Arkose Labs

Level Up: Protecting Online Gaming Against Fraud

Keep the hordes of bad guys out while giving users a good game.

The Gaming Industry's Meteoric Rise

The video game industry has undergone a drastic evolution during the digital age. 40 years ago, the Atari 2600 was the pinnacle of gaming technology. Today, gamers have powerful consoles from Sony and Microsoft, as well as PCs, with 4K video quality and photo-realistic graphics; ultra-fast streaming services from Google and Apple, and even smartphones that can play games which 15 years ago required bulky physical consoles to run.

Perhaps no industry has matured as quickly and as rapidly over the past few decades as gaming. Parents who grew up playing video games now play with their children, and even older adults (55+) whittle away many hours playing popular mobile games, often being taught by and playing with their grand children.

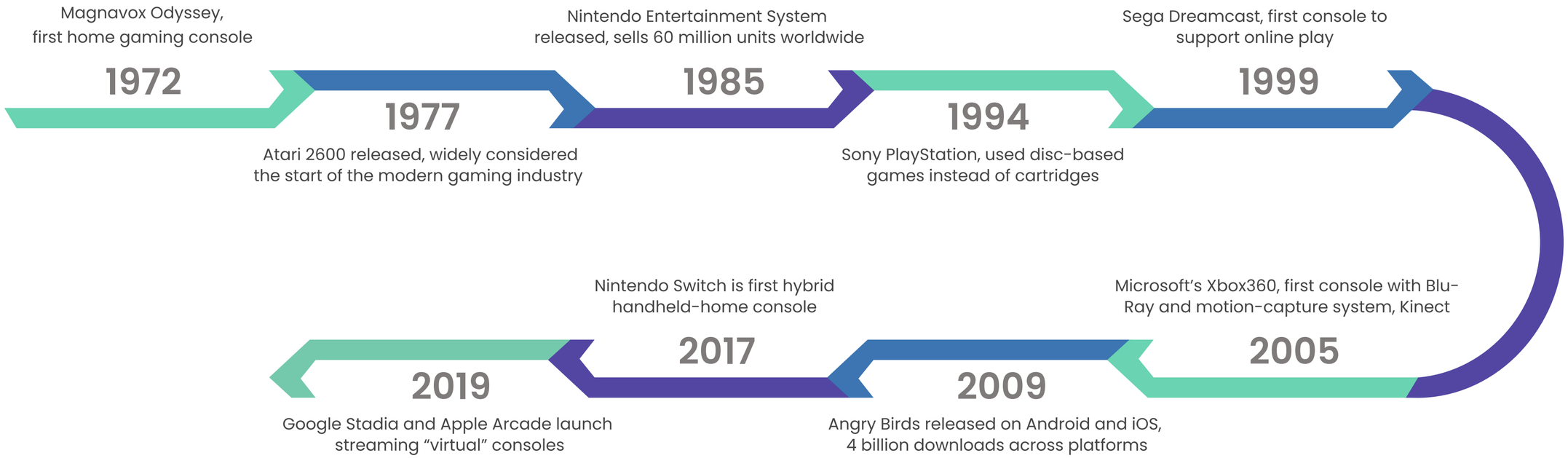
Gaming has grown far beyond a singular, self-contained experience. Most games attract thousands or even millions of players from around the world competing in online platforms, replete with intricate in-game economies, social structures and world-building possibilities. It's estimated there are about 2.2 billion gamers, or about one-third of the world's population.

It's a highly competitive industry, and to capture the attention (and dollar) of today's busy gamer, companies need to offer the most user-friendly platform and experience.

Gamers Flock to Online Worlds

Online gaming has been around in some form for more than 20 years, but it has now suprassed offline gaming in popularity. Gamers interact with others from around the world in a digital setting and build alliances, fight enemies and buy and sell digital goods.

