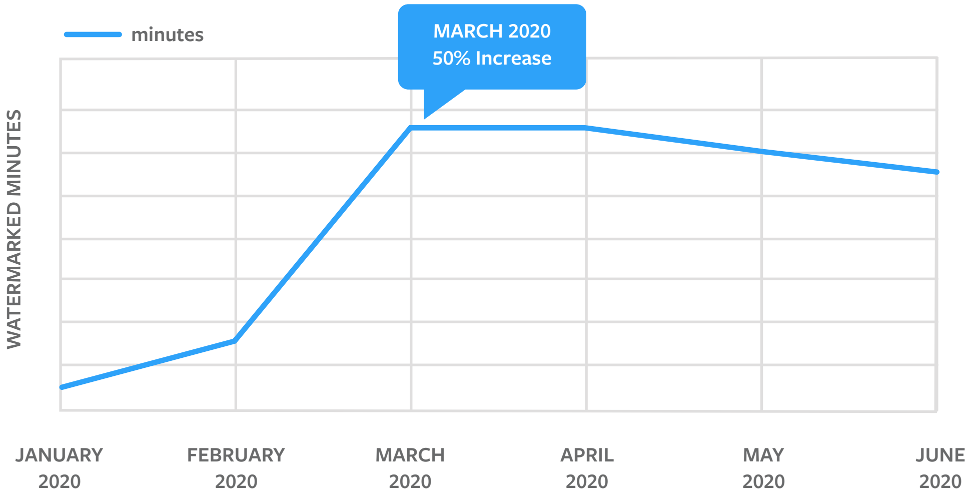
SafeStream
BY SHIFT

Content Security Report
Protecting Your Content in 2020 and Beyond

WE SURVEYED OUR CUSTOMERS TO FIND OUT THEIR CONTENT PROTECTION AND SECURITY NEEDS, FEARS, AND SOLUTIONS.

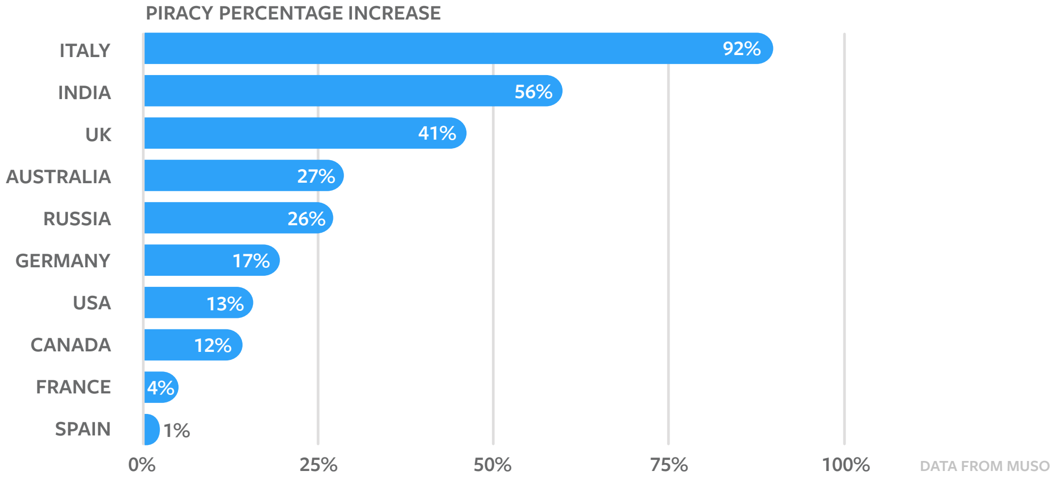
Your content needs protection now more than ever.

If there is one thing we have learned during the COVID-19 pandemic, it is that piracy and leakage is a growing problem impacting the titans of the media and entertainment industry (as well as a host of other industries). Since most companies in the United States have mandated employees to work remotely starting in March 2020, **we've seen almost a 50% increase in watermarked minutes of video content.**



Experts in the anti-piracy industry are also seeing a spike in activity on sites synonymous with piracy. With over 10 years of experience protecting digital IP for some of the world's leading content owners, MUSO has built comprehensive datasets measuring global streaming and torrented digital piracy across the TV, film, music, publishing and software sectors.

