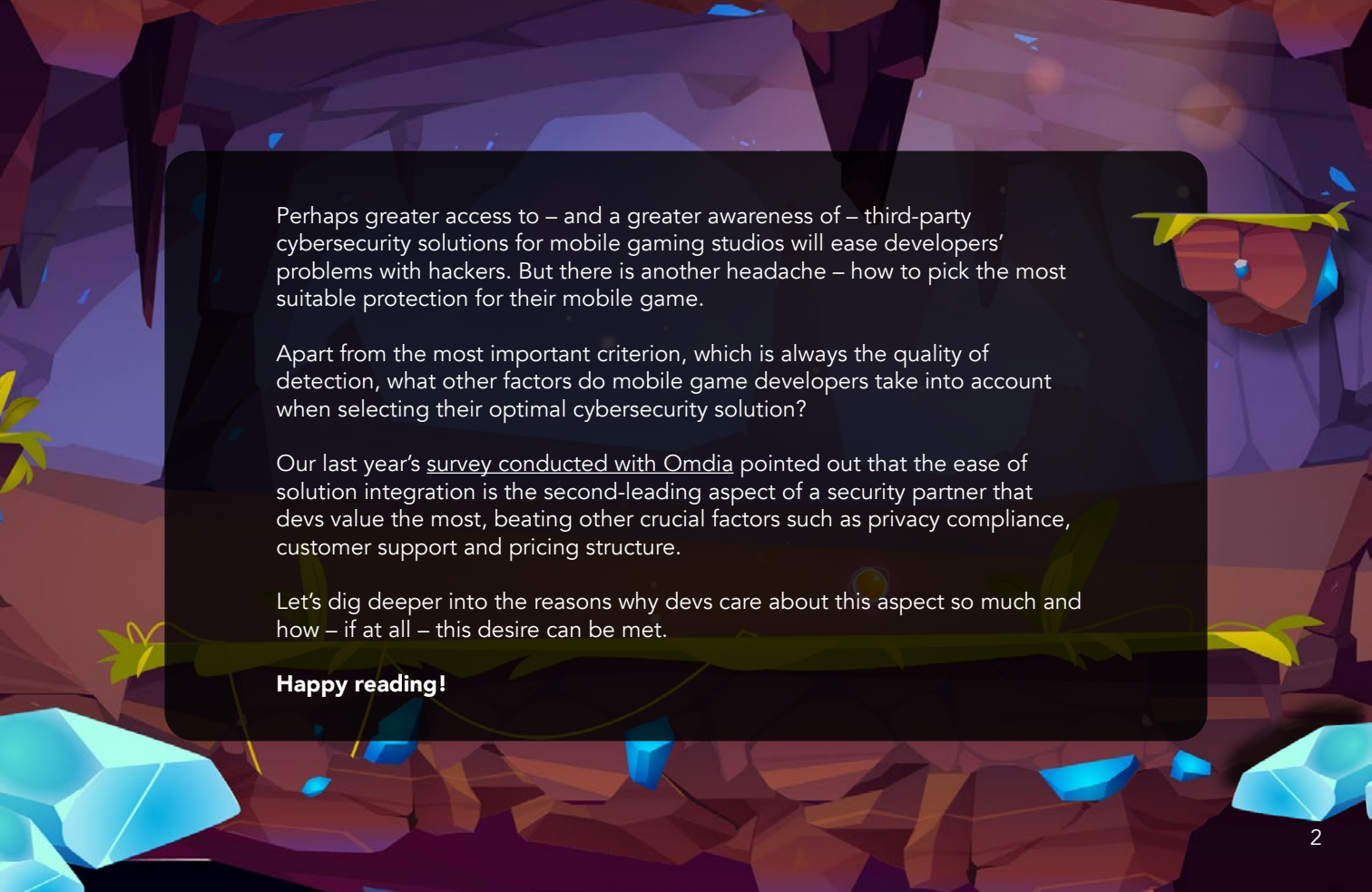


HOW DO YOU PROTECT YOUR MOBILE GAME WITHOUT A TON OF EFFORT?



Perhaps greater access to – and a greater awareness of – third-party cybersecurity solutions for mobile gaming studios will ease developers' problems with hackers. But there is another headache – how to pick the most suitable protection for their mobile game.

Apart from the most important criterion, which is always the quality of detection, what other factors do mobile game developers take into account when selecting their optimal cybersecurity solution?

