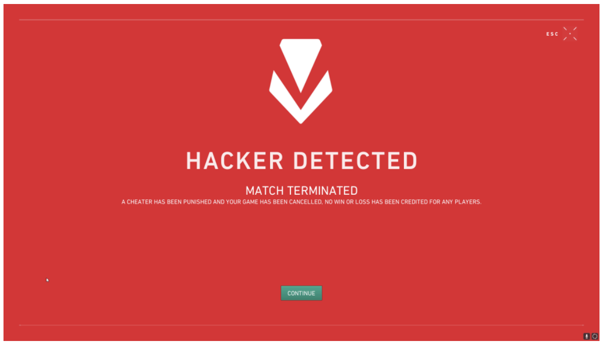
Vanguard Anticheat is Incredibly Invasive— Just Like All Anticheat Software

Uku Sirkelmaa

In 2023, Riot experienced a significant data breach that resulted in public exposure of the source code for both League of Legends and its anti-tamper software, Packman. This, alongside outdated anti-cheat software and a rise in botting and scripting, prompted them to use Vanguard as a more sophisticated security system. The macOS version of League of Legends would use an alternative method due to the operating system architecture being vastly different from what Vanguard supports.

This paper will explore the ethical issues of not only Vanguard anticheat, but also all other anticheat software developed after the 2010s.



HACKER DETECTED

MATCH TERMINATED

A CHEATER HAS BEEN PUNISHED AND YOUR GAME HAS BEEN CANCELLED, NO WIN OR LOSS HAS BEEN CREDITED FOR ANY PLAYERS.

What is Vanguard Anticheat?

Riot Vanguard is a two-part anti-cheat solution rolled out by Riot Games to defend its games from cheating software. It consists of a client-side application and a kernel-mode driver, which is where much of the controversy lies.

The client-side application works similarly to traditional anti-cheat programs. It monitors for suspicious behavior while a game is running, detecting unauthorized modifications or programs that could provide an unfair advantage. This is a fairly standard approach and exists in several competitive titles like Counter-Strike: Global Offensive or Fortnite.

The kernel-mode driver, however, operates at a much deeper level. Generally, any program that runs inside the kernel and its environment will be referred to as a driver. So, in essence, Vanguard has the same privileges on your computer as a display or memory driver would.

Vanguard’s Service History

When Vanguard launched together with Valorant in 2020, Riot Games made the decision to have Vanguard utilize its on-boot positioning to prevent known signed-but-vulnerable drivers from loading in their entirety. However, Riot were not aware of the extraordinarily specific hardware configurations utilizing bespoke's broken kernel drivers to communicate instructions to relatively obscure devices. In one infamous case, this included a driver that was responsible for keyboard lighting. Cheaters unfortunately were able to use this otherwise properly signed driver to load their own malware, allowing them to "look" like a clean Windows installation (with cert verification still enabled), yet still be running kernel-level cheats. Because this driver was only for keyboard lighting and macros, Riot kept the driver deny-listed until the developers released a new one.

Seeing the old anti-tamper software, Packman, on its last legs, Riot brought their new software to League of Legends in patch V14.9.

In the week following Vanguard's launch, less than 0.03% of active players had reported issues adjusting to the new client, predominantly related to common errors resolvable through player support or troubleshooting.

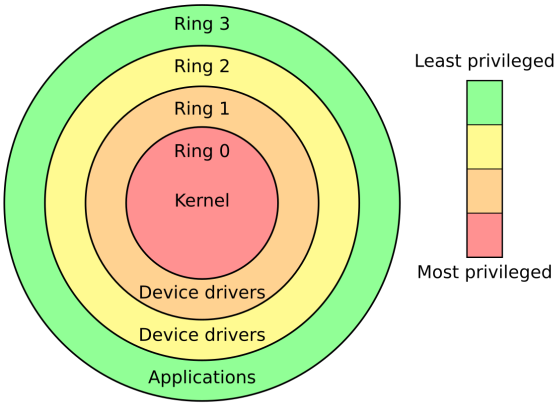
```
Protected by packman, a Riot Games product. Developed with <3 by the Anti-Cheat team.

We're always hiring talented individuals. If you've found this message, we implore you to take a look
```

Anticheat Software Design and Ring0 Privileges

We're going to be talking a lot about the kernel here, so let's define that real quick.

