Report

Perceptions around cheating, tampering, and piracy – analysis

Publication date:
January 2022

Authors:
Dom Tait, George Jijiashvili, Steve Bailey, Matt Bailey

DENUVO by irdeto

OMDIA

THE BACKGROUND OF THIS SURVEY

To gain insight into the needs and pain points that game developers experience when using cybersecurity products, Denuvo by Irdeto – the world leader in Video Games Protection and Anti-Piracy Technology – conducted a survey in collaboration with Omdia, the leading market analysis company. The survey was sent in October 2021 to a panel of developers run by Omdia and its sister company, GDC. The 70 respondents represented a wide range of geographies, device types and job roles within the game development industry.

Omdia's survey was grouped into four key parts:

1. **Illustrating the challenge**
2. **Awareness and hurdles of adoption**
3. **Competitive intelligence**
4. **Understanding developer needs**

This report analyzes the most relevant findings of the survey.

NB: For the purposes of this analysis, companies have been grouped into three size brackets. Respondents who worked in groups of five people or fewer were categorized throughout this report as independent or indie developers. Developers who worked in companies of six to 99 people were called small-to-medium, and 100+ personnel outfits were deemed large developers.

INTRODUCTION: WHAT IS CHEATING, TAMPERING AND PIRACY?

Cheating

Cheating in a game means modifying it to gain a disproportionate advantage over other players. This can be achieved either by exploiting an internal weakness found within a game, or by using external tools. Cheating causes great imbalance in how other players experience the game and – if left unsolved – can potentially be ruinous to it.

How come? It's simple: players affected by cheating become frustrated and can quickly give up the game, turning to other titles – especially given the wealth of content available. In particular, games based around competitive elements or the use of leagues can be brought to their knees if cheaters aren't tackled at the earliest possible point in time or – preferably – dissuaded from trying.

The threat to user engagement, however, is only half of the problem. The other half is the spread of reputational damage. If a game is known to be struggling with cheating, then why should a player risk giving their precious play time over to the title in the first place? It is not uncommon for gamers' social media accounts to be overrun with requests to developers to sort out these issues; these messages are even published as comments on posts that have little to do with the topic. This may hold back player engagement and, ultimately, future revenue.

Not all games (single-player titles, for example) are wrecked by cheating, but a threat to revenue is serious to every part of the industry.

Tampering and piracy

Tampering means modifying a game in an unauthorized way with an intention to pirate it. This usually involves the creation of a 'crack' or a software patch that allows the game to be shared and downloaded for free, rather than distributed from behind a payment platform.

Piracy has changed over the years based on device. For example, the piracy on console used to be more alarming than it currently is. Without connectivity and regular firmware updates, consoles would be left vulnerable to hardware modifications that were sometimes very easy to make. With consoles now operating 'live' – enjoying regular updates, content delivered via Internet and multiplayer at the heart of experiences – the platform is more easily regulated and so piracy is less of a threat. But the possibility still exists and needs to be guarded against.

By contrast, the openness of PC and mobile operating systems represents an ongoing vulnerability – they can be easily pirated. While some may argue that piracy leads to an increase in user engagement, it is engagement that exists outside of the usual parameters of business operations, especially distribution and player retention. And as a game evolves, its design and content tend to change significantly via authorized patching. This means that cracked versions start to diverge from what the gaming company is attempting to offer.

For single-player games sold upfront, the opening weeks can be a particularly critical sales period given how the commercial cycle differs from 'live' multiplayer games. Any piracy here could be particularly impactful, compared with later periods in that title's lifespan.

Tampering can also affect monetization beyond upfront payments, or for free-to-play games. For example, players can access in-game currency or items that otherwise require significant investment of either time or money to achieve, weakening the sense of value for legitimate players.

