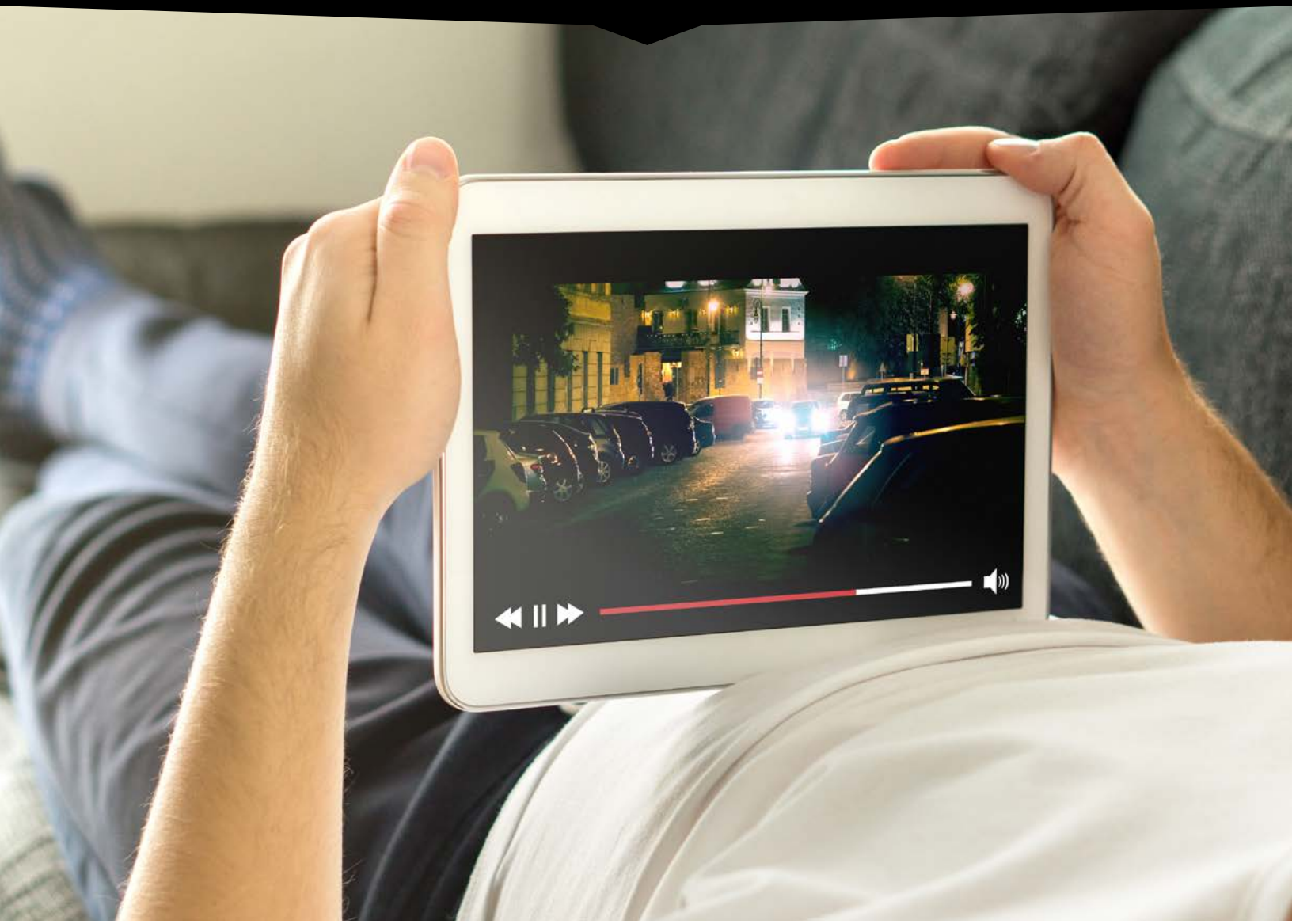
WHITE PAPER

Hijacked Residential IPs – A New Threat to Studios, OTTs and Rightsholders

How to stop the COVID-19 related surge in content piracy via VPNs and DNS Proxies



3RD PARTY TESTED

STUDIO APPROVED

VPN

GEOGUARD

Fraud Has No Place To Hide

Table of Contents

Executive Summary

This white paper provides insight on how millions of users who downloaded “free” VPN software to bypass territorial content restrictions while staying at home during COVID-19, have unwittingly had their residential IPs hijacked by these VPN providers. These users have allowed their residential IPs to be “leased” by unknowingly consenting to the complex terms and conditions of the free VPN service.

