FROST & SULLIVAN

Total Cost of Ownership: The Key Metric for Multi-DRM Strategy

As Multi-DRM Becomes the Norm, Buy is a Smarter Strategy than Build

INTRODUCTION

Digital rights management (DRM) systems are designed to protect content and revenue streams from piracy. DRM systems are most effective when they simultaneously deliver robust security and a transparent user experience. Creating a managed content experience on unmanaged devices with over-the-top (OTT) streaming is critical to the success of an online service. Achieving a high level of success with online services is becoming increasingly urgent as TV Everywhere and OTT continue to see exhilarating growth at the expense of conventional pay TV. The profitability and growth of content businesses are thus heavily dependent on getting their monetization components right. **Well-designed DRM literally and figuratively holds the key to unlocking a best-in-class online content service.** **Tweet this!**

2015 was a noteworthy year, our research finds, as the number of pay TV households in the United States fell across the board, while online video service subscribers continued to grow at a strong double-digit pace. Broadcasters have found that online on-demand views are reaching parity with traditional linear views. Video service operators, including pay TV service providers, online video service providers, and broadcasters, are collectively moving toward delivering more content at higher resolutions online. Accordingly, there is increasing need to move away from simpler streaming encryption solutions and adopt full-fledged DRM protection.

This paper captures our insights based on the typical process and value judgement that companies go through as they seek to build their own anti-piracy infrastructure, and provides best-practice guidance on deploying secure content services that provide consistent, compelling user experiences across all devices and consumption scenarios.

DRM: A BUSINESS-CRITICAL PROGRAM

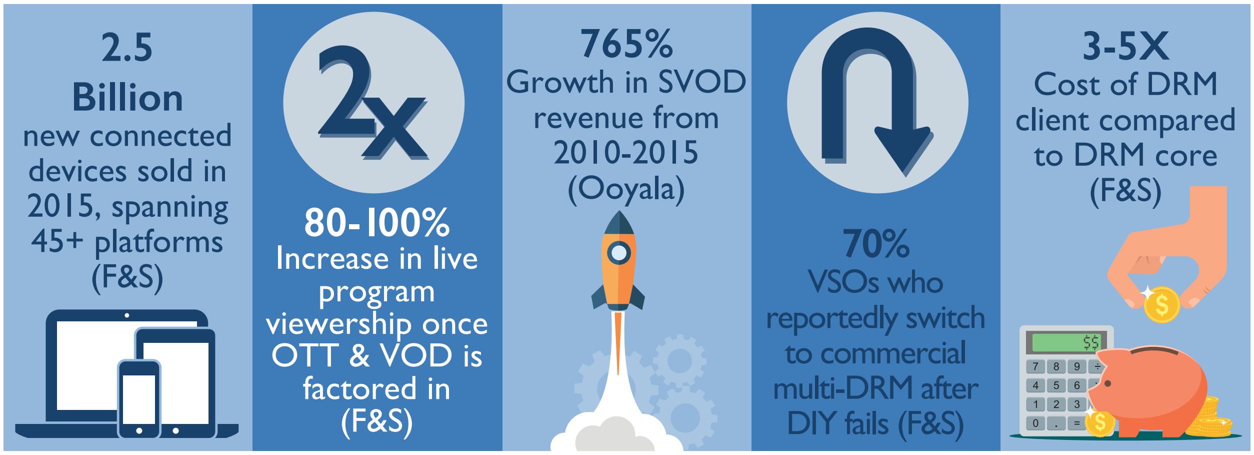
Video service operators (VSOs) are immensely pressured to counter the cord-cutting juggernaut and to harness the elusive monetization potential of online consumption. As a result, there is often an internal rush to quickly roll out an online service through an app and/or through a Web browser. As VSOs seek to emulate the success and growth of Netflix, for example, they often underestimate the complexity of building and consistently maintaining secure players across a diverse mix of hardware and software platforms. As OTT workflows are outsourced to online video platform (OVP) vendors and managed service providers, these companies are often making the same underestimations themselves.

