



DRM ECOSYSTEM AND SECURITY BEST PRACTICES

- For complete security, DRM falls short
- Security best practices are emerging
- An ecosystem approach is key



1 Introduction & Executive Summary

Digital Rights Management (DRM) has long been the centerpiece of online video security. In fact, it is the beating heart of a complex orchestra of services that ensures the smooth delivery and protection of media assets.

Despite common practices, DRM with token-based authentication can still be hacked. Furthermore, breaches to delivery and device environments are outside the scope of what DRM can protect. To fully thwart the efforts of hackers and pirates, additional tools are needed and comprehensive best practices should be followed. It's an uphill battle.

That's why this DRM Ecosystem Best Practices Guide was created. It provides up-to-date, field-tested insights to help media professionals balance studio-recommendations, state-of-the-art security, and business performance when compiling a solution for controlling access to and usage of video content.

It takes a wise choice of connected technologies to securely deliver digital content worldwide - and it's easy to become confused about how things work, or make selections solely based on price, or choose a solution or supplier merely to satisfy a checkbox requirement.

Whether you are a content owner, rights-holder or distributor – from the Chief Revenue Officer to the Security Operations team to the Chief Information Officer – all are responsible for maintaining a balance between driving revenue, maintaining competitive advantage and preserving relations with suppliers, while protecting media assets, company information and providing a good user experience that's cost effective to operate.

We “the industry” need to do things right every time to protect valuable content while a video pirate only needs to be right once. DRM is amazing technology - but alone, it's not enough. An ecosystem approach is key.

We “the industry” need to do things right every time to protect valuable content while a video pirate only needs to be right once.

The path to secure video content



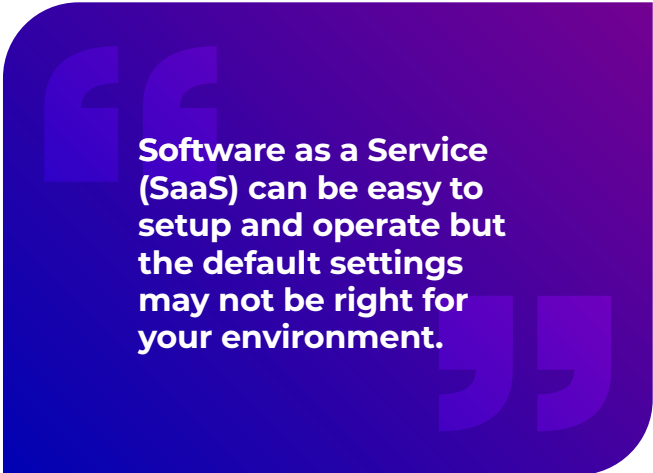
Table of Contents

01	Introduction & Executive Summary	1
02	Why Security?	3
03	The Media Delivery Ecosystem	5
04	Threats to Security of Video Programming and Services	6
05	Piracy: Defining the Risks	9
06	Security Technologies	12
07	Implementing a Secure Service: Major Considerations	14
08	Technical Best Practices	18
09	Operational Best Practices	28
10	Key Takeaways	31
11	Conclusions and Recommendations	32
12	Closing Thoughts	35
13	About Verimatrix	35

2 Why Security?

For those tasked to maximize revenue, security may not be a first consideration, but a good defense is needed when it comes to protecting that revenue from erosion through theft, and to protect the enterprise from other threats.

Good security not only protects the video content and services themselves: it also protects the integrity of the broader business offering, protects private data and helps preserve relationships with business partners. Properly implemented, with comprehensive internal safeguards, procedures and documentation in place, good security also helps video providers optimize their own costs of operation.



Software as a Service (SaaS) can be easy to setup and operate but the default settings may not be right for your environment.

Preserving service revenue

To help preserve revenue potential, security begins with the basics: upholding consumer access parameters. These include granting access permissions only to authorized and authenticated end users, enforcing the number of users in a household who have access to that service – concurrently or in total - and enforcing territorial constraints.

Video providers can model permissible use parameters in the “typical” household, such as the maximum number of devices, concurrent users on an account, permissible level of license requests, or the consumer’s location; to give them a baseline that they can compare with actual use and enable them to escalate anomalous use for mitigation. Mitigation tactics can be carrot or stick: a friendly marketing offer or adjustments to service.

Meeting obligations

Beyond enforcing consumer-facing safeguards, it’s equally important to protect business terms such as those between content providers and their distributors. Some might argue it’s more important, since inadequate protection could result in a breach of distribution agreements, resulting in no service at all!

Modern video providers must comply with content security requirements and content protection schedules before they can deliver content to end users. Examples include ¹Movielabs’ Enhanced Content Protection and Digital Distribution specifications, and for the interchange of assets between content producers and their business partners, the movie industry’s emerging production ²security guidelines as well.

Reducing loss

Another side of security is to reduce loss, which can happen in a variety of ways. These include protecting exclusive sports rights against theft and re-distribution to unlicensed territories. If a video provider is unable to prevent theft - or at least demonstrate that they are executing on plans to do so - the rights licensor may refuse to grant or renew rights to distribute their programming.

Conversely, video distributors have been known not to carry original programming because the programmer can’t guarantee against piracy, in which case, paying the price for exclusivity would not be justifiable. One example of this occurred in 2020 when beIN Media declined to renew its contract with Deutsche Bundesliga over piracy concerns³.

¹ <https://movielabs.com/distribution-specs/>, ² <https://movielabs.com/production-specs/>

³ <https://www.sportspromedia.com/news/bundesliga-tv-rights-bein-mena-piracy-saudi-arabia-beoutq/>

Advertising revenue

Other security-related situations that could damage a video provider's reputation include fraudulent apps and fraudulent advertising. Software developers, working for pirate operations, could reverse-engineer or replicate the look and feel of an app, and pre-program them to deliver stolen content and services, configure them to implant malware, or present fraudulent advertising that leads the user to other threats.

To provide consumer incentives to take a service, many video distributors offer premium programming at a promotional price or even free of charge, with the cost offset by ad revenue. For app-based viewers, advertising is often injected by the viewing application, which can be hardened against - and monitored for - manipulations by users trying to skip ads, or by malicious players trying to inject their own fraudulent advertising or malware.

Optimizing distribution

Another set of risks associated with online distribution relates to distribution itself, including:

- ▶ Attacks that grant access to services and content by non-subscribers or by pirates acting as illegal aggregators, such as the illegal distribution of live events - resulting in revenue loss.
- ▶ Spikes in traffic from illegal requests that could force a video provider to over-provision its distribution network to help it guarantee service quality to legitimate consumers.
- ▶ Illegal traffic carried over the video provider's network increases the cost of network services.
- ▶ CDN access is often controlled through tokenization. Tokens in the distribution chain are attacked by pirates to get hold of these assets.
- ▶ Pirate aggregators rely upon intercepting key requests, authentication secrets and tokens. Countermeasures should be in place to harden against theft and detect attempts at stealing data used for authentication.
- ▶ Reducing attacks on the OTT content distribution ecosystem by clandestine actors with illegal intent.

Attacks on OTT distribution by clandestine actors can be detected and mitigations put in place reduced through monitoring.

Preserving reputation

Good security boosts consumer confidence that they are accessing services and content from legitimate sources. This is difficult to quantify because, when carefully implemented, these security practices may never be seen by the end consumer – even if they experience it's benefits every day.

Good security involves a variety of interdependencies, with interdependent benefits. One example is credential fraud, which can lead to a variety of threats. Databases of consumer IDs and passwords are obtained by industrial hackers and sold in clandestine markets. Pirates buy these databases for pennies per name and use automation to test them against media accounts. Those which work are set aside.

Pirates may then use the credentials to conduct phishing attacks which could lead to malware attacks against the unsuspecting account holder, who might blame the video provider for the attack. Video providers that detect credential fraud by detecting anomalous use are in a position to prevent such attacks, which reduces such risk to a video provider's reputation.

3 The Media Delivery Ecosystem

Media delivery is complex, involving a seeming myriad of interdependent media processing, storage, networking and service delivery components and software that must work in harmony to recognize and implement service rules, content entitlements, distribution constraints and operations roles.

Defining the context: An end-to-end worldview

Consider the challenges. Content must first be ingested into the service platform, then processed and packaged in ways that content can be delivered securely and compatibly to - and recognized by - authenticated end-user environments. All that, before it's actually consumed.