ILLUSTRATING THE CHALLENGE

Cheating, tampering, and piracy – levels of concern

The survey opened by establishing the scale and nature of the challenge faced in protecting games from cheating, tampering and piracy. **In total, 70% of all respondents find cheating some sort of concern, a feeling that increases among larger companies, where 85% express worry. Indie developers, by contrast, are the least concerned, perhaps tending to view any form of interaction with their game as good, regardless of whether that comes in the form of cheating or not.**

These concerns increase when it comes to tampering and piracy – 84% of all respondents state their concern about this aspect, with reasonably consistent views across both studio size and device type. The level of concern is also high, with 56% of respondents calling tampering and piracy either a moderate or major concern, compared with only 39% for cheating. Taken together, this characterizes a simple truth: not all games (single-player titles, for example) are wrecked by cheating, but a threat to revenue is serious to every part of the industry.

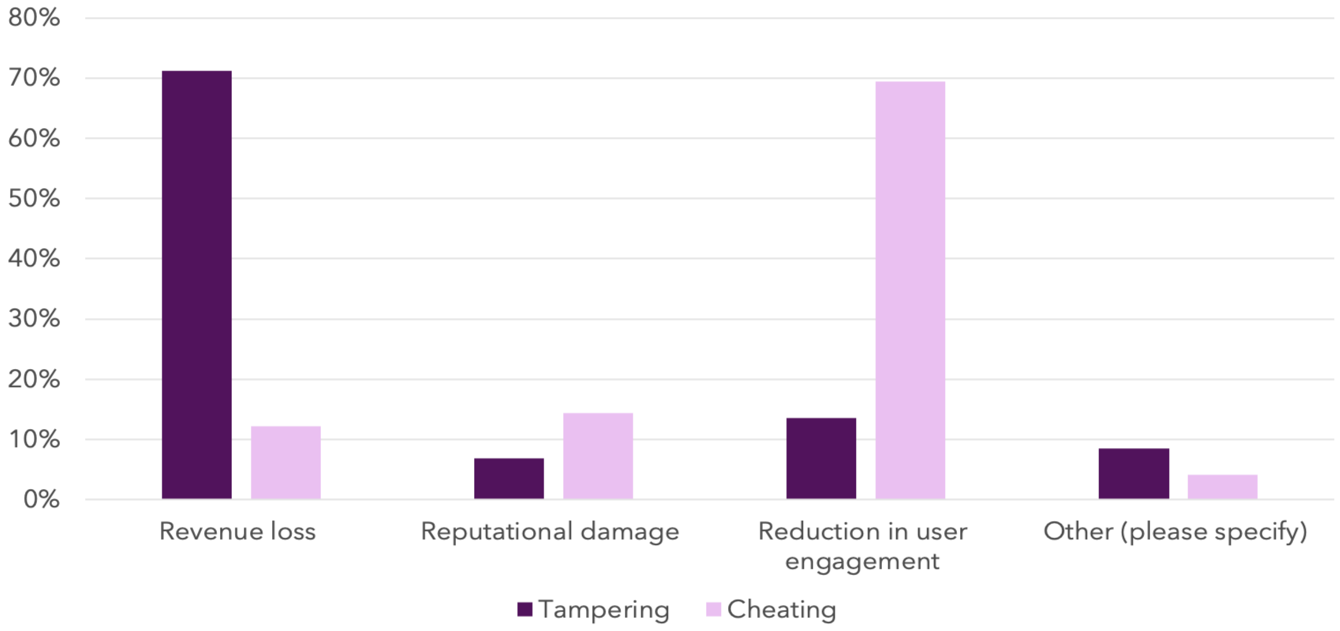
84%

of all respondents have concerns about tampering and piracy

70%

of all respondents find cheating concerning

What is your primary concern about tampering and cheating?



