Publication date:
Dec 2021
Author:
Luke Pearce

Omdia Market Radar: Media and Entertainment Application Shielding

Protecting streaming and gaming

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Verimatrix

Contents

Summary

Catalyst

Driven by the likes of Netflix, video content delivery has evolved to put consumers more in control of whatever, whenever, and wherever they wish to consume. App-based viewing is quickly becoming the primary way for users to engage with content, both in and outside the home, across smartphones, tablets, smart TVs, games consoles, streaming media devices, and pay-TV boxes. All video service providers have had to adapt to changing behavioral patterns and create app-based experiences for watching content on devices with underlying hardware and software they do not control. These applications, available in quasi-regulated public app stores, offer a window of opportunity for malicious hackers to delve into the structural integrity of the software, bypassing restrictions to access copyrighted material or make illicit modifications. Creating secure apps is critical to securing the financial value of content assets and protecting against access to the wealth of user information stored within them.

In this Market Radar report, Omdia explores the landscape for application shielding (app shielding) solutions and their growing importance for stakeholders in the media and entertainment industry to protect video and gaming content from would-be pirates or hackers. Omdia outlines the evolving need for such products and compares six current vendors' solutions with the aim of understanding the breadth of and differences in capabilities, ease of integration, and added-value features offered.

Omdia view

The wider content security market has, until recently, shown relatively limited focus on the vulnerabilities presented by mobile applications. Digital rights management (DRM) technology does provide some level of security against unauthorized access to content on apps, and service providers implementing such content protection solutions will have been indirectly using some existing elements of built-in app shielding techniques. However, hackers are increasingly making use of vulnerabilities in the wider unprotected app to make more sophisticated attacks. Armed with knowledge gained by unveiling the inner app's code, attackers are increasingly finding ways to deconstruct and reverse engineer the app, including finding the hidden DRM keys and getting access to the content. These techniques have drawn more attention to the app protection proposition, particularly with the rise of higher-value content, such as 4K UHD or theatrical releases (premium video on demand), increasingly distributed direct to the consumer. Record levels of investment in original content have created more valuable digital assets, all available on a multitude of user-owned unmanaged devices. There are also signs that more studios and rights holders are beginning to recognize the need to protect the whole over-the-top (OTT) app to prevent pirating of content, and app protection is becoming an increasingly mandated element in contracts with operators. These market forces have prompted a growing number of content security vendors to develop app protection solutions as part of their wider offerings.

Mobile gaming is a significant part of the app ecosystem: it accounted for 74% of global app store revenue in 2020 according to Omdia's *App Ecosystems Forecast Report – 2020–25*. Mobile gaming applications have unique security considerations in addition to the vulnerabilities experienced by other industries. Mobile gaming is subject to a user base that has additional incentives to break down the integrity of the application in order to tweak games rules and provide gameplay advantages over other competitors. This can harm the fairness and hence the playability of the game, bringing reputational damage to the game and its publishers. This is especially crucial in the early-window release period of new games, when media attention and revenue are at their peak. In addition, hackers can exploit in-game microtransactions, leaving publishers vulnerable to loss of revenue.

App protection is a nascent technology proposition but will likely increase its influence in the wider media and entertainment market because of the considerable weight of market forces at play. The unique considerations of this industry, such as the importance of minimal impact on performance, demand specific and dedicated solutions to limit the damaging effects of streaming and mobile piracy.

Definition and characteristics of application shielding

Application shielding includes a variety of techniques used in cybersecurity and cryptography that aim to protect the source code and integral software of applications across a number of different devices. Of these techniques, the three that form the basis of most app shielding products are code obfuscation, rooting/jailbreak detection, and anti-tampering. Most firms discussed in this report also provide cryptographic key protection, which is more specific to the media and entertainment industry and is sometimes provided as an additional add-on or standalone product. All solutions on the market offer protection for Android or iOS mobile devices; some also provide support for web-based applications used on PCs, smart TVs, and games consoles.

App shielding products are predominantly delivered as a set of on-premises "tool" libraries, sometimes as a software development kit (SDK) or APIs. These tools are provided to developers to use on top of their source or compiled code and integrate with most of the different development languages. They differ in terms of their ease of integration, but support and training are often available.

In the last couple of years, new product improvements aimed at simplifying the integration process have been made by several vendors. These cloud-based software-as-a-service (SaaS) models are app protections delivered with either no code or low code. Utilizing a vendor's cloud-based infrastructure, an unprotected app is uploaded to an interface, and app protections are automatically applied to relevant vulnerable code. This process is reported as taking a matter of minutes, dramatically reducing integration time and cost. This is especially suitable for customers that lack much security expertise or in cases where a short time to market is essential.

Once implemented, app shielding products will require ongoing maintenance and updates, particularly when new threats appear or new versions of the operating system become available, so a vendor's support capability and responsiveness should be a key consideration.

Additional features such as analytics and monitoring are also available with some app protection solutions. These provide real-time feedback on potential threats or attacks and can prompt further action if necessary. Some can also be linked into external third-party dashboards.

Evaluation and testing features are also common parts of the process, with app shielding vendors performing internal threat assessments or testing an app's security protocols before it is launched. This enables the identification of any weakness in a test environment before an app is compromised by attackers.

Pricing is often on a subscription-based model with variation according to a tiered, per subscriber system.

The most common use cases for app shielding

- **Protect from reverse engineering.** Unprotected apps are vulnerable to being reverse engineered by pirates or unauthorized third parties. With the code exposed, illicit actors can modify, repackage, or duplicate functions to serve unintended purposes.
- **Protect media application licensing.** DRM encryption requires a cryptographic key to unlock content. Hackers are increasingly able to expose DRM access keys in the application code to decrypt content, allowing illicit access and distribution.
- **Protect media application content against rooted/jailbroken devices.** Rooted (Android) or jailbroken (iOS) devices can bypass the original hardware manufacturer's software to gain full access to the root of the operating system, overriding several restrictions.
- **Protecting anti-cheat for gaming.** In gaming apps, hackers are able to modify game dynamics to provide unfair advantages. Hacking can also disrupt in-game e-commerce, harming microtransaction revenue.