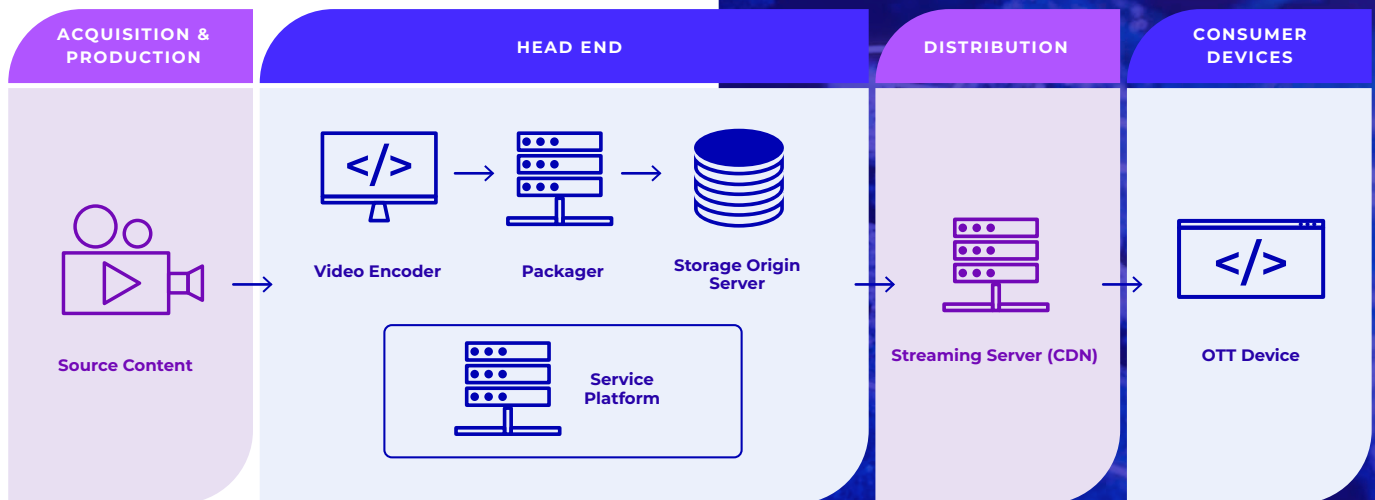


Figure 1: End-to-End video service ecosystem

Even at the point of playback, the work of protecting valuable content and services remains incomplete. As we described earlier, consumer endpoints are also subject to attack and are targets for piracy.

Consumer endpoints are a particular challenge to secure, as there are many categories of devices, each with their own operating system and chipset environments, each with their own video profile and packaging requirements, which force video providers to maintain multiple protection frameworks.

**Media delivery is
more than the sum
of its parts.**

4 Threats To Security of Video Programming and Services

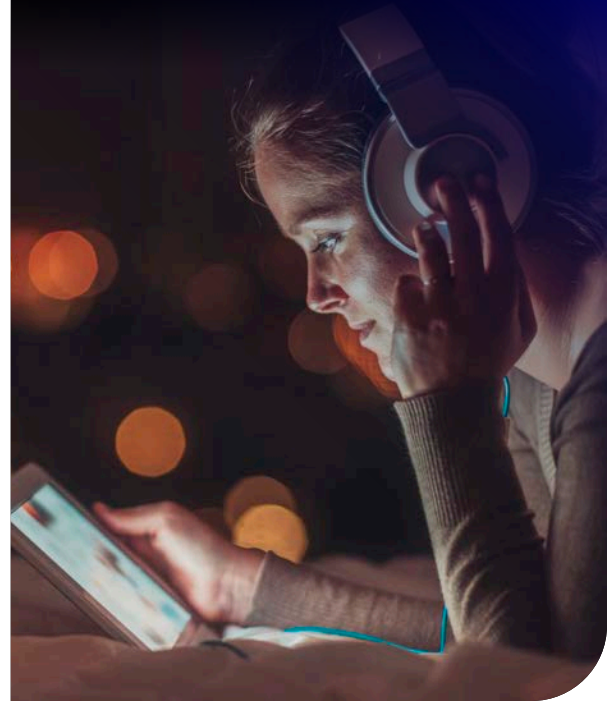
Now that we have identified why security is important and illustrated the complexities of media distribution, albeit at a very high level, we have more of a context in which we can evaluate the threats: current, emerging and intangible.

Widely recognized security threats

Threats that are widely recognized across the media and entertainment industry today are primarily about the theft of content and services, and their redistribution online. These include:

- ▶ **Stream-ripping**, in which a stream is acquired, decrypted and decoded by a player, diverted to an output device, and stored on a local computer or server for illegal re-distribution. This includes screen recording and capturing content from device outputs such as HDMI.
- ▶ **Password sharing**: For many years, video providers have blamed piracy on password sharing by consumers, to friends or family members who in turn would share to others. Without other safeguards in place, an email address and a password are sufficient to access the service.
- ▶ **Credential fraud**: A much greater risk arises from criminal actors - pirates - that purchase large databases via clandestine markets and, by using automation, test them against media services; setting aside those which unlock consumer accounts for resale. This practice is sometimes called 'credential stuffing.' The pirates' profit from selling services 'behind' these credentials, and because the consumers' email addresses are known, pirates also get avenues to inflict further damage. Credential fraud is often also used by pirate content aggregators, to have a set of basic accounts targeted at video provider, used to get all needed information for accessing content for redistribution, without having a direct link to these accounts.
- ▶ **Media center software**: running on computers or servers in home networks, such as Kodi and Plex, for which pirate apps are available, to give end users access to illegal instances of content and services.
- ▶ **Illicit streaming devices (ISDs)**: Devices that are built to a pirate's specification by integrators that acquire the parts and software needed to construct and pre-program them to access illegal instances of live and series television programming, and video-on-demand. Active marketplaces exist online for the component parts and open-source software.

Pirates steal content from a variety of consumer end-points.



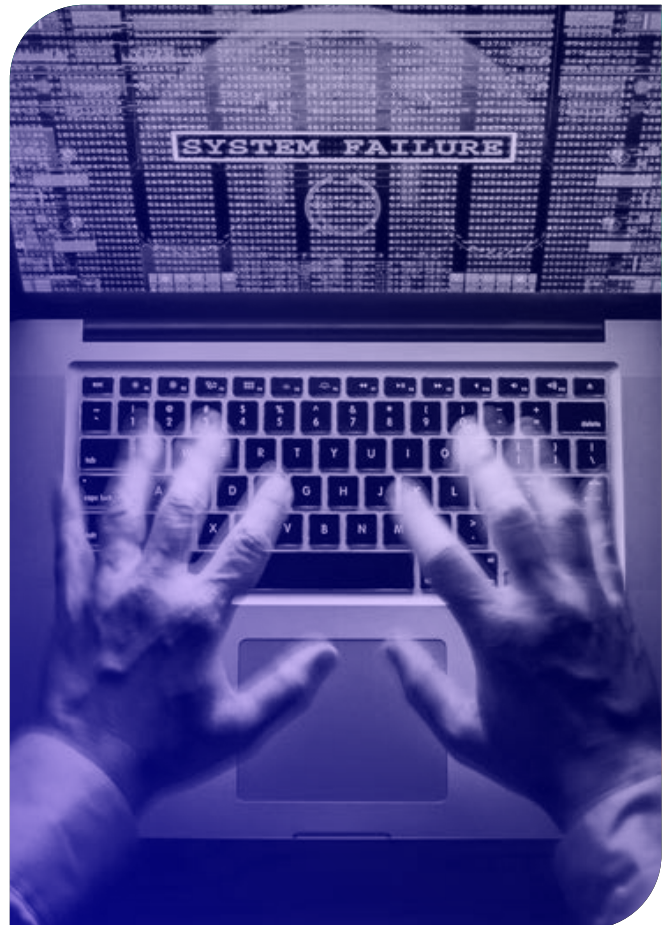
Additional paths to piracy

- ▶ **Inadequate session management:** Sessions that have not been closed at the end of a session can be penetrated, to access streaming servers and other systems resources in order to steal content.
- ▶ **Lack of virtualization:** Systems that are configured in ways that reveal actual sources and destinations (e.g. IP addresses that are not virtualized) can also expose video providers to attack.
- ▶ **Security hacking:** Exploiting known breaches in commercially-available security platforms.
- ▶ **Token theft:** Stealing or illegal reuse of access tokens for access to licenses and Content. Pirates steal tokens from the applications on client devices as well as by illegally accessing token proxies.
- ▶ **Manipulations of advertising:** Skipping ads illegally by manipulations of the viewing app or by allowing redirection of the requested advert to be replaced by one from the pirate.
- ▶ **Personally Identifiable Information (PII):** This can include personal information such as customer names, addresses, and payment details, as well as intelligence related to back-end systems and other intellectual property (IP) such as source code and content.

Emerging threats

An additional array of vulnerabilities has become increasingly recognized. These include:

- ▶ **CDNs (Content Delivery Networks):** Criminal actors can break in via open streaming sessions (or sessions that have not been properly closed), through improperly implemented APIs, and by launching cyberattacks
- ▶ **API attacks:** APIs (Application Programming Interface) are points of information exchange between processes – such as consumer requests to interact with a service - or between elements in a video provider’s delivery framework, such as a playout server and a distribution network. The attacker can gain access to a video provider’s platform via Man-in-the-Middle attacks, where the attacker intercepts and manipulates the communication between the API and the client. This could allow the attacker to steal sensitive data or inject malicious code into the API. Attacks through a video provider’s payment processing pipeline or through other APIs can also open access to steal sensitive PII data.



- ▶ **Devices and software:** While device platforms have beefed up their compliance requirements, devices are still vulnerable to a range of attacks, both to penetrate their hardware and software infrastructures, and to discern the information (data, keys, content) traveling within the device.
- ▶ **App vulnerabilities:** An attacker could weaponize a broadcaster or pay TV operator's mobile app to steal consumer PII, content and services, the video provider's code or intellectual property. For example, an attacker could reverse engineer the app to discover vulnerabilities or create modified versions of the app that contain malicious code or steal sensitive data.
- ▶ **Fraudulent advertising:** Software developers are available as “pirates for hire”, to reverse-engineer legitimate media apps, use phishing attacks to entice users to download fraudulent apps that look authentic, and later, suffer attacks via the theft of personal information and through malware.
- ▶ **Legitimate advertising delivered to fraudulent end-points:** While it's recognized as a threat in the advertising industry, the mainstreaming of AVOD services will shine a spotlight on ad fraud to video distributors. According to a 2021 ⁴study by the Digital Citizens Alliance, as much as 40% of advertising through the most dominant online ad platforms is delivered to pirate apps.