The key concerns

The responses in our survey represent a clear call to action for cybersecurity companies that protect games revenue streams. The concerns about tampering and piracy confirm it – 71% of respondents cite revenue loss as the primary problem and the guiding fear. Simply put, tampering and piracy are more of an immediate threat to both the gross sales and the net income. With cheating, however, for 69% of respondents reduction in user engagement is the top concern – which makes perfect sense as it usually precedes revenue loss.

When asked to put a hard figure on the revenue loss attributable to cheats and pirates, the opportunity cost – and the need for further education – becomes clearer. Nearly 20% of respondents felt that 6% or more of their revenue had been impacted by some kind of foul play, while only 16% believed they were entirely unaffected by this. Tellingly, nearly 40% more simply didn't know to what degree they had been affected, a figure which rose precipitously to 54% among indie developers.

71%

of respondents cite revenue loss as the primary problem of tampering

69%

of respondents are concerned cheating will result in reduction in user engagement

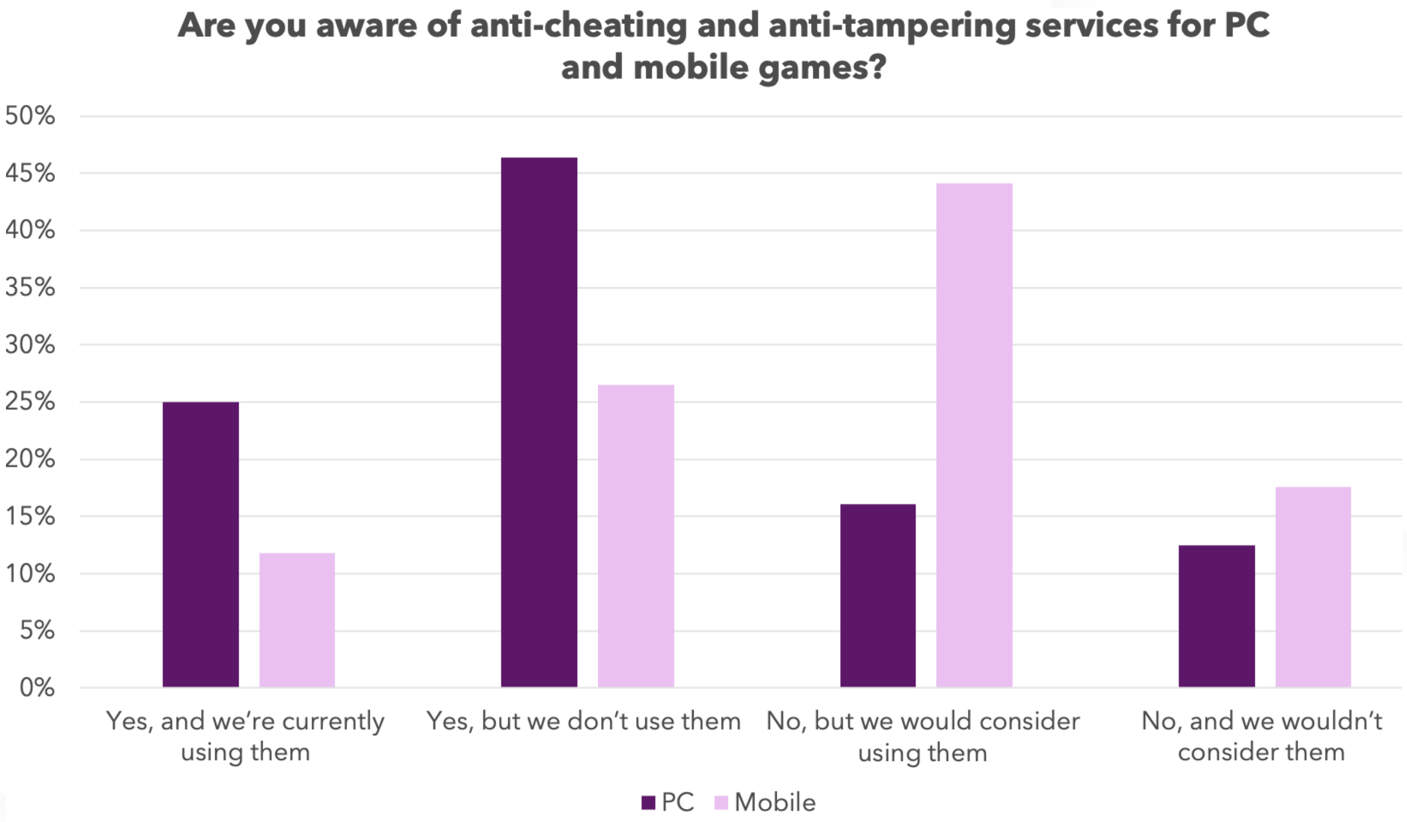
AWARENESS AND DIFFICULTIES OF ADOPTION

How well-known are anti-cheat services?

