Whitepaper

Content Piracy is a Cybersecurity Problem

Building the Cybersecurity and Revenue-protection Layer for Pay-TV

Authors

Jay Chauhan (Tech Mahindra)

Nivendran Veerappan (Astro Malaysia Holdings Berhad)

Executive Summary

Pay-TV piracy has outgrown its old definitions and is no longer only about stolen channels, illegal set-top boxes or lost subscription revenue. It has become a distributed cyber-enabled threat that affects sports rights, advertising, cybersecurity and platform integrity.

Legacy responses such as legal notices, raids and domain blocking still matter, but they cannot keep pace with piracy that emerges, shifts and monetizes in near real time. The challenge is no longer simply removing illegal streams, but detecting, disrupting and preventing piracy through coordinated operations. This paper argues that pay-TV operators must treat piracy as a cybersecurity and revenue-protection discipline, supported by an anti-piracy control plane that enables continuous monitoring, automated escalation, evidence generation, repeat-offender tracking and coordinated disruption. While piracy cannot be eliminated, its economics and reach can be significantly reduced.

Table of Contents

Introduction

Pay-TV piracy has outgrown a cyber-enabled threat that encompasses sports rights, advertising fraud, data theft, malware exposure, and platform integrity.

For broadcasters and pay-TV operators, legacy models characterized by legal notices, raids, and domain blocking continue to matter, but they fall short of solving the whole problem. They react slowly when pirate streams appear minutes before a live match, move across domains, spread through chat groups, and monetize through ads or payments. The operational question has shifted from 'How do we remove illegal streams?' to 'How do we detect, disrupt, and prevent piracy in near real time?'

The anti-piracy control plane is the solution that bridges the gap. It connects data signals that typically originate from separate teams, including content security, streaming operations, content delivery networks (CDN), subscriber identity, watermarking, takedown workflows, legal evidence, and regulator coordination. The anti-piracy control plane's job is to turn piracy response from manual casework into an always-on operating system. This implies 24x7 monitoring, faster evidence generation, automated escalation, repeat-offender tracking, and coordinated piracy disruption and recovery.

Content piracy is unlikely to be eliminated; however, piracy economics can be damaged and its reach reduced. The goal here is not to build a bigger legal department, but rather to evolve into a faster anti-piracy operating model.

How Content Piracy Has Advanced

Before the rise of generative AI, piracy was simpler to understand. It typically involved a household buying an illegal set-top box (STB), a diner showing a live game without a license, or a website carrying unauthorized content. In response, a legal team would file notices, and law-enforcement agencies would act where possible. While this model still exists, it no longer covers the full spectrum of piracy.

The headline trend isn't that piracy has increased. Instead, it has now evolved into a sophisticated attack on the operator's own infrastructure. Four key trends that matter here:

- **Pirates stopped breaking encryption and started stealing the keys.** When it comes to digital rights management (DRM), pirates target the weakest link, i.e., where decryption happens in software rather than in hardware. Here, the content keys can be extracted and the stream reduced to unprotected 'clear key.' Even though the encryption stays intact, the keys are now easily accessible. Software DRM on its own is no longer enough; it represents a soft target. Real protection now demands hardware-based DRM anchored in a trusted execution environment on the viewer's device.

- **CDNs have become the new piracy battleground**. Instead of capturing and re-hosting a stolen feed, pirates steal an access token from legitimate apps and use it to extract original, broadcast-quality streams directly from the operator's own CDN. Once this is complete, they redistribute the stream at scale. Ultimately, this leaves the pay-TV operator to pay the cost. Firstly, the CDN bills for pirate traffic, and secondly, genuine subscribers experience buffering issues and reduced QoE due to illegal bandwidth demand. Because concurrency limits and 'heartbeat' checks are easily spoofed, a single account can deliver stolen streams to thousands of illegal devices without breaking any encryption.

- **Piracy 'corporatized' into a services business.** Piracy has evolved into an organized commercial operation with tiered pricing, card and crypto payment processing, electronic program guides, and even customer support. In fact, many pirate services match the sophistication of legitimate platforms.

