

Report



# Mobile games development in 2022: trends, challenges and solutions

**Publication date:**  
November 2022

**Authors:**  
Liam Deane, Dom Tait

**DENUVO**  
by **irdata**

**OMDIA**



## BACKGROUND

Irdeto, the digital platform cybersecurity company, has several solutions for anti-tamper, anti-cheat and mobile game protection aimed at game developers.

To support this, Irdeto sponsored a survey of mobile game developers. The aim of the survey was to gain insight on the needs and pain points that developers experience when using security products. Omdia produced an online survey taken by 200 respondents in August/September 2022 across a wide range of geographies, device types and job roles in the mobile games development industry. Omdia's survey was grouped into four parts:

1. Expository questions
2. Trends in mobile gaming
3. Challenges in mobile gaming
4. Security solutions

**NB:** For the purposes of this analysis we have grouped companies into three size brackets. Respondents who worked in groups of 49 people or fewer were categorized throughout this report as independent or indie developers. People who worked in companies of 50 to 500 people were called small-to-medium and 500+ personnel outfits were deemed large developers.



## THE SURVEY

This report is based on a comprehensive survey of mobile games developers. The fieldwork for this survey, carried out by Omdia in partnership with Irdeto, was conducted in August and September 2022 and garnered responses from 200 mobile games developers across nine territories in Asia Pacific, North America and Europe. This large and varied sample ensures a robust set of findings on the state of mobile games development in 2022. In total, 74% of respondents worked in information technology or software engineering, making this a highly technically informed sample — while further respondents in functions such as senior management, art and design and operations provide a broader perspective.

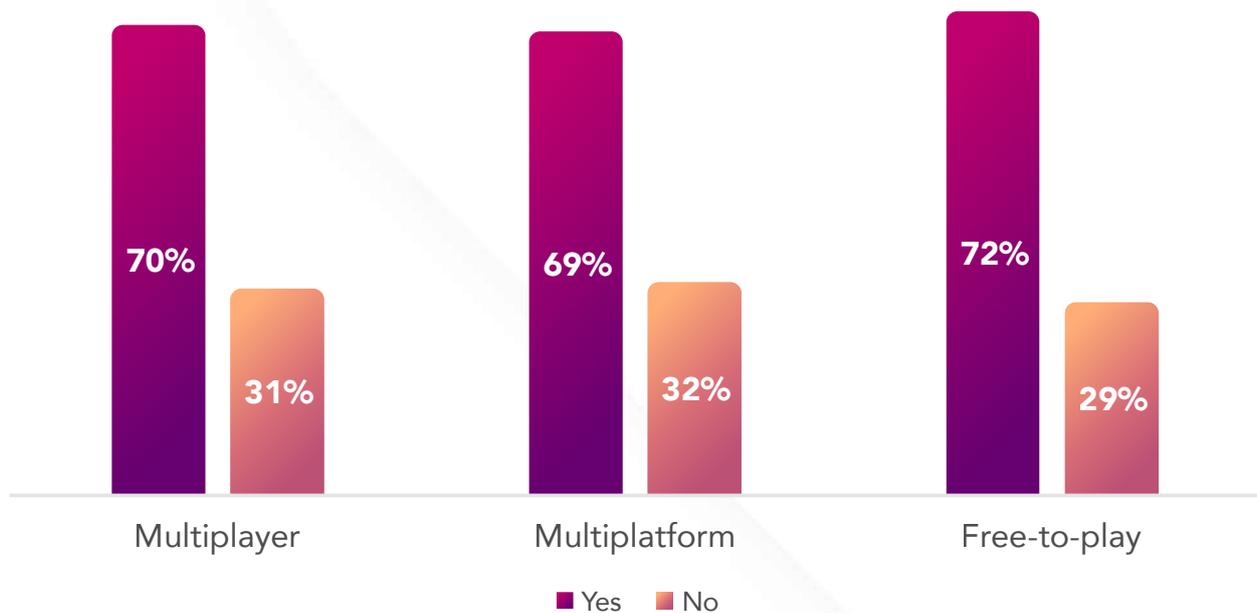
The sample also cuts across the mobile market in terms of company size. At the lower end, 24% of respondents worked in companies of up to 49 employees. The majority of the sample, 57%, came from companies of between 50 and 500 employees, the range in which most mid-sized mobile game developers sit. A further 19%, meanwhile, work at companies of more than 500 people, which in a mobile games context defines the biggest companies producing technically demanding, visually impressive (so-called 'AAA') titles and the biggest and most popular mobile games.



## THE STATE OF MOBILE GAMES

Three key trends are playing an increasingly central role in the modern mobile games market: the rise of online multiplayer, free-to-play and multiplatform development. While all three have existed for some time, this survey confirms that these have all become defining traits of the mobile games market.