The user’s residential IPs are then sold to the highest bidder, which are often other VPNs who then sell these IPs as a premium priced option, to enable users to by-pass the existing VPN detection (which identifies the data center IPs commonly used by standard VPNs) in order to access territorially restricted content by pretending to be an “undetectable” residential IP in the specific geographical territory. In this white paper, we provide an easy to deploy solution to the residential IP problem for content owners and rightsholders.

The white paper explains geo-piracy and the bypassing of territorial content restrictions via VPNs and DNS Proxies, in terms of both datacenter IPs and the residential IPs, as well as ways to combat both types with advanced detection solutions integrated at the content delivery network (CDN) level.

Introduction

Demand for premium content during the COVID-19 pandemic has led to an increase in use of streaming services. This has also resulted in an increase in the use of VPNs and DNS Proxies for users to spoof their IP address in order to access geo-restricted content. The resultant growth in geo-piracy via VPNs and DNS Proxies undermines the territorial business model that studios, content owners, media rightsholders and premium OTT broadcasters rely on for revenue.

VPN providers are exploiting the pandemic by aggressively marketing their products to promote wide-spread content piracy. With studios, sports leagues, content rightsholders and OTTs under significant economic pressures, this loss of revenue from content piracy threatens their very existence.

A newly popular technique uses hijacked residential IP addresses, linked to real homes and businesses and issued by legitimate ISPs, to leverage tens of millions of compromised devices around the world to route traffic to OTT sites via these hijacked IP addresses.

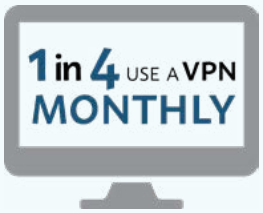
Millions of users worldwide have unwittingly had their residential IP addresses hijacked by "free" VPN and DNS Proxy providers (through a complicated term of service agreement), and sold to the highest bidder – usually other VPN who offer them as a premium "undetectable"' service.

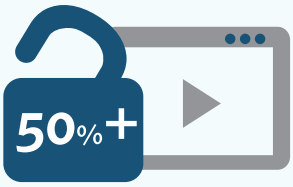
Globally, more than 50% of VPN users, according to Statista's 2018 research, admit that their primary goal in using a VPN is not privacy, but instead to access geographically restricted content. Traffic to VPNs (one of which claims over 140 million customers), is driven by OTT content popularity.

At the time of writing, GeoGuard has identified at least six major VPN and DNS Proxy providers using the residential IP technique. Fortunately, our VPN and DNS Proxy detection solutions can help the digital media ecosystem and other industries guard against geo-piracy and location-based fraud, including residential IPs.

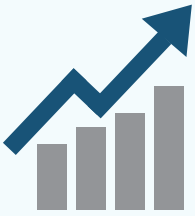
GeoGuard provides a suite of geo-filtering and fraud detection solutions, combined with human intelligence, to stop internet users from spoofing their location. In fact, our solutions are already in use by some of the world's leading broadcasters and OTTs at the CDN level on both Akamai and AWS CloudFront, as well as many others. Contact us at **solutions@geoguard.com** for more information.