In terms of fixing this problem, it turns out that there is a real gulf in awareness about the available options between PC and mobile game developers. While 71% of PC game makers know of the existence of anti-cheat and anti-tamper services, this figure falls radically to 38% for mobile developers. However, this highlights a major opportunity too. In total, 44% of mobile games developers say they would consider the use of anti-cheat software now that they know it's there and are aware of the options.

This willingness to invest in anti-cheat on mobile spans across all team sizes, with indies the most likely to consider anti-cheat technologies use at 57%. It becomes clear that smartly positioned anti-cheat and anti-tamper software targeted at mobile games developers could well enjoy a market.

As for those anti-cheat services which already enjoy market recognition, a clear divide emerges between three leading providers and the rest. Easy Anti-Cheat, Denuvo by Irdeto and Battleye take the top three slots here with 45%, 38% and 32% of developers being aware of them respectively.



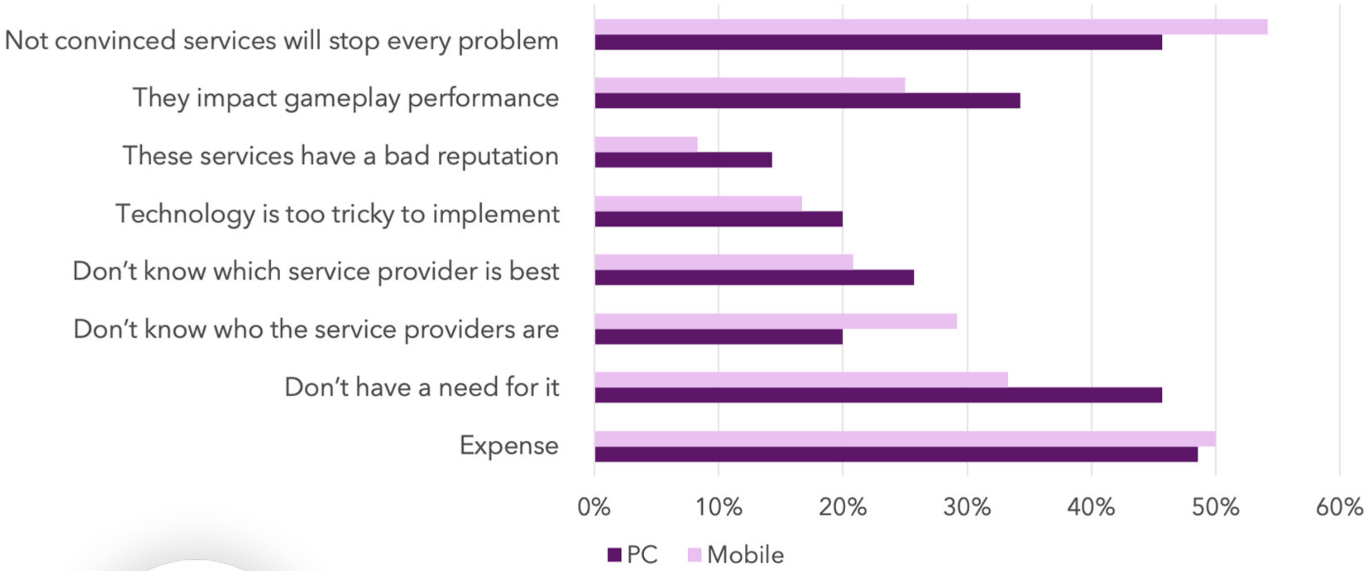
Tencent somewhat bridges the gap to the rest with 23%, but with the Chinese tech giant operating in so many spheres, name familiarity may come from some other aspect rather than its anti-cheat services. No other service makes any real impression, with 28% of respondents having heard of none on the list.

