MYTH #3

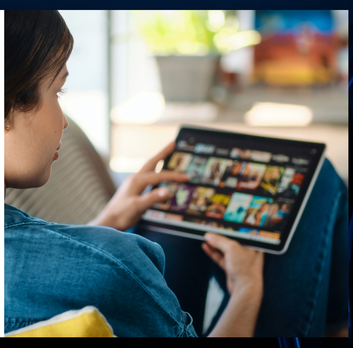
DRM is vulnerable and there's nothing I can do about it

The Myth

Since their introduction some four decades ago, digital rights management (DRM) technologies have been the go-to solutions for protecting copyrighted works.

While DRM remains relevant, OTT services have introduced a new level of complexity when it comes to delivering and protecting media.

Here are several examples of technological developments impacting both you and pirates, and what you can do in response.



The Truth

The rise of unmanaged devices increases vulnerability

Thanks to OTT video streaming, your users can access content anytime, anywhere and on any device. But there's a trade-off. Today, many of your users' devices, such as smartphones, browsers and smart TVs, are vulnerable 'unmanaged' device platforms that are susceptible to exploitation.

Vulnerability exploits are automated and traded among pirates

In today's piracy marketplace you do not have to be sophisticated or tech savvy to establish a piracy service. You can buy anything from specific technology hacks, through DRM decryption services, all the way to a cloud-based, managed piracy-as-a-service. That is why piracy is thriving; a market demand for more content at a lower price, combined with high efficiency in illicitly obtaining and delivering the content.

Common DRM breaches enable pirates to restream your content

Some DRM systems are more commonly targeted than others, equipping pirates with a supply of tools. By exploiting these vulnerabilities, pirates can impersonate legitimate applications, obtaining seemingly legitimate direct access to your service, while stripping away the DRM protections to restream content in the clear. Pirates no longer need to re-encode a raw HDMI output in order to deliver a high-quality, low latency service with a full selection of audio and subtitle tracks.

OTT service theft makes the piracy supply chain very efficient

In the piracy supply chain, some pirates help other pirates obtain quick and easy access to your content, directly from your CDN, through service vulnerability exploits. In this form of service theft, numerous clients access your CDN using a single account, circumventing any concurrency limitations, to obtain the required DRM licenses and CDN access tokens. These streams then go to different piracy services, while **you** incur the related CDN costs of servicing them.

The Response

What can you do to go beyond DRM and protect against service vulnerabilities?

Pirates are masters at exploiting any vulnerability that comes their way. That's no myth.

A dire situation? Far from it... that is, as long as you turn to an expert with domain knowhow. One who understands the ins and outs of the protocols used by OTT services and is familiar with cyber solutions so they can offer countermeasures, as shown in the table below.

Service Vulnerability*	What You Can Do
Pirates impersonate legitimate applications through hacked/jailbroken devices to gain service access and strip away DRM protections.	Verify application authenticity and apply measures to immediately recognize when the client device has been tampered with. Restrict the service to the client based on internal policies.
Pirates duplicate CDN access tokens to gain direct access to, and stream content from, the CDN.	Enable the CDN to validate that any request is only made from an authorized client and could not have been duplicated.
Pirates duplicate service authorization tokens to gain access to content and/or a DRM licence.	Ensure that content is delivered only to strongly identified authorized devices to prevent pirates from impersonating legitimate clients.
Pirates trick the concurrency mechanism of an account, enabling simultaneous viewing of an unlimited number of streams.	Secure your heartbeat mechanism - used for concurrency - so that it cannot be forged or manipulated.
Pirates can steal content directly from the CDN when the DRM encryption keys to the content are already known.	After ensuring your service is difficult to breach, make sure you rotate keys frequently.

*Our research shows that among over a dozen OTT streaming applications belonging to direct-to-consumer services, 100% of them are vulnerable to piracy attacks.

While a DRM is not enough in today's OTT-driven environment, a solution that protects both your content and service will help you prevent this attack vector.

Synamedia