**Figure 1: What would best describe your current, or most recent, mobile game?**



Over 80% of developers describe their current or most recent mobile game as multiplayer, with less than 20% working on a single-player title. Multiplayer games development is inherently more complex than single-player and entails a raft of additional challenges including managing game servers, matchmaking and chat and communications. Multiplayer games are also vulnerable to cheating — players will try to find any edge in competitive games, forcing developers to take measures to ensure fair competition.

As well, multiplayer, mobile games are increasingly multiplatform. No less than 69% of mobile developers have released a multiplatform title — that is, available on mobile and also on PC or console (or both). A further 26% have plans to go multiplatform in future. This means that, in total, a remarkable 94% of mobile developers either have already, or plan in future, to develop across multiple platforms. The success of games like Fortnite and Genshin Impact in developing seamless experiences across mobile, PC and console has been a major inspiration for developers aspiring to go multiplatform. This presents another complicating factor, however: multiple platforms means working across a wider variety of hardware, operating systems and licensing systems, meaning more cost and more complexity for developers.



But perhaps even more profound than these two trends is the decisive shift to free-to-play. 72% of surveyed developers reported that their current or most recent game is free to download. A large majority of projects are free-to-play across all studio sizes, with 69% of indie and midsize developers working on free-to-play games, rising to 82% among those working at the largest development studios. We can see that while free-to-play business models were initially driven by the larger studios which realized some years ago that this was the most profitable business model for mobile games, it has now trickled down to all segments of the mobile games market.

Just like the growth of multiplayer and multiplatform development, free-to-play too introduces additional challenges and complexity for developers. For a start, free-to-play is not a single business model, but a variety. The majority of developers (60%) utilize paid in-game items, a mainstay of free-to-play games. But this is supplemented by a variety of other revenue streams. Lootboxes, subscriptions, battle passes and a variety of forms of advertising are all employed by many developers.

Interestingly, however, none of these are used by a majority of developers, with most clustering in a range between 30-40%, indicating a diverse selection of monetization mechanisms are being employed to suit the characteristics of different games and audiences. Ultimately, there is no one-size-fits all solution for game monetization. Each game has different mechanics and a different audience, making selection of an optimal business model yet another complex task faced by developers.

**Figure 2: What business model(s) are you using for your current or most recent mobile game?**



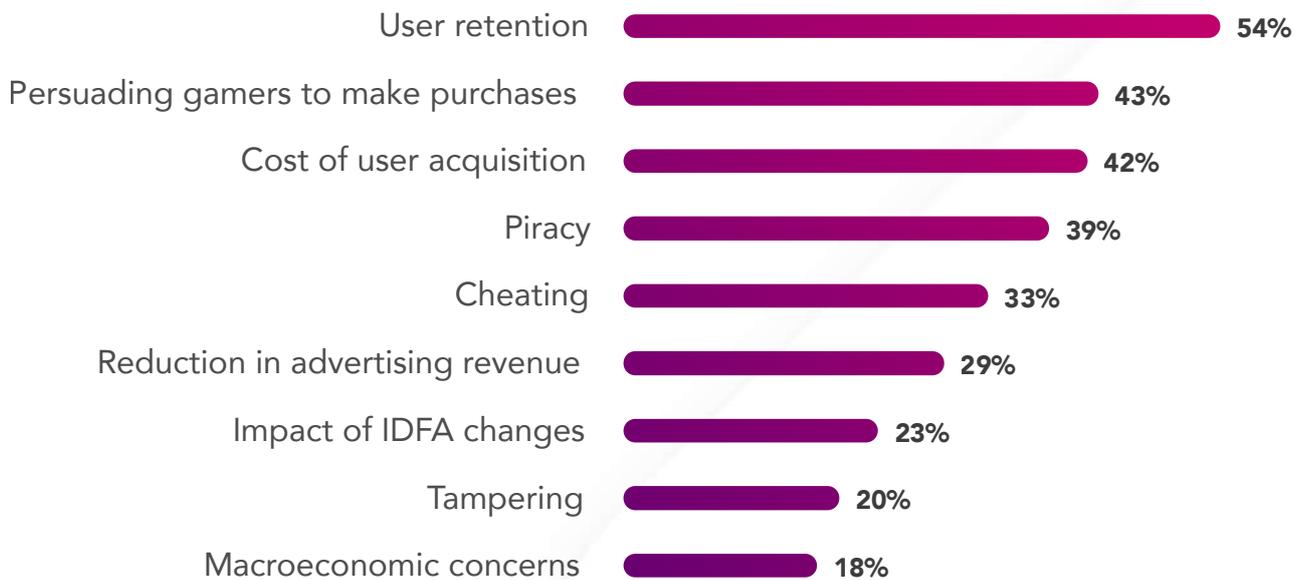
Regardless of the exact monetization streams, something that all free-to-play games have in common is the need to drive user acquisition, engagement and retention. With revenue earned not at a single point of purchase but over time, the key for developers is to maximize the number of users playing the game and to keep them engaged. This means not just attracting players, but also providing them with a steady stream of new and engaging experiences. As we will see, this is the number one challenge facing mobile game developers today.

