MUVI

SECURING
MEDIA CONTENT

www.muvi.com

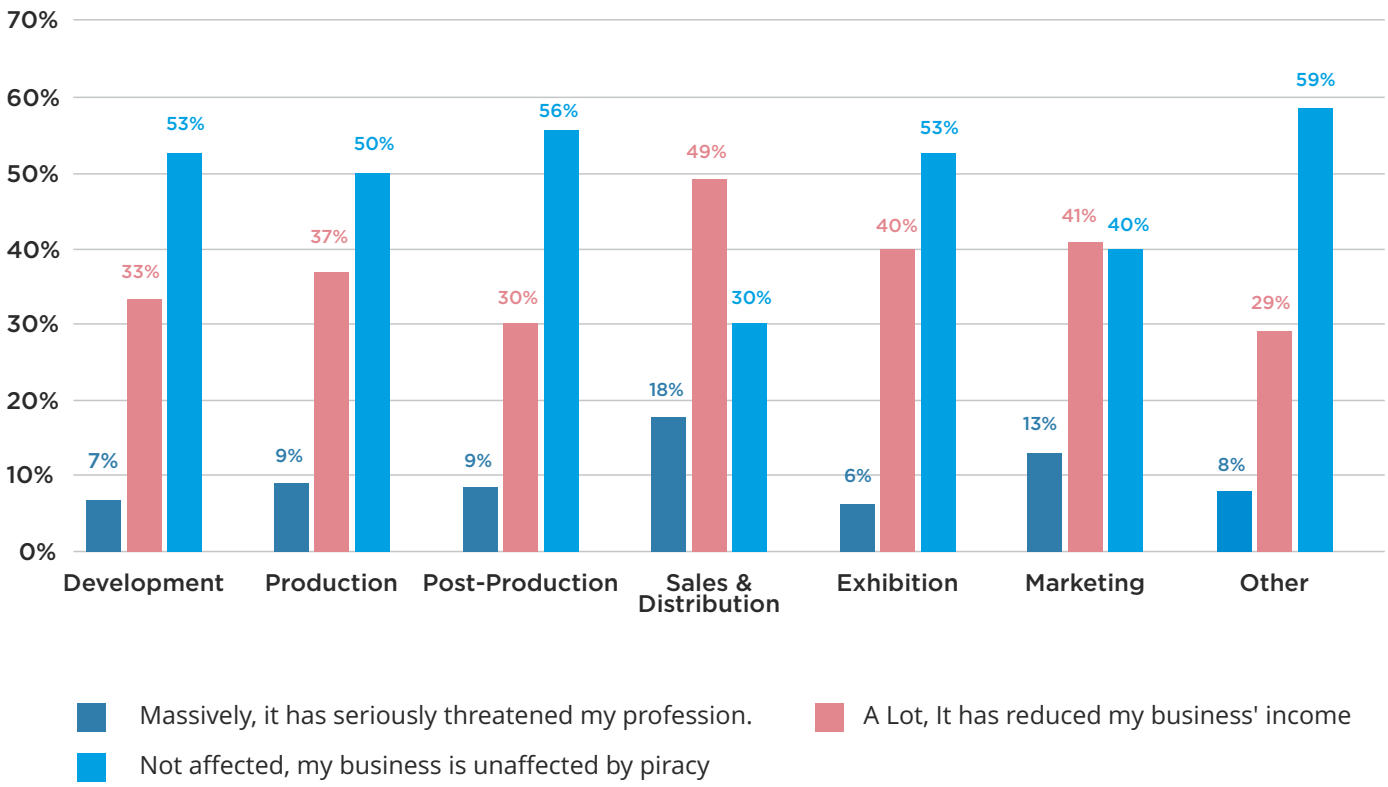
Introduction

Now, viewers are looking for fast, secure online media viewing experience irrespective of their devices and location. In this environment, protecting online media content is a multifaceted challenge. This whitepaper inspects content security problems in the digital media industries. It emphases on content piracy and Digital Rights Management (DRM) challenges companies are dealing with and the effective methods to cope with the problem.

Each year brings latest set of devices with more portability, higher resolution displays, more computing power and more bandwidth. To keep up with this demand, service providers and network operators including Internet-based over-the-top (OTT) services, terrestrial broadcasters, IPTV as well as traditional cable and satellite are competing with each other. However, in this digital media revolution, one major concern is the security of media content.

