Protect or plunder

Surgical strikes to disrupt industrial-scale piracy

2022

In partnership with Verimatrix

verimatrix
DRIVING TRUST

Caretta Research

In a nutshell

With content piracy reaching industrial scale, old-school blunt security has less and less impact and risks annoying paying consumers as much as pirates. A new data-driven approach can target the riskiest behaviour with surgical precision: cutting off criminals while improving the user experience for everyone else.

In a super-aggregation world, supporting apps across hundreds of devices and platforms no longer means a tradeoff between security and user experience.

1. New approaches like **zero-code app hardening** reduce development effort, improve security and maximise the number of platforms and consumers reached.
2. Content and platform owners can **improve user experience** by reducing friction and offering additional features — like higher quality video, casting or downloadable content — that were previously deemed too risky.
3. With analytics-based tools in place to **monitor on-device behaviour**, content security is maintained by reducing or cutting off access only on those devices showing suspect activity.

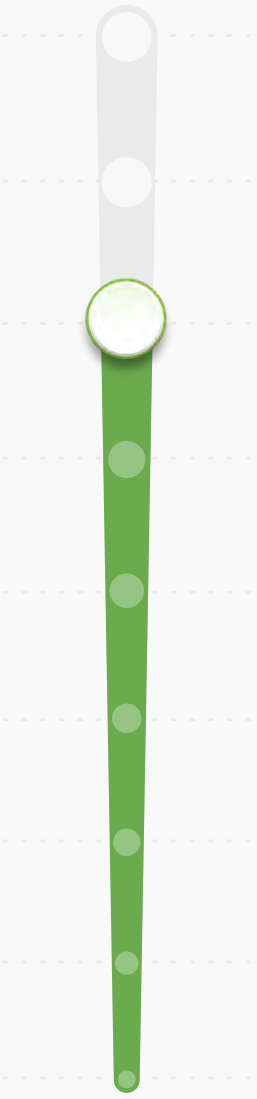
The financial benefits of content security are becoming easier to quantify and justify by linking investment directly to outcomes.

1. Understanding **individual consumer behaviours** means content and platform owners can target their security budget where it will have the most impact.
2. A modern analytics-led anti-piracy approach creates a **feedback loop**, constantly adjusted to avoid the wasted cost of over-responding to a lower risk, or the revenue impact of under-responding to a higher risk.
3. It's now much easier to create a **positive ROI for security** measures — lowering content and technology costs while increasing user retention and revenue.

Delivering piracy countermeasures is being transformed from a fragmented game of whack-a-mole to a targeted operation driven by data.

1. **A layered approach** ensures the most appropriate security measures from a comprehensive toolbox are deployed to the right user, on the right device at the right moment.
2. More effective, but costly, measures like forensic watermarking can be **targeted on devices and behaviours** most likely to be the source of illegal content.
3. The **response is always aligned with the risk**, maximising the chance of disrupting pirates, while remaining transparent to everyone else.

HIGH RISK



Traced leak (watermark/fingerprint)

Environmental sensors
- ambient lighting
- G-force
- behavioral analysis

Behavioral analysis
- who whatches
- what
- when
- how long
- behaviour after forced
- restart

Copy protection alert
- blacklisted HDCP
- overlays used

Devices environment alert
- installed apps rooting
- VPN
- IP location does not match
- cellular network