At present, Frost & Sullivan finds limited understanding of the true levels of cost and complexity associated with a do-it-yourself approach to DRM. Teams often focus on the initial rollout of the service and fail to fully anticipate the effort or difficulty of maintaining security on an ongoing basis in the face of growing pressure from hackers and in the face of new technology advances.[1] Ongoing maintenance and enhancement of DRM implementations is a formidable challenge that requires specialized experience if it is to be handled effectively and in a cost-efficient manner.

Frost & Sullivan research reveals that the perceived high cost of a commercial DRM system and perceived low complexity of building DRM in-house are compelling well over half of video service operators and OVPs today to attempt to build their own security platforms. This in-house approach is often driven by the consideration of secure playback as a checkbox required to gain content rights or meet licensing regulations, rather than as a business-critical component that provides differentiation and profitability. While this may seem like a good short-term tactic, it is rarely an effective long-term strategy.

[1] The Future of Cardless Broadcast Security, A Farncombe White Paper

Figure 1: The Story in Numbers for DRM-secured OTT Content



2.5 Billion new connected devices sold in 2015, spanning 45+ platforms (F&S)

80-100% Increase in live program viewership once OTT & VOD is factored in (F&S)

765% Growth in SVOD revenue from 2010-2015 (Ooyala)

70% VSOs who reportedly switch to commercial multi-DRM after DIY fails (F&S)

3-5X Cost of DRM client compared to DRM core (F&S)

ASPECTS OF TOTAL COST OF OWNERSHIP FOR DRM

The total cost of ownership (TCO) of a DRM system includes capital expenditure (CAPEX) and operational expenditure (OPEX) aspects. Unlike many software systems, the OPEX aspect of TCO relates to a far more significant chunk of security products due to an inevitable arms race against hackers and the constantly growing value of content. In the case of DRM, CAPEX itself is a recurring expense as new devices enter the market and new technologies supersede older ones. As DRM underlies all content business models, a lack of agility in updating and adapting the DRM layer also results in reduced revenue and lost subscribers.

The basic issue with building a security infrastructure in-house is that VSOs are faced with having to create and permanently fund a dedicated product management, development and testing team with competency in security. As a result, VSOs are committing themselves to a significant ongoing R&D investment in maintaining and expanding the secure playback and monetization platform. Tasks for these engineering and testing resources include continuously updating the enforcement layer, testing updates, and distributing them to all current **and past** devices and platforms that are deployed in the service's customer base.

In contrast, a specialized multi-DRM vendor has core competency in cross-platform, cross-DRM development. Since multi-DRM specialists can amortize development and upgrade costs across a number of customers, savings can be passed on to customers. Accordingly, with a high-quality commercial solution, VSOs can expect stronger protection, more scalable infrastructure, and significantly more agile services than what could be built and maintained in-house for a comparable investment. Taking the longer-term view, multi-DRM vendors are proactively aware of changing standards for encryption standards, decryption protocols, streaming technologies and more—lifting that burden off of individual service providers and abstracting underlying complexity in a unified, easily integrated interface.

For most VSOs, partnering with a multi-DRM solution provider makes sense simply from core competency and business agility points of view. A dollars-and-cents analysis, in terms of TCO, further justifies this approach. The need for business agility in the face of trends such as growth in HD and 4K content, and a consequent reliance on native secure hardware paths for content decryption, lends further urgency to this best practice.[2]

[2] DRM in the Age of HTML5, Frost & Sullivan, December 2015

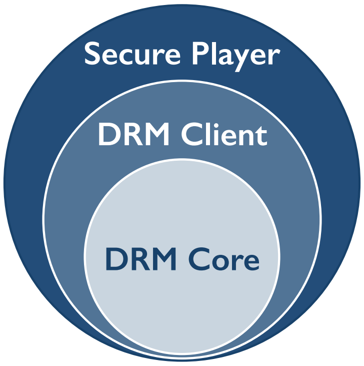
FIVE FACTORS TO CONSIDER WHEN EVALUATING TCO FOR A DRM SOLUTION

In this section, we take a deeper look at five misunderstood aspects of TCO for DRM in the context of OTT video market trends and DRM technology trends.