“Pirates exploit your trust in the tools of daily life.”



- ▶ **Attacks on virtualized production:** Another emerging area is in virtualizing video production to the cloud. Modern video production relies increasingly upon the cloud to enable geographically dispersed work-groups to collaborate and to exchange assets with outside suppliers of content-related services such as subtitling, audio re-versioning, with business partners such as advertisers and distributors; and with manufacturing partners such as toy companies to build action figures. This adds a layer of complexity to security.

In the 'old days' when video production was facilities-based, it was less of a challenge to air-gap production platforms so they had no access to the Internet. But today's production practices can't air-gap the cloud. As noted earlier, the film industry has published distribution guidelines. MovieLabs is now several years into its “Vision 2030” ⁵initiative to standardize cloud-based access, workflow and security practices. But at the outset of 2023, industry stake-holders were just beginning to harmonize their respective platforms with one another and present a consistent face to outside resources.

⁴ <https://www.digitalcitizensalliance.org/issues/breaking-bads>, ⁵ <https://movielabs.com/production-specs/2030-vision-papers/>

5 Piracy: Defining the Risks

In a video services context, piracy is the theft and illegal re-distribution of content and services, without having the rights to do so. Video pirates infringe copyright and destroy the value of media stake-holders; not to mention inflicting collateral damage on end users and often as a result of that, damage to the reputations of video service providers.

Illegal acquisition of content

In addition to theft at the point of end-user playback, theft can also occur as a result of breaches to the user authentication process, by exploiting open sessions, from breaches to delivery infrastructure, or from breaches to video processing and storage facilities; as we see from the following diagram.

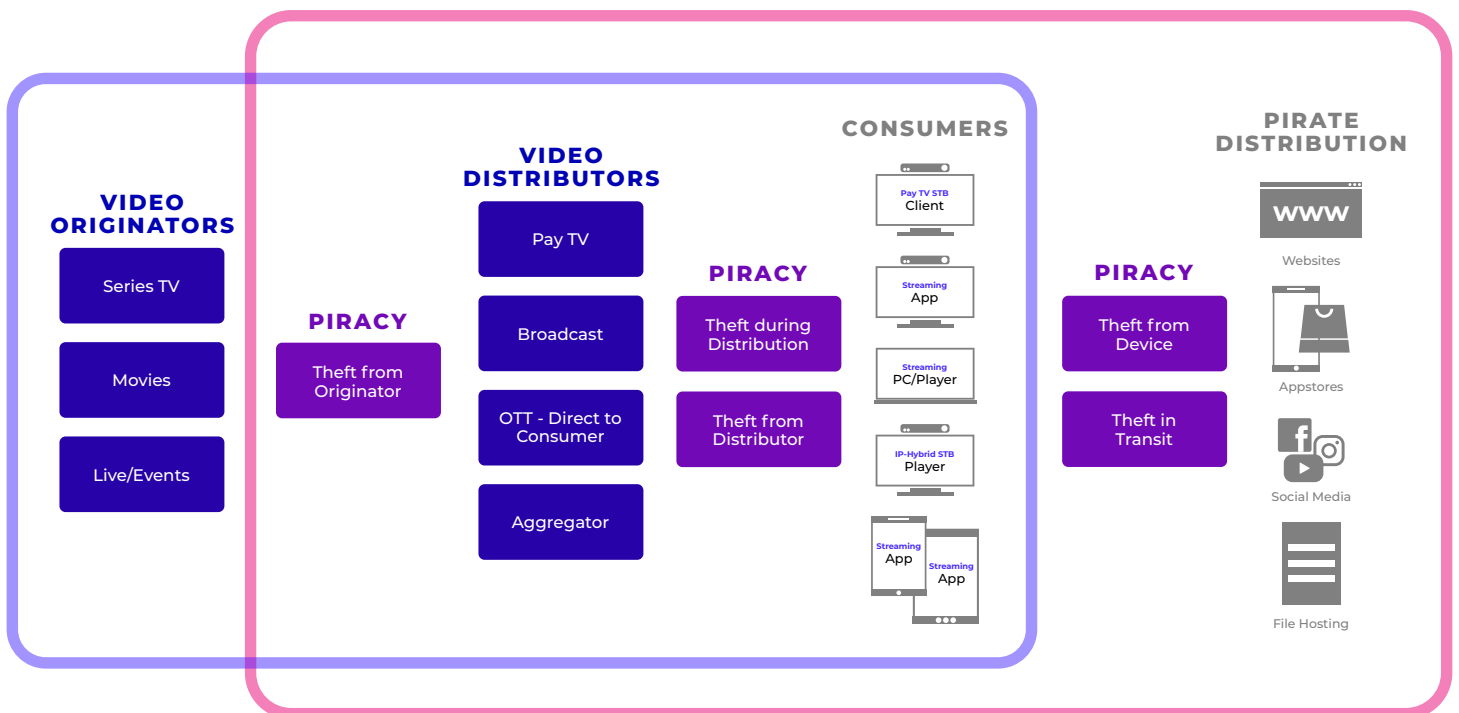


Figure 2: Piracy is also an end-to-end concern

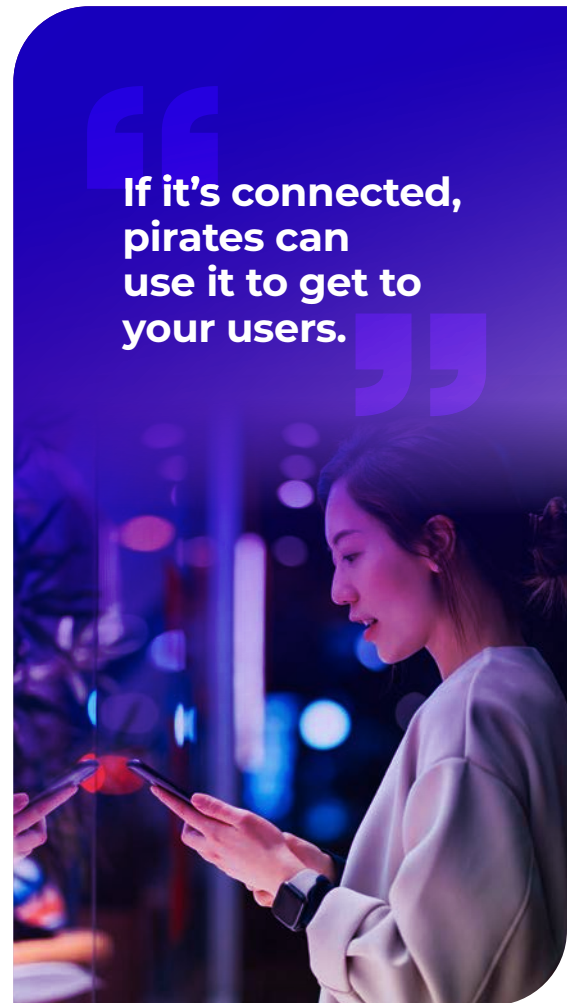
The items in the diagram that are highlighted in blue represent the industry of video production and legal avenues of distribution. The intersecting ecosystem highlighted in red represents illegal acquisition (theft) of content.

The previous sections framed our discussion and illustrated a wide variety of threats. The task is now to recognize how pirates redistribute valuable content and services illegally. The sections following this one delve into how to protect against piracy and how to mitigate these threats.

Once a pirate obtains content, several distribution alternatives are available to them. They are the biggest competition to pay TV operators, studios and series television programmers selling direct-to-consumer online video services.

Business-to-consumer channels of distribution include

- ▶ Direct download from 'cyberlockers' via the Internet.
- ▶ Peer-to-Peer (P2P) online distribution using protocols such as Bit-torrent, which source content from computers connected to the Internet.
- ▶ Illegal "IPTV" services: retail 'storefronts' used to distribute stolen content and services via streaming. They routinely offer hundreds of channels and thousands of TV programs, movies and live programming. There's little limit on how much programming they can offer. A simple Web search is all that's needed to find thousands of these providers.
- ▶ Illicit streaming devices (ISDs): Consumers can buy pre-built / pre-integrated IP and hybrid set-top boxes that are programmed with access to premium TV channels, live streams and high-value on-demand programming at a fraction of the cost of legal devices and subscriptions.
- ▶ Apps for mobile devices and media center platforms: Software-based media center platforms such as Kodi and Plex, have been notorious distribution channels for pirate apps, but again, these platforms have been increasingly vigilant against pirate apps. Similarly, the major mobile platform providers have also put strict compliance and security requirements in place. But these requirements only defend against illegal redistribution and not against device hacking.



Business-to-business channels of piracy distribution

- ▶ **Hosting sites:** Content is hosted directly by the pirate, which maintains its own servers and service infrastructure, in support of direct download, cyberlocker, P2P, streaming distribution and app downloads.
- ▶ **Linking sites:** Because some jurisdictions offer only limited legal or legislative countermeasures, pirates can open a storefront, and rather than hosting the content themselves, they link to programming that is hosted by others and escape prosecution.
- ▶ **Cloud distribution:** Criminal actors can capture, store and distribute stolen content via their own server infrastructure, or by storing and distributing it via the cloud. They can hide or disguise their locations, making them difficult to catch and stop.
- ▶ **Piracy-as-a-Service:** Piracy has evolved from an industry that expanded access to download illegal instances of content, streaming portals, marketplaces for stolen credentials and illegal streaming devices, into a multi-tiered application development and content distribution ecosystem that can equip pirate retailers with pre-built turnkey platforms and virtually unlimited supplies of content, using a SaaS model. Many of these wholesalers also offer end-user technical support and custom app development. Those wholesalers which also offer malware-as-a-service split the proceeds gained from end users between the malware developer and the pirate.