## UNDERSTANDING DEVELOPER CHALLENGES

The common thread between the three key trends of the growth of multiplayer, multiplatform development and the rise of free-to-play is that they all make development harder and more complex. Moreover, they have compounding effects on each other. For instance, implementing multiplayer across several platforms is far more complicated than on just one. Similarly, differing policies on payments and advertising across platforms makes it a challenge to operate free-to-play business models cross-platform. And implementing in-game purchases of items and power-ups in a way that maintains a balanced and fun multiplayer experience is tricky to pull off while keeping content refreshed over a game's lifetime — particularly as it can incentivize players to cheat and tamper with game systems, potentially undermining the experience for other players and impacting revenue streams for developers.



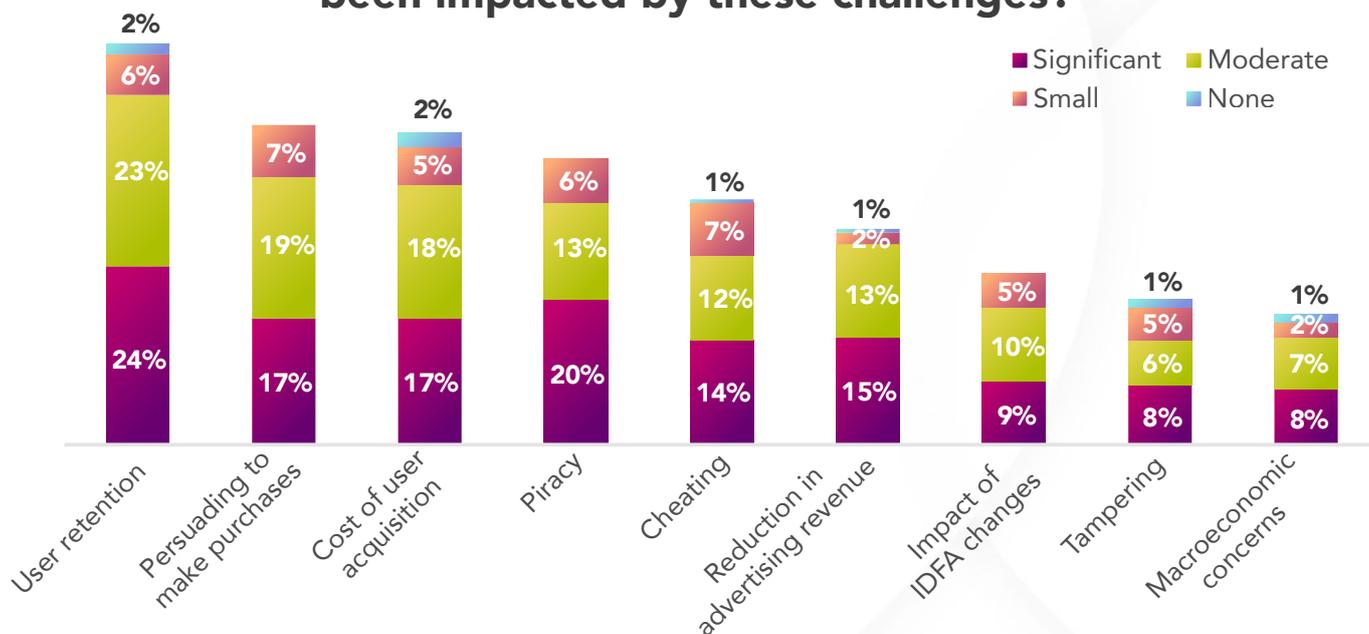
**Figure 3: Which of these are the biggest challenges for mobile gaming right now?**



All of this adds up to an unprecedentedly complex and challenging development environment for mobile games. When asked to consider specific challenges, the number one issue cited by mobile game developers is user retention (54% of respondents), followed by persuading free-to-play gamers to make microtransactions (43%) and the cost of user acquisition (42%). These are the core challenges of implementing a profitable free-to-play business model, so it's no surprise to see them top of mind among developers. The next biggest group of concerns centers around security, in particular piracy (39%), cheating (33%) and — to a lesser extent — tampering (20%).

Developers were also asked to consider to what extent each of these challenges impacted on revenue. We see a similar picture by this measure, with user retention perceived to cause the biggest hit to revenues — 47% of developers estimate that revenue had been impacted to a moderate or significant extent. Persuading gamers to make purchases and user acquisition were also highly likely to be linked directly to revenue impacts. In terms of security threats, piracy was strongly linked to revenue loss, with 33% reporting a moderate or significant impact on revenue. This is significantly higher than the proportions who cited direct revenue loss due to cheating (26%) and tampering (14%).