Common features of app shielding

- **Code obfuscation:** scrambling well-engineered source or compiled code to make it difficult for an attacker to read
- **Root/jailbreak detection:** identifying and blocking access to devices that have been unlocked to allow unregulated access to the core device operating system
- **Anti-tamper:** performing binary integrity checks to match what is executed with the original source to ensure the software has not been changed
- **White-box cryptography:** a cryptographic approach to concealing access keys within an application and building in countermeasures to key-extraction attacks
- **Hooking framework detection:** a range of techniques used to intercept function calls or messages, aimed at discovering whether hooking is being used by malicious code such as rootkits, which fake the output of API calls that would otherwise reveal their existence
- **Debugger detection:** checking whether anyone is stepping through an application's code as it runs, which should only be done by legitimate developers
- **Emulation detection:** detecting when software is being used that reproduces how an operating system works via a virtual, "pseudo" OS or simulated hardware

Vendor landscape

The vendor landscape for app shielding is extensive and covers a wide range of cybersecurity firms catering to different markets. While most app protection methods and practices are applicable to most industries, firms opt to specialize in industries where they can better understand and design products for the differing requirements of each industry. For this Market Radar, we have only included firms that offer products for the media and entertainment industry, protecting video-streaming and gaming applications. These six firms are Verimatrix, Irdeto, Digital.ai, Zimperium, INKA Entworks, and Synamedia.

Verimatrix, Irdeto, and Synamedia are vendors that have built a reputation on offering content security products for media and telecommunications companies and that offer a wide selection of additional video content security products beyond app protection such as conditional access systems (CAS), multi-DRM, watermarking, and piracy monitoring. These firms, which have in the past offered app protection in some capacity, have more recently and particularly within the last five years put resource into developing and rebranding standalone app protection offerings to adapt to the growing need of their media customer base.

AppSealing is an offering from INKA Entworks, which has been offering multi-DRM and other content security products to video content security firms through its subbrand PallyCon. AppSealing is a standalone brand that addresses industries including media and entertainment, gaming, and financial technology (fintech).

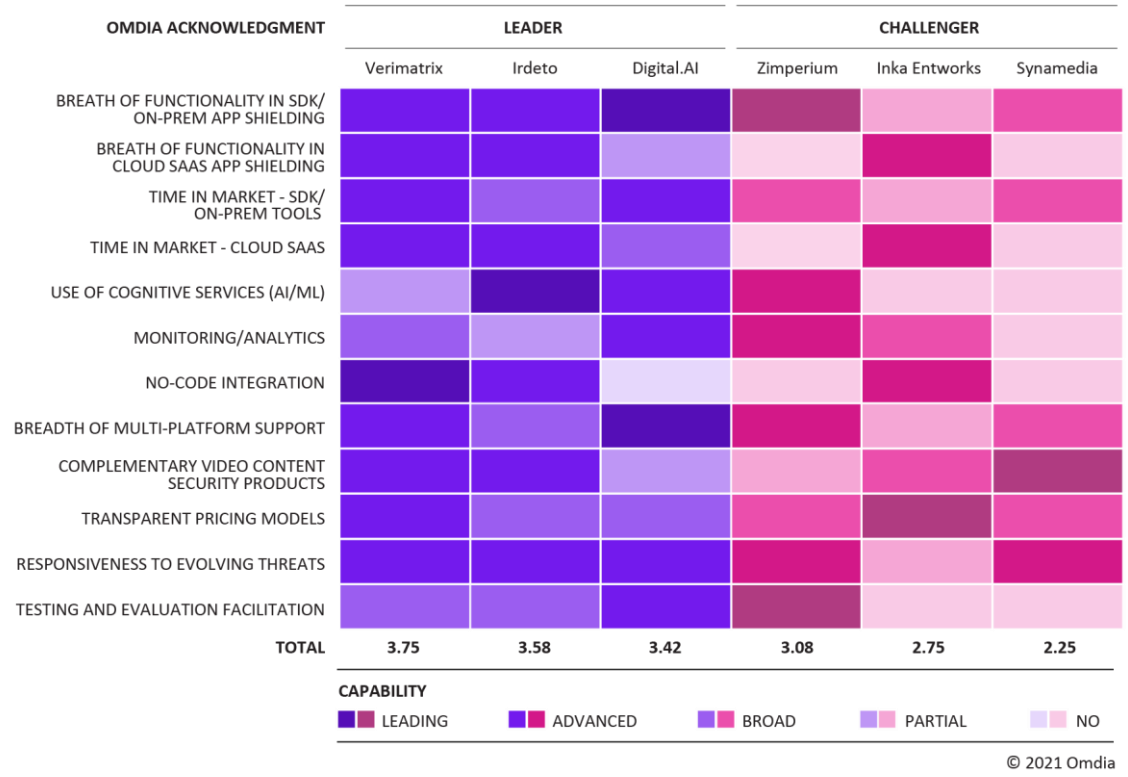
Zimperium is a specialist mobile threat defense firm founded in 2010. The 2H21 acquisition of whiteCryption, previously owned by Intertrust Technologies, has strengthened its capability in white-box cryptography and opened doors to the media and entertainment industry, which has justified its place in this Market Radar.

Digital.ai is a rebranded composition of the former Arxan, CollabNet Version One, and Xebia Labs. It combines value-stream delivery and management, agile planning, and software delivery with its application protection. Digital.ai offers application protection to some of the larger OTT video providers and AAA games publishers.

This report evaluates each of these vendors and their offerings in this space, scores each on an evaluation matrix, and provides commentary on all of them.

