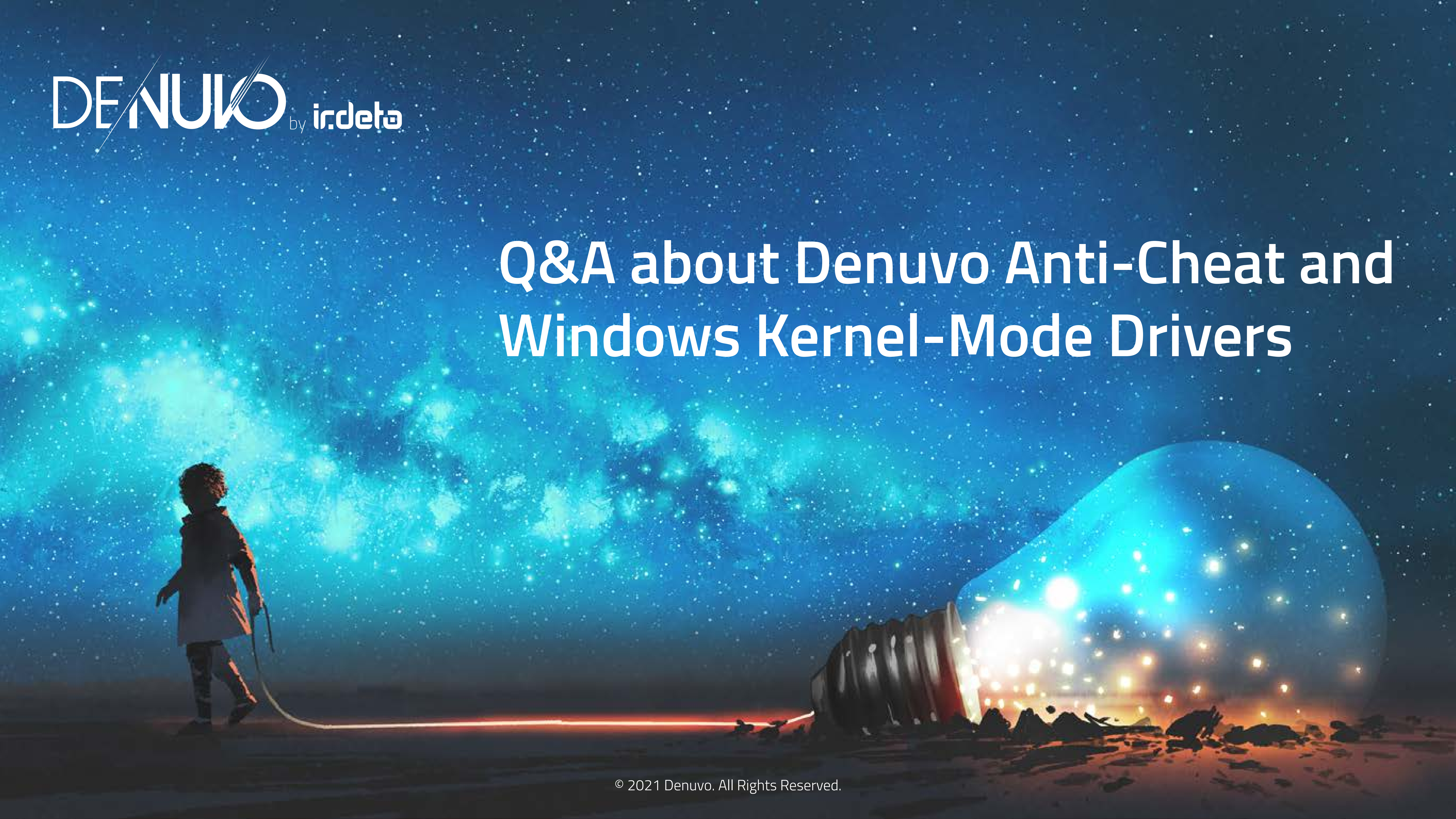
DENUVO by irdeto

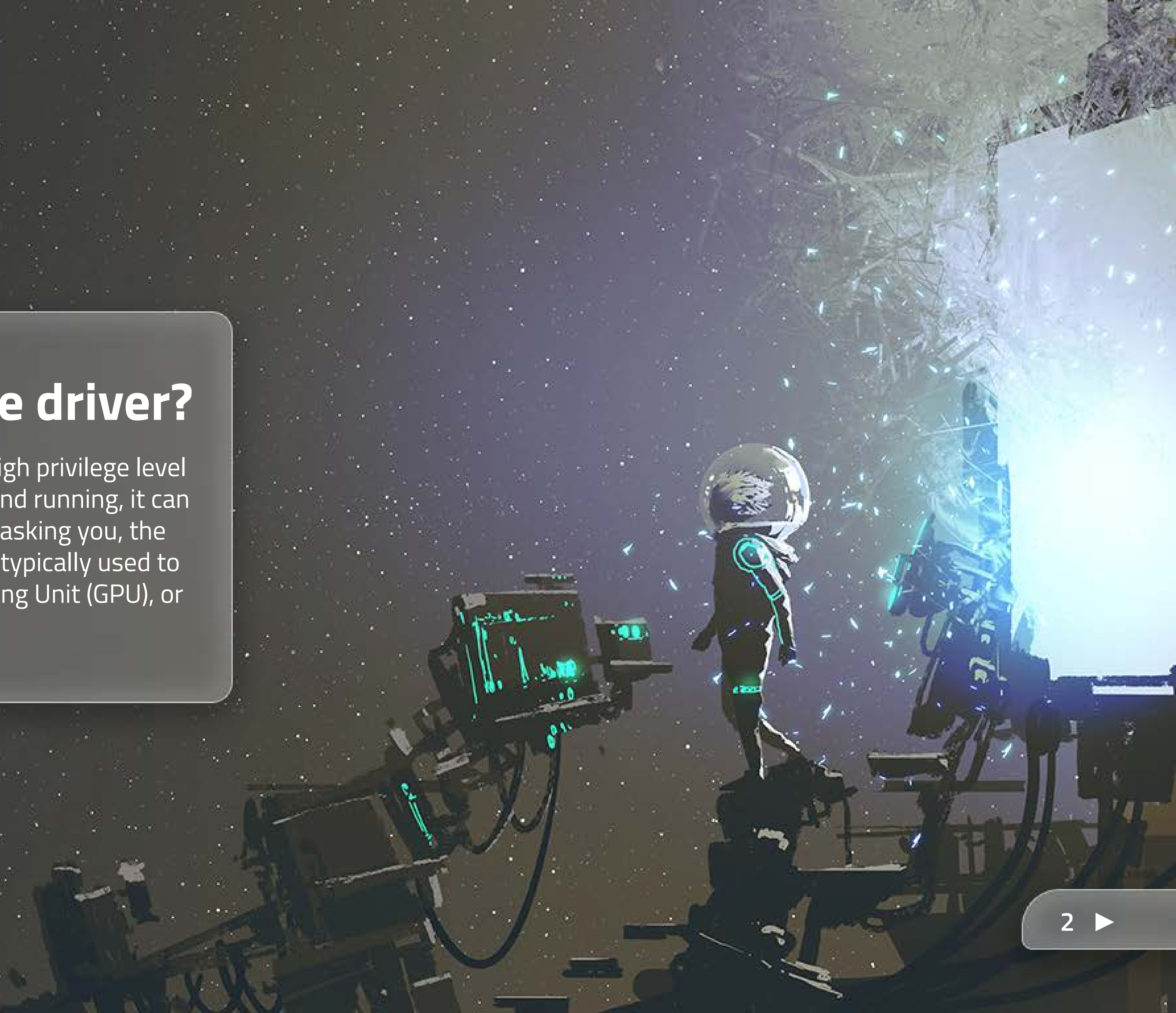
Q&A about Denuvo Anti-Cheat and Windows Kernel-Mode Drivers



© 2021 Denuvo. All Rights Reserved.

What is a kernel-mode driver?

A kernel-mode driver is code that runs at a high privilege level on your system. Once the driver is installed and running, it can access all resources on your system without asking you, the user, for permission. A kernel-mode driver is typically used to control hardware, like your Graphics Processing Unit (GPU), or to provide system security, like an anti-virus.



Why do anti-cheat solutions use kernel-mode drivers?

User-mode applications, like games and web browsers, have limited access to the kernel and other user-mode processes. This access is gained via well-defined APIs provided by Microsoft, and these APIs are designed to protect the kernel from user-mode introspection. This means that kernel-mode cheats, by Microsoft’s design, are protected from user-mode anti-cheat introspection.