- **AI made piracy easier.** Pirates deploy AI to bypass automated content recognition by subtly altering frames, audio, and aspect ratios. AI is also used to strip or defeat watermarks, automate extraction of high-quality streams, and auto-scale distribution across cloud servers, making it hard to shut down every region. Pirates also deploy AI agents to scrape content from platforms and restream trending content within minutes, resulting in bad actors becoming faster and more resilient, treating every content takedown as a detour to find newer routes.

These four trends have compounding effects, especially during live sports, which is the most time-sensitive content. A stolen match is most valuable while it is live; a pirate site takedown does little to recover lost revenue after the match is over. The same stolen live event can surface in hundreds of places within minutes, and when one stream or domain is removed, the illegal traffic just gets redirected to a mirror site. This is why we believe anti-piracy now has to behave like a SecOps function, i.e., detect fast, act fast, and learn continuously.

The Anti-Piracy Control Plane

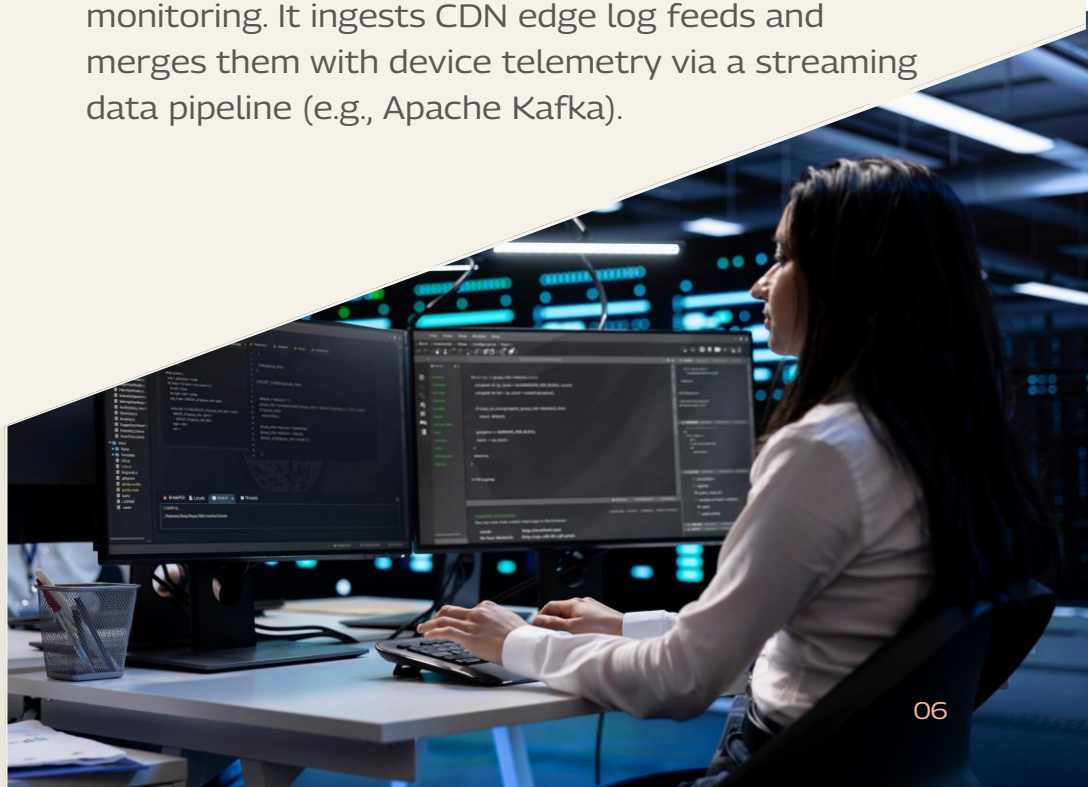
This acts as an operating layer that connects detection, intelligence, disruption, enforcement, and recovery.

The control plane has to provide answers to five key questions:

- Where is the illegal stream or asset?
- What source or account is leaking the asset?
- How far has it spread?
- What action will disrupt it fastest?
- What evidence is needed for repeat enforcement?