Evaluation matrix

Figure 1: Omdia heatmap for app shielding



Source: Omdia

Omdia's Market Radar evaluation matrix provides comparison scores over several key criteria. Typically, when buyers are looking to purchase app protection products, they consider five core criteria: ease of integration into current workflows, compatibility with as many devices as possible, minimal impact on end-user performance, studio certification and third-party evaluation, and cost. These criteria, along with additional comparable competencies, form the basis of the evaluation matrix:

- **Breadth of functionality in SDK/on-premises app shielding** measures the quantity and perceived quality of solutions and techniques of the on-premises tools, SDKs, and APIs offered by vendors.

- **Breadth of functionality in cloud SaaS app shielding** measures the quantity and perceived quality of solutions and techniques of the cloud SaaS-implemented protections offered by vendors.
- **Time in market: SDK/on-premises tools** measures the length of experience the vendor has of offering this solution. Vendors that score highly have sophisticated, proven techniques that have been tried, tested, and developed over a lengthy period of time.
- **Time in market: cloud SaaS** measures the length of experience the vendor has of offering a cloud SaaS-based product. Time in market for these products is comparatively short, with most only having been available for less than two years.
- **Use of cognitive services (AI/ML)** measures the extent to which the vendor is using trained algorithms on learned data to enhance responsiveness, efficiency, or effectiveness of the security tools. Note: this does not include use of artificial intelligence or machine learning (AI/ML) in any additional monitoring or analytics offered.
- **Monitoring/analytics** measures a vendor's capability to provide a dashboard tool that provides real-time feedback of implemented tools' actions against incoming threats. High-scoring vendors offer functionality that enables interactive actions rather than pure visualization or hooks to third-party tools.
- **No-code integration** evaluates the level to which a vendor's solution allows for limited previous coding experience or reduced additional integration time and knowledge to implement protection mechanisms. High-scoring vendors offer protections that can be applied in a matter of minutes.
- **Breadth of multiplatform support** evaluates application support across several different platforms including iOS, Android, desktop, web, smart TV, set-top box, and games consoles. Firms that score highly in this metric support most or all platforms.
- **Complementary video content security products** measures the capability of a firm to offer additional video content security products alongside or integrated with app protection. This might include CAS, multi-DRM, watermarking, or piracy monitoring to provide a more holistic content security approach for OTT vendors.
- **Transparent pricing models** measures the vendor's willingness to provide clear and flexible pricing models upfront without any hidden costs required to maintain security after initial implementation.
- **Responsiveness to evolving threats** measures the perceived capability of the vendor's research and development team to continue to provide new and updated features to target ongoing threats from hackers or pirates.

- **Testing and evaluation facilitation** measures a vendor's capability to test and evaluate current app vulnerabilities before launch in the public domain, usually via a virtualized or physical device farm.

Vendors on the Omdia Market Radar in application shielding

Overview: Leaders and challengers

Verimatrix, Digital.ai, and Irdetoare the *leaders* in this market and have a wealth of experience in providing app protection tools to media customers. All provide a comprehensive suite of on-premises app shielding tools and have released cloud-based SaaS implementation methods within the last two years. Digital.ai's on-premises solution provides more breadth in comparison with the others, but its cloud-based product is inferior to those of Verimatrix and Irdeto, which offer uncompromised protections via no-code solutions. While the types of offerings from Irdeto and Verimatrix are similar, some differences mean Verimatrix scores more highly on Omdia's matrix. Irdeto has more of a presence in the gaming industry through its subbrand Denuvo and can be acknowledged for its use of AI in code obfuscation, but Verimatrix scores higher for its developed implementation methods and pricing models that cater to a wider range of devices. Verimatrix's new analytics tool also makes a more well-rounded offering, which scores highest overall in this radar.

Zimperium, Synamedia, and AppSealing are rated as *challengers* in this space. Zimperium is the most significant challenger of the three, having developed experience across several different industries with app protection as its sole product focus. Its recent acquisition of Intertrust's whiteCryption enhances its position in the media market, and its strong suite of solutions could rise to more prominence over the next few years. AppSealing has the smallest, value-focused offering in the market and is the challenger that offers the most transparent pricing model with a list of features and monitoring that punches above its weight. Synamedia provides a managed end-to-end solution specifically aimed at OTT service providers, but because of the nature of its app protection service being used in this way, it scores comparatively lower on the matrix than the other vendors.

Verimatrix: App shielding suite

Figure 2: Verimatrix Omdia acknowledgment: Leader

Source: Omdia

Verimatrix has been offering video content security products to media and entertainment clients for more than 25 years, and its products have significant market presence, covering CAS, DRM, and watermarking. Its reputation for security and support in this market is strong, and elements of its app protection products have been in use in these products for around 15 years.

Its core and longest-serving standalone app protection product is offered via on-premises tools. Branded Code Shield, it offers developers a tool kit to wrap compiled code in protections covering code obfuscation, anti-tampering, and jailbreak/root detection among others. It also has a product branded Key Shield (formerly Whitebox), which utilizes white-box cryptography to protect access keys from key-extraction attacks.. These tools are highly effective and are trusted by several Tier 1 media operators. In addition, its security credentials have passed the strict requirements for Visa and Mastercard.

Verimatrix's approach to iOS bitcode requirements provides a unique differentiator. Apple's bitcode requirements will modify an app's code to optimize compiled code for iOS platforms, which has an impact on the anti-tamper aspect of many alternative solutions on the market. Verimatrix's patent-pending Elastic Anti-Tamper allows for the bitcoding from Apple while still rendering anti-tamper effective.

In addition to the on-premises tools, Verimatrix offers implementation via a cloud-based SaaS platform called App Shield, launched more than two years ago and one of the first of its kind. This product is focused on making implementation of app protection products much easier. It is marketed as a simple "upload and protect" no-code solution. Verimatrix's tools do automated analysis to understand the performance profile of the application's code, allowing the tools to intelligently apply protection while minimizing performance impact. Verimatrix reports that an application can be fully protected within a few minutes of upload. Functionality of the App Shield is

comparable with that of the on-premises tools, with the same levels of protections automatically applied, promoting faster time to market.