**Figure 4: To what extent would you estimate revenue has been impacted by these challenges?**



However, developers may be underappreciating the degree to which security threats are deeply connected with the other challenges impacting their revenue streams. One particularly notable statistic is that though the biggest cost for most mobile game studios is user acquisition — often running to many times the core cost of game development — it is user retention that is rated as the number one challenge and the number one impact on revenue. This reflects the fact that while user acquisition is expensive, it is a relatively well-addressed problem with many companies specializing in helping mobile developers reach their target audience. Keeping users engaged, on the other hand, is a challenge which developers have fewer tools to address.

It's clear that there is a strong link between concerns around user retention and around security. That's because cheating, tampering and piracy are major drivers of player churn and minimizing them is one of the most effective steps developers can take to improve retention. In fact, this is just one example of the many respects in which security is a critical issue for mobile games in a multiplayer, multiplatform and free-to-play world.



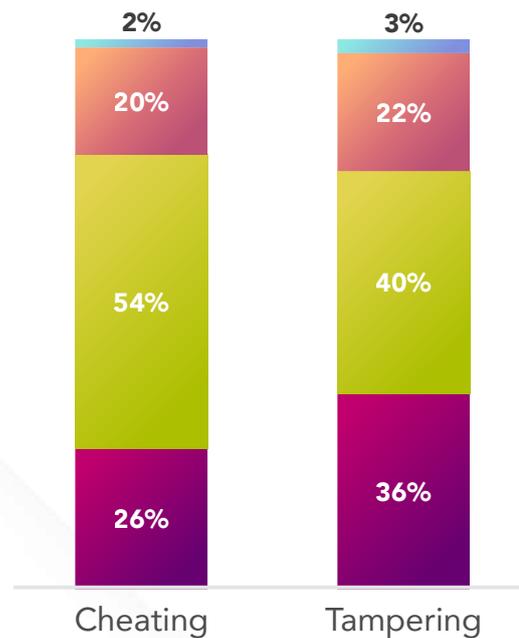
**Piracy was strongly linked to revenue loss, with 33% reporting a moderate or significant impact on revenue**

# SECURITY IN THE MODERN MOBILE GAMES MARKET

Developers are well aware of the importance of security for mobile games. 79% of developers consider cheating to be a major or moderate concern, while 76% are similarly concerned about tampering. Notably, while the share of developers expressing some level of concern about tampering is slightly lower, tampering actually ranks higher when it comes to major concerns, with 36% of developers putting tampering in this category, compared to 26% for cheating. This shows that while tampering may be less high-profile compared to cheating, a growing share of developers are recognizing the seriousness of the problem.

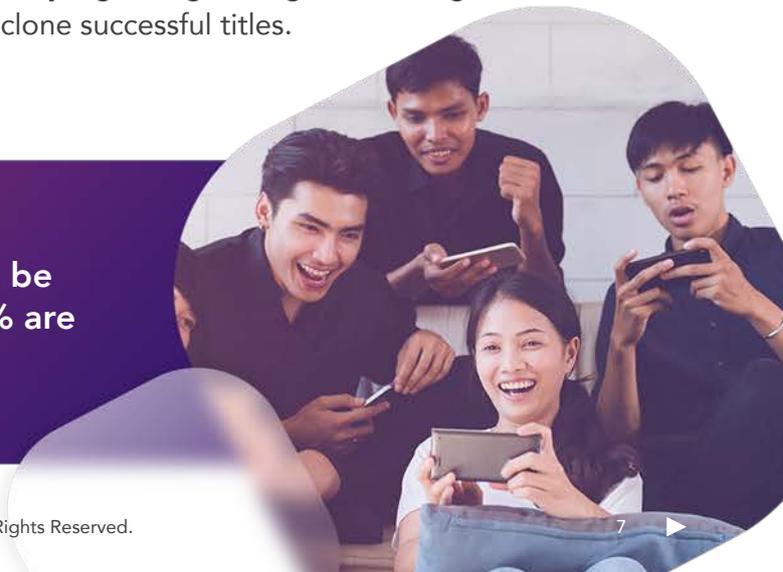
**Figure 5: Slightly more developers are concerned about cheating, but tampering is more likely to be a major concern**

