Friend MTS

12

Questions to Ask Your Prospective Monitoring & Enforcement Vendor

Choosing a content security solution to best protect your revenue

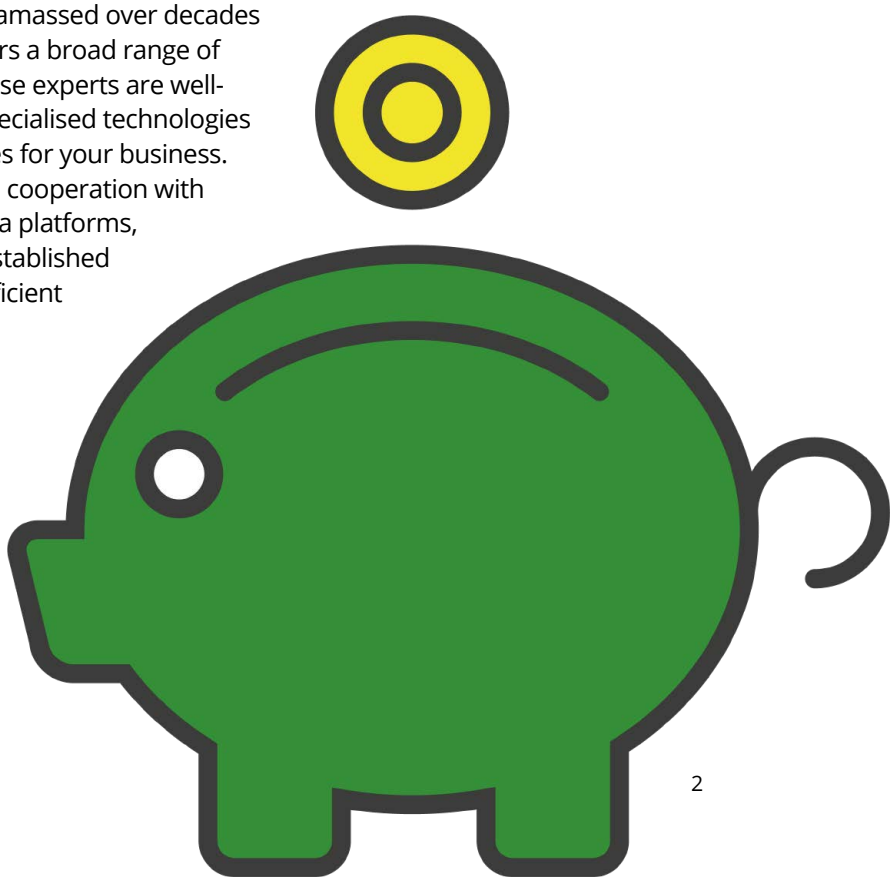
So you need to implement a content fraud detection and takedown solution. But how do you decide which solution, and which vendor, are the right ones for you? You need to thoroughly investigate which content monitoring and enforcement services are most suitable for your content protection needs. Of course, there are a large number of factors to examine and you might have dozens of questions, but here is the dozen that you should definitely ask to help determine whether your prospective vendors' monitoring and takedown services are the right ones for you.

Question 1.

Does your vendor have a monitoring solution proven to disrupt revenue-damaging content fraud?

For content monitoring and enforcement to be effective in preserving your revenue, it needs to provide comprehensive detection and effective disruption of revenue-damaging piracy. It's important to check with your prospective vendor whether they have existing examples of successful operations with other customers that have similar platforms and challenges, and what piracy sources they cover. Though important, it's not enough to simply clean search results or have fraudulent content sites removed from search engines.

A monitoring trial can help you understand what you are dealing with: where your content is available illegally and what is required to take those instances of piracy down. Content protection and anti-piracy experts conduct ongoing monitoring of the industry's most high-value live and on-demand content. Based on the intelligence amassed over decades of protecting content, such monitoring covers a broad range of piracy sources and fraudulent activities. These experts are well-equipped with expertise, experience and specialised technologies to illustrate the scope of content fraud issues for your business. Effective piracy disruption is only possible in cooperation with internet service providers (ISPs), social media platforms, law enforcement, etc., i.e. a wide and well established network of partners that ensure fast and efficient disruption of illegal activities.



Once you have ensured that your vendor is an established content protection expert and a trusted member of a wide network of organisations in the content security ecosystem, it's time to ask the 'deeper dive' questions that will help you understand whether this vendor's solutions suit your revenue protection needs.