Verimatrix's app protection solution covers a wide range of platforms, with most platforms and coding languages supported, including web app support through a recent partnership with Jscrambler. The only current exception is applications running on games consoles.

During the sales process, Verimatrix offers an app evaluation service: an app is automatically scanned and evaluated for potential security vulnerabilities. The app is then scored on a scale from A to E, and potential customers are provided with an actionable piece of insight into how vulnerable the app is in its current form.

App protections are continuously tested using virtual device farms to make sure that any updates to the security tools are able to function with a multitude of different devices. When OS updates are announced, Verimatrix uses physical devices to make sure the updates do not damage the product performance. The app protections have survived more than six years of iOS updates without any modifications to core functionality being necessary.

Verimatrix has recently launched a monitoring/analytics feature included within the App Shield service. Today, it is a visualization dashboard that provides intelligence around real-time attacks and vulnerabilities and provides a confidence score. This enables customers to ingest insights on security effectiveness, and hooks are provided if a customer wants to combine with other third-party security dashboards. Verimatrix hopes to enhance the analytics service in the immediate future with a remote-control feature that will enable customers to define rules or suspend accounts in real time.

Pricing is transparent and competitive considering the level of security protection offered. Pricing is publicly available for the cloud service, which can be administered via e-commerce self-service. It is modeled on a tier-based system, with enterprise-oriented tiers available. The cloud-based implementation is comparatively cheaper than the on-premises product because it is able to pool lower support and maintenance costs.

Analyst comment

Verimatrix offers the most well-rounded solution on the market compared with other competitive solutions, scoring well across many of the features in Omdia's matrix. A focus on top-level security and a development strategy focused on building the simplest implementation ensures Verimatrix its strong position among the contenders. Verimatrix's cloud SaaS-based product, its additional features, and its widespread compatibility make it the best solution of its type on the market.

Verimatrix's momentum going forward is secured by the continual development of the product: its roadmap includes bolstering its analytics platform and closer synergies with its content security products. Verimatrix's solution fits very well for many current and prospective high-profile video customers, but it is perhaps this stickiness of a focused customer base that is a disadvantage for Verimatrix. While its technical capabilities cannot be questioned, there are solutions on the market that might better cater to gaming applications and offer greater experience of dealing with gaming's specific needs.

Overall, however, both its on-premises and cloud-based SaaS app shielding products should offer media companies a one-stop shop with security, support, features, and simplicity in the implementation process, all key considerations for buyers.

Operating systems and platforms supported

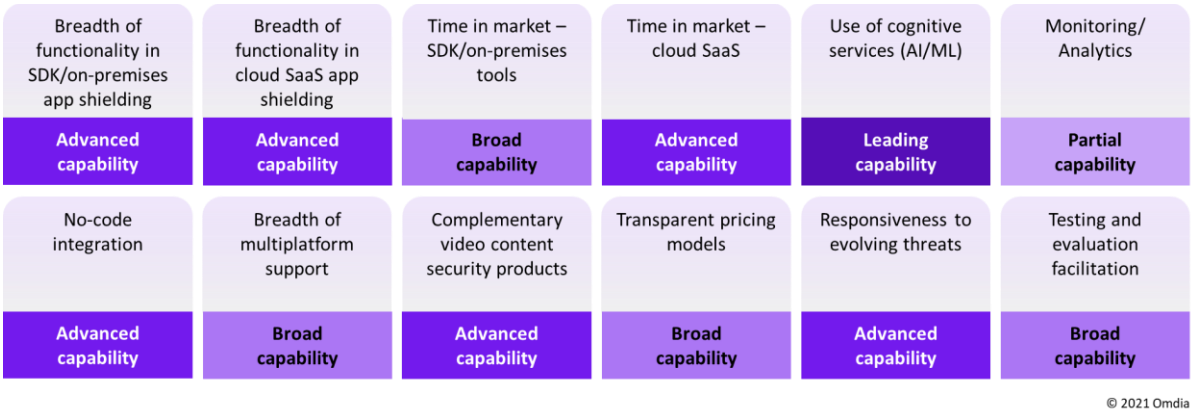
- Android
- iOS
- Hybrid mobile apps
- Web
- Desktop

Product names

- Shield (formerly Code Protection)
- App Shield
- Key Shield (formerly Whitebox)

Irdeto: Active Cloak for Apps, Trusted Software, and Denuvo Mobile Game Protection

Figure 3: Irdeto Omdia acknowledgment: Leader



Source: Omdia

Irdeto, part of the South Africa–based MultiChoice Group, was formed in 1969 and has a long history in securing content for media companies. In app protection it continues to hold a significant market share for additional video content security products such as CAS, DRM, piracy monitoring, and watermarking. Irdeto was also the inventor and key patent holder of white-box cryptography. Under the subbrand Denuvo, Irdeto also has a significant presence in the gaming security industry across PC, console, and mobile games. Irdeto has three products targeting the app shielding market, which fit into its wider video and gaming security portfolios.

The first, Active Cloak for Apps, is an on-premises tool kit originally designed to provide the necessary compliance protections for studios. This product has been in the market for eight years and is often bundled with other video content security products as part of a package. Trusted Software, Irdeto's latest product, is an evolution of Active Cloak for Apps and provides a wider selection of protections as well as more advanced implementation methods. Denuvo Mobile Game Protection is essentially based on the same technology as Trusted Software but is aimed at gaming use cases. Both these more recent products have been in the market for less than two years.

Irdeto's innovative approach to using ML in its Trusted Software and Denuvo Mobile Game Protection security products provides its unique differentiator. Both products are available as either on-premises tool kits or cloud-based SaaS implementation, and the same level of protection is offered across both formats. With the cloud-based product in particular, the ML approach automates the process of finding and applying the security techniques to the compiled code, significantly reducing the often human-intensive implementation resource needed. The app protection utilizes multiple convolutional neural networks trained separately on things such as security and performance, and the ML models selectively adjust the protection level applied to the code segment by segment. The unsecured application can be dragged and dropped, and automated protections are applied within a matter of minutes. For potential customers that might be concerned about uploading to a vendor-hosted cloud, Irdeto is flexible enough to offer these services on a client cloud instead. As a result, Irdeto scores highly for the functionality of its cloud SaaS shielding, which maintains the same protections as the on-premises version, and for its no-code integration and use of cognitive services.

