DENUVO by irdeto

How do you get your indie game protected without spending a fortune?

Contents

As an independent game developer, you spend months or even years working on new and exciting games. You invest your time, hard work and creativity – only to discover that as soon as your game is released, it becomes a target for pirates and cheaters. The intense work and efforts of your studio are ruined.

It sucks.

You're probably aware that there are tools for protecting your game, but these are intended for the big players, right? Cybersecurity requires a lot of time, effort and money, doesn't it?

Well, not really.

From this e-book you'll learn all the key facts about cybersecurity for smaller game developing studios. We're explaining the why, the what, the how and how much.

Happy reading!

Why should you care more about cybersecurity?

Our recent survey ran on a panel of developers representing a wide range of geographies and device types within the game development industry. The results show that **indie game developers** – those who work in groups of five people or fewer – are **the least concerned** of all size brackets within the industry **as far as cheating is concerned**.

So, what makes you so relaxed about this issue that is increasingly worrying the industry?

Perhaps you're viewing any form of interaction with your game as good, regardless of whether it comes in the form of cheating or not. You may simply assume that cheaters help you achieve greater exposure and wider reach and that in the future it can lead to more revenue from honest players.

This may seem a reasonable approach: the more people play a game (even if they do so unfairly), the more popular it becomes. This additional "free" exposure may bring fair players that would otherwise have never heard about the game.

However, such a permissive approach towards cheating can be harmful to both your company and the industry.

What are the risks of not protecting your games?

Put simply, cheaters not only ruin games for honest players, but also they pose challenges for game publishers. What are these risks?

- When a game is seen as a **cheater's game**, honest **players abandon it** and move to games with less or no cheating. And they not only take their engagement away, but also their money with them. According to Irdeto's Global Gaming Survey, 78% of respondents do just that! With no players remaining, there's no business – especially today, with the video game industry generating a sizable proportion of its income through in-game purchases. Almost half of those surveyed (**46%**) said that they were **less likely to buy in-game content** if they encounter cheating.
- When gamers are playing a **pirated** version of a game, they aren't experiencing the game as intended. Pirated games not only l**ack some of the key features** of the legitimate game – high score leaderboards, multiplayer real-time gaming – but also **don't receive the critical updates** that keep the games up to date and competitive.
- Sometimes **pirated games** are repurposed and published as different titles. In that way honest developers are forced to compete with hackers who **copied** their intellectual property **for profit**.
- There is also the spread of reputational damage. Users who download **cloned** or copycat **versions** of the game that **contain malware** get **frustrated** and **spread bad words** about the game, sometimes leaving a poor rating and negative reviews on the app stores.

What are the risks of not protecting your games?

Finally, bear in mind that **accepting any form of unfairness in the game as not being 100% bad weakens the industry's resolve to tackle cheating and piracy problems**. If game developers are to thrive, they should all – no matter the size – accept the fact that they are in this together, despite their competitiveness, and support each other's efforts to get rid of cheating, tampering and piracy.