Piracy: Other infringing conditions

- ▶ **Violations of release windows:** The Internet has enabled immediate distribution of programming stolen from a market where programming is available, into markets where the release date is in the future.
- ▶ **Violations of territoriality:** The Internet has also enabled distribution of programming stolen from a region where programming is available, into regions where the rights-holder/owner wants to restrict distribution or offer it under a different pricing model.
- ▶ **Time is of the essence:** For live events, Theft and illegal redistribution must be detected and stopped quickly.

“Pirates also infringe on contractual conditions related to release windows and location.”



6 Security Technologies

In a video services context, piracy is the theft and illegal re-distribution of content and services, without having the rights to do so. Video pirates infringe copyright and destroy the value of media stake-holders; not to mention inflicting collateral damage on end users and often as a result of that, damage to the reputations of video service providers.

Protecting access: DRM, access keys, key rotation and location

DRM uses advanced encryption standards and specialized techniques to securely store and deliver encryption/decryption keys, preventing hacking and unauthorized downloading. DRM systems associate assets and services with keys. When a request is made using a recognized key, access is granted.

Most native DRMs do not include end user authentication. This authentication may come with some multi-DRM systems but is more commonly available from security vendors with traditional CAS pedigrees. The majority of available multi-DRM systems use token exchange to mediate the authentication required between the end-user and different components of a playout system. Tokenization and its pitfalls are further explained later in this paper.

Geo-location capability complements DRM, since encryption and key exchange are not location-aware. The objective of geo-filtering - which can also be used to detect the use of VPNs to circumvent location rules - is to provide a high degree of confidence that content is only being consumed within the licensed territory and that common approaches to circumvent these checks, are detected and mitigated.

Tracking content: Forensic watermarking

Watermarking is a technique used to track and identify the original consumer of content, specifically in regards to deterring screen and audio-capturing software used by pirates.

In addition to being a deterrent, watermarking can also be used as a forensic tool to prosecute perpetrators by tracing shared video back to the individual responsible. This technique is particularly useful in the context of live streaming events such as sports, where each viewing session can be given a unique watermark to monitor for illegal sharing.

There are several approaches to watermarking. Many video producers watermark the asset itself, as a way to document its ownership. Video distributors can apply watermarks to individual streaming sessions, to an individual instance of an asset or from within a consumer device to associate them with individual end users. A watermark can then be 'extracted' from a session or file that is suspected of being illegally distributed, to read its identifying information.



With traditional or old school CAS/DRM solutions authentication came as standard.



Technology situation

Video producers and distributors have launched exciting new streaming services, delivered over Internet protocol access and protected by DRM under a variety of business models; enabling them to reach growing audiences that no longer subscribe to pay TV or buy physical media.

In addition to providing operators with the option to choose and switch technology providers more easily, the relative ease by which this multi-service, multi-DRM approach enables new services to be brought into operation also masks the complexity related to operating a secure solution.

While operators perceive DRM as enabling strong security for content and services, security attacks can also take place before and after encryption by the DRM platform, as well as on the encrypted content itself. Therefore, DRM alone isn't sufficient to protect delivery, service end-points, or an operator's service delivery infrastructure. Software-as-a-Service (SaaS) approaches, combined with ever-increasing processing power available in the cloud have exposed them to new challenges as well.



Protecting software and apps, both at-rest and in operation



There is an industry of software developers working in service to organized crime and pirate actors, who analyze and reverse-engineer legitimate apps to create fraudulent apps that resemble their legitimate counterparts, but in reality, are used to attack consumers to steal personal information, implant malware, or to open windows into a video provider's video infrastructure to steal content and services.

Two aspects of protection are required: static protections that obscure an app's internal structure, software components and interfaces to deter attempts to tamper with these components and dynamic protections that detect attempts to intercept keys and data during runtime.

7 Implementing a Secure Service: Major Considerations

Just as it takes an ecosystem to produce and deliver video services, it takes an ecosystem to protect it. Taking a service life-cycle approach to security helps to de-mystify the process.

Gaps exist between market needs and available security solutions. In some situations, there is demand for solutions that don't exist. In others, solutions are coming but are not yet available. Compounding the challenge is that the situation differs in various parts of the world, due to differences in how copyright law is enforced, differences in government regulation and cultural differences both in business and in society.

To effectively secure against risks to a service, there are several areas to consider.

Business considerations

To govern how a video service is defined and operated – streaming or otherwise - business rules must be established. These rules may be driven by externally- or internally-driven factors.

External influencers include licensing and contractual terms with suppliers, reseller relationships, consumer expectations, competitive pressures and other conditions in the marketplace.

Examples of externally-driven business rules include:

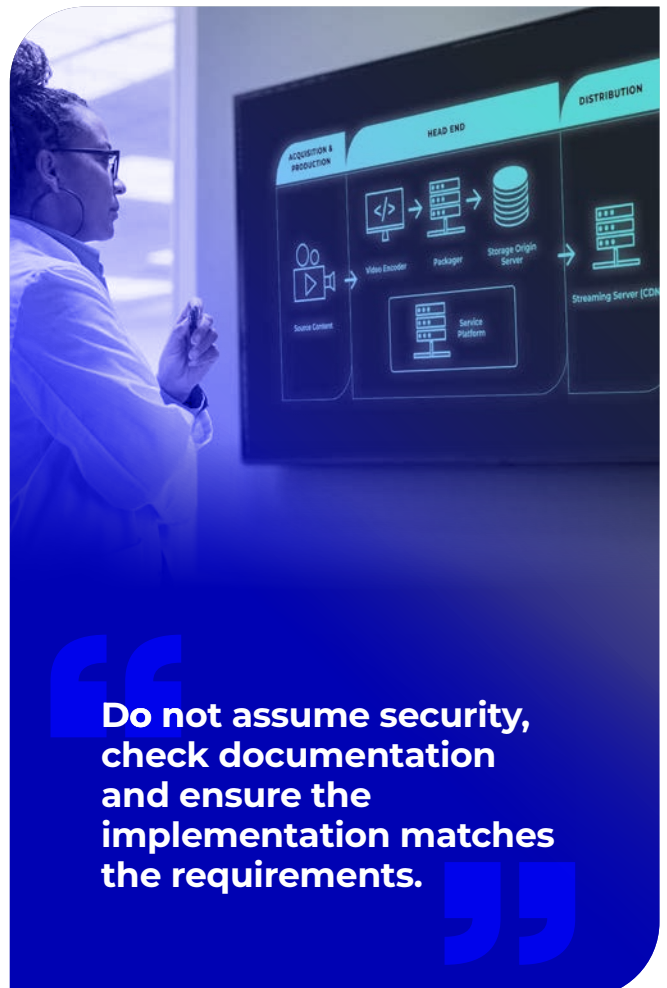
- ▶ Enforcement of content release windows over time by market territory, geographic region or country.
- ▶ Permissions to access content or services within a household, and with users that may reside outside the primary service address but permitted to access service as family members.
- ▶ The definitions of bundles and service tiers such as "Good" "Better" and "Best," plus add-on packages with specialized programming.
- ▶ The number of concurrent streams that may be consumed in a subscriber household, or permitted in a sharing plan. This significantly impacts shared or stolen credentials.
- ▶ The number of active devices permitted in a consumer household overall and permissions to access content concurrently within the same household.
- ▶ The types of devices that are permitted to access the content, and the video profiles that are permitted by the rights-holder to deliver to these devices, which may differ based on the service tier that the consumer subscribes to.
- ▶ Permissions for time-shifting, ranging from none ('live' local programming only, for example), to Pause, Trick-play (fast-forward, Rewind, +10 seconds/-10 seconds, etc.)
- ▶ Whether or not DVR is available, where the content resides (cloud vs. device), and storage allocation by user or subscriber household.
- ▶ Content exclusivity, in which a single distributor may have rights to distribute in a given market.
- ▶ Blackouts in which a national distributor is prohibited from distributing in a local market because a local distributor takes precedence.

Static platform considerations

These are factors for the service *as defined*. They should enable the service models, service features, and implement the permissions and constraints defined at a business level.