Code protection alert
- debugger active
- binary tampered

No suspicious activity

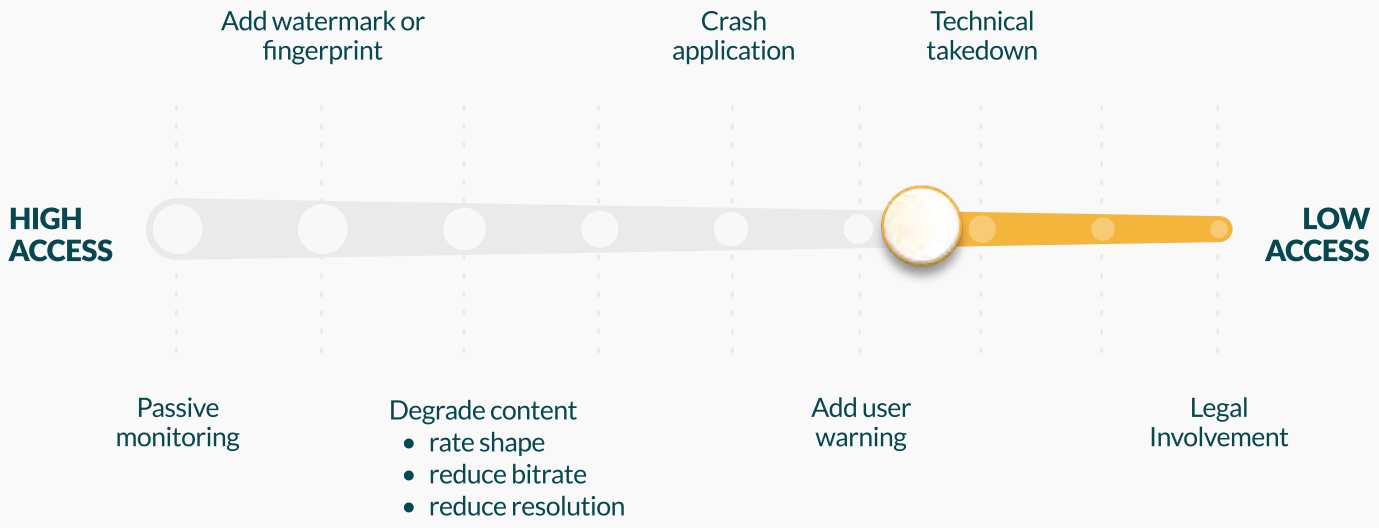
LOW RISK

Moving the levers

Content and platform owners can use a range of interventions to tackle piracy, tuned to the outcomes that provide most benefits to their business in terms of user experience and revenue.

"Quick win" interventions can address opportunistic lower-risk piracy while maintaining unimpeded access to content for the majority.

More strategic interventions based on data analysis can target content takedowns on those users with behaviour patterns indicating a high-risk of commercial levels of piracy.



Piracy: a revenue opportunity

Tackling content piracy is often described by industry insiders as a game of "whack-a-mole". A random and often futile fight against the industrial scale of content criminals.

But making more precisely-targeted interventions, based on tracking the actual behaviour of pirate distributors and consumers, leaves it much less of a game of chance. Now it becomes easier to target the precise location of the mole while predicting when it will pop up next.

Content and platform owners have a range of intelligence and tools at their disposal, allowing them to fine-tune a response based on the level of threat. They can detect and cut off the hardcore pirates, while encouraging the more reluctant, or unintentional, consumers of illegal content to switch to legitimate service, all while avoiding degrading the user experience for paying customers.

This approach can transform anti-piracy from a cost-centre with a compliance focus to a revenue opportunity with the aim of maximising user experience. Identifying and cracking down on criminal behaviour, while directing and converting viewers towards high-quality legal options.

The analysis in this report is based on Caretta's continual industry research with content owners, rights holders, streaming services and platform owners. Some of the key content security challenges identified include:

- How to extend user and data and analytics into monitoring piracy and usage behaviour
- How to reach people who are watching content but not paying
- How to moderate behaviour of high-risk users to prevent leakage
- How to target investments in content security to maximise impact.

Managing user experience

The super-aggregation app challenge

Content security has often been at odds with user experience (UX). Operators have made trade-offs between making content services easily accessible on a wide range of devices and super-aggregation platforms, and managing the security of those apps.

Content owners face a dilemma: **risk degrading user experience and revenue** by reducing the number of platforms and devices supported or by imposing intrusive security restrictions on apps, or increase the risk of less-secure devices becoming the source for pirates — particularly legacy devices which may be harder to secure.

Doing nothing isn't an option either: the evidence shows that high-quality pirated content is available almost immediately after any digital distribution and piracy subsequently spikes.

