Watermarking

10 Questions to Ask Your Prospective Video Watermarking Vendor

So, you need to implement a video watermarking solution. How do you decide which solution and vendor are the right ones for you?

When choosing a content protection partner for video watermarking, finding the right solution for your needs is important. Many factors come into play, but here are key questions to ask potential vendors to ensure their watermarking solution:

- is viewer-friendly and pirate-unfriendly
- provides a universal, cost-efficient approach
- and actually works!

Question 1

Is the watermark imperceptible to the viewer?

Video watermarking must be virtually imperceptible to the viewer. Security is highly important, but it cannot compromise the viewer experience. A good watermarking solution is virtually imperceptible, which not only doesn't impact viewer experience, but also makes it harder for a pirate to discover and circumvent.

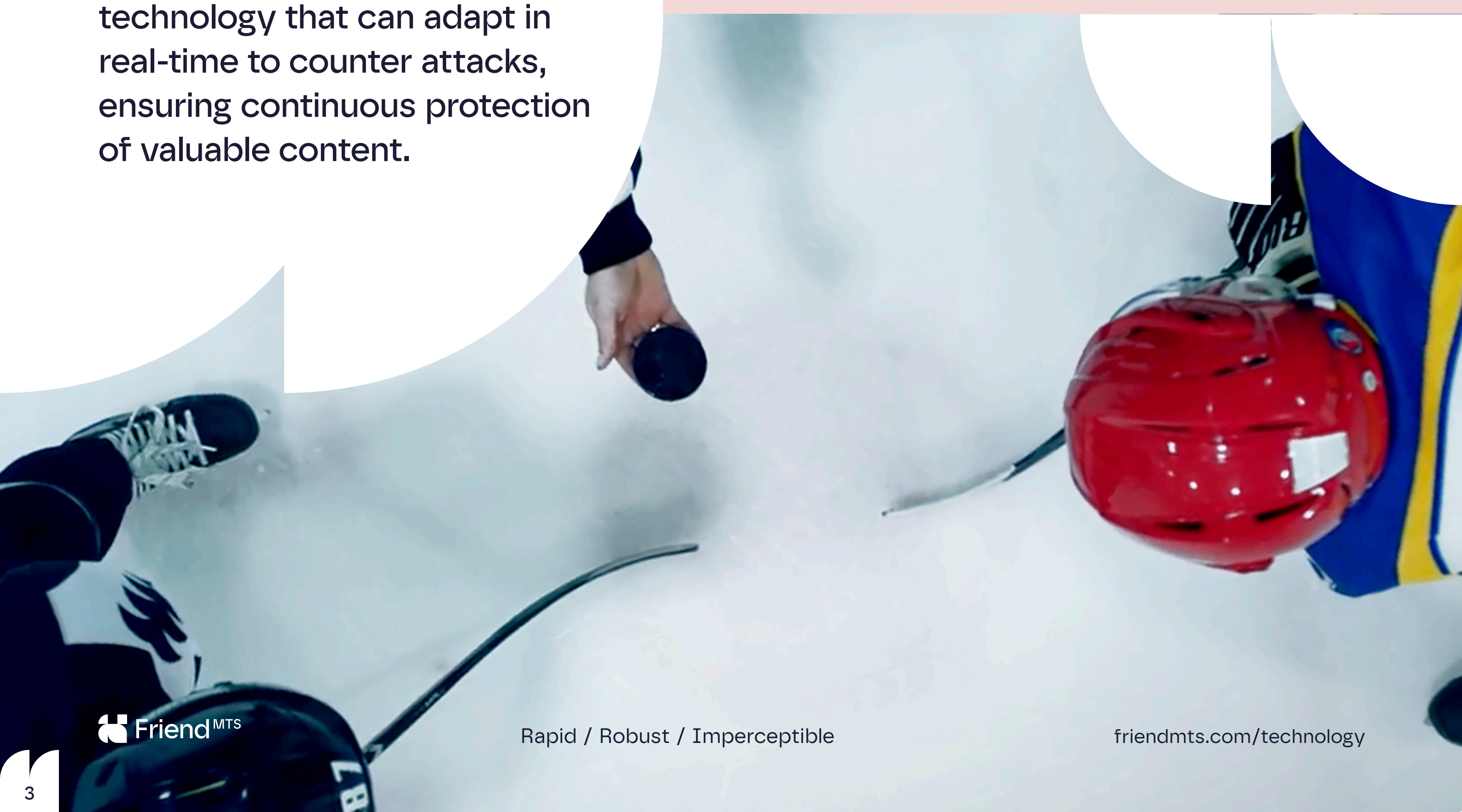
With live sports being a prime target for piracy, it is crucial to deploy watermarking technology that can adapt in real-time to counter attacks, ensuring continuous protection of valuable content.

Question 2

Is the watermark robust against real-world pirate attacks?

In an era of AI-powered video manipulation, pirate attacks are increasingly technically sophisticated, with professional pirates motivated by high-margin income from selling stolen content. Pirates constantly invest in new techniques to circumvent security, and live sports are the most lucrative targets. Deploying a watermarking technology resilient to various manipulations (including with the use of AI) that adapts in response to attacks in real-time is crucial for protecting this content. Therefore, the watermarking solution must be offered as a managed and supported service rather than an off-the-shelf product or set of tools.

A data-driven AI-assisted approach is crucial for a watermarking vendor. Collecting and analysing vast datasets while monitoring content globally at scale enables the vendor to generate valuable intelligence. This insight allows for accurate predictions of pirate countermeasures and the development of proactive solutions that stay ahead of emerging threats.



Question 3

Is the watermark always embedded during playback for all content types?

