



Today's Topics

- Introduction to Cartesian
- Video Streaming Consumer Access Trends
- Solutions to Mitigate the Unwanted Access



About Cartesian

We provide consulting and managed services for the communications sector; we deliver strategic advice, project delivery, and technology solutions

Insight & Advice

Consulting and analytics to give new perspective and vision

Management & Expertise

Successful delivery of complex projects for our clients

Solutions & Technology

Software to automate and improve business operations



Where We Help

We apply our industry knowledge, analytical skills, project management, and software capability to solve many different client issues



Telco Transformation

Leading and supporting change programs that help clients grow new revenues, improve efficiency, and reduce operational costs.



Video and Broadcasting

Developing, launching and operating cuttingedge video platforms that attract subscribers and build loyal audiences.



Network Economics

Increasing product profitability and return on capital by applying a data driven approach to network strategy and deployment.



Revenue Assurance

Helping clients to mitigate revenue and margin risks with best-practice controls and our own proprietary tool set.



Data Science

Harnessing service provider data to obtain action-oriented insights for business leaders and operational teams.



Transaction Services

Providing commercial and technical advisory services for target identification, market assessment and due diligence.



Our Clients

Cartesian has been delivering value to the service provider, media and entertainment sectors for over 30 years

Service Providers			Media/Entertainment		
SAT&T	verizon√	Frontier COMMUNICATIONS		NETFLIX	SPORTS
Sprint	WINDSTREAM	sky		WB)	20 A
Charter	TalkTalk	COMCAST	SONY	***	
BT	Virgin media	Hughes Net.	amazon instant video	BBC	UNIVERSAL. A COMCAST COMPANY
Century Li	nk° LEBARA	vodafone	france•tv	TFI	O/N



Streaming Video Access Trends



Online Video Piracy

Pirate activity and traffic increased while stay-at-home orders were in effect

>1B

U.S. visits to piracy sites in March

41%

Increase in US film piracy

12%

Increase in US TV show piracy

Coronavirus Lockdowns Lead to Surge in Digital Piracy

Traffic to black-market television and film sites has jumped 30% or more in many countries