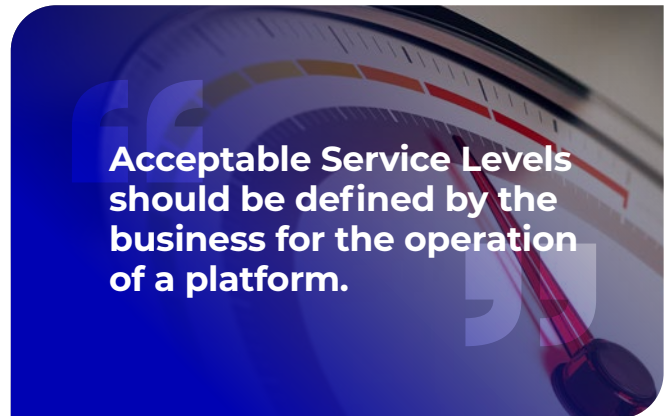
Considerations that apply to the definition of the security platform include:

- ▶ **Architecture:** The defined solution should be constructed from the outset with business requirements, operational balances, monitoring and stability in mind. When components are moved to cloud solutions, the ethos of security should always be considered and architects should ensure cloud solutions have documentation from the technology provider that answers all the questions that would have been expected for a hardware implementation (i.e. do not assume security, check documentation and ensure the implementation matches the requirements).
- ▶ **Software coding:** Use defined coding practices that allow for automated code validation and checking. Ensure code is documented, tested and allows for rolling back if required.
- ▶ **Interfaces:** By default, all interfaces, services and ports should be closed and only opened when absolutely required by the design. All connections should be secured between platform components and external entities with a current and up to date variant of the chosen technology.
- ▶ **Software integrity:** The platform should check the integrity of the host they are running on and ensure any operating systems or application and player software is up to date. Solution designs need to provide defenses against Dedicated Denial of Service (DDoS) attacks.
- ▶ **Systems validation:** Systems and service elements that make up the service platform should have their operations benchmarked.
- ▶ **Device profiles:** The service platform should securely store the devices capabilities against the business rules so that services and content are delivered in accordance to business rules.
- ▶ **Use-case modeling:** A service platform should have a reference model of “acceptable” usage behavior and platform utilization so that it possible to detected abnormalities or increased system load.
- ▶ **A reference model:** Of the service platform should be available to test updates and new features outside of the live customer facing service .
- ▶ **Feature specifications:** To be able to support the specified use-cases.



Dynamic considerations

These are factors for the service ‘in motion.’ When a user requests a service, the service platform interrogates business rules and service parameters, and then grants or denies the request based on business rules. The response to the user request is facilitated by the kinds of considerations listed above, which are built into the platform.



Service requests

Usage requests and the users making them should be verified and authenticated.

- ▶ Usage sessions need to be opened, monitored, and closed in an orderly fashion.
- ▶ Technical measures should be put in place to protect the service platform from attempts to spoof a device's identity and thus gain access to a content type/tier it is not authorized to access.

Anomalous requests

The platform should be provisioned to ‘model the typical subscriber, as a reflection of business terms and considerations such as those listed earlier. Volumes and types of requests need to be monitored and alarms raised when events outside of baseline normal behavior is detected.

An alarming/monitoring service should be enabled on the platform to identify and alert out-of-normal situations while in service. These alerts should at minimum include:

- ▶ **Number of devices:** Allowing account holders to use a defined number of simultaneously active devices. Detecting sudden changes in the range or number of devices associated with an account.
- ▶ **Allowed devices:** To permit delivery to specific types of devices (e.g. HD STBs and streaming devices, but not smartphones).
- ▶ **Location of use:** To recognize attempts to access services from unrecognized or un-licensed locations.
- ▶ **Registered devices:** To detect when someone whose device is not registered in a subscriber's household attempts to watch a program - with or without access credentials.
- ▶ **Anomalous service usage:** For example spikes in service access or excessive license requests in a short period of time.
- ▶ **Malformed license and authentication request** with verbose logging to enable subsequent analysis.
- ▶ **Requests for content** that isn't yet released but may be staged on the system.
- ▶ **Anomalous content attempts:** For example, attempted requests through broken or nonexistent links (the equivalent of a Web '404')
- ▶ **Unrecognized IP address** ranges, VPN links, or unrecognized NAT-ted addresses.

...and others

Mitigation considerations

- ▶ An operator should as a minimum have worked through a basic set of scenarios that it considers likely on its service and document its planned responses.
- ▶ Implement and document countermeasures that conform to terms of use, and if it's a distributor, the terms of a distribution agreement.



Considerations that apply to the operation of the platform

- ▶ **Operational load balancing:** Tools and capabilities like scheduling of additional capacity should be designed into a platform to monitor the performance and adjust (manually or automatically) where necessary such that peak loading is handled smoothly. Care should be taken to test and confirm capabilities offered from a technology provider are fit for purpose i.e. allowing a cloud solution to auto scale may be to slow for peak demand from a sports event.
- ▶ **Disaster Recover (DR) & failovers:** Business rules should define the acceptable behaviour of these capabilities, however the architecture should be constructed such that resilience is built in and allow smooth transition to a DR solution and back again. Scheduling and testing of these capabilities are essential if they are to work seamlessly with today's complex solutions.
- ▶ **Geographic Separation:** Ensure geographic separation of data where possible to mitigate against localized failures
- ▶ **Penetration Testing (aka Pen Testing):** Ensure that all service platforms and components are penetration tested ahead of use in service and schedule annual testing to ensure continued security.

Management considerations

- ▶ An executive sponsor should be designated within the service platforms business unit who has sufficient seniority and budget that can drive the security ethos within their organization. Examples of this would be a CTO or board member that can influence budget and company methodology.
- ▶ Procedures should be implemented around operations, personnel roles, and escalation alternatives.
- ▶ Document these procedures and schedule annual reviews to ensure they remain current and viable.
- ▶ Conduct regular documented reviews of operational data. For example, to compare revenue/subscribers against usage to look for abnormal behavior and investigate findings promptly.



8 Technical Best Practices

Video providers that have taken the time and made the effort to identify security risks and the considerations around resolving them should spare no effort in selecting the technologies and implementing the practices that best address those risks and considerations in production deployment. Here, we provide a range of considerations with the hope that it may help with that alignment process. The video provider should also document a roadmap that bridges between the platform currently deployed and the needs of the foreseeable future.

Contractual obligations

- ▶ The Contractual licensing of the content should drive the technical usage rules adopted by the operator with a documented formal business process in place which clearly articulates the technology rules implemented as these may need to be rationalized when content is sourced from multiple licensors.
- ▶ Where multiple platform or services are operated a single entity within the business should implement technical and operational processes that ease compliance with business rules.
- ▶ Business rules should be considered a variable component of the service platform and business logic SHOULD NOT be hardcoded.

Service requests

- ▶ Once a client device is authenticated, the operator's system should securely store the device's capabilities against the business rules such that when the device requests access to content it will only be served up content within its approved capabilities. i.e. if an old web browser has been classified in the Business Rules to only be allowed to consume SD content it MUST NOT be passed a DRM KEY, Manifest or URL which points to or contains any links to anything higher than SD.
- ▶ URLs, file names and services should employ obfuscated names such that access to files or services which may point to higher level of content cannot be easily guessed. Location information (IP addresses) should be virtualized and not direct.
- ▶ Technical measures should be put in place to protect the service platform from attempts to spoof a device's identity and thus gain access to a content type/tier it is not authorized to access.
- ▶ Consider the viability of security mechanisms that create virtual traps that lure attackers, sometimes known as 'honey pots,' which are created intentionally to allow attackers to access data or service so you can study them to improve your security policies. Honey pots are designed to direct service requests by attackers to verbose monitored services, which in turn trigger alarms within the service platform to indicate an attack may be underway.
- ▶ Manifest obfuscation is not considered a suitable method of device tiering.



Release windows

- ▶ In cases where content has a defined release window and the operator has been allowed to process the content ahead of the release window, the service must not publish, move or otherwise make the content accessible via any means before the release window.
- ▶ Availability dates MUST be enforced by the DRM technology, CDN and all appropriate service components that make up the operator's platform.

Concurrency

- ▶ The service platform should maintain an accurate record of the number of devices that are consuming content at any given instance such that.
- ▶ New requests to access content are validated against the service platform to ensure business rules will remain compliant if a new play request is granted.

Static platform practices

A variety of considerations should be made for the service platform "at rest": where the platform is built and deemed ready for testing and later production use. These practices help video providers build security into their platforms from the start, and not retrofitted at a later date. Experienced operators know that retrofitting can be expensive and is often disruptive to a system "in motion."

These considerations include device management, output protection, session management.

Device management

Consumer devices should be registered to the operator's system where possible. Checks should be performed at registration, authentication, and content consumption to ensure that the device is:

- ▶ An allowed approved device.
- ▶ Running an operating system at or above the defined minimum software version.
- ▶ Running a player or browser at or above the defined minimum software version.
- ▶ Operating a DRM/CDM client at or above the defined minimum software version.

Another factor in honoring business rules is to match services to device profiles. For example, if a rule has been set to limit delivery to an outdated browser to SD only, and an old web browser is detected, the platform should be blocked from passing a DRM KEY, Manifest or URL that links to anything higher than SD.



Hardware protection

Once content has been delivered to a consuming device it must honor both the output requirements set by the licensee and that of the DRM license with respect to copy protection technologies. As such the consuming devices should be tested as part of the acceptance into service process to ensure that:

- ▶ HDMI outputs are allowed or disabled as required.
- ▶ HDCP of the correct version is being applied as required and hot plugging does not bypass these settings.
- ▶ The ability for a device to screen record or take screen shots/photos is disabled.
- ▶ The ability for a device to cast, mirror or otherwise pass content off to another device is disabled or operating within the bounds of the contractual license i.e., Airplay, Chromecast.

While analog outputs are somewhat a thing of the past where a contractual obligation exists to use a defined protection system or constrain the maximum resolution it must be implemented.

Another consideration is in the heart of the device - the runtime environment, which consists of the device's processor chipset and memory. If app protection is not in place, an attacker might be able to discern points in the secure video pipeline from which they can extract data.

The moral here is to never trust the device. A chip supplier may say that the next generation will address a current issue, but hardware development is notorious for long lead-times, and by the time a corrected device hits the market, there may be new risks. Pirates attack devices to detect vulnerabilities, which is the justification for app protection, discussed below.