- Major concern
- Moderate concern
- Minor concern
- No concern

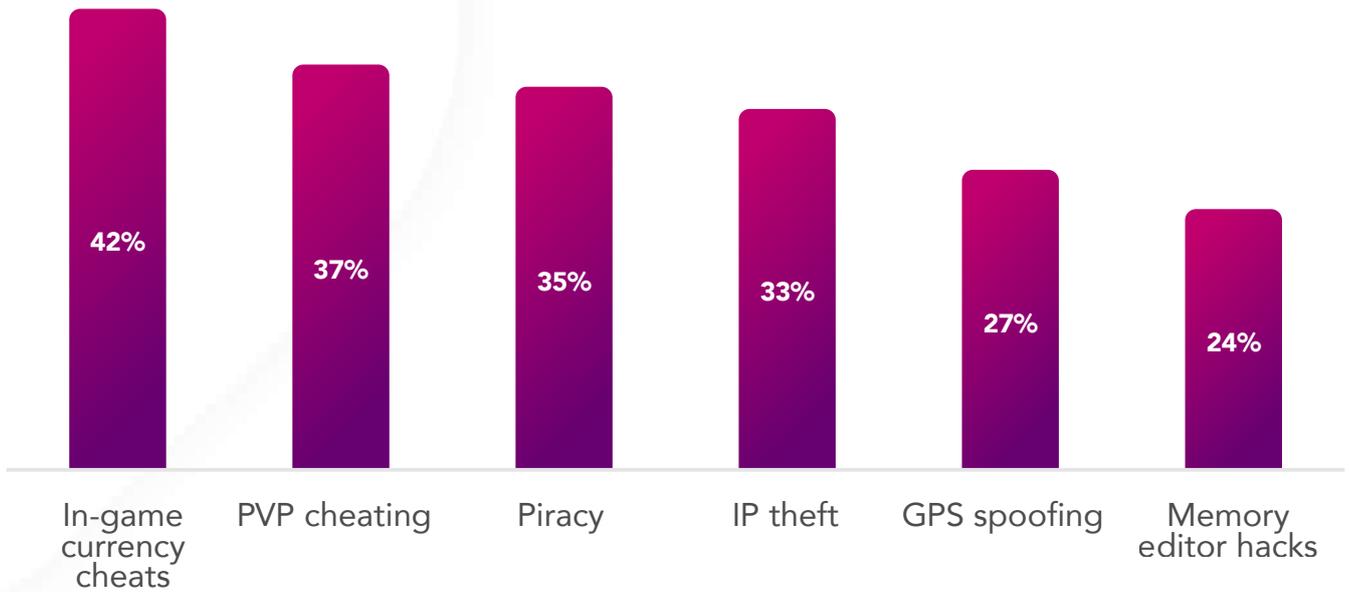


Significantly, the leading specific security problem cited by developers was in-game currency cheats. This is a form of tampering in which attackers exploit vulnerabilities in game code to freely award themselves in-game currency. From the point of view of developers, in-game currency cheats are particularly insidious as they undermine the competitive balance (by unfairly giving some players an advantage) and also often hurt the monetization of the game (by circumventing the need to buy in-game currency, for games that offer that option). Currency cheats rank ahead even of traditional player-vs-player (PVP) cheating, where players use cheats to directly gain an advantage in multiplayer contests. Traditional piracy is the third highest concern, followed by IP theft — unfortunately a growing issue given the large number of unscrupulous ‘copycat’ developers that aim to rapidly clone successful titles.

**79% of developers consider cheating to be a major or moderate concern, while 76% are similarly concerned about tampering**



**Figure 6: Are there any specific security problems that you are still having issues with?**



When asked to specify their reasons for concern about cheating and tampering, developers cite revenue loss, reputational damage and reduction in user engagement approximately equally. This is not unexpected given that, as we have seen, all of these issues are deeply interrelated. Significantly, while there is variation among developers in the level of concern attached to these challenges, there is essentially universal recognition that they are a problem to at least some degree: just 1% say they have no concerns at all.

It comes as no surprise, then, that developers are motivated to scale up their security efforts. Some 30% of developers feel that their efforts to ensure security in mobile games should be greatly increased over the next 12 months, while another 58% feel they should be somewhat increased. This means that in total 88% of developers recognize the need to take steps to improve security in the immediate future.