For a user-mode anti-cheat to find a kernel-mode cheat, one of the following is required:

- The cheat must make a mistake and leak information that is detectable from userspace
- The anti-cheat must exploit a Windows vulnerability to peek into the kernel from userspace

Developing an esports anti-cheat that depends on cheaters making mistakes or requires shipping exploits in commercial software is not in line with Denuvo’s values, and thus we have opted to deliver our security in the kernel, as recommended by Microsoft.

How does Windows defend users from malicious kernel-mode drivers?

Microsoft's Virtualization-Based Security (VBS) and their Hyper-V hypervisor run at a higher privilege level than kernel-mode drivers and protect sensitive code and data on your system. Before a Windows driver can be installed, Windows asks for your permission via the "Do you want to allow this app to make changes to your device?" dialog. Clicking yes to this dialog, or running an application "as administrator", grants software with the same privilege as kernel-mode drivers. On Windows, administrator-to-kernel is not a security boundary. For more information, check the "kernel boundary" entry in Window's Security Servicing Criteria.

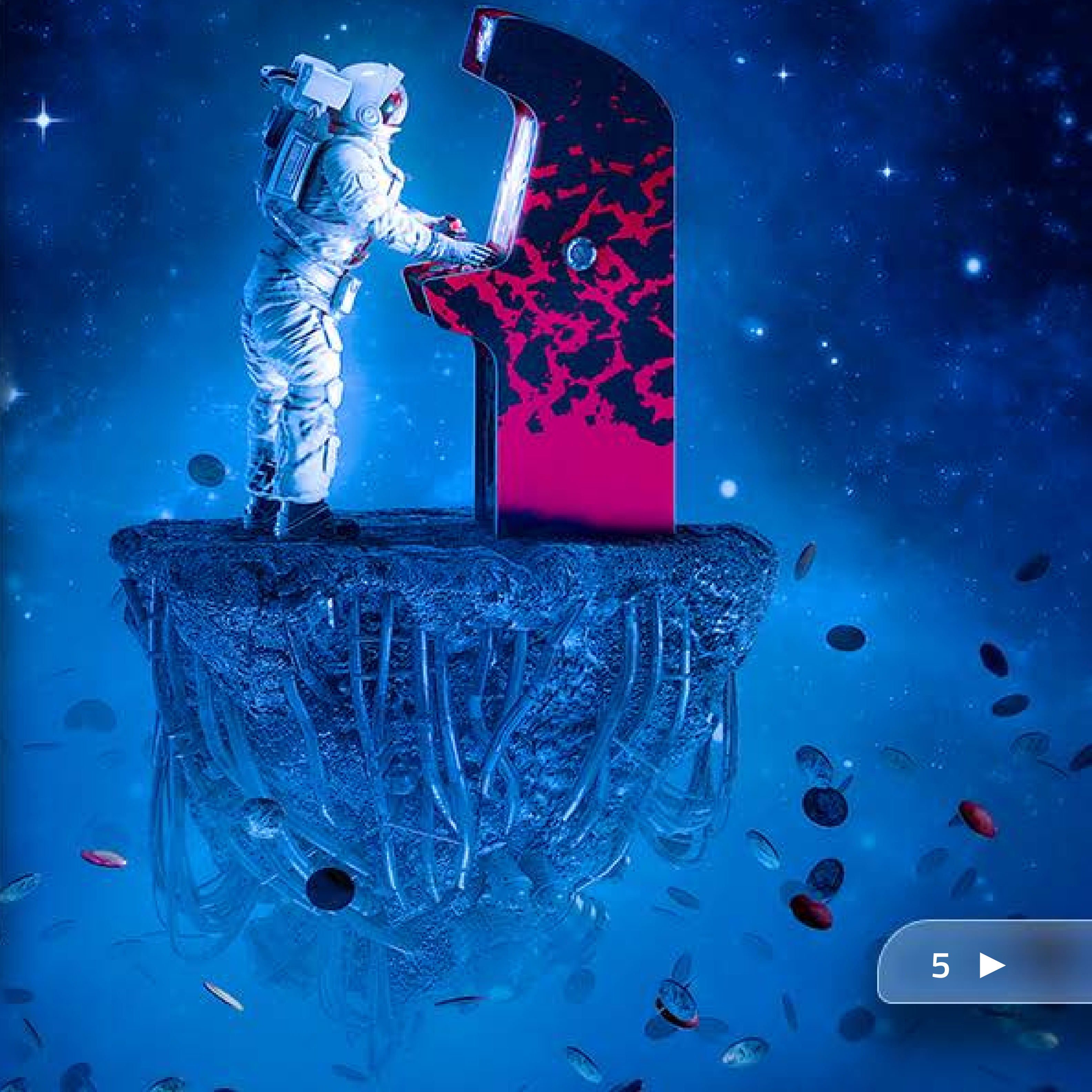
Steam often bypasses the "Do you want to allow this app to make changes to your device?" dialog via Steam's privileged service, allowing drivers and services to be installed on your machine without your permission. This is done for your convenience as gamers often don't want to click dialogs and just want to play. Other anti-cheat providers use the Steam service to place themselves onto your machine silently. Denuvo Anti-Cheat **does not** do this and always asks permission to install.