ENTERTAINMENT

More people are pirating movies during the coronavirus lockdown

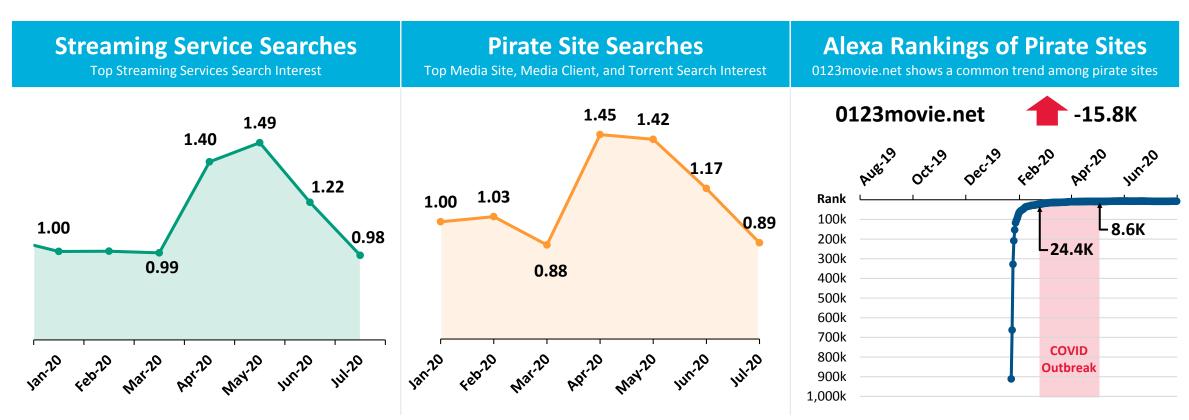
PUBLISHED MON, APR 27 2020-12:19 PM EDT | UPDATED MON, APR 27 2020-3:19 PM EDT





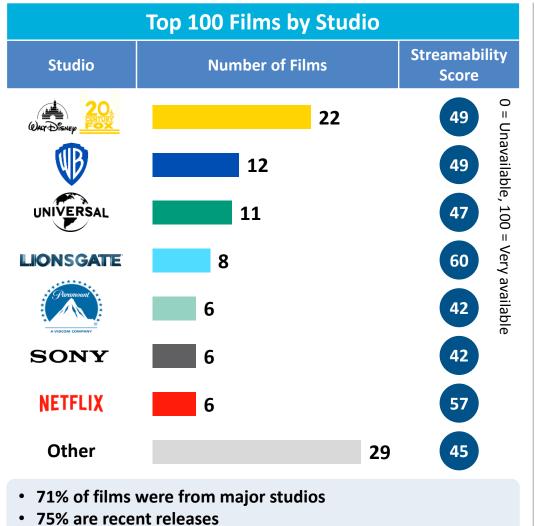
How Demand for Pirate Content Grew

- Popularity for streaming services spiked
- Video piracy rose roughly 33% during the initial COVID-19 period
- March 2020 it was observed more than 1b visits to the top 10 pirate streaming sites
- Interest in Torrent sites saw the biggest increase peaking at 70%
- Estimated 30m users in the US accessed pirate media sites like 0123movie

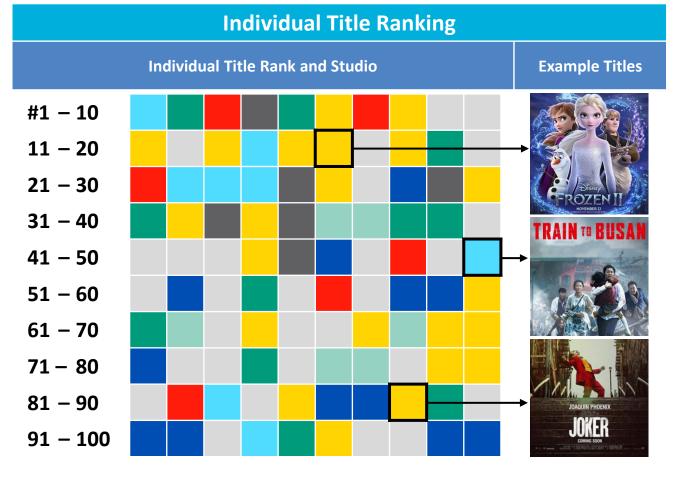


Top Films on Popular Torrent Site

We scanned popular content on torrent sites and found that most films are recent releases from major studios



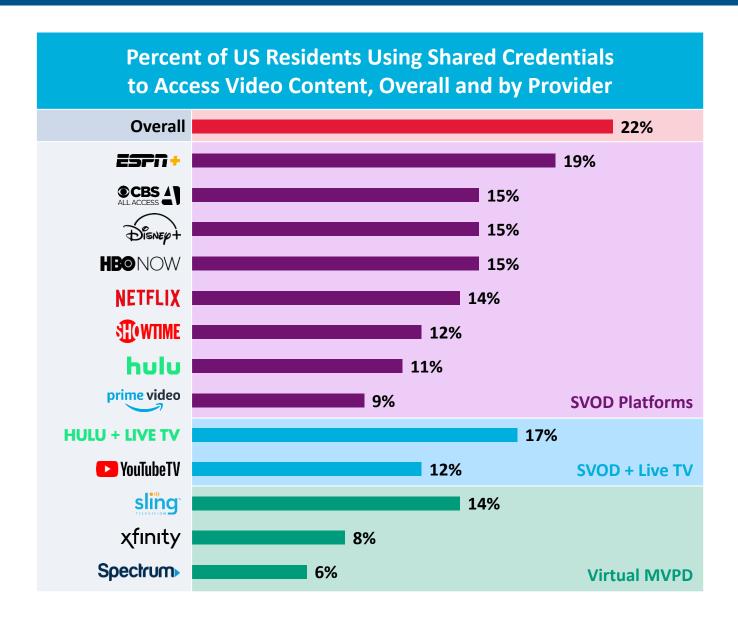
- 34% are 2020 releases, 41% are 2019 releases