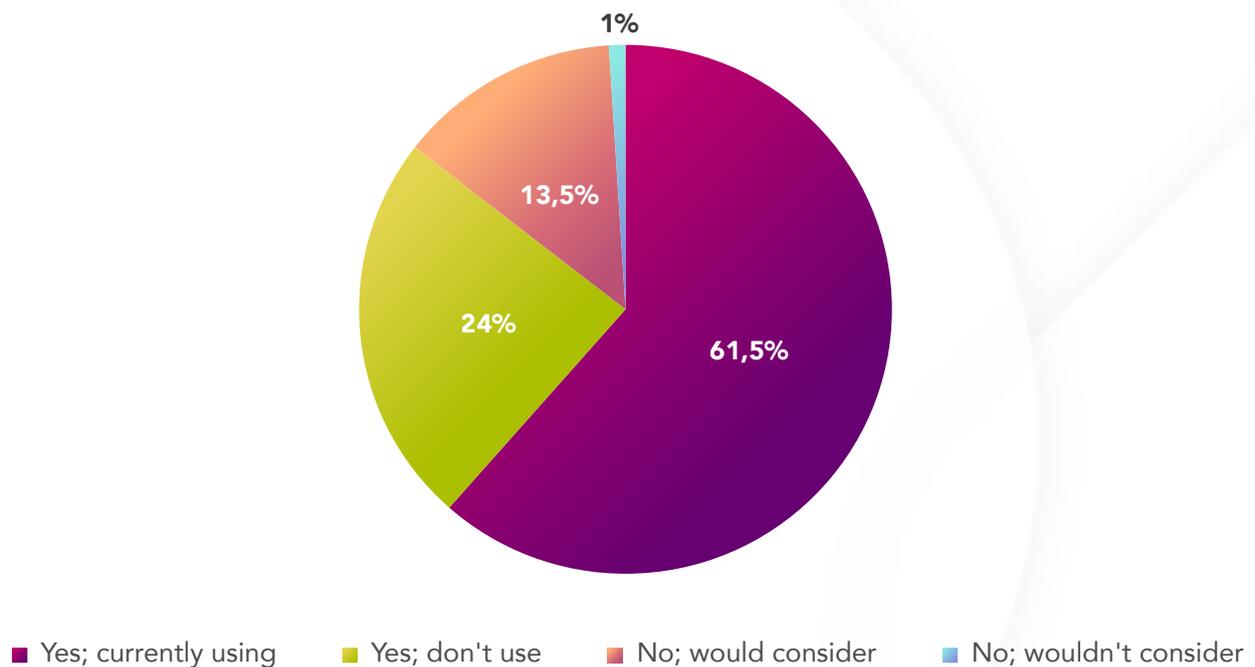
Happily, developers now have more options to address these challenges than in the past. High proportions — over 80% in each case — express confidence that their company is equipped to address the problems of cheating, tampering and piracy. Very likely, this is to a large degree the result of increasing awareness of security solutions for mobile games. A full 86% of developers are now aware of anti-cheating and anti-tampering solutions for mobile games. This is a far higher proportion than has been found by similar surveys in the past and reflects the rapid move into the mainstream of mobile games security solutions. Far from being a niche product, these services are now used by a clear majority (62%) of developers.



**Only 1% have no concerns on cheating and tampering**



## Figure 7: Are you aware of anti-cheating and anti-tampering services for mobile games?

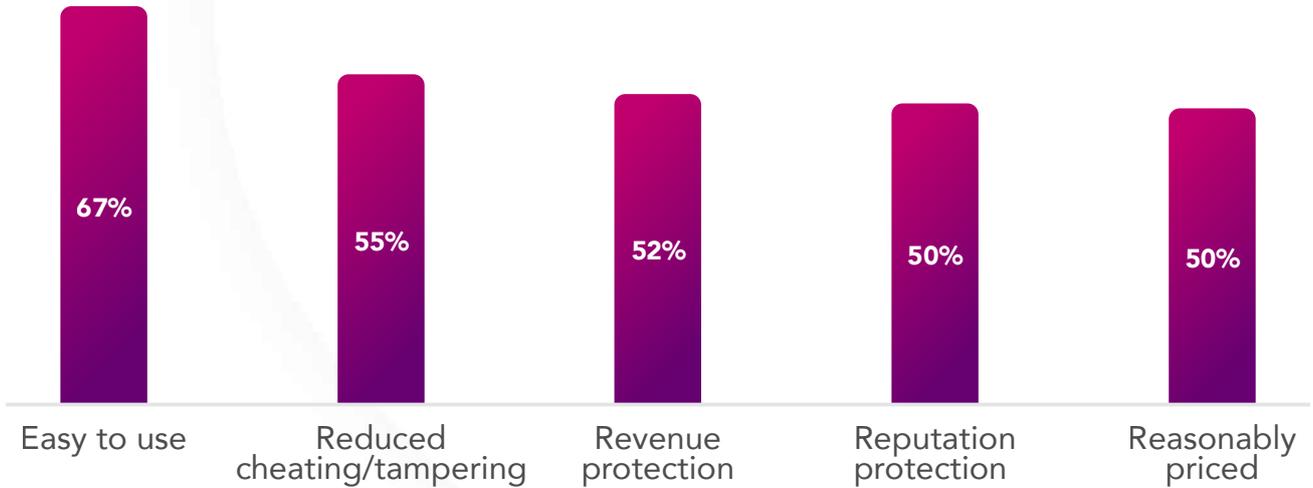


Digging a bit deeper into the types of solutions being utilized, we can see that developers are employing a range of strategies to ensure a secure experience in their games. Only one in eight of those employing anti-cheat/tamper measures rely purely on in-house solutions, which place a high burden on developers who do not necessarily have strong security expertise in-house. Significantly more, 31%, rely instead on solutions provided by specialist external companies. Interestingly, however, the most popular option, employed by 56% of developers, is to combine in-house solutions and external ones. For many studios, this is an effective way of maintaining an optimal balance of cost and expertise.