Question 2.

Does your vendor have truly global coverage?

Content fraud is an offence that has no borders. Modern distribution allows pirates to spread stolen content in high quality far and wide, beyond any geographical restrictions imposed by content licensing agreements. Hence, a content monitoring service needs to cover multiple territories across the globe. If your valuable live sports content is leaked by your distribution partner or a subscriber located in, say, Latin America, the same content is sure to appear in other territories very quickly: viewers of fraudulent content often don't mind commentary in a different language if it means cheaper access to sports.

A content fraud detection and takedown service needs to be geared appropriately to have that global reach. Without revealing any sensitive security information and going into operational details, it's sufficient to say that appropriate highly scalable technology, business processes and staff need to be in place to enable global detection operations and response 24x7x365.

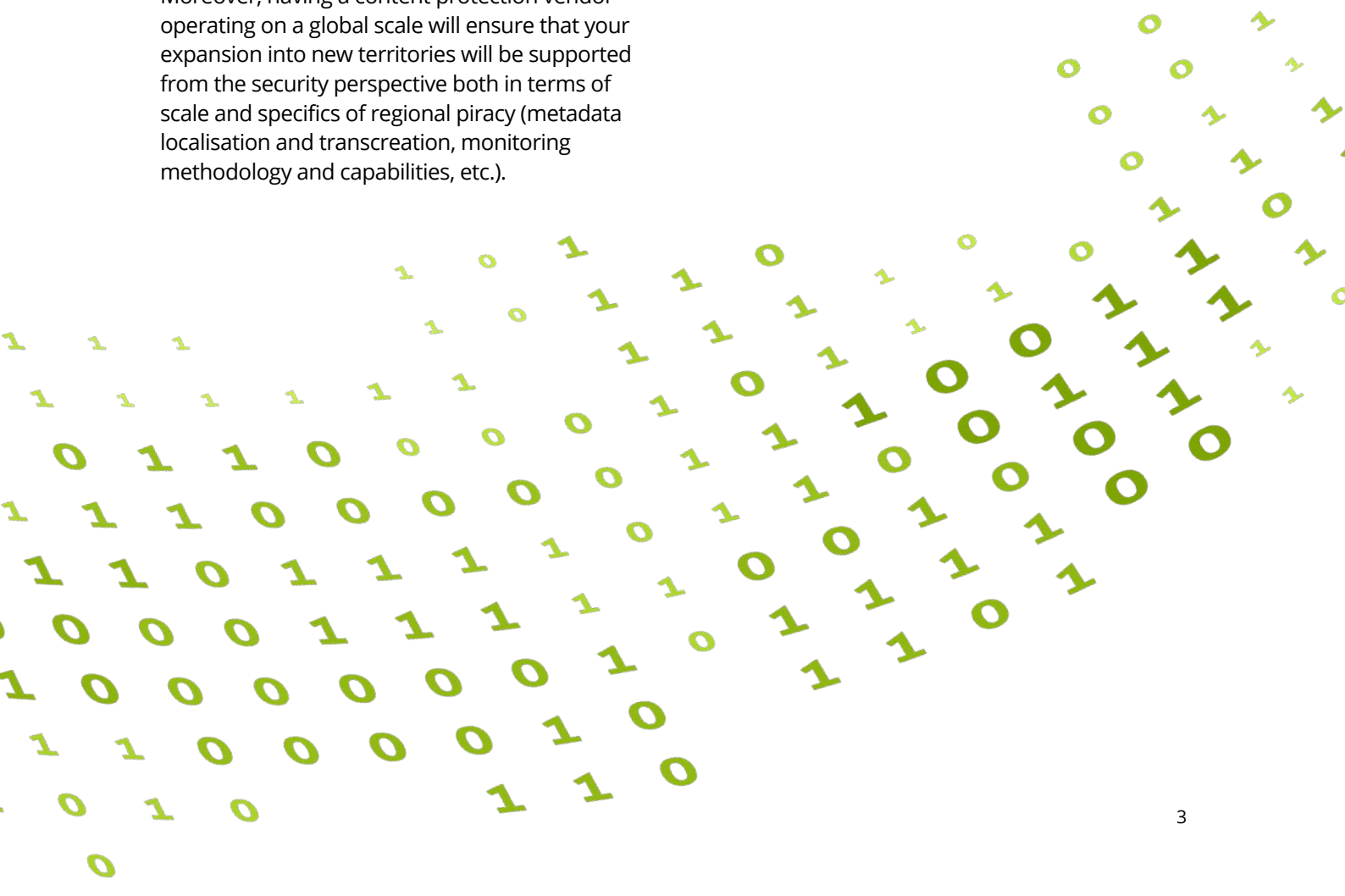
Moreover, having a content protection vendor operating on a global scale will ensure that your expansion into new territories will be supported from the security perspective both in terms of scale and specifics of regional piracy (metadata localisation and transcreation, monitoring methodology and capabilities, etc.).