Recent MUSO data uncovers the wider developing trends in film piracy during the COVID-19 lock down, where over one-third of the world's population observed mandatory stay-at-home policies in over 42 countries or territories. This data revealed film piracy spikes in the last week of March as countries went into lock down, and April's data shows a continuation of this trend:



DATA FROM MUSO

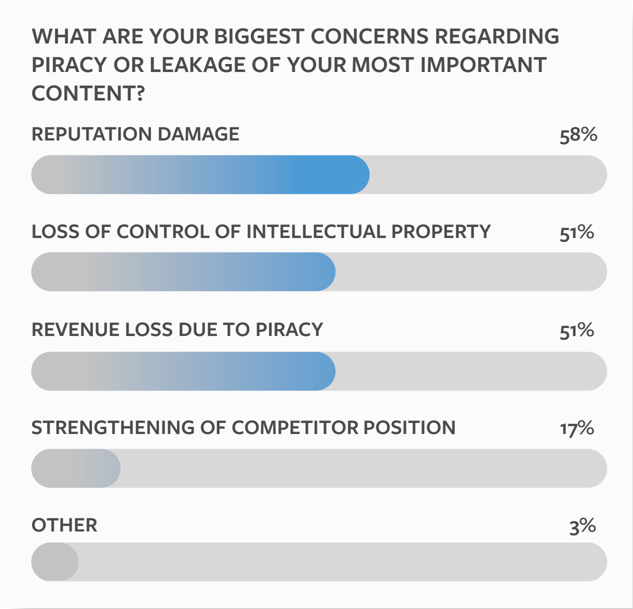
Overall, during the first 6 months of 2020, MUSO measured an astonishing 68.3 billion visits to piracy sites, peaking at 445 million per day at the height of the recent lock down.

Given the increase in piracy activity, and more individuals working remotely and on less secure internet connections, content security is more necessary than ever. *So, what are the most common reasons our customers choose to protect their content?*

We surveyed our customers, and 58% of respondents said securing brand reputation was a major reason for investing in content protection. Across all industries, being known as an entity with suboptimal security standards has a trickle down effect that impacts both the top and bottom line. It drives customers away, leads to downstream operating expenditures (e.g. legal fees, crisis PR costs), and tarnishes your ability to expand into new markets.

> Fifty-one percent of survey respondents cited protection against revenue loss as a concern.

Fifty-one percent of survey respondents cited protection against revenue loss as another concern. If you're a movie studio and your upcoming feature film is leaked onto Bittorrent sites, your box office revenue is at risk. If you're a learning and development service and your most watched training videos end up on a message board, customers lack a reason to subscribe.



If you're a global quick service restaurant chain and an internal town hall discussing sanitization policies leaks, you're at risk of turning off consumers from visiting your storefronts.

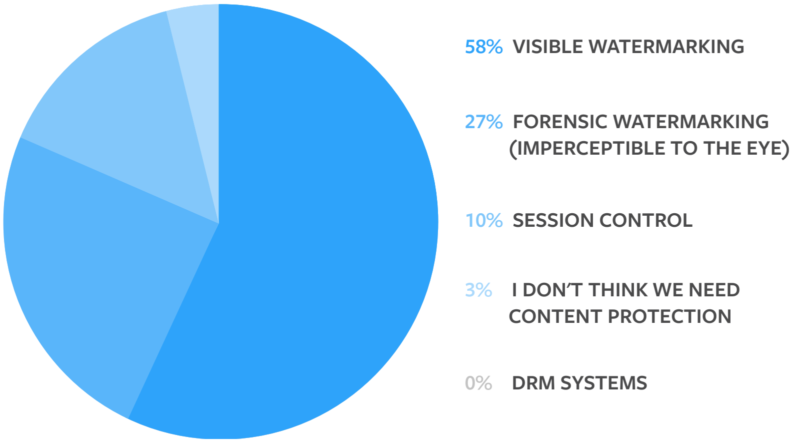
Four ways to protect your content

Content protection comes in many flavors, and addresses different areas of the delivery chain. We'll cover two pre-stream technologies (Advanced Encryption Standard and digital rights management) and two in-stream technologies (visible watermarking and forensic watermarking).