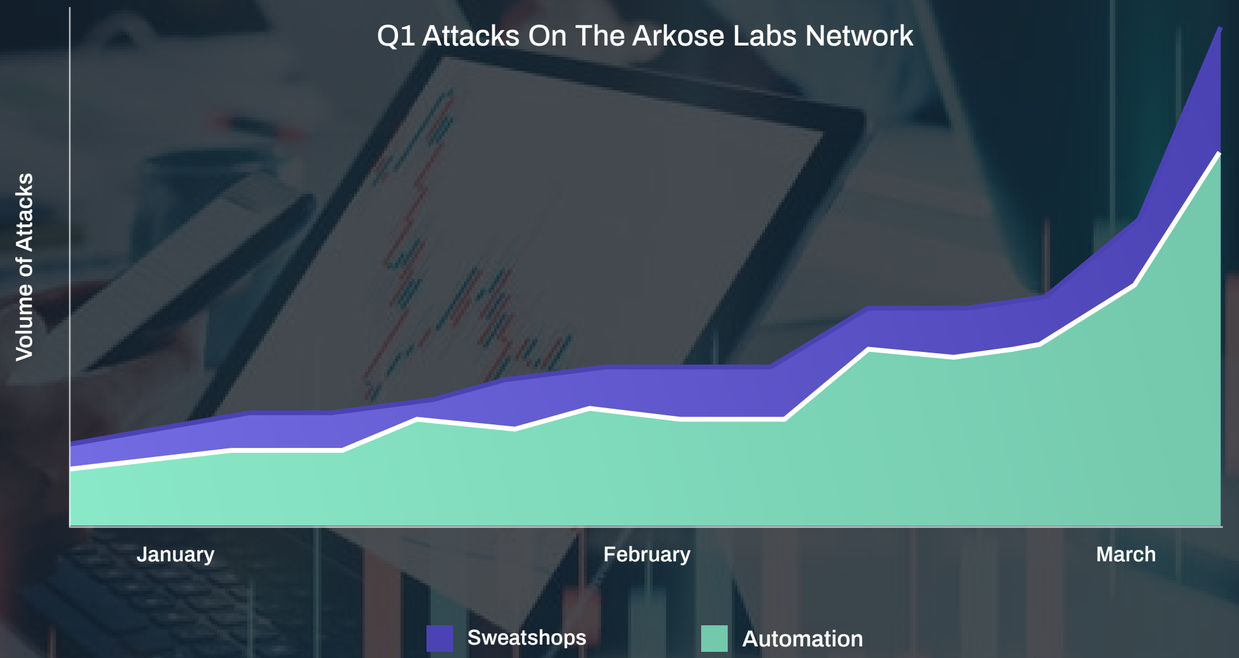
According to recent data, around 700 million people around the world play games online. For many, online gaming doesn't even involve their own direct participation. People aged 18-25 are spending 77 percent more time watching online gaming on platforms such as Twitch than traditional sports on television.



A Ripe Landscape for Fraud

This explosion in popularity and traffic has not gone unnoticed by fraudsters. The massive shift to online gaming platforms means ample opportunities for bad guys to attack. Furthermore, the huge adoption of free-to-play games, many which have millions of daily active users, also create ample opportunitie for fraudsters to attack.

According to data from the Arkose Labs network, transactions on gaming platforms grew 21% in Q2 of 2020, while there has also been a 23% rise in attack rate against gaming networks during that same time period. Attacks against gaming have also risen daily since the beginning of COVID-19 related lockdowns, eschewing the old normal patterns of high traffic during weekends and low traffic during weekdays. This new paradigm can be expected to remain even after lockdowns ar lifted, as more people permanently shift to remote work or school.



Many Different Attack Vectors

Since online gaming ecosystems are so complex and intricate, there are many different ways for fraudsters to exploit them for their own gain. These include new account registration fraud, account takeover attacks, payments fraud, auction house abuse and other manipulation of in-game economies, and much more. Some of the most sophisticated and complex fraud attacks seen today in any industry are those targeting gaming segments. Attack rates are on a steady rise and will only continue to increase.

Gaming platforms have several areas that attackers can exploit and monetize

Bot-Powered Abuse and Theft

In-game currency or items can be stolen or amassed at scale via hundreds of bot-powered accounts. Fraudsters deploy bots en masse to perform new account fraud and use these fake accounts to initiate and complete gaming sessions in order to collect in-game currency. They are also used to disrupt the gaming environment and ruin the experience for legitimate users of the platform. These fraudulent accounts can further take advantage of promotional offers at scale.

Account takeover and resell

Online gaming faces distinct challenges around account takeover attacks. Attackers break into accounts to steal payment credentials, resell in-game assets and even resell the account to provide a way of bypassing the true cost of purchasing a game.

Spam and malicious content

Bad actors can create fake profiles to send spam and malicious messages to real users. Or they can downvote videos or other user-created content. Sometimes this isn't even done for monetary gain but simply "griefing," — the act of harassing or targeting other players online.

Collusion

Collusive play allows bad actors to manipulate the outcomes of games using a series of associated accounts. This can lead to huge fraud losses and frustration for trusted users who are trying to enjoy the game.

Keeping the Most Vulnerable Safe

While video games have long moved past just being a hobby for kids, the fact is that children are still among the biggest segment of gamers. They are also among the most vulnerable. That's because they are more susceptible to the tactics used by fraudsters that adults may be wary of.

