Publication date:
Feb 2022
Authors:
Dom Tait, George Jijiashvili

Cheating, hacking, piracy, and esports: critical steps needed to protect the industry

In partnership with:

OMDIA

verimatrix
DRIVING TRUST

Brought to you by Informa Tech

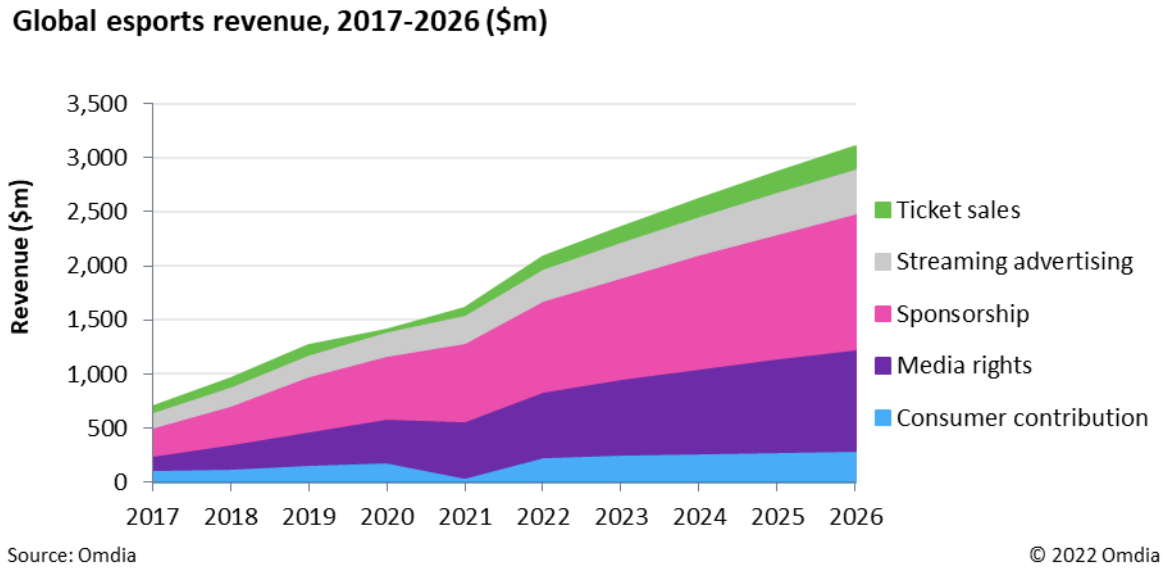
Cheating, hacking, piracy, and esports – background

- Verimatrix, a company specializing in protecting digital content, applications and devices, has several security services available to protect the integrity of esports competition by tackling hacking, cheating, and piracy.
- To better understand the current and future needs of the esports market, Verimatrix sponsored both a survey and video interviews of esports event organizers and team representatives; work performed by analyst house Omdia. In response, Omdia produced an online survey taken by 31 key industry players, and conducted three in-depth interviews, between December 2021 and January 2022. The work's aim was to highlight the scale of cheating, hacking, and piracy in terms of industry fears and challenges; to understand who industry players felt was responsible for tackling these scourges in such a complex value chain; and to shed light on the solutions available.
- This report goes into analytical depth about the most striking findings from the survey, using the data to construct the clearest possible picture of how esports needs to change to protect the industry from damaging threats to reputation and revenue.

Introduction: Esports – what's at stake

Total esports revenue reached $1.6bn in value worldwide in 2021. This is despite the ongoing effects of the pandemic more or less shuttering live events, with a major hit to consumer revenue lines as a result. Revenue is forecast to rise to $3.1bn in 2026 at a compound annual growth rate of 14.1%, illustrating the major growth potential still available in this fast-maturing industry.

Figure 1: Esports revenue will nearly double over the next five years



Though events had to be held predominantly online through most of 2021, brands have retained – in fact, increased – their interest. That, in turn, has encouraged major media rights deals. The most striking example of the sums involved comes from a rights deal of April 2021, when Chinese video streaming company Huya spent $310m on a five-year exclusivity agreement. This sum was spent for the streaming rights to just one country (China) and just one game (*League of Legends*), and even then it excluded *League of Legends*' flagship event (the World Championships). This is the best illustration of the value of intellectual property that needs to be protected in esports, and that value is only growing. Esports media rights revenue alone will near US$1bn by 2026, having risen 27% year-on-year to above $500m in 2021. Rights deals in turn enable esports streaming advertising revenue, which passed one-quarter of a billion dollars in 2021, an 18% year-on-year rise. Piracy places these revenue streams in huge danger.