Visible Watermarking

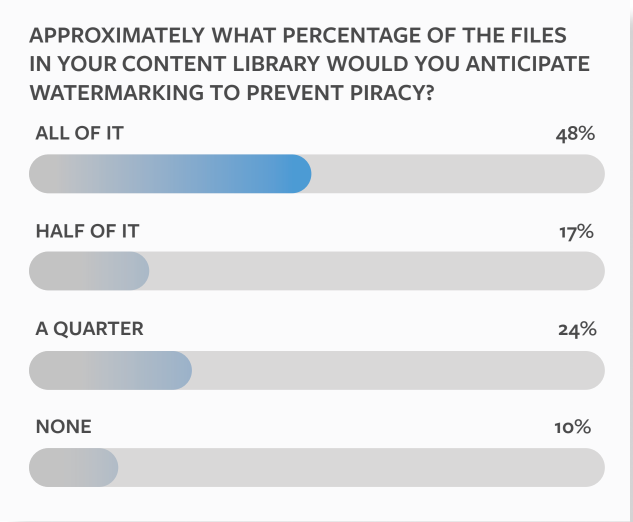
Now, for in-stream technologies. **Fifty-eight percent of survey respondents cited visible watermarking as the most valued feature for their content protection.** Visible watermarking provides high value by acting as an excellent theft deterrent. And with a personalized mark including full name, email address, and sometimes IP address burned into each frame of sensitive content, content thieves are less likely to leak the content publicly. SHIFT's visible and forensic watermarking is on demand and in real time, meaning the mark is burned into each frame of the video as you play it back. This is inherently more secure and much harder to remove than a simple video overlay mark.

WHICH OF THESE CONTENT PROTECTION FEATURES DO YOU VALUE **MOST**?



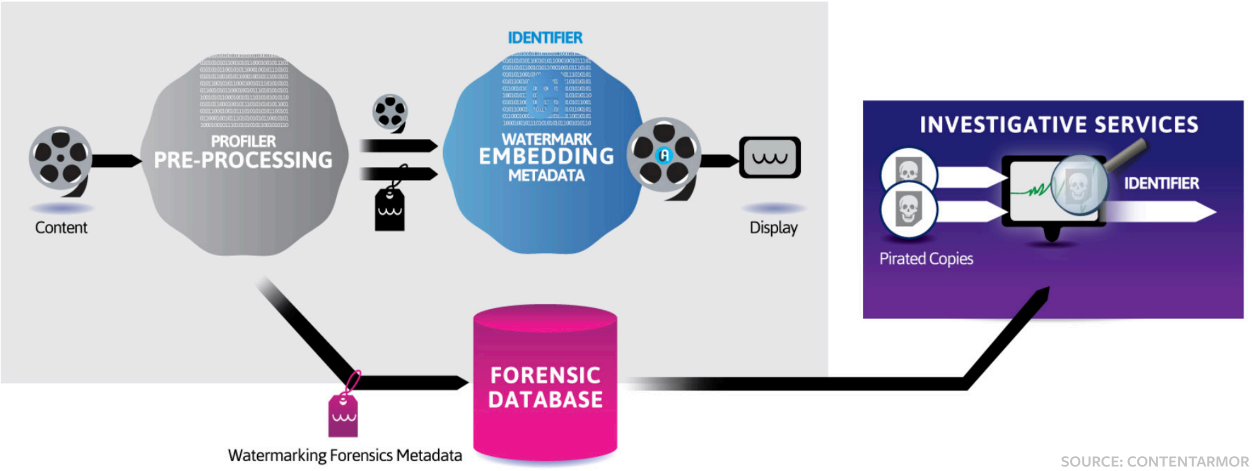
Forensic Watermarking

While visible watermarking primarily acts as a piracy deterrent, forensic watermarking offers the ability to trace down leakage of content after someone has taken the step to share illegally. For studios and broadcasters, forensic watermarking provides an invaluable tool to find and take down illegal streams of their most valuable content. In fact, **nearly half of survey respondents** stated that they would watermark their entire catalog of content.



We spoke further with some of our most loyal customers, and most agreed with the survey results. “Our media & entertainment clients benefit from our secure content testing powered by SafeStream,” says Aaron Burch, CEO of Touchstone Research, a SafeStream customer. “They’re able to leverage the insights gained to create, produce, distribute, and market content that scores with consumers and grows profits. The insights gleaned from securely testing content with the target audience allow marketers to fully understand consumer interest and reaction and provide insights on a granular level. This can lead to increased audience/viewers, potential remarketing audience, and driving customer engagement with the brand while safeguarding IP. The ability to mitigate IP theft through the SafeStream watermarking technology deterrence allows clients to achieve the ROI benefits of content vetted by their customers.”