For example, children may not be as aware as adults of the importance of keeping sensitive information, such as log-in credentials or payments information, private. They may be more likely to fall for scams perpetrated by bad actors such as phishing messages or clicking on malicious links. A 2019 report from Experian found that cybercriminals are increasingly targeting children in online gaming platforms. The old adage "don't talk to strangers" has never been more relevant.

While some onus is, of course, on parents to educate their children about safety practices online, gaming companies must take every measure possible to protect minors that use their platform.

A Holistic Approach to Protecting Gaming Platforms

All of this is why gaming companies need a more nuanced, layered approach to protecting their users and their business. They need to accurately distinguish fraudsters from genuine users and incrementally deplete the returns from the attack.

Online gaming platforms need to utilize technology that will enable them to gain in-depth insights into attacker activity and assign appropriate risk profiles. Depending on the risk assessment of traffic, each individual user is identified and classified as malicious or genuine, and the appropriate countermeasures are then deployed.

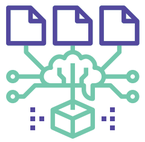
This kind of nuanced approach is not only effective at fighting fraud, but also reducing false positives and maintaining a great customer experience. Instead of blocking potentially good users, no one is outright blocked; instead suspicious traffic is fed increasingly time-consuming authentication challenges. This is especially critical as the massive amount of traffic to gaming sites makes it easier for the bad guys to blend in with good traffic.

Analytics And Machine Learning

Customer Interaction Assessment

Anomaly Detection

Historical Attack Patterns

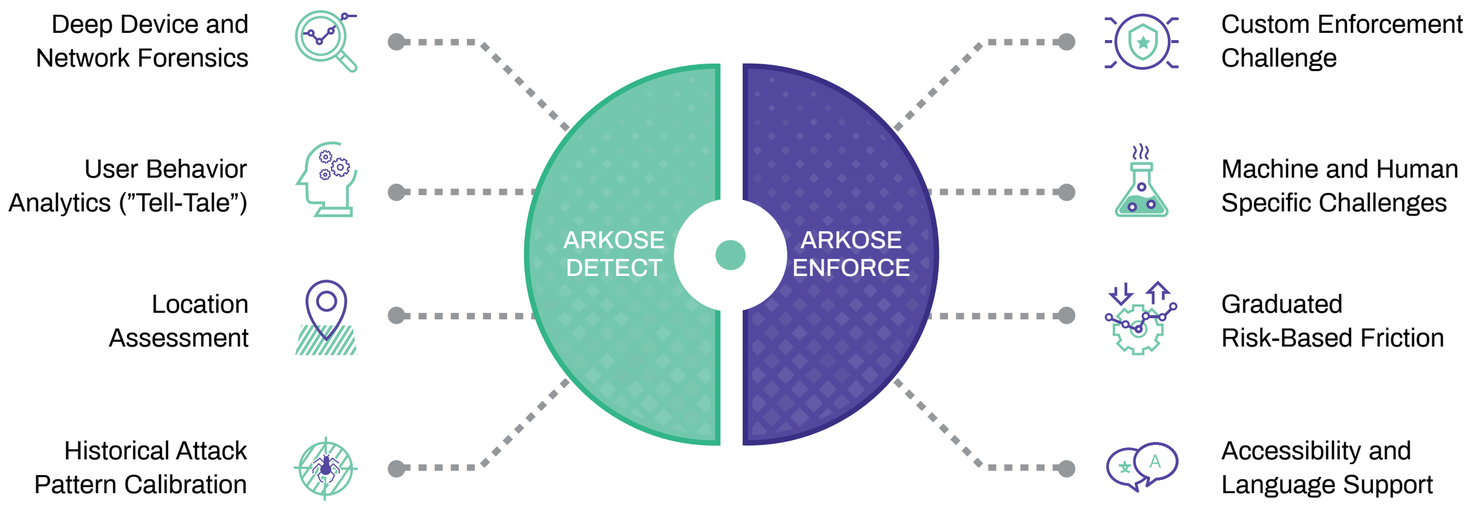


Traffic Pattern Analysis

Game Over for Fraudsters

The Arkose Labs platform takes a two-pronged approach to segmenting and authenticating traffic. Arkose Detect is a dynamic risk engine that assesses behavioral patterns of users across devices and networks to assign a risk profile. Arkose Enforce then presents authentication challenges to suspicious traffic. The platform is continually evolving and utilizes machine learning to analyze data from user sessions in real-time to help recognize the context, behavior, and past reputation of every request and assign a risk score.