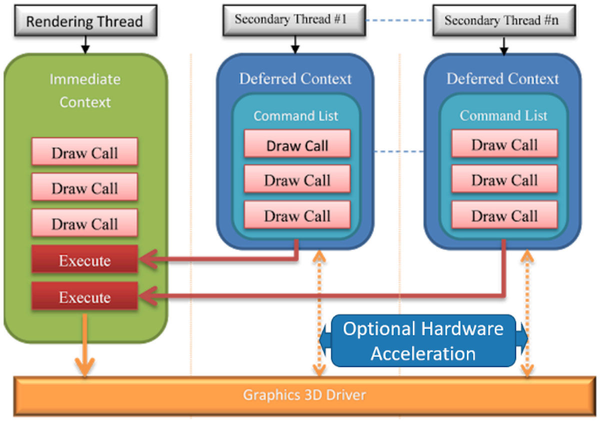
In a computer, the kernel is the core software of the operating system. It handles all the fundamental operations, like managing memory, processing tasks, and communicating between your hardware (like your keyboard, mouse, and monitor) and software (like your games and applications).

The kernel operates at the **deepest** level of your system and has complete control over anything happening in your computer. It decides which programs get resources, serves as a bridge



between software and hardware using drivers, and controls essential security measures.

Both applications and drivers operate under a hierarchy of Ring protection levels. Their purpose is to define an access level hierarchy in your system. Your everyday apps and games run at Ring3 (least privileged, safest for your system). Specifically, Vanguard runs at Ring0. If you've ever heard some stable genius hit you with a "lol my cheat is ring 0 undetected," this is what they were referring to right before they were banned.

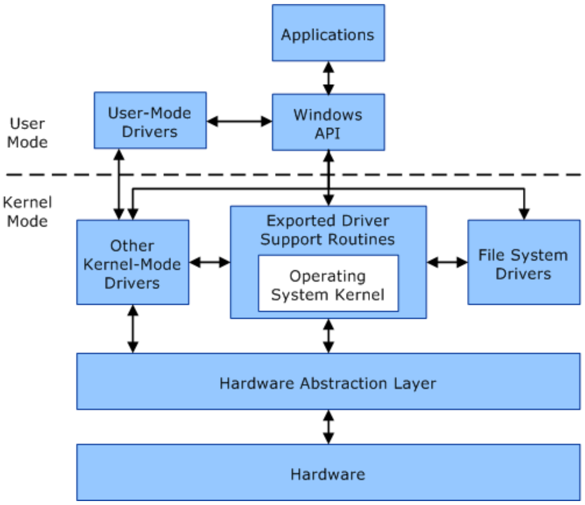


Software that runs on a given ring has a hard time interacting with things on lower rings, unless it's through system calls or API.

For example, when your computer runs CS:GO, it keeps the CS application on ring3, or what's called "user mode". To draw map geometry and visual effects, it needs to access your GPU's drivers, which operate on ring0 or “kernel mode”. To do this, it uses an intermediary API that turns game geometry into system calls to allocate memory and change what your monitor’s currently displaying. In this case, it uses DirectX 9.