1. The Fallacy of Free:The DRM Core Logic is Only One Component of Secure Playback

DRM vendors monetize their own cores, which contain their DRM logic, in varying ways. As two contrasts, Microsoft PlayReady charges a modest royalty on consumer products while Google Widevine is royalty-free. Other pricing models include content-based charges or charges based on number of subscribers. As vendors bow to pricing pressure and competition, there is a growing perception that DRM is increasingly becoming "free." This is a significant misconception, as the licensing cost of a DRM core logic is typically only a small fraction of the total cost of ownership.

Figure 2: Any DRM core logic must be augmented with a full client to enable secure playback



The DRM core logic encompasses the fundamental logic of the protection system. The core is seldom adequate on its own and must be augmented with a full-fledged client when deploying a secure player, as shown in Figure 2. While the core manages authentication, trust verification and key exchange, it is the full client which manages the full range of entitlement checks, permissions enforcement, device integrity verification, timing verification, output control, and similar functions. TCO calculations must account for the complete cost of developing and maintaining a portfolio of secure clients. The price of a given implementation will often vary as a function of how much of the functionality required for the complete secure player is being included in the deliverable; VSOs and OVPs must keep this in mind when comparing options.

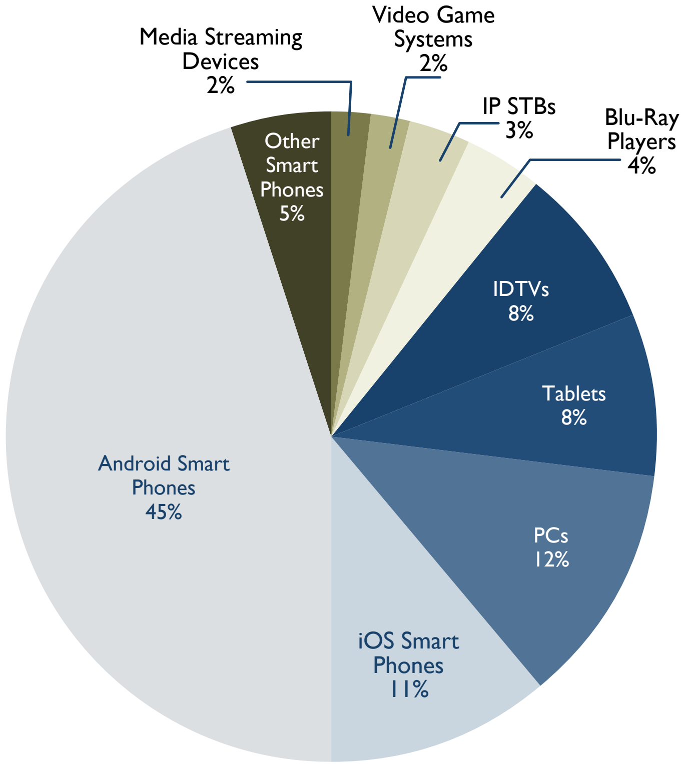
As services become fragmented between browser-based and app-based viewing across myriad devices, VSOs must be prepared to choose different DRM systems for different use cases based on cost, features, native integration, and other considerations. Increasingly, the client needs to be more tightly integrated with native hardware, browser or both. If there is a failure of security in this enforcement layer, repercussions can range from fines to revocation. Remedying such events is expensive and disruptive, and there is a reasonable probability that such incidents may occur on one or more platforms when building secure clients in-house.

2. Increasing Fragmentation in Devices and Platforms

Less than 10 years ago, Internet Explorer and Firefox on Windows PCs accounted for the vast majority of OTT viewing. In contrast, 2016 will see the shipment of nearly 2.5 billion connected devices across nine device types, spanning myriad chipsets and platforms, browsers and application interfaces—as shown in Figure 3. Broadcasters have typically measured infrastructure half-life in decades, but online viewing models are evolving at the speed of the cloud. Bouquets of live, linear services gave way to on-demand, browser-based content consumption, which has quickly given way to an app economy. New devices emerge and claim disruptive market uptake every year—some of these endure while others fade quickly into oblivion. Keeping track of new devices, platforms and technologies places significant strain on player and server teams.

At the same time, delivering a consistent, high-quality user experience across all these devices, screens and networks is a non-negotiable requirement for customer satisfaction. Delivering a service consistently, reliably and securely to this vast plethora of endpoints is a formidable undertaking, but one that must be achieved if a service is to break out of the noise to achieve significant growth and retention of subscribers.

