The video game industry is a black hole for cybersecurity. Compared to banks or ecommerce, store passwords are robust and making it difficult to crack compared to places that only require credential stuffing attacks. Most video game companies use low-friction authentication measures since friction drives customers to turn away, which results in loss of revenue. Cloudflare for Gaming tackles the issues that most companies within the videogame industry have: security.

To note from the consumer perspective who plays videogames: gaming is seen to have low financial risk, which results gamers to use less secure passwords. Note that the consumer's base for most video games is mainly people in elementary school to people in high school and they are less likely to use secure passwords, which result in security issues through these accounts.

And the consumer base use forums to learn more about these games and unfortunately it is up to the forum administrators to update patches and maintain security, which results people to hack into video game forums and most people reuse passwords, so not only accounts that are attached to the forum are affected, but accounts from other industries get attacked.

One company that has been successful in employing these measures of security is Microsoft as they managed to deploy vigorous security measures with Xbox as well as the rest of its business, which results in Xbox credentials on the dark web, and Microsoft is restricted in providing security to Xbox and its consumer base. Cloudflare can easily provide that type of security to not only one company, but multiple companies.

Cloudflare Workers for Gaming will be essential for companies that plan on expanding their servers into other games. Companies such as Riot Games, Blizzard, Nexon, and so on would face many issues when it comes to deploying a new game or a massive update into one of their games, which result in affecting the entire server for the other games that they hold.

In fact, recently Riot Games had issues for a whole day when they deployed Legends of Runeterra to the public, and it forced others who were playing League of Legends or Team Fight Tactics to not play within a team that they can queue into because of the number of users that were playing Legends of Runeterra. Similarly, with Team Fight Tactics when it was first released, for a couple of days it failed to put players in games and in fact, put them in queues that can last up to an hour. As companies like Riot Games that rely on servers in terms of deployment, they face a huge issue when they decide to release new games or updates that change the scene for the company. With that, Cloudflare Workers for Gaming creates an opportunity for these companies to handle these servers.

There is one particular issue with Cloudflare for Gaming though: if someone were to breach its security for one company that uses it, it could affect the other companies that use it as well since patterns would persist among the security measures used through Cloudflare for Gaming. But, the product uses machine learning to learn about any DDos or security breach that it can make up as well and can update the tight security that Cloudflare for Gaming has to offer.

Through Cloudflare for Gaming, companies can focus on creating products rather than focusing on security, which relieves a lot of pressure to produce products that are secure. The product can address some of these security issues for the company without having the company to compromise them delivering more products at a fast pace. Cloudflare addresses these issues and will be the forefront for companies within the gaming industry to use.