72+ MILLION
RESIDENTIAL IP ADDRESSES COMPROMISED





OF VPN USERS USE THEIR VPN TO UNLOCK CONTENT



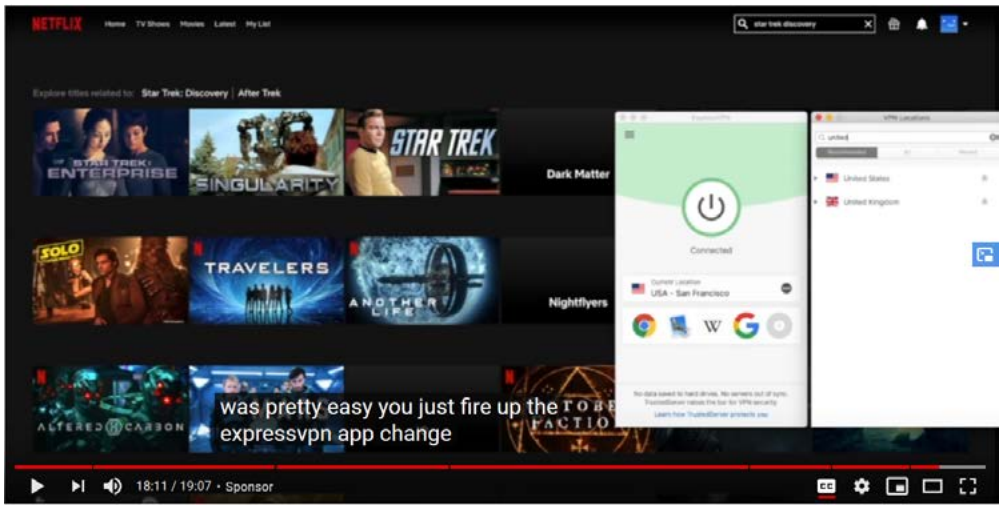
VPN use has increased 124%
during the two weeks between March 8th and March 22nd, 2020

Why is this becoming a problem now?

The persistence of IP based geo-blocking as the solution of choice by OTT platforms has led to tens of millions of devices worldwide being compromised with "Free VPN Software" that offers users the ability to access content from anywhere illegally free of charge.

These "free" VPNs actually act as Trojans on devices to covertly "sublease" access to them (through complicated terms of service agreements) and their home broadband connections on an enterprise-level to the highest bidder. Who are some of the highest bidders? Other VPNs and DNS Proxies that charge their users premium prices for access to these "undetectable" IP addresses to enable spoofing of any location in the world. This tactic avoids the use of data centers VPNs and DNS Proxies have traditionally relied on, making geo-filtering by IP address almost useless.

With the dramatic increase in use of streaming services following the COVID-19 pandemic comes an increase in the use of VPNs and DNS Proxies to access geographically restricted content. As more people are staying home to stop the spread, VPN and DNS Proxies providers are using the pandemic to market their location spoofing products.



This marketing strategy is aggressive, widespread and effective, with YouTube influencers like Marques Brownlee being sponsored by ExpressVPN to specifically target his 11.8 million subscribers and encourage the use of VPNs to circumvent territorial content restrictions. In fact, this episode features Apple's senior vice president of Software Engineering Craig Federighi, yet Apple itself offers a geo-restricted content platform on Apple TV+.

Is "Grey Market Access" via VPNs/Proxies a victimless crime?

Let's look at it from four perspectives:

1. If you are an OTT broadcaster, or one of their technology providers, and you are paying comparatively modest sums for premium Sports, Film & TV rights for a small market like New Zealand or Taiwan but you're also getting subscribers from major English or Chinese speaking markets, then you are firmly of the opinion that this is a victimless crime.

2. If you are a Satellite/Cable/OTT broadcaster, you are losing market share and money because you are facing grey market competition from foreign OTT broadcasters with leaky geofencing in the UK or US. Despite paying billions a year for premium content, you're seeing your subscribers canceling contracts and ratings dropping, then you are far from happy (assuming you even know about it).

3. If you are a rightsholder, in the short term, you see your international packages for smaller markets rise because of OTT and you are ahead of your budget forecast. This might be tempting because selling media rights is the only revenue stream left during lockdowns when theaters are closed and there are no live events. However, in the long term, you start seeing your core premium market packages (where you make the lion's share of your revenues) slipping in value. Your biggest customers embark on cost-cutting exercises, and over time you see less bidders for your content as broadcasters drop out of the running since they can no longer commercialize their "exclusivity" in the same way, resulting in a hugle loss of revenue.

4. If you are a broadcaster that relies on revenue from advertising then by accepting traffic from VPNs and DNS Proxies, you run the risk of any traffic to these ads being flagged as invalid traffic (IVT). Companies that pay you for advertising spots on your platform employ companies such as Moat Analytics, who ensure that ads are receiving valid traffic, and they will flag any VPN or DNS Proxy traffic as IVT. Because of the high prices that these companies must pay for these spots, they are happy to drop any platform that serves their ads IVT. That means you don't get paid for running those ads anymore, resulting in a huge loss of revenue.