Cheating, meanwhile, threatens the integrity of esports altogether. Sponsorship is the largest contributor to esports revenue, at $728m in 2021, but sponsors simply won't associate themselves with contests that are in any way compromised. Consumers, too, will vote with their feet if competition isn't free and fair.

Another ongoing trend in the industry is the rise of mobile esports – a phenomenon that's already highly popular in Asia, but rising in interest in the West. Mobile esports naturally has a far larger potential user base than console or PC-based esports, thus the democratized competition allows games to offer truly global playing fields and provide a larger pool of desirable targets for sponsors and streamers. Popular mobile esports titles such as *PUBG Mobile*, *Arena of Valor* (known as *Honor*

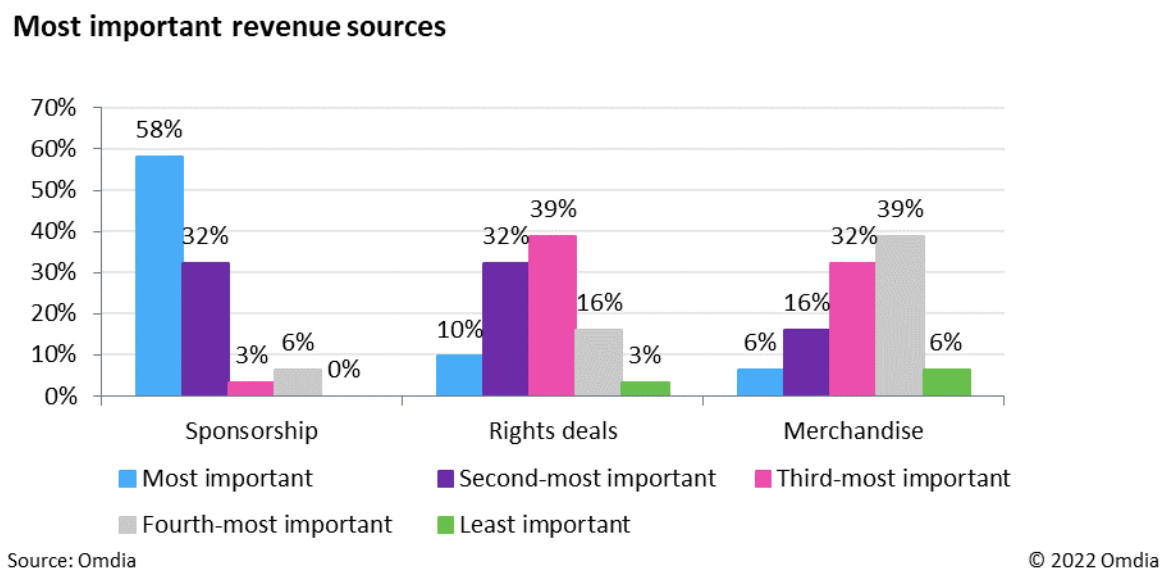
of Kings in its domestic market), *Garena Free Fire,* and *Peacekeeper Elite* are in turn propelling mobile games revenue. In the second quarter of 2021 alone, these four titles contributed almost $1.2bn to mobile games revenue, placing them among the top ten worldwide. It should be self-evident how this revenue stream would be at risk from app hacking, in turn torpedoing mobile esports just as it is poised to have a pronounced positive effect on esports in general. Taken in sum, this is the context of what's at stake in protecting esports from bad actors.

Cheating, hacking, and piracy in esports – the survey panel

The panel taking Verimatrix's survey was more or less evenly split between event organizers (55%) and representatives of esports teams (45%) to give as broad a picture as possible of the current landscape. Of the organizers, three-quarters used both streaming and broadcast technology for their events, with the remainder focusing solely on streaming. There was also a wide geographical range surveyed, with 42% from North America, 29% Europe, and nearly 20% from Asia Pacific, while participants worked in companies that ranged from solo outfits to more than 500 people. Interestingly, more than half of the panel had worked in traditional sports as well as sports, thus imbuing them with an extra perspective on how ruinous piracy can be to mainstream sports rights holders.