Following the answers, the control plane needs to connect the following layers as illustrated in Figure 1:

- **Content Identity Layer:** Determines the protected media assets, i.e., live channels, sports feeds, VOD assets, highlights, clips, subtitles, audio tracks, and metadata.
- **Signal Collection Layer:** Captures real-time data from app telemetry, watermark matches, subscriber behavior, social media, and suspicious domain monitoring. It ingests CDN edge log feeds and merges them with device telemetry via a streaming data pipeline (e.g., Apache Kafka).



The Anti-Piracy Control Plane

Integrating content security, CDN logs, device intelligence, and legal workflows into one framework.

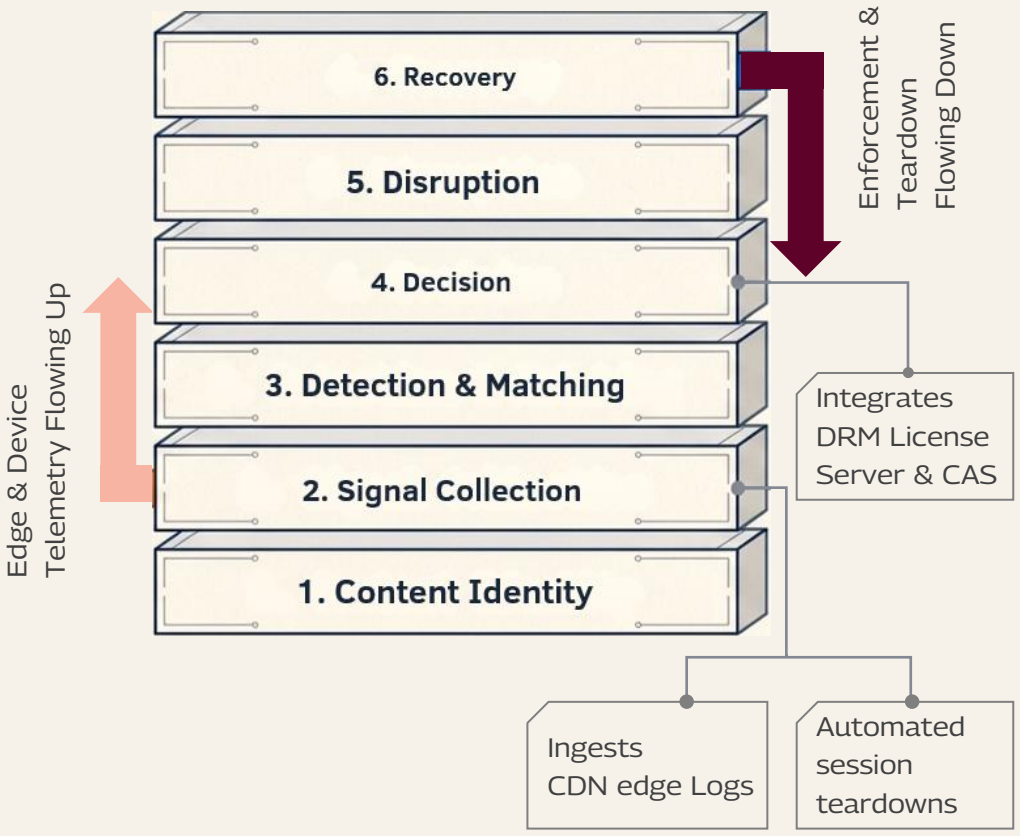


Figure 1: Digital Resilience Framework

- **Detection and Matching Layer:** Identifies piracy using stream fingerprinting, watermark detection, content-matching techniques, and credential abuse. Two distinct vectors are handled in this layer:
  - Credential and Token Abuse: By conducting concurrency analysis, the aim is to detect sessions in which a single authenticated credential or token appears across multiple distinct networks (ASNs) within a short correlation time span.
  - DRM Key and CAS Compromise: The objective is to prevent the extraction of decryption keys and conditional-access exploits through DRM/CAS integrity monitoring and revocation.
- **Decision Layer:** Determines the appropriate countermeasure, like a takedown notice, domain blocking request, account suspension, or escalation to the regulator. When supported, it connects to DRM and CAS systems through APIs to automatically revoke access.
- **Disruption Layer:** Includes platform takedowns, domain blocking, automated session teardown, payment disruption, ad disruption, and criminal enforcement.
- **Recovery Layer:** Measures KPIs, i.e., reduced instances, recovered subscriptions, and enforcement outcomes.