HOW FORENSIC WATERMARKING WORKS



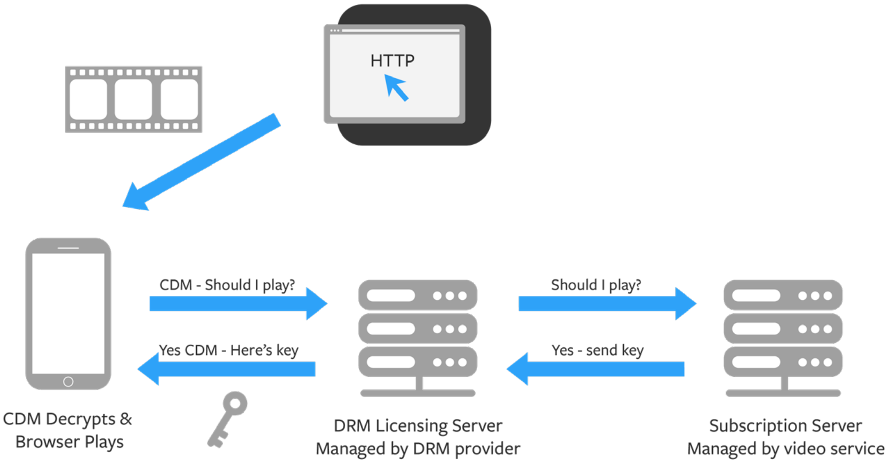
SOURCE: CONTENTARMOR

Forensic watermarking has many flavors, but SHIFT's SafeStream uses bitstream modification. In this process, imperceptible unique identifiers that can be traced back to individual users are embedded in the video. SafeStream can then detect any leaked files back to individual users by referring to user-specific metadata created during the watermark embedding stage. This process ensures optimal security, while remaining cost efficient in comparison to other forensic watermarking technologies.

Encryption

At a basic level, encryption is the process of limiting playback of video files to only those who have been assigned an encryption key. The most common form of encryption for videos is a format called Advanced Encryption Standard 128 bit Encryption (or AES-128). The NSA recommends this encryption algorithm and it is used to protect top secret communications.

How does this work? When the viewer hits play, the video player begins to download the file from a server. At the same time, the browser in which the video is playing seeks to acquire a decryption key from the location identified in the adjoining metadata accompanying the video file (what is called a Manifest File). If you have credentials to access the file, you're able to watch. If you don't..... well, you can't.


HTTP
CDM - Should I play?
Yes CDM - Here's key
Should I play?
Yes - send key
CDM Decrypts & Browser Plays
DRM Licensing Server Managed by DRM provider
Subscription Server Managed by video service

SOURCE: STREAMINGMEDIA.COM

Digital Rights Management (DRM)

Many content owners turn to DRM as another form of content security. DRM takes encryption to the next level by requiring that the encryption process flows through a third-party licensing server. As seen in the diagram from Streamingmedia.com, the Content Decryption Module (CDM) facilitates receipt and application of the decryption key from the DRM licensing server. This process keeps the encryption key hidden, and allows for additional business rules to be applied to playback authorization. For example, you can determine which browsers are acceptable for players back, how long the content is available to the user, and which geographic locations are approved for viewing.

Playback occurring on different browsers and devices requires different DRM formats, including Apple FairPlay, Google Widevine and Microsoft PlayReady. As one would imagine, Apple browsers and operating systems support FairPlay, Android browsers and operating systems support Widevine, and so on. Custom applications are able to support several different technologies, as our SmartTVs and Connected TV devices.

Summary

Now that you've learned a bit about content protection, which is right for you? If you're interested in our more robust SafeStream visible and/or forensic watermarking technology (including AES-128 encryption) and have some questions on how to integrate DRM, please contact us at **info@safestream.com** and we can help you determine what's the right solution.

Survey Methodology

We surveyed roughly 4,100 non-SafeStream MediaSilo users and 1,200 SafeStream users. We received 29 responses between July 7th and 11th, 2020. We asked them six multiple choice questions online via Typeform with this prompt: "SafeStream is an anti-piracy content protection product that saves customers lost revenue and protects intellectual property. We're interested in understanding your content protection needs."