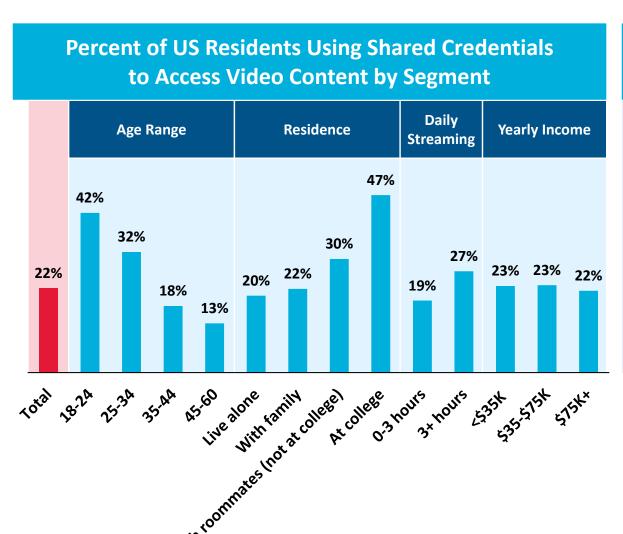
Credential Sharing is Common

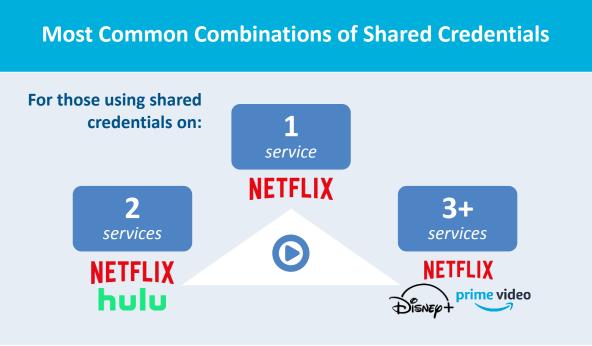
- 22% of our survey respondents are using shared credentials
- 45% of college students and 42% of 18-24-year-olds used shared credentials
- On average, those used shared credentials do so on 2.2 streaming platforms





Credential Sharing Is a Common Consumer Behavior







Solutions to Mitigate Unwanted Access



Streaming Video Credential Sharing Detection Programs

We work with streaming video companies to identify and stop credential sharing behavior

Streaming Video Challenge

Cartesian Solution

Results & Impact

Identify and prevent unwanted credential sharing behavior



Define

No existing framework to classify accounts engaged in credential sharing



Quantify Problem

Inability to analyze billions of raw log records to apply abuse and fraud classification to accounts

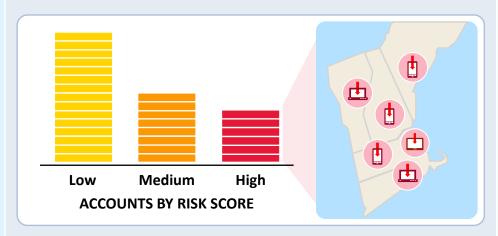


Take Action

Inability to determine the most appropriate actions to prevent unwanted behavior while minimizing risk to customer experience

Develop algorithms to score and identify accounts engaged in video credential sharing

- Calculate risk indicators across various behavior dimensions (e.g., geography, usage, applications)
- 2 Calculate a risk score for each account
- Prioritize accounts into actionable segments based on scoring outputs (e.g., fraud and abuse)



We quantified the scale of video theft and developed action plans to mitigate unwanted behavior

- Identified millions of accounts engaged in fraud/abuse to date
- Facilitated a process to take action (e.g., account notifications of suspicious behavior, forced sign-out and password reset)
- Provide continuous monitoring to track trends and measure impact of actions



Streaming Video Credential Sharing – Indicators

Credential sharing indicators span multiple dimensions of behavior

Example Credential Sharing Indicators

- **Unique Devices**
- New Registered Devices
- **6** Content Engagement
- Suspicious IPs
- Distant Events
- **Concurrent Sessions**
- Network Activity Clusters
- Location Activity Clusters