From Takedown to Disruption

Piracy continues to evolve, and anti-piracy strategies must evolve with it. Instead of relying on manual casework, operators need a coordinated system that detects, disrupts, and removes illegal streams in real time. Through signals from content security, streaming operations, CDN, subscriber identity, watermarking, takedown workflows, and regulator coordination, it offers constant monitoring, tracks repeat offenders, enables quicker escalation, and automates disruption.

Pay-TV and streaming operators must move from removing illegal streams to disrupting the piracy ecosystem itself. That means targeting the sources, intermediaries, and revenue channels that allow pirate networks to survive repeated takedowns, including:

- Accounts, devices, and locations that are likely to be sources
- Suspected domains, chat groups, and apps
- Payment and advertising sources that fund piracy operations

This is critical because piracy networks survive through speed and repetition. If pay-TV operators merely have their links removed, pirate networks will adapt much faster than law enforcement can. By correctly identifying patterns, sources, and recurrence, they can make piracy far more expensive for bad actors to run.

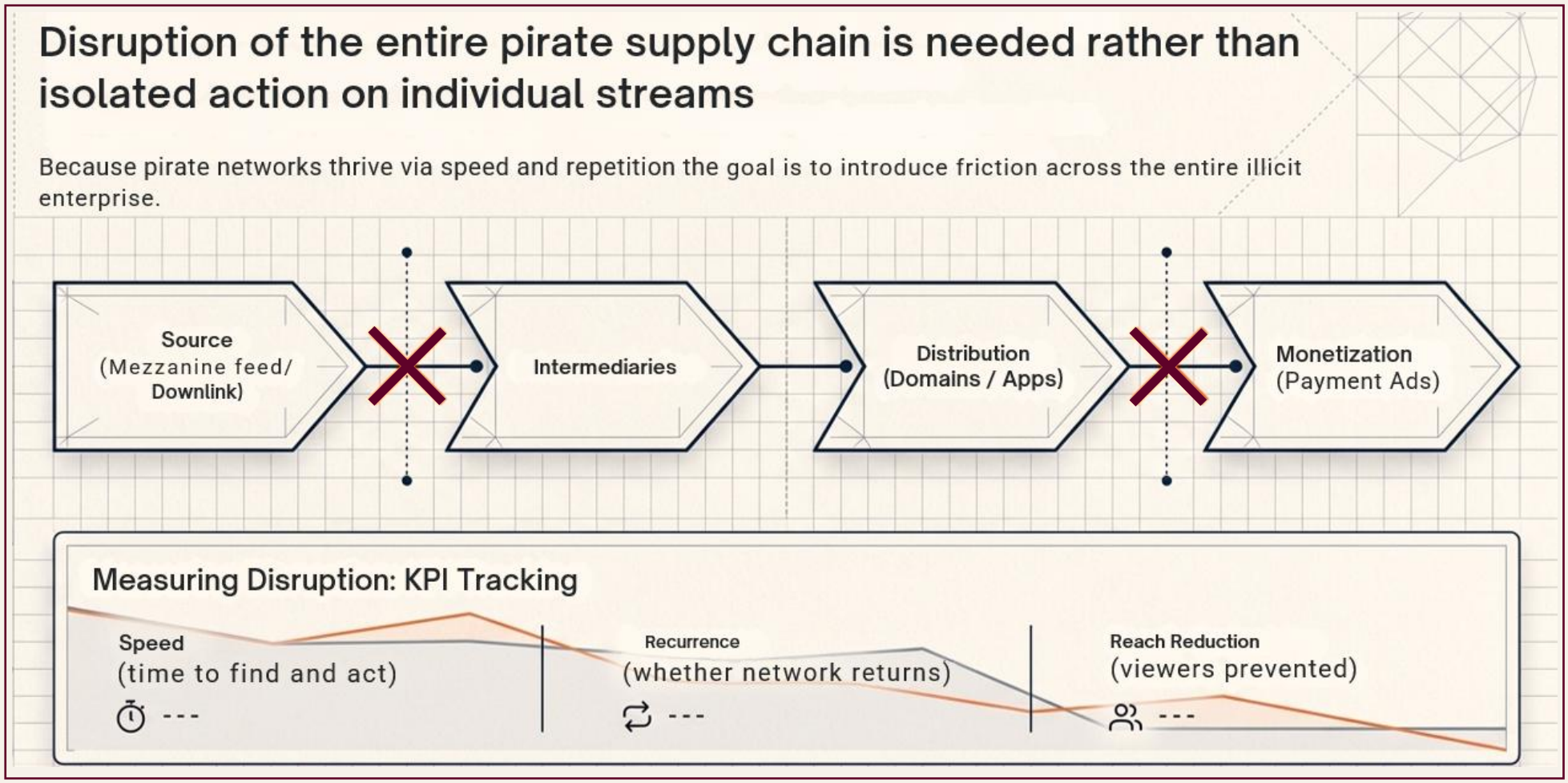


Figure 2: Disruption of the Content Piracy Supply Chain

Disruption can be measured in three ways

- **Speed:** How quickly illegal streams are found and acted on.
- **Recurrence:** Whether the same source or network returns.
- **Reach reduction:** How many illegal viewers were prevented or redirected.

A Coordinated Operating Model

A Pay-TV broadcaster or streaming operator cannot solve piracy alone. It demands a collective defense, built on coordinated action across the ecosystem. A sound operating model connects the broadcaster with rights owners, ISPs, social platforms, payment providers, regulators, and law enforcement.

This is because each stakeholder tends to see and address only a part of the problem:

- Broadcasters are concerned with content, subscribers, and operational impact.
- Rights owners view it through the lens of contractual exposure and revenue leakage.
- ISPs can help with blocking and network-level enforcement where legally permitted.
- Social and messaging platforms control distribution points.
- Payment solution providers can disrupt pirates' monetization.
- Regulators and enforcement agencies provide legal authority.

The anti-piracy control plane must support low-latency execution and automated coordination across key stakeholders. This enables the creation of structured evidence packs that legal, technical, and platform teams can act on immediately. A typical evidence pack includes:

- Content title or event
- Exact timestamp of infringement