As for the survey respondents' revenue mix, it was sponsorship that was of critical importance, as is borne out by Omdia's total esports revenue forecast. In total, 58% of respondents named this as their most important revenue stream, with a further 32% placing it second. Rights deals were the clear runner-up in terms of importance – 71% saw them as either second or third-most important to their finances. This is the context in which the respondents operate, with protection of these key revenue lines vital to ensure the viability of their business.

Figure 2: Sponsorship and rights deals are key to esports revenue mix



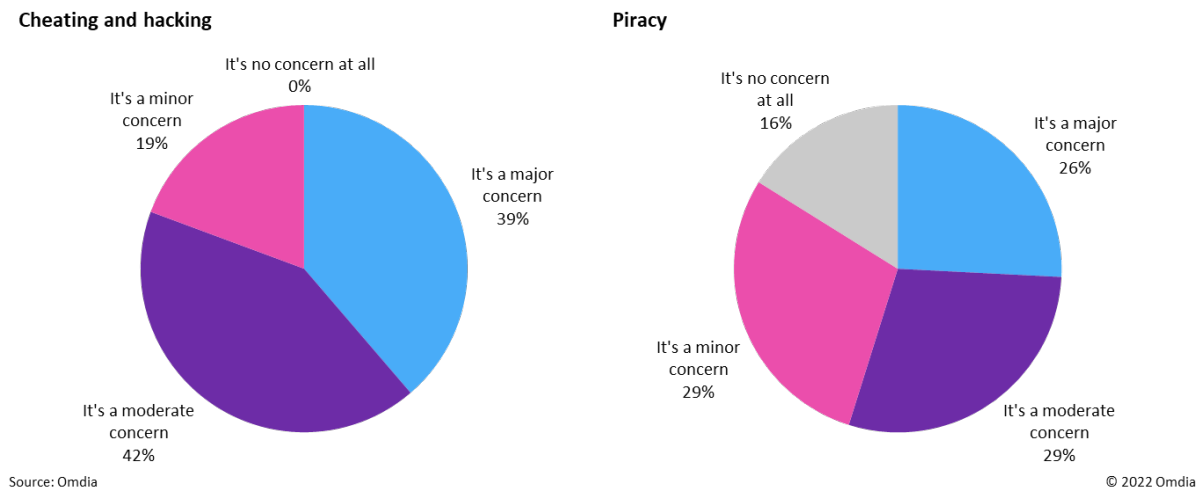
Source: Omdia

© 2022 Omdia

Cheating, hacking, and piracy – the scale of the problem

When asked about their perceptions of cheating or hacking in esports, the respondents were largely of one voice. 81% flagged such acts as either a major or moderate concern, with nobody answering that it was no concern at all. To an extent this is unsurprising – with many high-profile cheating scandals affecting esports, it would be a shock were any industry players to seem blasé about the threat. What was more surprising, however, were attitudes to piracy. Although piracy might be deemed by some as a niche problem, concern about its operation was widespread, with only 16% responding that they didn't see it as a problem. Meanwhile, 55% answered that it was either a moderate or major concern, indicating a growing realization that the streaming and broadcast of esports events is a facility that is increasingly under attack.