Number of unique devices that access an account

Number of new non-home devices identified over the screening period

Overall session duration or frequency on non-home devices

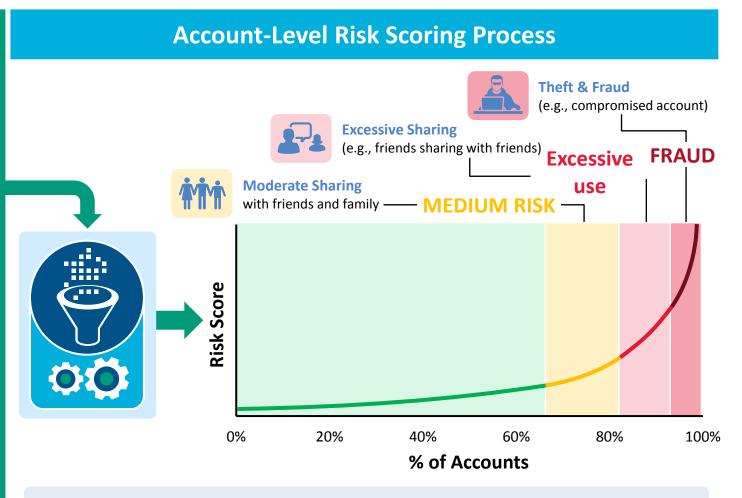
Number of logins from suspicious IPs (e.g., remote locations, VPNs)

Number of non-home logins occurring far apart within a short timeframe

Number of instances of concurrent logins on non-home devices

Distinct clusters of IP-based network use on an account

Distinct clusters of geographic patterns on an account

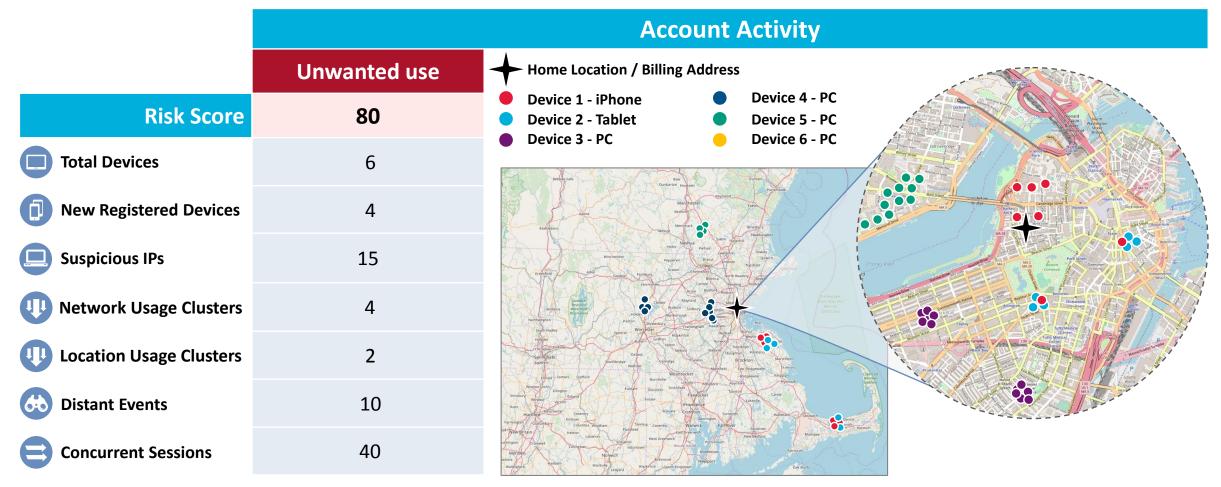


Indicators are combined in a scoring algorithm and accounts are rank-ordered based on severity and risk of credential sharing



Streaming Video Credential Sharing – Illustrative Account

The highest scoring accounts demonstrate suspicious credential sharing behaviors



High Likelihood of Credential Sharing

Devices 1 & 2 are used in consistent geolocation patterns and near the billing address, but devices 3-6 are all new registered devices used in disparate locations in frequent overlapping login sessions – this activity suggests multiple non-primary users on the account



Video Streaming Pattern – Mitigation Actions

We help our clients select the best mitigation actions to address unwanted behavior or outright theft