Meanwhile, proprietors of premium digital video content, including sports leagues, cable networks, major Hollywood studios and others, are working on licensing their content for distribution under an increasing range of business models. A key element of these business models is the requirement of protecting the video distribution network from unauthorized distribution and consumption.

How has film piracy affected your business? (1)



Protection of digital content is essential as most of the digital media industries today are losing their revenue because of unauthorized file sharing and content piracy. Lack of process control and advanced technologies are fast-tracking illegal file sharing and piracy. Hackers are now using various sophisticated ways to access online content. These may include, web content tampering, stealing from the cache, stream ripping, player hijacking, deep linking, link sharing and many more...

Different methods can be implemented from server level to application level to secure the media content. This includes securing content at server, securing content at application level like website and mobile / TV apps, the content itself (DRM and stream protection) and preventing misuse.

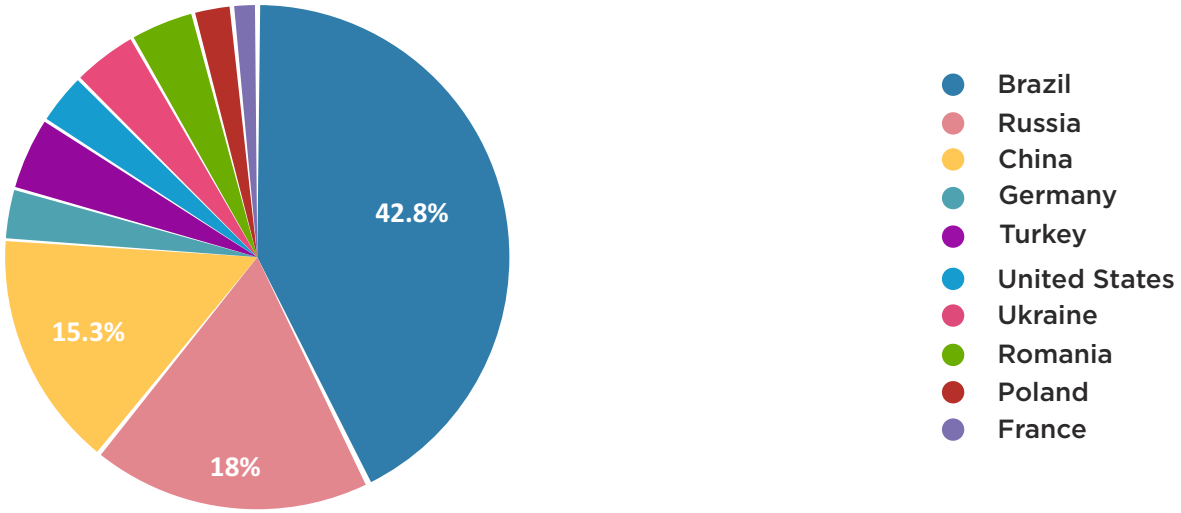
Stats on online piracy

Nowadays, one of the most critical problems encountered by digital media industry is the loss of revenue due to unauthorized file sharing over the internet and content piracy. It has become more of a problem in the past decade than it ever has before, specifically video piracy. Today, mainly 4 factors are driving video piracy. These include the rising costs of premium content, the increasing availability of high bandwidth, easy online distribution and the rise of OTT.

Production companies invest huge amount of money on creative development and promotion. However, due to piracy they are unable to get the return on investment. Because of this many production companies are planning to redefine their businesses which raise a serious question about the future of media and entertainment industry.

There are certain regions in the world where losses due to piracy are considered to be the greatest; for example, in Russia and China. In the year 2004, the piracy revenue for these two countries was accounted for around $5 billion.[2] Only in China, the piracy market of movies and music is estimated to be more than 95 percent. There are few countries like Thailand and Afghanistan where the marketplace penetration of piracy is almost 100 percent.