Question 3.

Is your vendor's solution effective against pirates' changing tactics?

Pirates are extremely inventive in their security circumvention attempts: they don't have to pay for the expensive content they profit from, so can easily channel part of their illegal revenue towards their "R&D", circumventing protective technology to ensure they maintain access to the content they sell. In turn, legitimate service providers need to ensure that their content protection and anti-piracy solutions are robust against vulnerabilities.

Make sure that your vendor has the depth of knowledge and technology that accurately captures, maps and analyses the constant evolution of tools and methods employed by pirates, not only to capture content, but to circumvent the technology that protects against this. How rich is your vendor's knowledge of the piracy landscape? Which tools do they have in their toolkit, and how much experience do they have of real-world content fraud?



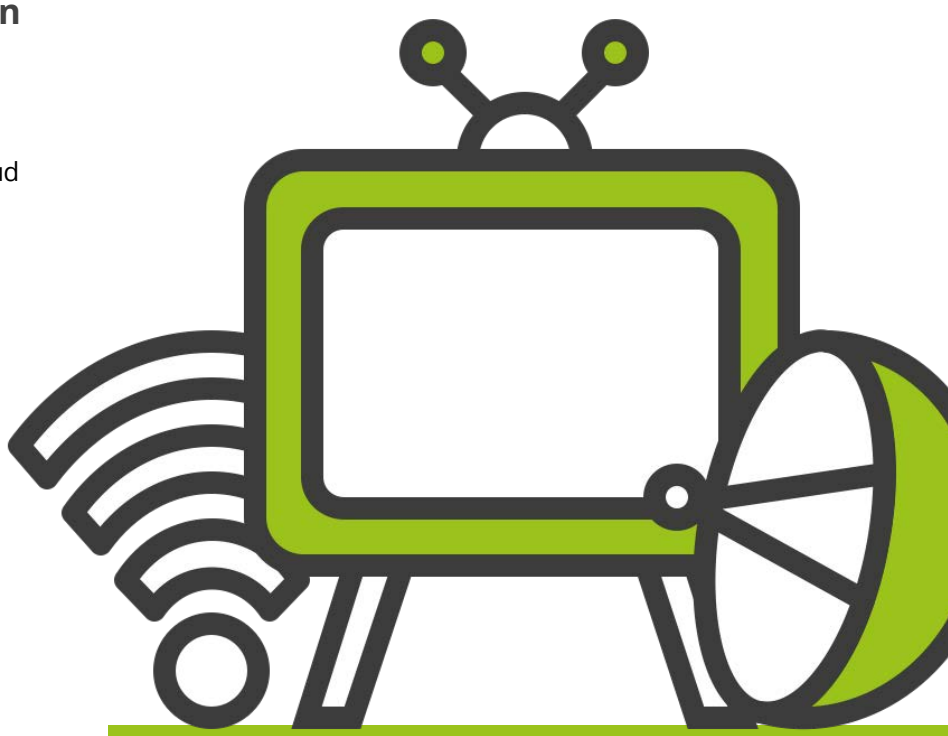
Question 4.

How accurate is your vendor's monitoring and enforcement solution when operating at large scale?

While it's important to make sure valuable content is protected from fraud and illegal redistribution, legitimate content owners and service providers hiring an anti-piracy company need to ensure they won't be incurring erroneous takedowns, especially when dealing with large volumes of content. Errors can result in your content being removed from legitimate channels, or the removal of other legitimate content; this can create negative publicity and an undesirable impact on your relationship with distribution partners.

Understanding the processes and technologies an anti-piracy company uses is key. Learning how content is detected, whether there is a reliable and robust content verification process in place, what this process entails and what technologies are used, and the effectiveness of the remedial mechanisms – these are all important points to consider. These points all need to be vetted through the lens of scale: it's much easier to achieve accuracy with small numbers while large-scale operations present a much higher level of complexity.