Figure 3: Unit Shipments of CE Device by Type, Global, 2015

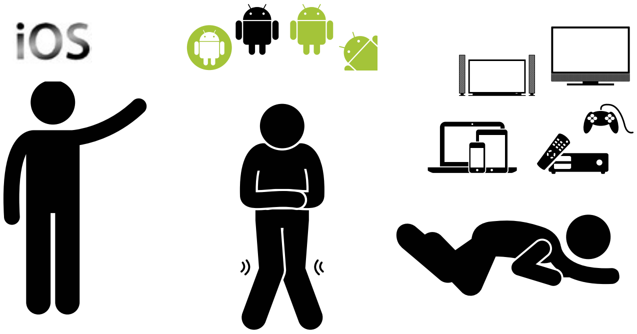


Source: Frost & Sullivan

IMPLICATION OF DEVICE FRAGMENTATION ON TCO

Figure 4 depicts the misplaced confidence often found among VSO engineering teams regarding the cost and timeframe for building secure players in-house. This typically stems from an under-appreciation of the magnitude of the fragmentation challenge. In-house development as a tactic works quite well for the homogenous Apple product portfolio, including the iPhone and iPad lines. Given that Apple devices are typically the first targets of any new online system, this provides an early sense of satisfaction and confidence in a team's ability. However, this confidence is quickly undermined as teams then embark on tackling the fragmented Android ecosystem. The in-house approach nearly always degenerates once services enter the next phase of expansion, whose aim is typically to span the complete ecosystem of connected devices.

Figure 4: The Complexity of Building out a Service for the Complete CE Ecosystem Quickly Becomes Overwhelming



As previously noted, achieving consistency of experience for every consumer, on every network, on every device is absolutely crucial to the reach of a service, which directly affects its ability to attract and retain subscribers. Frost & Sullivan research finds that the average cost of porting a secure player to a new platform is in the range of $100,000 to $250,000. Services must support a minimum of 10-12 devices to be considered viable and ideally should be supported via browsers or apps on more than 40 devices (with that number growing every year) in order to be competitive. DRM core logics must be chosen optimally for each device, creating another layer of management overhead and complexity. Accordingly, the R&D investment required simply for upfront development itself can quickly run into the millions of dollars.

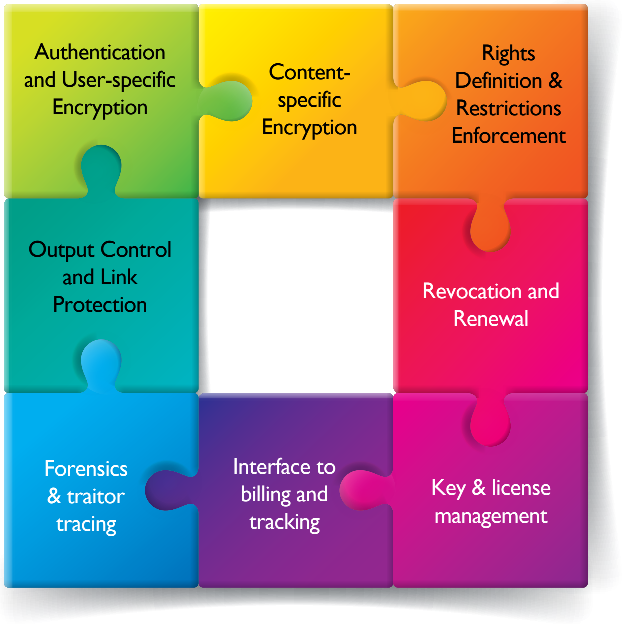
3. Consistency Amidst Fragmentation and Technology Disruptions

Encrypted media extensions (EME) is a standardized framework allowing the same encrypted data to be accessed via different DRM systems. EME is used in conjunction with MPEG-DASH, the new unified standard for media streaming. For various practical reasons, EME has been deployed in such a way that each browser will likely only support one DRM system, and each device will likely support between one and three. While the content transcoding problem has definitely been simplified, the DRM management problem will become more complex. As the use of HTML5 and app-based content consumption grows, it is no longer practical to expect a content service to rely on a single DRM system to reach all its target devices and Web browsers. This drives the need for a multi-DRM approach, which essentially leverages an abstraction layer to hide the underlying complexity of handling multiple DRM systems under a consistent API.