Robustness rules

These are KPIs that a licensee can be held to account for implementing them "to spec". For a solution to remain secure, all of the components within it need to be trusted and implemented in a secure, robust manor. For consuming (client) devices, this used to be largely under the control of the operator when they provided the STB and had oversight of all of its components. However in today's world where the consumer generally owns the hardware and the environment is shared as applications within an operating system this is rarely possible. For this reason its essential that steps are taken to ensure that any player or app implements the security providers rules with regards robustness. It is no longer best practice to just use an approved DRM and player, the solution needs to look at the complete client environment to ensure security.

- ▶ For each consuming device the operator MUST maintain documented evidence that the device implementation meets these robustness rules.
 - ▶ To protect against API attacks and the weaponization of mobile apps, it is important for broadcasters and pay TV operators to implement robust security measures such as encryption, authentication, and access controls. They should also regularly assess the security of their payment processing connections and mobile apps to identify and address any vulnerabilities.
- Examples include:
- An up-to-date certificate from the technology vendor or where the technology vendor supports self-certification - the completed control/check list.
 - A 3rd party audit of the device.
 - ▶ The best practices within "App protection" should be employed where technically possible.

Video providers should regularly review operational data/logs to look for abnormal behavior that should be investigated.

Forensic watermarking

Operators should consider the use of a distributor forensic watermarking (a single watermark applied to all content passing through the service platform) for content that is distributed via their service.

- ▶ Where content is deemed high value, an additional watermark should be applied to identify the individual device and/or consumer session.
- ▶ The forensic watermark must be applied in a secure manner. Such watermark should be from a technology provider that has been approved by the content owner.



App protection

Security does not stop with protecting the content. Part of protecting the end-to-end service is to implement app shielding technologies.

Benefits include:

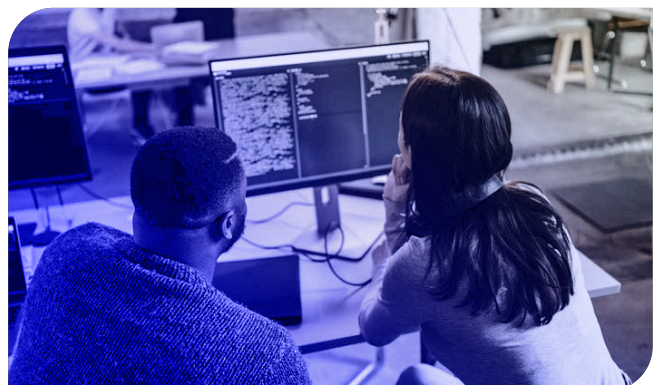
- ▶ Protect the app by obfuscating its code such that it cannot be easily reverse-engineered.
- ▶ Protect the device by checking that it has not been modified or altered by techniques such as jailbreaking and rooting.
- ▶ Protecting the software from tampering, and to detect attempts at tampering.
- ▶ Detect and prevent attacks at runtime, including memory access, emulator/debugger prevention.
- ▶ Data encryption to foil attempts to steal data traveling through the app and at rest.
- ▶ Implemented according to the device and OS environment guidelines and always sign an app in such a way so as to stop it being altered and re-signed.

Some app protection techniques simply place a 'wrapper' around the app, but leave the app itself largely untouched. Anything that is wrapped, can be unwrapped. Another approach is to modify the app itself in such a way that the components within the app look the same to an attacker and therefore can't be discerned or penetrated - making the app more attack-resistant.

Service delivery infrastructure

How servers should be built and maintained, and the benefits of moving to cloud/platform:

- ▶ A defined process must be in place to grant, modify or revoke access credentials to the service platform which should be audited.
- ▶ Where cloud or 3rd party components/services are used:
 - Service level agreements (SLAs) or contracts and or contracts must exist and it's the service platform operator who needs to ensure these meet the design requirements.
 - Root level access credentials should be held only by very senior personnel within the service platform.
 - Reviews of users with administrator access should be conducted regularly.



Further housekeeping considerations

- ▶ A defined process must be in place to grant, modify or revoke access credentials to the service platform which should be audited.
- ▶ All infrastructure should undergo an acceptance into service process to confirm it meets business and operational requirements.
- ▶ Geo resilience and redundancy should always form part of the design.
- ▶ Images and backups should be maintained for the service.
- ▶ System restoration and disaster mitigation processes should be documented and tested at least annually.
- ▶ Reference environments should be maintained for testing.

Dynamic security practices

A variety of security practices apply to the video platform “in motion” – e.g., in production operation. In addition to overseeing basic service access requests and associating requests and sessions with users, they include watching for attempted breaches, and monitoring for anomalous use.

User authentication is one of the foundations of service access. While it is commonplace to look carefully at the DRM and security solutions, its often a case that the authentication to a service platform is weak or exposes easy to exploit vulnerabilities. The key takeaway here is that there is little point building a strong vault if you give the keys to anyone that asks.

Even when video providers have DRM and token-based authentication in place, they should engage in some basic practices around keys and tokens, such as frequent key rotation and different keys for different quality-levels of the same content so it only plays on an intended device.

And yet, even despite these practices, pirates can still circumvent or steal tokens, steal content via native DRM exploits, skip ads within the media app.

Adverse consequences include:

- ▶ CDN leaking content to pirates, inflating content distribution costs because operators are paying for pirated content over their networks.
- ▶ Revenue loss when subscribers don't renew or signup (because they left and paid for a pirate service instead), or due to loss of ad revenue.
- ▶ Real customers having a bad user experience – often locked out of their own subscriptions and unable to view content.

All of these are reasons why piracy and the associated revenue loss are increasing and not decreasing.



Encryption: Key rotation, random number generator best practices

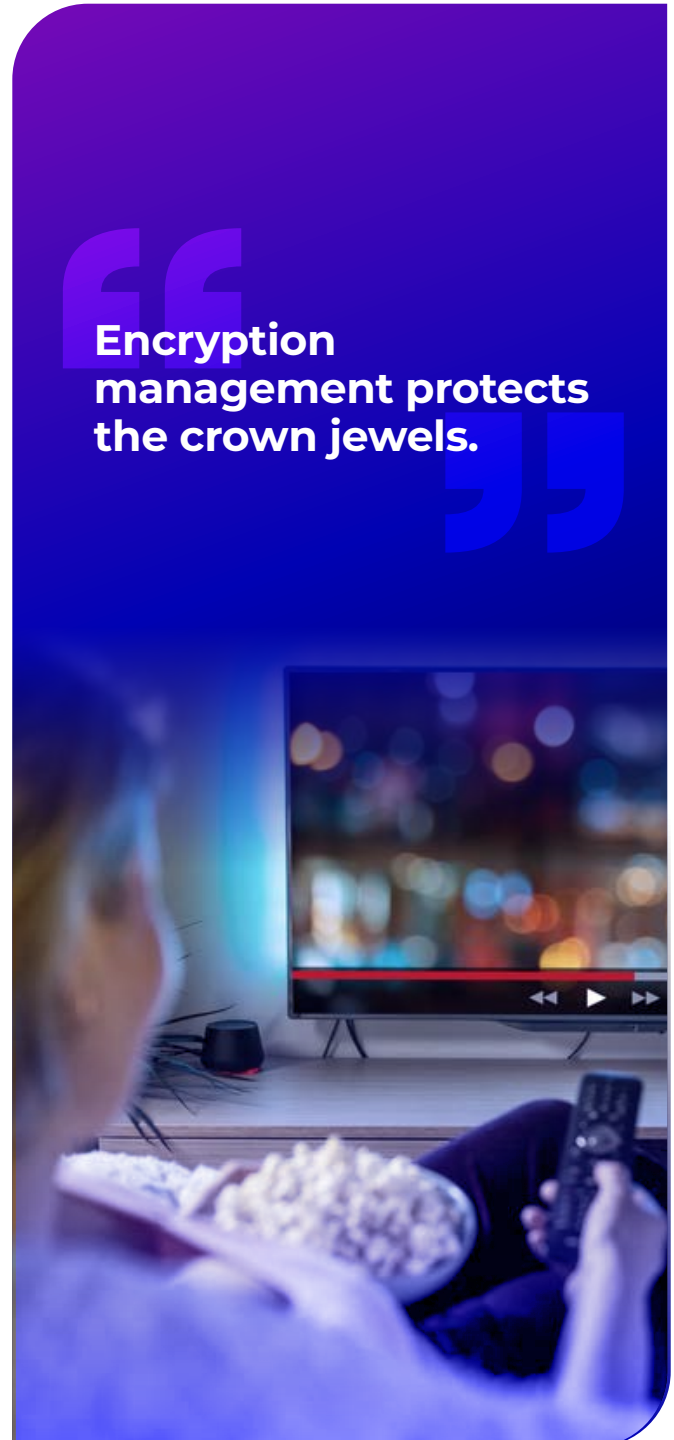
Token-based authentication was supposed to be the holy grail of DRM security gaps and solve everything but it didn't. And not all DRM suppliers seem to be addressing recent security vulnerabilities.

For on-demand

- ▶ Each asset needs to be encrypted with its own key. Where the service offers multiple tiers of content quality such as SD/HD/4k/HDR, each rendition should be encrypted with a separate key to the lower renditions such that if the lower quality key is compromised, it does not also give access to the higher quality content.
- ▶ The seed used for the encryption of the asset should be originated from a hardware (or Cloud equivalent) random number generator that meets or exceeds NIST 800-90A.