User Mode and Kernel Mode

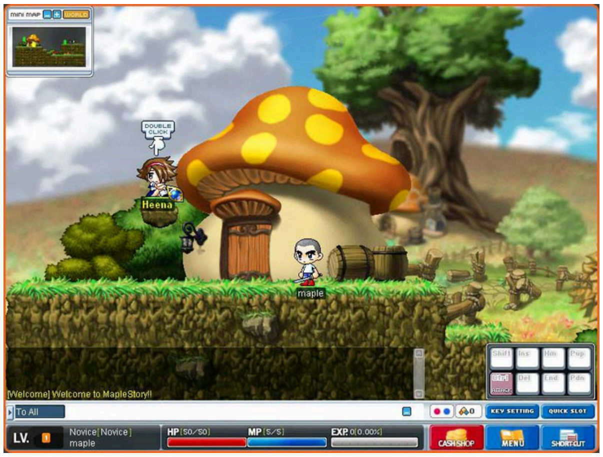
Your web browser, your copy of WinRAR, and your favorite games all run in user-mode. Within it, an application cannot directly “see outside” of itself, and instead, code must generally rely on OS’ native APIs (or third party APIs, such as DirectX or Vulkan, as mentioned before) to read or write memory not within the process and memory that it was allocated to.



This measure is safe and highly efficient, but the user still ultimately has the choice to give kernel mode privileges to an application, which can give it free reign to influence user mode applications.

This is the basic philosophy of how all cheating software worked before the advent of ring0 anticheat software. A program, let’s say, Cheat Engine, would be given special privileges to read and write memory anywhere on your system, which would allow you to change stats and resources inside a game. The game itself would be none the wiser, and without a way to directly interact with the kernel mode application, it’d depend on a central server for data redundancy. Even then, it would need to constantly check and make calls to the server, sapping away system resources and making the application incapable of running offline.

This is largely why single player games have no anti-tampering measures, they’re far too costly to maintain. Until the mid-2000s, cheating would remain widely accessible, and even valid in some online games.

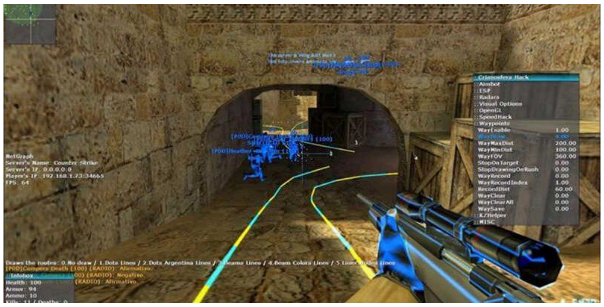


However, the mid-2000s also brought the explosion of MMORPG content, with huge players like MapleStory, Runescape and World of Warcraft. Each game heavily relied on stats attached to the character, such as attributes, professions, what the character was currently carrying in their inventory, their level, etc.

The first measure of redundancy checks was easy to introduce, and eventually developed into the modern practice of *memory scanning*, which would compare the game’s memory against known cheats and injectors, along with file integrity checks and client-server validation.

However, with the advent of botting as a business in the early 2000s, it became quickly obvious that scanning memory in user mode would not be enough. As such, even in 2000, we started seeing ring0 anticheat software being added into games. Examples include GameGuard (*MapleStory, Combat Arms, Ragnarok Online, Flyff, Lineage*), HackShield (*Elsword, Mabinogi*), nProtect (*GunZ: The Duel, Silkroad Online, Cabal Online, Atlantica Online*) and PunkBuster (*Return to Castle Wolfenstein, Battlefield 1942, Call of Duty, Far Cry*).

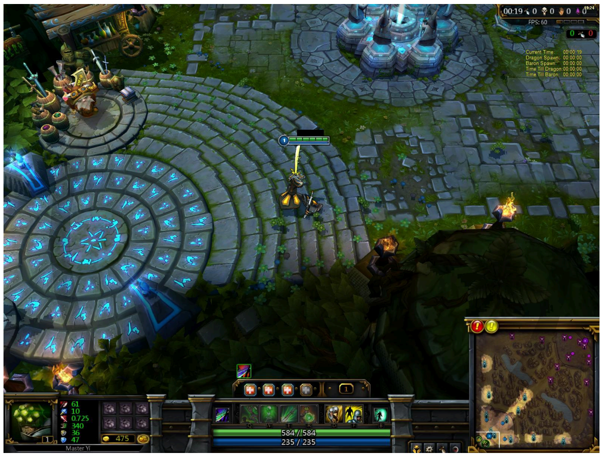
Some companies still opted for ring3 software, such as Blizzard's Warden (*Diablo, World of Warcraft*) and Valve's ValveAntiCheat or VAC (*Team Fortress Classic, Day of Defeat, Counter Strike 1.6*).

