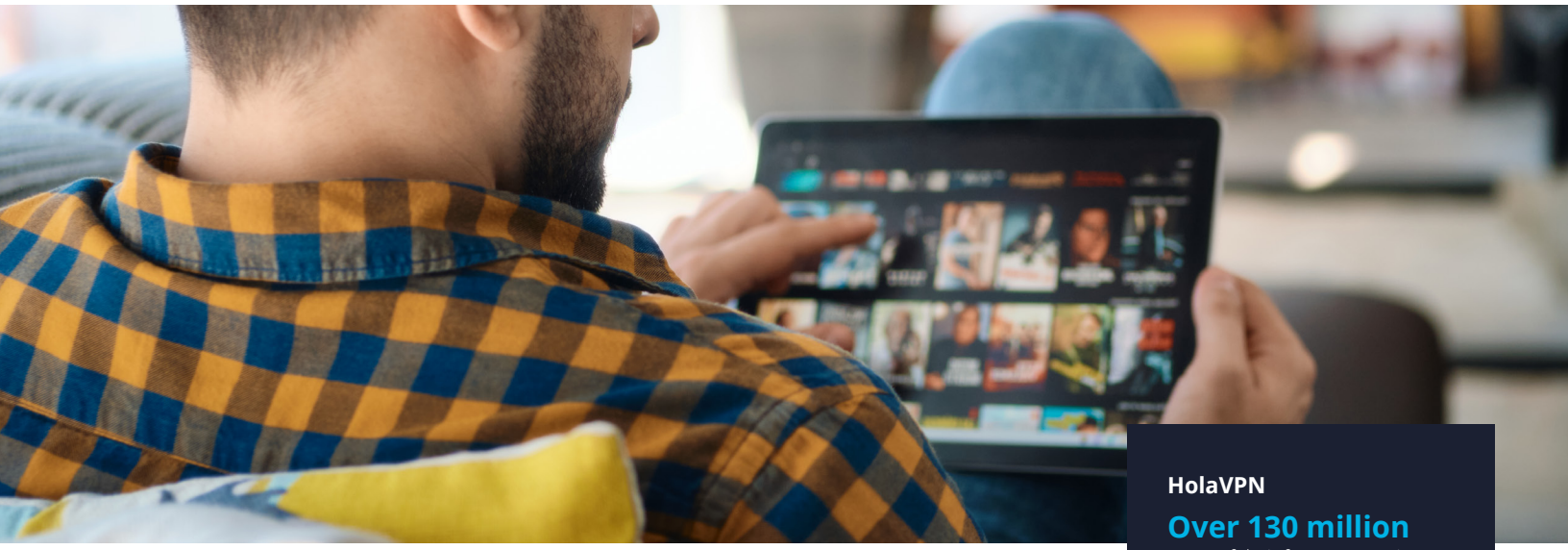
CASE STUDY: **National Broadcaster Tackles Geo-Piracy to Protect Content and Revenues**

GEOGUARD
Fraud Has No Place To Hide



Content Was Leaking to 60 Million Users for Free

A national broadcaster and content creator distributes its premium, original programming for free via an online streaming platform to viewers within its home country. It generates a significant portion of its revenue by selling exclusive rights to its premium content to foreign broadcasters. However, a massive volume of geo-piracy put this critical revenue stream at risk:

60+ Million

People out-of-country were using VPNs and DNS proxies to spoof their location in order to access their premium content

Foreign broadcasters didn't want to pay premium prices for unprotected "exclusive" content that their subscribers could easily access for free

Another Threat Loomed: Hijacked Residential IPs

An ongoing threat all broadcasters face is "free" VPN providers that essentially "hijack" the residential IP addresses of the people who download their software. These VPN providers then sell (or "sublease") these residential IPs to other VPN providers who promote them as undetectable IP addresses.

Residential IPs pose an even greater danger because they are not included in conventional VPN IP databases (which consist of data center IPs). As a result, the users of premium VPN services that offer residential IP addresses are able to circumvent traditional VPN detection methods. In fact, VPN services are specifically targeting their "premium" services to out-of-country users in order to illegally access this broadcaster's content.

HolaVPN
Over 130 million
users of their free VPN service have had their residential IP hijacked

Oxylabs
70 million
residential IP addresses

Luminati
72 million
residential IP addresses

SmartProxy
40 million
residential IP addresses

Staying Ahead of the Pirates

After testing other solutions, the broadcaster selected GeoGuard to meet their VPN/DNS proxy detection needs. The other solutions only implemented VPN and DNS proxy detection at the website level and didn't check again at the content delivery level. This deficiency allowed VPN/DNS proxy providers to bypass the check by using a residential IP when accessing the broadcaster's website, and then changing to a cheaper, data center IP as soon as the stream began.

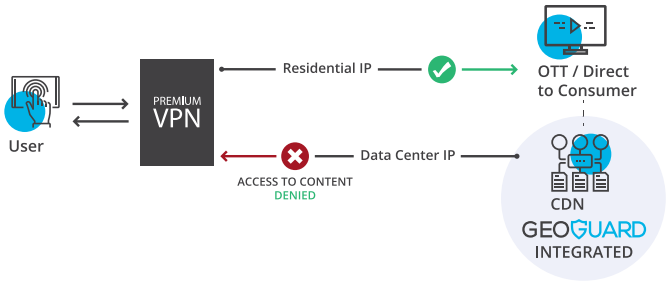
GeoGuard collaborated with the broadcaster to integrate GeoGuard Database (DB) with both their primary content delivery network (CDN) provider and their "fail-over" CDNs to ensure the solution worked across their entire network of edge servers. GeoGuard DB:

- Integrates with multiple CDN providers across the network
- Runs on a SaaS platform, eliminating the overhead of hosting and additional infrastructure
- Can simply be "turned on" at the CDN for enhanced protection from geolocation fraud and geo-piracy
- Is continuously updated (up to hourly) with both new and expiring IPs used by VPNs and DNS proxies

Solving the Residential IP Problem

Residential IPs are very expensive to use for actual content delivery. So, they are only employed at the website level to grant users access to content. Once the actual video starts streaming at the CDN level, the VPN switches to a cheaper non-residential IP address (a data center IP). Because the broadcaster integrated GeoGuard DB at the CDN level, the switch could be detected by the CDN and the illegal stream stopped.

Secondary Check at the CDN level to Stop Residential IPs:



Safeguarding Content and Protecting Revenue with GeoGuard

The problems facing this national broadcaster were large, complex and threatened their most critical revenue stream. GeoGuard's solution protected the broadcaster's geographically restricted content and the licensing revenue they rely on from widespread geolocation fraud and geo-piracy caused by the use of VPNs and DNS proxies.

As a result, the broadcaster was able to:

- Prevent foreign viewers from accessing territorially restricted content
- Ensure that local viewers could continue to seamlessly access and view content as usual
- Protect revenues by selling exclusivity rights on premium content to foreign broadcasters

By complying with its content distribution obligations with its foreign rightsholders, the broadcaster could protect their business model from geo-piracy threats.

aws partner network
Select
Technology
Partner

Buy Now

Akamai

Learn More

At GeoGuard, we focus solely on geolocation-based security, fraud detection and the protection of digital content and assets. We provide a suite of geolocation-based solutions that ensure accurate, authenticated and unaltered location data to a wide variety of industries and use cases.

GEOGUARD
Fraud Has No Place To Hide