Players abandon cheater's games

Pirated games lack key features and don't get updates

Cheater's games generate less money from in-game content

Games are cloned and repurposed for profit

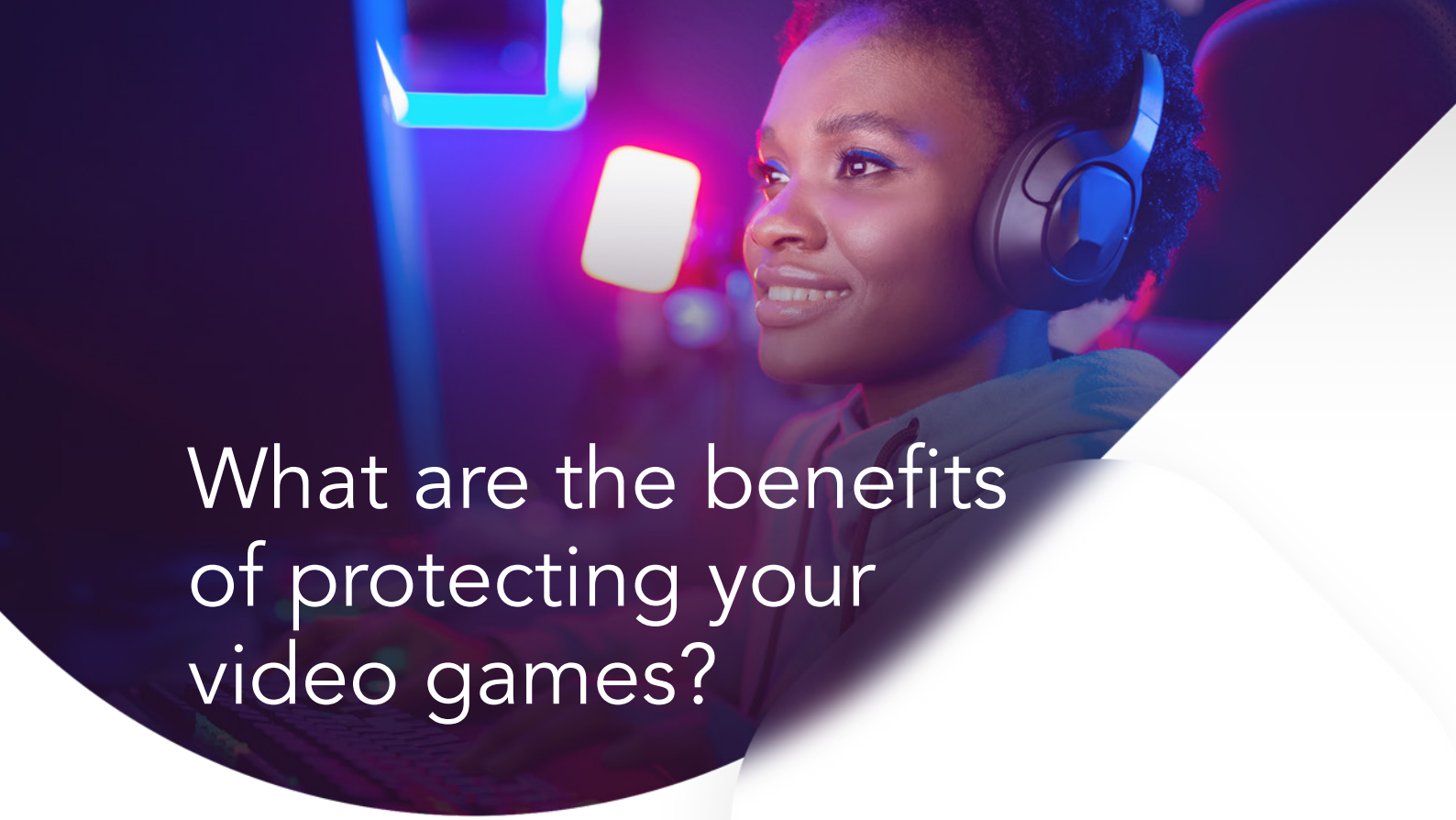
Pirated games contain frustrating malware

How much of your income is at stake due to piracy and cheating?

There may be another reason indie developers are the least concerned by unfair gaming practices: they simply do not know exactly how much they lose because of them. When asked to put a hard figure on the **revenue loss** attributable to cheats and pirates, **54% of independent game developers simply were not able to give an estimate**. Yes, over half of them do not know how much money they lose because of cheating and piracy!

Would you be able to answer this question?

It is, of course, difficult to put a hard monetary figure on the cheating problem. But considering the findings of Irdeto's Global Gaming Survey, we can give you an estimate. The annual global online gaming market alone is about US$37 billion. So, if 78% of gamers are put off a game because of cheating, as reported in the survey, nearly **US $29 billion of revenue is at stake**! Of course, they will not spend all this money on cookies instead. They will still spend it on a game – but it will not be yours if it is plagued with cheaters.



What are the benefits of protecting your video games?

A shattering **93% of companies** that invest in anti-cheat and anti-tamper technologies are **satisfied** with the protection and value brought by game protection technologies.

So, what are the biggest positives of using such services?

- About 60% of users check for ratings and reviews before downloading an app. If the rating is less than 4-stars, 80% of users will not trust the application. So, you want to achieve **higher star ratings with only positive reviews**. A fair gaming experience and an untampered game will ensure that you get just that.
- With no cracked version of your game available, your **sales figures** will typically be **higher**. Combined with **additional** downloadable content, as well as **in-game purchases**, it will generate you more money.
- With **no malware-infested, or self-crashing copies** circulating on the internet, your brand will be protected and trusted more by existing and prospective players.