Irdeto's app protection products cover most significant platforms and operating systems. However, Irdeto does not currently support JavaScript/HTML5-based web apps, so it is marked down on the breadth of its multiplatform support. Irdeto also does not have many additional features and lacks a first-party monitoring or analytics platform. It does provide hooks for third-party analytics dashboards, however.

Pricing is transparent and competitive, with flexible monthly pricing available, avoiding vendor lock-in. Cloud-implementation versions of these products are relatively cheaper, primarily because of the additional support for updates and upgrades needed when an on-premises variant is used.

Protections are regularly updated alongside major operating system updates as are the general-purpose defenses against a wide range of known and unknown security threats, ensuring apps will be defended against emerging threats. After successful deployment, no further customer interaction is necessary.

Analyst comment

Irdeto's app protection products strongly address the ease of implementation demanded from the prospective customer base. Those looking for a quick, easily understandable way of applying app protection methods should consider the Trusted Software option. Its use of ML algorithms is unique and will provide faster time to market and confidence in minimizing performance concerns.

For gaming, Irdeto/Denuvo has a fantastic reputation for security and has the longest crack-free window in video games at more than 100 days on average. Irdeto's high-profile gaming security reference customers include EA, Ubisoft, SEGA, and Konami. For mobile gaming application developers, Denuvo Mobile Game Protection should be a consideration with its wealth of experience and specialized knowledge in this area.

In addition, Irdeto's wide range of video content security products complements the app protection portfolio. For service providers using Irdeto as a content security vendor already, Irdeto's Active Cloak for Apps is the simple option, although it is beginning to look like a legacy product in comparison with other available solutions.

Irdeto offers a solid portfolio for media and gaming vendors and provides a great deal of flexibility with cloud hosting and pricing. However, with its lack of support for JavaScript apps and its lack of additional features such as analytics, Irdeto does fall down against some of the competition if these are key considerations.

Operating systems and platforms supported

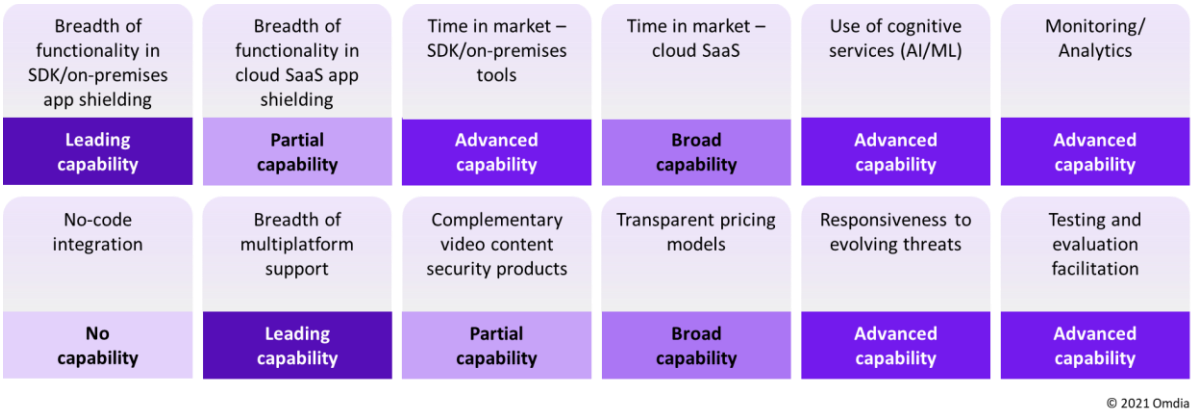
- Android
- iOS
- Windows
- Linux
- macOS

Product names

- Active Cloak for Apps
- Trusted Software
- Denuvo Mobile Game Protection

Digital.ai: Essential and comprehensive protection

Figure 4: Digital.ai Omdia acknowledgment: Leader



Source: Omdia

Digital.ai was formed in 2020 from the combination of CollabNet VersionOne, XebiaLabs, and Arxan. Much of its application protection technology came from Arxan, which specialized in anti-tamper and DRM for Internet of Things (IoT) devices.

Digital.ai offers its app shielding products segmented by platform. App shielding products are available for apps on all major platforms, including Android, iOS, desktop, and web, which results in a high score for the breadth of multiplatform support.

Its on-premises tools, branded as “comprehensive application security,” are well developed, and Digital.ai has been offering solutions for longer than all other vendors included in this report (15 years’ experience in the market protecting desktop applications, 10 in mobile, and 5 in web apps). Its protections include guards against more than 60 different attack vectors, including detection and prevention engines. Formerly part of Arxan, Digital.ai also offers Key & Data Protection, utilizing white-box cryptography using symmetric and asymmetric key encryption to protect data from network eavesdropping. Digital.ai demonstrates a high level of configurability and customization, trusted by an impressive reference client list, which includes AAA game publishers and Tier 1 media vendors. For this reason, Digital.ai scores a leading capability for the breadth of its on-premises functionality and its time in market.

Digital.ai also has a cloud SaaS implementation proposition tool, which has been available since 1H21, the most recent among vendors in this report. Branded “Essential,” Digital.ai’s capability here provides a more limited selection of protections than the comparable on-premises tools offering. While it requires less dedicated resource and knowledge to implement, the solution is described as “low-code” rather than “no-code” integration. It is positioned more for less valuable assets, for example, to provide some basic security functions for internal applications.

The high configurability and level of knowledge needed to implement the on-premises tools and a low-code SaaS model rather than the no-code offerings provided by other firms in this report account for the low score for the integration metric in Omdia's matrix.