Notification



Notify account holder of suspicious logins

Password Reset



Reset the account password

Upsell



Upsell increased registered/active devices

Device Limits



Adapt concurrency or device limit policies

Two Factor Authentication



Implement two factor authentication

Further Investigation

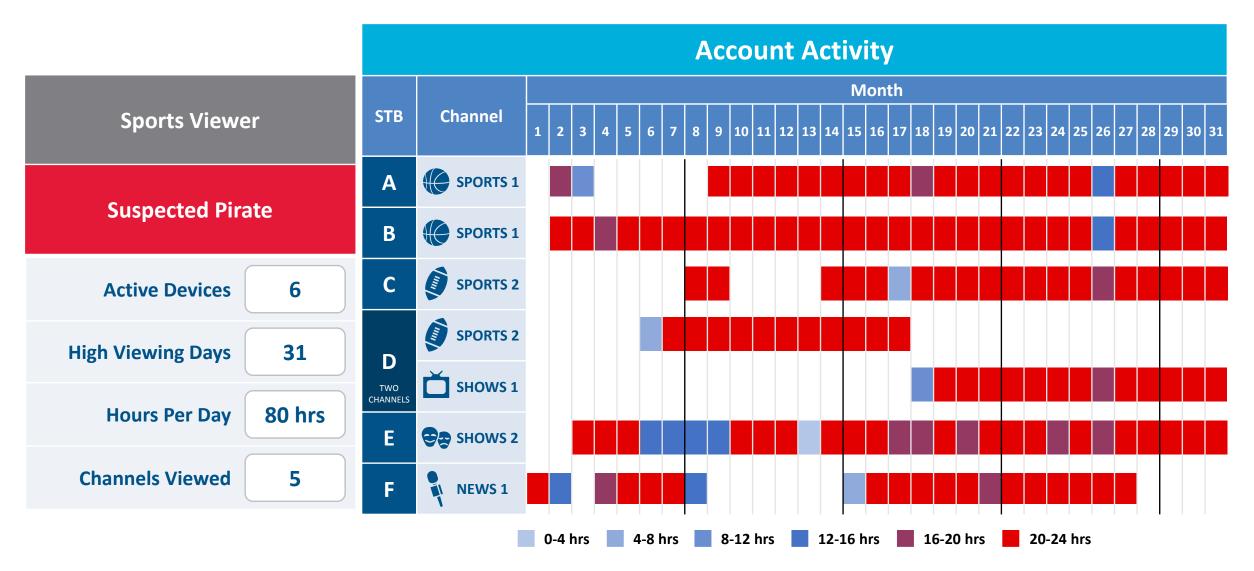


Research, customer focus groups



Video Stream Piracy

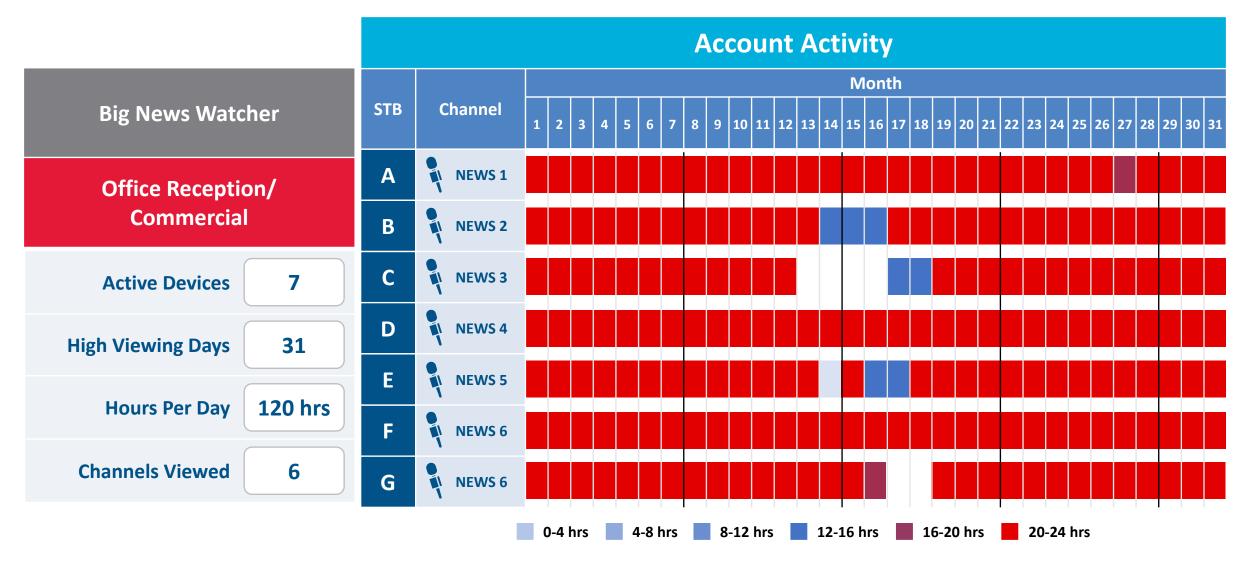
High value content patterns can warrant investigation