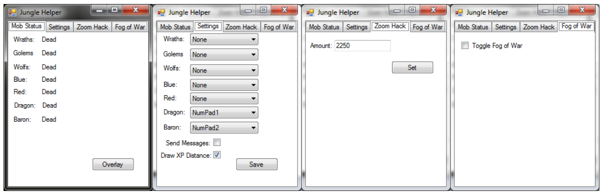


In League of Legends' launch in 2009, it was released along the Riot-developed anticheat software, Packman, which ran on ring3.

As gaming rolled in the 2010s, cheat developers started to leverage vulnerabilities with Windows' signing verification to move their applications (or portions of them) from user mode to the kernel level. The problem here arises from the fact that code executing in kernel-mode can hook the very system calls League would rely on to retrieve data, modifying the results to appear legitimate in a way League cannot detect, by design of how Windows works. This is how most scripts and cheats in League of Legends would work, before Vanguard. Packman quickly became a gentle anti-cheat suggestion rather than an anti-cheating measure.

As League of Legends became a more popular game in the 2010s and it started competing with DotA, botters found both VAC and Packman incredibly easy to crack. They utilized corrupted Windows copies that leveraged vulnerable system calls to read and write game memory—a vector that is completely undetectable from within ring3.





Jungle Helper

Mob Status | Settings | Zoom Hack | Fog of War

Wraths: Dead
Golems Dead
Wolfs: Dead
Blue: Dead
Red: Dead
Dragon: Dead
Baron: Dead

Overlay

Jungle Helper

Mob Status | Settings | Zoom Hack | Fog of War

Wraths: None
Golems None
Wolfs: None
Blue: None
Red: None
Dragon: NumPad1
Baron: NumPad2
Send Messages: □
Draw XP Distance: ☑

Save

Jungle Helper

Mob Status | Settings | Zoom Hack | Fog of War

Amount: 2250

Set

Jungle Helper

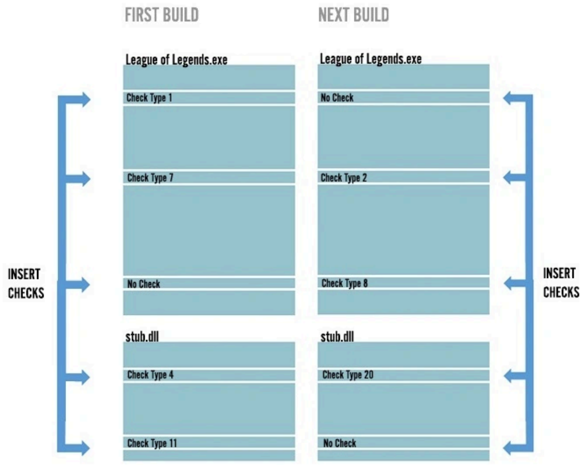
Mob Status | Settings | Zoom Hack | Fog of War

□ Toggle Fog of War

Now, while most players might find the idea of a corrupted Windows installation objectionable, a disturbing number of cheaters have shown themselves to be downright enthusiastic about the opportunity to jump onto some guy's botnet in exchange for the ability to orbwalk or track jungle camps perfectly.

And so, the meta for tampering with the League client became obvious— simply run your cheats at ring0, where Packman has no possible way of interacting with them (and therefore detecting said tampering). This created an incredibly inefficient ecosystem, where nobody would even attempt to develop ring3 cheats, but Packman was completely incapable of detecting ring0 cheats by nature. Barely anybody was being directly banned by the software.