You should be able to do anti-cheat in the userspace

Denuvo has a good understanding of userspace limits thanks to the experience we've gained from developing Denuvo Anti-Tamper, a security solution that keeps games piracy-free for an average of 160+ days. The most popular multiplayer games, with hundreds of millions of players, have adopted kernel-mode anti-cheat for effective protection.

Popular games using kernel-mode anti-cheat:

- Fortnite (1)
- Fall Guys: Ultimate Knockout (1)
- Halo: The Master Chief Collection (1)
- Player Unknown's Battlegrounds (2)
- Rainbow Six Siege (2)
- Apex Legends (1)
- VALORANT (3)



Do I need to surrender my privacy just to play video games?

No. Just because a kernel-mode driver can do something, it doesn't mean it does. Not every anti-cheat is built the same.

Consider the following characteristics of anti-cheat solutions when it comes to the potential to violate your privacy.

	Denuvo Anti-Cheat	Anti-cheat 1	Anti-cheat 2	Anti-cheat 3
Kernel driver starts when Windows starts (1)	No	No	No	Yes
Kernel driver required to play single-player or non-competitive game modes (2)	No	Yes	Yes	Yes
Kernel driver required to play competitively online	Yes	Yes	Yes	Yes
Kernel driver scans files when opened (3)	No	Yes	Yes	Yes

(1) Anti-cheat 3 uses Windows' Early Launch AntiMalware (ELAM) security feature which allows the kernel-mode driver to start before all others. This behavior is often mistakenly referred to as a rootkit, which it is not because it does not attempt to hide from the user and is effortless to remove.

(2) Denuvo's Anti-Cheat is the only solution that doesn't require players to install or start a kernel-mode driver to access non-competitive game modes. All other anti-cheats require the kernel-mode driver to start together with the game.

(3) Anti-cheat 1, 2 and 3 access all files on your disk that are opened while the anti-cheat is running by using a file system minifilter, a formal operating system hook. This minifilter passes all opened files to the anti-cheat software, not just those that interact with the game.