Developer resistance explored

What's also clear, however, is that there remains resistance to anti-cheat services. 26% of mobile developers and 46% of PC game makers are aware of anti-cheat solutions, but do not wish to make use of them. Of course, cheating will not keep developers of single-player titles awake at night. When it comes to titles featuring elements of competition, however, the dominating false perception that anti-cheat services will not solve every problem needs to be addressed by marketing messages.

Concerns around costs also feature highly and are the top answer for PC developers. 46% also believe they simply don't need anti-cheat solutions or anti-tamper software. To correct this impression, cybersecurity companies need to clearly articulate their value proposition while highlighting the revenue or reputational threat of inaction.

What are your reasons for not seeking out anti-cheat or anti-tamper services for your PC and mobile games?



46%

of PC game makers are aware of anti-cheat

26%

of mobile developers are aware of anti-cheat

46%

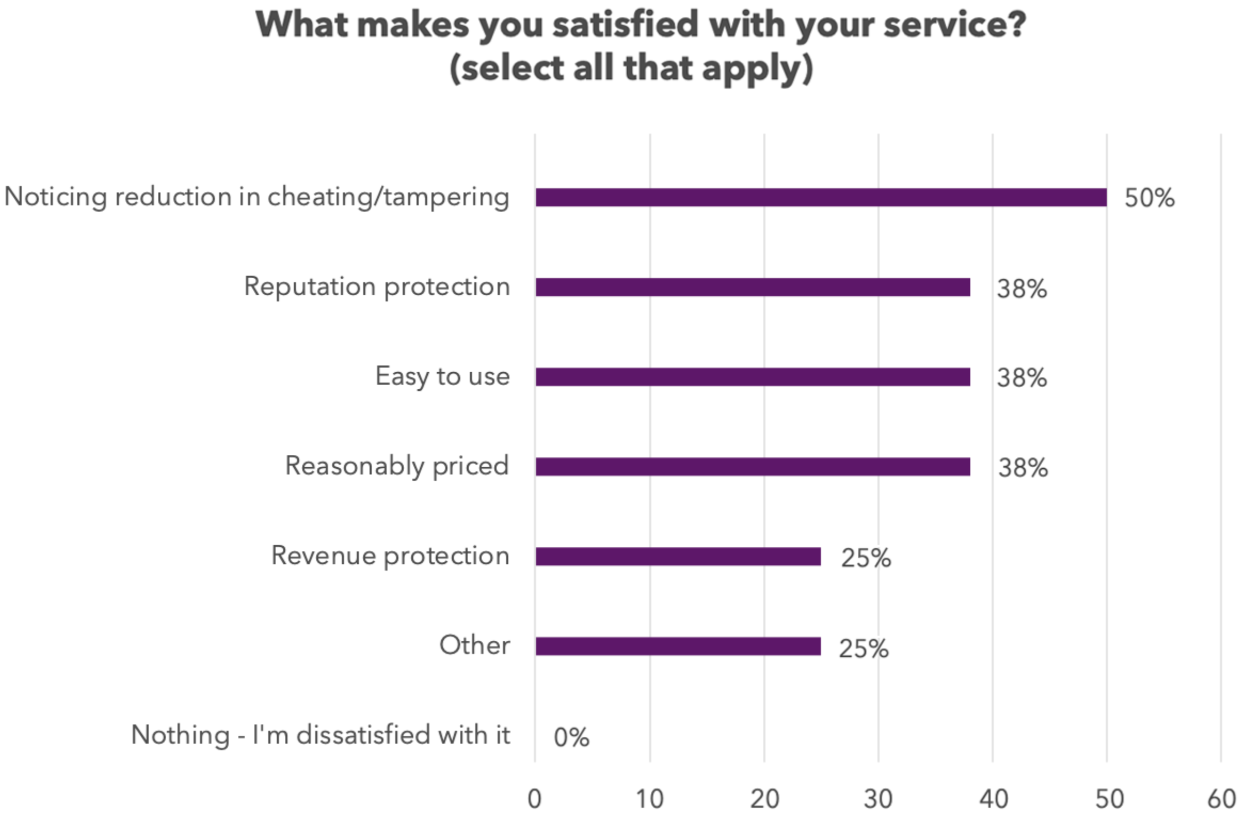
believe they simply don't need anti-cheat or anti-tamper software