Figure 3: Cheating is the largest concern, but piracy is registering as a threat

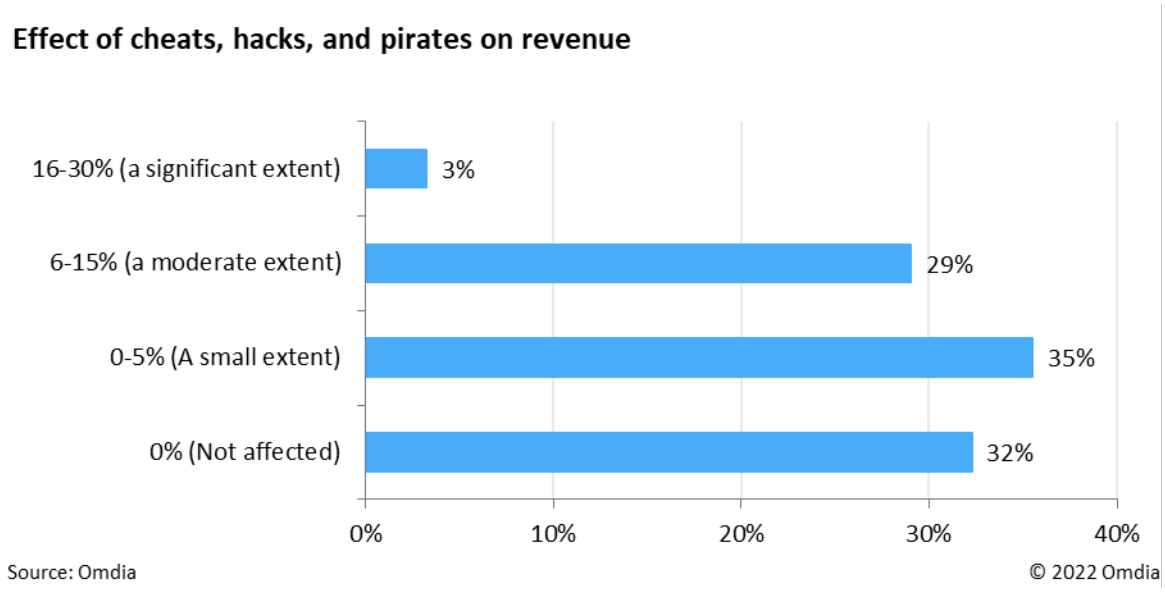


Source: Omdia

Reputational damage was the key concern listed *about* cheating, hacking, and piracy, with more than four-fifths selecting this option. This was followed by poor viewer experience (48%), a reduction in user engagement (45%) and revenue loss (39%). It is interesting to see these results since they effectively work as a flow chart; a poor reputation and bad viewer experience in turn lead to a reduction in user engagement, and all roads lead to a drop in revenue. This is the ultimate consequence of unprotected esports.

As for how reputations have been affected, 65% said that the esports industry had been impacted either a meaningful or a significant extent by cheats, hacks, or pirates. Although they were much more confident in their own company's reputation, with only 19% answering with these same two options, there is real concern as to the context in which esports operates. What's more, respondents are prepared to put a number to the impact of cheats, hacks, and pirates, and that number is significant. More than two-thirds have had revenue affected by bad actors, with 32% saying that 6-15% of revenue or more had been impacted. Furthermore, 16% of respondents had experienced sponsor reluctance, or even refusal, to invest due to their concerns over cheating, hacking, or piracy – particularly troubling given the primacy of sponsorship with regards to esports revenue. "The company heard there was a hack tool in the hands of some people and pulled the sponsorship in an… event," was one respondent's story.

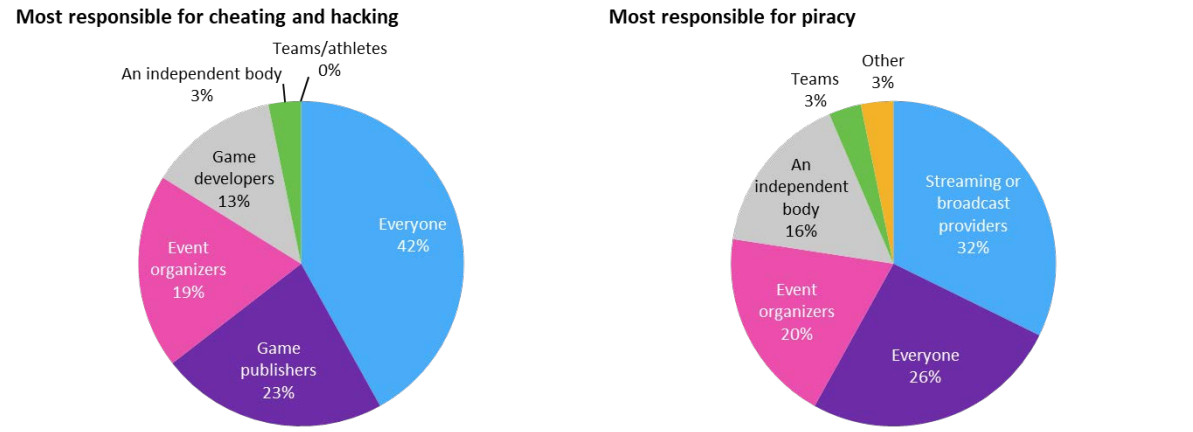
Figure 4: Nearly one-third of respondents have had more than 5% of revenue affected



The issue of who should be responsible for addressing such problems is more vexed, with no clear consensus on where the buck stops. For example, when it comes to cheating and hacking specifically, while 42% say everybody should have a role in prevention, a further 23% say games publishers must be the ultimate gatekeeper, with event organizers pinpointed by another 19%. This is a view backed up by one of the interviewees, who said: “Obviously the [esports] team should be held accountable, but I also think there’s some accountability on almost all parties… If you have a competitive mode, there shouldn’t be gaps in there for people to cheat.” Another interviewee approved of this joint approach: “I think everybody has a role, but I don't think one person has more of a role than the other.”