Crude initiatives to protect content make it harder for legitimate users to view what they've paid for on their device of choice. Or, security-led restrictions — such as limiting downloading or casting, throttling frame rates or image resolution, or imposing visible watermarking — negatively impact all users, rather than just those demonstrating risky behaviours

Worse still, many platforms stop supporting older devices altogether, cutting off swathes of potential customers, and a particular challenge for public service media providers with obligations of universal service.

App owners worry that updating apps, including making security enhancements and app hardening, will cause issues on legacy devices, impacting UX, and resulting in complex, costly and time-consuming testing.
The end result? Content apps, particularly on smart TV platforms, often end up as a security weak spot, App owners shy away from adding more protection, fearing the negative impact on UX.

In a competitive media market, where protecting the value of premium content and delivering a great user experience are equally important, a new approach is needed —one that is better able to manage the risk of piracy and maximise access to content.

An emerging solution is using "zero code" app hardening. These tools can secure and protect apps by simply adding a "wrapper" to the existing code. This approach greatly simplifies the process of securing a large volume of apps, without needing additional developer resources.

The number-one pain point we hear from streaming platforms is the challenge of delivering content and apps to a wide range of devices, from smart TVs to set-top boxes, to streaming sticks, mobiles and tablets — all with wildly variable specs and capabilities. Smart TVs in particular tend not to receive updates after the first 2-3 years of model life, yet have a service life of 5-10 years.

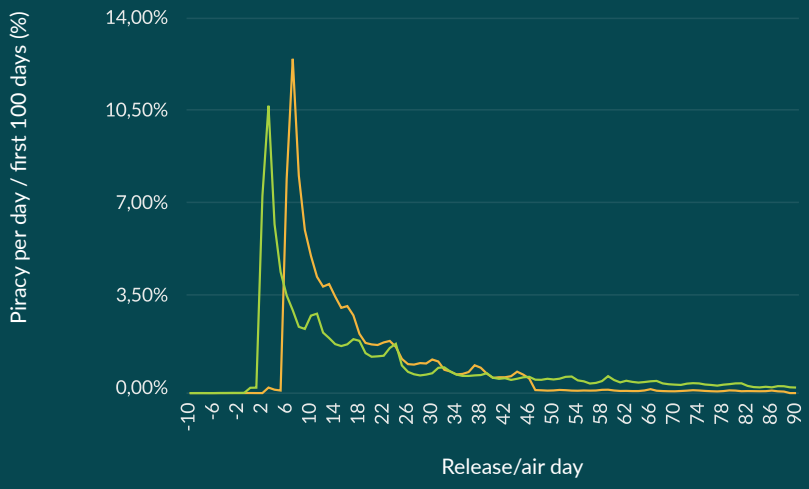
Devices that aren't updated are less likely to support the latest encryption standards, or may have weakly-protected certificate stores. They may be more easily rooted, or have limited HDMI/HDCP protection.

The streaming piracy peak

Piracy is an immediate problem from the date of any release, and particularly from the date of digital (non-theatrical) release. There is a pronounced spike in piracy from the moment a high-quality digital copy is released, and piracy is persistent after that.

Day-and-date releases have much higher initial piracy than theatrical-then-digital releases. Camera rips from theatrical are almost always lower quality than digital copies - enough to discourage downloading or streaming of these in of waiting for a higher quality version to be available at digital release.