Broadcasters in Canada have long been struggling with the competitive challenges associated with US content leaking across the border. David Purdy, SVP at Rogers was quoted as saying that VPN access to US based Netflix made the competitive landscape in Canada unfair. Their true competitor at the time, Canadian Netflix, had limited content however consumers could easily view the superior US version. Rogers' streaming product, Shomi – a joint venture with Shaw, subsequently shut down leaving Netflix as the dominant local player since. With only one local player, there is less competition for content which means lower bids for programming and therefore lower revenue for creators, studios and rightsholders.

Another example of the far-reaching effects of geo-piracy can be seen in the 2020 case of BeIN Media Group. BeIN Sport is a Qatar-based sports network, and they classified Serie A's football matches as non-exclusive content because of rampant piracy.

Its chief executive, Yousef Al-Obaidl, told the streaming video ecosystem that, if rightsholders don't do everything they can to protect their content from piracy, then he's either not going to bid for those rights or will price them lower accordingly. The price of the piracy for Serie A? Around $200M dollars, which is the estimated amount that Serie A refunded to BeIN.

But only a small number of people are actually doing this, right?

Wrong.

Fully 25% of all internet users regularly turn on a VPN, with the majority of them doing so PRIMARILY TO WATCH GEO-RESTRICTED CONTENT. This equates to 900 million people masking their IP address monthly.

HolaVPN has over 130 million users of their VPN services, their Chrome browser extension alone has almost 9 million weekly users. ExpressVPN admits that during major sporting events and show releases, they've witnessed their traffic volumes increase.

Indeed, during the COVID-19 pandemic, ExpressVPN has been using influencers to advertise its products, specifically for the purpose of bypassing territorial restrictions so users can access content from other countries while they stay at home. For example, on the Tony Kornheiser podcast (which has 110k Twitter followers), ExpressVPN exploits the current crisis to encourage content piracy. If VPN providers themselves are aware of the potential of this market and are willing to spend the money to advertise to tap it, then rightsholders and OTT broadcasters definitely need to take notice.

Background

How did we get here?

The Need for Geo-Blocking

To produce acceptable returns from investments in content, rightsholders apply a territorial pricing strategy to content licensing. Broadcasters with the highest willingness to pay – those in developed countries with large subscriber bases – pay considerably more for access to content than those in poorer regions. This is particularly pronounced for sports rights, where consumer demand is highly localized – up-to 70% of revenues can come from a single country. Geo-blocking stops this strategy from being undermined.

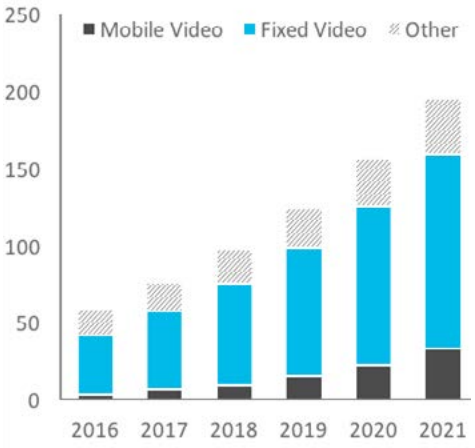
It's Easier Than Ever to Commit Geo-Piracy

Online video has become even more prevalent during COVID-19 as people stay at home and watch streaming content, and as OTT becomes a bigger part of rightsholders' business models – at the expense of traditional pay-tv methods – enforcing geo-boundaries plays an increasingly important role in revenue generation and protection.

Unlike piracy methods of the past, any user can download a VPN or DNS Proxy easily and start watching content illegally from across the globe. The barrier to entry is low and the payoff is high, and VPN and DNS providers know this. They actively encourage users to circumvent geographical restrictions using their products, making it clear just how fast and easy it is to do so.

To complicate matters further, each OTT service is delivered across many platforms: web browsers, iOS or Android Smartphones, Smart TVs, Roku or another streaming device. This range of delivery methods makes consistently monitoring and validating location data a challenge for OTT broadcasters. With free/cheap, easy to use geo-blocking circumvention methods available to consumers, the task becomes even more complex. Targeting the use of one method of location spoofing results in users simply turning to the next weak link in the chain.