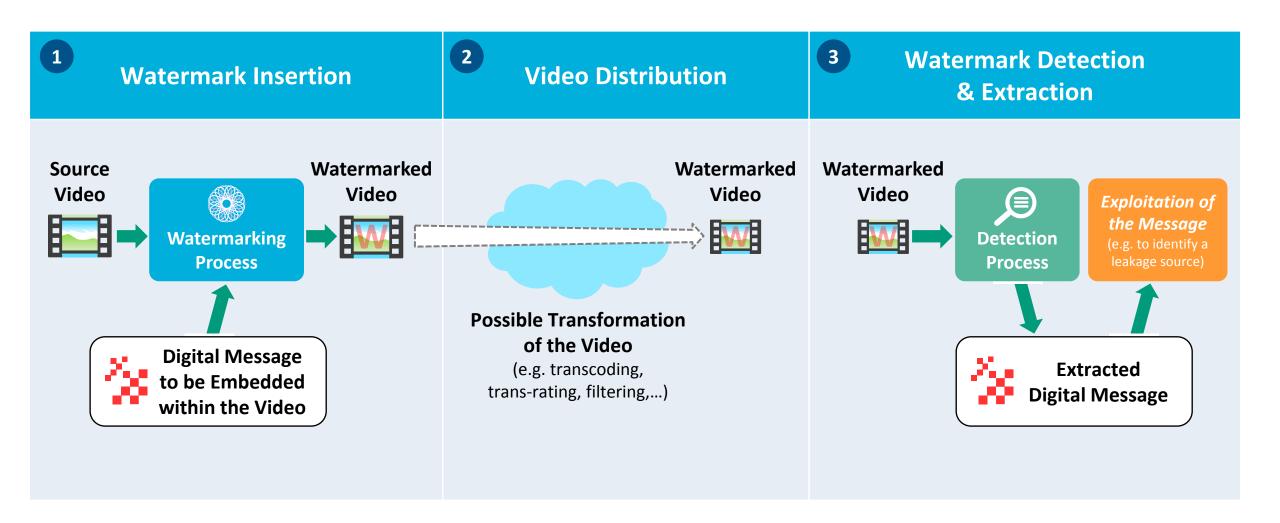
Video Stream Piracy

Constant single-channel tuning can be used to detect potential environments of use



Watermarking Solutions

We test how effective the watermark solution is in identifying where content is being used in illicit ecosystems





Evaluating Watermarking Solutions

We evaluate the characteristics of both the watermarking solution and the end-to-end ecosystem

Ecosystem Watermark Ability of a watermark to remain detectable by the dedicated tools, Robustness Security of the end-to-end despite possible attacks (transformations and alterations on the video) watermarking workflow Watermarking should be done in a way that it is not perceptible by **Imperceptibility** the human visual system, but strong enough to be reliably detectable Level of sophistication, by the dedicated tools performance and efficiency of the detection tools **Extraction Time** The time it takes to extract the watermark information from the video **Detection services,** The quantity of information that the watermarked message can reactivity and processes **Capacity** contain (expressed in number of bits). The more information contained in the watermark the easier it is to identify

Audits must check all of these items for a specific implementation with its specific set of parameters

Improving any one of these criteria can degrade the others.

Therefore, a case-by-case parameterization is needed to adjust the trade-off to a specific context (threats, QoS, constraints, objectives...)