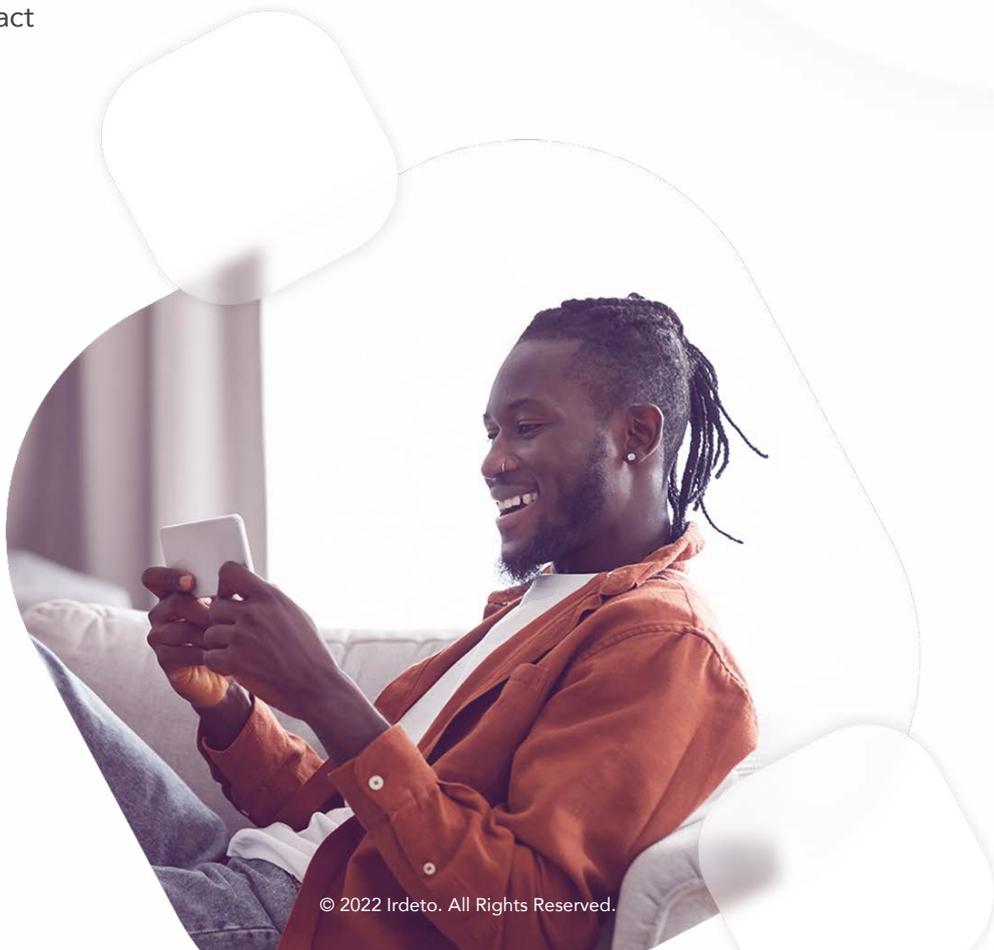
What is driving the uptake of mobile game security solutions? Positive customer experience is a clear driver, with virtually all users of anti-cheat and anti-tampering services feeling extremely (28%) or quite (69%) satisfied with their current provisions. The leading reason that developers express satisfaction is that their service is easy to use, which is reported by 67% of respondents. This is a very high priority among developers, who are loath to complicate their development workflows unnecessarily. It's fortunate, then, that developers predominantly do find mobile game security solutions easy to use. Other major reasons for satisfaction include a noticeable reduction in cheating/tampering (55%) and confidence that revenue is being protected (52%).