A critical function of a multi-DRM approach is harmonizing rights and user experience across different devices. Different DRM systems utilize different rights languages, and hence expertise is necessary to ensure that a system translates a given set of rights equivalently across the rights languages of all the different DRMs. This ensures that the end-user experience on all corresponding devices and browsers is consistent. We cannot emphasize enough that users expect consistency and predictability as they consume a given service from different devices; there are significant negative consequences for getting this wrong. When different devices deliver differing rights and privileges because of limitations of the underlying technology components, users become confused and frustrated. With an in-house solution, managing fragmentation across devices and DRM systems can become an overwhelming and error-prone process. A mature multi-DRM solution, in contrast, unravels this exponential complexity into an automated, uniform interface that ensures transparent consistency in user experience and glitch-free service upgrades and expansions.

This uniformity is also important on the server side of the system, which interfaces with customer management and billing systems, delivers licenses, and ideally generates metrics and reports for various internal stakeholders. Servers form the single point of failure from scalability and reliability points of view. They also bear the full brunt of complexities introduced by device and format fragmentation, and evolving business models. On the one hand, license server-side infrastructure is closely intertwined with subscription management systems. On the other hand, the servers must be able to accomodate for usage scenarios; for example, license issuance must be device- and location-aware for each user. Figure 5 depicts the multi-functional nature of DRM infrastructure, across server and client components.

Figure 5: Client-side and Server-side Components of a Complete DRM Implementation


Authentication and User-specific Encryption
Content-specific Encryption
Rights Definition & Restrictions Enforcement
Output Control and Link Protection
Revocation and Renewal
Forensics & traitor tracing
Interface to billing and tracking
Key & license management

As new DRM systems and new encryption configurations arise over time, and business models evolve, server complexity can quickly get out of hand, often resulting in silos that again hinder service growth and limit consistency of consumer experience. A recommended best practice is to build in an abstraction layer that can allow content services to treat the underlying device-specific intricacies as a single outward-facing interface. When built in-house, there is a significant element of risk as well as potential delay and expense caused by reinventing the wheel. Commercial multi-rights DRM vendors will typically have solved this problem for many customers, and are dedicated to maximizing server performance and agility.

4. DRM is a Program, not a Project

When modeling the TCO for DRM, companies are often preoccupied with the initial release and fail to plan for DRM as a long-term undertaking. More than any other component in the digital content workflow, DRM will always remain a work in progress.

For example, security requirements continuously evolve—partly to keep pace with increasing hacker sophistication, but also because of increasing content resolutions, changing business models, and changing usage scenarios. As on-demand OTT delivery to consumer devices reaches parity with conventional TV delivery to secure set-top boxes, these demands will continue to rise and will do so at an accelerated pace. To maximize consistency and quality of service, these enhancements must be implemented not only for new devices, but also back-ported as updates to as many existing deployments as possible.

We have already discussed the level of fragmentation in terms of deployed devices and browsers that video service operators must tackle. There is an additional moving piece to supporting these deployed form factors, which is the ongoing cycle of upgrades to operating systems and browsers for these devices. When a new version of iOS is released, for instance, DRM clients may need to be retrofitted to account for differences in how integrity may be verified, which security interfaces may be accessible, or how data is reported back. The more technologies contained within a single umbrella, the more moving parts there are to keep track of and keep up to date. This requires specialized, dedicated resources when being managed in-house.

DRM core logics themselves are not infallible. As DRM vendor priorities evolve or as their own system features change, services may need to periodically revisit their choices of DRM system(s) on various devices. With a well-architected system that is designed upfront to be flexible and agile, these updates and transitions can be made efficiently over time.

Last but most importantly, there is always the likelihood of a breach or circumvention of the secure player that results in leakage of revenue and/or content. These breaches must be properly fixed, for all existing deployments, on a very short timeline. Breach management and renewability is the most crucial characteristic of any DRM implementation. Planning for the costs of ongoing DRM management and improvement is arguably the most important, and yet often the most overlooked, aspect of TCO estimation.