The picture becomes even murkier when it comes to piracy – streaming or broadcast providers are seen as marginally the most responsible for prevention here, with 32% selecting this option, but 26% opt for everyone, 19% choose event organizers and another 16% believe an independent body should be in control. Defeatism can even rear its head: one interviewee expressed a belief that “there's always going to be some dude that can capture his screen that paid for it and then rebroadcast it.” An overall picture is emerging – respondents are clear about the problems caused by cheating and piracy, but confused as to the remedy.

Figure 5: No clear picture on who should address cheats, hacks, and pirates

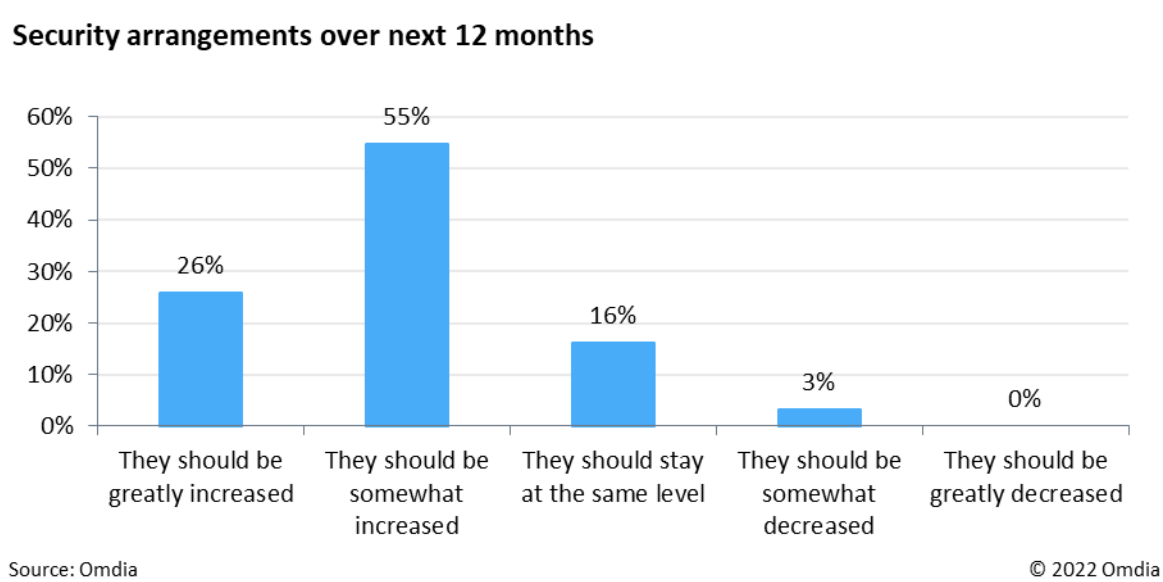


Source: Omdia

Cheating, hacking, and piracy – addressing the problem

The second half of this survey helped to tease out solutions to some of the problems facing esports today, as well as identifying any barriers that might prevent their uptake. One heartening finding was that respondents had, en masse, accepted that cheating, hacking, and piracy were sufficiently troubling issues to justify more effort with regards to security. 81% felt their security arrangements should be either somewhat or greatly increased over the next 12 months, a striking statistic.

Figure 6: Industry players are increasingly aware of the scale of the problem



Source: Omdia

When pressed on specific examples of new and emerging threats, responses included NFT and blockchain-based games, which “open up new avenues of fraud,” as well as “the use of ransomware against event organizers just prior to events.” As the landscape becomes ever more complex, so the range of possibilities for foul play is increasing. One interviewee reflected more generally on the