Meanwhile, Arkose Enforce delivers adaptive step-up challenges after Detect accurately distinguishes between authentic users, malicious humans, and bots. The 3D challenges are rendered in real-time and gradually increase in difficulty depending on the associated risk of the user. This increases the time required to solve them and wastes the fraudster's resources. Since increasing costs diminish the profitability of the attack, fraudsters are compelled to stop.

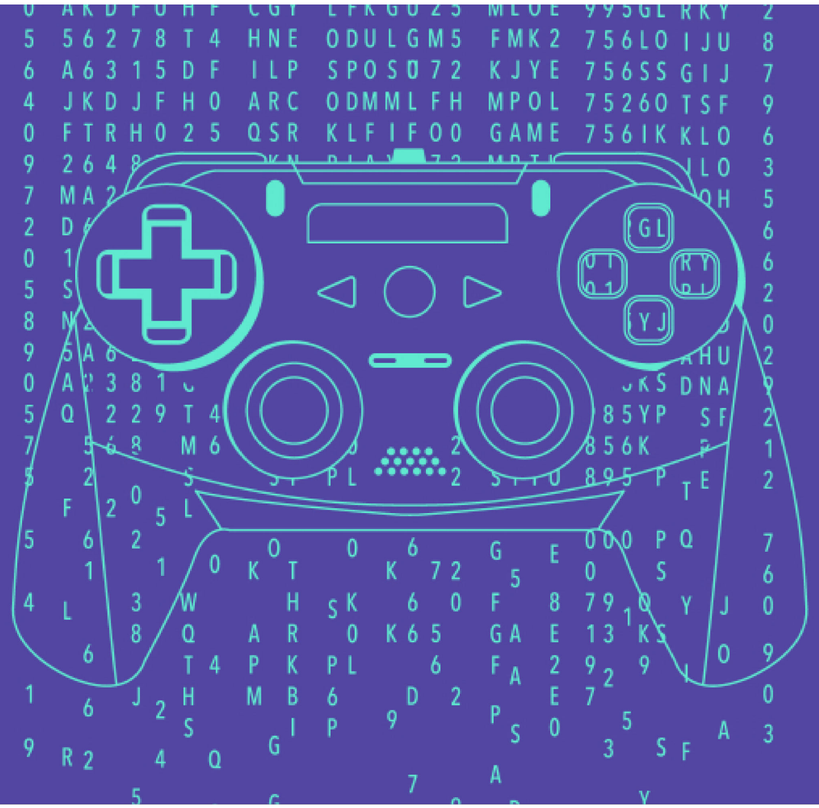


Arkose Labs Solution for Online Gaming

The two components of the Arkose Labs platform work seamless together in tandem using real-time risk analysis of traffic and enforcement challenges to stay ahead of attacks. This is how the Arkose platform is able to constantly identify and react to an evolving threat landscape. Deploying machine learning further sharpens anomaly detection and trains the platform in real-time, with the challenge as the feedback loop. The platform is also informed by trends seen across our entire customer network across industries.

Designed With Gamers in Mind

In many ways, the Arkose Labs platform was optimally designed for the gaming industry. The technology was built from the outset with interactive entertainment design principles in mind. This gamification aspect to the authentication challenges makes them different from any other kind currently on the market. Not only should good users — if they see them — be able to solve the challenges quickly, but they will have a fun time doing so.