Digital.ai scores highly in its additional services such as monitoring/analytics and testing and evaluation facilitation. Its App Aware monitoring service is the most advanced of all vendors' and provides real-time identification of risks, enabling customers to take actions such as disabling app functionality or locking account access. Fortified with ML, the app shielding products acquire intelligence from billions of Digital.ai-protected apps to provide deeper analysis into which conditions make security issues more likely, providing the benefit to customers from the sum total of Digital.ai's security knowledge.

The company's use of AI/ML is extensive. It has APIs to notify customers of different risks and provide app shutdown, user sandbox, code self-repair, and remote logging. The APIs can alter an application's responses to threats and dynamically change logic without an update of the application. This innovative approach results in high scores for responsiveness to evolving threats and use of cognitive services.

Pricing is transparent, but although this could not be verified in the scope of this report, it is likely one of the more premium solutions offered. Digital.ai no longer offers additional video content such as DRM from Arxan and is more broadly covering a range of different industries rather than focusing just on video or gaming.

The company cites continuous testing within app shielding as its most important forward-looking plan. This will include

- Mobile and web-based script recording export capability for open source automated testing framework Appium/Selenium
- New secured shared devices module with features such as site-to-site virtual private network
- Support for Cypress all-in-one testing framework and continued mobile-app software integrity testing

In the future Digital.ai expects its app shielding product to be adopted in conjunction with other software lifecycle orchestration solutions.

Analyst comment

Digital.ai has a comprehensive suite of sophisticated, data-fortified on-premises tools, as exemplified by its use by many Tier 1 and AAA media vendors and gaming companies. Its use of AI/ML is extensive, and the large number of deployments spanning multiple industries benefits the entire proposition. This capability extends into its App Aware analytics system, which provides a lot of control and adds value to the whole proposition beyond competitive solutions.

Service providers considering this solution should, however, be aware of its integration time. Because of the high level of customizability and the sophistication of the tools, high levels of dedicated security knowledge and resource will be required. While Digital.ai has a cloud SaaS product in market, its use is difficult to justify because it loses some of the protections while still

requiring some coding time, which negates much of its advantage and looks weak in comparison with other cloud-based offerings in this report.

Ultimately, Digital.ai is a top-tier premium on-premises solution for a wide variety of large firms that are willing to put in the extra resource to protect their apps. It also presents itself as a good solution if the aim is to gain synergy from Digital.ai's intelligent DevOps delivery and management platforms or to take advantage of any extensive testing and launch facilitation included in the proposition.

Operating systems and platforms supported

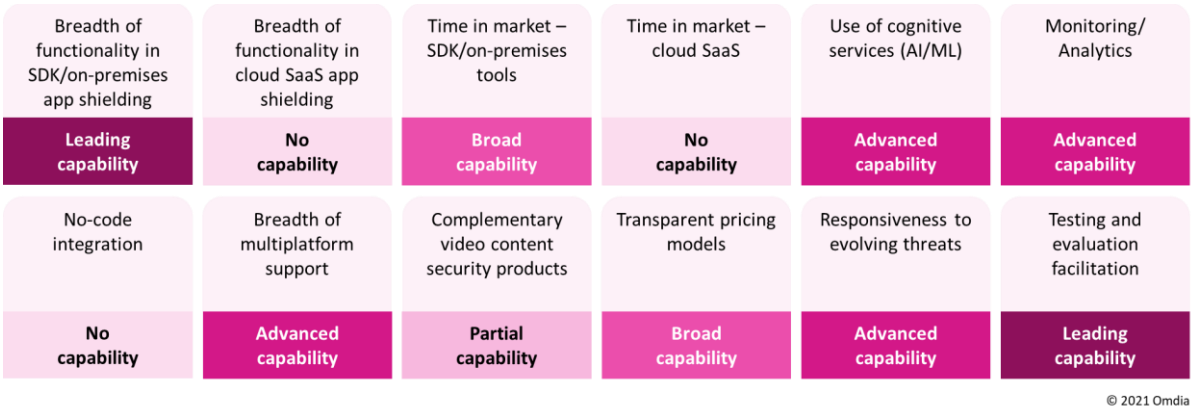
- Android
- iOS
- Hybrid mobile apps
- Web
- Desktop

Product names

- Application Protection for Hybrid
- Application Protection for iOS
- Application Protection for Android
- Application Protection for Web
- Application Protection for Desktop or Server

Zimperium: Mobile Application Protection Suite

Figure 5: Zimperium Omdia acknowledgment: Challenger



Source: Omdia

Zimperium, founded in 2010, is a privately held mobile security company based in the US. In 2021, Zimperium acquired whiteCryption from Intertrust Technologies, further enhancing its mobile protection suite with the addition of whiteCryption knowledge and resource, particularly in white-box cryptography. Intertrust has reference customers and presence in the content security market with DRM technologies, so the addition of this subbrand opens potential avenues into the media and entertainment market for Zimperium, justifying its place in this Market Radar.

Zimperium offers a suite of mobile security solutions called Mobile Application Protection Suite (MAPS), which can be purchased together as a whole suite or as separate products and which address all considerations in a DevOps mobile application process.

The core app shielding product is zShield, which protects the source code, intellectual property, and data from potential attacks such as reverse engineering and code tampering. Zimperium uses a variety of techniques including control flow flattening for code obfuscation, which aims to provide no logical flow for hackers attempting to trace the code. Another technique used is diversification, which is based on the source code compiler. Diversification changes the compiled code all the time, like changing languages, and is particularly effective for release cadence. All products are built with ML engines at their core since 2016 and go 70 or 80 techniques deep, resulting in Zimperium's best-in-class rating on our matrix. Offered as an on-premises tool that wraps the compiled and source code, zShield supports all major coding languages and goes as far as converting Java code into C code for its tighter security procedure.

For key protection, zKeyBox provides resistance to attack from the vast majority of hackers. This product has been bolstered by the acquisition of whiteCryption, which offers market-leading capabilities in this area of security. It is implemented as a C library.