5. Agility in Adopting to New Content Features and Business Models

The only certainty in the quicksilver world of OTT video is that disruption, innovation, opportunity and risk will all arise in predictable regularity with unpredictable specifics. VSOs have yet to find the silver bullet in terms of business models and customer satisfaction, and OTT is far from realizing its full monetization potential. Thus, agility and flexibility are critical requirements for any content service—and the service can only be as agile as its DRM infrastructure permits.

There is immense need for flexibility of OTT business models spanning streaming, renting and purchasing to own. We have discussed at length the fragmentation in CE devices, and the evolving device landscape translates into shifts of user viewing preferences. While tablets were the fastest growing OTT destination only two years ago, IP streaming devices have quickly overtaken tablets, and Smart TVs are poised to make a comeback of their own. We anticipate that security requirements for premium content will grow immensely as content resolutions increase and release windows are pulled in. Companies that are not equipped to adapt with agility to these changing demographics and evolving requirements will inevitably incur significant opportunity cost.

Research shows that the more vivid the video you can deliver to a given device or screen, the longer and more deeply your viewer will stay engaged with your content. Video quality is often considered to be a problem of transcoding and bandwidth. However, it is also dictated by the strength of the DRM implementation. Copyright owners may, for example, only allow SD content to be delivered to a player implementation, which does not include adequate hardware protection or comprehensive checks for device integrity. A competing service provider with a more robust player may be allowed to deliver HD or even UltraHD content to the same device. The debate between app-based and browser-based content delivery, in the age of HTML5, stems in part from this consideration. A trusted partner with visibility into current and future requirements can help service providers better and more profitably navigate these uncertain waters.

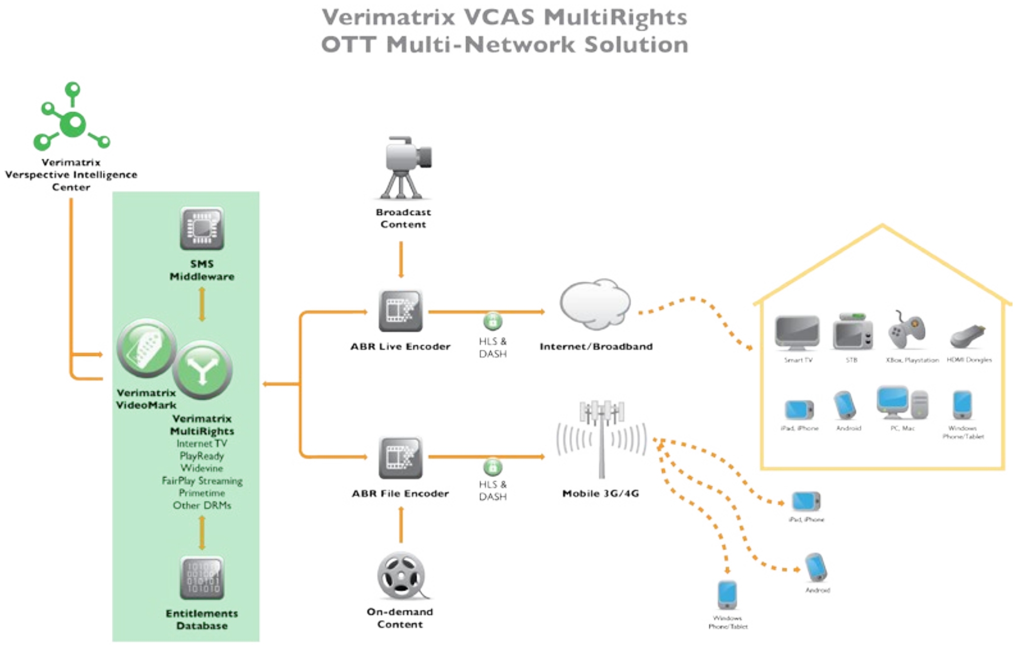
Frost & Sullivan sees DRM not simply as an anti-piracy solution, but as a business-enabling monetization technology. This monetization layer needs to scale and adapt with the same agility as the OTT ecosystem does, and this needs to be possible in a cost-efficient and time-efficient manner. Customer loyalty for content services today is fickle. First-mover advantage for delivering delightful user experiences in a consistent manner across all relevant devices goes a long way in attracting and retaining subscribers and in growing hours viewed per subscriber. Conversely, if the monetization layer cannot—or does not—adapt with the same agility, it can hold back progress, negatively impact competitive positioning, and hinder revenue growth.