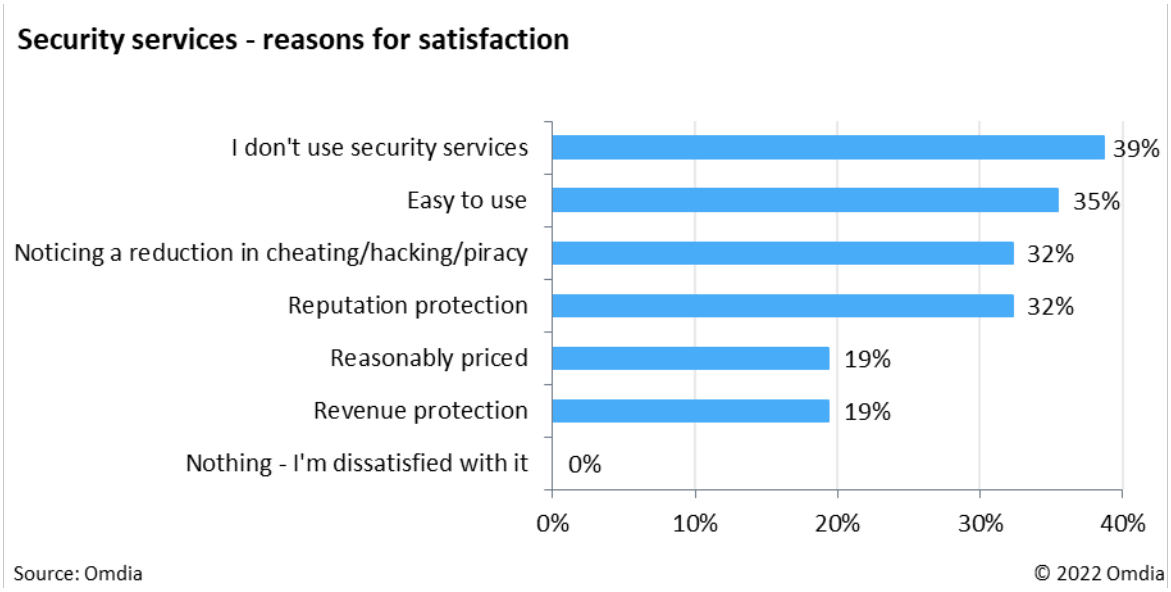
opening up of the games landscape to streamers and influencers, and the effect that has had: that while some people are “trying to build community… a lot of people [are] seeking to weaponize that.”

What’s more, for those respondents who had been involved in mainstream sports, it seems there is no one-size-fits-all solution – 88% said that their anti-cheating, anti-hacking, or anti-piracy arrangements were either somewhat or very different from those they worked on in sports. One such respondent, an interviewee, commented: “It's different from a normal sport because there is a lot more risk… a collective responsibility and accountability… which is different from turning up at a rugby match with a single camera.”

Solutions are at hand, but awareness of services designed to target these issues could certainly be improved, with 29% unaware of anti-cheating or anti-hacking services, and a particularly striking 50% not realizing that anti-piracy services are available. Another facet that needs to be worked upon are negative perceptions about such services, with 73% citing expense as a reason for not seeking them out. This indicates a disconnect between services’ value proposition and their target market’s appreciation of them, particularly given only 32% of respondents stated their revenue had been entirely unaffected by cheats, hacks, and pirates. Finally, name recognition in the market is something that all providers should strive to improve, with no single service truly cutting through when respondents were asked to name one unprompted.

The positive aspects of security services need to be broadcast far and wide, particularly given the rather troubling level of holdouts – almost 40% of respondents still do not use a security service. Hearteningly, however, that number of holdouts can be synthesized against the 81% of people wishing to up their security arrangements over the next 12 months, which indicates more investment is incoming for such services. And for those who already have them, a raft of benefits is noticed including ease of use, reputation protection and – the fundamental key – a reduction in criminal behavior. This is an open-and-shut case that nevertheless needs magnifying to help others protect their business.