A highly-scalable model that combines fingerprinting and other verification technologies for automated content identification, backed up by human oversight for cases that require deeper examination, is extremely efficient at identifying false positives and preventing takedown errors while 24x7 remedial mechanisms ensure a high level of responsiveness.



Question 5.

Does your vendor cover all impactful sources of content fraud or just open web?

Financially damaging content fraud comes in all shapes and sizes. While illegal restreaming on open web is often mentioned, revenue is lost to other types of piracy too. The catalogue of possible threats includes content fraud across social media, mobile apps, streaming devices, paywalled pirate IPTV services, various add-ons, plugins etc., in addition to open and ad-driven pirate streaming sites. Understanding the types of threat that have the greatest impact on your business is key. If your business is suffering revenue losses due to your content being redistributed illegally across multiple channels, make sure that your security vendor provides references of having detected and taken down piracy across all of them.

Question 6:

Is your vendor an established partner with the major social media platforms?

For several years now social media misuse has been one of the major concerns of content owners and rights holders. There are a few factors that contribute to the complexity and scale of the problem but the main ones are the popularity of these platforms and the simplicity of sharing video content. While the quality of the content shared on many social media platforms is usually low, it still poses a threat to content owners – if it's the right content, illegal viewers will often be happy to take a resolution hit. The issue is further exacerbated by the existence of non-compliant platforms, those that are not as stringent in their tracking and enforcement against illegal content.

The biggest and most popular social media platforms would certainly have the most impact on the value of your content should it be shared on these platforms in an unauthorised manner. Many of these platforms have their own rights management solutions (e.g. Facebook's Right Manager, YouTube's Content ID, etc.) so it's worth checking that your vendor operates a compliance programme with social media platforms to ensure that takedowns are swift. It's also worth checking if your vendor has developed relationships and established enforcement processes with popular regional social media platforms.

Question 7.

Can your vendor protect content of very short duration?

As the popularity of social media platforms continues to grow, content of shorter duration is highly attractive. From comedy to sports highlights, this content is highly engaging and easy to share. Some licensing agreements stipulate very strict rules and even such short duration content can only be shared by authorised sources.

However, not all content monitoring solutions are capable of monitoring for content of short duration: some content verification technologies might not be as good at matching content if it's just a few seconds long so for these vendors it's just not feasible to include such content into the list of the content they protect. If you are looking to protect short content, you'll need to check your vendor has the right technology to support you.

Question 8.

Does your vendor collect and maintain evidence to support possible litigation?

Some security vendors can help with legislative enforcement, for example as part of blocking services that involve blocking access to IPs by ISPs – something that requires a judge to issue a pertinent injunction.

However, even in territories that are yet to make legal advances in terms of blocking orders, a content protection vendor is still required to supply admissible evidence when they face non-compliance. A traceable trail of issued and ignored legal notices, as well as other evidence, is crucial for content owners and service providers to build their case in court, and to win against fraudsters who damage their bottom line.

Cumulative data is crucial for building your case, so it's important to check your vendor's data retention policy including how long the data is stored, how it's stored, the chain of custody protocol, etc. and how these processes and procedures align with the evidence handling protocols set out by law enforcement organisations in various territories.

Question 9.

Can your vendor secure the largest and most popular live events?

The complexity of setting up coverage and distribution of a very popular global live event such as a sporting competition, a music or film festival, a global premier, etc. is staggering. Platforms have to be able to handle huge spikes in demand, and quality of experience is paramount. Any security technology deployed to protect this content needs to work well in harmony with other deployed solutions and be just as rapidly scalable.

In order for a monitoring service to be effective in protecting live content at scale, it needs to be highly automated. A content monitoring platform can automatically capture thousands of suspect streams simultaneously, i.e terabytes of data. Fingerprinting technology can be used to automatically analyse great quantities of captured streams to swiftly and accurately pinpoint illegally those that are illegal redistributions.

One of the advantages of fingerprinting is that this technology is extremely lightweight – just a few kilobytes representing a few gigabytes of video. Even this small sample size allows the technology to accurately identify a video: hence the term fingerprinting – just like in forensic police work, the probability of fingerprints of two different videos being the same is low enough to be negligible.