MARKET LANDSCAPE

The solution and its benefits

Just over 20% of respondents use an external company for their anti-cheat and anti-tamper services, either on its own or alongside an in-house solution. This is surprising, considering cybersecurity companies are the experts on this and can help the game developers keep their content safe. This is a relatively small proportion, albeit one that rises to 35% for large companies. An eye-catching statistic is that almost no indie developers use anti-cheating services, again most likely tied to such developers being focused on single-player titles.

What is equally clear, though, is the value derived by those implementing such services: **93% of those who use anti-cheat and anti-tamper software indicate they are satisfied** to some extent with what they have in place. But surprisingly, 50% of respondents state that they've experienced a reduction in cheating and tampering after implementing game protection technology, a similar percentage believes that such services will not fix every cybersecurity problem. Ease of use, competitive pricing, and, of course, protection of reputation and revenue are also frequently cited as the positives of such services. There is a strong disconnect, then, between the positive experiences and negative beliefs which needs to be bridged.



What also comes through from the results of this survey is that game developers should choose services that are as non-invasive and non-interruptive as possible. While better detection and more streamlined integration will be crucial in increasing the perceived value of such services, new and upgraded features must not impact the core gaming experience or the entire enterprise fails. Clearly, not impacting the player experience is as top-of-mind for developers and publishers as it would be for consumers.

UNDERSTANDING DEVELOPER NEEDS

Top security concerns

In terms of current developer requirements regarding the dark arts – that is techniques or practices that are regarded as mysterious or dishonorable – **piracy remains top of mind for all company sizes**. For indies, in-game currency cheats are of higher concern than Player vs Player (PVP) cheating. Aside from such cheats directly impacting the bottom line, this is probably due to the fact that their smaller audience bases make such manipulations more obvious, and because of the lower prevalence of PVP functionality in indie games.

Proportionately, indies are the most concerned about piracy, with large developers the "least" concerned of all developers, albeit this remains their top-rated threat. Again, this is likely due to economies of scale meaning that pirated copies have a much more direct impact on the top and bottom line of indie games compared with larger titles. Even so, large companies still cite piracy as their biggest concern.

IP theft, by contrast, is relatively low in the pecking order of ongoing concerns, but is a more common issue for large companies, which tend to have more valuable IP and are more prominent targets for hackers and other criminal activity.

Mobile developers are just as concerned about in-game currency cheats as they are about piracy, and for mobile-only publishers, in-game currency cheats become the clear leader in terms of ongoing concern. This is likely due to the fact that mobile games remain highly dependent on in-game currency-based transactions (that is, in-app purchases) for the bulk of revenue generation. So, making this the lead feature of any mobile-focused anti-cheat services will likely appeal to the largest proportion of prospective mobile-focused customers.