Benefits of cyber protection for video games

- Better reviews
- More trust
- More sales
- More in-game purchases
- No malware-infested or self-crashing copies

How does cybersecurity protection work?

When speaking about cybersecurity, we are mainly focused on anti-tamper and anti-cheat technologies. So, let's have a look at those two.

Anti-tamper technology prevents hackers from debugging, reverse engineering and changing your gaming application, or to put it simply: it **prevents them from stealing your game**. It works on top of any digital distribution platform, allowing you to deploy the technology seamlessly into your games. By doing so, anti-tamper technology provides a crack-free window during the initial sale of a new game, when the most sales are generated.

So, as a result, anti-tamper software makes it harder for a pirate to modify or crack a game. The measures involved can include hardening the existing DRM (Digital Rights Management) solutions, code obfuscation and deep hardware binding. Importantly, a good anti-tamper product provider will allow you to achieve this with **no source code modification** of your game.

Anti-cheat software, on the other hand, **prevents** players of online games played in multiplayer mode from gaining an **unfair advantage** using third-party tools. Typically, anti-cheat services monitor a player's game and detects unauthorized use of third-party programs or modifications to the game. Depending on the solution, anti-cheat will first prevent the user from playing the game, and then it will ban their account for a certain time period.

You can think of anti-cheat as **your own game's policing unit**. It keeps an eye on gamers, identifies cheaters, and if necessary, sanctions cheaters so that the honest players can enjoy their game.

How much does cybersecurity protection cost?

The popular misconception is that protecting a game is too expensive for independent developers, and as such it is only available for blockbuster games from AAA studios.

That is not true.

In fact, it costs **less than you think** to protect a game. The cybersecurity industry has different pricing models available for game developers. Some cybersecurity providers offer **a pricing scheme dedicated specifically to small developer teams** with costs being very low for first time gaming releases. And others offer **payment models based on the actual sales volume of your game**.

Recently, our team worked closely with Traplight to secure their latest mobile game: Battle Legion. Traplight is a small but enthusiastic team of 30, working together with their shared passion for game development. Through our partnership, Traplight was able to integrate protection affordably and easily on their game with exceptional results.

Bear in mind that if you **compare the cost** of implementing anti-cheat and anti-tamper protection to your game **with the potential lost revenue** due to less license sales or in-game purchases, investing in such a solution is the only logical move.

Did you know?

57% of indie developers would consider using anti-cheat technologies to protect their games?

Learn more about devs perceptions around cheating, tampering & piracy.

DOWNLOAD FREE REPORT!

What factors should you consider when looking for cybersecurity providers?

You likely have considered assigning a member of your team to deal with security related topics. If not, you should check for solutions that **do not need additional expertise or require little integration effort**.

Second, check if the **pricing models** available are **flexible enough** and cater to your specific business situation. Some of the best cybersecurity providers offer payments based on actual sales volume of your gaming app. If your game doesn't sell, you don't end up losing your money invested in cybersecurity.

Third, make sure you pick an **experienced provider** that has been on the market for a while and protects a wide range of games.

What does the entire process of implementing cyber protection look like?

In the case of the top anti-cheat and anti-tamper technology providers, the entire implementation process of their solutions is simple: you only need to provide your build of the game and choose the type of protection you need. As protection works best if applied before release, you must do it at least a month before the planned game premiere.

In the next step, your provider does the set-up on their side and once complete, you can automatically protect each build of your game directly in your pipeline without any further work required from either party.

It is also possible to apply protection to a game that has already been published, also when there are already cases of cheaters bending the rules.

DENUVO by irdeto

How do you get started with protecting your game against pirates and cheats?

It's easy.

Reach out to us today and tell us more about your upcoming release.

Irdeto is the world leader in digital platform security, protecting platforms and applications for video entertainment, video games, connected transport, connected health and IoT connected industries. The **Denuvo** team at Irdeto is the world leader in gaming security, protecting games on desktop, mobile, console and VR devices. We provide core technology and services for game publishers/platforms, independent software vendors, e-publishers and video publishers across the globe. Denuvo technology enables binary protection for games and enterprise applications across multiple platforms, including desktops (Windows), consoles, VR devices and mobile gaming. Denuvo's gaming security technology prevents revenue loss for game publishers and disruptive, undesirable cheating in the gaming environment.