Zimperium's app protection products are not described as no code or low code and require deep integration and collaboration with security teams and engineers. Customers will need to spend a few days with the Zimperium team and tools to customize the protections and make sure the impact on end-user performance is minimized. No cloud SaaS implementation variants are available within Zimperium's suite.

Zimperium's solution for testing and evaluation is zScan, a service designed to scan the apps to discover and fix compliance, privacy, and security issues within the development process before the app is publicly released. It can integrate directly with a development process, and once findings are discovered, zScan opens tickets in ticketing systems to provide developers with detailed information to address the risk. Its "Build Compare" capability quickly shows whether risks are trending up or down in each subsequent version. Its leading score indicates that zScan is the most advanced testing and evaluation service covered in this report.

The embedded, ML-based SDK zDefend provides outputs and configured remedial actions in real time for determining when a user's device is compromised, whether any network attacks are occurring, and whether malicious apps are installed. It is a unique proposition and effectively acts as a self-learning monitoring/analytics tool.

For analytics, zShield provides callouts for hacking and tampering attempts directly into a Zimperium console, which can be easily integrated with a security information and event management system for further analysis and action. Zimperium also provides a threat intelligence service, a thought-leadership proposition that provides security scores, actionable results, clear reports, and identification of mobile risk trends, prompting its advanced capability score for responsiveness to evolving threats.

Analyst comment

Zimperium, while a comparatively newer company than others discussed in this report, is one with a lot of momentum, and the acquisition of highly regarded whiteCryption adds further credibility to its existing comprehensive portfolio. Zimperium's differentiator is its core focus on mobile-app security with a suite that covers all bases in a DevOps process, and its complementary portfolio helps create something more than the sum of its parts.

Zimperium's zDefend and zScan are value propositions in themselves rather than purely just an additional feature to zShield and warrant a high score for their uniqueness and inclusion of useful and value-add features.

As with Digital.ai, Zimperium's app shielding tools are deeply integrated and require significant time and resource to implement. With no option for any cloud-based SaaS platforms or no-code or low-code solutions, potential buyers will need to look elsewhere for simple, easy implementation or products that "tick the box."

Zimperium covers a wide customer base of differing industries but is relatively new to the media and entertainment space. While whiteCryption brings a lot of experience in video applications, gaming applications are currently underserved by this product.

Ultimately, Zimperium is a company that has gathered a significant amount of momentum and seed investment and provides a lot of forward-looking thought leadership around existing and emerging

threats in this space. It has the most comprehensive mobile application security suite of all offerings in this report and should be considered if you are willing to spend time and resources in developing your app security, but its lack of media or gaming experience may mean it is too early to consider its solutions for this type of service in 2021.

Operating systems and platforms supported

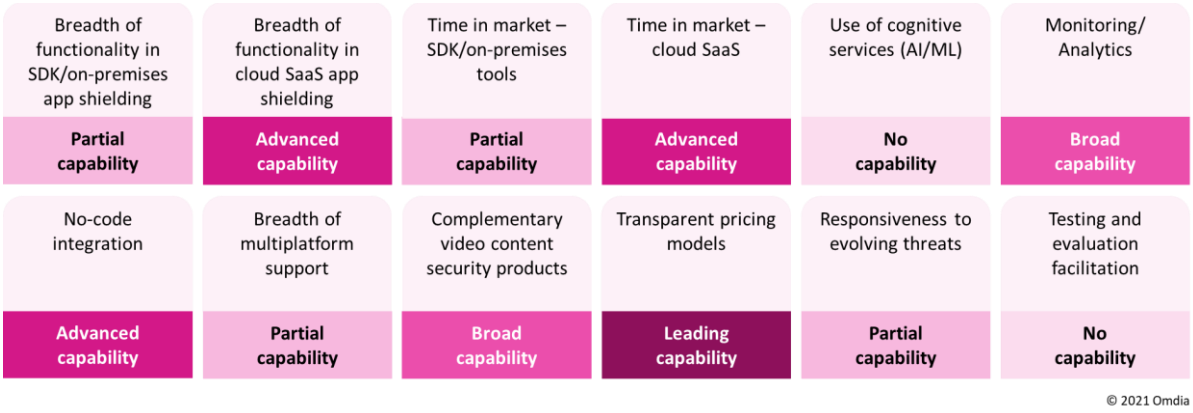
- Android
- iOS
- Hybrid mobile apps
- Web
- Desktop

Product names

- zShield – application shielding
- zKeyBox – cryptographic key protection
- zScan – application security testing
- zDefend – runtime application self-protection

INKA Entworks: AppSealing

Figure 6: AppSealing Omdia acknowledgment: Challenger



Source: Omdia

AppSealing is a subbrand of INKA Entworks, a company based in Asia. INKA Entworks has been operating for more than 20 years and has its roots in developing DRM solutions. PallyCon is INKA Entworks' additional subbrand, focused on content protection and offering tools such as cloud-based SaaS multi-DRM frameworks, watermarking, and piracy monitoring services. AppSealing was spun off in 2015/16 because of a desire to appeal to additional industries; current focuses include protecting gaming and fintech applications as well as video.

AppSealing focuses on mobile applications and has products catering to Android, iOS, and hybrid JavaScript apps. AppSealing protections cover source code protection, app integrity, anti-debugging, network packet sniffing, and gaming-specific cheat tools. AppSealing claims all products have no impact on app performance and do not affect memory, CPU, battery usage, or frames per second.

AppSealing offers a cloud-based SaaS platform for integration of its security functionality. Applications are uploaded to AppSealing's cloud-hosted platform, and protections are automatically applied within a matter of minutes. It is important to note, however, that this is for Android-based or hybrid apps only and excludes iOS. For iOS apps, protection is implemented via a no-code SDK but excludes core protections such as code encryption, anti-tampering/modding, emulator detection, and a host of others. This exclusion for iOS has a direct impact on Omdia's partial capability score for the functionality of AppSealing's on-premises tools.