Cartesian's Watermarking Assessment Certificate

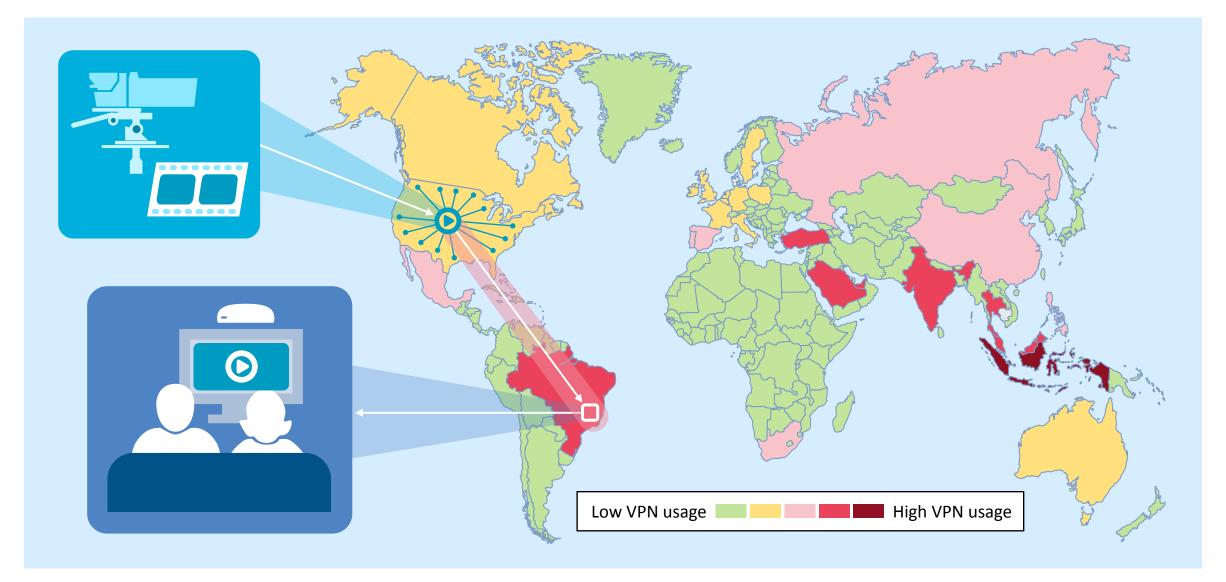
After an audit, we present the organization with a certificate to show that the solution has been independently reviewed





Geo-Circumvention Monitoring

Geo-blocking circumvention is also a common way consumers access restricted content





Cartesian's Approach to Geo-Filtering Testing

Our automated approach to geo-filtering testing service uses hundreds of combinations to attempt to access restricted content through circumvention mechanisms

Video Services and Mechanisms

Devices for Testing

Conduct
Automated Testing

Develop
Summary Report









- We have the capability to test any IP-streaming video service (app and browser-based)
- We test each video service using a methodology that incorporates keyword searches and Alexa ranking to choose the most popular services
- Tests are performed on a wide variety of devices
- We ensure devices are running latest operating systems
- Video services and circumvention mechanisms are installed on each device
- Geo-filtering tests for each video service, device, and circumvention mechanism are performed
- All relevant information is captured (e.g. test outcome, geo-location details, IP address information)
- Summary and trends of testing conducted presented in dashboards and reports
- Contains market comparison and analysis



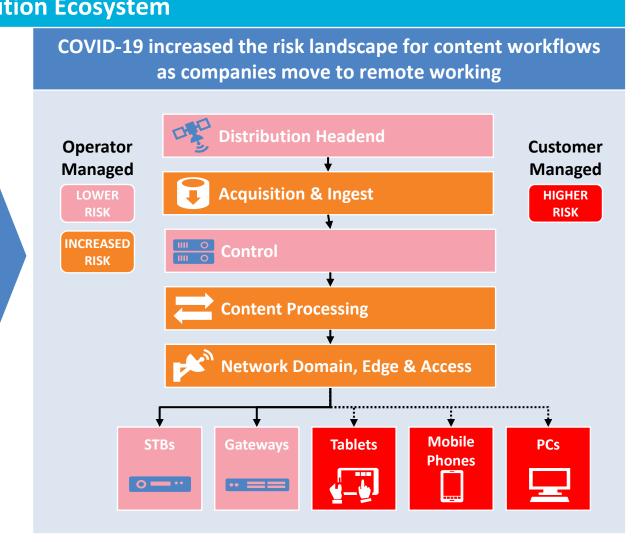
Once the circumvention mechanism has been identified the content provider can take the appropriate steps to block the offending IP addresses



Content Protection

Because of COVID-19 response measures, the security risks have increased

Video Distribution Ecosystem Over the years, the risk landscape has remained consistent **Distribution Headend Operator** Customer Managed Managed **Acquisition & Ingest** HIGHER RISK Control **Content Processing** Network Domain, Edge & Access Mobile **STBs Tablets PCs Phones** 0 --- ...