Stats on online piracy



According to the White House estimate, back in 2012, the U.S. film industry alone suffered a loss of $58 billion due to piracy. (3)

In 2015, an Arxan study estimated over one million pieces of premium video content being made available on pirate sites, and cautioned that video piracy was a rising issue. (4)

As stated by the Wall Street Journal, the cost of video piracy is as much as $19 billion, is lost in sales each year. You are probably losing sales because of this piracy if you are in the business of selling video content.(5)

For acquiring and distributing unauthorized content, most pirates around the world rely on the Internet. With the emergence of the Internet as a medium for uncontrolled and free global interactivity, widespread piracy began concurrently.

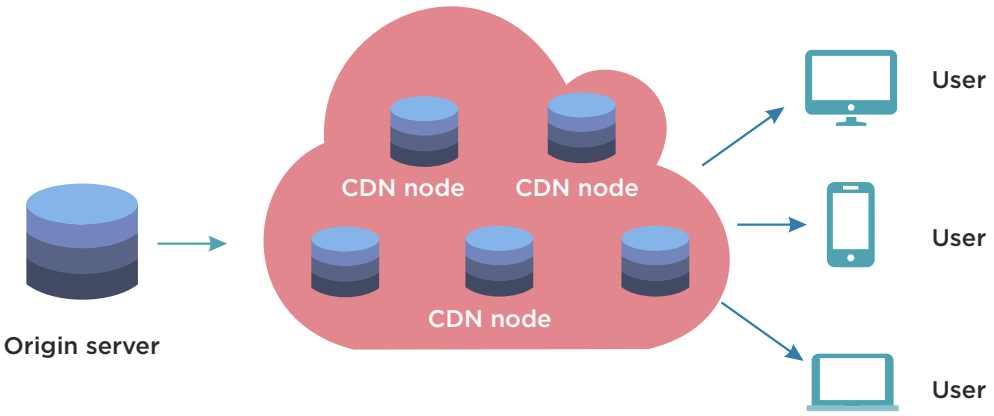
Most believe that instantaneous action is essential even though several organizations are still taking a wait and watch tactic. They are not just taking a defensive stance. They are in search of ways to take benefit of the opportunities presented by the unprecedented changes in how people access, share, and enjoy media, whether it's applying creative marketing strategies or leveraging electronic distribution channels.

Securing server

Most of the server related security requirements from content owners comes under standard security requirements for server facilities, such as access audit trails, intrusion detection systems and controls on physical access to server facilities. Muvi understands the significance of securing your video content. We provide end-to-end content protection solutions, to ensure your content is only watched by authorized subscribers and prevent illegal distribution channels to record and use your content.

Today, with the explosion of mobile device use, video streaming server technology plays an even bigger role in entertainment. Video streaming server distributes video content to a user over the Internet with a Smartphone, computer or another connected device. Through a streaming server users view the content without any lag; it feels like watching video from your local hard drive.

Once you upload your video, it is temporarily stored on various servers throughout a Content Delivery Network (CDN). It acts as an intermediary between a content server and its end users or viewers. Through a process called HTTP caching, video streaming server technology can accelerate the delivery of your video content. Content will never be lost or stolen and a live stream will be redirected to another server in the instance of a server crash.



To meet strict security regulations, CDNs constantly monitor, improve, and test their services, infrastructure and networks. From PHI to HIPAA to PCI standards, Content Delivery Networks take the necessary steps essential to keep delivery compliant to these strict regulations and shield important data.

At Muvi, we take stream security very sincerely. We make sure that all streams, both free and paid, offer the most advanced security to evade unwanted viewing from happening as we provide a monetization approach.

Concerning your video storage and streaming, our infrastructure has been designed to provide the utmost security. You can secure anything you stream or upload with the video service as Muvi manages the underlying infrastructure. We store video files in AWS (Amazon Web Service) S3 Bucket and stream the videos through AWS CDN.

In order to provide a high level of service performance and availability, Muvi utilizes an extensive range of automated monitoring systems. At, way in and way out communication points, our monitoring tools are designed to identify unauthorized or unusual activities and conditions. These tools monitor unauthorized intrusion attempts, application usage, port scanning activities and server and network usage.

Securing application
(Website and mobile apps)

Once your video content is uploaded and stored in the server, it is then delivered to the users through a Content Delivery Network (CDN). Content is delivered by the CDN in an encrypted form to the viewers' device (Smartphone, Tablet, Laptop, Desktop, Smart TV etc.), where it is decrypted for viewing. The decryption is done by various applications (mobile apps, web applications, web browsers etc.) installed inside different devices. Hence, it is important that these applications must be secure and effective to decrypt the content properly that is delivered by the CDN.