Scripts for dodging and hitting skillshots were easy to detect by other players, sure. Most people using these would have them on for a couple of games, then be immediately banned after the system detected that most of their opponents wound up reporting them.



However, with how Packman was built, it couldn’t possibly detect a cheater without somebody reporting them first. Even though cheating and scripting wasn’t a huge problem, the incredibly large business around boosting and selling bot accounts for ranked play became deeply entrenched in the community.

By 2013, Riot Games already knew that they needed kernel-level software to have any chance at deterring botting as a practice. After years of development, they gave Vanguard a test run in Valorant in 2020, before finally rolling it out gradually in League of Legends in 2024.

Vanguard’s Design Philosophy

Where Vanguard starts to distinguish itself from other anti-cheats is in its enforcement of security standards even further than the game client—on the operating system itself. By restricting the hardware (or the “environment”) its games can run in, it can create hurdles for people developing cheats and botting software. This approach of tightly controlling the hardware the game is capable of running in is called **Environment Security**.

The aim is not to make it unhackable, since no software on Earth is unhackable. Rather, the aim is to add a new cost to running bot accounts, and to keep scaling this cost by blacklisting known vulnerable firmware and frameworks until the cost of botting offsets the profit developers can get from it.

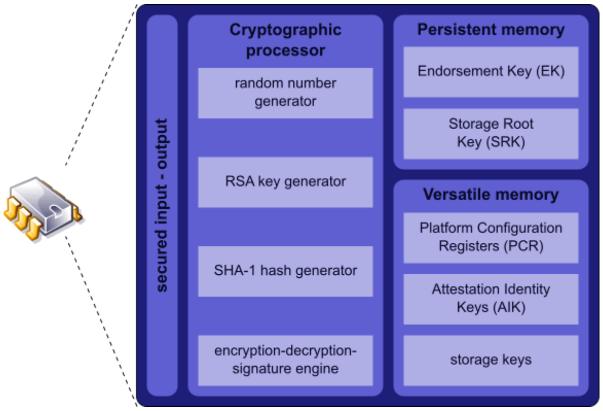
This is the main benefit of Vanguard running at ring0— it’s able to directly read memory and system calls to detect what hardware is currently present. It can identify vulnerable hardware and processes that would be invisible to other user mode software and block it from being used again.

This is how Vanguard intends to keep League of Legends from running within things like a virtual machine or docker container.

TPM 2.0

The way Vanguard uses to identify their environment is the Trusted Platform Module (TPM) 2.0 cryptoprocessor, which became a standard addition to all computers from Windows 11 and on.

It’s a physical processor inside most machines used to generate and store cryptographic keys, passwords, and other sensitive data used for verifying that your computer’s boot process starts from a trusted combination of hardware and software.



LoL x Vanguard uniquely comes with a TPM 2.0 requirement. While Microsoft originally intended to require TPM 2.0 to be enabled for all new Windows 11 installations, their actual implementation was relatively weak and easily bypassable, especially in pirated copies of Windows. Riot Games chooses to enforce the cryptoprocessor’s usage on their own, which caused a select few Windows 11 users may find their ability to play League is impacted, usually because their registry keys were modified in a way that TPM 2.0 identified their system as too vulnerable to boot.

Vanguard requires TPM for two reasons: The first is because it adds security to cert signing validation (something it relies on to know if other software can be trusted). The second and more important function, is because TPM is able to assign identifying hashes to hardware, which acts as an extremely non-fungible form of hardware ID. It becomes easy to detect hardware meant for botting or cheating, and if new hardware is developed they can easily add it to the blacklist. Since it's incredibly hard to change the TPM hardware ID, Vanguard can also just refuse to connect if your chip is in the cheater list, working as an extreme permaban on that piece of hardware.