Our last year's [survey conducted with Omdia](#) pointed out that the ease of solution integration is the second-leading aspect of a security partner that devs value the most, beating other crucial factors such as privacy compliance, customer support and pricing structure.

Let's dig deeper into the reasons why devs care about this aspect so much and how – if at all – this desire can be met.

Happy reading!

Why is the ease and speed of integration important for developers?

Developers today are well aware of the importance of cybersecurity service providers for the development of their studios and mobile games. Many of them, however, are not simply looking for a security solution; they are searching for an easy-to-use product as well. 40% of our aforementioned survey's participants consider it the second-most important aspect that they are looking for in a cybersecurity service provider, only behind the effectiveness of the solutions offered (45%).

Why does this aspect matter to developers?

The main purpose of utilizing third-party security solutions is to lessen the significant load on developers, particularly independent, or small to medium-sized game studios, which do not necessarily have strong security expertise in-house. For this reason, no developer wants to complicate their development workflows unnecessarily by applying a time-consuming solution or modifying their game in order to make it work. Particularly with development resources being stretched thin by the demands of modern game development, a hassle-free solution that can save them a lot of time and effort in terms of human resources is highly needed.

What are the common integration methods available on the market?

Currently there are two common integration methods available for gaming studios looking to protect their titles: using the Software Development Kit (SDK) or binary-only.

SDK approach

In general, with the SDK approach, the provider has a decent amount of flexibility to incorporate security into the app because it is based on the source code level.

The developer, however, needs to implement the SDK into their code making the integration of an SDK cumbersome in many cases. Installing and combining it with their gaming apps is also not simple. In fact, they need to add the SDK source code to their project and use specific functions from the SDK to secure their game. The more game functions they want to protect, the greater the integration effort will be.

As a result, from the developer's perspective, the SDK approach may demand a significant amount of integration work if they want their games to be fully protected. Additionally, this solution's effectiveness is greatly influenced by how it is implemented; if done incorrectly, it may impair security or even result in performance or compatibility problems.

Binary-only approach

Meanwhile, a binary-only approach is a better solution in terms of integration effort for developers as there is no additional source code integration required.

Instead, the final app needs to be given to the cybersecurity service provider. This, however, presents some difficulties for the provider in integrating security into the mobile game. They have no access to the initial or intermediate source code representations and have to work with machine code. It is still possible to have almost the same feature set compared to the SDK approach, but with the help of some techniques and a lot of background work. Plus, operating and developing at the machine code level is never an easy task.

Both of these strategies have their benefits and drawbacks, but what they have in common is that their integration process is not as hassle-free as they'd prefer – neither for developers, nor for cybersecurity service providers. Since the popular methods of applying mobile game protection are a deal breaker for some studios, is another, more simplified approach possible?

Is there an easier way of integrating a third-party protective solution to a mobile game?

The short answer: yes!

Fortunately, hassle-free implementation and deployment can take place without the need for developers to change the game's source code or high integration efforts from providers. Thanks to a new approach of using bitcode, which is a low-level intermediate representation of the source code, you have an advantage and more flexibility compared to plain app modifications.

This bitcode is also usually straight-forward to generate during the build phase. By utilizing undocumented functionalities deep inside the game engines, no execution of additional tools is necessary during the process of bitcode generation. Instead, developers only need to add a small script to their codebase.

This approach does not only simplify the integration process but also makes it more efficient in the long run for both parties because updating and maintaining a codebase is always easier than using files or tools on a file system.

How to ensure efficiency and ease of use at the same time?

A more efficient and less time-consuming approach would require several crucial steps. To place protection where it is most beneficial for the gaming experience, the mobile game needs to be profiled at the beginning in order to identify the optimal location for protection with the least impact. The protection setup is also optimized on a case-by-case basis, depending on the profiling data and static analysis. This preliminary analysis is implemented to ensure that there will be no gameplay impact and to make final performance optimizations. Thereafter, the integration process only takes a few minutes to complete.



Protect your mobile game effectively with minimal integration effort!

The mobile game sector is quickly turning into a breeding ground for hackers, taking away the income that you deserve. Fighting them on your own is good, but having a specialized weapon that is optimized only for your mobile game is even better.

There is no need to be concerned about challenging implementation procedures and complicated upkeep requirements. Contact us today, integrate the solution in a matter of minutes and then take pleasure in the outcomes.

DENUVO
by **irdeho**

Denuvo by Irdeho is the world leader in game 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, Irdeho is dedicated to being the security partner to empower a secure world where people can connect with confidence.