Cartesian's Farncombe Content Security Audit®

Our Security Audit Review is an unbiased appraisal of an organization's content security solution



Tailor

- We understand that one size does not fit all, and so our assessments are tailored to the organization
- Under NDA, we investigate where good practice exists and where there are areas for further investigation



Deep-Dive

- Our phased approach allows for areas of risk to be deepdived
- We review non-technical business processes such as onboarding and off-boarding of employees, risk management, InfoSec, as well as technical processes such as DevOps, Content Management Workflows and Cloud Storage, Obfuscation and Encryption



Observe

- We give the organization a summary of the observations, risks, and recommendations which will appear in the Security Review reports
- If issues are found, the organization will have time to remedy



Report

At the end of the assessment, the organization receives two reports:

- Security Technical Review: A detailed review of our finding that is kept in-house
- Security Executive Summary:
 Informs the organization's customers and content providers of the level of protection the solutions provides for their content

Our experts have the capability to assess both commercially available and internally developed content protection solutions



Cartesian's Farncombe Security Audit® Certificate

After an audit, we present the client with a certificate to allow potential customers to see that a system and been independently reviewed



The companies below recognize the Farncombe Security Audit for access to their content:

WarnerMedia SONY DISNEP







Business Analytics

Analytics can the drive the customers experience and improve business outcomes

IP Video
Churn Reporting

Prioritize drivers and initiatives to reduce early tenure IP Video package removals

Streaming Video
Quality Measurement

Recalibrate and tailor quality measurement to better reflect TV Platform experience

Streaming Video
Engagement Modeling

Segment and analyze usage patterns to identify successful engagement drivers

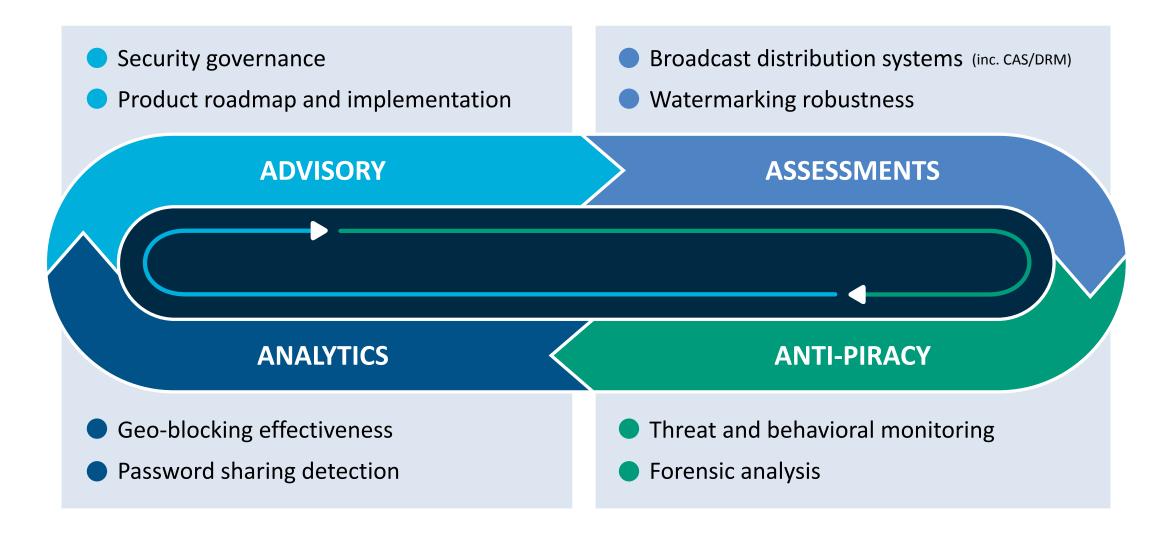
- ✓ Analyze removal drivers (engagement, QoE, sales channel, customer survey)
- Monthly reporting to track performance against ongoing initiatives
- Explore removal drivers and evaluate ongoing experiments

- Recalibrate KPI for streaming video services
- Use historical customer data to optimize scoring in line with quality perception indicators using logistic regression and grid search models
- ✓ Identify new engagement success metrics to feed into ongoing product testing and experimentation
- Explore differences in content preferences and behaviors to inform actions that will promote successful engagement on the TV service



Cartesian Content Security Services

Our consulting services and solutions protect video content end-to-end







Lee Kent

Head of Content Security
+44 (0) 7944 684 559

lee.kent@cartesian.com



www.cartesian.com