Common Misconceptions

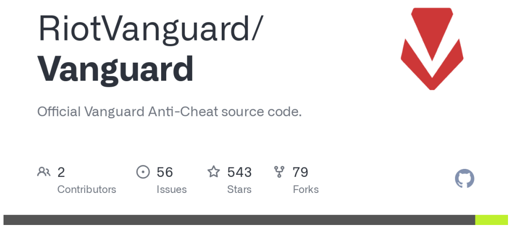
As a ring0 application, Vanguard's implementation and functionality have raised concerns amongst the player base. However, it’s important to be asking the right questions, and to deliver the correct criticisms. Let’s get some common misconceptions about Vanguard anti-cheat out of the way:

1. **Vanguard doesn't give Riot Games any user mode surveillance capabilities they didn't already have.** If they wanted to install a keylogger, spyware or a crypto miner, these things can all be done without Ring0 privileges, while inside a user-mode application. They could have been easily added onto Packman, since it was an anti-cheat users had very few interactions with, and barely anybody knew the inner workings of.

2. **Ring0 anticheats are not new, and Riot Games did not invent them.** Several third party anti-cheat systems—like

EasyAntiCheat, Battleye, Xigncode3 and PunkBuster—are already utilizing a kernel driver in the exact same way. Games that already use this technology include Apex Legends, ArcheAge, Arma 3, virtually all Call of Duty titles, Dead by Daylight, Helldivers, Genshin Impact, Fortnite, PUBG, Overwatch 2, Smite, Rust, War Thunder, and many, MANY more.

3. **Riot Games has put up bug bounties for Vanguard.** To reinforce their commitment to the new system, Riot Games has put up a bug bounty program for the anticheat. The program offers significant rewards—up to $100,000—for anyone who can demonstrate practical exploits leveraging the Vanguard kernel driver.
4. **Vanguard is completely open-source.** This means the entirety of the code is public for anybody to see, dissect, review and possibly contribute to. The uncompiled source code is here, which you can download completely for free.



RiotVanguard/
Vanguard

Official Vanguard Anti-Cheat source code.

2 Contributors · 56 Issues · 543 Stars · 79 Forks

5. **Vanguard itself has no connectivity to any server, and therefore, no use as a spyware tool.** Forensics on what the application is doing at any given time points towards it primarily conducting preventative checks upon booting to ensure Windows is in a trusted state. Once a game is launched, Vanguard merely confirms system integrity for gameplay and sends them directly to the League client, without transmitting files back to Riot servers. Koskinas asserts that data collection is kept to a minimum, with stringent retention rates and a focus on shipping queries to clients with binary responses (true or false).

Tencent腾讯

6. **Tencent is completely disconnected from Vanguard's development.** A common concern is the perception of Riot's ties to its parent company, Tencent, headquartered in China. Many players worry that due to the fact that Tencent operates within the People's Republic of China, Riot Games is subject to the National Intelligence Law of China. This law states that in the scenario where the Chinese government finds it necessary for its nation's state security, it is able to compel businesses that are registered or are operating in the People's Republic of China to divulge data regardless of which country that data came from and to do so clandestinely. Koskinas clarified that Tencent does not have access to Vanguard and highlights minimal interaction between the two companies. Tencent does not utilize Vanguard in China, mainly because they have different problems to solve. They instead use Tencent's anticheat, ACE. Their attack surface is huge and they

still have to support Windows 7, an operating system not supported by Riot Vanguard.

7. **Vanguard cannot alter BIOS settings.** Some niche bugs involved users' BIOS settings, which some rumors claimed were changed by Vanguard. Users are responsible for configuring BIOS settings as needed. Programs that are able to do this are usually incredibly secure, rare and specialized. Examples include things like utility tools for specific motherboards, such as ASUS. A tool like this has to be tailor-made for each specific motherboard, though. It'd be impossible to create a program that's authorized to change BIOS settings on such a wide array of motherboards and BIOS versions.