AppSealing does, however, score highly for transparent pricing. All products are billed through AWS marketplace to simplify the payment process with a price per app or per month model available on the website, with a slider scale displaying the prices for up to 30 million monthly active devices. A 30-day free trial is also available for potential customers wanting to demo its services, operating much like a consumer-facing e-commerce website. Data encryption (white-box cryptography) is available as an add-on feature.

All AppSealing's products are complemented by its monitoring/analytics dashboard, which provides real-time insights into hacking activity, cheating tools, and reverse engineering methodology. Alerts, notifications, reactions, and terminations can also be configured. API hooks are available should a customer want to integrate the data into separate dashboards.

Analyst comment

While it is still a relatively small operation, particularly in comparison with some of the larger vendors in this report, AppSealing's security credentials appear solid. AppSealing's product is primarily suited to the value-end of the market, and although it cites a global customer base, many of AppSealing's reference customers are regional enterprises based in Asia & Oceania. Its core differentiator is its competitive transparent pricing and no-frills experience. However, AppSealing is let down by its comparatively dialed-down offering for iOS products, which offers minimal protection and a different integration method. If you plan to protect an iOS app, this compromise should be considered when you weigh up AppSealing's offering.

AppSealing can be commended for its simple implementation and the inclusion of a monitoring feature in an offering of its scale. Its pricing is competitive and will suit customers just looking for quick and easy security. AppSealing's products are skewed toward gaming applications, with anti-cheat and gaming-specific functionality, so if you have a mobile game based on Android, this solution might work for you.

Operating systems and platforms supported

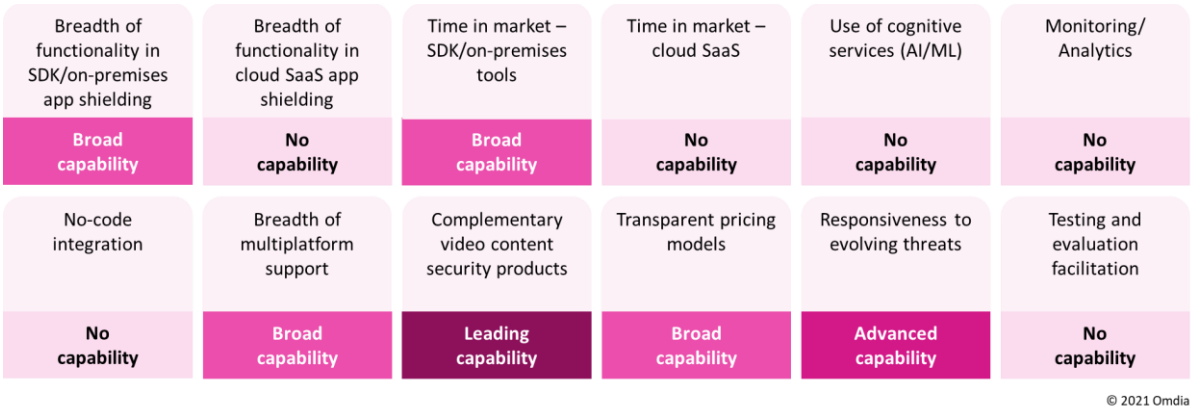
- Android
- iOS

Product names

- Android Application Security
- iOS Application Security
- Hybrid App Security for React Native Framework on Android
- Data Encryption Solutions

Synamedia: OTT ServiceGuard

Figure 7: Synamedia Omdia acknowledgment: Challenger



Source: Omdia

Synamedia's app protection proposition is unique in that it is part of a wider managed service aimed at OTT service providers rather than a standalone proposition. However, its inclusion in this Market Radar is warranted because it includes common functionality such as rooting/jailbreak detection, code obfuscation, and cryptographic key protection. It is important to note that this solution cannot be extrapolated for use for gaming applications or in any other area beside video applications, at least in the immediate future.

Synamedia's OTT ServiceGuard is designed as an end-to-end OTT solution that provides defenses against common vulnerabilities such as a service authorization system, concurrency management system, and content delivery network (CDN) workflows. Synamedia provides software on both the

client side and the cloud side, which prevents pirate scripts from impersonating clients. Therefore, when vendors are opting for this solution, they are protecting not only the apps but also the protocol between the clients and the server. Multi-DRM can also be implemented as part of the solution, using either Synamedia's solutions or those of a third party.

Implementation of app protection is via an on-premises API library, which is integrated into the DevOps process. Synamedia describes its solution as low code because it does not take a long time to reengineer the client. Its solution has negligible effects on performance since its application is more about signing and validating messages, so it does not need to be implemented in performance-sensitive areas. No cloud-based SaaS platform for simpler integration is currently available.

Platform support is broad with the code obfuscation part able to work on any platform, but wider platform rollout support such as for web applications is not yet available. Synamedia does not provide monitoring/analytics with this service as it does with some other video content products such as CSFEye, although synergies are a possibility in the future.

Analyst comment

Synamedia's proposition is strongly positioned for OTT service providers. It includes unique differentiators that go beyond the scope of this report, but adopting those will provide a holistic approach to security for a video service beyond competitive solutions. Its approach to protecting CDN access keys is unique in the market and provides Synamedia's most compelling advantage. OTT ServiceGuard offers premium OTT service providers a high degree of security, not just for apps but also for wider content delivery workflows.

But for buyers with gaming applications or looking to procure standalone app security to add to an already existing portfolio of content security, this solution is likely above and beyond. In comparison with other vendors' offerings, Synamedia's OTT ServiceGuard lacks additional features such as monitoring, testing/evaluation, or cloud-based SaaS tools, which means it has perhaps a lower score on Omdia's matrix than it deserves.

Operating systems and platforms supported

- Android
- iOS
- Hybrid mobile apps

Product names

- OTT ServiceGuard

Appendix

Methodology

Omdia conducted detailed briefings with several rounds of follow-up questions. We also carried out background interviews with a number of companies and software developers within the customer target market. The report was peer reviewed by at least two different analysts.

Author

Luke Pearce, Senior Analyst, Video Tech
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.