Global Consumer Data by Traffic Type 2016-21 (Exabytes/Month)



Source: Cisco VNI Mobile, 2017

Traditional Geo-IP Method

Traditional geolocation methods rely solely on looking at a user's IP address as an accurate indicator of a user's location. It's a popular method since it's cheap, simple and doesn't impose on the user experience. This method is not only highly susceptible to geolocation spoofing but it also lacks industry standardization and does not include location checking at the CDN layer at intermittent intervals.

Some of the common mistakes around using IP for geolocation are:

- Implementing cheap or free vendors of geolocation data where accuracy is not at all verified.
- Failure to implement VPN & DNS Proxy Detection at all.
- Implementing poor VPN & DNS Proxy Detection so that the most popular providers get through, making multiple updates a day essential.
- Failure to differentiate between standard and mobile connections. (Cellular connections will resolve their IP through the carrier base station, meaning that a roaming customer from the UK will still show a UK IP address even when they are in the US.)
- Failure to integrate the vendor's geo-fencing solution (satisfy contract requirements with rightsholders but not enforcing restrictions) at all or not properly (infrequent updates).
- Failure to collaborate/share data points with geolocation vendors to target specific threats.
- Failure to collect network status on certain streaming devices to target DNS Proxies set at device/router level.
- Failure to check location information at the CDN layer.

Geo-IP Spoofing Detection Methods

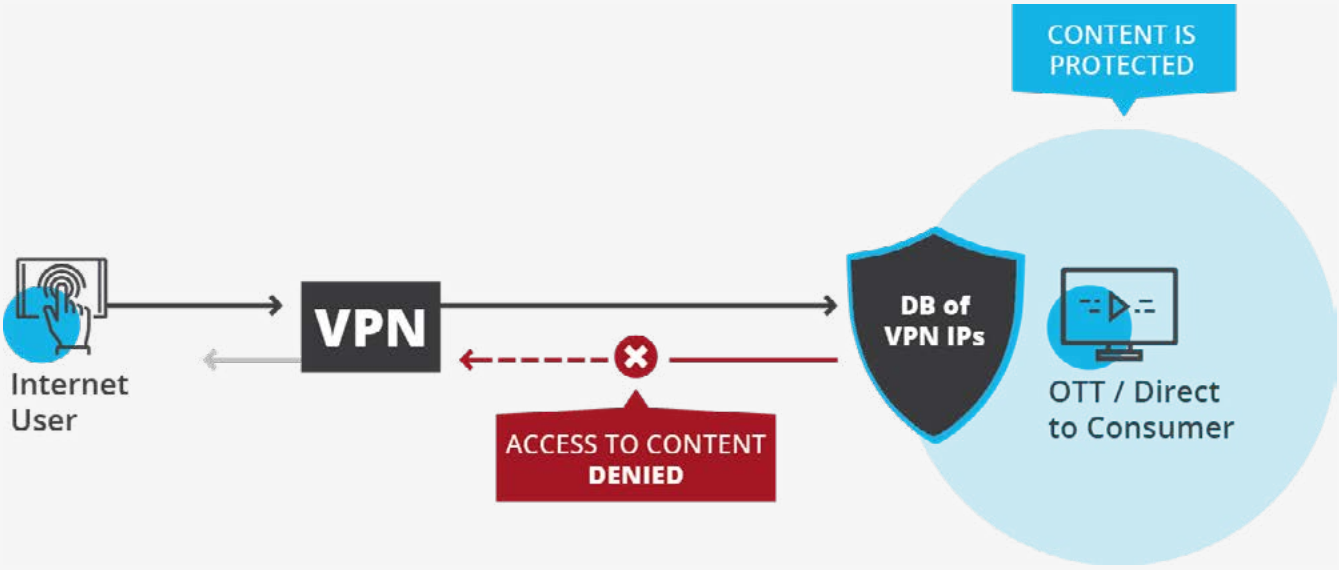
To combat the rise in geo-IP spoofing, a handful of reputable OTT broadcasters – often under pressure from rightsholders – have upped their game with help from vendors such as GeoGuard to make geo-IP spoofing significantly more challenging. Implemented properly, advanced geo-IP spoofing detection solutions can identify such IPs and users attempting to circumvent territorial restrictions will be unable to access the content.