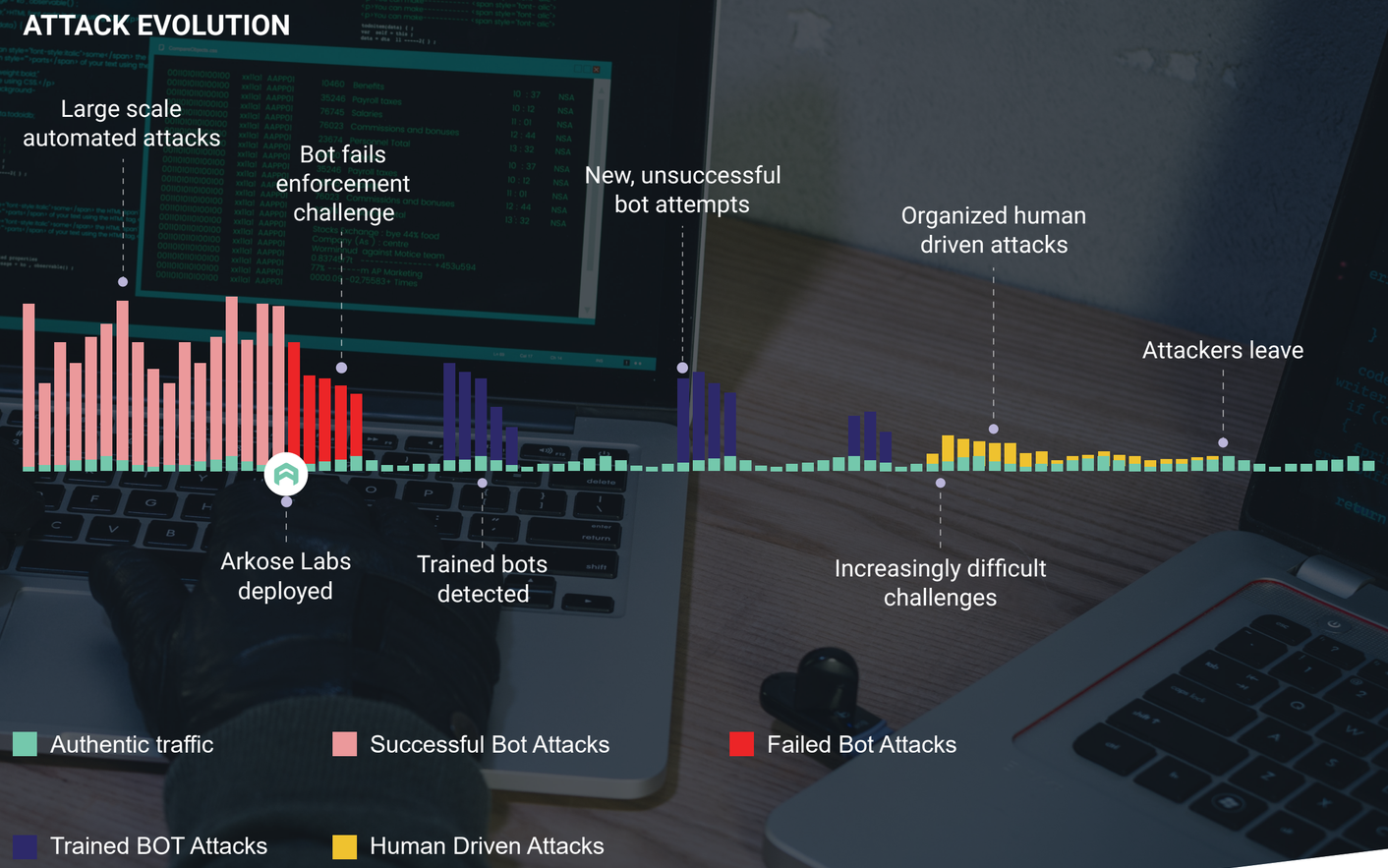


Let them Attack Us, Not You

As one of the most highly-trafficked industries that is only increasing in popularity, it is critical that gaming companies don't get overwhelmed by volume. Servers crashing or interruptions in gameplay will lead to dissatisfied — and often angry — customers. Not only will these users abandon the platform, but many will take to social media to share their frustration, which can lead to a negative brand perception.

Arkose Labs' approach shifts the attack surface from the business to Arkose Labs' independent platform. By shifting the attack surface, internal fraud and IT teams are freed up to be deployed on other resources while we take care of the bad guys.

As a result, fraudsters are no longer attacking their targeted customer touch point but are diverted to an intelligent step-up authentication challenge that saps their time, money and resources. It should be noted that these are white label challenges; they will appear brand-affiliated with the gaming company so as not to disrupt the experience for any good users that may see them.



Conclusion: The Time to Act is Now

Now is a critical time in the gaming industry. More and more people are online playing games than ever before and traffic is at record levels. These are habits and trends that will continue for the rest of their lives, meaning that gaming companies need to be prepared for ever-increasing volume and the fraud that comes with it. It's imperative that gaming companies future-proof their business now with a platform that continually evolves and adapts to meet any threat, now or in the future.

As more and more people every day continue to adopt and increase their usage of online gaming, this puts the industry directly in the line of fire of fraudsters. Stopping the fraudsters at the front door before they can target gamers, while at the same time keeping the user experience as smooth and friction-free for legitimate customers, is how gaming platforms will survive and thrive now and going forward. The ones that are able to do this most effectively will be the winners that emerge from this crucial crossroads as clear market leaders.

In many games, it only takes one mistake for the player to lose all progress and return to the beginning. For gaming companies this is an apt metaphor; even one successful fraud attack can drive away customers and undo positive business growth. The time to act is now.

Arkose Labs

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Sales: (800) 604-3319

Offices

San Francisco
250 Montgomery St 10th Floor, San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane, Queensland AU