For live

- ▶ Each linear channel needs to be encrypted with its own key.
- ▶ Where the service offers multiple tiers of content quality such as SD/HD/ 4k /HDR each rendition should be encrypted with a separate key to the lower renditions such that if the lower quality key is compromised, it does not also give access to the higher quality content.
- ▶ The seed used for the encryption of the asset should be originated from a hardware (or Cloud equivalent) random number generators that meets or exceeds NIST 800-90A.
- ▶ Keys should be rotated frequently and a balance between the events duration and potential impacts on the user experience considered. By default a 4 hour rotation would be a minimum expectation.



Encryption management protects the crown jewels.

DRM proxies have come into widespread use among Multi DRM and SaaS solutions. While their use eases integration, great care is needed with respect to client authentication and communication in the service platform to ensure that the DRM proxy does not become the weak link in gaining access to content.

A no-proxy model can help to ensure that subscriber devices are always trusted and entitled to the content. This approach reduces the possibility that client devices might bypass security tokens if clients hit the proxy directly.

To ensure this is the case, the operator should assess the suitability of the following techniques:

- ▶ Only expose/open required ports/services needed by the proxy server
- ▶ Building strong client identity validation schemes that can operate on each request received
- ▶ Build capabilities to reject and or throttle malformed requests
- ▶ Build capabilities to feed logs/usage data into an alarming/monitoring service
- ▶ Authentication via hardware-linked certificate or similar where it is supported
- ▶ The use of certificates
- ▶ Strong single use tokens for client and proxy authentication
- ▶ Strong TLS protocols between client and proxy
- ▶ Time bound communications between client and proxy (max 20mins recommended for each interaction)
- ▶ Request limits between client and proxy
- ▶ Verbose login of proxy operation
- ▶ Regular reviewing of proxy logs
- ▶ Dedicated communication paths with strong encryption between the proxy and DRM server

Tokens: Handle with care

While the introduction of tokens several years ago initially closed gaps in the authentication chain, piracy has evolved to stealing and abusing tokens. Token-based authentication piracy now poses a significant threat to VOD/OTT security as it allows unauthorized access to protected content.

Effective measures must be implemented to protect the authentication of the viewer's authorization to access the requested content. Where a service architecture is such that multiple services (often provided by different entities are used) need to communicate over the open internet it is best practice to:

- ▶ Ensure all communications are encrypted with transport layer (TLS 1.3) or higher.
- ▶ All communications must be authenticated before responding to the request.
- ▶ Where token type authentication is used, the requirements should match or exceed that of the "Proxies" section.
- ▶ Employ techniques to ensure token cannot be stolen and reused.
- ▶ Employ techniques to ensure the use of tokens cannot be spoofed or stolen.
- ▶ Where tokens or security sensitive information is stored (even transiently) it is never stored in the clear and steps are taken to obfuscate and scramble information of this nature.
- ▶ Never assume the client devices operating system provides adequate isolation and security.

Platform monitoring

The service platform should be equipped with an industry standard alarming and monitoring service that presents a view to real time Network Operations Centre (NOC).

- ▶ Build alarming and monitoring capabilities into all service platform components and client devices from origination of the service.
- ▶ Define standard usage and benchmarks for all service platform components and client devices.
- ▶ Define alarming, logging and alerting levels for all service platform components.

Geofiltering/VPN detection

To ensure that obligations defined within the contractual license and business rules can be applied, an approved industry standard technology must be used to determine a devices location at

- ▶ Service setup
- ▶ Payment
- ▶ Authentication
- ▶ Content consumption

The chosen technology solution **MUST** be regularly updated (at least weekly) with new data such that it maintains a high degree of accuracy. Where a service is provided in the cloud or SaaS, it's the responsibility of the licensee to obtain documented evidence from the technology provider with respect to updates of the database.

A clear definition of when the checks take place and what proportion of data/packets are checked should be documented and agreed with the content owner at the design stage.

Operational data/logs should be reviewed to look for anomalous (out of the normal) behavior, and investigated. To place the video provider in a position to do this, it must have a benchmark model of permitted behaviors and activity ranges, so out-of-range parameters can send alarms.



Mitigation practices

As part of the service establishment process a clear set of mitigation scenarios should be defined and documented. Video providers should be sensitive towards maintaining a balance between consumer friendliness and use-case enforcement. For example, if suspicious activity on a subscriber account is detected, it may be sufficient to request that the subscriber enable two-factor authentication (2FA) and log in again, rather than de-registering their device. 2FA reduces the likelihood that a criminal actor could further access the account.

Consumer-facing countermeasures

A range of countermeasures can be considered in response to anomalous behavior

► Further analysis

- Flag for additional monitoring
- Turn on forensic watermarking
- Increased logging
- No perceived impact on customer

► Light touch interventions

- Force visible on-screen identifiers
- Turn on or increase strength of forensic watermarking
- Degrade service to SD
- Require the user to set up 2FA
- Require the user to log in again
- Present the user with a marketing offer, to capture potential revenue

► Disruptive interventions

- Disrupt the video (Black holes / UI pop ups)
- De-register the device from the account
- Disable the user account and notify the user to re-confirm registration

Maintaining the fine balance between consumer-friendliness and bussiness requirements.



Infrastructure protection practices

Implement an internal program to define privilege levels and assign all users to a set of privileges that align with their duties. Register internal users of the service platform, such as engineers, customer service agents, field service technicians, and others, according to their privilege levels.

Record internal usage activity so that internal breaches can be traced to their origins – which may have been caused by an internal user.

Video providers should include security requirements and performance metrics in any RFPs that are presented to vendors. Any vendor responding to the RFP should be required to respond explicitly to any KPIs in any requirements document.



Secure coding practices

Under the premise that service protection should extend to the video provider's infrastructure and the software that enables it, it's important to take precautions against malicious activity against software

- ▶ Where code may reside outside of secure locations (like client applications), the implementations should at a minimum:
 - Perform root and jailbreak detection
 - Code should be obfuscated, shielded and scrambled such that it cannot easily be viewed or modified
- ▶ Careful design of client application should be undertaken such that the client does not reveal sensitive information related to the service platform and its operation. It is often overlooked but the client may be a source of information related to the service platform or operator and not the focus of an attack itself.
- ▶ Service platforms and Clients should be designed such that, where practical the service which the client interacts with only exposes interfaces relevant to it. For example a client video app may not need to connect to the billing/payment service if this is handled only via a website or call center.

9 Operational Best Practices

Service operators should treat piracy as a real threat, and allocate budget and resources to security initiatives that counter it. It's a best practice to consider security monitoring from both internal and external perspectives.



Internal security monitoring

Video providers should implement a Network Operations Center (NOC), specific to piracy detection and anti-piracy, or to complement an existing NOC. There are several best practices that a Network Operations Center (NOC) can follow to effectively detect and prevent piracy:

- ▶ **Implement strict access controls:** NOCs should have strict access controls in place to ensure that only authorized personnel have access to the network and its resources. This helps to prevent unauthorized access and potential "insider" piracy.
- ▶ **Monitor network activity:** NOCs should continuously monitor network activity to detect any suspicious activity that could potentially be related to piracy. This includes monitoring for unusual traffic patterns, unauthorized access attempts, and any other anomalies that could indicate a potential threat.
- ▶ **Utilize both anti-piracy and cybersecurity tools to protect, prevent, predict and respond to threats:** NOCs should utilize a variety of security tools and technologies, such as firewalls, intrusion prevention systems, antivirus software, DRM, watermarking, anti-piracy, endpoint and mobile threat defense, to protect the network and its resources from potential threats.
- ▶ **Take advantage of internal or outsourced data science teams** working with new AI/ML tools to detect piracy attack patterns, in the pursuit of prediction and prevention of piracy and hacking.
- ▶ **Regularly update software and systems:** NOCs should ensure that all software and systems are regularly updated with the latest security patches and updates to protect against known vulnerabilities that could be exploited by pirates.
- ▶ **Conduct regular security assessments:** NOCs should conduct regular security assessments to identify any vulnerabilities or weaknesses in the network and implement necessary measures to mitigate those risks.
- ▶ **Have a response plan in place:** NOCs should have a well-defined response plan in place to handle any potential piracy threats that are detected. This should include procedures for containing the threat, identifying the source of the threat, and implementing remediation measures to prevent future incidents.
- ▶ **Testing & Validation:** Implement a test lab specific to piracy, to reproduce and isolate errors, manage software and systems updates; or complement the existing lab.
- ▶ **Failover:** Systems and software configurations should be saved, backed up and documented. Backups and spares should be available to allow rapid rebuilding if needed.

By following these best practices, NOCs can effectively detect and prevent piracy and protect their networks and resources from potential threats.

Security policy administration

Designate a responsible party to meet measurable success metrics. The video provider should assign a lead anti-piracy member within its team whose objective is to:

- ▶ Increase awareness within their company as to the scale of piracy.
- ▶ Designate a dedicated program manager for anti-piracy and provide a single point of contact for piracy-related communications.
- ▶ Report into executive/content rights teams the levels of piracy at least every 6 months.
- ▶ Manage the internal or external anti-piracy capability.
- ▶ Implement role-based administration with permissions and parameters for each role: Super-admin, admin, department-level, individual level, security level.