Most spoofing detection solutions on the market work by providing customers with an up-to-date database of IP addresses currently being used by VPN/ Proxy providers, pertaining to IPs owned by data/hosting centers. The OTT platform queries the database with a user's IP address and it returns either a yes or no.

VPN/Proxy providers have attempted to defeat these IP blacklists by upping the range of IPs they offer and switching to new IPs more frequently, but this is no match for an effective VPN/ Proxy detection system. GeoGuard's DB solution is updated multiple times per day to tackle this issue, since once per day is not enough.

However, the size and scale of the private VPN/Proxy industry (independently forecast to increase from US$1.3bn to US$ 2.7bn 2017 - 2023) has driven VPN/Proxy providers to seek new solutions to protect their revenues.

How GeoGuard DB Protects Your Content From Location Spoofing



How to Combat the Residential IP Issue

A solution that is now being deployed by VPN providers is to use hijacked residential IP addresses, which are linked to real homes and businesses and issued by legitimate ISPs.

As discussed earlier, millions of users worldwide have unwittingly had their residential IP addresses hijacked by "free" VPN and DNS Proxy providers (through a complicated term of service agreement), and sold to the highest bidder – usually other VPNs who offer them as a premium "undetectable"' service.

At the time of writing, GeoGuard has identified at least six companies using residential IPs, including Luminati, Oxylabs and SmartProxy; who are selling 72 million, 70 million and 40 million residential IP addresses, respectively, to VPN providers.

The use of residential IPs by VPNs and DNS Proxies is growing, and it endangers the viability of any streaming video provider that relies on territorial exclusivity and geographical restrictions to support their revenue model.

There is a catch, however.

Residential IP addresses are expensive to use for the actual content delivery, so they are only employed at the website level to grant users access to the content. Once the actual video starts streaming at the CDN level, the VPN or DNS Proxy provider switches to a cheaper non-residential IP address (a datacenter IP), and this switch can be detected by the CDN and they can immediately stop the stream.

By integrating VPN detection at the CDN level, residential IP addresses can be easily detected, and the illegal stream stopped. In fact, rightsholders and content owners are increasingly requiring their streaming services and OTT broadcasters to use third party CDNs for this very reason.

This CDN strategy provides rightsholders and content owners with the highest level of protection from geo-piracy caused by both the standard datacenter IPs used by VPN and Proxy providers as well as the more advanced residential IPs that they provide as a "premium" service to users.

GeoGuard's industry leading VPN/DNS Proxy detection is fully integrated at the CDN level with Akamai, AWS CloudFront and others to provide fast and easy access to our award-winning technology. This enables online broadcasters to utilize GeoGuard's solutions to remain compliant with studio and sports rightsholders content protection obligations. Our detection solutions are updated multiple times per day and can distinguish between mobile and fixed IPs, residential IPs (via CDN) and IPv6 addresses. GeoGuard has been independently tested and rated as 97.5% effective in detecting and blocking VPNs by Kingsmead Security.

About GeoGuard

At GeoGuard, we focus solely on geolocation-based security and protection of digital content. **As the only independently rated market leader for protection against VPNs and DNS Proxies and a Hollywood Studio Approved solution,** we help the digital media ecosystem and other industries guard against geo-piracy and location-based fraud. GeoGuard provides a suite of geo-filtering and fraud detection solutions, combined with human intelligence, to stop internet users from spoofing their location.

GeoGuard's solutions are based on the award-winning geolocation compliance and geo-protection technologies that its parent company GeoComply developed for the highly-regulated and complex digital gaming industry. Our software is installed in over 300 million devices worldwide, putting GeoGuard in a uniquely powerful position to identify and counter both current and newly emerging geolocation fraud threats.

GEOGUARD

Fraud Has No Place To Hide

With GeoGuard, fraud has no place to hide.

Contact us today to learn more about how GeoGuard can help you stop Geo-Piracy.

solutions@GeoGuard.com

Learn More