PVP cheating is also a relatively high concern for mobile developers and is more prevalent across those that develop for mobile in addition to other platforms, likely because such cross-platform games have a higher chance of being competitive titles.

Mobile developers are just as concerned about in-game currency cheats as they are about piracy.

Funding protection

The industry has different pricing models available for game developers. Generally speaking, a variable pricing model seems to be favored by indie developers while AAA developers seem to be more in favor of a fixed-price model. On average, respondents would be willing to pay between 0.5% and 1% of their revenue for cyber security services. Importantly, medium and large developers tend to be willing to spend lower percentages of revenue than indie developers, reflecting expectations of economies of scale.

However, there is still a small number of respondents that are willing to spend over 5% of revenue on such solutions, and over 10% of large developers are ready to spend more than 10%, demonstrating how seriously they take this issue.

CONCLUSION

The end comments from those taking the survey were typically illuminating. One respondent noted how Easy Anti-Cheat "was on the cutting edge" of protection until they became "just another Epic Games store service provider", showing a clear opportunity to differentiate through innovation. Another noted: "Most of our piracy occurs in regions where they don't have easy ways to purchase the game", indicating that emerging markets without payments infrastructure make piracy a case of addressability as much as anything else.

Consumer perception, once again, was a key concern. One respondent voiced their wish for "a robust spectating mode… so that players can submit blatant captures of cheating to review". Reducing complacency needs to be addressed too. "Piracy will still happen and from everything I've seen it doesn't significantly impact sales", wrote one indie developer. Anti-cheat and anti-tamper software may well have progressed faster than developer perception of such software, demonstrating the critical importance of education campaigns.

This survey's critical findings, then, are that despite cheating, tampering and piracy being a stated threat to developer reputation and revenue, too many of them do not know what solutions are available, or – if they do – they are uncertain about their efficacy. However, once sampled, developer satisfaction with products addressing these problems is clear. If providers of anti-cheat and anti-tamper services can tackle this knowledge gap, they can help protect the integrity of games to the benefit of all industry players.

APPENDIX

The survey and this report were commissioned by Irdeto and carried out by Omdia

Authors

Dom Tait
Research Director, Games
Dom.Tait@omdia.com

George Jijiashvili
Principal Analyst, Games
George.Jijiashvili@omdia.com

Steve Bailey
Principal Analyst, Games
Steven.Bailey@omdia.com

Matthew Bailey
Principal Analyst, Games
Matthew.Bailey@omdia.com

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 supportbusiness 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.

Denuvo by Irdeto is the world leader in gaming security, protecting games on desktop, mobile, and consoles. Denuvo provides core technology and services for game publishers/platforms, independent software developers, e-publishers and video publishers across the globe, enabling binary protection for games and enterprise applications across multiple platforms. Denuvo's gaming security solutions prevent piracy and expose cheats in competitive multiplayer games, empowering publishers to innovate while also protecting their revenue, the integrity of their game, and the gaming experience. With a rich heritage of security innovation and rapid adaptation to the changing demands of the cyber security space, Irdeto is dedicated to being the security partner to empower a secure world where people can connect with confidence.

www.omdia.com
askananalyst@omdia.com

https://irdeto.com/denuvo/
support@denuvo.com

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") 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 and agents, 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.

Irdeto is the world leader in digital platform cybersecurity, empowering businesses to innovate for a secure, connected future. Building on over 50 years of expertise in security, Irdeto's services and solutions protect revenue, enable growth and fight cybercrime in video entertainment, video games, and connected industries including transport, health and infrastructure. With teams around the world, Irdeto's greatest asset is its people and diversity is celebrated through an inclusive workplace, where everyone has an equal opportunity to drive innovation and support Irdeto's success. Irdeto is the preferred security partner to empower a secure world where people can connect with confidence.

Last modification: 25-01-2022 / 12:55 pm GMT+01:00