If the watermark is displayed throughout the duration of the protected content playback, be it a live linear channel or VoD asset, then any capture of pirated content from that source should include the watermark and therefore deliver a result.

Conversely, if the watermark is only displayed intermittently during playback, the capture process will become more complex, as the content monitoring system will need to align video capture with the display time of the watermarking. Accordingly, the number of failed captures will inevitably be higher, and the extraction/identification process may require frequent manual intervention, resulting in higher costs.

Question 4

Can the watermark be extracted from a short pirate video capture?

This question is especially important to ask when you are considering protecting live content. Some watermarking solutions, notably those that use A/B variant sequencing to create a unique temporal pattern to identify the infringing subscriber, can require video captures of longer duration for successful extraction. This renders them less effective for the protection of live content – remedial action, such as service suspension, usually has to happen in real-time – it's of little benefit after the event is over!

In addition, the need for extended video captures can reduce the reliability of the capture process, and larger video files will always mean higher storage costs. Finally, solutions that support watermark extraction from just a few minutes (or even seconds) of captured pirate video will be equally proficient at protecting both live and on-demand video.

Question 5

Is the watermark deployable on all devices, including legacy STBs and OTT apps?

For broadcasters and service operators distributing content across multiple channels, it's essential to ensure robust protection for valuable exclusive content across all client devices and platforms. Protecting an exclusive movie on OTT platforms offers limited value if pirates can still easily capture or restream it from an older broadcast device without fear of detection. Pirates will always identify the easiest way to steal content and exploit those distribution channels and devices. A universal watermarking solution deployable on all key devices will cover all the bases.

Question 6

Can the watermark protect broadcaster content across multiple distribution operators?

Broadcasters need to be able to work closely with their various distribution partners to avoid premium content being leaked to pirate networks. A single leaking source compromises the entire distribution ecosystem, eliminating the content's exclusivity. A universal watermarking solution should allow the same technology to be deployed across a number of distribution partners/ operator platforms with a joined-up approach to content monitoring, watermark extraction, and subsequent notification of successful extraction. Adding a subscriber-level watermark in addition to the distribution one yields the ultimate protection for all content.

> Pirates will always identify the easiest way to steal content and exploit distribution channels and devices. A universal watermarking solution deployable on all key device categories will cover all the bases. And using the same watermarking technology on subscriber level ensures ultimate protection for your valuable content.

Question 7

Is the watermarking solution compatible with any monitoring provider?

Service providers often work with anti-piracy companies to monitor and detect piracy. A watermarking solution should seamlessly integrate with these partners, allowing them to submit captured pirate content or links for extraction.

Question 8

Has the watermarking solution actually been deployed?

This is the critical question that must be addressed. A watermarking solution confined to a lab environment—or worse, merely a concept in a slide deck—lacks the proven real-world performance and resilience required for effective content protection. Only a field-proven solution, deployed at scale across significant subscriber populations, can ensure reliability against piracy threats. Verify that the watermarking vendor has successfully implemented their solution in environments similar to yours and can substantiate their claims with reference deployments.

Question 9

Can the watermarking support large-scale deployments?

Many watermarking solutions simply do not scale, so it is important that the vendor can offer evidence of large-scale deployments. Note that the requirements for subscriber-level watermarking are very different from those for distributor-level (network-level) or pre-production watermarking, where only a limited number of streams or playback sessions are watermarked. When a watermarking vendor discusses their existing deployments, ask the simple question: "How many concurrent client devices/apps can the system support?"

Question 10

Does the watermarking solution deliver real results?

The goal of watermarking is to identify and shut down piracy at its source. Whether tracing illegal redistribution to individual subscriber accounts or pinpointing security gaps in distribution networks, a solution must go beyond mere compliance to provide actionable intelligence.

A watermark without robust monitoring and extraction is merely a checkbox feature—it does little to combat piracy effectively or add lasting value.

> The requirements for subscriber-level watermarking are very different to those for distributor-level (network-level) or pre-production watermarking where only a limited number of streams or playback sessions are watermarked.

Bonus question 11

Are you comparing like for like?

Watermarking is just one component of a broader content security strategy, and some vendors bundle it with additional components. When evaluating pricing, ensure you're making a fair comparison. Consider what's included and whether vendors are transparent about any discounts.

Pricing should also reflect real-world usage. The true cost driver in watermarking is extraction, and the required volume varies by content type. Pre-release movies may need only a few extractions, while live sports could demand millions per month. Make sure your vendor's quote aligns with your actual extraction needs.

Summary

The effectiveness of content protection through watermarking depends on the ability to detect stolen content, extract watermarks, and take decisive action against infringing subscribers. When evaluating watermarking solutions, broadcasters and service providers must ensure they choose comprehensive, end-to-end systems that are proven at scale in real-world deployments and capable of delivering tangible business benefits.

We stop piracy.

Nobody does it better

Transforming content security from cost centre to revenue source.

Friend MTS is the world leader in content security and anti-piracy. Our solutions are deployed in tens of millions of devices and apps, and we protect content whose collected media rights value is well in excess of $60 billion. We provide the world's biggest brands with the best anti-piracy services and solutions available, including monitoring & enforcement, watermarking, business intelligence and server blocking.

Our partners trust us to help them detect, deter and disable piracy, using gamechanging tools that enable engagement with potential customers, converting pirate audiences into legitimate subscribers, thereby increasing revenue.

Our solutions are unrivalled. But don't take our word for it. FMTS works with the largest brands in media and entertainment to safeguard their content. Delve into our latest case studies to learn more at friendmts.com/case-studies.

Contact us today to discover more.