Figure 7: Multiple benefits of security services identified

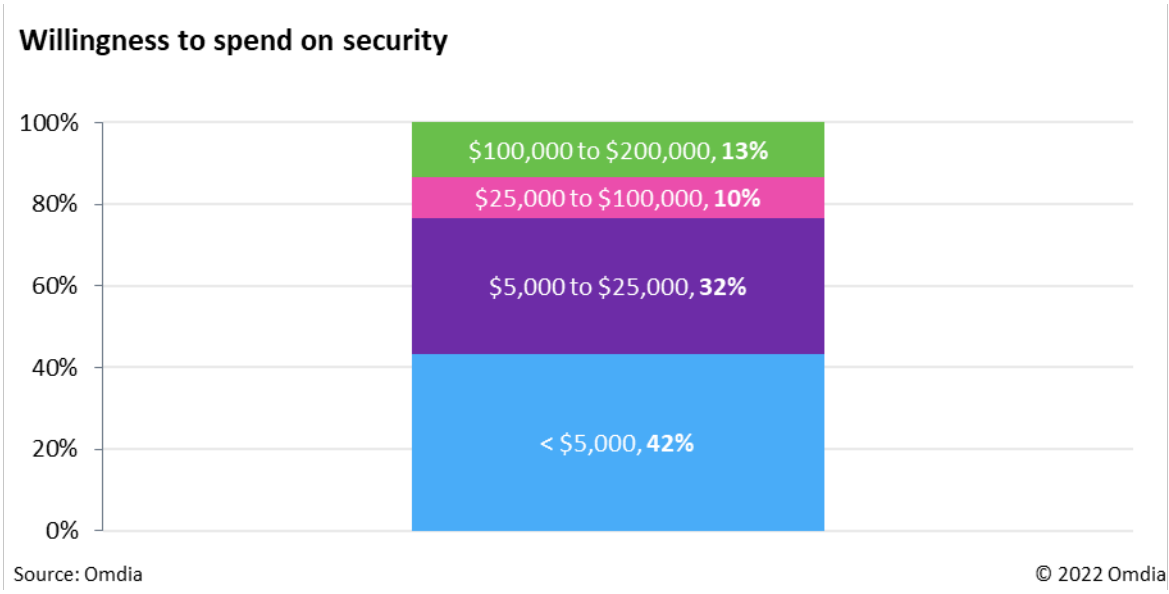


Finally, the questions turned to both a qualitative and quantitative look at value. Quality of detection leaps out as the most valued aspect of a third-party security service, underscoring the necessity for the basics to be nailed by any aspiring provider. However, multiple other facets are valued by respondents, with around one-fifth flagging each of reasonable pricing, ease of integration, 24-hour

access and no discernible effect on gameplay as important. This is a difficult balancing act, but providers able to satisfy all these requirements should be confident that they have a compelling proposition.

But what should these services cost? Respondents largely signaled that they wanted to spend below $25,000, a surprisingly low figure given the benefits they would receive from anti-cheat, anti-hack, and anti-piracy, not to mention the risk of inaction. Indeed, 42% wished to pay below just $5,000. On the other side of the ledger, 16% would pay more than $100,000 for protection, likely suggesting that expectation around pricing scales with size of company. More education seems to be required with regard to revenue impact in order to increase willingness to spend on prevention.

Figure 8: Most wish to pay under $25,000 for security



Conclusion

The final comments from the survey once again illustrate how in large part this is a matter of education, with associated responsibility for both esports industry player and security vendor. Said one: “I work for a large public broadcaster who has just started broadcasting esports. Awareness of cheating and hacking is pretty low.” Another declared: “I'd say that there should be more options on the market, or at least better marketed at event organizers so that they know what options they have to protect the integrity of the sports.”

What this survey has laid bare, then, is clear. Esports is under threat, and more so than ever before. Industry players are suffering in terms of reputation and revenue. They are well aware that something needs to be done, but less sure about who is able to remedy it, or how that would be achieved. Others retain negative perceptions about security providers that don’t seem to materialise for those who utilize them. It is equally clear that security vendors need to assist this process of education. Esports cannot operate without a level playing field. Companies that can provide this must take industry players through the advantages that come with protected competition – and the existential threat caused when that competition is compromised.

About Verimatrix

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

Visit verimatrix.com

Appendix

Methodology

The underlying methodology of Omdia's gaming forecast data is based on a collaborative, integrated process involving both quantitative and qualitative analysis. The forecasts are the result of a rigorous process of scoping, market mapping, data collection, statistical modeling, and validation.

The forecast model is built around the historical and current data alongside informed assumptions from market experts about the factors likely to have an impact on future trends. A number of factors have been considered, including economics, demographics, behavior, technology, competition, government legislation, and a host of individual segment drivers that have an impact on specific markets. As part of building our forecast models, all leading gaming and game subscription companies were carefully analyzed, after which our future growth assumptions were applied, based on our market knowledge.

When Omdia was building the models, a number of approaches, such as a time series technique (i.e., logistic curves) and causal technique (i.e., linear regression), were used to provide a more rigorous methodology.

Authors

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

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

Get in touch

www.omdia.com
askananalyst@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 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.