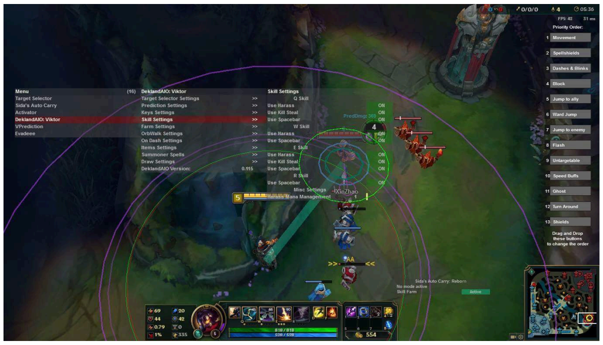
   For instance, one player had inadvertently enabled SecureBoot with a highly customized configuration. While Vanguard utilizes SecureBoot for Valorant, it is not employed for League due to potential compatibility issues with older hardware.

8. **Vanguard is not "running all the time."** The driver loads at boot and stays on for the entire session (just as any driver does), but nothing is making calls to it, and there's no network connectivity until you run one of Riot's games. It's literally just sitting there (menacingly), so that it can attest to the fact that nothing's happened between Windows loading and the game starting that would break the operating system.

   When you launch League, the Vanguard client contacts the driver to confirm that it thinks everything is 100%, and if so, you receive a valid anti-cheat session and may connect to the game server. Instructions from the client then start enabling features within the driver to watch for things that might tamper with the signed League process and prevent them. You can always disable the driver whenever you'd like-you'll just need a fresh reboot to "recertify" the integrity of the trust chain before you jump into the game.

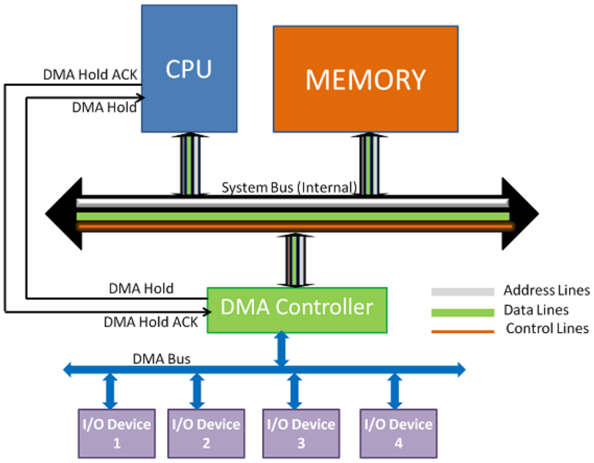
Vanguard's Limitations

Vanguard was designed to address a very specific brand of cheating. However, just like any other anti-cheat application, it can be circumvented. As the old saying goes, the only thing a 10 foot wall creates is a demand for 11 foot ladders.



Vanguard operates at the kernel level, allowing it to identify cheat software that also functions at this level or lower, which encompasses most cheats. However, some cheats may operate with elevated privileges, which can enable them to avoid detection.

For instance, DMA-based cheats employ specialized hardware can access system memory directly, circumventing standard detection methods that monitor external processes. Likewise, scripts made with Auto Hot Key and Pixel bots can automate gameplay actions in a way that closely resembles human behavior, enabling them to bypass Vanguard.



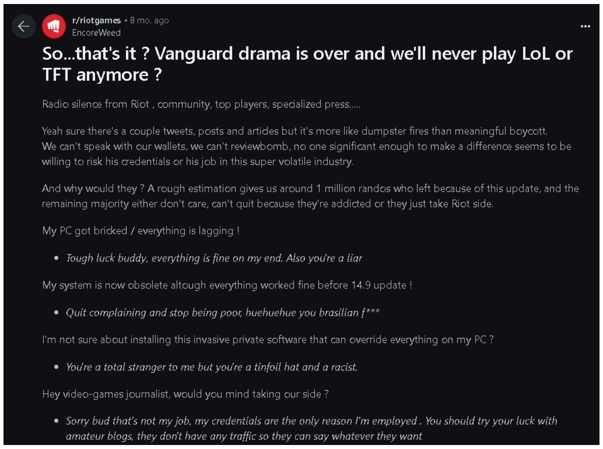
On the other hand, external or hardware methods of cheating, such as modified mice or cheat-specific devices, can completely evade software detection. As cheating algorithms continue to evolve, it raises the question of whether a kernel-level anti-cheat driver like Vanguard can effectively counter the occasional kernel-level cheats. This challenge is common across all competitive gaming environments.