A MULTI-RIGHTS SOLUTION: VERIMATRIX

Verimatrix specializes in securing and enhancing revenue for multi-network, multi-screen digital TV services around the globe. The Verimatrix Video Content Authority System (VCAS™) family of solutions enables next-generation video service providers and OVPs to cost-effectively extend their networks and enable new business models. As shown in the figure below, the company provides a convenient "black box" revenue security platform to unify different security models and optimize the overall strategy by ensuring that the most appropriate security mechanisms are used on each platform.

Figure 6 - Verimatrix MultiRights System

MultiRights features multiple DRM-specific license servers to handle requests from a variety of device types. The rights requests from different device agents are arbitrated by common VCAS application logic to harmonize entitlement.



By leveraging the company's MultiRights™ OTT solution, operators can deploy multi-network services in the knowledge that they have a platform that will absorb changes in security schemes as they occur and evolve compelling multi-screen services on top. MultiRights brings CE devices and HTML5 browsers with embedded non-Verimatrix clients under the VCAS unified revenue security umbrella together with other subscriber devices already incorporating Verimatrix client security. The goal is not "DRM unification" as much as user rights unification to enable transparent content consumption for end users. The MultiRights framework allows for the inclusion of any third-party DRM scheme and any client devices under the VCAS umbrella for complete, consistent, end-to-end management of revenue security.

Maintaining close relationships with major studios, broadcasters, standards organizations and its unmatched partner ecosystem enables Verimatrix to provide a unique perspective on video business issues beyond content security as operators introduce new services to take advantage of the proliferation of connected devices.

THE LAST WORD

Video service operators specialize in creating branded content experiences that delight viewers, with the goal of creating popular services and generating subscription and/or advertising revenue. Undertaking in-house development of a full-fledged DRM platform is equivalent to instituting a new product line that is tangential to your intended product roadmap, outside your core competency, and a drag on your bottom line. Spending scarce resources in an attempt to experiment in reinventing the wheel is a risky business strategy.

Video service operators are already challenged by the unsolved problem of delivering delightful online experiences in a profitable manner. Can you really afford to incur the risk of self-engineering the anti-piracy and monetization layer that is crucial for ongoing access to content and to ensuring your business can stay on top of new business models, support new computing platforms, enable new usage scenarios, and combat the latest hacking technologies?

Globally, video service providers and OVPs are finding that the modern OTT ecosystem is a treacherous landscape and is best navigated in partnership with an experienced multi-DRM vendor. Multi-DRM vendors are much better equipped to handle the underlying fragmentation of various devices, core DRM systems, and compression and streaming standards, as compared to all but the largest and most technologically savvy operators and OVPs. By tapping into this expertise, companies gain agility, reduce costs, strengthen security, tighten protection of revenue, and yet at the same time broaden reach of their service and improve customer experience. What is technologically revolutionary with an in-house implementation can become simply evolutionary with a reliable partner. The revolution can then move to customer attraction and revenue growth, allowing you to successfully ride the OTT opportunity wave.

ABOUT VERIMATRIX

Verimatrix specializes in securing and enhancing revenue for multi-network, multi-screen digital TV services around the globe and is recognized as the global number one in revenue security for connected video devices. The award-winning and independently audited Verimatrix Video Content Authority System (VCAS™) family of solutions enable next-generation video service providers to cost-effectively extend their networks and enable new business models. The company has continued its technical innovation by offering the world's only globally interconnected revenue security platform, Verspective™ Intelligence Center, for automated system optimization and data collection/analytics.

Its unmatched partner ecosystem and close relationship with major studios, broadcasters and standards organizations enables Verimatrix to provide a unique advantage to video business issues beyond content security as operators introduce new services to leverage the proliferation of connected devices. Verimatrix is an ISO 9001:2008 certified company. For more information, please visit www.verimatrix.com, our Pay TV Views blog and follow us @verimatrixinc, Facebook and LinkedIn to join the conversation.

FROST & SULLIVAN

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

SILICON VALLEY

331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

SAN ANTONIO

7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON

4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041