Administrative processes

The standardized review process should be put into place, including:

- ▶ Acceptance testing should be carried out before new service platform elements and clients are placed into service to ensure all the security and business requirements have been met.
- ▶ All changes to a service platform should undergo a security review which should define if retesting/validation of security functionality is required. Such reviews should be documented.
- ▶ At least annually the service platform and its approved consumer devices should be revalidated to ensure security functionality is still functioning as per design.
- ▶ Licensees should consider biannually a 3rd party review of the service platforms configuration and operation with respect to security functionality.
- ▶ Develop test procedures, to ensure compatibility with new software versions, new systems components; perform regression testing.

Documentation

- ▶ The service platform itself should have clear documentation with respect to topology, design and process flows.
- ▶ Develop as-built documentation: Standard bills-of-materials.
- ▶ Maintain a reference resource for versions in place and update plans.
- ▶ Implement a reference resource for “adds, moves and changes”
- ▶ Identify and document error thresholds.
- ▶ Operational process flows should be fully documented, including authentication, session management and inter-process communication.
- ▶ Error-handling processes should be documented, including problem escalation procedures.
- ▶ In situations where cloud or 3rd party components/services are used, documentation must be obtained by the service platform operator to confirm the capabilities of the 3rd party meet the design requirements.



External security/ Anti-piracy monitoring

The manager of the service platform, which may also be a 3rd party professional services organisation, should proactively search the open internet and other entities for content that has originated from your service platform.

The results of monitoring should be reported on a regular basis, including:

- ▶ Volume of content pirated from the service platform.
- ▶ Data related to the entity pirating (service name, URL, territory).
- ▶ Linking or other methods by which the pirates promote their service.
- ▶ Payment mechanism used.

Services will take proactive measures to reduce piracy from the service platform by at a minimum:

- ▶ Operate commercially available interfaces to remove content from compliant platforms.
- ▶ Submitting cease and desist notices to the hosting provider.
- ▶ De-listing from search engines / app stores.

Services will consider the following activities:

- ▶ Legal actions.
- ▶ Technical counter measures to remove content.
- ▶ Where supported provide data that allows the service platform to disable the offending user.

10 Key Takeaways

Readers should now see that video delivery consists of a multitude of interdependent components and processes, that real security requires an ecosystem approach, and that off-the-shelf security solutions need to be implemented carefully to ensure good end-to-end security.

While DRM has the capability to add security to a video platform, full security can only be realized by carefully considering the design of the overall solution which must consider strong robust implementations of all the service components. Furthermore, while DRM itself has a lot of potential, implementing it “out of the box”, may not provide optimal security. Video providers should be cautious of multi-DRM solutions that tout simplicity as an advantage, as they may not be sufficiently robust in their default configuration to meet stringent content requirements.

Some technologies have natural complements. One example is to match DRM in combination with forensic watermarking. Another is to implement software protection not only to defend the execution environment, but also to complement DRM by obfuscating keys and the key-exchange process.

Moving solutions to the cloud is often a logical progression, but the onus is on the designer and operator of the platform to ensure security and integrity is maintained. Always ensure documentation from technology providers exist to confirm how a solution works or needs to be configured to ensure it’s secure. Don’t just accept default settings/parameters.

- ▶ Anti-piracy monitoring provides a real-world insight of how well your security is performing.
- ▶ Piracy monitoring can provide valuable business insights into products and services that the consumers are seeking, but may not be available legitimately.
- ▶ You don’t always have to spend on new infrastructure – you can make improvements by doing audits, identifying gaps, seeing if you can apply what you have.

Another takeaway is that security is an evolving process that takes time and patience. For example, vendors can claim that the next generation will use new chipsets with better hardware security. But hardware development has long lead-times, and by the time a corrected device hits the market, there may be new risks. Fortunately, forensic watermarking is another way to associate a device with services and content, to provide an audit trail in cases where content was suspected of having been stolen.



11 Conclusions and Recommendations

This Guide has presented a sufficiently broad range of concepts and practices that finding the right place to start might pose a challenge. With that in mind, we close with some organizing thoughts.

Is your service platform current, documented, secure and supportable?

Video providers should conduct a careful survey that revisits their technical requirements, based on the business requirements and market conditions that they currently face and then work their way 'backwards' to define the infrastructure, service flows, security technologies, countermeasures and best practices that they actually put in place to frame the resulting service.

We recommend that video providers begin by re-familiarizing themselves with their existing service platforms, and comparing the systems in production use with the goals and objectives of the business.

A complete and careful (re)evaluation can enhance security before any incremental security investments are made. Areas to evaluate include:

- ▶ **Architecture:** Are current systems elements all known? Are they secure? In construction and as architecture, does it support the business rules set down by your content suppliers? With the platform's feature roadmap? With company objectives? With current regulation?
- ▶ **As-built:** Is the full end-to-end platform documented sufficiently as a reference for those who operate it? Do you track the current versions of every element in the platform, and the versions of its software?
- ▶ **Testing:** Is there an available lab system, separate from the production platform, where problems can be tested and analyzed for correction? Is the lab used to test all of the advertised service use-cases? Are software updates tested before being implemented in the production platform? Is it used to prove-in a new hardware platform? Are newly-introduced devices tested for compatibility with your apps and do they enable end-users to operate the features without error?
- ▶ **In-production use:** As a service delivery platform, are the sources and destinations known and are they secure? Are the interchange points across the platform (APIs) correctly implemented? When a session is opened, does the platform check whether the request is from a known or knowable source? Are user sessions managed and ended in a tidy fashion?
- ▶ **Housekeeping:** Is support adequate, for end users, for customer service, for engineers? Are service and request flows documented and tested? Is there a 'data dictionary' for metadata, so the platform is understood consistently by all who use it? Are errors logged?
- ▶ **Vendor evaluation criteria:** Does the video provider develop formal requirements documents for vendors that clearly describe the service, its business requirements and its technical and supportability requirements. Does the video provider run a formal RFP process that includes lab testing of proposed solutions?
- ▶ **Content supplier requirements:** Do suppliers recognize or insist upon KPIs, practices for DRM?

Some of these are self-evident but we are often surprised when they are not in place in large-scale deployments.

Are current security measures and countermeasures adequate?


While streaming services have been more of a focus in this Guide, Pay TV operators should ensure that not only their streaming platforms are secure and correctly implemented, but they also should survey their set-top box installed-base and their CAS for any needs there. Should they retire or limit services to old Customer Premise Equipment, update its software – including security clients – or cap-and-grow by ending the deployment of certain devices and starting new subscribers (for example) with more recent or otherwise more-appropriate solutions.

There seems to be a conventional wisdom about DRM in the fight against piracy. These assumptions should be re-visited:

- ▶ While DRM uses advanced encryption standards and specialized techniques to securely store and deliver encryption/decryption keys, most native DRMs do not include end-user authentication. This authentication is usually added by multi-DRM systems, many of which use tokenization to mediate the authentication required.
- ▶ Tokenization has closed gaps in the authentication process by mediating the authentication of end users between different components of a playout system. But because pirates can intercept tokens, token-based authentication piracy has come to pose a significant threat to VOD/OTT security by allowing unauthorized access to protected content.
- ▶ The third, watermarking, complements DRM to help track and identify the original consumer of content. In addition, watermarking can also be used to trace video back to the individual responsible for suspected theft by assigning a unique watermark to the session or instance.

Even when operators have DRM plus token-based authentication in place, and even when operators follow best practices – rotating keys frequently, separating keys for all content types, restricting high-quality content to protected devices – pirates are still able to:

- ▶ Steal tokens
- ▶ Steal content via native DRM exploits
- ▶ Replace ads within the CDM/media app



It's time to revisit some long-standing assumptions about DRM and its role in security.

The impacts associated to pirate activity may be:

- ▶ A potentially broken end-user experience, in which they could be locked out of their own subscriptions and unable to view content.
- ▶ Revenue loss when subscribers don't renew or signup (because they left and paid for a pirate service instead), or due to loss of ad revenue.
- ▶ CDNs leaking content to pirates, inflating content distribution costs because operators are paying for pirated content over their networks.

Effective measures must be implemented to protect the authentication of the viewer's authorization to access the requested content.



The security roadmap

This Guide has described security as an end-to-end concern that DRM alone doesn't fully address. Video providers should take a serious look at the full range of vulnerabilities described herein and consider how they should be prioritized and staged for implementation. If the video provider designates a single point of responsibility with executive sponsorship, that person should drive this effort.

Security enhancements beyond CAS and DRM include:

- ▶ Strengthening DRM with complementary solutions such as watermarking.
- ▶ Software protection to obfuscate keys, key-exchange, and the execution environment.
- ▶ Leverage non-security technologies such as AI/ML, analytics, automation, etc.
- ▶ Mobile app security and device security.
- ▶ Network and API security.

It's also key to recognize the evolving nature of security threats, and apply critical thinking to determine which ones are truly important and which others may be red herrings before making security investments. The emerging security risks and threats to video producers and distributors are real and they are constantly evolving.

12 Closing Thoughts

We hope that this guide has provided valuable information and insights on how to navigate the DRM ecosystem and implement best practices for protecting your digital content. By following the guidelines outlined in this document, you can ensure that your content is secure and accessible to your intended audience. We believe that by following these best practices, you'll be able to confidently and successfully navigate the DRM landscape, knowing that your valuable digital assets are protected. We are confident that you will be able to enjoy the peace of mind that comes with knowing your digital assets are secure.

13 About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners get to market faster, scale easily, protect valuable revenue streams, and win new business.

Visit www.verimatrix.com.