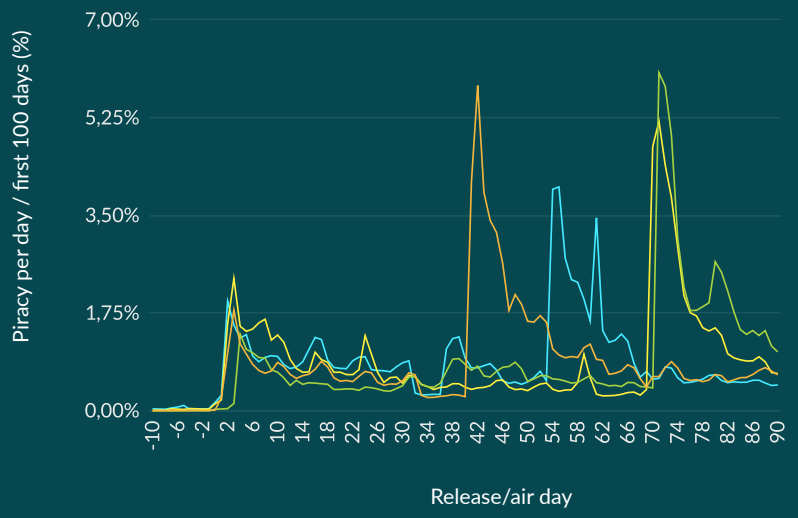
If it were possible to reduce access to high-quality content in the piracy market then it follows that piracy would be reduced. Even relatively subtle reductions in quality such as manipulating the resolution, framerate, bitrate and audio syncing may introduce enough of an annoyance to customers that legal options are favoured, particularly for live events such as sports. It then becomes incumbent on the operators to find ways to target the piracy audience and guide them towards higher quality content on legal platforms.



Piracy following day-and-date release strategy

- Black Widow (Disney+)
- Matrix Resurrections (HBO Max)

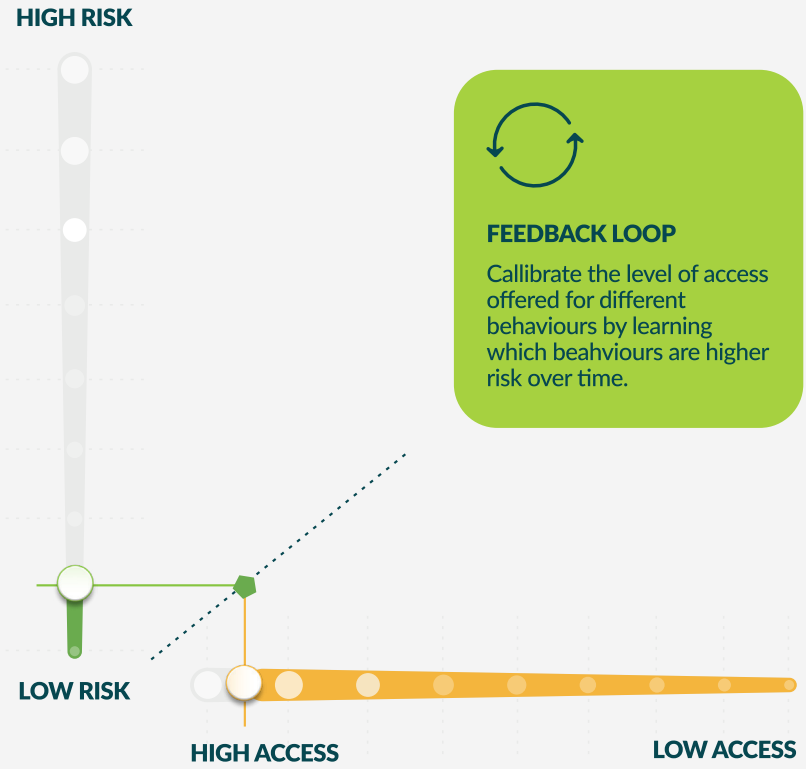
Release/air day



Piracy following theatrical-then-digital release strategy

- Venom (50 days to TVOD, 60 to DVD)
- Shing-Chi (70 days)
- F9 (70 days)
- No Time to Die (40 days)

SOURCE: DATA FROM MUSO.COM



Core content security

Providing a core level of content security with the aim of eliminating lower-risk piracy weak spots with minimum time and cost, while maximising user experience.

An example is hardening apps for smart TV, streaming sticks and mobile platforms, to detect when these are being used on rooted or insecure devices, or where the binary has been tampered with.

An appropriate response to the level of risk is made: for example maintaining users' access to the content but downgrading the video (to deter HDMI copying), or adding a visible watermark to warn a user that their device is insecure.

Content and platform owners can use feedback loops to fine-tune their approach to securing content. By learning over time which device types and behaviours present higher risk, they can restrict access to content only in these cases — avoiding negative impact on user experience for everyone else.