Now, due to the availability of high-end mobile devices in the market, most of the viewers prefer to watch streaming video content using the same. However, natively installed apps on these mobile devices face risks for example, sensitive data leakage, insecure data transmission and insecure data storage. The line between business and personal data & apps has become indistinct as Tablets and Smartphones become a business standard nowadays. This has leads to revealing of confidential and sensitive data, due to sharing of data between apps, peer-to-peer file and data transfers, through cloud storage and sharing and access given on social networks.

At Muvi, we develop highly secured, native apps for Android and iOS to ensure that your streaming videos can be accessed by your viewers anywhere they want. The content is delivered securely by CDN to your devices. Our advanced and secured mobile apps ensure that only the authorized viewers can view the content and makes sure that the content neither can be downloaded or shared illegitimately.

Many people watch streaming videos through their laptop or desktop's browser. When a user clicks on a video content, the request goes to the CDN. The CDN sends the content in encrypted form to the user's browser. The content is then decrypted at the browser and the user can view the content.

It has been a challenge to integrate protected quality video content into browsers, given that HTML browsers were not developed with content security in mind. In some cases, the decryption key might sit unprotected in the browser's buffer as decryption is often managed by the browser. One can capture the decryption key from the buffer to decode the video.

This issue can be resolved by integrating third party DRM (Digital Rights Management) technology. The playback client has to communicate with a license server to get the decryption key as technologies separate the content from the decryption key. The decryption key can never be captured as it is securely stored in the browser or player.

At Muvi, we provide our clients an option to use a studio approved DRM to protect their content. Mostly, DRM's use their own third party video player to show their video, which may be bottleneck sometimes, whereas we use latest HTML5 video player, which is tested in all browsers. It has an option preload='auto'. That means video URL is loaded automatically, or in simple terms - 'The browser loads the video when the page loads' which decreases the video load time considerably making it lightning fast to the viewers.

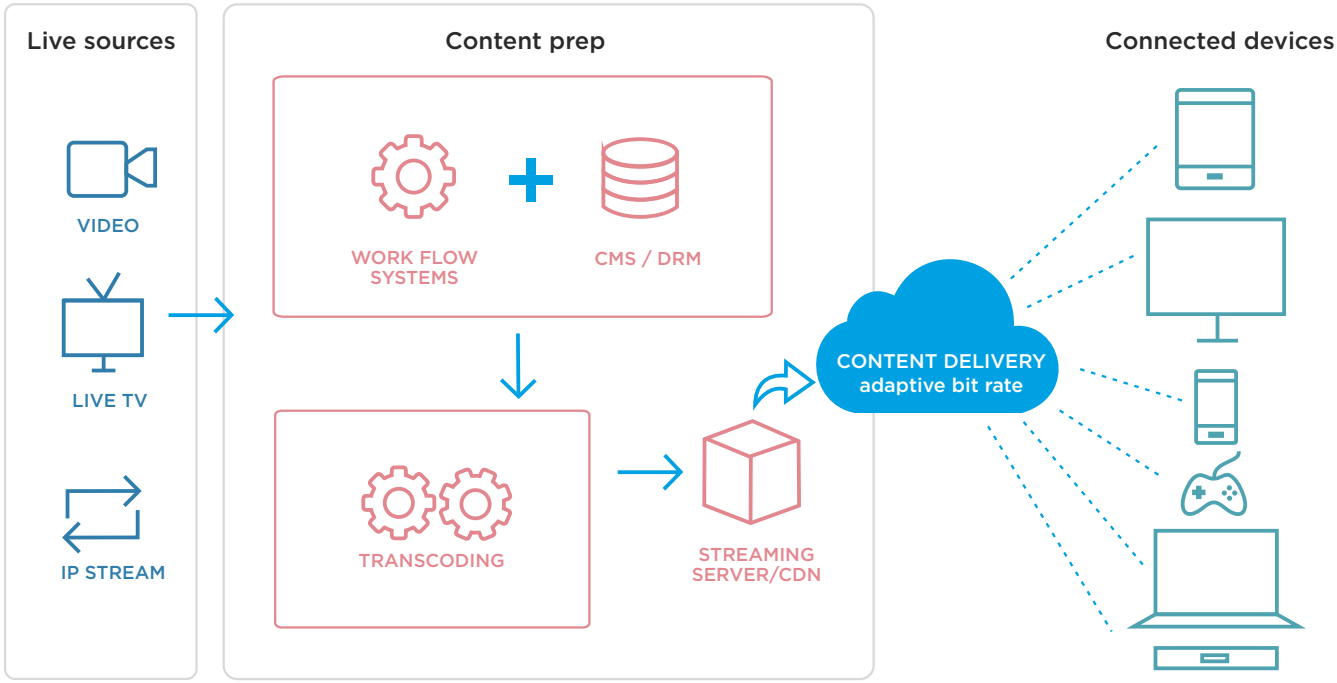
DRM
(Digital Rights Management)