**87% of developers rely on external security company to some extent to keep their games safe**

**Figure 8: What, if anything, makes you satisfied with your service?**



However, given that a significant percentage of mobile game developers are yet to adopt security solutions, it is also worth considering reasons for dissatisfaction. On the negative side of the ledger, we see that 30% of users feel they are still suffering revenue loss, while 29% report a negative impact on gameplay performance. These concerns are comfortably outweighed by the positives — for instance, far more respondents (52%) cite satisfaction with revenue protection they receive than those dissatisfied. What's more, it is notable that respondents provided nearly twice as much feedback on reasons for satisfaction than for dissatisfaction; highlighting the overall positive experiences of security solutions. On average, respondents selected 2.8 different reasons for satisfaction with their service, but only 1.6 reasons for discontent. Nonetheless, it's clear that not all security solutions are perfect and developers must take care in selecting the right provider for their game to reach the right balance of cost, effectiveness and performance impact



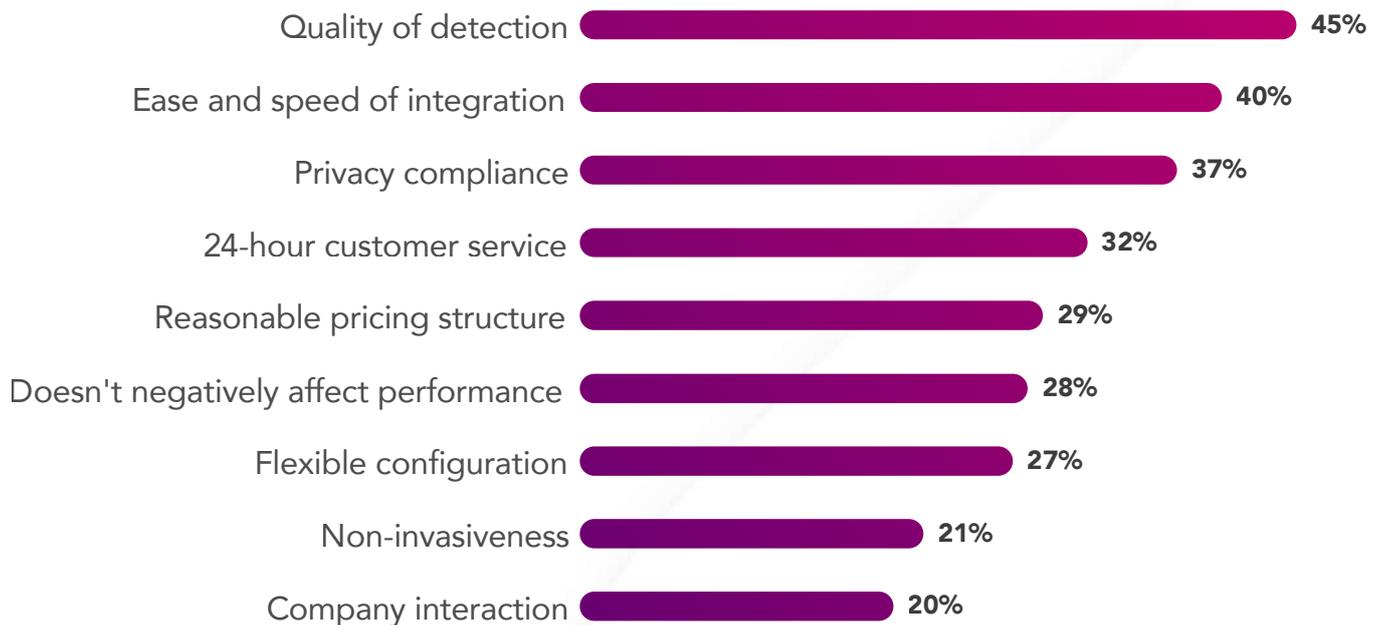


## WHAT DEVELOPERS NEED

Mobile game developers need tools to help them compete in a rapidly evolving market. As this report has shown, the market is characterized above all by the set of interlocking challenges created by the rise of multiplayer-focused games published across multiple platforms using free-to-play business models. In this environment, user retention is a critical challenge, making it essential that developers provide a secure environment in which players do not feel demotivated by cheaters or believe that other players are gaining unfair advantages. Similarly, it's vital that free-to-play monetization is not undermined by currency cheats or other forms of tampering.

Fortunately, mobile game developers do now have much greater access to solutions. In choosing a vendor there are many factors to consider. The leading aspect valued by developers is effectiveness — 45% rank quality of detection as one of the most valuable aspects of their security provider. Developers want to be sure any solutions they invest in get the job done. This is closely followed, however, by ease and speed of integration (40%). Particularly with development resources spread increasingly thinly by the demands of modern game development, this is a critical requirement for many developers.

**Figure 9: Which aspects of your third-party provider do you value the most?**



Being sure a vendor can balance these two central demands effectively is a key requirement, while also bearing in mind other factors that may play an important role for individual developers, such as performance impact, access to customer service and an attractive pricing structure. It's clear, however, given the rapidly growing adoption of anti-cheat and anti-tamper solutions that a growing majority of mobile game developers feel the solutions are available to ensure that these challenges can be met.



## 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](mailto:dom.tait@omdia.com)

#### Liam Deane

Principal Analyst, Games Tech  
[liam.deane@omdia.com](mailto:liam.deane@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 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.

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.

## 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 and offices 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 dedicated to being the security partner to empower a secure world where people can connect with confidence.