For example, this can take the form of detecting watermarked content, sourcing the leak, and then identifying common behaviours leading to that leak, such as device hacking/rooting, or unusual playback habits.

→ Start with 'High Access' and then restrict this in a highly-targeted way according to Risk.

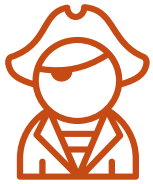
Return on investment

Cost vs. gain

Content owners and platforms have often been reluctant to invest more than the minimum in anti-piracy initiatives, creating a minor deterrent but doing little to fundamentally tip the balance away from pirates and back in favour of the legal business.

But making carefully-targeted interventions based on real consumer behaviours can start to convert some of the pirate viewing to new revenue streams. This transforms content security operations from a cost centre to a potential source of profit.

Targeting consumer behaviours



There will always be a (relatively small) group of consumers who are hardcore consumers of pirate content. These **freeloaders** are very unlikely to ever pay for content, so there is no risk of revenue loss by focusing on frustrating them to the max.

Identifying the sources of the content they consume and disrupting access is key.

Other less-savvy consumers don't always realise they are watching pirate services, or at least choose not to worry about it. These **chancers** may find illegal content via social media platforms, or they may buy a "fully loaded" streaming stick that seems identical to the real thing. They may find a free streaming site full of ads for familiar brands that's indistinguishable from a real AVOD service.

Here the opportunity is to detect the source of the illegal content and disrupt it, while helping consumers shift their spend to genuine providers, for example by displaying on-screen warnings in place of the pirate feed.

Other consumers are less-determined viewers of pirate products. Many users turn to illegal sources when they find they are unable to access the content in their market, on their device, or within their current pay TV and streaming subscriptions. Or they don't want to commit to a long-term subscription to watch one thing. These **seekers** are also more likely to use VPNs to access content from another market, or share passwords with friends and family. But many are willing to pay if they could get access in the way they want.

The opportunity for content and platform owners is to understand the market gap the pirates are filling, address it, and use anti-piracy interventions to nudge users towards the legitimate product.

Similar targeting can address the different types of pirates originating illegal content. The well-meaning superfan who shares episodes of their favourite new season requires a very different response to the criminal gangs providing wholesale "IPTV" services and illegal streaming sticks.