It is very important to protect your digital content from unauthorized use. Digital Rights Management (DRM) gives the control that you require to ensuring your content is used only as proposed whether it's non-commercial corporate videos or monetized premium content.

When it comes to digital content, there are so many ways of copyright infringement, including copying, downloading, uploading, password or registration key sharing, burning and ripping etc. When people obtain digital content in this fashion, they do variety of things with it from sharing the content with other people, selling soft or hard copies of it to posting it online. It is costing you the cost of one item or subscription, each time they share your content with someone else for any reason.

Digital Rights Management (DRM) is an organized process to copyright protection for digital content such as video, music, eBooks etc. The intention of DRM is to put a stop to illegal redistribution of digital content and limit the ways consumers can copy content they have already purchased. In the past few years, there is a significant increase in online piracy of commercially marketed digital content, which is reproduced by the extensive use of peer-to-peer file exchange programs. Hence, DRM products were developed to put an end to the digital content piracy. Usually, DRM is put into practice by inserting code that puts a stop to copying, limits the number of devices the content can be accessed on or stipulates a time period in which the content can be accessed.

In normal standard DRM, server side key verification is essential. A key contains two parts: a key seed or private key, and a key identifier or public key. One must use both the keys and expire time to access the video file.



Some of the most used DRM methods include:

Restrictive Licensing Agreements:

The access to digital content, public domain and copyright is controlled. When downloading digital content or as a condition of entering a website, some restricted licenses are imposed on consumers.

Scrambling of source material, embedding of a tag and encryption:

This technology is designed to control access and imitation of digital content. This consists of prohibiting making of backup copies for private use.

Most Important DRMs Available for Browser-Based Video

- **Marlin,** released in 2006, from an association led by Intertrust Technologies, (Deployed in Actvila (IPTV service in Japan), Sony PlayStation Network).

- **Primetime DRM,** released in 2012, previously known as Adobe Access, part of the Adobe Primetime suite of Internet video solutions. (Deployed in NBC Sports, Comcast Xfinity).

- **Widevine,** acquired by Google in 2010, formerly a streaming video protection system. (Deployed in Google Play Movies & TV, VUDU, Netflix).

- **FairPlay from Apple,** first released in 2003, then modified in 2005 to support iTunes video downloads.

- **PlayReady from Microsoft,** released in 2008 within the Silverlight web application environment. (Deployed in Amazon Instant Video, Netflix).

Apart from Apple FairPlay, all of these DRMs can be ported to various platforms through SDKs; FairPlay only runs on iOS and OS X.

To make things simpler, there is a need of a single DRM that can work with all browser-based streaming video implementations. However, no such technology is available as of today. So, one has to decided which DRM to implement that can fulfil their requirement to protect their digital content.

At Muvi, we provide standard security, as well as studio approved DRM level security as an option.

Standard security uses token mechanism of CDN. It protects against download using browser plugin, but is not actually a DRM. The encoding is in MP4.

Whereas studio approved DRM is an industry-standard DRM such as Google Widevine and Microsoft Playready. The encoding is in MPEG-DASH. Muvi's studio approved DRM ensures that video is in encrypted format and available in parts so that the complete video can't be accessed in one file. Even if someone download some parts of the video, he can't play the video as it requires a License key to play the content. To decrypt the video, downloader needs 2 things - Content Unique Key & License Key. Token generated is device specific, means, token generated for one device won't work on another.