Riot Games has faced difficulties in addressing new cheats. Koskinas pointed out DMA-based cheats, which often use external hardware to subtly inject cheat code into gaming systems. Nick 'Everdox' Peterson has dedicated nearly six years to researching this technology, and his knowledge has helped Riot stay ahead of the most significant threats.

Player's Perspective

For many players, the question of whether Riot Vanguard is safe comes down to balancing privacy and security with the need for a fair, cheat-free gaming environment. The majority of Valorant players seem to have fared just fine during the earlier versions of Vanguard.

However, there remains a vocal group of players who are uncomfortable with the idea of kernel-mode access, no matter how necessary it may be for stopping cheats. They argue that the risks, while minimal, are still present, and that the gaming industry should focus on developing anti-cheat systems that don't require such deep-level access to users' computers.



r/riotgames • 8 mo. ago
EncoreWeed

So...that's it ? Vanguard drama is over and we'll never play LoL or TFT anymore ?

Radio silence from Riot , community, top players, specialized press.....

Yeah sure there's a couple tweets, posts and articles but it's more like dumpster fires than meaningful boycott.
We can't speak with our wallets, we can't reviewbomb, no one significant enough to make a difference seems to be willing to risk his credentials or his job in this super volatile industry.

And why would they ? A rough estimation gives us around 1 million randos who left because of this update, and the remaining majority either don't care, can't quit because they're addicted or they just take Riot side.

My PC got bricked / everything is lagging !

- *Tough luck buddy, everything is fine on my end. Also you're a liar*

My system is now obsolete altough everything worked fine before 14.9 update !

- *Quit complaining and stop being poor, huehuehue you brasilian f****

I'm not sure about installing this invasive private software that can override everything on my PC ?

- *You're a total stranger to me but you're a tinfoil hat and a racist.*

Hey video-games journalist, would you mind taking our side ?

- *Sorry bud that's not my job, my credentials are the only reason I'm employed . You should try your luck with amateur blogs, they don't have any traffic so they can say whatever they want*

This is a universal issue for all anti-cheat software, however. The fact that people single out Vanguard is not a testament to how invasive it is, but rather a testament on how good other anti-cheat systems at hiding how invasive they are.

People Are Still Cheating— so What Gives?

From a technical standpoint, the anti-cheat team has gone to great lengths to ensure that Vanguard doesn’t compromise users' security or privacy. Their bug bounty program and transparency efforts help reinforce their commitment to a safe anti-cheat solution. However, ANY kernel-mode driver inherently carries risks, and it’s up to individual users to decide whether they trust developers to manage these risks responsibly.

For now, Riot Vanguard *appears* to be incredibly effective at stopping cheaters, while maintaining a respectable degree of transparency. There’s still a possibility for a time where Riot Games could choose to go for less transparent solutions, but as of 2024, Vanguard remains more transparent and stable than most other anti-cheat systems like PunkBuster or EasyAntiCheat.

However, an absence of evidence is not evidence of absence. Riot Games has shared that the release of Vanguard coincided with a drop in bans related to things like botting or scripting, along with an ensuing drop in how many of these cases are being detected. Many players will insist that botting and smurfing is still very much alive in the community’s ecosystem. It’s very much possible that the drop in bans coincides with a drop in cheating, but it’s also possible that it coincides with Riot now dealing with cheating that is undetectable to their current methods.

This, again, is a natural thing that happens with all anti-cheat systems. The modern philosophy of anti-cheat software is not to eliminate cheating through making the program itself unhackable. The aim is to make it as costly as possible to do so, making the business that supports cheating unsustainable.