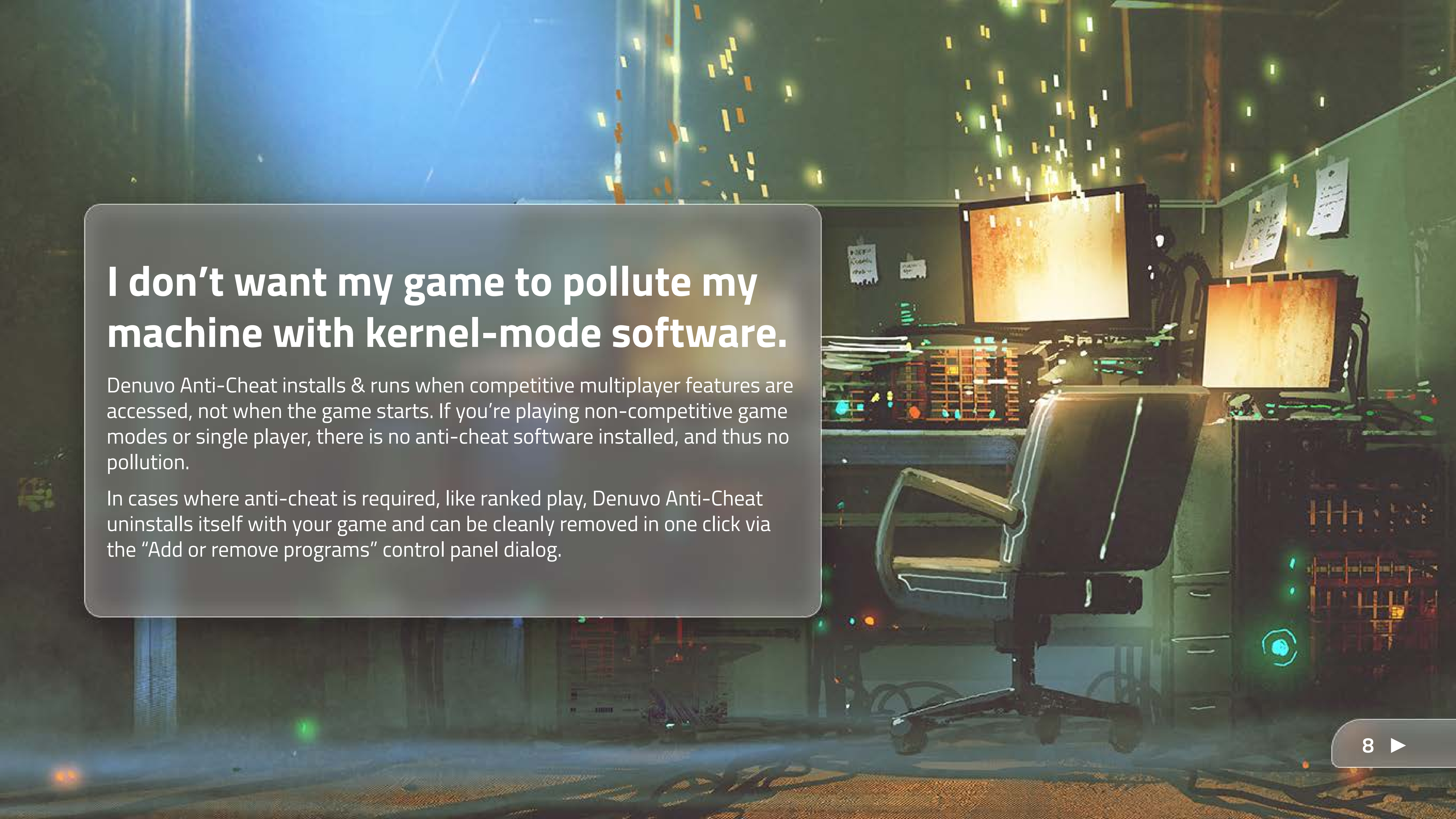
Denuvo Anti-Cheat is built with privacy as a key design pillar. No personally identifiable information (PII) leaves your machine, and Denuvo is GDPR and CPRA compliant.

Can hackers exploit a kernel-mode driver to attack my computer?

Before Denuvo came along, anti-cheat solutions have been streaming kernel-mode shellcode to gamers' machines from the Internet. Shellcode is arbitrary instructions generated remotely and executed at a privileged level. If an attacker could gain control of the anti-cheat system, they could stream kernel-mode malware from a remote location. These practices have been around for about a decade, so why haven't hackers used this to take control of gamers' machines?

Attacking a hardened anti-cheat driver for the purpose of sending malware does not make much sense because it is literally the most secure piece of code running on a gamer's machine. There are thousands of softer targets on the system without defenses and are available outside of gameplay. Targets like Steam's Client Service, which has privileged access to your machine to install redistributables, or NVIDIA graphics services, which maintain an online connection for telemetry. The services and drivers in those examples start with the machine, so the attacker doesn't need to wait for you to play a game.

Regardless, Denuvo Anti-Cheat does not stream shellcode from the web, and there is no remote control surface for attacks to abuse.



I don’t want my game to pollute my machine with kernel-mode software.

Denuvo Anti-Cheat installs & runs when competitive multiplayer features are accessed, not when the game starts. If you’re playing non-competitive game modes or single player, there is no anti-cheat software installed, and thus no pollution.

In cases where anti-cheat is required, like ranked play, Denuvo Anti-Cheat uninstalls itself with your game and can be cleanly removed in one click via the “Add or remove programs” control panel dialog.

© 2021 Denuvo. All Rights Reserved.