Preventing misuse

We have already discussed various stages of securing your video content from server level to application level and implementation of DRM. Even though, after implementing all these techniques, there is not a full proof way to protect your content. But, you can take some precaution and employ other techniques like watermark insertion to track your content when someone misuse it.

There are various methods available to copy or download video content. However, streaming video offers rather good protection as the video is not downloaded to the user's device and user is only able to watch the video online.

In fact, now there are few stream capturing tools available through which one can capture the video stream and saves it as a file, Though, this can be prevented by denying access to recognized stream capture utilities.

Even if you stop stream capturing, you cannot stop screen capturing. There are various screen capturing tools available through which one can capture the video that is played on screen. Here one can define a particular area of the screen such as, video screen and when the video starts playing one can easily capture the entire video without any difficulty.

Another easy way to capture the video content is setting up a video camera in front of a computer monitor. One can get fair quality video content by removing the flicker. Even though it is not a usual way to copy video content but a good example of how one can illegally access your content and misuse it. (i.e. distribute it to other people)

How to Stop Misuse of Content

There are few methods available through which you can stop this to some extent. One of such method is insertion of digital watermark to video content. When someone plays your video, the digital watermark will appear on the video and you can easily identify your content.

At Muvi, we provide the facility to add watermark to your videos. When anyone plays your video, the watermark will be displayed on the different parts of the video player randomly. Which makes it impossible for someone to remove it. You can also add your logo to the player. When someone plays your video, the logo will be visible on the bottom right corner of the player. So, if anyone tries to copy your video using screen capture tool or using video camera you can easily identify your video by looking at these details.

Conclusion

In order to provide a better experience to your OTT viewers and have your service intact from any means of security breach, you should employ multiple security measures and protect your videos at every level of delivery. We at **Muvi** understand how difficult it can be to manage the entire security system, when you are engrossed into creating and deploying content constantly. And thus, we bring together an unmatchable blend of online video platform and high level of video security measures that not only secure your videos at every step of the way but also prevents any and all forms of content theft.

Muvi uses encryption technology to encrypt all of your end viewer's passwords and sensitive information. All Muvi powered apps have role-based access control so platform owners are aware of their platform access with multiple people. Muvi's platforms are also PCI compliant and thus adhere to all security requirements related to online payments. We also keep monitoring our platform and solutions time to time to keep all security measures in check and improve on any dodges.

Muvi also employs several server level security measures, SSL certificates, premium Amazon Route 53 DNS, multi-level firewalls, automatic security updates, multiple backups for disaster recovery, DRM and watermarking practices, 24x7 monitoring & security audits so that your videos are completely safeguarded, leaving your focus only on improving core services.

Acknowledgement

Pragyan Priyadarshani
Chief Technology Officer
Email: pragyan@muvi.com

Abhinav Mohanty
Product Manager
Email: abhinav@muvi.com

Manas Mohapatra
Technical Writer
Email: manasm@muvi.com

Contact Us
Muvi LLC,
6H Legacy Ln, Halfmoon, NY 12065
Email: sales@muvi.com

References

(1) : https://stephenfollows.com/has-piracy-affected-the-film-business-2014-survey-results/

(2) : http://globalstudy.bsa.org/2007/studies/2007_global_piracy_study.pdf

(3) : http://www.ooyala.com/videomind/blog/video-piracy-simple-solution-6-billion-global-problem

(4) : http://www.streamingmedia.com/Articles/Editorial/Featured-Articles/Video-Piracy-The-Simple-Solution-to-a-%246-Billion-Global-Problem-109060.aspx

(5) : http://blogs.wsj.com/numbers/putting-a-price-tag-on-film-piracy-1228/
https://www.wsj.com/articles/SB114662361192442291

About Muvi

Muvi is an Enterprise Grade End-to-End Video Streaming Platform that allows video content owners to launch their own Multi-Screen OTT Platforms Instantly! Muvi takes care of everything including Fully Managed IT Infrastructure, Online Video Player, DRM, Security to Website and Apps for Mobile & TV, all deployable at a click of button, allowing you to focus completely on your business.

Sign up for Muvi's 14 Days FREE Trial Today and unlock the world of video streaming backed by unmatched security practices.

Stream your Videos on Multiple Platforms

www.muvi.com