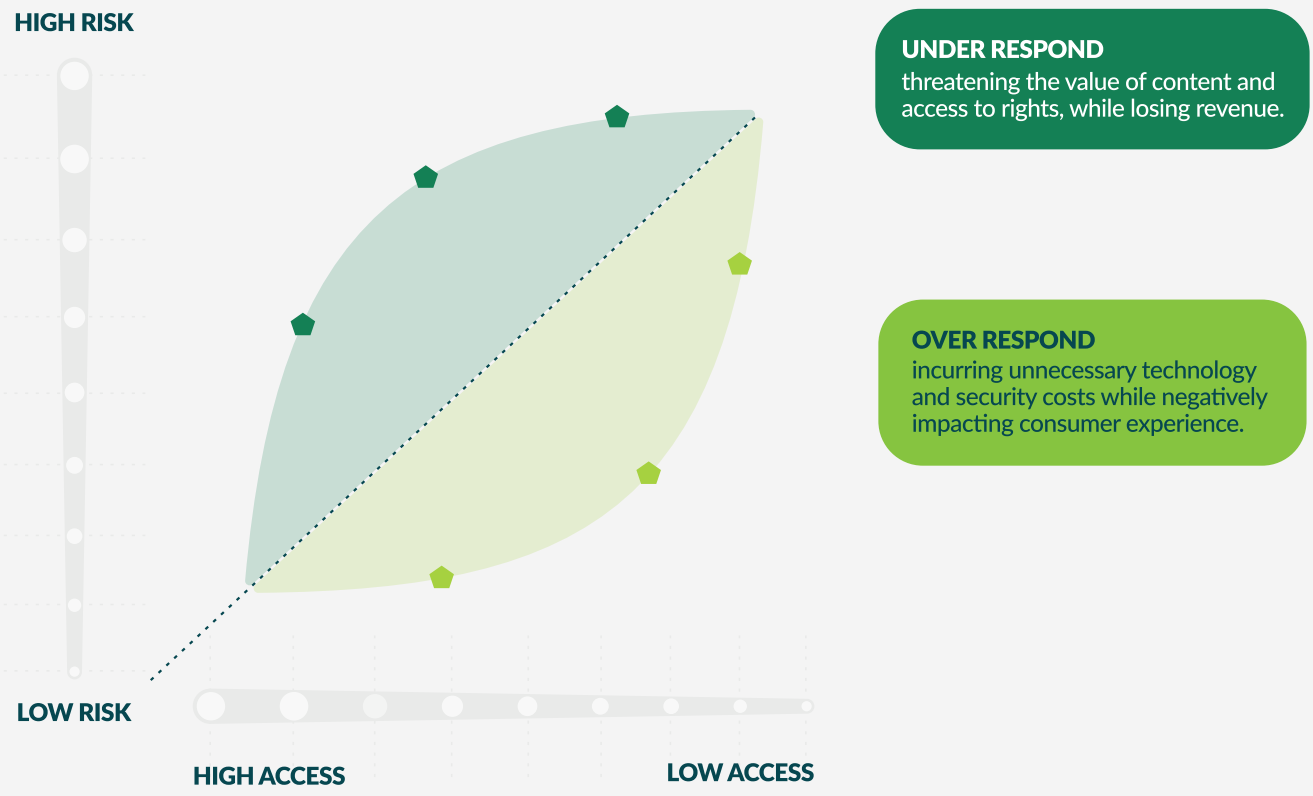
Tailoring the response to maximise ROI

Feedback loops mean content and platform owners can fine-tune their response to illegal content consumption by identifying what works best for:

- Different groups of consumers and their individual behaviour
- Types of content (e.g. live channels and sports vs. video-on-demand)
- Each platform and device
- Diverse markets and geographies

The response can then be kept balanced with the nature of the threat:

- **Avoiding over-responding to a lower-level risk** — incurring unnecessary technology and security costs while negatively impacting consumer experience.
- **Avoiding under-responding to a higher-level risk** — threatening the value of content and access to rights, while losing revenue.



Building the business case

A tailored response to content piracy ensures that investment in security technology is targeted where it will have the greatest impact. In turn, this can drive the ROI. Some of the key areas of benefit for platforms with better security are:

Better, cheaper content

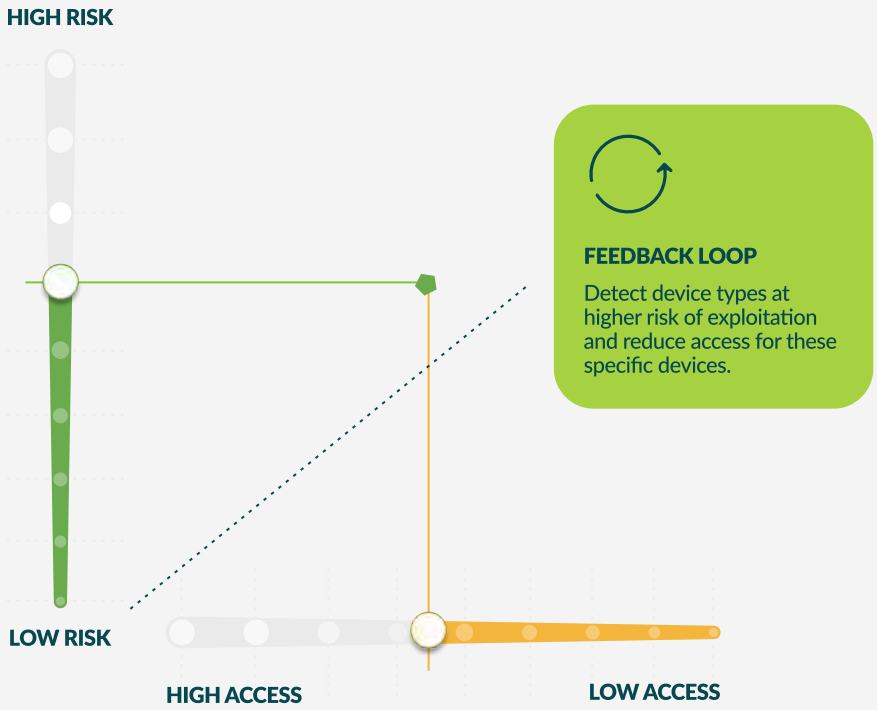
- Gaining access to a wider range of premium content and rights.
- Agreeing content deals on better terms, maintaining better relations with studios and sports rights holders.
- Sailing through studio security audits, reducing compliance costs.