- Illegal URL, app, group, or account
- Screenshots or captured stream samples
- Forensic watermark payload or fingerprint result
- Estimated reach or group size
- Recurrence history
- Suspected source pattern
- Recommended action
- Contractual basis for escalation

In doing so, the operating model shifts anti-piracy efforts from isolated interventions to coordinated, intelligence-led disruption across the ecosystem.

AI and Automation in Anti-Piracy

A key role of AI in today's anti-piracy systems is to extend their scope to social and messaging platforms and automate the identification of suspect channels. Detecting the probability of infringement in shared messages facilitates faster takedown requests and counters the speed at which piracy networks spread across messaging platforms. Other key AI use cases include:

- **Real-Time Edge-Log Clustering:** Instead of relying only on reactive web crawling, AI models process very high volumes of live CDN logs at the network edge. They flag rapid IP rotation, headless browser signatures, and automated user-agent modifications. This helps pinpoint piracy bots and disable their access at the edge before content can be restreamed.
- **Live Sports Stream Detection:** AI scanning of web, social, and messaging ecosystems for suspected live restreams is a key use case. This is then matched against known content, match schedules, and event windows to first prioritize potential high-impact infringements.
- **Link and Domain Clustering:** AI models can, in real time and at scale, group mirror sites, redirect chains, and recurring domains, enabling enforcement teams to act against entire networks rather than isolated links.
- **Credential and Account-Abuse Detection:** Similar to fraud detection in banking, detecting abnormal subscriber behavior that indicates restreaming, credential sharing, or the presence of device farms is a critical AI use case.
- **Automated Evidence Packs:** A good AI 'back-office' use case is automating the manual tasks involved in preparing structured evidence for legal, platform, and regulatory workflows. This can dramatically shrink the time between detection and action.

Implementation Roadmap

A realistic deployment requires a phased approach that accounts for typical legacy broadcast hardware and digital streaming stacks found within Pay-TV environments.

Phase 1: Establish Visibility

- Identify high-exposure premium content assets (live sports, linear feeds, VOD, etc.).
- Build secure APIs between third-party monitoring agencies and one's own infrastructure.
- Build an organization-wide taxonomy of piracy incidents and a real-time registry.
- Establish baseline metrics for detection latency, recurrence intervals, and unverified stream requests.