Augmented by the lightweight fingerprinting technology, highly automated video search and capture monitoring can secure even the largest live sporting competitions and entertainment events.

Question 10.

Does your vendor disrupt illegal operations in real time?

Sports content, especially live events, are extremely popular and valuable. Content owners, broadcasters and OTT service providers all want to ensure this content is safe and any fraudulent activity that involves diverting revenue from legitimate rights holders is stopped while the content is still worth what they asked for or paid for it in terms of licence fees.

As the value of live content quickly diminishes, the success of any fraud counteraction is measured in minutes if not seconds for such time sensitive content. Enforcement needs to be a part of highly automated monitoring that includes video capture and verification. Following confirmation of piracy incidents, tens of thousands of takedown notices need to be sent automatically every day. These are notices sent to both infringing domains and hosting providers (escalation notices). Other bespoke enforcement processes need to be in place and actioned on a regular basis to ensure responsiveness and compliance of infrastructure providers for the removal of infringing content in real time.

It's worth checking if your vendor has established relationships with these organisations for smooth real time enforcement. It's also good to check if your vendor offers blocking services (during the event as well as pre-blocking) as these are highly effective in ensuring infringing content is not available while the event is on.

Question 11.

Does your vendor's solution work seamlessly with other technologies to deliver end-to-end protection?

Businesses that allocate big budgets to content creation and distribution are constantly vying with other media and entertainment players for eyeballs, and therefore their content protection strategy requires a multifaceted approach, often involving their legal, engineering and other departments. In terms of security technologies that are needed to ensure full end-to-end protection across the value chain, content protection and anti-piracy can become quite a complex undertaking.

It is important therefore that each technology component needs to work seamlessly with the rest of the stack. For broadcasters and pay-TV service providers, some of whom have legacy systems to maintain and protect, there is nothing worse than a technology that makes matters even more complex than they already are. The independent security technology and service providers that are the best at what they do have a laser focus on their solutions, and their partner network of the best experts in the respective fields provides an opportunity for you to pick and choose the security components you actually need, rather than taking a whole bundle you might not.

Question 12.

How does your vendor's solution provide measurable and immediate impact on the overall piracy landscape?

In addition to the tactical wins that content monitoring definitely brings, it is important to assess how the implementation of piracy detection and enforcement services and solutions impacts the bigger picture: does it actually have a tangible impact on the availability of illegal streams of the given rights holder? And, importantly, has there been any significant impact following the enforcement actions?

Comprehensive piracy detection followed up by extensive enforcement in cooperation with other industry players (including payment, hosting and other infrastructure providers) can bring substantial changes to the piracy landscape – almost immediately in the case of live sports. Pirates move fast to get live content that they want to profit from and when enforcement actions make one source more difficult to access they will turn to the lowest-hanging fruit, away from the well-protected sources.

Now having asked your prospective content monitoring vendor all of these questions, there is one thing to ask yourself. Is your content low-hanging fruit for fraudsters, or is your protection top-notch, making your content very difficult to steal?

Bonus question:

Are you making an "apples to apples" comparison?

As we discussed in our series of questions on content watermarking, piracy detection and takedown are components of a comprehensive ontent security system, and some vendors offer multiple components alongside them. So it's important to understand if you are comparing like for like when considering pricing.

You should make sure that measurement is aligned across vendors. High percentages require a closer look at the actual numbers behind them - 95% of 20 cases isn't actually as impressive as 80% of 20,000 cases. Likewise, you should always check definitions in use: one company's "incident" is another company's "unique stream", or another company's "linking stream".

For instance, is "an incident" an actual video playback source? Or is it a simple text page linking to the source (which is then also classed (and counted!) as an incident)? Obviously, taking down more of the former has a bigger positive impact on your bottom line than the latter, where you might find yourself just chopping off hydra's heads.

Summary

Highly scalable, automated monitoring for fraudulent content, and swift, effective enforcement tools to address the results, sit at the heart of your content security strategy. This helps you protect your valuable content, and to actively generate revenue from diverted audiences. But this level of service requires a field-proven, expert partner with a longstanding background in content security, who has the knowledge, expertise and technology to understand how piracy works, how to disrupt it and turn content security into a revenue generating centre.

Make sure to ask your prospective provider(s) the questions in this guide, and if they can answer positively to all of them, together you'll be able to make a measurable impact on the piracy landscape and, more importantly, your business.