Lower technical costs

- Avoiding inflated CDN costs from token-spoofing attacks.
- Reducing app development costs by using zero-code app hardening.
- Targeting more-costly technology such as watermarking precisely where it can help identify the source of piracy.

Better UX and revenue conversion

- Serving a bigger universe of devices (including those with weaker security) and hence a larger audience.
- Migrating viewers of illegal content to legitimate products.
- Avoiding unnecessary constraints on low-risk consumers and devices to enhance UX (e.g. enabling downloads for offline viewing).



Conversion strategies

Identifying opportunist and unintentional consumers of pirate content with a targeted intervention.

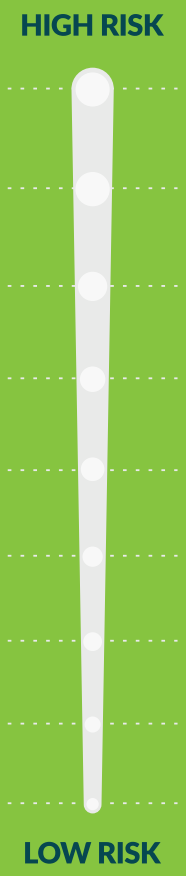
Interventions that maintains high levels of access to the content for the majority of consumers, but focuses on understanding and targeting consumer groups and devices most at risk.

The aim is not to "punish" these users but to provide a route to convert them to legitimate viewing.

Countermeasures

Fighting on multiple fronts

An effective approach to protecting apps and content needs multiple strategies, a layered approach which frustrates and degrades illegal content. There are many levers that content and platform owners can use — dialling up the response when the risk level demands:



- Analysing environmental sensors in a mobile device, such as ambient lighting and accelerometer, to detect if it's being used normally.
- Behavioural analysis of content playback to detect potential pirate-origination patterns (such as end-to-end playback without pause) from regular viewing.
- Reducing HDMI copying by using a server-side blocking list of suspect HDCP IDs, doing this in real-time at the server/headend, rather than trying to download the blocking list to the device (which is more problematic).
- Identifying CDN token spoofing.
- VPN detection
- Matching device location, cellular network and IP address for consistency
- Hardening apps and browser-based content including malicious browser extensions (lowest-hanging fruit). Smart TV apps are often vulnerable, especially those which don't require additional authentication, leading to URL cloning or exploitation of weak certificate stores.
- Detecting attempts to tamper with device or certificate store (e.g. rooted devices), or running on a virtual machine

Detecting suspect behaviours

Even with app hardening for mobile, smart TV and streaming stick apps, the HDMI connector on a device remains the weakest link. Analytics and monitoring can address this weak spot.