Phase 2: Integrate Workflows

- Connect content security, streaming engineering, network ops, and subscriber billing platforms.
- Implement automated dynamic server-side session teardown for authenticated OTT streaming connections.
- Impose cross-referencing of repeat offenders against active billing accounts and device IDs.
- Bring in live-event monitoring dashboards for live sports broadcasts.

Phase 3: Automated Disruption and Conditional Access System (CAS) Revocation

- Implement agent-based automation of link clustering, threat prioritization, and creation of verified evidence packs.
- Integrate automated satellite smartcard and CAS revocation loops into the decisioning engine.
- Fuse forensic watermarking extraction with live enforcement engines for real-time stream tracing and isolation.

KPIs: Indicative Operating Targets

The images below are indicative target SLAs that may be treated as design goals for the control plane. Real-world performance will vary depending on an operator's CAS/DRM vendor, EMM cycle design, and scale.

Figure 3: Control plane KPIs

The KPIs to design for include:

- **Detection Latency:** Restricts content pirates from intercepting, extracting, and illegally distributing premium feeds during high-value live event broadcasts
- **Session Revocation:** The time taken to intentionally degrade the pirate consumer experience.
- **Watermark Extraction:** Turnaround time to provide immediate, auditable attribution so that account terminations can be executed.
- **Conversion Yield:** Displays a measure of the financial return from redirecting intercepted pirate traffic to the operator's own subscriber sign-up workflows.
- **Constraint Violation Rate:** Shows the measure of the error in the control plane. This must be measured to ensure that AI-driven automated anti-piracy actions don’t disrupt legitimate subscribers.

Conclusion

AI misuse by content pirates will ensure piracy becomes increasingly sophisticated. As a countermeasure, streaming, broadcast, and pay-TV operators should start treating it as an always-on operating risk.

The solution goes beyond stronger laws, better takedowns, or increased consumer warnings. They are necessary but not sufficient to control piracy and strengthen measures against it. The real shift must be operational. Building a control plane that connects identity, signal collection, detection, decisioning, disruption, and recovery is an immediate priority.

Content piracy is no longer a legal concern; it is a cybersecurity breach and an operational challenge that must be managed with technical discipline and an action-oriented approach. With vulnerabilities compounding by the minute, delaying active mitigation is a risk one cannot afford.

References

- U.S. Chamber of Commerce, Global Innovation Policy Center. (2019, June). Impacts of digital video piracy on the U.S. economy. U.S. Chamber of Commerce. https://www.uschamber.com/assets/documents/Digital_Video_Piracy_June_2019.pdf
- Alliance for Creativity and Entertainment. (2025, July 22). Study finds consumers up to 65 times more likely to be infected with malware when using piracy sites. Alliance for Creativity and Entertainment. https://www.alliance4creativity.com/news/study-finds-consumers-up-to-65-times-more-likely-to-be-infected-with-malware-when-using-piracy-sites/

Jay
Chauhan

Group Practice Head,
Tech Mahindra

About the Author

Jay is leading the global M&E business and its AI-led growth strategy at Tech Mahindra. He works across shaping market strategy, driving innovation, and advising media leaders on AI transformation. Jay led the development of Tech Mahindra's M&E service line's first Agentic AI IP for the media industry and is a recognized thought leader through industry research and whitepapers.

Nivendran
Veerappan

Vice President, Head of
Broadcast Technology,
Astro Malaysia Holdings Berhad

About the Author

Nivendran Veerappan is a broadcast and media technology executive with nearly 25 years of experience spanning television, OTT, content delivery, and platform engineering. He currently leads Astro's broadcast technology organization, overseeing the strategy and evolution of broadcast, media supply chain, OTT, and broadband platforms. His work focuses on technology modernization, workflow automation, and the delivery of scalable, high-performance media services across an increasingly converged digital ecosystem.

About **Tech Mahindra**

Tech Mahindra (NSE: TECHM, BSE: 532755) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 146,000+ professionals across 90 countries, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognizes global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies.. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

www.techmahindra.com
www.linkedin.com/company/tech-mahindra
www.x.com/Tech_Mahindra