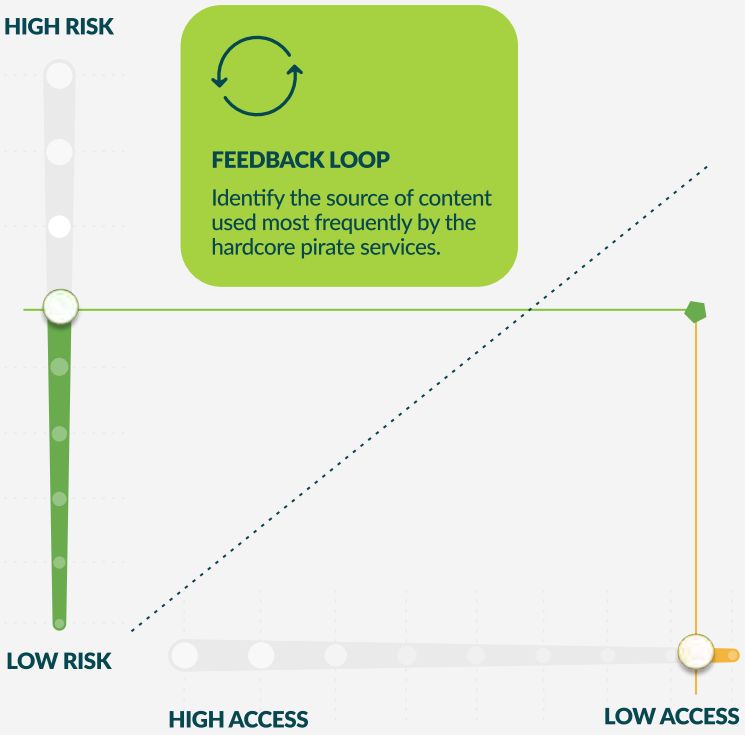
Many platform owners and super-aggregators are already adept in using analytics to manage quality of service and tracking user experience. Now analytics can be deployed to detect usage patterns that indicate potential pirate behaviour, allowing operators to target their anti-piracy interventions more effectively — delivering better results at lower cost.

This also solves a key challenge in using watermarking to identify and cut off the source of a pirate stream. Many operators have been reluctant to implement it because of the cost, technical complexity, and ability of some pirates to circumvent it. Analytics enables watermarking to be used far more effectively:

- **Monitoring device behaviour for likely piracy indicators, such as streaming content from first to last frame without pausing or skipping; or a device streaming the same TV channel or service for days on end.**
- **Applying watermarking — whether invisible forensic watermarks or visible on-screen markings — only to suspect devices.**
- **This more efficient process allows operators to target and interrupt the most likely sources of pirate content..**
- **While also making it much harder for pirates to defeat the watermarking as they can't see it till it's too late.**

Targeting the response

Data analysis allows content and platform operators to target a reduction in the level of content access for a given user. This might be to reduce the resolution, or lower the bitrate or framerate, or even insert a visual warning. Where more risk is detected, access to certain devices or content can be cut — and where justified, access to entire platforms or devices that are more likely to be linked to piracy behaviours.



Tackling the hardcore pirates

More active monitoring can be focused on the riskiest activities that drive the hardcore commercial pirates — in particular identifying the root source of pirate content.

For example, monitoring device and app usage can identify those that remain on the same channel for an extended period (acting as the source for an illegal IPTV feed), or those that routinely play new release content from the first frame to the last frame without interruption.

These are both examples of riskier behaviour, which can then the used to add a watermark to detect the precise source, or down-res an HDMI output — reducing access and deterring pirates.

Have you got piracy right?

Get in touch to evaluate risk factors and tailor your response

LEARN MORE AT VERIMATRIX.COM →

Caretta Research

About Caretta Research

Caretta Research is helping media technology buyers and suppliers make better technology decisions by using real information. We combine decades of experience in the industry with continuous hands-on research and an extensive network of technology buyers and decision-makers to help vendors understand and target their potential market, and to help buyers identify the most-suitable solutions—saving time, reducing risk and lowering costs.

To learn more visit www.carettaresearch.com

verimatrix
DRIVING TRUST

About Verimatrix

Verimatrix (Euronext Paris: VMX) creates security solutions for the most vulnerable and unprotected aspects of our digital world. Our enterprise threat defence and anti-piracy solutions secure content, apps, and devices with intuitive, people-centred and frictionless security across a diverse range of global industries from streaming media, broadcast and sports, to automotive, financial services and healthcare. Verimatrix enables the trusted connections our customers depend on to deliver safe, compelling experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

To learn more visit www.verimatrix.com

info@carettaresearch.com
+44 20 7112 8395
carettaresearch.com

Caretta Research